Surveillance, Censorship, and Countermeasures

Professor Ristenpart

http://www.cs.wisc.edu/~rist/

rist at cs dot wisc dot edu

Google Outage Shows Risk of Doing Business In China

Posted by **samzenpus** on Monday November 12, @10:58AM
from the price-of-doing-business dept.

Hugh Pickens writes writes

> "The WSJ reports that widespread disruptions to Google in China over the weekend halting use of everything from Google's search engine to its Gmail email service to its Google Play mobile-applications store underscore the uncertainty surrounding Beijing's effort to control the flow of information into the country, as well as the risks that effort poses to the government's efforts to draw global businesses.The source of the disruptions couldn't be determined but Internet experts pointed to China's Internet censorship efforts, which have been ratcheted up ahead of the 18th Party Congress. 'There appears to be a throttling

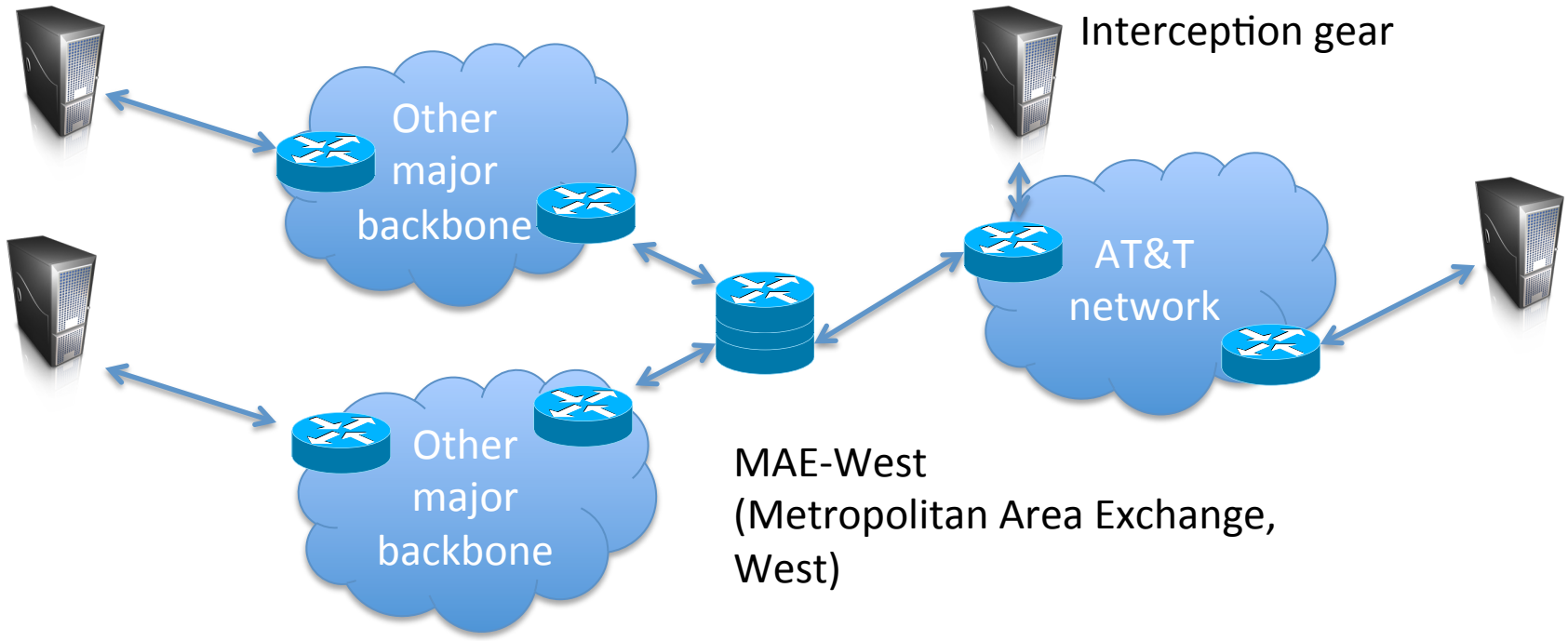
Announcements

- HW3 is up – web security
- Lectures next week cancelled for Thanksgiving
  - More time to work on HW3
- Lecture on Nov 28th maybe cancelled, stay tuned

AT&T Wiretap case

- Mark Klein discloses potential wiretapping activities by NSA at San Francisco AT&T office
- Fiber optic splitter on major trunk line for Internet communications
  - Electronic voice and data communications copied to “secret room”
  - Narus STA 6400 device

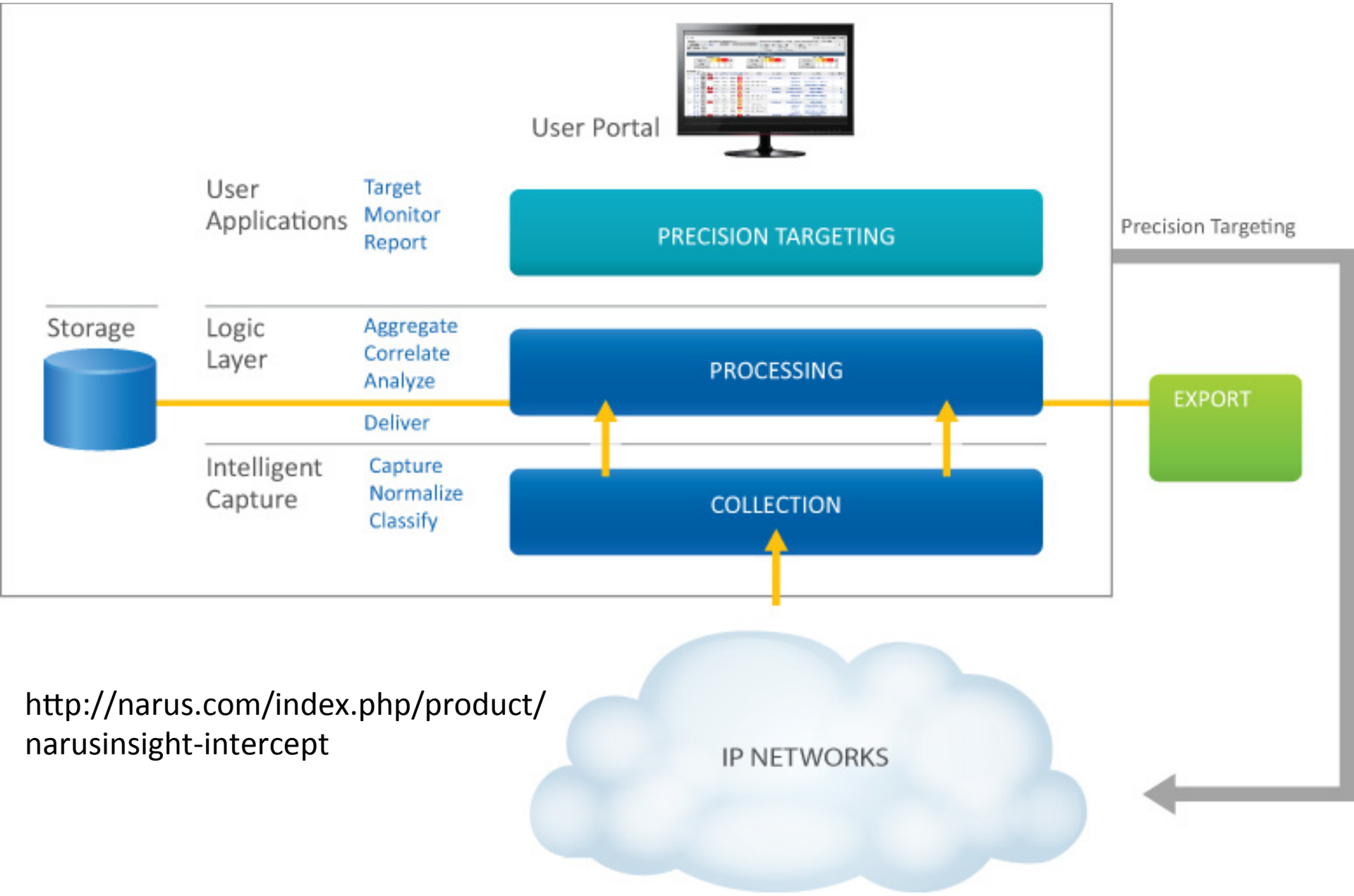
Wiretap surveillance



Large amounts of Internet traffic cross relatively few key points

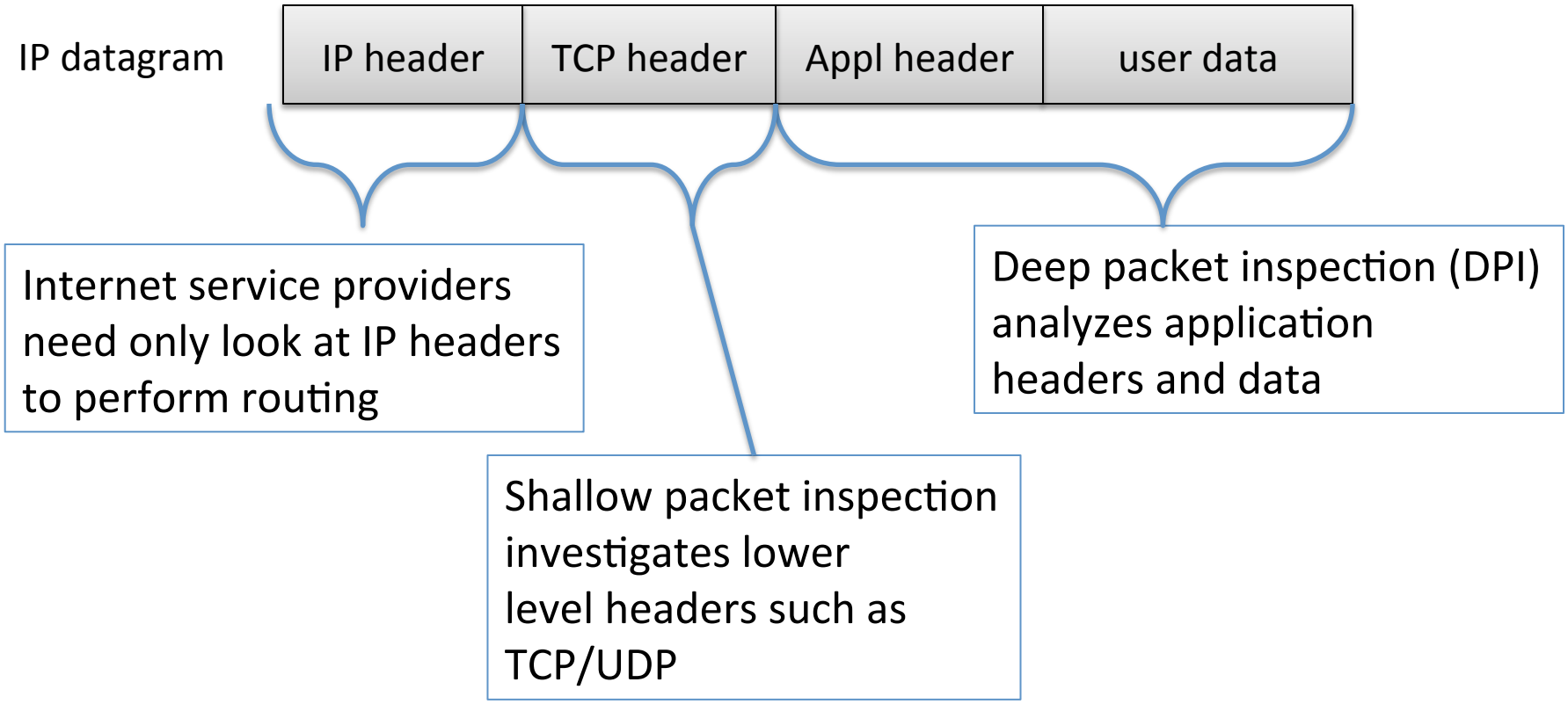
Interception technology

- From Narus' website (http://narus.com/index.php/product/narusinsight-intercept):
  - "Target by phone number, URI, email account, user name, keyword, protocol, application and more", "Service- and network agnostic", "IPV 6 ready"
  - Collects at wire speeds beyond 10 Gbps



http://narus.com/index.php/product/narusinsight-intercept

Types of packet inspection



Is dragnet surveillance technologically feasible?

- CAIDA has lots of great resources for researchers about traffic levels
- From their SanJoseA tier-1 backbone tap:

Application	Min	Avg	Max
HTTP	51.20M	2.20G	11.01G
UNKNOWN_UDP	4.08M	168.79M	711.57M
UNKNOWN_TCP	3.62M	136.02M	660.50M
HTTPS	3.96M	125.80M	543.15M
RTMP	2.00M	78.09M	314.79M
SMTP	289.75k	14.76M	55.82M
QUAKE	300.58k	8.31M	36.02M
SQUID	42.88k	7.25M	37.58M
IPSEC	213.15k	7.09M	23.97M
SSH	248.25k	6.73M	28.40M
WOW	72.88k	6.12M	34.40M
ABACAST	285.74k	3.43M	14.98M
NOPORTS_UDP	64.46k	2.04M	14.83M
other	1.23M	40.23M	161.56M

generated 2011-11-15 17:13 UTC

http://www.caida.org/data/realtime/passive/?monitor=equinix-sanjose-dirA

Key Features

From http://narus.com/index.php/product/narusinsight-intercept

Precision Targeting at Broadband Speeds

- Broad range of target types from Layer 2 through Layer 7, including ATM/MPLS/VPN support
- Target by phone number, URI, email account, user name, keyword, protocol, application and more
- Service- and network agnostic
- IPV 6 ready

Capture and Delivery

- Passive model collects from the line at wire speeds beyond 10 Gbps with support for asymmetric networks
- Efficient encoding of full packets and associated metadata for economical backhaul
- Flexible delivery for remote monitoring, retention or forwarding to alternate agencies

Reconstruction and Rendering

- Reconstruction and playback of captured traffic in near real time
- Integrated rendering of voice, video, email, Web mail, chat, and more
- Access to extensive metadata for all traffic types

Lawful intercept

- CALEA
  - Communications Assistance for Law Enforcement Act (1995)
- FISA
  - Foreign Intelligence Surveillance Act (1978)
  - Demark boundaries of domestic vs. foreign intelligence gathering
  - Foreign Intelligence Surveillance Court (FISC) provides warrant oversite
  - Executive order by President Bush suspend need for NSA to get warrants from FISC
- Almost all national governments mandate some kind of lawful intercept capabilities

Lots of companies

- Narus (originally Israeli company), now owned by Boeing
  - Partnered with Egyptian company Giza Systems
- Pen-Link (http://www.penlink.com/)
- Nokia, Nokia Siemens
- Cisco
- …

NarusInsight™ Selected To Save Pakistan's Telecommunications Networks Millions Of Dollars Per Year

NarusInsight™ Selected to Save Pakistan's Telecommunications Networks Millions of Dollars Per Year

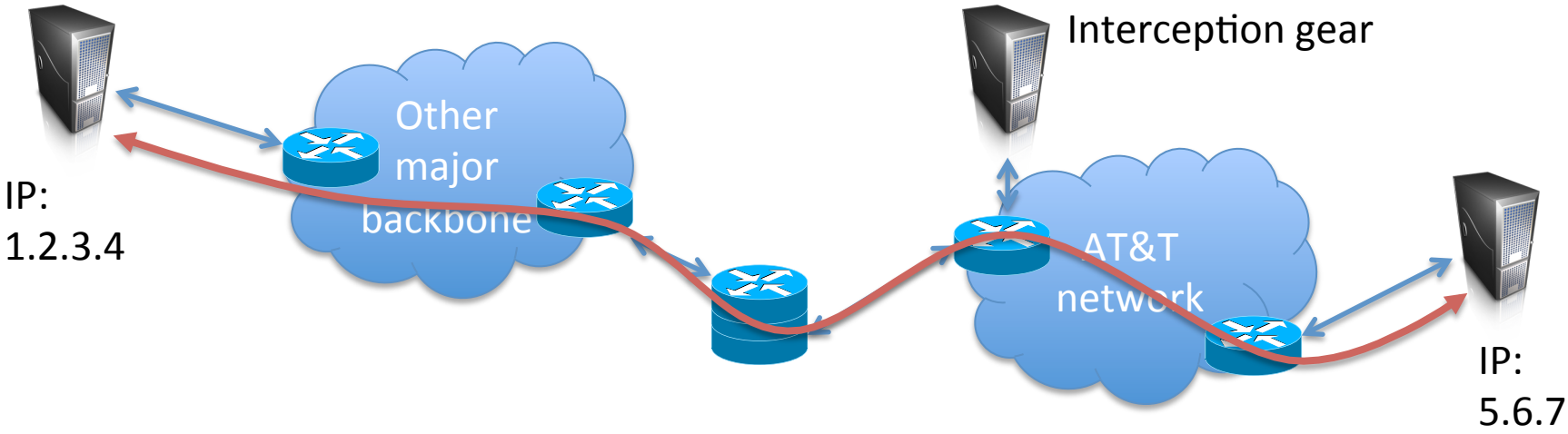
Narus System Chosen to Detect Rogue VoIP Traffic

MOUNTAIN VIEW, Calif.—September 21, 2007—Narus, Inc., the leader in carrier-class security for the world's largest IP networks, today announced that the company has teamed up with Inbox Business Technologies Pvt. Ltd, a leading total IT solution provider in Pakistan, to keep Pakistan's telecommunication networks clear of illegal, rogue and malicious IP traffic. NarusInsight was chosen by the Pakistan Telecommunication Authority (PTA) (the government administration responsible for regulating the establishment, operation and maintenance of telecommunication systems, and the provision of telecom services) to detect rogue VoIP traffic flowing through the telecommunications network in Pakistan.

http://www.narus.com/index.php/news/279-narusinsight-selected-to-save-pakistans-telecommunications-networks-millions-of-dollars-per-year

Preventing intercept

- End-to-end encryption (TLS, SSH)

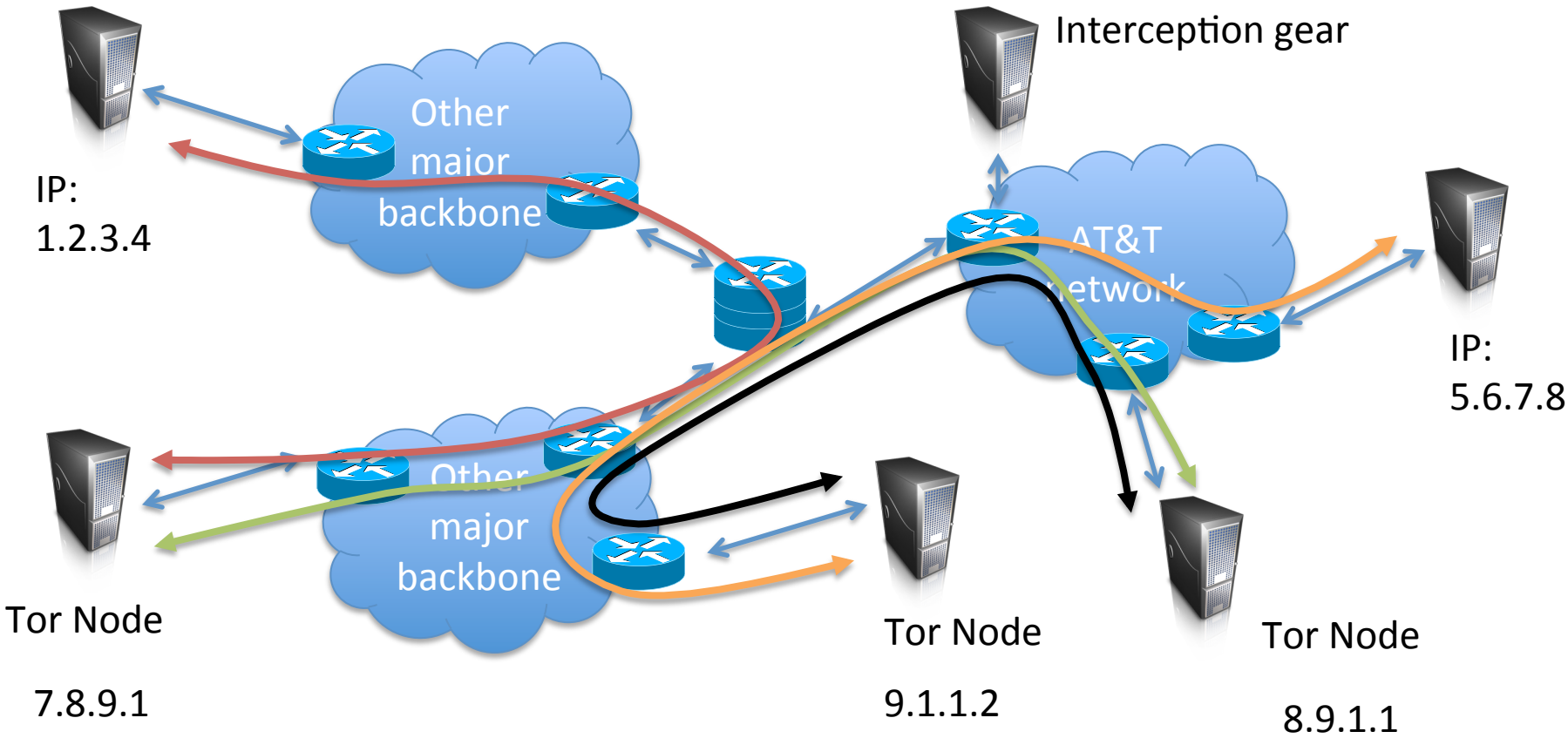


- What does this protect? What does it leak?
- What can go wrong?

Hiding connectivity is harder

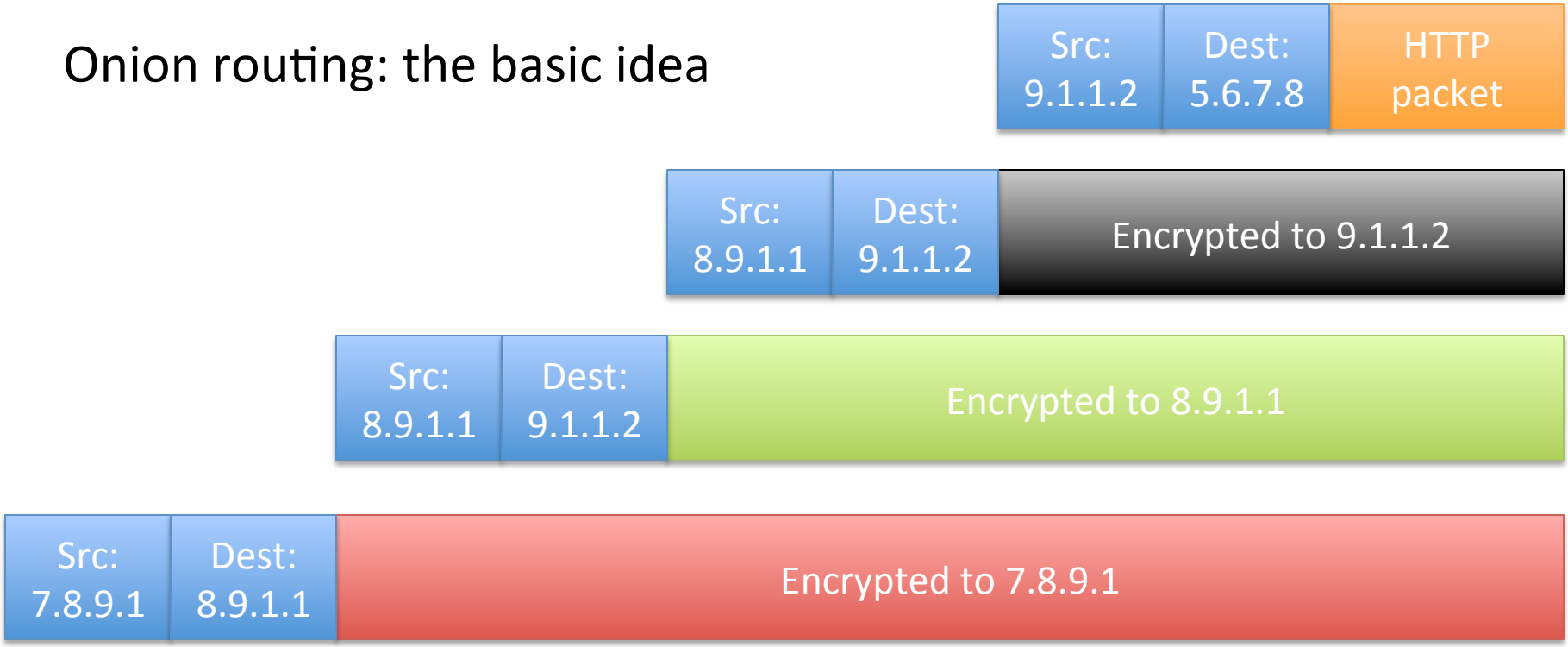
- IP addresses are required to route communication, yet not encrypted by normal end-to-end encryption
  - 1.2.3.4 talked to 5.6.7.8 over HTTPs
- How can we hide connectivity information?

Tor (The Onion Router)



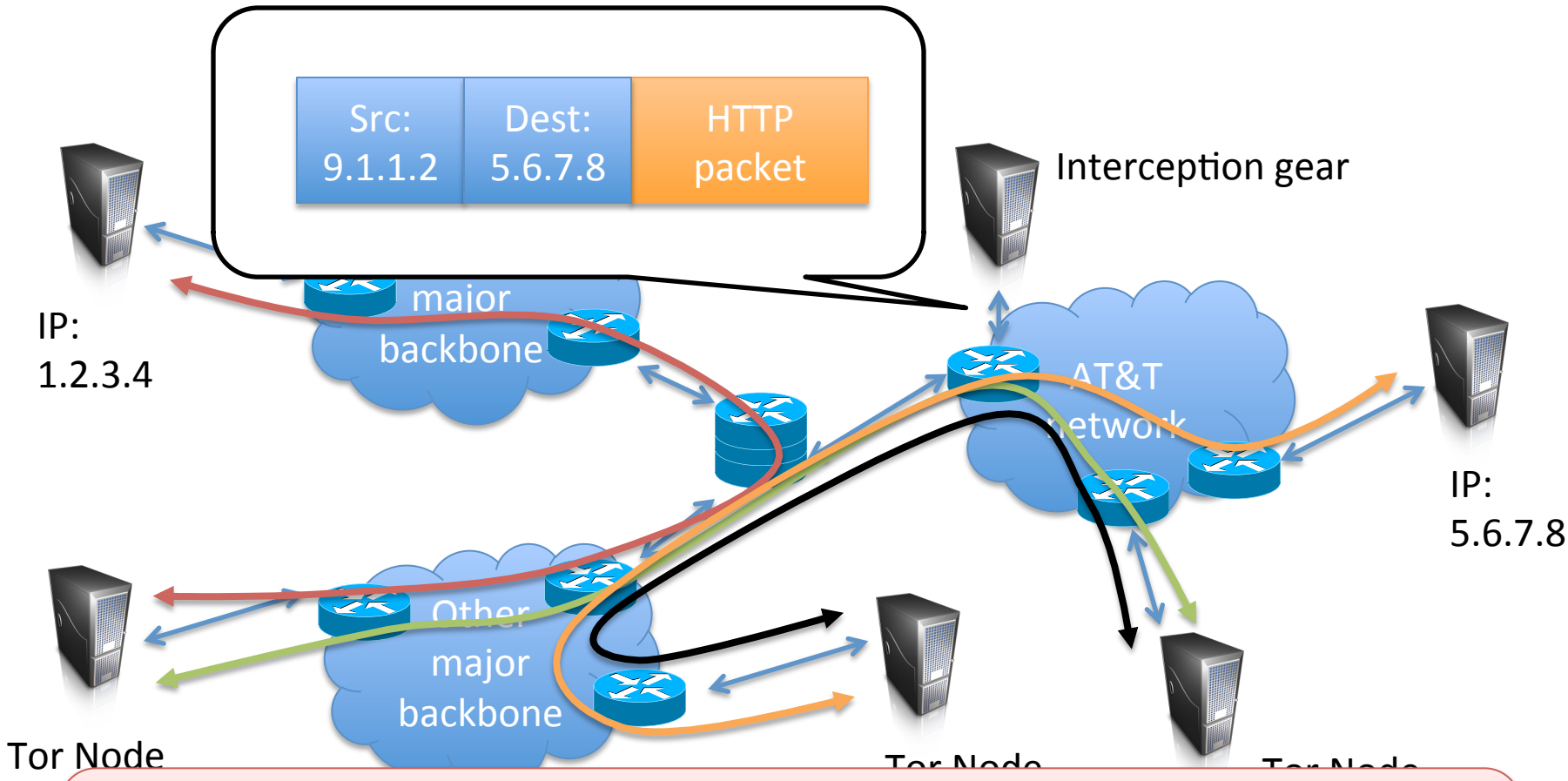
March 12: Roger Dingledine of Tor will come be giving a talk at UW

Onion routing: the basic idea

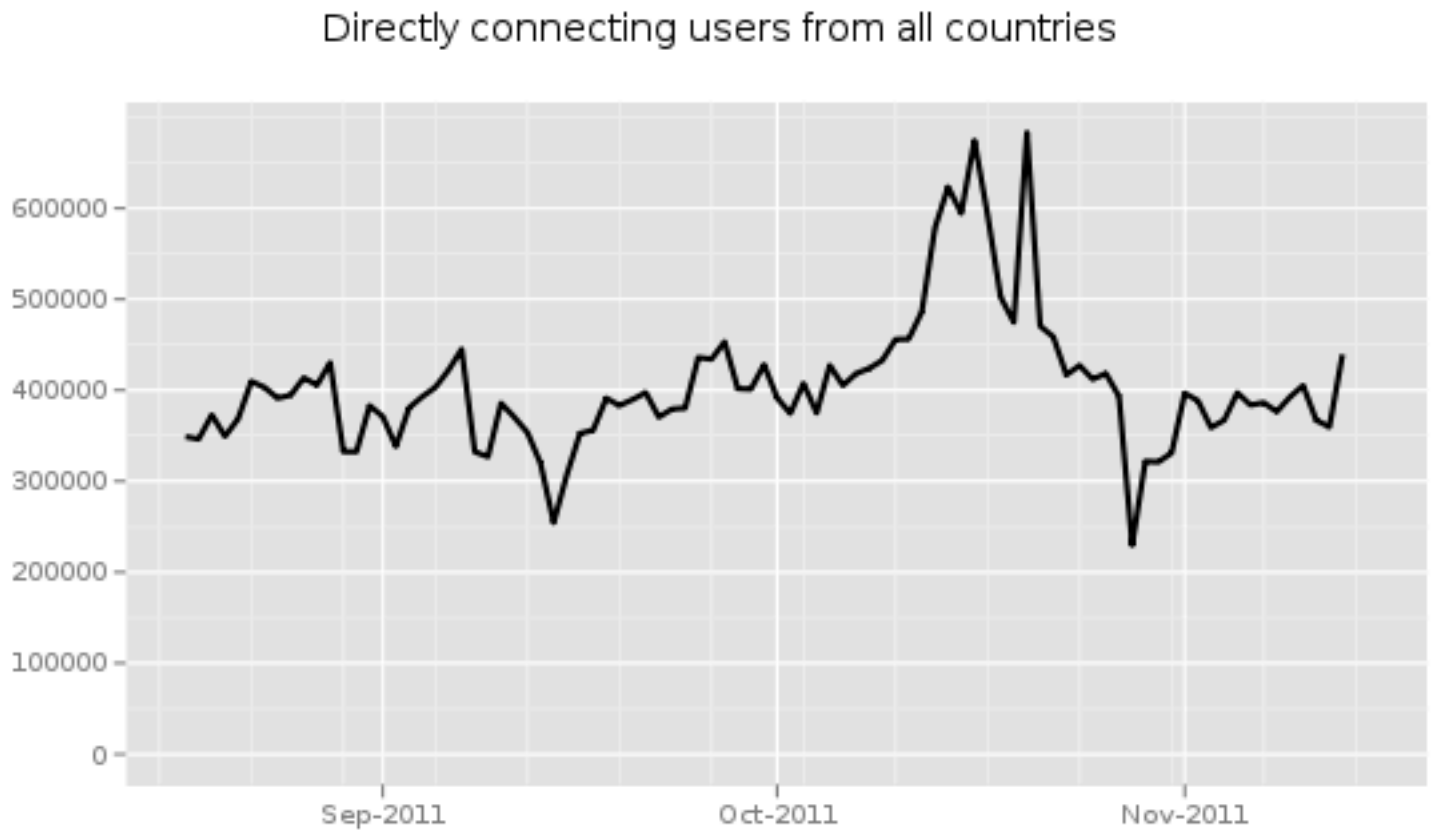


Tor implements more complex version of this basic idea

What does adversary see?



Tor obfuscates who talked to who, need end-to-end encryption (e.g., HTTPS) to protect payload


Directly connecting users from all countries
600000
500000
400000
300000
200000
100000
0
Sep-2011
Oct-2011
Nov-2011
The Tor Project - https://metrics.torproject.org/

Other anonymization systems

- Single-hop proxy services

- JonDonym, anoymous remailers (MixMaster, MixMinion), many more…

Surveillance via third-party

- “Thus, some Supreme Court cases have held that you have no reasonable expectation of privacy in information you have "knowingly exposed" to a third party — for example, bank records or records of telephone numbers you have dialed — even if you intended for that third party to keep the information secret. In other words, by engaging in transactions with your bank or communicating phone numbers to your phone company for the purpose of connecting a call, you’ve "assumed the risk" that they will share that information with the government.”

From the EFF website

https://ssd.eff.org/your-computer/govt/privacy

Third-party legal issues

- Under Electronic Communications Privacy Act (ECPA) government has access via subpoena to:
  - Name, address
  - Length of time using service
  - Phone records (who you called, when, how long)
  - Internet records (what/when/how long services you used, your assigned IP address)
  - Info on how you pay your bill

Example: AT&T Hawkeye database

- All phone calls made over AT&T networks since approximately 2001
  - Originating phone number
  - Terminating phone number
  - Time and length of each call

Example: Google data requests

Country	Data Requests	Percentage of data requests fully or partially complied with	Users/Accounts Specified
United States	5,950	93%	11,057
India	1,739	70%	2,439
France	1,300	48%	1,622
United Kingdom	1,273	64%	1,443
Germany	1,060	67%	1,759
Italy	934	60%	1,263
Brazil	703	87%	1,822
Spain	460	63%	709
Australia	361	73%	412
Poland	266	11%	319

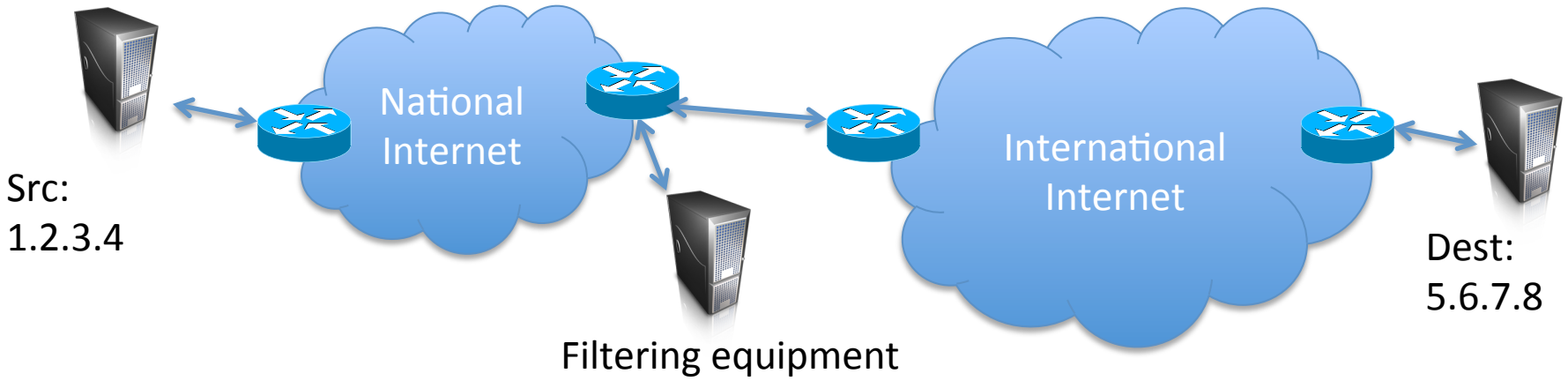
January to June 2011

From http://www.google.com/transparencyreport/governmentrequests/userdata/

Prevention

- One can encrypt data that is stored, but no current way to protect data that needs to be used
- Companies have little incentive to support encryption
- Policy?
- Legal protections?

Censorship via Internet filtering

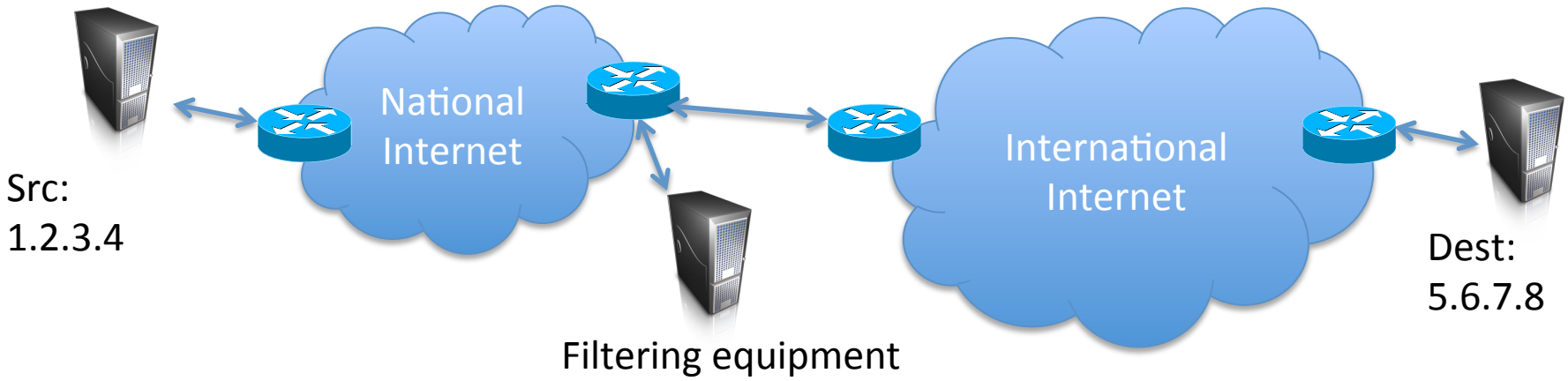


- Golden Shield Project most famous example
- But many other nations perform filtering as well including
  - Iran, Syria, Pakistan (YouTube anecdote),
  - Singapore, Australia (proposed legislation)
  - Other countries?

Big business

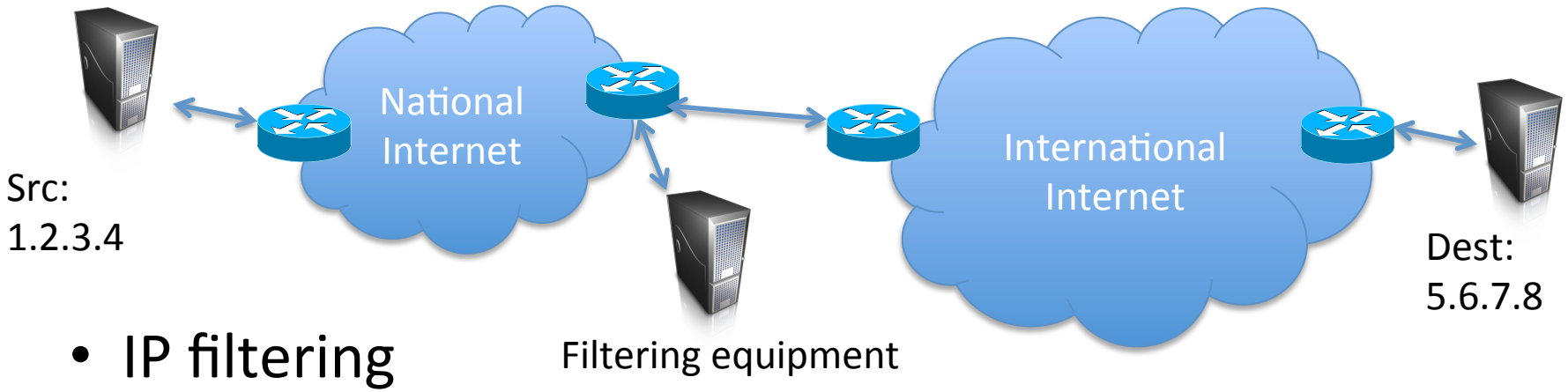
- Recent reports of products being used in Syria
  - Blue Coat (http://www.bluecoat.com/)
  - NetApp (http://www.netapp.com/)
- Iran, Saudi Arabia
  - Secure Computing's SmartFilter software
  - Secure Computing recently bought by McAffee
- Embargos prevent selling directly by USA companies, but resellers can do so

Filtering



- IP filtering
- DNS filtering / redirection
- URL filtering
- Packet filtering (search keywords in TCP packets)
- Protocol filtering (detect Tor protocol)

Circumvention of filtering



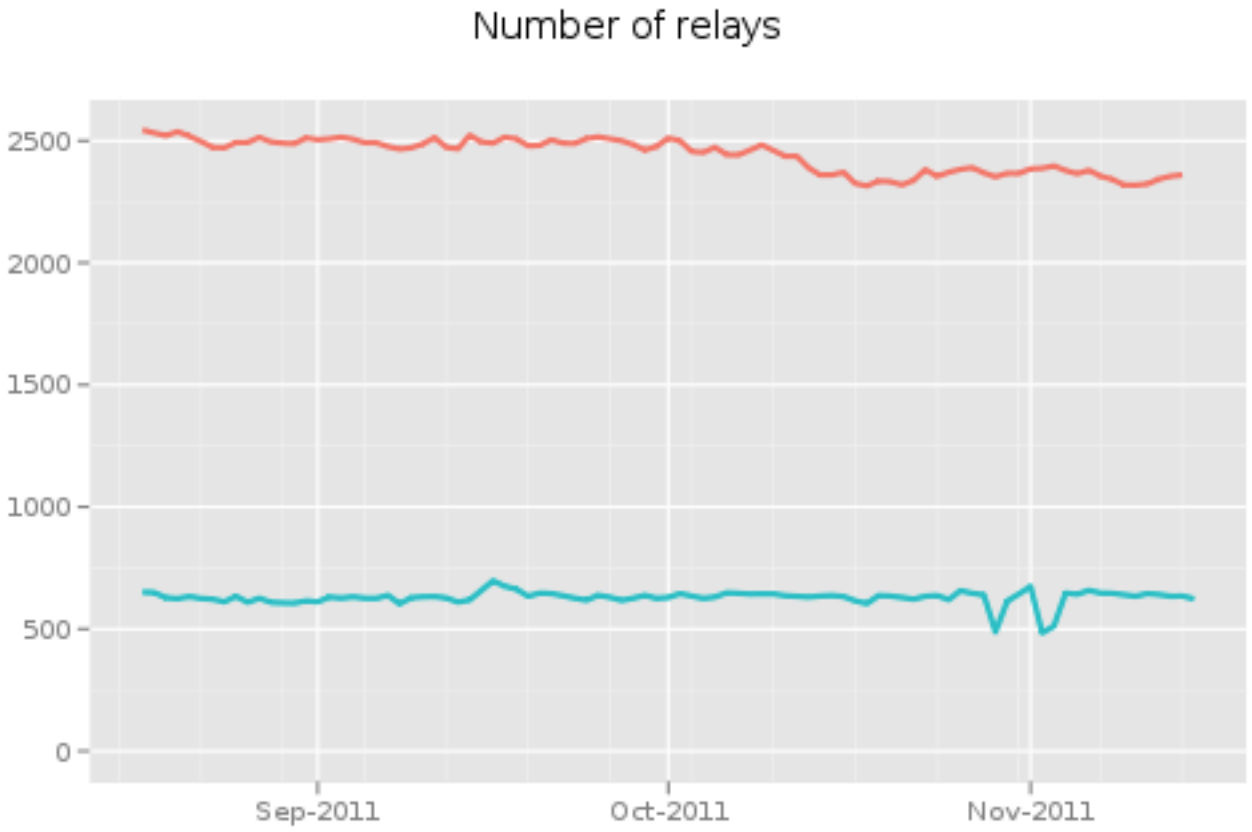
- IP filtering
  - Proxies
- DNS filtering / redirection
  - DNS proxy
- URL filtering or Packet filtering
  - Encryption / Tunneling / obfuscation
- Protocol filtering
  - Obfuscation techniques? (Current research topic!)

Golden Shield Project (Great Firewall of China)

- IP filtering
- DNS filtering / redirection
- URL filtering
- Packet filtering (search keywords in TCP packets)
  - Send TCP FIN both ways
- Protocol filtering (Tor is shut down)

Great Firewall targeting of Tor (circa 2011 and before)

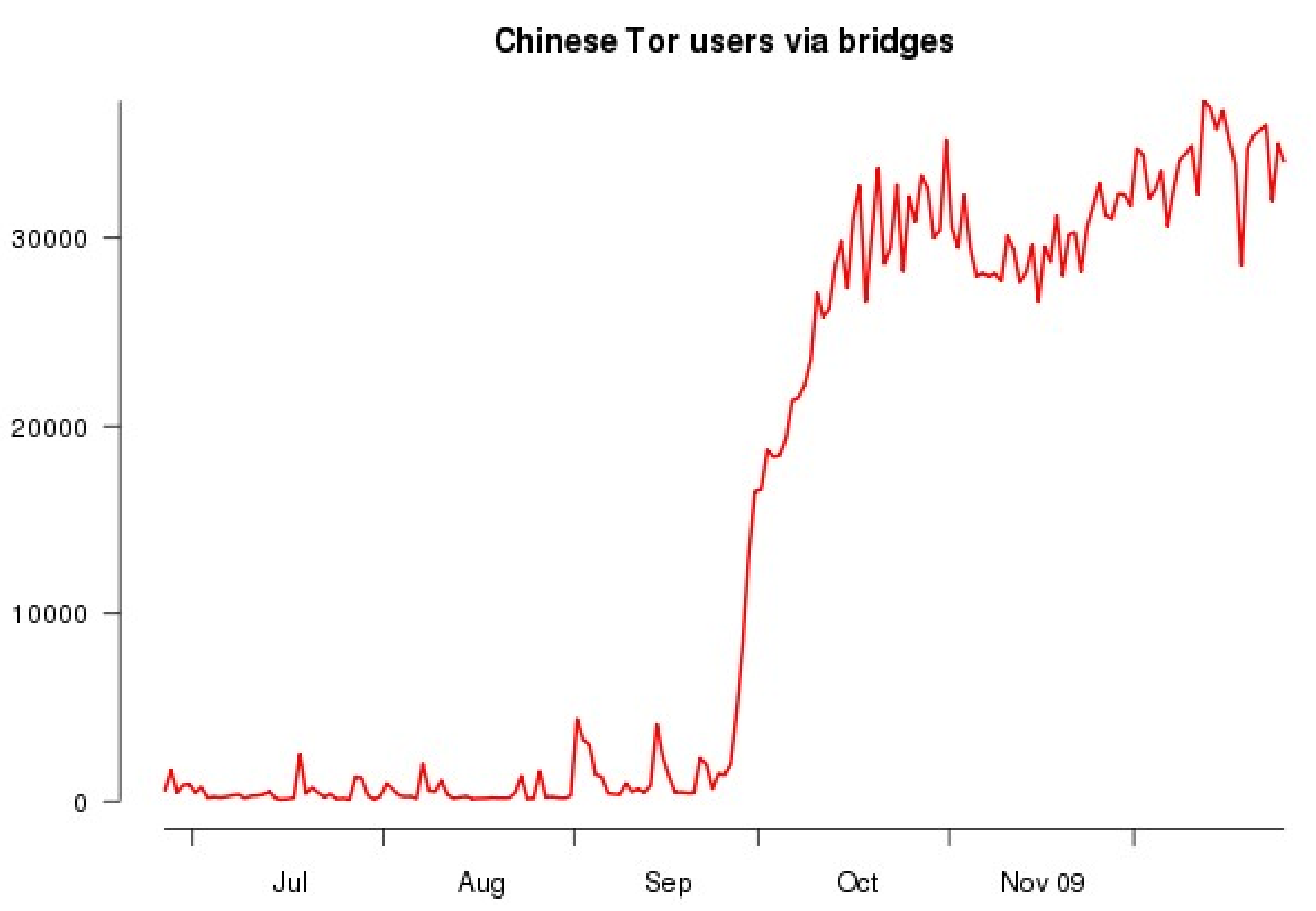
- Enumerate Tor relays and filter them



Relay is publicly listed Tor node

Bridge is Tor node not publicly listed

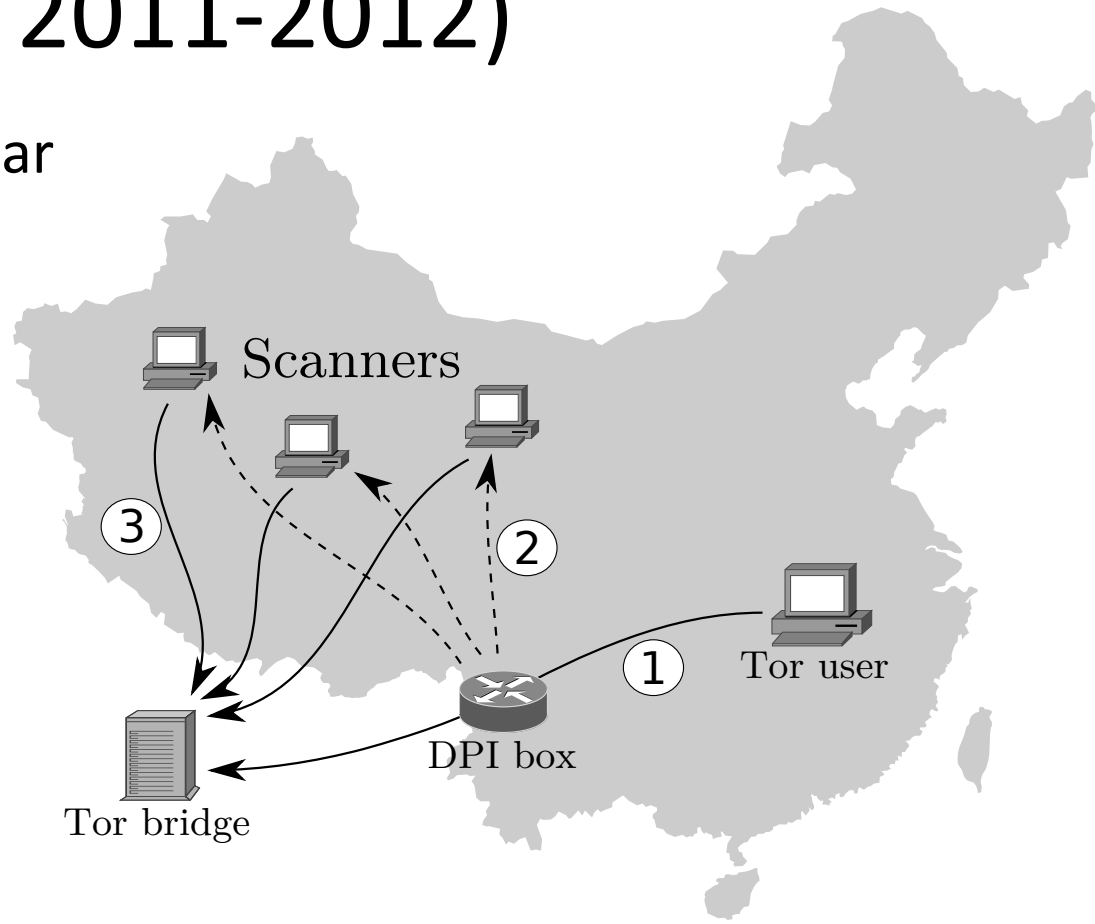

Number of directory requests to directory mirror trusted
10000
8000
6000
4000
2000
0
Sep 10
Sep 17
Sep 24
Oct 01
China
https://torproject.org



Tor project -- www.torproject.org

Great Firewall targeting of Tor (circa 2011-2012)

TLS connections with particular ciphersuites flagged



From [Winter, Lindskog 2012]

https://gist.github.com/da3c7a9af01d74cd7de7

Tor client

TLS Handshake

Tor bridge

Pick random Nc

ClientHello, MaxVer, Nc, Ciphers/CompMethods

ServerHello, Ver, Ns, SessionID, Cipher/CompMethod

Pick random Ns

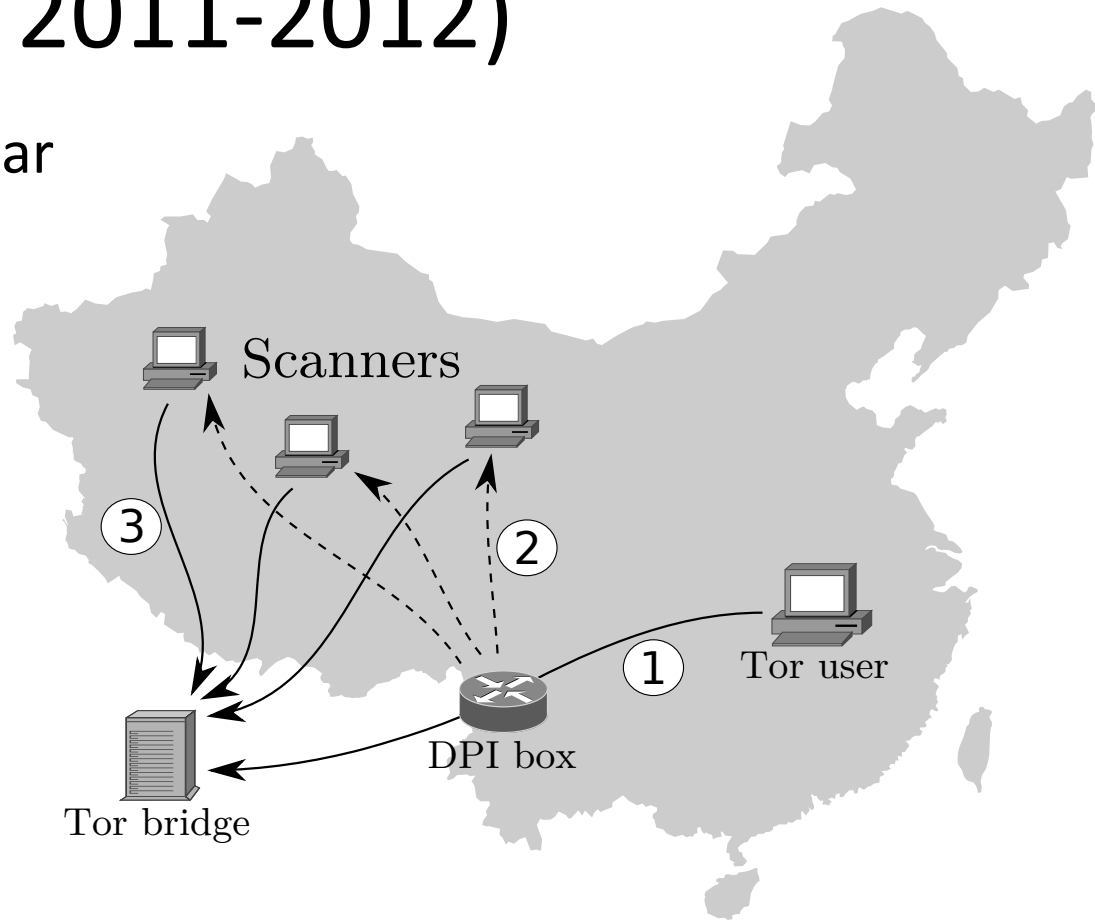
Tor clients use relatively non-standard Ciphers

Great Firewall targeting of Tor (circa 2011-2012)

TLS connections with particular ciphersuites flagged

Attempt to connect to dest IP by Tor client (source IP may be spoofed)

If server speaks Tor, then IP added to GFW black list

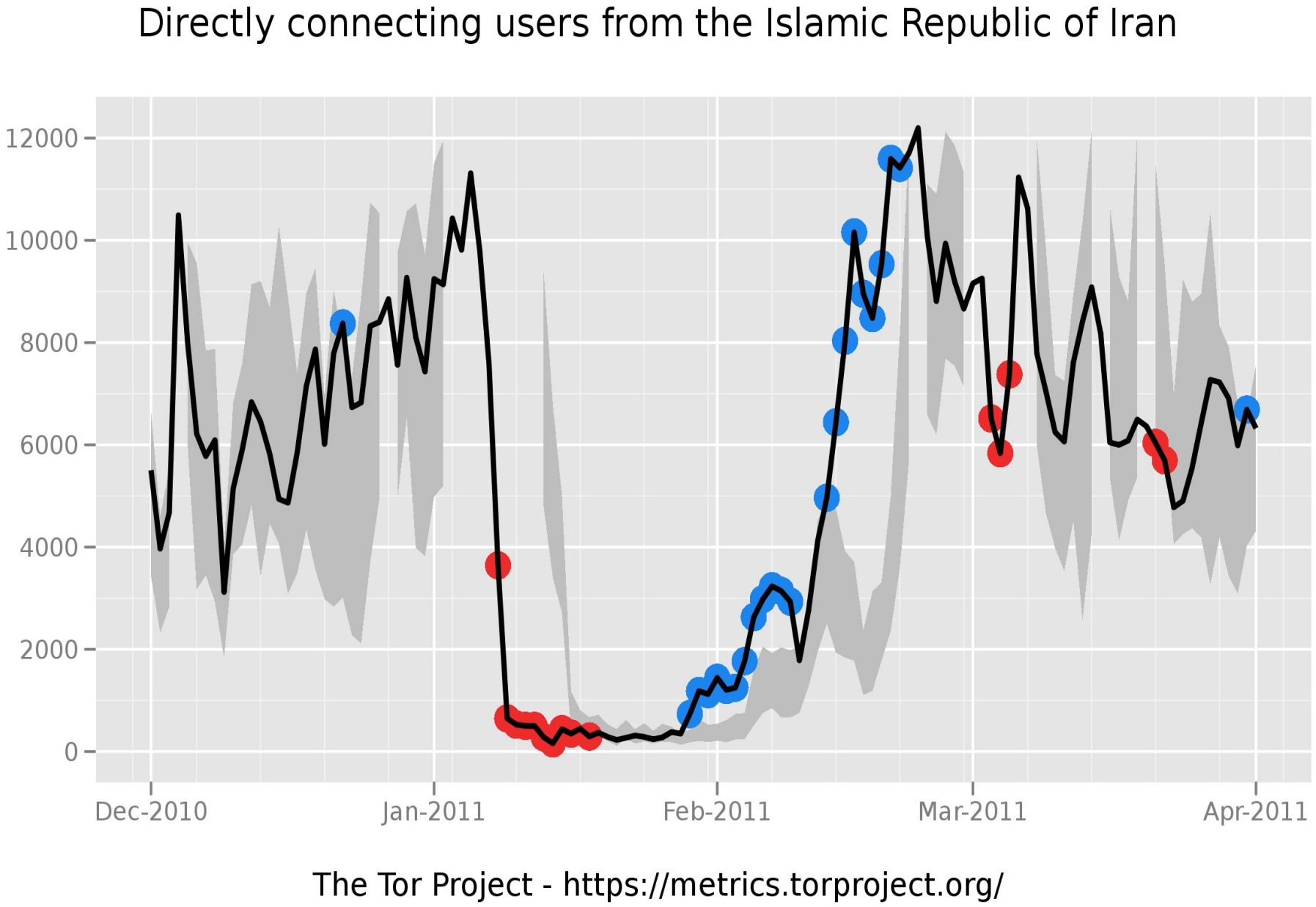


From [Winter, Lindskog 2012]

https://gist.github.com/da3c7a9af01d74cd7de7

Islamic Republic of Iran

- Every ISP must run “content-control software”
  - SmartFilter (up until 2009)
  - Nokia Siemens DPI systems
- According to wikipedia Facebook, Myspace, Twitter, Youtube, Rapidshare, Wordpress, BBC, CNN, all have been filtered
  - Big Web 2.0 security officer by way of Roger Dingledine (Tor project):
    - 10% (~10k) of traffic via Tor
    - 90% (~90k) of traffic via Amazon-hosted proxies


Directly connecting users from the Islamic Republic of Iran
12000
10000
8000
6000
4000
2000
0
Dec-2010
Jan-2011
Feb-2011
Mar-2011
Apr-2011
The Tor Project - https://metrics.torproject.org/

Iran DPI to shut down Tor

- Tor makes first hop look like TLS/HTTPS connection

Bank customer

TLS Handshake

Bank

Pick random Nc

ClientHello, MaxVer, Nc, Ciphers/CompMethods →

Pick random Ns

← ServerHello, Ver, Ns, SessionID, Cipher/CompMethod

Check CERT using CA public verification key

← CERT = (pk of bank, signature over it)

Pick random PMS
C <- E(pk,PMS)

C →

PMS <- D(sk,C)

ChangeCipherSpec,
{ Finished, PRF(MS, “Client finished” || H(transcript)) } →

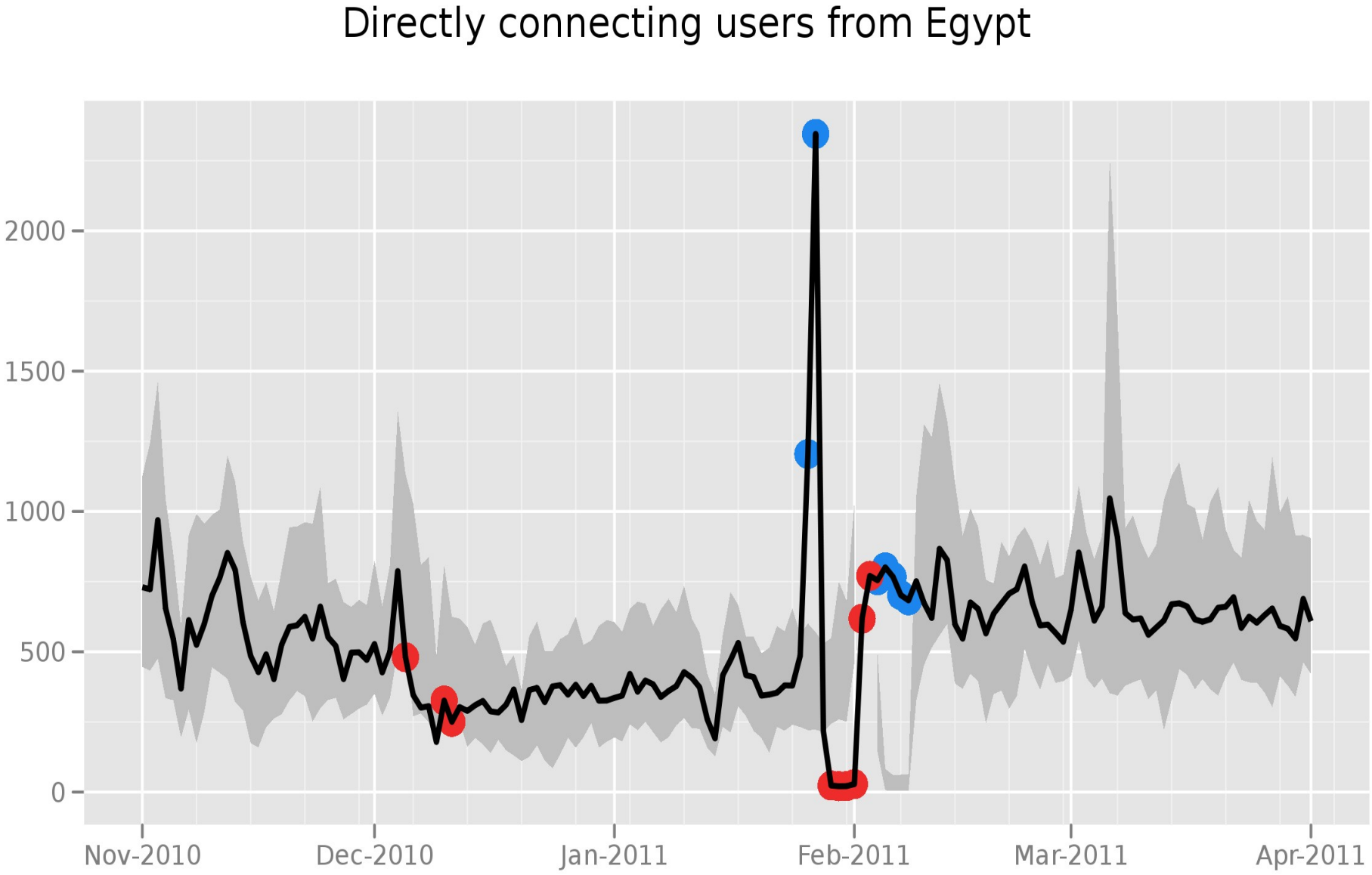
ChangeCipherSpec,
{ Finished, PRF(MS, “Server finished” || H(transcript’)) } ←

Bracket notation means contents encrypted

MS <- PRF(PMS, “master secret” || Nc || Ns)

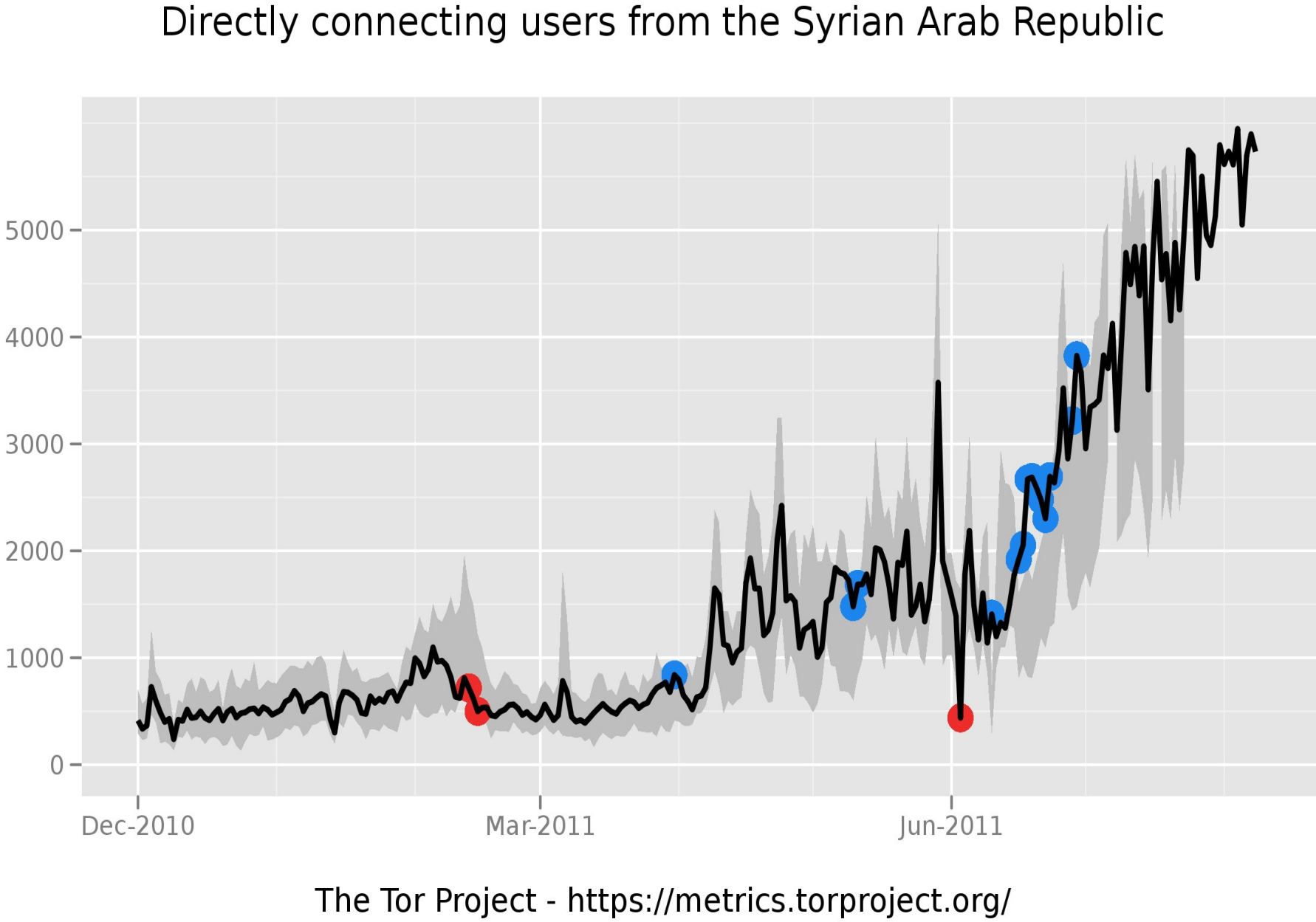
Iran DPI to shut down Tor

- Tor makes first hop look like TLS/HTTPS connection
- Use DPI to filter Tor connections:
  - Tor has short expiration date
  - Most websites have long expiration date
  - Shut down those connections with short expiration dates
- Tor fixed via longer expiration dates


Directly connecting users from Egypt
2000
1500
1000
500
0
Nov-2010
Dec-2010
Jan-2011
Feb-2011
Mar-2011
Apr-2011
The Tor Project - https://metrics.torproject.org/

From BlueCoat:

- Our awareness of the presence of these ProxySG appliances in Syria came from reviewing online posts made by so-called “hacktivists” that contained logs of internet usage which appear to be generated by ProxySG appliances. We believe that these logs were obtained by hacking into one or more unsecured third-party servers where the log files were exported and stored. We have verified that the logs likely were generated by ProxySG appliances and that these appliances have IP addresses generally assigned to Syria. We do not know who is using the appliances or exactly how they are being used. We currently are conducting an internal review and also are working directly with appropriate government agencies to provide information on this unlawful diversion.


Directly connecting users from the Syrian Arab Republic
5000
4000
3000
2000
1000
0
Dec-2010
Mar-2011
Jun-2011
The Tor Project - https://metrics.torproject.org/