IETF 110 TEEP Hackathon

March 10, 2021
Akira Tsukamoto (AIST)

IETF Hackathon

Date March 4, 10:00-15:00 in JST

Participants:

Akira Tsukamoto, AIST
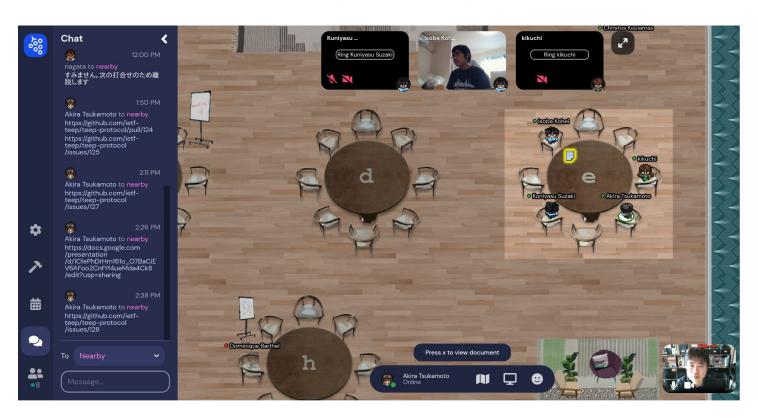
Kuniyasu Suzaki, TRASO/AIST

Kohei Isobe, Secom

Ken Takayama, Secom

Masashi Kikuchi, TRASIO

Takahiko Nagata, TRASIO

Gathering at the gather

Plan (1/3)

- Objective:
  - Adopt draft-05, which had many changes
    - 32 Pull Requests (PR) were merged after IETF109
  - Try following the latest draft in implementations and purify the draft

- Implementations used in Hackathon:
  - TAM: tamproto from Secom
  - TEEP device: teep-device from Lepidum and AIST
  - teep library: libcteep from Secom

Plan (2/3) : Testing between TAM and teep-device

- Generating digest of TC and create suit manifest. Have not generated a suit-manifest before. Upload this suit manifest to tamproto and use it for other tests.
- Test unneeded-tc-list、check if deleting TC would work or not and fixing it.
- Test token that the type have changed from uint to bstr.
- Add implementation in teep-device to verify every entry of suit-manifest properly.

Plan (3/3) : Others

- Discuss SUIT draft discription of preventing rollback updates
- Discuss how to use URI externally in suit manifest
- Making PR at github: the teep-protocol binary example:
  - Change Token example from 8byte to 16 byte, Change component-id example from 15 byte to 16 byte
- Making Issue at github:
  - Should digest region contain only data entry or with type-id and length of cbor.

Result (1/3): Testing between TAM and teep-device

- Test token that the type have changed from uint to bstr.
  - Success, communicated fine after changes TAM (tamproto) <-> teep-device
- Generating digest of tc and create suit manifest. Have not tried generating a suit-manifest before. Upload this suit manifest to tamproto and use it for other tests.
  - Could not finish it.
- Test unneeded-tc-list、check if deleting TC would work.
  - Success, deleting TC worked fine. However, already this is obsolete feature in draft-05
- Implement in teep-device to verify every entry of suit-manifest properly.
  - Could not finish it. We learned that it is unlikely to be finished soon.

Result (2/3): Others

- Making PR at github:
  - Change Token example from 8byte to 16 byte, Change tc-id example from 15 byte to 16 byte
    - https://github.com/ietf-teep/teep-protocol/pull/124
  - Unify the upper/lower cases and remove the leftover unneeded-tc-list
    - https://github.com/ietf-teep/teep-protocol/pull/126
- Making Issues at github:
  - TA Signer or TC Signer -> Discussion topic at IETF 110 TEEP session
    - https://github.com/ietf-teep/teep-protocol/issues/125
  - Use token in teep message or using nonce in eat-claim-set in the future   -> Discussion topic at IETF 110 TEEP session
    - https://github.com/ietf-teep/teep-protocol/issues/127
  - How to generating suit manifest for delete   -> Discussion topic at IETF 110 TEEP session
    - https://github.com/ietf-teep/teep-protocol/issues/128

Result (3/3): Investigate and discussion

- Check suit draft for preventing rollback updates.
  - Run out of time, could not discuss
- Discuss how to use uri externally from signed area in suit manifest
  - Run out of time, could not discuss -> Discussion topic at IETF 110 TEEP session
    - https://github.com/ietf-teep/teep-protocol/issues/104
    - https://github.com/ietf-teep/teep-protocol/issues/105

Summary

- Was able to have consensus of maturity of draft-ietf-teep-protocol on top of draft-ietf-teep-otrp-over-http is mostly fine now from implementation perspective.

- Where to focus after IETF110?
  - Trying COSE on teep-protocol
    - we only have tried CBOR portion.
  - Move majority of effort on how to use SUIT manifest properly inside teep-protocol
    - Nobody have tried yet.
- After IETF 111?
  - Probably integrating RATS in TEEP.