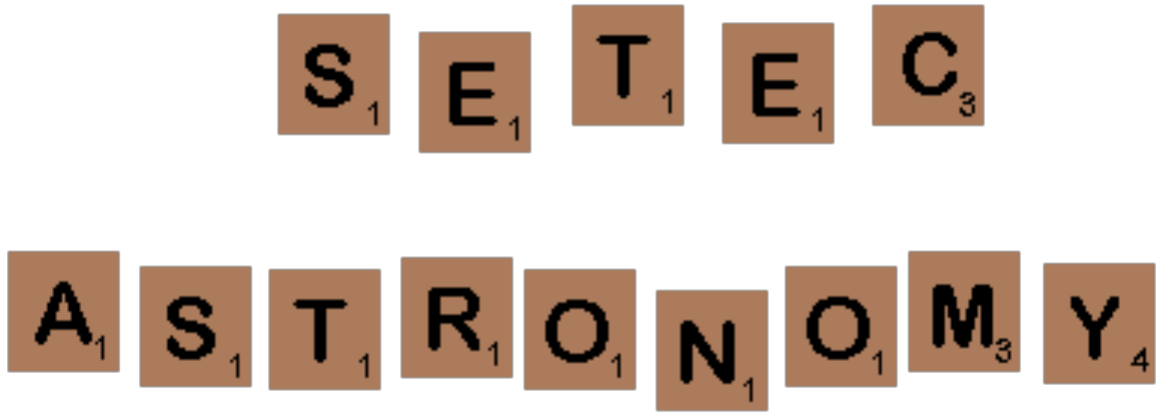

Summary of Recent Pervasive Monitoring Threats

Dave Thaler

November 6, 2013

Potential Threats

- We do not know what exactly has been done
  - Some might be real
  - Some might be pure speculation
  - Some might be research about what could be done in the future

- That said, we can try to reason about *potential* threats

- Allegations often generate demand to defend against threats

“Targeted” vs. “Pervasive” Monitoring

- Targeted: surveillance with a limited scope, e.g. a specific individual
- Pervasive: blanket surveillance, e.g. all users
- To paraphrase Bruce Schneier:

pervasive monitoring often seen as easier than targeted monitoring

- Bruce calls for goal to reverse this

- Goal of privacy mechanisms is usually:

Cost to get the information > Value of the information

Goal of surveillance is to collect information

- Common reasons given
  - Surveillance saves lives, combats crime
  - Surveillance used to protect against viruses, spam, hackers
  - Surveillance protects against information leaks (e.g., corp firewall)

- Information may or may not be encrypted
  - If so, goal is to get decrypted information

- Types of information
  - **Data:** files, email content, phone conversations, chat logs, etc.
  - **Metadata:** address, location, timestamps, size, keywords, etc. about data or traffic
  - **Keys:** secrets needed to decrypt data or metadata, or to impersonate
    - e.g., in order to collect more data via man-in-the-middle

Multiple strategies discussed in news

I. Overly get a cooperating entity with access to hand over info
   E.g. government may legally compel an entity within jurisdiction

II. Subvert a general service (serving many users) and covertly collect the information
   Often easier than overt mechanisms

III. Subvert target's system and covertly collect the information

Multiple ways to get secret/private keys

a) Obtain secret keys directly

b) Lower entropy used to generate keys, in order to more easily break them

c) Use existing known weaknesses

Multiple points of influence

1. Trusted roots & certificate authorities (e.g. DigiNotar)
2. Software creators & distributors
3. Data repositories (e.g. PRISM)
4. Protocol/algorithm designers (e.g. Dual_EC_DBRG)
5. Network operators (e.g. QUANTUM)
6. Physical fiber, wireless tower, satellite, etc. owners (e.g. MUSCULAR)
7. Hardware designers & factories (esp. with IoT)

Security/privacy is only as strong as the weakest link

Just about every combination of the last three axes is interesting

1. Trusted roots & certificate authorities

- Could get a fake cert from less trustworthy/compelled/compromised one
  - https://www.net-security.org/secworld.php?id=15579
- DigiNotar compromised, issued certs that were then used for impersonation
  - http://www.net-security.org/secworld.php?id=11555
- Flame used older cert issuing software to issue bad cert to spoof Microsoft
  - http://blogs.technet.com/b/msrc/archive/2012/06/03/microsoft-releases-security-advisory-2718704.aspx
- Debugging tools like Fiddler add another trusted root in order to act as man-in-the-middle and decrypt SSL
  - http://security14.blogspot.com/2010/07/how-to-use-fiddler-and-wireshark-to.html

2. Software creators & distributors

- Random number generators in code often unsafe, enables dictionary attacks or compromising a host with a weaker duplicate key
  - "There no need to panic over factorable keys – just mind your Ps and Qs"
- Compromised crypto APIs might leak key bits via fields that look random but actually relate to key
  - http://www.metzdowd.com/pipermail/cryptography/2013-September/017571.html
- Anonymity tools like Tor shift focus to attacking vulnerable software (e.g. browser), influencing development of such tools, or disrupting them to force using something else
  - http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption
  - https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html
- Checkin without sufficient review could introduce security backdoor
  - https://freedom-to-tinker.com/blog/felten/the-linux-backdoor-attempt-of-2003/
- Could be coerced into building in backdoors or handing over keys
  - http://www.upi.com/Top_News/US/2013/09/06/Documents-show-NSA-can-crack-most-Web-privacy-encryption/UPI-60871378450800/
- Could "Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets"
  - http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=0

3. Data repositories

- Could be compelled to hand over information, including secret key
  - http://www.theguardian.com/world/2013/jun/12/microsoft-twitter-rivals-nsa-requests
- Concerns over cloud storage also negatively affect such companies, e.g. Lavabit
  - http://www.wired.com/threatlevel/2013/10/lavabit_unsealed
- Other repositories may include airlines, energy companies, financial orgs, …
  - http://leaksource.files.wordpress.com/2013/09/nsa-brazil-4.png
- Bank transfers across borders go through a common system (SWIFT)
  - http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html
- Email metadata with two degrees of separation from target could be obtained
  - http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama
- Metadata can be correlated with other records (e.g. hotel guest lists) to identify individuals
  - http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance

4. Protocol & algorithm designers

- Potential for products influenced to use crypto known to be breakable, e.g. Dual_EC_DBRG (random number generator) is weak
  - http://arstechnica.com/security/2013/09/stop-using-nsa-influence-code-in-our-product-rsa-tells-customers/
- Could “Influence policies, standards and specification for commercial public key technologies”
  - http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=0
- Fear of influence over standards by governments or companies
  - http://policyreview.info/articles/news/technical-community-debates-over-taking-back-internet/215

5. Network operators

- Could install surveillance at exchange point, customer link, etc.
  - http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story_1.html
- "Tech firms and ISPs said they were coerced into handing over their master encryption keys or building in back doors"
  - http://www.upi.com/Top_News/US/2013/09/06/Documents-show-NSA-can-crack-most-Web-privacy-encryption/UPI-60871378450800/
- Attacker could hack into router to redirect traffic to man-in-the-middle
  - https://www.net-security.org/secworld.php?id=15579
- Could redirect target to website that plants malware, e.g. to subvert target
  - http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

6. Physical fiber, wireless tower, satellite, etc. owners

- Could tap links if have physical access
- Even those used by private clouds without knowledge of companies (data repositories, etc.) using them
- Especially if data is not encrypted between data centers
  - http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
  - http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
  - http://www.techdirt.com/articles/20131030/09554125066/nsa-breaks-into-yahoo-googles-data-centers-without-their-knowledge.shtml
  - http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story_1.html

7. Hardware designers & factories

- Manufacturer could insert a backdoor into product before shipped to a target
  - http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption
- Can insert hardware Trojans at designer or at factory, e.g. to reduce entropy or leak secret keys
  - http://people.umass.edu/gbecker/BeckerChes13.pdf
- Could influence encryption chips used in VPN and Web encryption devices
  - http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=0

Summary table (rough)

- Current discussions cover many possibilities
- More combinations are possible

		certs	software	repository	spec	operator	cables	hardware
		1	2	3	4	5	6	7
I. Compel/entice non-target		x	x	x		x	x	
	a) Get keys	x	x	x		x		x
	b) Lower entropy		x		x			x
	c) Insert weakness		x		x	x		x
II. Subvert non-target		x	x	x		x		
	a) Get keys		x					
	b) Lower entropy		x		x			
	c) Exploit weakness	x	x	x	x	x		
III. Subvert target		x	x	x				x
	a) Get keys		x					
	b) Lower entropy		x					
	c) Exploit weakness		x	x				