TEEP Protocol
draft-ietf-teep-protocol-16

Dave Thaler <dthaler@microsoft.com>

Timeline

- June 1: WGLC ended
- July 3: draft-15 posted
- July 19: document shepherd writeup
- July 22: Hackathon 117 raised two issues
- Sept 4: draft -16 posted

Normative references

- draft-ietf-cose-key-thumbprint
- draft-ietf-rats-eat: submitted to IESG
- draft-ietf-suit-manifest: submitted to IESG
- draft-ietf-suit-trust-domains: WGLC done, revised I-D needed
- draft-ietf-suit-mti: in WGLC
- draft-ietf-suit-report: getting ready for WGLC

Changes since IETF 117

Draft-16

Changes in draft-16

Agreed by implementers at Hackathon 117 and presented at IETF 117:

- #347: err-code and err-msg in Update message
- #349: kid in EAT profile, COSE Key Thumbprint

Editorial addition to Security Considerations

- Replay Protection
  - The TEEP protocol supports replay protection as follows. The transport protocol under the TEEP protocol might provide replay protection, but may be terminated in the TEEP Broker which is not trusted by the TEEP Agent and so the TEEP protocol does replay protection itself. If attestation of the TAM is used, the attestation freshness mechanism provides replay protection for attested QueryRequest messages. If non-attested QueryRequest messages are replayed, the TEEP Agent will generate QueryResponse or Error messages, but the REE can already conduct Denial of Service attacks against the TEE and/or the TAM even without the TEEP protocol. QueryResponse messages have replay protection via attestation freshness mechanism, or the token field in the message if attestation is not used. Update messages have replay protection via the suit-manifest-sequence-number (see Section 8.4.2 of [I-D.ietf-suit-manifest]). Error and Success messages have replay protection via SUIT Reports and/or the token field in the message, where a TAM can detect which message it is in response to.

New issues

#354: No mention about EATs and SUIT Reports created by the TAM

- Ken writes:
  - “Section 8.2. of draft-ietf-teep-protocol-16 doesn't mention about EATs and SUIT Reports in the QueryRequest message created by the TAM. I'm not sure that they SHOULD be encrypted for each TEEP Agent.”

#355: Do we need to refer SUIT Report as normative?

Ken: “As SUIT Report can be embedded into measres claim of EAT, the attestation-payload is also appropriate option to carry it.

- Do we refer SUIT Report as normative or informative?
- Can we remove suit-reports option? And then, from which message? {QueryRequest and QueryResponse messages, or all messages}

I prefer option 1 but it might be a drastic change. The next best is option 2.

- option 1: Remove suit-reports option from all messages
  - Mentioning about SUIT Reports as one of claims of attestation-payload, and refer it as informative document
  - Change the data type of attestation-payload from bstr to [+bstr] to carry multiple SUIT Reports
- option 2: Remove suit-reports option from QueryRequest and QueryResponse messages
  - Embedding "boot" time evidence in EAT and set it in attestation-payload option
  - Because it doesn't match to manifest-list, and it can be conveyed in attestation-payload option
- option 3: Remain suit-reports option and normative reference
  - Because they match to manifest-list option in Update message”

- Previously discussed in TEEP, rational for option 3 (current state) was:
  - When the attestation payload contains Evidence, the attestation payload instead is opaque and goes to the Verifier.
  - The TAM often needs to process the SUIT reports itself, and should not rely on the Verifier copying them into Attestation Reports.

#356: No reference to each suit-cose-profiles

- draft-ietf-suit-mti-02 has replaced two profiles we depends.

Before -01	After -02
suit-sha256-es256-ecdh-a128gcm	suit-sha256-ecdsa-ecdh-a128ctr
suit-sha256-eddsa-ecdh-a128gcm	suit-sha256-eddsa-ecdh-a128ctr

- Should we replace each of them?

Next steps

- Anything else before submitting to IESG?
- Goal is to be done by IETF 118