IETF 114 TEEP Hackathon

July 28, 2022

Akira Tsukamoto, AIST (presenting)
Dave Thaler, Microsoft
Hannes Tschofenig, ARM
Laurence Lundblade, Security Theory LLC.
David Brown, Linaro
Kohei Isobe, SECOM
Ken Takayama, SECOM

IETF 114 COSE SUIT TEEP Hackathon

- Date July 23 Saturday, July 24 Sunday
  - Jointly COSE, SUIT and TEEP

- First time to meet face to face after Hackathon in Berlin, February 2020

- Participants:

  Dave Thaler, Microsoft
  Hannes Tschofenig, ARM
  Laurence Lundblade, Security Theory LLC.
  David Brown, Linaro
  Kohei Isobe, SECOM
  Ken Takayama, SECOM
  Akira Tsukamoto, AIST

Objective and Plan

- Objective
  - Tackle all consideration points what we found after IETF113 for supporting EAT and COSE in TEEP protocol implementation

- Plan, going though issues list as much as possible on the github

The default values when selected-cipher-suite is empty in QueryResponse (Device -> TAM).
https://github.com/ietf-teep/teep-protocol/issues/182

SUIT_Report or SUIT_Parameters for device identifying information and TEE identifying information in QueryResponse.
https://github.com/ietf-teep/teep-protocol/issues/189

CDDL format of challenge and attestation-payload for supporting all CPUs.
https://github.com/ietf-teep/teep-protocol/issues/214

Additional message may require for local attestation on sgx
https://github.com/ietf-teep/teep-protocol/issues/215

Passing TEE hardware properties and TEE firmware properties
https://github.com/ietf-teep/teep-protocol/issues/213
teep-evidence -> sw-version-type -> other type of manifest -> 4.2.16 The Software Manifest claim ->

How to run CDDL diagnose with cddl file for TEEP Protocol.
https://github.com/ietf-teep/teep-protocol/issues/198

Behavior when selected-cipher-suite is empty in QueryResponse

- Query Request is sent from TAM to Device (TEEP-Agent) with asking `supported-ciphersuite` in Device.
- If `selected-ciphersuite` in QueryResponse was empty from Device, then it is nice to have specified default behavior what to do on TAM.
  - Issue
    https://github.com/ietf-teep/teep-protocol/issues/182

- Treated as if Device (TEEP-Agent) accepts any cipher suites listed in the QueryRequest, so TAM can select one.
  - PR
    https://github.com/ietf-teep/teep-protocol/pull/204

How TAM to obtain TEE identifying information of TEEP-Agent

- **Details covered in the Dave's TEEP Protocol slides**
- The device identifying information and TEE identifying information are critical for the TAM to determine which Trusted Components to install in the TEE on Device
  - Issue
    https://github.com/ietf-teep/teep-protocol/issues/189

- Two ways
- Adding `SUIT_reports` in QueryResponse to provide TEE identification on boot time at Device (TEEP-Agent)
  - PR
    https://github.com/ietf-teep/teep-protocol/pull/187
- Use `system-property-claims` instead of `tc-info` to determine Trusted Components to install in the TEE.
  - PR
    https://github.com/ietf-teep/teep-protocol/pull/228

Able to support both Evidence and Attestation Result

- Went though many iterations. Initial intention was to creating attestation-payload able to contain either Evidence or Attestation Result in QueryResponse. Was able to have only Evidence.
  - Issue
    https://github.com/ietf-teep/teep-protocol/issues/214
  - Issue
    https://github.com/ietf-teep/teep-protocol/issues/217
  - Issue
    https://github.com/ietf-teep/teep-protocol/issues/224 **in Dave's TEEP Protocol slides**

- Add description for the attestation-payload-format to have a string to let TAM to checks whether it contains Evidence or Attestation Result by inspecting the attestation-payload-format
  - PR
    Change the name of evidence to attestation-payload to make it contain both Evidence or Attestation Result
    https://github.com/ietf-teep/teep-protocol/pull/211

    Use `attestation-payload-format` for distinguish Evidence or Attestation Result
    https://github.com/ietf-teep/teep-protocol/pull/216/

May require additional message for Attestation

- **Details covered in the Dave's TEEP Protocol slides**
- For the "passport" model of Attestation, the way to include Attestation Result in a message coming from TAM to Device (TEEP-Agent) after the Query Response, was not specified in the current draft. Initially the issue came up when implementing it on both SGX and ARM.
  - Issue
    https://github.com/ietf-teep/teep-protocol/issues/215

- Adding `attestation-payload` in the Update message for this purpose
  - PR
    https://github.com/ietf-teep/teep-protocol/pull/230

Passing TEE hardware properties and TEE firmware properties

- Also went though many iterations. Initially was including hash values of TEE properties (hardware and/or firmware) in the QueryResponse, so TAM could check if they are healthy or not.
  - Issue
    https://github.com/ietf-teep/teep-protocol/issues/213
- Decide to use `manifest` in `evidence` in QueryResponse instead of `sw-version` for TEE firmware.
  - Issue
    https://github.com/ietf-teep/teep-protocol/issues/221 **in Dave's TEEP Protocol slides**

- The "manifests" claim should include information about the TEEP-Agent as well as any of its dependencies such as firmware.
  - PR
    https://github.com/ietf-teep/teep-protocol/pull/231

supported-ciphersuites mandatory in QueryRequest

- **Details covered in the Dave's TEEP Protocol slides**
- 2 ciphersuites defined as mandatory now, those could change in the future and making the TAM put `supported-ciphersuites` into the QueryRequest message explicitly is more future proof.
- Unify both strings `cipher-suites` and `ciphersuites` used in the CDDL to be `ciphersuites`.
  - Issue
    https://github.com/ietf-teep/teep-protocol/issues/222

- Moving `supported-ciphersuites` which were inside `option` to mandatory member.
- Locate the `supported-ciphersuites` under `option` member for
  - PR
    https://github.com/ietf-teep/teep-protocol/pull/223

Running cddl tool for CDDL grammar check

- Running the full CDDL diagnoses are recommended in RFC 8610.
  - Issue by Penglin Yang
    https://github.com/ietf-teep/teep-protocol/issues/198

- **Needs help here.** Not sure the correct way of using cddl tool at the moment. Finding my way of doing it after many try and error. Description in Appendix.
- To run the CDDL grammar, it require all other CDDL file dependent on TEEP protocol draft. Resulted finding some grammar error in SUIT manifest draft.
  - PR

    Splitting CDDL file from Markdown file for ease of use of cddl tool. SUIT doing the same
    https://github.com/ietf-teep/teep-protocol/pull/200

    Fixing errors in TEEP Protocol draft
    https://github.com/ietf-teep/teep-protocol/pull/201

    Feedback to SUIT manifest draft
    https://github.com/suit-wg/manifest-spec/issues/65
    https://github.com/suit-wg/manifest-spec/issues/67
    https://github.com/suit-wg/manifest-spec/pull/68

Summary

- The most drastic change in the TEEP Protocol draft in the past. Great achievement by meeting in person.
  11 Issues fixed in draft:
  #189, #202, #213, #214, #215, #217, #220, #221, #222, #224, #227
  9 PRs:
  #219, #223, #225, #228, #229, #230, #231, #232, #233

- Ruled out most of the issues for supporting COSE and EAT in TEEP Protocol draft. Getting closer for TEEP Protocol draft to become RFC.

- Next:
  - Revising implementations with changes made in the draft at IETF 114 and validate the completeness of the draft.

A part of this hackathon presentation is based on results obtained from a project, JPNP16007, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

Appendix

My procedure of cddl tool usage (1/2)

(1) Install cddl tool
$ sudo gem install cddl

(2) Prepare other CDDL files required for TEEP Protocol

(a-1) CDDL file for SUIT manifest
$ wget https://raw.githubusercontent.com/suit-wg/manifest-spec/master/draft-ietf-suit-manifest.cddl

(b-2) Fixing errors temporary by adding four lines to draft-ietf-suit-manifest.cddl just downloaded
COSE_Sign_Tagged = 98
COSE_Sign1_Tagged = 18
COSE_Mac_Tagged = 97
COSE_Mac0_Tagged = 17

(c) CDDL file for SUIT_Report
Create suit-report.cddl file by going at https://github.com/ietf-teep/teep-protocol/issues/212

(3) Creating CDDL file of TEEP Protocol

$ cat draft-ietf-suit-manifest.cddl suit-report.cddl draft-ietf-teep-protocol.cddl > check-draft-ietf-teep-protocol.cddl

(4) Run cddl tool
$ cddl check-draft-ietf-teep-protocol.cddl generate

Initial Items to tackle at Hackathon

The default values when selected-cipher-suite is empty in QueryResponse (Device -> TAM).
https://github.com/ietf-teep/teep-protocol/issues/182

SUIT_Report or SUIT_Parameters for device identifying information and TEE identifying information in QueryResponse.
https://github.com/ietf-teep/teep-protocol/issues/189

CDDL format of challenge and attestation-payload for supporting all CPUs.
https://github.com/ietf-teep/teep-protocol/issues/214

Additional message may require for local attestation on sgx
https://github.com/ietf-teep/teep-protocol/issues/215

Passing TEE hardware properties and TEE firmware properties
https://github.com/ietf-teep/teep-protocol/issues/213
teep-evidence -> sw-version-type -> other type of manifest -> 4.2.16 The Software Manifest claim ->

How to run CDDL diagnose with cddl file for TEEP Protocol.
https://github.com/ietf-teep/teep-protocol/issues/198

Apr 10, 2022 – Jul 25, 2022

Contributions: Commits

Contributions to master, excluding merge commits and bot accounts

ietf-teep / teep-protocol Public

Notifications | Fork 6 | Star 8

Code | Issues 25 | Pull requests | Actions | Projects | Wiki | Security | Insights

- Pulse
- Contributors
- Community Standards
- Commits
- Code frequency