IETF 109 teep hackathon report

Nov. 18, 2020

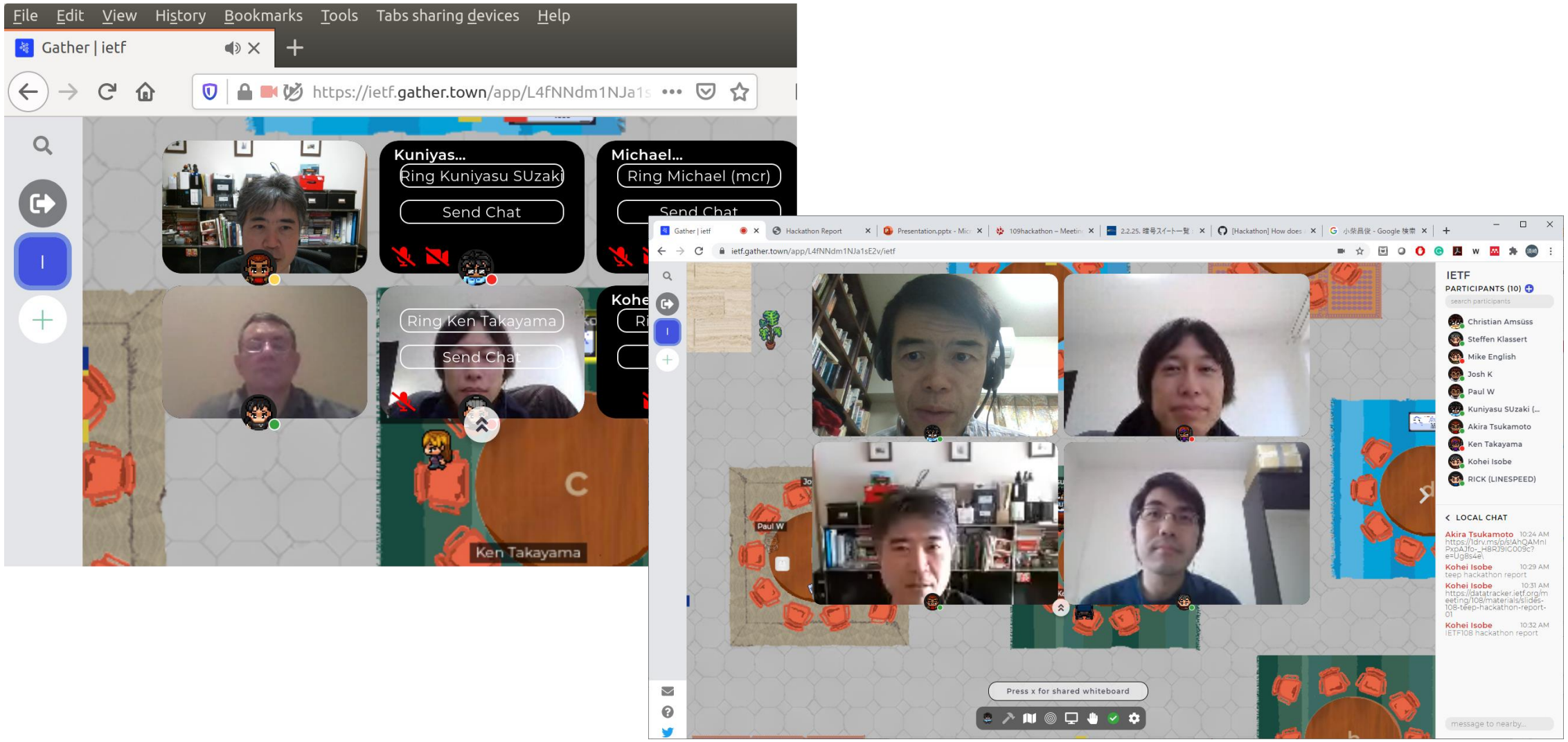
Akira Tsukamoto (AIST)

Agenda

- TEEP Hackathon (11.9 – 11.13)
  - Individual each participant working from home!
  - Meeting at 11.13

- Photo during hackathon
- Implementations, TAMs and TEEP devices brought at Hackathon
- Issues raised and still open at hackathon
- PR created and open
- PR closed
- What we achieved, what we learned

Gathered at the gather



Implementations, TAMs and TEEP Agents brought at Hackathon

- TAM server
  - Dave (Microsoft)
    - https://github.com/dthaler/OTrP
  - Tamproto: Isobe (SECOM)
    - https://github.com/ko-isobe/tamproto

- TEEP Agent
  - TEEP-Device: Kikuchi (AIST)
  - libteep: Takayama (SECOM)
    - https://github.com/yuichitk/libteep
  - Dave (Microsoft)
    - https://github.com/dthaler/OTrP

Issues raised and still open at hackathon (1/2)

- https://github.com/ietf-teep/teep-protocol/issues/67
  - Adding example SUIT and EAT manifest to example section
  - Added SUIT example. EAT is still missing.
- https://github.com/ietf-teep/teep-protocol/issues/70
  - Trusted Component identifiers in SUIT manifests
  - Require SUIT manifest to reference as an unique identifier, need further discussion from SUIT.
- https://github.com/ietf-teep/teep-protocol/issues/71
  - Guide require to generating Token to reduce collision. Pasting guidance from other RFC.
- https://github.com/ietf-teep/teep-protocol/issues/72 and https://github.com/ietf-teep/teep-protocol/issues/73
  - Two perspectives to consider. One is which cipher suit to add more commonly used in the market to enhance the adaptation and use cases of teep, e.g. adding RSA.
  - Another is, should not include cipher suit which is already known to be low security.
  - SHA256 above?, RSA 4096 above?, AES256 above? eddsa, ed25519, or refer other RFC or NIST doc.
  - Clarify how to construct cipher suit bit map representation.

Issues raised and still open at hackathon (2/2)

- https://github.com/ietf-teep/teep-protocol/issues/76
  - Not clean how to describe extension in cbor, I prefer reading the teep-protocol will be one kind of tutorial of cbor representation as much as possible, for the developer to prevent fragmented implantation.
- https://github.com/ietf-teep/teep-protocol/issues/78
  - Prefer restricting `teep-message-framework` to make the implementation consistent and easy to parse after trying implement teep in cbor for the hackathon.
- https://github.com/ietf-teep/teep-protocol/issues/79
  - Clarified after the hackathon of who signs TEEP's "security wrapper" and UIT's "suit-authentication-wrapper". Would prefer to have the refering the link to the teep-archiecture draft which states this.
- https://github.com/ietf-teep/teep-protocol/issues/80
  - Ambiguous of request tc-list should be in QueryResponse or not. PR #82 was made to clarify to make it mandatory.
- https://github.com/ietf-teep/teep-protocol/issues/81
  - How does Agent get unneeded-ta-list, require further discussion. Should we have what to do in Architecture draft?
- https://github.com/ietf-teep/teep-protocol/issues/83
  - Detail token consideration for how the token should be used and not to be used for Security consideration and scalability of TAM server. This discussion relates how much the teep-device has the hardware resources, e.g. PC or 8bit micro. Probably biggest topic to consider for the next draft.

PR created and open

- https://github.com/ietf-teep/teep-protocol/pull/82
  - Clarify the teep message description of QueryResponse when there is mandatory tc list.
  - Reviewed and Ready to merge.

PR closed

- https://github.com/ietf-teep/teep-protocol/pull/74
  - Renaming requested-ta-info to requested-tc-info to reflecting the changes in teep from changing the name from Trusted App to Trusted Component.
- https://github.com/ietf-teep/teep-protocol/pull/75
  - Fix error on draft 04 depending the versions of xml2rfc. Now supports both version 2 and version3 of xml2rfc when generating xml and txt rfc file from md file.
- https://github.com/ietf-teep/teep-protocol/pull/77
  - Fix some binary representation values in the teep-error example.

What we achieved, what we learned

- Goal
  - Adopt latest draft of both teep-protocol 04 and teep-otrp-over-http
    - https://tools.ietf.org/html/draft-ietf-teep-protocol-04
    - https://tools.ietf.org/html/draft-ietf-teep-otrp-over-http-09
- Achieved
  - Updates on github
    - https://github.com/ietf-teep/teep-protocol
  - Individual developments
    - Finished supported 04 draft, mostly
      - TAM & Agent Dave, tamproto, TEEP-device, libteep
  - Interop developments
    - Tamproto (SECOM) and TEEP-device (AIST) now talking each other!
- Learned
  - Necessity of discussing and defining fundamental design topics
    - Token
    - Deleting trusted components
  - Necessity to improve details of binary representation for combability among implementers
    - Completeness of teep-messages are drastically improved, pretty good shape now
    - More examples, SUIT and EAT are future action items, COSE too :)

Hackathon Members

Akira Tsukamoto (AIST)
Dave Thaler (Microsoft)
Kohei Isobe (SECOM/TRASIO)
Ken Takayama (SECOM)
Kuniyasu Suzaki (TRASIO/AIST)
Masashi Kikuchi (Lepidum)
Nagata Takahiko (Lepidum)

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).