IETF 115 TEEP Hackathon

November 09, 2022

Akira Tsukamoto

Dave Thaler, Brendan Moran, Hannes Tschofenig, Laurence Lundblade,
Kohei Isobe, Ken Takayama, Shinichi Miyazama

IETF 115 TEEP SUIT COSE RATS Hackathon

- Date: November 05 Saturday, 06 Sunday
  - Jointly with COSE, SUIT, RATS and TEEP

- Participants:

  Dave Thaler, Microsoft
  Hannes Tschofenig, ARM
  Brendan Moran, ARM
  Laurence Lundblade, Security Theory LLC.
  Kohei Isobe, SECOM
  Ken Takayama, SECOM
  Shinichi Miyazama, SECOM
  Akira Tsukamoto, AIST

Pictures

TEEP/SUIT
COSE/RATS
CONFIDENTIAL
COMPUTING
HACKATHON
IETF115
ENTIAL COMPUTING
NSORTIUM

Objective and Plan

- Objective
  - Hackathon items
    - Tackle all consideration points what we found after draft-11 for supporting EAT and COSE in TEEP protocol implementation

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

  - Method of distinguishing Evidence or Attestation Result in EAT profile
    - https://github.com/ietf-teep/teep-protocol/issues/263
  - Use CBOR tag on SUIT_Envelope or not.
    - https://github.com/ietf-teep/teep-protocol/issues/273
  - Having CDDL compilation warnings, would like to remove them
    - https://github.com/ietf-teep/teep-protocol/issues/278
  - Adding support of EdDSA in the implementation, now TEEP mandates both ES256 & EdDSA, Changed from using COSE sign1 to COSE sign only for QueryRequest
    - https://github.com/ietf-teep/teep-protocol/pull/267
  - Adding support of Unneeded manifest list in the implementation
    - https://github.com/ietf-teep/teep-protocol/pull/261
  - Update implementation of libcsuit to support the changes in draft-ietf-suit-manifest-20

Evidence or Attestation Result in EAT profile (1/2)

Link to the issue
https://github.com/ietf-teep/teep-protocol/issues/263

- If the TAM could distinguish attestation-payload would contain Evidence by only reading attestation-payload-format then the TAM could handover to the attestation-payload to Verifier without reading it or opening it.

- TEEP QueryRequest message has two members for this purpose
  ? attestation-payload-format => text
  ? attestation-payload => bstr
- Example of attestation-payload-format

/ Evidence /	Any string
/ Attestation Result /	"application/eat-cwt; eat_profile=https://datatracker.ietf.org/doc/html/draft-ietf-teep-protocol-10“

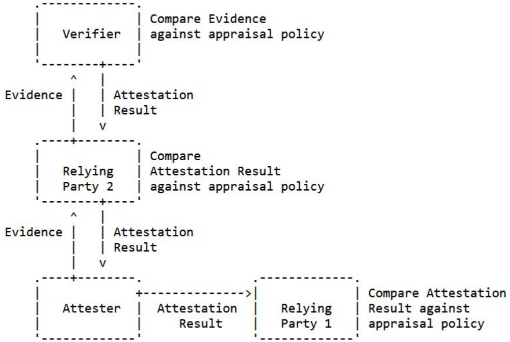
- If the attestation-payload-format has the exact matching string of above Attestation Result (AR) string, then the TAM will handle attestation-payload as AR and anything else will handover it to the Verifier because attestation-payload has Evidence.

- Did not have to change the draft

Evidence or Attestation Result in EAT profile (2/2)

- Combinations of Background check model and Passport model in RATS

draft of RATS Architecture

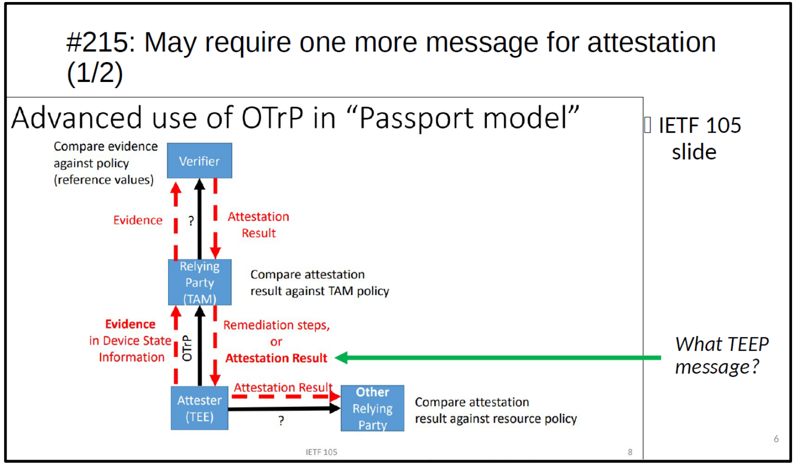


```
          .----------------.
          |                | Compare Evidence
          |    Verifier    | against appraisal policy
          |                |
          '--------+-------'
                ^      |
       Evidence |      | Attestation
                |      | Result
                |      v
          .-----+----------.
          |                | Compare
          |    Relying     | Attestation Result
          |    Party 2     | against appraisal policy
          '--------+-------'
                ^      |
       Evidence |      | Attestation
                |      | Result
                |      v
          .-----+----------.            .------------.
          |                +----------->|            | Compare Attestation
          |    Attester    | Attestation|  Relying   | Result against
          |                |    Result  |  Party 1   | appraisal policy
          '----------------'            '------------'
```

Figure 7: Example Combination

https://datatracker.ietf.org/doc/html/draft-ietf-rats-architecture

Slide of TEEP Protocol at IETF 114



#215: May require one more message for attestation (1/2)

Advanced use of OTrP in “Passport model”

Compare evidence against policy (reference values)
Verifier
Evidence
?
Attestation Result
Relying Party (TAM)
Compare attestation result against TAM policy
Evidence in Device State Information
OTrP
Remediation steps, or Attestation Result
Attestation Result
Attester (TEE)
?
Other Relying Party
Compare attestation result against resource policy
IETF 105
8
6

 IETF 105 slide

What TEEP message?

https://datatracker.ietf.org/meeting/114/materials/slides-114-teep-teep-protocol

- Update message was revised to have attestation-payload-format and attestation-payload to carry Attestation Result at IETF 114 hackathon.

- Add description in Update that attestation-payload uses only AR.
  Make PR later

Use CBOR tag or not on SUIT_ Envelope

Link to the issue

https://github.com/ietf-teep/teep-protocol/issues/273

- The TEEP messages were decided not to use CBOR tag on the Envelope but how about the Envelope for the SUIT manifest included in the TEEP Update message? The chapter “Complete CDDL” using untagged, and examples uses tagged.

- Consensus was to use untagged SUIT_Envelope (no CBOR tag).
- The purpose of having the tag on SUIT_Envelope for the SUIT manifest is to distinguish the SUIT manifest from other types of data stored in a generic repository, e.g. files in the file system
- In the TEEP Message, the spec of the Update message is identified to have the SUIT manifest and no other data, so not need to add more identifying information.

```
? manifest-list => [ + bstr .cbor SUIT_Envelope ],
```

- Conclusion

  Make no changes in the draft, decided to use untagged SUIT_Envelope.

  Links for this PRs are in other page.

Adding support of ES256 & EdDSA in the implementation

Link to Dave’s TEEP implementation

https://github.com/dthaler/teep

- Change was made the TEEP mandates to support both ES256 and EdDSA.
- QueryRequest requires having two signature in ES256 and EdDSA. For this purpose, decision was made to use COSE sign (supports multiple signatures) and not COSE sign1 (able to have only one signature).

- The t-cose only supports COSE sign1, wait for Laurence to add support COSE sign. Expected around December.
- Revised the TEEP Agent to be able to use both ES256 and EdDSA but selectivity only one of them, waiting COSE sing is ready in t-cose.
- Revised the TAM to support both ES256 and EdDSA

Fixing CDDL Syntax errors

Link to the issue
https://github.com/ietf-teep/teep-protocol/issues/278

- The syntax errors were detected by cddl tool. The fix is mandatory to be accepted as RFC.
- The cddl of teep-protocol require dependent cddl files from suit-report and suit-manifest.

- Mainly two errors were on SUIT_Parameters and suit-reference.
- The type SUIT_Parameters was defined inside suit-manifest and used in suit-manifest. Fixed the type mismatch between definition and usage.
- Required values were missing for suit-reference.

- Created PRs for the fix
  https://github.com/suit-wg/suit-report/pull/3
  https://github.com/ietf-teep/teep-protocol/pull/287
  https://github.com/ietf-teep/teep-protocol/pull/292

SUIT digest in unneeded-manifest-list

Link to the issue

https://github.com/ietf-teep/teep-protocol/issues/282

- Decision was made after IETF 114 to use suit-manifest for deleting a trusted-component in the teep-agent.
- What to use identifying the installed trusted-component.

- Instead of using SUIT_Digest, use SUIT_Component_Identifier which has one SUIT_Component_Identifier in each suit-manifest.

- Conclusion, make PR to revise the draft

  https://github.com/ietf-teep/teep-protocol/pull/283

Implementations

- Miyazawa-san
    - Implementing Passport model of Remote Attestation
    - teep_armadillo_trial
      https://github.com/s-miyazawa/teep_armadillo_trial

      Four sequences to implement
      1. TAM sends to armadillo-agent challenge
      2. armadillo-agent sends Evidence to Verifier
      3. Verifier sends Attestation Result to armadillo-agent
      4. (Under construction) armadillo-agent sends Attestation Result to TAM
- Ken's
    - Update libcsuit to support the changes in draft-ietf-suit-manifest-20 in a new branch
      https://github.com/yuichitk/libcsuit/tree/v20
- Isobe-san's
    - For supporting the Remote Attestation
      1. Adding QueryRequest to contain challenge
      2. Verify ARs in QueryResponse

      (WIP) https://github.com/ko-isobe/tamproto/tree/rats
    - Supporting Miyazawa's implementations.

IETF 115 Hackathon Summary

- Implementations
    - https://github.com/s-miyazawa/teep_armadillo_trial
    - https://github.com/yuichitk/libcsuit/tree/v20
    - https://github.com/dthaler/teep
    - https://github.com/ko-isobe/tamproto/tree/rats
- Solved topics
    - Clarified details of handling payload-format for EAT
    - Clarified when combinations of Background model and Passport model
    - Use untagged SUIT manifest, and the reason for it
    - Supporting both ES256 & EdDSA (on going)
    - Fixed cddl syntax errors by all the relevant people in the same room (Carsten too)
- 8 PRs, updates on drafts
    - #287, #292, #283, #3 (suit-report), #280, #290, #8 (suit-multiple-trust-domains), #293
- New issues filed
    - #281, #285, #286, #289

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

Items to tackle at Hackathon

- Method of distinguishing Evidence or Attestation Result in EAT profile
  - https://github.com/ietf-teep/teep-protocol/issues/263
- Use CBOR tag on SUIT_Envelope or not.
  - https://github.com/ietf-teep/teep-protocol/issues/273
- Having CDDL compilation warnings, would like to remove them
  - https://github.com/ietf-teep/teep-protocol/issues/278
- Adding support of EdDSA in the implementation, now TEEP mandates both ES256 & EdDSA, Changed from using COSE sign1 to COSE sign only for QueryRequest
  - https://github.com/ietf-teep/teep-protocol/pull/267
- Adding support of Unneeded manifest list in the implementation
  - https://github.com/ietf-teep/teep-protocol/pull/261
- Update implementation of libcsuit to support the changes in draft-ietf-suit-manifest-20

Links

- PRs

  https://github.com/suit-wg/suit-report/pull/3
  https://github.com/ietf-teep/teep-protocol/pull/283
  https://github.com/ietf-teep/teep-protocol/pull/287
  https://github.com/ietf-teep/teep-protocol/pull/292
  https://github.com/ietf-teep/teep-protocol/pull/280
  https://github.com/ietf-teep/teep-protocol/pull/290
  https://github.com/bremoran/suit-multiple-trust-domains/pull/8
  https://github.com/ietf-teep/teep-protocol/pull/293

- Branch
  - https://github.com/yuichitk/libcsuit/tree/v20

- New issues
  - https://github.com/ietf-teep/teep-protocol/issues/281
  - https://github.com/ietf-teep/teep-protocol/issues/282
  - https://github.com/ietf-teep/teep-protocol/issues/285
  - https://github.com/ietf-teep/teep-protocol/issues/286
  - https://github.com/ietf-teep/teep-protocol/issues/289
  - https://github.com/ietf-teep/teep-protocol/issues/291