IETF Hackathon
Attested TLS

IETF 115
5-6 November 2022
London, UK

SCITT/
RATS

Hackathon Plan

- TLS extensions to support attestation evidence (and results) as first-class authentication credentials
- Relevant I-Ds
  - draft-fossati-tls-attestation
  - draft-bft-rats-kat
  - draft-ftbs-rats-msg-wrap

What got done

- Extend TLS handshake in mbedTLS
- Extend Attestation Verifier to handle TPM-based Key Attestation
  - Verification and endorsement path
- Extend Attester to produce endorsements and evidence in the correct formats accepted by the Verifier

- Code
- https://github.com/veraison/services/tree/ietf-115-hackathon
- https://github.com/ionut-arm/parsec-se-driver/tree/attested-tls
- https://github.com/hannestschofenig/mbedtls/tree/tls-attestation

What we learned

- Integration highlighted
  - The need to modify slightly the evidence format to include an in-band reference to the verification key
  - The need to modify the attestation result format to embed the verified identity key

Wrap Up

Team members:

Ionut Mihalcea

Hannes Tschofenig

Thomas Fossati

First timers @ IETF/Hackathon: Ionut

Confidential Computing Consortium:

- Attestation SIG POC