IETF 110 TEEP Hackathon

March 10, 2021

Akira Tsukamoto (AIST)

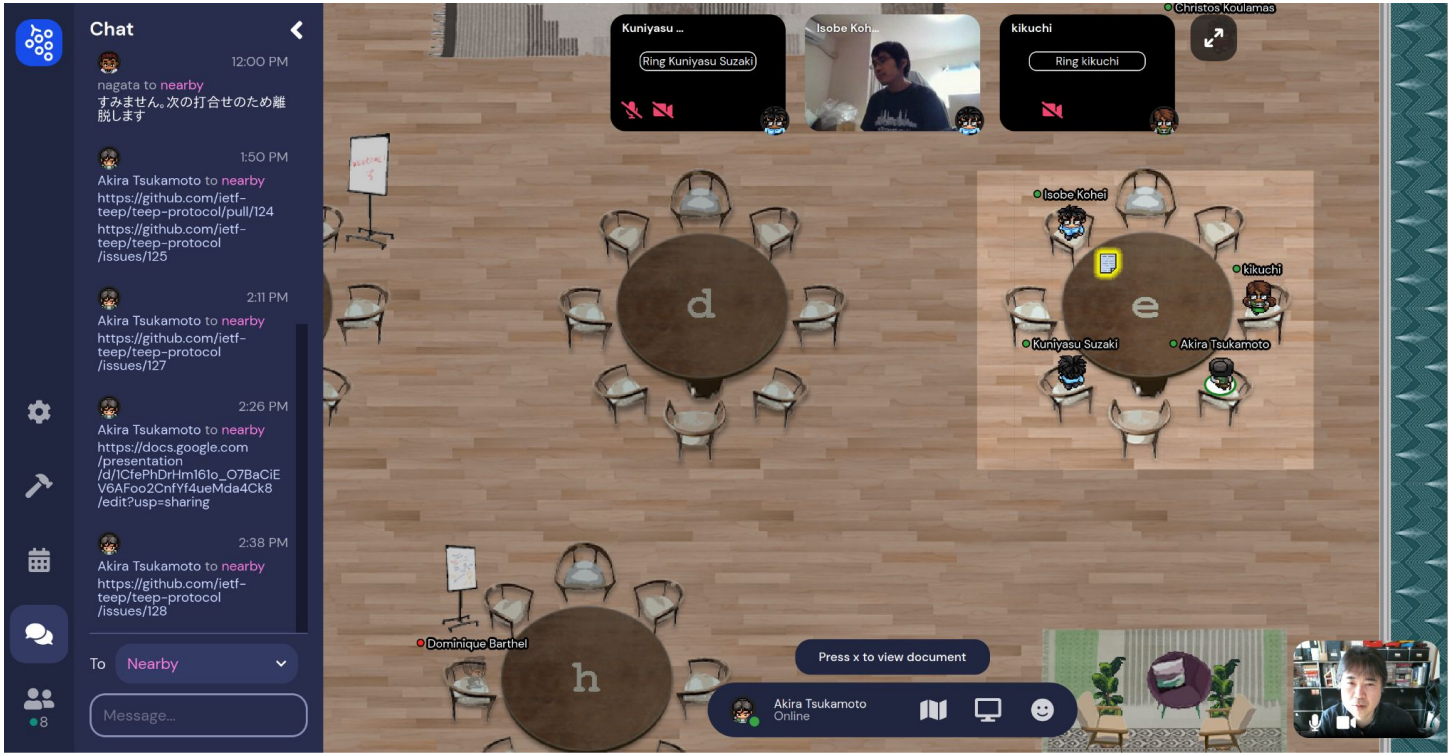
IETF Hackathon

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
- Dave Thaler, Microsoft

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, this method is already 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, component-id example from 15 byte to 16 byte
    - https://github.com/ietf-teep/teep-protocol/pull/124 -> Merged
  - Unify the upper/lower cases and remove the leftover unneeded-tc-list
    - https://github.com/ietf-teep/teep-protocol/pull/126 -> Merged
- 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
  - Errors processing QueryRequest
    - https://github.com/ietf-teep/teep-protocol/issues/129 -> Discussion topic at IETF 110 TEEP session
  - Intel SGX attestation requires challenge to be 512 bytes (was 64 bytes max)
    - https://github.com/ietf-teep/teep-protocol/issues/130 -> Resolved

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.

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).

SUIT manifest use-cases in TEEP

- TAM to have a way to choose uri for TC
  - https://github.com/ietf-teep/teep-protocol/issues/104
  - Would SUIT manifest support the following use-cases?
  - A TC Signer will generate TC binaries inside/alongside with SUIT manifest and hand the TC binaries to the TAM-A vendor and the TAM-B vendor, and TAM-A vendor and TAM-B vendor will host the TC binaries independently.
  - This use-case would require URI information to be able to specify by TAM vendors and not by TC Singers.
- Construction of SUIT_Envelope of URI outside the digest region
  - https://github.com/ietf-teep/teep-protocol/issues/105
  - If the above use-cases is valid, then how to write the SUIT manifest as the external region with URI by TAM vendors while the main body of SUIT mafinest are signed by TC Signers.
- The way of generating suit manifest for delete
  - https://github.com/ietf-teep/teep-protocol/issues/128
  - It was decided to use delete command inside SUIT manifest instead of using unneeded-tc-list in TEEP message from dfraft-05 when deleting TC at TEEP client.
  - There are tools (suit-manifest-generater) and able to construct with install command, however, it does not generate with delete command and not sure how to construct the SUIT manifest with delete command.