TLS BCP, THE NEXT GENERATION

YARON SHEFFER, RALPH HOLZ AND PETER SAINT-ANDRE

IETF-107

BACKGROUND

- RFC 7525 (BCP 195) was published May 2015
  - With a companion RFC 7457 on TLS attacks
- Part of an industry push to mandate TLS 1.2
  - TLS 1.3 had not been published yet (RFC 8446, August 2018)
- As of Jan. 2020, we have 96% adoption of TLS 1.2, 22% adoption of TLS 1.3 (source: SSL Pulse) and these numbers continue to improve
- The document has been very successful
  - Over 100 IETF citations, dozens of external citations

INITIAL PLAN (1/2)

- Keep the scope and target audience: people who implement/deploy services that use TLS
- Add TLS 1.3 — as a SHOULD or a MUST?
- Definitively deprecate earlier TLS versions (cf. draft-ietf-tls-oldversions-deprecate)
- Update treatment of fallback in view of SCSV (RFC 7507)
- Indicate issues that are relevant only to TLS 1.2 vs. those that remain in TLS 1.3
- Specific TLS 1.3 gotcha: 0-RTT – what should we say here?
- Mention Certificate Transparency
- Mention Encrypted SNI

INITIAL PLAN (2/2)

- Recommend 1.3-only (no 1.2) for new "greenfield" protocols and embedding in a different context (e.g., as in QUIC)
- Provide guidance on handling of multiplexed protocols (RFC 8740)
- Provide guidance on handling TLS 1.2 renegotiation / tickets to ensure forward secrecy
- DTLS versions (recommend DTLS 1.3 if draft-ietf-tls-dtls13 is approved in time?)
- Remove (or move to appendix) issues that are mostly fixed (e.g., compression, renegotiation)
- Reword some of the background but leave the motivation (i.e. attacks) for TLS 1.2
- **Not** planning to revamp RFC 7457

NEXT STEPS

- Publish draft-sheffer-uta-bcp195bis-00 [done]
- Ask the UTA WG – home of the original document – to adopt

THANK YOU!

yaronf.ietf@gmail.com
ralph.holz@gmail.com
stpeter@mozilla.com