IETF-88 Update: Pervasive Monitoring

Jari Arkko  Russ Housley
IETF Chair  IAB Chair

I. IETF-88 hot topics
II. The pervasive monitoring problem
III. What is the IETF doing about it?
Hot Topics at IETF-88

• Pervasive monitoring
• HTTP 2.0
• TLS 1.3
• Codec choices for WebRTC
• Evolution of transport protocols
Pervasive Monitoring - Scope for Discussion

- IETF is not a forum for political discussion
- Problem is actually wider issue in the world
- But we MUST understand what dangers in general face Internet traffic
- And we SHOULDN'T have an idea how Internet technology can better support security and privacy
It Is an Attack 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- Bad random number generators (case Dual_EC_DBGRG withdrawn by NIST)
- Weak crypto (case RC4 in 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, shift attacks from wholesale to targeted, ...

• 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
Some Directions for Protection

- Unprotected communications - protect them!
- Vulnerable standards - public review, decommissioning old algorithms, additional review
- Implementation backdoors - diversity, open source, review
What Is the IETF Doing?

- Discuss the topic - openly
  - PERPASS, Plenary, IAB WS, WGs, ...
- 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
- Bring together the different stakeholders to discuss the different solutions
Some High-Interest Efforts

- Various services turning on TLS far more in recent years than before -- this trend will now accelerate
- Algorithm clean-up -- implementations & specifications
- Security to be on by default for HTTP 2.0?
- What about DNS?
Further Reading & Watching

- Watch Bruce Schneier and others speak about the pervasive monitoring problem & technical solutions: http://www.ietf.org/live

- Join the IETF “perpass” mailing list: https://www.ietf.org/mailman/listinfo/perpass

- Join various working group mailing lists:
  - APPSAWG: http://tools.ietf.org/wg/appsgaw
  - HTTPBIS: http://tools.ietf.org/wg/httpbis
  - TLS: http://tools.ietf.org/wg/tls
Thank You