IETF 116 TEEP Hackathon

March 27, 2023

Akira Tsukamoto, (presenting)
Dave Thaler, Microsoft
Kohei Isobe, SECOM
Ken Takayama, SECOM
Shin’ichi Miyazawa, SECOM
Yuichi Takita, SECOM
Daisuke Ito, Roboc
IETF 116 TEEP Hackathon

- **Date** March 25 Saturday, 26 Sunday
  - Jointly COSE, and TEEP

- **Participants:**
  - Dave Thaler, Microsoft
  - Kohei Isobe, SECOM
  - Ken Takayama, SECOM
  - Shin’ichi Miyazawa, SECOM
  - Yuichi Takita, SECOM
  - Daisuke Ito, Roboc
  - Carsten Bormann, CDDL
  - Laurence Lundblade, t-cose
  - Akira Tsukamoto
Pictures
Objective and Plan

● Objective
  ○ Refine the draft from issues found in the implementation

● Action Item list

  ● Clarification of cnf recently added to Query Response
    https://github.com/ietf-teep/teep-protocol/pull/321

  ● Compromised Broker and keys in multiple TEEP-Agents on SGX
    https://github.com/ietf-teep/teep-protocol/issues/310#issuecomment-1467297393

  ● Token and Challenge coexistence in TEEP Messages, from IETF110
    https://github.com/ietf-teep/teep-protocol/issues/127

  ● Easy synchronization of cddI definitions between md file and cddI files.
    https://github.com/ietf-teep/teep-protocol/issues/208

● Work on implementations
Clarification of cnf recently added to Query Response
Only for Japan member

- After the consideration of compromised TEEP Agent discussion, the cnf was added to the Query Response.
- PR
  https://github.com/ietf-teep/teep-protocol/pull/321
- The cnf will contain the hash value of public key of the TEEP Agent.
- Among only Japan member, was not sure whether cnf only contain the hash value of TEEP Agent or both TEEP Agent and Verifier.

- No, it was misunderstanding. The cnf only contains hash value of TEEP Agent
Compromised Broker and keys in multiple TEEP-Agents on SGX

- Initial discussion was compromised Agent.  
- The TEEP Broker may be compromised but the TEEP Agent itself is protected by SGX.
- When TEEP Broker is compromised, it may have multiple TEEP Agent instances in the same SGX chip.

- Conclusion was we only consider compromised Broker and not Agent in the TEEP design.
- The key pairs are different in different SGX chip which do not contradict with the TEEP design.
Clarification of *token* and *challenge* in TEEP Messages

- This topic was resolved once at IETF 110. Revisiting.
- Decision was made to use either of *token* or *challenge* at IETF110.

```
OPEN #127: Use of token vs challenge in QueryRequest

query-request = [...
  ? token => bstr .size (0..64),
  ? challenge => bstr .size (0..64),
  [...]

The token is not needed when the attestation bit is set in the data-item-requested value. The size of
the token is at least 8 bytes (64 bits) and maximum of 64 bytes, which is the same as in an EAT Nonce
Claim

- Intent was:
  * token is present if attestation bit is clear (used in response token)
  * challenge is only allowed if attestation bit is set (used in evidence)
  * Currently have separate CBOR label values
  * QUESTION: Should we combine them into one label?
```

- Always having *token* may make TAM implementation easier.

- Keep it as it is, and do not change the draft.
- If using timestamp for the freshness, able to reuse AR in QueryResponse.
Synchronizing cddl definitions between md file and cddl files

- Raised between IETF 113 March and IETF 114 July 2022 when attempting cddl syntax check before submitting the draft [https://github.com/ietf-teep/teep-protocol/issues/208](https://github.com/ietf-teep/teep-protocol/issues/208)
- The downloading dependent cddl files were fixed between IETF 114 and IETF 115 hackathon.
- The cddl syntax check command in Makefile was added at IETF 115 hackathon.
- When updating md file, it is burden to manually making the same changes to cddl files without making mistakes.

- Updating Makefile to extract cddl file from md file.
- Do not require updating cddl file manually anymore. [https://github.com/ietf-teep/teep-protocol/pull/322](https://github.com/ietf-teep/teep-protocol/pull/322)
Benefit of CBOR in TEEP (1/2)

CBOR がバイナリになるまで (1/2)

- TEEP query-response の例
- CDDL (Concise Data Definition Language)

```json
query-response = [
  type: TEEP-TYPE-query-response,
  options: {
    ? token => bstr .size (8..64),
    ? selected-cipher-suite => suite,
    ? selected-version => version,
    ? evidence-format => text,
    ? evidence => bstr,
    ? tc-list => [ + tc-info ],
    ? requested- => bstr,
    ? unneeded- => bstr,
    ? ext-list => [ + ext-info ],
    * $query-n,
    * $steep-op
  }
]
```

- Diagnostic Notation

```json
2, / type : TEEP-TYPE-query-response = 2 (uint (0..23)) /
/options : /
{
  20 : 0xa0a1a2a3a4a5a6a7a8a9aaabacadaeaf,
  / token = 20 (mapkey) : h'a0a1a2a3a4a5a6a7a8a9aaabacadaeaf (bstr .size (8..64)),
given from TAM's QueryRequest message /
5 : 1 , / selected-cipher-suite = 5 (mapkey) : TEEP-AES-CM-16-64-128-HMAC256-256-X25519-xEdDSA =
1 .within uint .size 4 ) /
6 : 0 , / selected-version = 6 (mapkey) :
0 .within uint .size 4 ) /
7 : ... / evidence = 7 (mapkey) :
Entity Attestation Token /
```
Smaller binary than JSON
Started downloading dependent CDDL files with wget/curl

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

   (b-2) Fixing errors temporary by adding four lines to draft-ietf-suit-manifest.cddl just downloaded
   COSE_Sign_Tagged = 98
   COSE_Sig1_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

(4) Run cddl tool
   $ cddl check-draft-ietf-teep-protocol.cddl generate
Added CDDL Syntax check with Carsten’s CDDL tool

- Added command ‘validate-teep-cddl’ in Makefile

To check syntax cddl syntax in TEEP file and not suit which is useful during debugging teep by using only QueryRequest which do not contain SUIT part.

```
make validate-teep-cddl
```

```
.PHONY: validate-teep-cddl
validate-teep-cddl: $(CONCATENATED_CDDL) ../cbor/query_request.dia.g.bin
cddl $(CONCATENATED_CDDL) validate ../cbor/query_request.dia.g.bin
@echo "Success: QueryRequest message matches TEEP Protocol CDDL"
```
Demo (1/3)

ARM OP-TEE

Figure 5: Passport Model

https://datatracker.ietf.org/doc/rfc9334/
TEEP with Passport model Verifier

Demo (2/3) ARM OP-TEE

TEEP Agent
TEEP Broker
ARM OP-TEE

TAM proto
Naive Verifier
Intel NUC

Display
ARM REE
TEEP with Passport model Verifier on SGX

Demo (3/3)
TEEP SUIT EAT demo

Come to Hackdemo!

18:30 27th Monday, room G304
Appendix
Items to tackle at Hackathon

- Clarification of cnf recently added to Query Response
  https://github.com/ietf-teep/teep-protocol/pull/321

- Compromised Broker and keys in multiple TEEP-Agents on SGX
  https://github.com/ietf-teep/teep-protocol/issues/310#issuecomment-1467297393

- Token and Challenge coexistence in TEEP Messages, from IETF110
  https://github.com/ietf-teep/teep-protocol/issues/127

- Easy synchronization of cddl definitions between md file and cddl files.
  https://github.com/ietf-teep/teep-protocol/issues/208