Lessons from “the Snowden Affair”
What this talk is not
HERO OR TRAITOR?
IT DOESN’T MATTER
What do we learn from it?
What should we do differently?
Caveat: It’s a short talk
Best begin at..
NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

- Read the Verizon court order in full here
- Obama administration justifies surveillance

Glenn Greenwald
The Guardian, Thursday 6 June 2013
Jump to comments (2511)
U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program
The extent of the leak?
HE SAID

SHE SAID
How many documents?
NSA chief says Snowden leaked up to 200,000 secret documents

BY MARK HOSENBALL
WASHINGTON Thu Nov 14, 2013 4:04pm EST

http://www.reuters.com/article/2013/11/14/us-usa-security-nsa-idUSBRE9AD19B20131114
"I wish there was a way to prevent it. Snowden has shared somewhere between 50 (thousand) and 200,000 documents with reporters. These will continue to come out," Alexander said.
Although four months have passed since Edward Snowden's explosive NSA surveillance leaks, the most revealing details have not yet been published, and could be rolled out in the international media over the coming weeks and months, beginning with U.S. spying activities involving Spain and France. That's according to Glenn Greenwald, the Guardian journalist who broke the Snowden story last June, and whose life has been drastically upturned since.
Only 1% of Snowden files published - Guardian editor

NSA: Snowden Stole 1.7 MILLION Classified Documents And Still Has Access To Most Of Them
They had no idea what he had
Would You ?
Are your execs properly trained?
Snowden revelations of NSA spying on Copenhagen climate talks spark anger

Documents leaked by Edward Snowden show NSA kept US negotiators abreast of their rivals' positions at 2009 summit

John Vidal and Suzanne Goldenberg
theguardian.com, Thursday 30 January 2014 17.54 GMT
Jump to comments (733)

Developing countries have reacted angrily to revelations that the United States spied on other governments at the Copenhagen climate summit in 2009.

US climate envoy Todd Stern (right) and US secretary of state Hillary Clinton (left) give a press conference at the Bella Centra at the COP15 UN Climate Change Conference in Copenhagen, December 2009.
Photograph: Olivier Morin/AFP/Getty Images

(TS//SI//REL) Analysts here at NSA, as well as our Second Party partners, will continue to provide policymakers with unique, timely, and valuable insights into key countries' preparations and goals for the conference, as well as deliberations within countries on climate change policies and negotiating strategies. A late November report detailed China's efforts to coordinate its position with India and ensure that the two leaders of the developing world are working towards the same outcome. Another report provided advance details of the Danish proposal and their efforts to launch a "rescue plan" to save COP-15.

(TS//SI//REL) Given such large participation (with all 192 UN member states invited to attend), leaders and negotiating teams from around the world will undoubtedly be engaging in intense last-minute policy formulating; at the same time, they will be holding frequent sidebar discussions with their counterparts -- details of which are of great interest to our policymakers. While the outcome of the Copenhagen Climate Change Conference remains uncertain, signals intelligence will undoubtedly play a significant role in keeping our negotiators as well informed as possible throughout the 2-week event.

Diplomatic targets from all nations have an MO of using smartphones.
Exploited this use at the G20 meetings last year.

http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits
This included:

- Setting up internet cafes where they used an email interception programme and key-logging software to spy on delegates' use of computers;
- Penetrating the security on delegates' BlackBerrys to monitor their email messages and phone calls;
- Supplying 45 analysts with a live round-the-clock summary of who was phoning who at the summit;
- Targeting the Turkish finance minister and possibly 15 others in his party;
- Receiving reports from an NSA attempt to eavesdrop on the Russian leader, Dmitry Medvedev, as his phone calls passed through satellite links to Moscow.

http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits
Attackers like that don’t care about me / us
Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm

A cyber attack on Belgacom raised considerable attention last week. Documents leaked by Edward Snowden
NSA and GCHQ spoofed LinkedIn to hack Belgian cryptography professor

by David Meyer    FEB. 1, 2014 - 2:24 AM PDT

SUMMARY: Jean-Jacques Quisquater says the Belgian federal police tipped him off that he had been hacked in an attack related to that on telco Belgacom, which fell victim to GCHQ last year.

[Image: photo: Thinkstock]
Whatever the precise motive, on the face of it Quisquater is very much a civilian target — a professor emeritus, not a spy, a terrorist nor a member of government. It would be difficult for any intelligence agency to claim that stealing information from him is a matter of crucial national interest. The aftermath of this revelation will be worth watching.

(U) What is TREASUREMAP?

(U//FOUO) Capability for building a near real-time, interactive map of the global internet.

Map the entire Internet — Any device*, anywhere, all the time

(U//FOUO) We enable a wide range of missions:

- Cyber Situational Awareness — your own network plus adversaries’
- Common Operation Pictures (COP)
- Computer Attack/Exploit Planning / Preparation of the Environment
- Network Reconnaissance
- Measures of Effectiveness (MOE)

(* limited only by available data)

A slide from an NSA presentation explaining Treasure Map
Treasure Map: The NSA Breach of Telekom and Other German Firms

By Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Michael Sontheimer and Christian Grothoff

http://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html
These guys were collateral damage
Does collaboration protect you from getting hacked?
Dates When PRISM Collection Began For Each Provider

- Microsoft: 3/12/08
- Yahoo: 1/14/09
- Google: 6/3/09
- Facebook: 12/7/09
- PalTalk: 9/24/10
- YouTube: 2/6/11
- Skype: 3/31/11
- AOL: (added Oct 2012)
- Apple: 9/11/07

PRISM Program Cost: ~ $20M per year
Current Efforts - Google

GFE = Google Front End Server
SSL Added and removed here!
SSL Added to clear text here.

GFE = Google Front End Server

How many times were they spotted?
Complete failure of detection & compartmentalisation
<table>
<thead>
<tr>
<th>Commonality</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>79% of victims were targets of opportunity</td>
<td>-4%</td>
</tr>
<tr>
<td>96% of attacks were not highly difficult</td>
<td>+4%</td>
</tr>
<tr>
<td>94% of all data compromised involved servers</td>
<td>+18%</td>
</tr>
<tr>
<td>85% of breaches took weeks or more to discover</td>
<td>+6%</td>
</tr>
<tr>
<td>92% of incidents were discovered by a third party</td>
<td>+6%</td>
</tr>
<tr>
<td>97% of breaches were avoidable through simple or intermediate controls</td>
<td>+1%</td>
</tr>
<tr>
<td>96% of victims subject to PCI DSS had not achieved compliance</td>
<td>+7%</td>
</tr>
</tbody>
</table>
The good news is...
Do sophisticated attackers exist?
Estonia: To Black Out an Entire Country – part one

Fig. 1: Cyber Arsenal at hand for waging a Baltic cyber-war

- DoS/DDoS
- Web Defacement
- Others
Sophisticated Bank Cyber Attack Said to Target Core ...
www.foxbusiness.com/.../sophisticated-bank-cyber...
Fox Business Network
Aug 28, 2014 - A respected cyber security expert tells FOX Business the hackers who targeted JPMorgan Chase’s (JPM) computer systems were trying to send ...

New cyberattack on banks 'very sophisticated' - USA Today
www.usatoday.com/story/money/business/.../14730183/
USA Today
Aug 28, 2014 - JPMorgan Chase is working with the Federal Bureau of Investigation and other authorities to determine the scope of a cyberattack that ...

Cyber attacks are more sophisticated than ever – interview ...
www.theguardian.com › Professional › Media Network
The Guardian
Jun 27, 2013 - Cyber risks are growing exponentially and attacks are getting more sophisticated. The fragmented nature of such risks, from opportunistic ...

Sophisticated cyber-attack hits Energy Department, China ...
www.foxnews.com/.../sophisticated-cyber-attack-hits-
Fox News Channel
Feb 4, 2013 - The Energy Department has been hit by a major cyber-attack which resulted in the personal information of several hundred employees being ...

Apple Computers Hit by Sophisticated Cyberattack ... - Bits
bits.blogs.nytimes.com/.../apple-computers-hit-by-sophisticated-cyberattack...
Feb 19, 2013 - After Facebook and Twitter announced that they were breached by
Conclusion?

- Attacking is (much) cheaper than defense.
- Attacker toolchains are far more complex than the public demonstrations we have seen so far.
- Just because it isn’t .mil, doesn’t mean it’s any less of a target.
- A reasonably funded, intelligent adversary can relatively easily make serious inroads into strategically important targets doing the same thing, some pen-test firms have been doing forever.

http://blog.thinkst.com/p/cyberwar-why-your-threat-model-is.html
So..

- The attacks we see are not the sorts of attacks we should be losing sleep over
  - Professionals can be really (really) patient
- We need to keep in mind that not every actor is a nation-state
- We need to consider non-military targets
- We (desperately) need to re-evaluate our threat models
  - Charlie Miller: “My exploit wouldn’t have crashed your browser/reader”

http://blog.thinkst.com/p/cyberwar-why-your-threat-model-is.html
Do sophisticated attackers exist?
This is profoundly important
Device Based Security
Anti Virus
Pen Tests
we said victory accomplished
Device based Security
The truth is, consumer-grade antivirus products can’t protect against targeted malware created by well-resourced nation-states with bulging budgets. They can protect you against run-of-the-mill malware: banking trojans, keystroke loggers and e-mail worms. But targeted attacks like these go to great lengths to avoid antivirus products on purpose. And the zero-day exploits used in these attacks are unknown to antivirus companies by definition. As far as we can tell, before releasing their malicious codes to attack victims, the attackers tested them against all of the relevant antivirus products on the market to make sure that the malware wouldn’t be detected. They have unlimited time to perfect their attacks. It’s not a fair war between the attackers and the defenders when the attackers have access to our weapons.
Anti Virus

Flame was a failure for the antivirus industry. We really should have been able to do better. But we didn’t. We were out of our league, in our own game.

http://www.wired.com/2012/06/internet-security-fail/
Pen Tests

http://blog.thinkst.com/2012/03/penetration-testing-considered-harmful.html
We are not modelling the right threats
Were all the attacks novel?
Nope.. Not even the ANT stuff
Many of these techniques were previously demonstrated.
**NIGHTSTAND**

Wireless Exploitation / Injection Tool

(TS//SI//REL) An active 802.11 wireless exploitation and injection tool for payload/exploit delivery into otherwise denied target space. NIGHTSTAND is typically used in operations where wired access to the target is not possible.

07/25/08

---

**IRATEMONK**

ANT Product Data

(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

06/20/08

---

**DROPOUTJEEP**

ANT Product Data

(TS//SI//REL) DROPOUTJEEP is a STRAIGHTBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

10/01/08

---

**GOPHERSET**

ANT Product Data

(TS/SI//REL) GOPHERSET is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls Phonebook, SMS, and call log information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08
Why didn't you know about them?
Q2 - 116 Security Events
257 conference days
http://thinkst.com/ts/free
Will the leaks make things better or worse?
Intelligence reforms may or may not happen..

but, from the point of view of sophisticated attacks
Courage is Contagious
life imitates..
Caveat
This doesn’t apply to everyone!
biggest mistake is thinking you are all the same..

http://blog.thinkst.com/2013/01/your-companies-security-posture-is.html
Summary

• If everything is important, nothing is important
• Your execs need training!
• Sophisticated attackers do exist
• It’s obvious the emperor has no clothes.
• Things are going to get a lot worse for a bit
Summary of Summary

Understand your threat model
Understand the space