IETF Hackathon: Trusted Execution Environment Provisioning (TEEP)

- IETF 104
- 23-24 March, 2019
- Prague

Hackathon Plan

- Flesh out implementation issues with OTrP specs:
  - draft-ietf-teep-architecture-02
  - draft-ietf-teep-opentrustprotocol-02
    - (draft is underspecified)
  - draft-thaler-teep-otrp-over-http-01
- Work on implementations and compare interpretations of spec
- Validate that spec is TEE vendor agnostic

What got done

- Multiple (2) implementations represented
  - Across 3 types of TEEs (Intel SGX, ARM TrustZone, RISC-V Keystone)

- Participants used Open Enclave SDK branch that supports both SGX and TrustZone

- SGX+TrustZone implementation of OTrP client & server in progress:
  - Ported to run over Open Enclave SDK
  - Added more of OTrP implementation (more use of JWS & JWE)
  - Updated to match latest HTTP transport spec (changes based on MNot feedback), straightforward
  - Implemented Trusted Application request mechanism designed (but not implemented) at hackathon 103 but only doc'ed in a github issue

What we learned

- Filed Issues: https://github.com/ietf-teep/OTrP
  - 5 new draft issues filed
  - 3 existing issues updated with more info

- Summary of new issues:
  - Relationship between OTrP and attestation (EAT/RATS/etc) needs work (on agenda for this week)
  - Some OTrP fields look redundant with others, opportunity for mismatch
  - OTrP spec uses two slightly different cert chain encoding mechanisms (JWS and custom), complicating code
  - Some OTrP fields (TEE name, TEE version) are underspecified and are interpreted differently by different people

Wrap Up

Team members:

- Dave Thaler
- Akira Tsukamoto
- Kuniyasu Suzaki
- Hannes Tschofenig (co-author)

First timers @ IETF/Hackathon: 2