IETF Report

Report for the ISOC Board
November 22, 2013, Buenos Aires

Jari Arkko
IETF Chair

Russ Housley
IAB Chair

Hot Topics at IETF-88

- Pervasive monitoring
- HTTP 2.0
- TLS 1.3
- Codec choices for WebRTC
- Evolution of transport protocols
- Internet governance

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 evolve the technology

Background: 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)

Background: Role of Technology

- Technology helps to an extent - but not with communications to an untrusted peer
- Technology helps in some cases - prevent on-path attacks, make surveillance riskier/ more costly, etc.
- It is also important to do and be seen doing something about this
- Also an opportunity to improve Internet security

What Is the IETF Doing?

- Discuss the topic - openly
- Work on the problem: threats, potential solutions...
- Specific proposals: TLS algorithms & PFS
- Ongoing efforts with impacts: HTTP 2.0, TLS 1.3
- Securing different applications: web, xmpp, mail, ...
- None of this is easy - but we are a place to bring together the different stakeholders to discuss
- We've been visible in all of this

Outcome #1: It Is an Attack

- Plenary discussion & hopefully upcoming RFC
- 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

Outcome #2: Some High-Interest Developments

- 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?
- Work on applications, UTA WG, TLS 1.3

Challenges going Forward

- Understand that we have a unique opportunity but a limited time window
- Recognize limitation of technology, the long time scales needed - need to manage expectations
- Not clear that everyone who needs to participate in the discussion is doing so
- Increased use of secure communications is not technically easy & has significant trade-offs - just witness the httpbis discussions
- Long-term, we probably need other solutions as well as merely turning TLS on for more traffic