TLS 1.3 Wish List

Eric Rescorla
ekr@rtfm.com

IETF 87
August 1, 2013
Overview

- Started discussing idea TLS 1.3 in Orlando
- This would require rechartering
- What follows is a wish list for TLS 1.3
- Focus for now is on functionality, not how we do it
Reduce Handshake Latency

- TLS handshake setup requires 1-2 RTTs
  - 2 RTT for initial handshake
  - 1 RTT for resumption
- Targets
  - 1 RTT for at least some full handshakes
  - Provide at least one zero RTT mode (for repeated handshakes)
Encrypt Significantly More of Handshake

• Current handshake leaks essentially all negotiated information
  – Both sides identities
  – All extensions

• Target
  – Protect both sides identities from passive attackers
  – Protect at least one side’s identity from active attackers
  – Protect as many extensions and other information as possible

• This may not be the only mode
Improve Cross-Protocol Attack Resistance

• Signature in Server Key Exchange doesn’t cover entire handshake
  – Possible to exploit this to create confusion on client
    [Mavrogiannopoulos et al 2012]

• Target: do something about this
AEAD Cipher suites

• Convert entirely to AEAD cipher suites
  – Convert from AtE to EtA?
  – Deprecate CBC?
More Detail about Ciphers and Versions (Popov)

- TLS only allows indication of maximum version
- And cipher suite list applies to all versions
- Potential approach: distinct cipher lists for each supported version
SSLv2

- Potentially deprecate SSLv2 entirely (Popov)
Bigger Random Values (Housley, Turner)

- Current handshake Randoms are 28-bytes long
  - + 4 bytes of time
- Should we make these longer?
Triaging the Cipher List: Probably for both TLS 1.3 and Earlier

- Remove symmetric algorithms we are sad about (RC4?, CBC?)
- Potentially provide replacements if this creates holes
- Maybe add another MTI cipher suite (Popov)
- Revise cipher suite addition policy (Farrell)
Anything else?