AIR WAR COLLEGE

AIR UNIVERSITY

ACQUISITION REGULATIONS

AND

OFFSHORE SOFTWARE DEVELOPMENT:

IMPLICATIONS FOR CYBERSECURITY OF DOD NETWORKS

by

Roman L. Hund, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. George J. Stein

14 February 2013

DISTRIBUTION A. Approved for public release: distribution unlimited

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Biography

Lieutenant Colonel Roman Hund is a U.S. Air Force cyber operations officer assigned to the Air War College, Air University, Maxwell AFB, AL. He graduated from the University of Minnesota with a Bachelor of Science degree in Mechanical Engineering and the University of St. Thomas with a Bachelor of Arts degree in Engineering in 1992. In 1996 he completed his Masters in Administrative Science at the University of Montana. He has served at both the MAJCOM and the Joint Staff level. He has completed successful tours as Mission Support Group Deputy Commander and Communications Squadron Commander.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Abstract

Malicious code, such as Zero-day exploits, utilize vulnerabilities in Commercial-Off-The-Shelf (COTS) software to cause damage in cyberspace. Because of the prevalence of offshore software development, COTS software is exposed to increased vulnerabilities and provides access for our adversaries to manipulate software code. Defense networks are built primarily on COTS products and software because our acquisition rules are focused on streamlined procurement of COTS Information Technology (IT) products in Federal government organizations. This paper will show that updates to our Federal Acquisition Regulations (FARs) could increase our understanding of the origin of software code and provide access to source code for in-depth vulnerability analysis providing improved cyber security.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Introduction

Current acquisition rules open the potential for increased Zero-day exploits on Department of Defense networks because of the globalization of the commercial software development process and the access this globalization provides to foreign competitors.

News headlines are filled with claims of cyber security and Zero-day vulnerabilities in commercial software. Java is a software product that is loaded on most everything connected to the internet from television set top boxes to computer web browsers that allow these devices to interface to internet servers in a virtual environment. The Department of Homeland Security (DHS) released a notification that Java software contains vulnerabilities that allow complete undetectable control of the device from a remote system.

Oracle Inc., the company that owns Java, didn't acknowledge the existence of this vulnerability until weeks after it was notified by the DHS.[1] A recent Computerworld article claimed Oracle Inc did finally patch its Java software; however researchers quickly pointed out that their patch itself was flawed.[2] Adam Gowdiak, founder and CEO of Security Explorations, has reported dozens of Java vulnerabilities to Oracle over recent years. He argued that Oracle has been guilty of sloppy work[3]. Andrew Storms, director of security operations at nCircle Security, stated, "Obviously, there's something broken in the Java development or design cycles."[4] These comments point to the software development process at Oracle as a part of the problem.

To make this issue more complex, software development teams at Oracle include of software programmers located in the United States and abroad. IT Outsourcing India, an organization that develops high quality software solutions in India, makes the claim that Oracle has their largest software development centers in India.[5] Most commercial software development processes

include some software coding from internal or external software development teams located off-shore.

This paper will show that the lack of understanding of the origin of software code in the software development process leads to increased vulnerabilities. Providing access to the software development process allows foreign competitors access to software code which may provide them with knowledge of vulnerabilities or the means to create vulnerabilities in the software code. These vulnerabilities might not be identified until long after they have been used to exploit systems. The Defense Science Board (DSB) Task Force on Mission Impact of Foreign Influence on DoD Software points out that, "…COTS development environments are more porous to attack than those of DoD custom development environments...The risk of damage from maliciously introduced vulnerabilities increases with the ease of adversarial access to the development environment."[6]

Because of our federal acquisition rules, we built defense networks primarily on COTS devices and software. The Federal Acquisition Regulation (FAR) language allows program managers to procure software with little understanding of how or where the software was developed. The GAO report on Defense Acquisitions, Knowledge of Software Suppliers Needed to Manage Risk, May 2004 states, "DoD's approach to software development and acquisition generally focuses on improving overall quality, leaving decision making on software suppliers and security with individual program managers. Despite the risks associated with foreign access to defense systems, DoD acquisition policy does not require program managers to identify and manage the amount of foreign involvement for software development in weapon systems. DoD information system security requirements focus on operational software threats, rather than potential threats posed by software developers."[7]

Digital Collections

Zero-Day Vulnerabilities

Zero-day vulnerabilities are defined as "an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability." This means that developers have had zero days to address and patch the vulnerability. "Zero-day exploits (actual software that uses the security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability."[8]

Zero-day exploits offer the attacker knowledge of a vulnerability before software developers can address the issue. The vulnerability could be a code flaw that is intentional or unintentional and may not look like malicious code. Intentional or unintentional malicious code is exploitable by those seeking to gain an advantage in cyberspace. Symantec presented a report on Zero-day exploits that shows hackers exploit Zero-day exploits for an average of 10 months before they are exposed.[9]

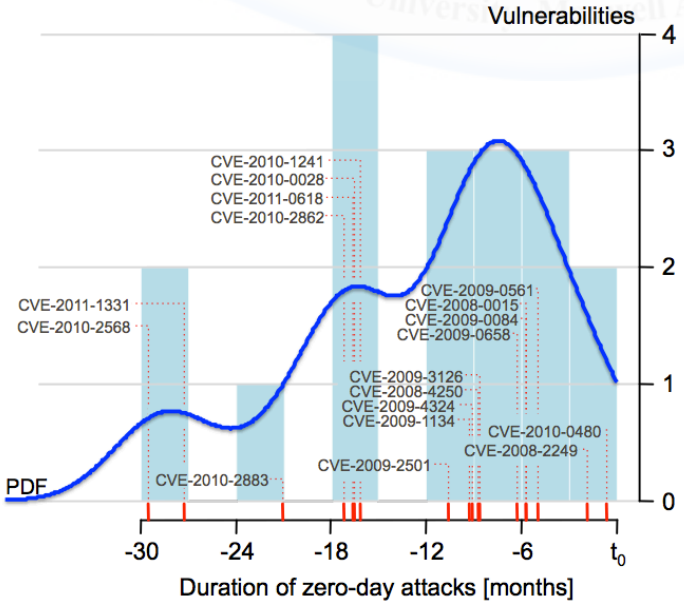
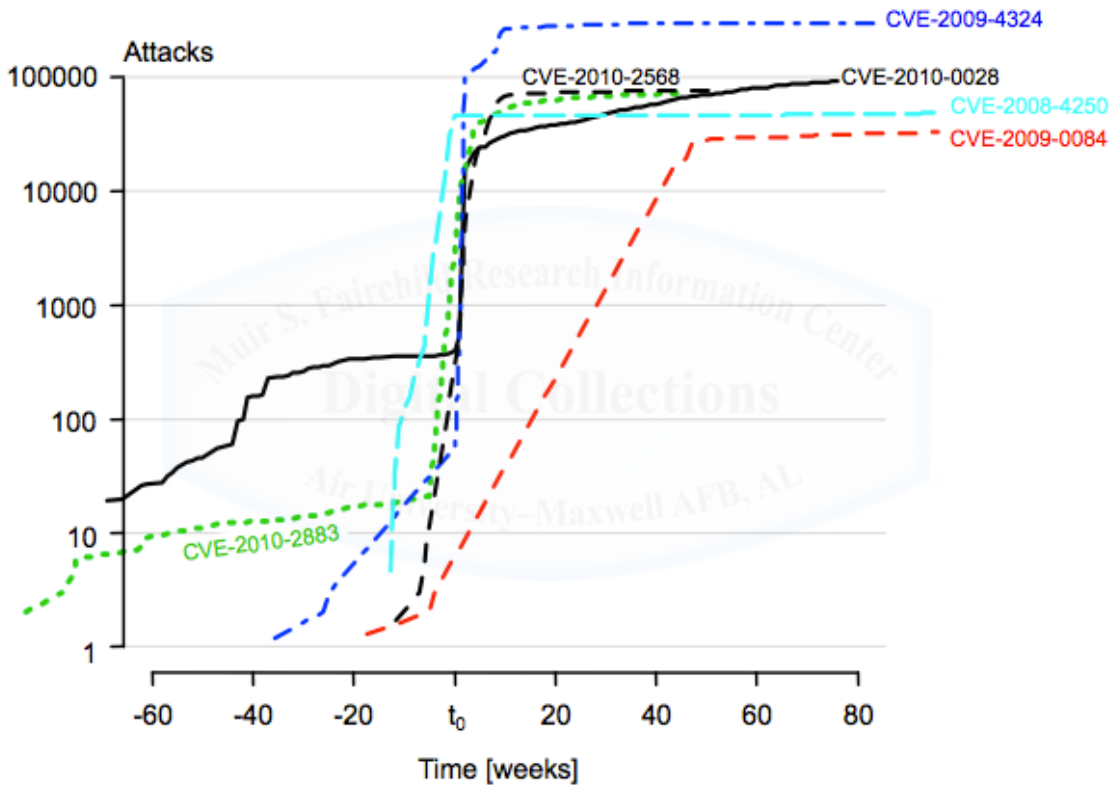


Figure 1. Duration of Zero-day attacks over time in months[10]

In the Java example introduced earlier in this paper, the attacker could have full control of the exploited device for months before the public could respond by creating a method to detect and/or mitigate the problem. The attacker could use a keylogger that records passwords, access bank accounts, or log into virtual private networks to gain more restrictive information. Figure 2 shows that hackers use these exploits hundreds or thousands of times around the time of their revelation to the public.[11]



(a) Attacks exploiting zero-day vulnerabilities before and after the disclosure (time = t_0).

Figure 2. Number of Zero-day attacks using exploits over time (in weeks)[12]

The spike shown in figure 2 indicate the explosion of attackers and attacks up to and after it is disclosed to the public. The vulnerability window for zero-day exploits starts when a developer creates software containing an unknown vulnerability (or known if intentional). The

attacker finds the vulnerability before the developer does (or while the developer is aware of but has neglected or been unable to fix it).[13]

Zero-day exploits are being sold through an underground market from "benevolent hackers" who find and report bugs they identify and hackers that are looking to cash in on their skills. In a recent Slate article, Adriel Desautels, a Zero-day exploit broker that has sold exploits for $16,000 to $250,000, was quoted saying "some legitimate companies operate in a legal gray zone within the Zero-day market, selling exploits to governments and law enforcement agencies in countries across the world." Brian Krebs, a former Washington post reporter stated, "Most organizations are one Zero-day away from compromise, if it's a widely used piece of software, you've just got to assume these days that it's got vulnerabilities that the software vendors don't know about—but the bad guys do."[14]

Offshoring Software Development

Offshoring is work that is done for an organization at a site that is in an overseas location. For the purposes of this paper, overseas is defined simply as crossing a border from one country to another. In other words, work can be offshored from the United States to Canada or Mexico.

Software development is defined simply as the process of creating software and can be divided into several activities or tasks. These tasks include: analysis, design, coding, testing, implementation, maintenance/support, project management, localization, and research and development.[15] Organizations that participate in offshoring will implement their approach to offshoring in many different ways. Some organizations offshore specific activities while others will move entire projects or processes.

Software development sent offshore is separated in to six categories (Table 1). This paper is focused on the first category; programming, software testing, and software maintenance. At this

Air S. Fairchild Research Information Center
Digital Collections

level, the offshore organization has access to the software development process and source code for software.

Table 1. Categories of work sent offshore[16]

1	Programming, software testing, and software maintenance
2	IT research and development
3	High-end jobs such as software architecture, product design, project management, IT consulting, and business strategy
4	Physical product manufacturing – semiconductors, computer components, computers
5	Business process outsourcing/IT enabled services
6	Call centers and telemarketing

Muir S. Fairchild Research Information Center
Digital Collections
Air University
Maxwell AFB, AL

Recent studies show that developed nations are primarily involved in the offshoring of work from their nation to other countries. The United States has historically dominated and continues to dominate the software and services industry, with about 80% of global revenue. The United States followed by the United Kingdom have been the largest offshorers, but countries in Western Europe, Japan, Korea, Australia, and even India send work offshore.
Western nations and India are handling the bulk of the in-house offshored work. India, Eastern Europe, and China are the leaders in performing the outsourced work.[17]

The DSB Task Force on IT Acquisition found that foreign sources of supply are rapidly growing, with notable increases in offshoring to India, Russia, and China. According to a 2007/2008 survey of 418 corporations, software and product development are the highest offshored functions, with over 70 percent of the software industry now offshoring. The survey also found that over 50 percent of companies are offshoring software development and over 30

percent new product development.[18] In an Internet survey of the Top 86 U.S. software firms identified by Software Magazine in December 2004, 48 firms had R&D facilities in India, while 14 had facilities in China, and only three were in Russia. However, in the 2012 Global R&D funding forecast showed that 35% of US offshore R&D operations went to China and 26% to India (Russia was not significant in this report).[19] These numbers include all R&D and not just software development. However, the trend is clearly shifting from India to China.

India is the world's largest engine for software development and has grown from simple coding in the 1970s to a leader in all areas of software development since the early 2000s. The Association of Computing Machines (ACM) study credits the work necessary for the United States and the world preparing for the Y2K problem for helping India's industry growth. Software and service export firms in India are growing at 20-25% per year according to the best statistics available.[20] India's largest export is software services.

Russia is noteworthy in this market because software was a relatively neglected field during the Soviet era, but in the 1990s as the country transitioned to a market economy, many scientists and engineers moved from low-paid government and university positions into entrepreneurial firms and Russian subsidiaries of multinationals; and some of these people entered the software field. So far there are relatively few programmers, but wages are low, and technical skill is high.[21] According to the 2006 ACM study, China does not currently have a major impact on the world software economy and the industry is highly fragmented into many small companies. Most of the offshoring in China is in the hardware industry. This may drive the Chinese software industry to focus on software embedded in hardware. Politically, the ACM study found that China was the most protectionists in its trade policies and there have been clear concerns of intellectual property rights infringement.[22] These political realities cause many businesses to

find other offshore software development locations. However, it is clear that the trend has shift in the past 6 years and China is quickly catching up to India and may surpass them in software development in the coming years.

COTS Software is Everywhere

The government clearly made a change in the 1990s to bring more military capability to the DoD through procurement of COTS products. Information Technology (IT) procurement was targeted as an area to streamline through the purchase of COTS products including software.[23] The focus of the attention on COTS was to make it easier to keep up with changing technology and for the IT community in the DoD to build out networks on flexible and interoperable commercial standards.

The Defense Science Board Task Force report on Mission Impact of Foreign Influence on DoD Software identified that, "COTS software producers may or may not know, manage or track the provenance of their software, except to the extent needed to ensure that the necessary license are obtained for embedded components. In addition, they generally do not make source code available, so supplier identity and software content is often blurred by the reuse of legacy code, subcontracting, outsourcing, and use of Open Source Software (OSS)."[24]

James A Lewis in his report, Foreign Influence on Software, states, "The DoD, the intelligence community, and very often the leading infrastructure companies once wrote almost all of the code they used, but today, only the most highly classified code is written at places such as the National Security Agency. Changes in defense industrial capabilities and the rapid pace and broad scope of technological change mean that the military and other government agencies are increasingly dependent on COTS software."[25] Lewis' article points out that inserting malicious code is an extension of existing operational techniques used by foreign intelligence

agencies. He also asserts that malicious code inserted surreptitiously by an insider during the software production process could be an effective element of a larger intelligence collection program or information warfare strategy.[26]

In open source research, zero-day exploits are only found to occur in COTS software. There is potential for exploits to be built for Government Off-the-shelf (GOTS) software, however there is little access to this software and COTS software offers more exploitable vulnerabilities. COTS is everywhere, including systems that are being used within defense networks. Air Force doctrine documents (AFDD 3-12) state that COTS technology presents 3 primary vulnerabilities in cyberspace; foreign ownership, control, and influence of vendors, supply chain, COTS and GOTS balance. The vast majority of the Air Force cyberspace operational components and capabilities are from COTS.[27]

Foreign Competitors

Bob Violino, in a recent InfoWorld article, identified the software industry as a battleground in the cyber war.[28] He quotes Pat Clawson, CEO of security products vendor Lumension, "we can expect to see more attacks against trusted software providers such as antivirus vendors. Attackers want to get to the unparalleled access to antivirus vendors customers. Once the antivirus vendors' payloads are compromised, the devastation could be staggering."[29] The countries most involved in the offshoring of COTS software development that our largest global competitors are China and Russia. Although India is the largest offshore actor in software development, there is very little documented malicious activity originating from India. In fact, India seems to be one of the larger targets of malware.

The 2010 Symantec Intelligence Report showed that China is the host of more than 30% of malicious attacks.[30] A recent Microsoft investigation, dubbed "Operation b70", identified

Air Force S. Fairchild Research Information Center
Digital Collections

malware embedded in counterfeit versions of Microsoft Windows Operating System. It was engineered to spy on users and conduct denial of service attacks. This software was resident on laptops and computers sold in China by Chinese companies.[31] Project 2049 Institute's report on countering Chinese Cyber Operations states, "from a military perspective, Chinese PLA authors view cyber operations as a basis for modern warfare. Chinese Computer Network Operations (CNO) often is placed in the context of information security, or 'network attack and defense,' based on the premise that 'without understanding how to attack, one will not know how to defend.'"[32] In a recent Pentagon report, U.S. Intelligence agencies called China's cyber-espionage a "persistent threat to U.S. economic security." Two U.S. house members went further stating, "Every morning in China, thousands of highly trained computer spies now wake up with one mission: Steal U.S. intellectual property…"[33]

Russia has had ties to malware for years. Bill Brenner's article, "How Russia became a malware hornet's nest," questions why people from that part of the world are so determined to earn a living writing attack code. From earlier in this paper, the high tech and scientific workforce in Russia is underutilized. Eugene Kaspersky explained that many Russian programmers compare themselves to weapons manufacturers—they build the technology but are not the ones using it. He also feels the Russian economy is shaky enough that people are looking for a steady living and building malware is one way to do it.[34]

Acquisition Rules

At the national level, there are two important trade acts that influence the government purchase of foreign goods. The Buy America Act (BAA), which requires the US government to prefer US-made products in its purchases[35] and the Trade Agreement Act (TAA), which allows for procurement of products if made in the U.S. or designated countries. These countries include

those with Free Trade Agreements with the U.S., those that participate in the World Trade Organization Government Procurement Agreement, or Caribbean Basin Countries[36]. China, Russia and India are not TAA countries. In the Belkin and Brown analysis, The Buy American Act Information Technology Exception, it is shown that, "there is no guidance to determine the country of origin for an end product purchase by the government made of multiple components with multiple points of origin where such items are not substantially transformed in assembling the final line item ordered by the government."[37] The U.S. government has relied on the US Customs and Border Protection (CBP) agency to determine the country of origin of a product. "Some of the CBP rulings suggest that there may be a single country of origin for the end product based upon the component that provides the end product with its "essential character," while other ruling suggest that the end product might actually have multiple countries of origin…" It is evident there is a disconnect between the IT waiver Congress passed on the BAA while the Executive Branch tends to try to enforce the TAA but only based on the country of origin.[38] The David A Kessler article, Protection and Protectionism, identifies that, "Congress…exempted information technology products from the BAA, expressing a preference to the purchase of government IT products from any country." However, the Trade Agreement Act (TAA) may still pose difficulties for information technology developed in countries such as India, China, Taiwan, and Thailand (countries not included in the Agreement on Government Procurement (AGP)). The White House and federal agencies adopted a contrary position from Congress for National Security reasons. The FARs retain the TAA "rule of origin" position. A product originates from an eligible country if it is "wholly the growth, product, or manufacture of that country, or has been substantially transformed in that country into a new and different product distinct from the product from which it was transformed." Kessler shows that existing

customs decisions on computer hardware indicate that substantial transformation of computer software code will be deemed to have occurred if: (a) foreign-manufactured software components or modules have no independent functions in and of themselves; (b) complex and meaningful assembly operations of the software components or modules into a single program occur in the United States or an APG-signatory country, as measured by the high level of skill, number of steps, and time required in assembly operations; and (c) foreign-manufactured software components or modules lose their individual identity when merged into a single unit, in that their name, character, and use must be distinct from their prior form."[39]

Prior to the mid-90s, Information Technology was procured under the same rules and processes that other equipment and supplies where procured. This led to the government quickly falling behind in systems and IT technology. The Clinger-Cohen Act, Public Law 104-106 states, "The Federal Acquisition Regulatory Council shall ensure that, to the maximum extent practicable, the process for acquisition of information technology is a simplified, clear, and understandable process that specifically addresses the management of risk, incremental acquisition, and the need to incorporate commercial information technology in a timely manner."[40] This Act was instrumental in moving the Federal Government forward quickly with an expansion automated data processing equipment, networks, and software.

The key term in the Clinger-Cohen Act is the statement "management of risk." A cyber security professional could interpret this to mean the process for acquisition of IT must addresses the cyber security risk of purchasing commercial IT. However, this act was written in 1996 and was interpreted by acquisition professionals.

The Federal Acquisition Regulation (FAR) chapter 39.102 discusses the "management of risk" in contracts for information technology. It states, "an agency should analyze risks, benefits,

and costs. Reasonable risk taking is appropriate as long as risks are controlled and mitigated. Contracting and program office officials are jointly responsible for assessing, monitoring and controlling risk when selecting projects for investment and during program implementation."[41] The types of risk include "schedule risk, risk of technical obsolescence, cost risk, risk implicit in a particular contract type, technical feasibility, dependencies between a new project and other projects or systems, the number of simultaneous high risk projects to be monitored, funding availability, and program management risk."[42] There is no security risk discussed.

The only mention of software and security in the FAR is in paragraph 39.101 Policy, subsection (d) states, "In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's (NIST) website at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.[43] The checklists provided by NIST simply provide configuration settings required on standard software to address operational software threats. These setting changes do nothing to address the threat of Zero-day exploits.

The FAR also clearly specifies how government agencies purchase software through license agreements. These licensing agreements give the government no additional rights over the software except those identified in FAR section 12.212, Computer Software. These rights include the government's right to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation except as mutually agreed to by the parties."[44] There is no right to or access provided to the source code of

the software license purchased. This limits the depth of the assessment that can be made when reviewing the software product for vulnerabilities.

Vulnerability Identification Processes

The current processes used to assess the confidence and trust that software is free of vulnerabilities is the Information Assurance Vulnerability Management (IAVM) and Common Criteria Evaluation Process. The IAVM is used to notify DoD components of vulnerabilities and ensure appropriate software patches or security configurations are set across the service networks. The DSB Task Force on Mission Impact of Foreign Influence on DoD Software stated, "there are simply more vulnerabilities than DoD can handle."[45] The Common Criteria Evaluation Process (CCEP) is a process used to, "evaluate the extent to which a product's security features comply with a formal description of those features. The description may be either a (government) user-provided "Protection Profile" or a developer-provided "Security Target." Evaluations against the Protection Profile assess the extent to which a product complies with user requirements – Evaluations against Security Target merely evaluate the extent to which the product does what its developers say it does."[46] In other words, our process for evaluating software for vulnerabilities is to test it against known targets. The problem is that there are vulnerabilities, such as Zero-day exploits, for which we cannot test in this method with compiled software.

Mark Harman of University College London, makes the case for source code analysis and manipulation (SCAM). This is because source code is the only precise description of the behavior of the system.[47] The DSB Task Force on Mission Impact of Foreign Influence on DoD Software found the problem of detecting vulnerabilities is deeply complex and there is no silver bullet on the horizon. However, they go on to note that "through source code analysis

tools….research has produced tremendous progress in software analysis tools and techniques for verifying safety and security of software prior to software deployment."[48]

Implications

Knowledge of software code provenance and access to source code are two important mitigation efforts that can improve cyberspace security for the DoD and could be initiated by tying cyber security principles more closely into the procurement process. Provenance and source code access are also the only way we will have access to identify zero-day exploits before our competitors get access to them.

The intent of this paper is not to limit the use of COTS software or place restrictions on which countries are providing software development to the commercial software industry. James A. Lewis stated, "greater use of COTS software and the changes in how companies make software mean that we can no longer make the same assumptions about security and trust." He proposes, "a remedy lies in better practices and processes for assurance and security and better knowledge of those practices and process for both producers and consumers."[49] The software development process is too complex for the US government to attempt to unwind and restructure the process.

However, it is vital for the government and commercial industry to know and understand the provenance or origin of software code used on their systems and networks. Provenance is defined by Godfry, German, Davies, & Hindle as "the documented history of a work of art, which can be used as a guide toward the work's authenticity." Applied in the software context, this is an understanding of where the code came from, why it exists, and what is its real history and origin.[50] This understanding provides government the ability to determine the risk and assign a level of "trust" in the software. FAR subpart 12.1, Acquisition of Commercial Items,

should be updated to require COTS software providers to account for the software "provenance" or proof of the origin of their software code.

Although the DSB Task Force on Mission Impact of Foreign Influence on DoD Software discourages the government from mandating access COTS source code, this may be a simple way to determine most vulnerabilities inherent in a complied software product. This report discouraged this mandate because of the fear of a loss of intellectual property by the government in the process of analyzing the source code. I feel that the government can establish a process to encourage software companies to provide source code in exchange for increased trust rating for their product and a government stamp of approval (similar to a UL label for safety on electrical equipment). Microsoft has provided the U.S. Government and institutes of higher education some access to its source code under certain conditions. However, it has also been reported that Microsoft provided the same access to China and Russia. Not all software development companies have this type of process established to provide access to source code.

FAR subpart 52.227.19, Commercial Computer Software License, should be updated to provide limited rights data and restricted computer software and license the Government to use pre-compiled source code to review software for vulnerabilities. FAR section 39.102 should be updated include the management of security risk in the procurement process and to assign more responsibility for the program manager to the security of the software. This action may drive the need for closer coordination between software acquisition organizations and the cyber defense and intelligence community.

Additional work is also required to clarify disconnects between the BAA and TAA and to ensure "country of origin" is clearly understood for goods and services provided to the United States over the internet.

The Zero-Day exploit market provides some unique implications for how the U.S. government can stay informed on emerging software vulnerabilities. The government should stay connected to what exploits are selling for what price on which software. This market provides the potential to confirm existing, identify new vulnerabilities. This market has also shown that there is a growing group of "entrepreneurs" willing to dedicate their computer science skills to exploiting software vulnerabilities. The US government should tap into this potential brain trust and incentivize the "hacktivist" to assist in the governments' efforts to secure the U.S. cyberspace.

Conclusion

Zero-day exploits are a dangerous threat to Defense networks which use vulnerabilities within COTS products to inflict damage in cyberspace. Vulnerabilities in COTS products can be introduced intentionally or unintentionally, but are exploited intentionally through Zero-day exploits. Globalization of the software development industry provides our competitors access to the software development process in ways that we don't understand unless we require this information from those developing the software. Access to source code that is used in COTS is the only way we can gain any situational awareness of how the code operates and where vulnerabilities exist. Finally, the FARs must be updated to ensure procurement of software products is balanced between streamlining access to advanced technology and cyberspace security.

Digital Collections

Notes

1. InfoWorld Tech Watch, "After silence on Java flaws, Oracle now says it cares.", *InfoWorld*, http://www.infoworld.com/t/java-programming/after-silence-java-flaws-oracle-now-says-it-cares-211610 (accessed 28 January 2013).
2. Gregg Keizer, "Experts prod Oracle to fix broken Java security," *Computerworld*, http://www.computerworld.com/s/article/9235997/Experts_prod_Oracle_to_fix_broken_Java_security, (accessed January 28, 2013).
3. Ibid.
4. Ibid.
5. IT Outsourcing India, "Software Outsourcing India", http://itoutsourcingindia.com/, (accessed 29 January 2013).
6. Office of the Secretary of Defense for Acquisition, Technology, and Logistics, Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software, September 2007. pg 24-25.
7. United States General Accounting Office, Report to Congressional Requesters, Defense Acquisitions, Knowledge of Software Suppliers Needed to Manage Risks, GAO-04-678, www.gao.gov/cgi-bin/getrpt?GAO-04-678.
8. Wikipedia contributors, "Zero-day attack," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/w/index.php?title=Zero-day_attack&oldid=534101510, (accessed February 1, 2013).
9. Andy Greenburg, "Hackers Exploit 'Zero-Day' Bugs for 10 Months On Average Before They're Exposed," *Forbes Security*, http://www.forbes.com/sites/andygreenberg/2012/10/16/hackers-exploit-software-bugs-for-10-months-on-average-before-theyre-fixed/ (accessed January 28, 2013).
10. Ibid.
11. Ibid.
12. Ibid.
13. Wikipedia contributors, "Buy American Act," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/wiki/Buy_American_Act, (accessed January 30, 2013).
14. Ryan Gallagher, "Cyberwar's Gray Market," *Slate Magazine*, http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html, (accessed January 16, 2013).
15. W. Aspray, F. Mayadas, & M.Y. Vardi, Eds., ACM Job Migration Task Force, (2006), Globalization and Offshoring of Software, *Association of Computing Machinery (ACM)*, pg 3.
16. Ibid, pg 3.
17. Ibid, pg 3, 10.
18. Office of the Under Secretary of Defense For Acquisition, Technology, and Logisitics, Defense Science Board report on Department of Defense Policies and Procedures for the Acquisition of Information Technology, March 2009, http://www.acq.osd.mil/dsb/reports/ADA498375.pdf, pg, 22, 23.
19. Jeffery, Wadsworth, "2012 Global R&D Funding Forecast: Battelle: The Business of Innovation." R & D , December 1, 2011, http://battelle.org/docs/default-document-library/2012_global_forecast.pdf, (accessed January 28, 2013).

Air University–Maxwell AFB, AL

20. W. Aspray, et al, Globalization and Offshoring of Software, *ACM*, pg 11.
21. Ibid.
22. Ibid.
23. Jaques S. Gansler and William Lucyshyn, "Commerical Off-The-Shelf (COTS): Doing it Right," Center for Public Policy and Private Enterpirise, School of Public Policy, University of Maryland, http://www.dtic.mil/dtic/tr/fulltext/u2/a494143.pdf, September 2008. Pg v.
24. Office of the Secretary of Defense for Acquisition, Technology, and Logistics, Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software, September 2007, pg 18.
25. James A. Lewis, "Foreign Influence on Software, Risks and Recourse, a Preport of the Technology and Public Policy Program," Center for Strategic and International Studies, The CSIS Press, March 2007, pg 8.
26. Ibid, pg 10-11.
27. AFDD 3-12. Cyberspace Operations, (15 July 2010): http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf. pp. 4-5.
28. Bob Violino, "Unseen, all-out cyber war on the U.S. has begun," *InfoWorld*, http://www.infoworld.com/print/211438. (accessed January 30, 2013).
29. Ibid.
30. Renee Oricchio, "China: Malware Capital Of The World, *Inc. Business Bytes*, http://www.inc.com/tech-blog/china-malware-capitol-of-the-world.html, (accessed February 2, 2013).
31. Ibid.
32. Mark A. Stokes and L.C. Russell Hsiao, "Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests, *Project 2049 Institute*, http://project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf, (accessed February 2, 2013), pg 4.
33. Anna Mulrine, "China is a lead cyberattacker of US military computers Pentagon reports." *Christian Science Monitor*, http://www.csmonitor.com/USA/Military/2012/0518/China-is-a-lead-cyberattacker-of-US-military-computers-Pentagon-reports, (accessed February 3, 2013).
34. Bill Brenner, "How Russia became a malware hornet's nest," *Search Security*, http://searchsecurity.techtarget.com/news/1275987/How-Russia-became-a-malware-hornets-nest, (accessed February 2, 2013).
35. Wikipedia contributors, "Buy American Act," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/w/index.php?title=Buy_American_Act&oldid=516905267 (accessed February 1, 2013).
36. Wikipedia contributors, "Trade Agreements Act of 1979," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/w/index.php?title=Trade_Agreements_Act_of_1979&oldid=469377970 (accessed February 7, 2013).
37. Jeffery A Brown, Esq and Donald G. Brown, Esq., Alston and Bird, "The Buy American Act information technology exception: Should it apply to the Trade Agreement Act-covered contracts?", *Westlaw Journal*, Vol 24, Issue 6, July 26, 2010. Pg. 6.
38. Ibid.

39. David A. Kessler, “Protection and Protectionism: The Practicalities of Offshore Software Devleopment in Government Procurement,” *Public Contract Law Journal*, Volume 38, Number 1, Fall 2008. Pg. 15.
40. Jaques S. Gansler and William Lucyshyn, “Commerical Off-The-Shelf (COTS): Doing it Right,” Center for Public Policy and Private Enterpirise, School of Public Policy, University of Maryland, http://www.dtic.mil/dtic/tr/fulltext/u2/a494143.pdf, September 2008. Pg v.
41. Federal Acquisition Regulation, current issue, https://www.acquistiion.gov/far/loadmainre.html, (accessed January 17, 2013).
42. Ibid.
43. Ibid.
44. Ibid.
45. Office of the Secretary of Defense for Acquisition, Technology, and Logistics, Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software, September 2007, pg 32.
46. Ibid. pg 32.
47. Mark Harman, “Why Source Code Analysis and Manipulation Will Always Be Important,” 10th IEEE International Working conference on Source Code Analysis and Manipulation, http://www0.cs.ucl.ac.uk/staff/M.Harman/papers.html., (accessed January 28, 2013).
48. Office of the Secretary of Defense for Acquisition, Technology, and Logistics, Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software, September 2007, pg 41.
49. James A. Lewis, “Foreign Influence on Software, Risks and Recourse, a Preport of the Technology and Public Policy Program,” Center for Strategic and International Studies, The CSIS Press, March 2007, pg X.
50. Michael W. Godfrey, Daniel M German, Julius Davies, Abram Hindle, “Determining the Provenance of Software Artifacts,” American Computing Machines, IWSC ’11 Proceedings of the 5th International Workshop on Software Clones,” pg 65-66.

Bibliography

Abuhantash, Medhat A. "In-sourcing or Outsourcing: What makes sense in today's operating environment". *Senior Service College Fellowship Independent Research Project Defense Acquisition University Research Report* 10-006. April 2010.

AFDD 3-12. Cyberspace Operations, (15 July 2010): http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf.

Aspray, W, F. Mayadas, & M. Y. Vardi, Eds., ACM Job Migration Task Force. (2006). Globalization and Offshoring of Software. *Association for Computing Machinery (ACM*).

Belkin, Jeffrey A. Esq., and Donald G. Brown, Esq. Alston and Bird, "The Buy American Act information technology exception: Should it apply to the Trade Agreement Act-covered contracts?", *Westlaw Journal*, Vol 24, Issue 6, July 26, 2010. http://www.alston.com/Files/Publication/def44ccb-05d6-4184-8639-a6f4b9a35202/Presentation/PublicationAttachment/260c331f-c337-41d5-bfab-2772cf731705/WLJ_GOV2406_Commentary_Belkin.pdf.

Brenner, Bill, "How Russia became a malware hornet's nest." *Search Security*, http://searchsecurity.techtarget.com/news/1275987/How-Russia-became-a-malware-hornets-nest, October 9, 2007, (accessed February 2, 2013).

Cohen, Michael. "Senate Probes Offshore Profit Shifting by Microsoft and HP", *Accounting Today*, http://www.accountingtoday.com/news/senate-probes-offshore-profit-shifting-microsoft-hp-64041-1.html?pg=4, 21 September 2012. (accessed 3 December 2012)

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, July 2009, Version 3.1 Revision 3, Final, CCMB-2009-07-001.

Department of Homeland Security, Software Assurance Forum, Software Pocket Guide Series, *Acquisition and Outsourcing*, https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html (accessed December 3, 2012).

Erran Carmel, J. Espinosa, Yael Dubinsky, 2010. "Follow the Sun" Workflow in Global Software Development." *Journal Of Management Information Systems* 27, no. 1: 17-37. Business Source Premier, EBSCOhost (accessed October 9, 2012).

Federal Acquisition Regulation, current issue, https://www.acquisition.gov/far/loadmainre.html, accessed 17 Jan 2013.

Gallagher, Ryan, "Cyberwar's Gray Market," *Slate Magazine*, http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html, January 15, 2013, accessed January 16, 2013.

Gansler, Jacques S., and William Lucyshyn, "Commercial-Off-The-Shelf (COTS): Doing it Right, *Center for Public Policy and Private Enterprise*, School of Public Policy, University of Maryland, http://www.dtic.mil/dtic/tr/fulltext/u2/a494143.pdf, Sept 2008.

Godfrey, Michael W., Daniel M German, Julius Davies, Abram Hindle, Determining the Provenance of Software Artifacts, *Association of Computing Machines*, "IWSC '11 Proceedings of the 5th International Workshop on Software Clones", pg 65-66, ACM, New York, NY, USA 2011.

Gosler, James. "The Digital Dimension", http://www.jhuapl.edu/urw_symposium/proceedings/2007/papers/Gosler.pdf, *Unrestricted Warfare Symposium Proceedings*, 2007.

Greenberg, Andy, "Hackers Exploit 'Zero-Day' Bugs for 10 Months On Average Before They're Exposed," *Forbes Security*, http://www.forbes.com/sites/andygreenberg/2012/10/16/hackers-exploit-software-bugs-for-10-months-on-average-before-theyre-fixed/, October 16, 2012, (accessed January 28, 2013).

Harman, Mark, "Why Source Code Analysis and Manipulation Will Always Be Important," *10th IEEE International Working Conference on Source Code Analysis and Manipulation* Timişoara, Romania, 12-13 September 2010, http://www0.cs.ucl.ac.uk/staff/M.Harman/papers.html, (accessed January 10, 2013).

InfoWorld Tech Watch, "After Silence on Java flaws, Oracle now says it cares," *InfoWorld*, http://www.infoworld.com/t/java-programming/after-silence-java-flaws-oracle-now-says-it-cares-211610, January 28, 2013 (accessed January 28, 2013)

"Internet Security Threat Report Symantec." Endpoint, Cloud, Mobile & Virtual Security Solutions, *Symantec*, http://www.symantec.com/threatreport/?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Apr_worldwide_ISTR17 (accessed January 28, 2013).

IT Outsourcing India, *Software Outsourcing India*, http://itoutsourcingindia.com/, (accessed 29 Jan 2013).

Jason Dedrick, Kenneth L. Kraemer, Erran Carmel and Debora Dunkle, 2009. Offshore software development: survey results. Irvine, CA: *Center for Research on Information Technology and Organizations*, University of California, Irvine. http://pcic.merage.uci.edu/papers/2009/SoftwareSurveyResults.pdf.

Keizer, Gregg, "Experts prod Oracle to fix broken Java security, Take a mulligan, redesign Java, urges one." *Computerworld*, http://www.computerworld.com/s/article/9235997/Experts_prod_Oracle_to_fix_broken_Java_security, January 22, 2013, (accessed January 28, 2013).

Kessler, David A., "Protection and Protectionism: The Practicalities of Offshore Software Development In Government Procurement," *Public Contract Law Journal*, Volume 38, No. 1, Fall 2008.

Khan, Qadeem and Shahbaz Ghayyur, "Software Risks and Mitigation in Global Software Development," *Journal of Theoretical and Applied Information Technology*, Vol 22 No. 1, December 2010.

Krik, Jeremy, "Microsoft finds new PCs in China preinstalled with malware." *PC World*, http://www.pcworld.com/article/262308/microsoft_finds_new_computers_in_china_preinstalled_with_malware.html, September 14, 2012, (accessed February 2, 2013).

Kreaemer, Kenneth L. Jason Dedrick and Debora Dunkle, 2010. "Offshoring of Software Development: Patterns and Recession Effects," *Personal Computing Industry Center*, Syracuse University and University of California, Irvine.

Lewis, James A., Foreign Influence on Software, Risks and Recourse, A Report of the Technology and Public Policy Program, Center for Strategic and International Studies, *The CSIS Press*, Center for Strategic and International Studies, Washington, D.C. 20006, March 2007.

Lockhart, Matt, "The True Costs and Potential Risks of Outsourcing Software Development," *Enterprise Systems Journal*, October 2, 2007, http://esj.com/articles/2007/10/02/the-true-

costs-and-potential-risks-of-outsourcing-software-development.aspx?sc_lang=en, (accessed 2 Feb 2013).
Maxon, Ryan A., Major, USAF AFIT/GIR/ENV/08-M13, Software Assurance Best Practices for Air Force Weapon and Information Systems – Are We Bleeding? Department of the Air University, March 2008.
Microsoft Enterprise Source Licensing Program, http://www.microsoft.com/en-us/sharedsource/enterprise-source-licensing-program.aspx, (accessed, 1 February 2013).
Mulrine, Anna, "China is a lead cyberattacker of US military computers Pentagon reports." *Christian Science Monitor*, http://www.csmonitor.com/USA/Military/2012/0518/China-is-a-lead-cyberattacker-of-US-military-computers-Pentagon-reports, (accessed February 3, 2013).
Nakashima, Ryan, "Oracle Says Java Patch Fixes Security Problem; Feds Maintain Warning," *Time.com*, http://techland.time.com/2013/01/14/oracle-says-java-patch-fixes-security-problem/, January 14, 2013, accessed January 28, 2013.
Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, Defense Science Board report on Department of Defense Policies and Procedures for the Acquisition of Information Technology, March 2009, http://www.acq.osd.mil/dsb/reports/ADA498375.pdf.
Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software, September 2007.
Oricchio, Renee, "China: Malware Capital Of The World, *Inc. Business Bytes*, http://www.inc.com/tech-blog/china-malware-capitol-of-the-world.html, March 30, 2010, accessed February 2, 2013.
Overby, Stephanie. "Is IT Outsourcing a dying concept." *CIO.com*, http://www.cio.com/article/721159/Is_IT_Outsourcing_a_Dying_Concept_?page=3&taxonomyId=3195, 9 November 2012. (accessed 1 December 2012).
Paul, Ryan. "US government shouldn't fear foreign participation in Forge.gov." *ARS Technica*, http://arstechnica.com/information-technology/2010/09/in-an-effort-to-reduce/, September 8, 2010, (accessed January 31, 2013).
Pollack, Peter, "Russian legislators say "nyet" to foreign software", *ARS Technica*, http://arstechnica.com/uncategorized/2006/05/6816-2/, May 11, 2006, (accessed January 31, 2013).
Ribeiro, John. "Outsourcing contracts down by 19 percent, says research firm." *CIO.com*. http://www.cio.com/article/720984/Outsourcing_Contracts_Down_By_19_Percent_Says_Research_Firm?taxonomyId=3195, 7 November 2012. (accessed 1 December 2012)
Shen, J., H. Li, "An Empirical Analysis on Industrial Organization Structure of Chinese Software Service Outsourcing," *Journal of Service Science and Management*, Vol. 3 No. 2, 2010, pp. 218-226. doi: 10.4236/jssm.2010.32027.
Sivaramakrishnan, Gopal A, K, Krishnan M, Mukhopadhyay T. Contracts in Offshore Software Development: An Empirical Analysis. *Management Science* [serial online]. December 2003;49(12):1671-1683. Available from: Business Source Premier, Ipswich, MA. (Accessed October 9, 2012).

Stokes, Mark A. and L.C. Russell Hsiao, “Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests, *Project 2049 Institute*, http://project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf, October 24, 2012, (accessed February 2, 2013).

United States General Accounting Office, Report to Congressional Requesters, Defense Acquisitions, Knowledge of Software Suppliers Needed to Manage Risks, GAO-04-678, www.gao.gov/cgi-bin/getrpt?GAO-04-678.

Violino, Bob, “Unseen, all-out cyber war on the U.S. has begun,” *InfoWorld*, http://www.infoworld.com/print/211438, January 28, 2013, (accessed 30 January 2013).

Wadsworth, Jeffrey. "2012 Global R&D Funding Forecast: Battelle: The Business of Innovation." *R & D* , December 1, 2011, http://battelle.org/docs/default-document-library/2012_global_forecast.pdf. (accessed 28 January, 2013).

Wan, J., D. Wan and H. Zhang, "Case Study on Business Risk Management for Software Outsourcing Service Provider with ISM," *Technology and Investment*, Vol. 1 No. 4, 2010, pp. 257-266. doi: 10.4236/ti.2010.14033.

Wikipedia contributors, "Buy American Act," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/w/index.php?title=Buy_American_Act&oldid=516905267 (accessed February 1, 2013).

Wikipedia contributors, "Trade Agreements Act of 1979," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/w/index.php?title=Trade_Agreements_Act_of_1979&oldid=469377970 (accessed February 1, 2013).

Wikipedia contributors, "Zero-day attack," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/w/index.php?title=Zero-day_attack&oldid=534101510 (accessed February 1, 2013).

Air University–Maxwell AFB, AL