IETF 118 TEEP/SUIT Hackathon

November 04-05, 2023

Akira Tsukamoto

IETF 118 TEEP/SUIT Hackathon

- Participants:

  Dave Thaler
  Kohei Isobe
  Okuda Tetsuya (Remote)
  Muhammad Usama Sardar
  Hannes Tschofenig
  Henk Birkholz
  Akira Tsukamoto (Presenting)

Objective and Plan

- Objective
  - Finalize and finish TEEP Protocol draft to able to send it to IESG during the session

- Action Items
  - TAM Server, Isobe-san
    - Adding QueryRequest using COSE_Sign, Isobe-san
  - Align TEEP Protocol draft with SUIT-MTI, Akira
    - Match the cipher-suits of TEEP in SUIT-MTI (Mandatory-to-Implement Algorithms for Creators and Consumers of Software Update for the Internet of Things manifests)
  - Formal Verification, Okuda-san
    - Write a sample formal verification code to check TEEP Protocol confirmation

TAM Server called tamproto

- Now the tamproto replies QueryRequest with COSE_Sign
  https://github.com/ko-isobe/tamproto/issues/17

- It required adding COSE_Sign capability in cose-js (node-js implementation of COSE)
  https://github.com/erdtman/cose-js

- Added COSE_Sign in forked cose-js
  https://github.com/ko-isobe/cose-js

Matching the ciphersuites for both TEEP and SUIT

- TEEP decided to use the same algorithms in TEEP Agent which are used in SUIT to make the implementation friendly of the TEEP Agent
- The ciphersuites using in TEEP and SUIT diverted after updating draft-ietf-suit-mti from -01 to -02
- The SUIT-MTI defines Mandatory-to-Implement Algorithms of ciphersuite profiles for the SUIT
  https://github.com/bremoran/suit-mti
- Ciphersuites in -17 of TEEP
  suit-sha256-es256-ecdh-a128gcm
  suit-sha256-eddsa-ecdh-a128gcm
- Ciphersuites in -02 of SUIT-MTI
  suit-sha256-es256-ecdh-a128ctr
  suit-sha256-eddsa-ecdh-a128ctr
  suit-sha256-eddsa-ecdh-chacha-poly
- Conclusion at the Hackathon, both list the same ciphersuites in TEEP -18 and in SUIT-MTI -03
  suit-sha256-es256-ecdh-a128ctr
  suit-sha256-eddsa-ecdh-a128ctr
  suit-sha256-es256-ecdh-a128gcm
  suit-sha256-eddsa-ecdh-chacha-poly

Formal Analysis of the TEEP Protocol

- Okuda-san started formal analysis of the TEEP protocol using ProVerif & Tamarin.

- The motivation is to use the TEEP protocol as an example of how to apply formal analysis.
  - Also helps to find potential bugs in the specification.
  - Think of it as a “deep review”.

- The current code is around 300 lines and found here: https://github.com/tetsuya-okuda-hco/public-teep-formal-verif

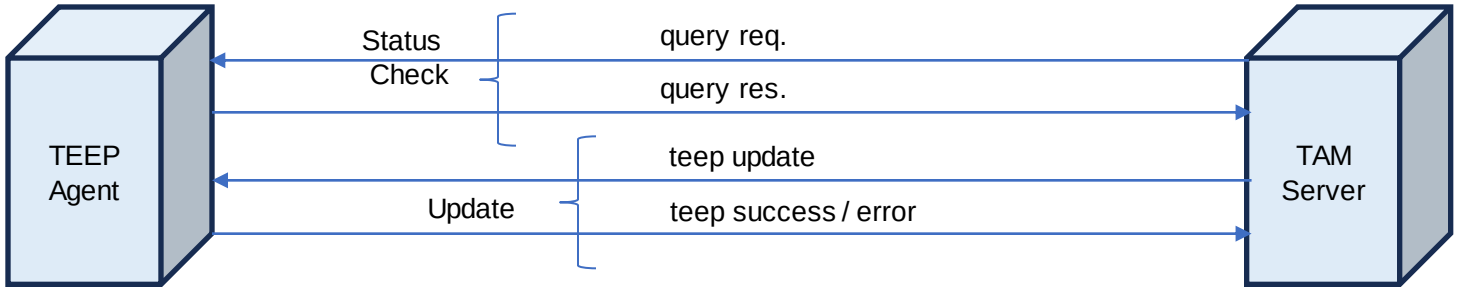
- Feedback from Muhammad Usama, Hannes and Cory.

Relevant Work

- Usama, Thomas, and Simon have written a paper:
  "SoK: Attestation in confidential computing"
  Analysis of attestation mechanisms in ARM CCA & Intel TDX using ProVerif.
  https://www.researchgate.net/publication/367284929_SoK_Attestation_in_Confidential_Computing

- Cory & Hannes have written the I-D for UFMRG:
  "A Usable Formal Methods Sample Problem from TEEP"
  https://datatracker.ietf.org/doc/draft-mt-ufmrg-teep-sample/

Current Focus



What did we learn so far?

- Defining the security properties is important
  (e.g., secrecy of what, authentication of whom)

- Deciding about the scope of the model can be challenging.
  - Analysis is based on the model.
  - The two teams came up with a different model.

- Are there documents you would like to get analysed?

Summary

- TEEP Protocol draft
  - No issue left for sending to IESG
- Formal analysis will continue
- PS: Nice to have the TEEP mascot ☺