TEEP Architecture

draft-ietf-teep-architecture-18

Dave / Hannes (presenting)

Ming Pei, David Wheeler, Hannes Tschofenig

Timeline

- JAN 2020: WGLC completed
- JUL 2021: Draft-15 submitted to IESG
- JAN 2022: AD (Ben) feedback
  - https://mailarchive.ietf.org/arch/msg/teep/QJCjyUP-0vErQODB5-_PkvrKMXc/
- FEB 2022: Updated draft-16 to address AD feedback
  - https://mailarchive.ietf.org/arch/msg/teep/eW5OokuMPYGIIdRGKn1vbF14uQs/
- JUN 2022: Updated draft-17 / draft-18 to address AD feedback
  - Russ Housley: https://mailarchive.ietf.org/arch/msg/teep/ZqnA29413S3cT_Quz-UJzCQLJ5E/
  - Brendan Moran: https://mailarchive.ietf.org/arch/msg/teep/0s96d_ufFUv5_L4ObU5n2NIkdJo/
  - Carl Wallace: https://mailarchive.ietf.org/arch/msg/teep/sKBF1n1myOSY0HRXB-P5XWOXkHo/
  - Ben Kaduk: https://github.com/ietf-teep/architecture/issues/239

Section 3.3: Clarification on IoT device threat

Section 3.3:

- Weak security in Internet of Things (IoT) devices has been posing threats to critical infrastructure that relies upon such devices.

Russ’s comment:

- I'm a bit confused by this opening sentence. IoT devices usually depend upon an infrastructure. This seems to be talking about an infrastructure that depends upon a collection of IoT devices. **I suggest a minor edits to help the reader understand that this sentence is not talking about network infrastructure.**

Fixed in draft-17 with the following:

- Weak security in Internet of Things (IoT) devices has been posing threats to critical infrastructure, i.e., assets that are essential for the functioning of a society and economy.

Section 9.3: Expand compromised REE threat

Section 9.3 says:

- The compromised REE … **might drop or delay** messages between a TAM and a TEEP Agent.

Russ's comment:

- This discussion should be expanded to include the **replay** of messages

Fixed in draft-17 with the following:

- The compromised REE may terminate the TEEP Broker such that TEEP transactions cannot reach the TEE, or might drop**, replay,** or delay messages between a TAM and a TEEP Agent.

Section 9.4: Clarification of Root CA vs Trust Anchor

Section 9.4 says:

- A root CA for TAM certificates might get compromised or its certificate might expire, or a Trust Anchor other than a root CA certificate may also expire or be compromised.

Russ’s comment:

- I do not understand the difference between a Root CA and a Trust Anchor. These are usually used a synonyms. Please explain the difference that in intended here.

Clarification:

- [Ming] When it is a certificate, it doesn't have to be the root certificate. It could be an issuing CA while it isn't a common practice.
- [Russ] I think the point about not a "Root Certificate" in all situations is very helpful. Please add that to the document.

Fixed in draft-17 by clarifying the Trust Anchor’s definition:

- The Trust Anchor may be a certificate, a raw public key or other structure, as appropriate. **It can be a non-root certificate when it is a certificate.**

Clarification on Trust Anchor Constraints

Trust Anchor Definition:

- “A trust anchor represents an authoritative entity via a public key and associated data. … The Trust Anchor may be a certificate or it may be a raw public key.”

Carl’s comment:

- Is it a certainty that constraints will not be needed for trust anchors? The trust anchor definition references “associated data”, which would be used constrain use of the trust anchor. An option other than certificate or public key may would be needed if constraints may be defined (because constraints can’t be added to the certificate without breaking the signature and a raw public key has no means to express constraints).
- **Perhaps, "The Trust Anchor may be a certificate, a raw public key or other structure, as appropriate." might be better to leave open the possibility of constraining a trust anchor.**

Fixed in draft-17 by revising the Trust Anchor’s definition:

- The Trust Anchor may be a certificate, a raw public key **or other structure, as appropriate.** It can be a non-root certificate when it is a certificate.

Section 4.4: Clarification about Personalization Data Protection Mechanism

Section 4.4 says:

- … Implementations must support encryption of such Personalization Data to preserve the confidentiality of potentially sensitive data contained within it, and must support integrity protection of the Personalization Data.

Russ’s comment:

- Why not say that implementation must support mechanisms for the confidentiality and integrity protection of such Personalization Data?
- Also, it seems like draft-ietf-suit-firmware-encryption offers one mechanism for such protection. Should it be referenced here?

Ben’s comment on revision draft-17:

- We may want to split the confidentiality and integrity protection guidance into separate clauses or even separate sentences to be clear about what behavior is required.

Fixed in draft-18 with the following: (Use two sentences to bring further clarity)

- Implementations must support encryption to preserve the confidentiality of such Personalization Data, which may potentially contain sensitive data. Implementations must also support mechanisms for integrity protection of such Personalization Data.

Other Nits Update (Russ’s comments)

1. Section 1 says:

  - … The problems in the bullets above, on the other hand, require a new protocol, i.e., the TEEP protocol, for TEEs that can install and enumerate TAs in a TEE-secured location and where another domain-specific protocol standard (e.g., [GSMA], [OTRP]) that meets the needs is not already in use.

- Recommend breaking this long sentence up into at least two sentences.
  - There are two points. First, the need for a protocol to address the items listed earlier. Second, where an existing domain-specific protocol does not already exist, a new more general protocol is needed.
- Fixed in draft-17 as follows:
  - The problems in the bullets above, on the other hand, require a new protocol, i.e., the TEEP protocol. The TEEP protocol is a solution for TEEs that can install and enumerate TAs in a TEE-secured location where another domain-specific protocol standard (e.g., [GSMA], [OTRP]) that meets the needs is not already in use.

2. Russ’s comment: App Store vs. Trust Anchor Store in Section 4

  - Section 4: Is an "App Store" a place where apps are stored, or is it a place where apps a purchased? The term seems to be used both ways, and in one place, the document is very general by saying, "an app store or other app repository". Elsewhere, the term "Trust Anchor Store" is clearly a place for storage of trust anchors.

- Resolution: added definition about “App Store”:
  - App Store: an online location from which Untrusted Applications can be downloaded.

3. Section 9.7: Please consider changing the section title to be something like: "**TEE** Certificate Expiry and Renewal” from “Certificate Expiry and Renewal”

  - Changed as suggested

Threat Modality

Section 1 says:

- TEEs are typically used in cases where a software or data asset needs to be protected from unauthorized **entities that may include the owner (or pwner)** or possesser of a device.

Brendan comment:

- The threat modality is is important for TEEs use cases; the user identity is not.

Fixed in draft-17 with the following:

- TEEs are typically used in cases where software or data assets need to be protected from unauthorised **access where threat actors may have physical or administrative access to a device**.