TEEP over HTTP

draft-ietf-teep-otrp-over-http-06

Dave Thaler dthaler@microsoft.com

April 6, 2020

Timeline

- NOV 2019 (IETF 106): got consensus on one remaining issue (#5)
  - “deal with #5 and we can proceed with WGLC”
- FEB 2020: Draft updated and WGLC started, ended Feb. 26
  - Two reviews received during WGLC (thanks Russ and Tiru!)
- APR 2020: Subsequent re-check by Mark Nottingham for conformance with bcp56bis

Summary of Issues
https://github.com/ietf-teep/otrp-over-http

Issues with resolutions as discussed at IETF 106, resolved before WGLC:

~~1. Terminology alignment on transport layer implementation~~
~~2. HTTP Bindings~~
~~4. Relationship to TEEP protocol~~
5. Demuxing to OTrP vs TEEP protocol (remove OTrP)

Issues raised since WGLC initiated:

8. TEEP Server must support all message formats in Single API?
10. TLS considerations
11. Update examples to use teep+cbor media type
12. TAM certificate caching

Plus editorial feedback from Russ and Tiru

Actions taken for issues

- #8: TEEP Server must support all message formats in Single API?
  - Akira filed issue about how to send TAM a list of TA's a TEEP Agent wants to delete
  - Per discussion, this should be a TEEP Protocol issue not a transport issue, so can be closed for this draft (now teep-protocol issue #16)
- #11: Updated Content-Type in examples to use application/teep+cbor (not json) per TEEP protocol decision
  - Value is normative in TEEP protocol draft, just informative in transport doc

#10: TLS considerations

- Tiru asked for guidance (and privacy/security implications) around TLS 1.2
- MNot said bcp56bis avoided the issue since not HTTP specific
- Such considerations are covered in BCP 195 (“Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”)

- PROPOSED RESOLUTION: added bolded text
  - When HTTPS is used, TLS certificates MUST be checked according to [RFC2818]. **See [BCP195] for additional TLS recommendations.**

- Rationale:
  - BCP 195 already has IETF consensus
  - TEEP is secured end-to-end inside, so TLS considerations shouldn’t be TEEP specific

#12: TAM certificate caching

- OTrP spec had discussion about TAM certificate caching
  - Caching allows OTrP Agent to skip a round-trip and submit state information immediately, encrypted with TAM's public key
- TEEP spec uses OCSP_DATA that contains certs in QueryRequest but doesn't yet mention caching (filed issue #17 on teep-protocol)
- Change to clarify:
  - If the TEEP implementation already had ~~a~~ cached TAM ~~certificate~~ **OCSP_DATA** that it trusts **based on a previous QueryRequest**, it could skip to step 9 instead and generate a QueryResponse.

Other changes per feedback from Russ & Tiru

- Added note about User-Agent strings being implementation specific
- Added informative reference for QUIC
- Added note about NAT to note about firewalls

Other questions raised

- Why allow HTTP?
  - Previously discussed by WG, not a new issue
  - Main answer is for constrained devices since TEEP is e2e secure
  - Secondary answer is for debugging
- Why not specify HTTP error codes?
  - Specific codes may vary greatly by implementation
  - Don’t want receiver to base behavior on specific error code just 2xx, 4xx, or 5xx type
  - MNot (as httpbis reviewer) said it looked ok as is
- Why is bcp56bis an informative reference?
  - Security Considerations are relevant
  - Not used in any normative statement