Pervasive Monitoring and the Internet

Jari Arkko Stephen Farrell Richard Barnes
IETF {Chair, SEC AD, RAI AD}*

*) Speaking as individuals & this presentation contains forward looking statements

What do we know?
What are the implications?
What can we do?

Background

- This year's allegations about the NSA, GCHQ, etc.
- But actually a wider issue around the world
- Not a surprise as such, but the scale and tactics have been surprising
- Strong reactions from many directions

Scope for This Discussion

- We should not have a political discussion
- Or use this forum to criticize activities
- But we MUST understand what dangers in general face Internet traffic
- And we SHOULD have an idea how Internet technology can better support security and privacy

These Are Attacks from the Perspective of Internet Protocols

- ... or indistinguishable from attacks
- Retrieved information could be used for good or bad; consider thieves stealing passwords
- Anything indistinguishable from an attack must be considered an attack

Likely Attack Vectors

- Unprotected communications (duh!)
- Direct access to the peer
- Direct access to keys (e.g., lavabit?)
- Third parties (e.g., fake certs)
- Implementation backdoors (e.g., RNGs)
- Vulnerable standards (e.g., Dual_EC_DBRG)

Vulnerable Standards?

- Bad random number generators (case Dual_EC_DBRG withdrawn NIST)
- Weak crypto (case RC4 & TLS)
- Some claims about other vulnerabilities in IETF standards (IPsec) and elsewhere but personally we believe this to be unlikely

What Can the Engineers Do?

- Technology may help - to an extent - but does not help with communications to an untrusted peer
- Prevent some attacks, make getting caught more likely, ...
- We need to do and be seen doing as much as we can - this **is** about the security of the Internet - and the time window is **now**

What Is the IETF Doing?

- Discuss the topic - openly
  - PERPASS, Plenary, IAB WS, WGs, RIPE, ...
- Work on the problem: threats, potential solutions...
  - A list at http://down.dsg.cs.tcd.ie/misc/perpass.txt
- Specific proposals: TLS algorithms & PFS
- Ongoing efforts with impacts: HTTP 2.0, TLS 1.3

Some Directions for Protection

- Unprotected communications - protect them!
- Vulnerable standards - public review, decommissioning old algorithms, additional review
- Implementation backdoors - diversity, open source, review

Final Words

- A crisis is painful, but it can also be an opportunity
- Maybe this is a reminder to us that there are challenges in Internet security [duh]
- We could now do even more than before: there's motivation, the web stack is undergoing significant evolution right now, TLS traffic is surging, ...
- It will not be easy - but set a high goal: web traffic 90% encrypted in 2016?

Welcome to Vancouver!
November 3-8, 2013

Wed 9am: Technical Plenary (IAB, Bruce Schneier, ...)
Wed 1pm: Handling Pervasive Monitoring in the IETF (BOF)
....

PERPASS list at https://www.ietf.org/mailman/listinfo/perpass

Thank You

Backup Slides for Reference and Links

(Note: We do not know how reliable and/or opinated this material is; it is merely provided here for your reference and easy access to the claims.)

Types of Reactions

- Various political and personal reactions
- Used as an argument in IG discussions
- NSA-envy in other intelligence agencies
- Increased the need for more diverse Internet (more IXPs, cables, services), good!
- Increased the calls for more nationally controlled Internets, bad!
- Engineers wondering what we can do

Known Existing Activities

- Lawful interception is a fact, at least for individual users (for both services and access)
- In some cases at least header information is collected for all traffic
- States are known to monitor Internet traffic passing through them

Low-Level Stuff

- Doping h/w from various places in production
  - http://people.umass.edu/gbecker/BeckerChes13.pdf
- Dual_EC_DBRG
  - http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf
  - http://arstechnica.com/security/2013/09/stop-using-nsa-influence-code-in-our-product-rsa-tells-customers/
- Other (P)RNG code in kernels etc. often unsafe
  - https://freedom-to-tinker.com/blog/nadiah/new-research-theres-no-need-panic-over-factorable-keys-just-mind-your-ps-and-qs/
- Stuxnet/Flame: different motive but similar modus-operandi
  - http://www.h4ckr.us/library/Documents/ICS_Events/Stuxnet%20Dossier%20(Symantec)%20v1.4.pdf
- *Even more paranoid: compromised crypto APIs might leak key bits through use of IVs that appear random but are actually related to application data encryption key*
  - *http://www.metzdowd.com/pipermail/cryptography/2013-September/017571.html*

Mid-Level Stuff

- Tempora
  - http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
- PRISM
  - http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
- XKEYSCORE
  - http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
- Phone records
  - http://www.theguardian.com/world/2013/sep/26/nsa-surveillance-intelligence-chiefs-testify-before-senate-live-updates
- Financial records
  - http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html
- Email records
  - http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama

High-Level Stuff

- MitM attacks on popular web sites (collaborating PKI?)
  - https://www.net-security.org/secworld.php?id=15579
- Directed breaches of ISP/provider n/w in Belgacom
  - http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html
- Meta-data vs. data
  - http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance
- Databases of passwords, secret and private keys, incl. Kerberos!
  - http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html reports on programme, from which some screenshots were posted...
  - http://leaksource.files.wordpress.com/2013/09/nsa-brazil-4.png (last bullet says “Results can frequently be verified using Kerberos etc. data”

Higher-Level Stuff

- "Legal" compulsion
  - http://www.theguardian.com/world/2013/jun/12/microsoft-twitter-rivals-nsa-requests
- Corporate collusion
  - (non-objective:-)
  - http://www.phibetaiota.net/2013/06/rickard-falkvinge-nsa-as-poster-child-for-government-corporate-corruption-collusion-treason/