Deprecating TLSv1.0 and TLSv1.1

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Stephen Farrell & Kathleen Moriarty

Updates and Questions

Updates since last revision primarily editorial including add of DTLS1.0 in abstract

RFC8261 has the following text:

- The DTLS implementation MUST support DTLS 1.0 [RFC4347] and SHOULD support the most recently published version of DTLS, which was DTLS 1.2 [RFC6347] when this RFC was published. In the absence of a revision to this document, the latter requirement applies to all future versions of DTLS when they are published as RFCs. This document will only be revised if a revision to DTLS or SCTP makes a revision to the encapsulation necessary.
- Should we be more explicit about DTLS 1.0 in light that this was recent work?
    -

Updates and Questions Continued

Outstanding questions for WG:

- TLS/NNTP - RFC 8143 (updating RFC 4642) states in Section 3:
  - The best current practices documented in [BCP195] apply here. Therefore, NNTP implementations and deployments compliant with this document are REQUIRED to comply with [BCP195] as well.
  - Authors think there's a slight distinction and doesn't hurt to include an update
    - SHOULD NOT != MUST NOT

Reference for 3GPP deprecating TLSv1.0 and 1.1

- Yes, you can find the 3GPP TLS profile in Clause 6.2 of 3GPP TS 33.210
- https://www.3gpp.org/DynaReport/33210.htm

Document updates

- Note added to the draft wondering what to do about that but didn't add 8261 to the list of RFCs UPDATEd by this.
- Should RFC7525 be on the list? We think yes, in editor’s copy.
- RFC 6460 is suite-B which is already historic, so it probably doesn't matter. Added to the mega-list of updated drafts by this draft.
- RFC 6353 is SNMP/TLS so seems like a straightforward case. Added to list updated
- RFC 6084, which is "GIST" whatever that is. Added to list updated
- RFC 6083 is DTLS/SCTP. Added to the list updated
- RFC 6012 is DTLS for syslog. Added ,/to the list updated
- RFC 5456 is some asterisk-related protocol. Added to the list updated
- RFC 5415 is CAPWAP. Added to the list updated

Ready for WG last call?