TLS Best Current Practices

draft-sheffer-tls-bcp

Yaron Sheffer and Ralph Holz
Presented by **Paul Hoffman**

IETF-88, Vancouver

Motivation

- Provide clear guidance to confused TLS implementers
  - Several outstanding vulnerabilities
  - Some require app-level mitigations
  - Conflicts: move away from CBC and into RC4?!
- Pervasive passive monitoring a secondary, but important, motivation
- The BCP is based on existing standards, and on current or near-future implementations
  - Absolutely no new extensions – save your creativity to TLS 1.3
  - Which will obsolete the BCP

Approach

- A single ciphersuite (or a very small number of them), that:
  - A client should propose, along with its other ciphersuites
  - A server should accept, unless a stronger one is offered
- Plus a few more recommendations
  - 2048-bit RSA certificates
  - Disable fallback to SSLv3
  - Disable TLS-level compression
  - Possibly a word on session resumption

The Ciphersuite

- Should be secure in default use
  - E.g. should not require weird formatting of data records
- Widely implemented (at least) in libraries
- Well analyzed
- Supports forward secrecy
  - Next slide on what this implies
- At least 128-bits of strength

- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**
  - Yes, this requires TLS 1.2

DHE vs. ECDHE

- Modular Diffie-Hellman widely available, much more than Elliptic Curve DH
- However:
  - 1024 DH is considered insecure, important client implementations will fail the handshake if presented with >1024 DH
  - We only have crypto agility with ECDH (negotiated curves)
- Recommendations, in priority order:
  - ECDH: Brainpool with a fallback to P-256 (expect P-256 to be the prevalent curve in use for a while)
  - Ephemeral DH-2048: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - Ephemeral DH-1024

Next Steps

- Adopt this draft to the WG
- Update and add implementation info to Sec. 5
  - Appreciate your help!
- LC soon (before London?)

Thank You!

draft-sheffer-tls-bcp