Updates to the TLS Transport Model (TLSTM) for SNMPv3

23 March 2022, for IETF Operations and Maintenance Area WG

K. Vaughn

Background

- Effort approved after IETF 112
  - Update required due to fingerprint algorithm
    - One-octet hash algorithm identifier (from TLS 1.2 hashing algorithm table)
    - Hash of X.509 cert using identified algorithm
  - TLS 1.2 hashing algorithm table will no longer be maintained
- Comments received and addressed
- New draft (draft-ietf-opsawg-tlstm-update-01) posted

Options Considered for Fingerprint Algorithm

1. “Replace” fingerprint algorithm and related MIB objects to use new identifier table
   - Results in major overhaul to MIB
2. Require IANA to maintain TLS 1.2 hashing algorithm table
   - Objections from TLS community as this would imply the new algorithms could be used in TLS 1.2
3. “Clarify” fingerprint algorithm to reference a new TLSTM hashing algorithm table
   - Revises the text of the DESCRIPTION clause of SnmpTLSFingerprint
     - Updated MIB is the biggest component of the document (21 of 33 pages)
   - Creates a parallel hashing algorithm table that can be extended without raising TLS 1.2 concerns
   - Avoids any semantic changes to the MIB
   - Document becomes a minor update for RFC 6353

Other Items in Update (compared to RFC 6353)

- Clarify that authentication and privacy are always provided (i.e., a part of TLS 1.3)
- Remind readers of RFC 8996, which prohibits TLS versions prior to 1.2
- Prohibit use of the 0-RTT feature of TLS 1.3
- Clarify TLS compliance requirements
- Updates related to BCP 14 (i.e., capitalize key words, replace “MAY NOT” with “MUST NOT”)

Proposed edits yet to be made

- Rename RFC to “Updates to the TLS Transport Model (TLSTM) for SNMPv3”
  - i.e., remove references to TLS 1.3 in the title
- Remove double quotes in SnmpTLSFingerprint DESCRIPTION clause
- Remove references not used in this document
- Remove appendix examples
  - i.e., these are now identical to wheat is in RFC 6353
- Should we change the name of the proposed table? (e.g., might be useful for other standards to reference)
  - Currently: IANA SnmpTLSFingerprintAlgorithm Registry
  - Proposed: IANA Multiversion TLS Hash Algorithm Registry

Next Steps

- Comments?

- Distribute for final review to both OPSAWG and TLS email reflectors
- Initiate process to approve