TEEP Protocol
draft-ietf-teep-protocol-17

Dave Thaler <dthaler@microsoft.com>

Timeline

- June 1: WGLC ended
- July 19: document shepherd writeup
- July 22: Hackathon 117 raised two issues
- July 23: Doc shepherd writeup done
- Sept 4: draft -16 posted
- Sept 11: SUIT/TEEP interim meeting discussion
- Oct 23: draft -17 posted, with suit-mti dependency issue remaining

Normative references

- draft-ietf-cose-key-thumbprint
- draft-ietf-rats-eat: Approved-announcement to be sent::AD Followup
- draft-ietf-suit-manifest: submitted to IESG
- draft-ietf-suit-trust-domains: WGLC done, revised I-D needed
- draft-ietf-suit-mti: WGLC done, revised I-D needed
- draft-ietf-suit-report: ready for WGLC

Changes since interim (draft-17)

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

- As discussed & agreed in interim
- So not repeated here

#364: *.suit Filename

- Removed “.suit” from end of example of suit manifest filenames
- Avoids implying this is a required or registered file extension

#365: Evidence opaque to TAM

- Removed unnecessary confusing sentence, in informative text:

"TEEP requires algorithms for various purposes:

- Algorithms for signing TEEP messages exchanged between the TEEP Agent and the TAM.
- Algorithms for signing EAT-based Evidence sent by the Attester via the TEEP Agent and the TAM to the Verifier. ~~(If evidence is not encrypted by the TEEP Agent then it will be opaque to the TEEP Agent and to the TAM.)~~
- Algorithms for encrypting EAT-based Evidence sent by the TEEP Agent to the TAM. (The TAM will decrypt the encrypted Evidence and will forward it to the Verifier.)
- Algorithms for signing and optionally encrypting SUIT reports sent by the TEEP Agent to the TAM.
- Algorithms for signing and optionally encrypting SUIT manifests sent by the Trusted Component Signer to the TEEP Agent."

#367: Encryption functionality incomplete

- ~~To perform encryption with ECDH the TEEP Agent needs to be in possession of the public key of the recipient, i.e., the TAM. See Section 5 of [RFC9397] for more discussion of TAM keys used by the TEEP Agent.~~
- Ephemeral-Static Diffie-Hellman (ES-DH) is a scheme that provides public key encryption given a recipient's public key. Hence, the TEEP Agent needs to be in possession of the public key of the TAM. See Section 5 of [RFC9397] for more discussion of TAM keys used by the TEEP Agent. There are multiple variants of this scheme; **this document uses the variant specified in Section 8.5.5 of [RFC9052]**.
- The following two layer structure is used:
  - Layer 0: Has a content encrypted with the Content Encryption Key (CEK), a symmetric key. For encrypting SUIT Reports and EATs the content MUST NOT be detached.
  - Layer 1: Uses the AES Key Wrap algorithm to encrypt the randomly generated CEK with the Key Encryption Key (KEK) derived with ES-DH, whereby the resulting symmetric key is fed into the HKDF-based key derivation function.
- As a result, the two layers combine ES-DH with AES-KW and HKDF.
- This document re-uses the CDDL defined in Section 6.2.3 of [I-D.ietf-suit-firmware-encryption] and the context information structure defined in Section 6.2.4 of [I-D.ietf-suit-firmware-encryption] although with an important modification. The **COSE_KDF_Context.SuppPubInfo.other value MUST be set to "SUIT Report Encryption"** when a SUIT Report is encrypted and **MUST be set to "EAT Encryption" when an EAT is encrypted**. The COSE_KDF_Context.SuppPubInfo.other field captures the protocol in which the ES-DH content key distribution algorithm is used.

#371: TEEP profile identification

- EAT spec now uses URNs for EAT profiles, e.g.:
  - The identifier for this profile is "**urn:ietf:rfc:rfcTBD**".
- OLD media type:
  - “application/eat+cwt; eat_profile= **https://datatracker.ietf.org/doc/html/draft-ietf-teep-protocol-12**”
- NEW media type:
  - “application/eat+cwt; eat_profile= **urn:ietf:rfc:rfcXXXX**”
  - (RFC-editor: upon RFC publication, replace XXXX above with the RFC number of this document.)

Changes this week (draft-18)

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

- draft-ietf-suit-mti has updated profiles we depend on

Before (-01)	After (-03)	Notes
suit-sha256-es256-ecdh-a128gcm	suit-sha256-es256-ecdh-a128gcm	Unconstrained w/ ES256
suit-sha256-eddsa-ecdh-**a128gcm**	suit-sha256-eddsa-ecdh-**chacha-poly**	Unconstrained w/ EdDSA
-	suit-sha256-es256-ecdh-a128ctr	Constrained w/ ES256
-	suit-sha256-eddsa-ecdh-a128ctr	Constrained w/ EdDSA

- TEEP consensus was:
  - TAM must implement both
  - TEEP Agent can pick either
- Propose resolution discussed at hackathon:
  - Same but now TAM has to implement all four

#379 [Hackathon 118] No selected-suit-cose-profile (1/3)

Freshness mechanism negotiation:

- QueryRequest: list all TAM has, use one
- Error: ERR_UNSUPPORTED_FRESHNESS_MECHANISMS, list ones Agent has
- QueryResponse: use the one from QueryRequest

TEEP cipher suite negotiation:

- QueryResponse: list all TAM has, use all
- Error: ERR_UNSUPPORTED_CIPHER_SUITES, list ones Agent has
- QueryResponse: use one, and list it (removed in -18)

#379 No selected-suit-cose-profile (2/3)

SUIT cose profile negotiation:

- QueryRequest: list all TAM has, maybe use one in suit-reports
- Error: ERR_UNSUPPORTED_SUIT_REPORT, list ones Agent has
- QueryResponse: -
- Update: use in manifest-list
- Error: ERR_MANIFEST_PROCESSING_FAILED, and suit-reports with details
  - suit-report-result-code
  - (no way to list all supported, but will be addressed in SUIT Report spec)
- Success: suit-reports with details

#379 No selected-suit-cose-profile (3/3)

So changes in -18 are:

- Remove (redundant) selected-teep-cipher-suite from QueryResponse
- Add optional supported-suit-cose-profiles to Error message
  - Like supported-teep-cipher-suites & supported-freshness-mechanisms
- Add ERR_UNSUPPORTED_SUIT_REPORT error code
- Specify how to use SUIT Reports in QueryRequest received:

  The TEEP Agent MAY also use (in any implementation specific way) any SUIT Reports in the QueryRequest in determining whether it trusts the TAM. If a SUIT Report uses a suit-cose-profile that the TEEP Agent does not support, then the TEEP Agent MUST send an Error Message with the error code ERR_UNSUPPORTED_SUIT_REPORT supplying the supported-suit-cose-profiles.

Next steps

- Anything else before submitting to IESG?
- Goal is to be done now