Surveillance, Censorship, and Countermeasures

Professor Ristenpart

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

rist at cs dot wisc dot edu
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
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
Wiretap surveillance

Other major backbone

AT&T network

Interception gear

MAE-West (Metropolitan Area Exchange, West)

Large amounts of Internet traffic cross relatively few key points
Types of packet inspection

Internet service providers need only look at IP headers to perform routing.

Deep packet inspection (DPI) analyzes application headers and data.

Shallow packet involves investigating lower level headers such as TCP/UDP.
Is dragnet surveillance technologically feasible?

• CAIDA has lots of great resources for researchers about traffic levels

• From their SanJoseA tier-1 backbone tap:

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

generated 2011-11-15 17:13 UTC

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

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.

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)

IP: 1.2.3.4
Tor Node 7.8.9.1

Other major backbone

IP: 5.6.7.8
Tor Node 8.9.1.1

AT&T network

Interception gear

Tor Node 9.1.1.2

Other major backbone
Onion routing: the basic idea

HTTP packet

Src: 9.1.1.2  Dest: 5.6.7.8

Encrypted to 9.1.1.2

Src: 8.9.1.1  Dest: 9.1.1.2

Encrypted to 8.9.1.1

Src: 7.8.9.1  Dest: 8.9.1.1

Encrypted to 7.8.9.1

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

The Tor Project - https://metrics.torproject.org/
Other anonymization systems

• Single-hop proxy services

• JonDonym, anonymous 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

• Ask Alan on Thursday more about legal issues
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

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

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?

Src: 1.2.3.4
Dest: 5.6.7.8
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
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 McAfee

• Embargos prevent selling directly by USA companies, but resellers can do so
Circumvention of filtering

- IP filtering
- DNS filtering / redirection
- URL filtering
- Packet filtering (search keywords in TCP packets)
  - Send TCP FIN both ways
Circumvention of filtering

- IP filtering
  - Proxies
- DNS filtering / redirection
  - DNS proxy
- URL filtering
  - Encryption / Tunneling / obfuscation
- Packet filtering (search keywords in TCP packets)
  - Encryption/Tunneling / obfuscation

Src: 1.2.3.4
Dest: 5.6.7.8
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

The Tor Project - https://metrics.torproject.org/
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
Great Firewall targeting of Tor

- Enumerate Tor relays and filter them
Number of directory requests to directory mirror trusted
Directly connecting users from Egypt

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

The Tor Project - https://metrics.torproject.org/