Early Attestation at SEAT, IETF-125

很遗憾我们不能亲自到场

draft-fossati-seat-early-attestation-03

Yaron Sheffer, Thomas Fossati, Ionuț Mihalcea, Tirumaleswar Reddy, Yogesh Deshpande

Progress from -02

- The protocol is now within the requirements of the SEAT charter
  - Replaced the Attestation message by an extension within the Certificate message (*Attestation Extension*)
  - Redefined the attestation binder to decouple it from the TLS key schedule

- Multiple design options for reattestation
- Discussion and diagram around the internal architecture of the TLS stack and TEE, and its security implications

Attestation Extension

- As in -02, we are transporting a Conceptual Message Wrapper (CMW) containing an Evidence or Attestation Results
- Instead of a TLS message, this is defined as an *CertificateEntry* extension for the end-entity certificate (TLS Certificate message)
  - From client, from server or both
- More specifically, an extension to the end-entity certificate

Attestation Binder

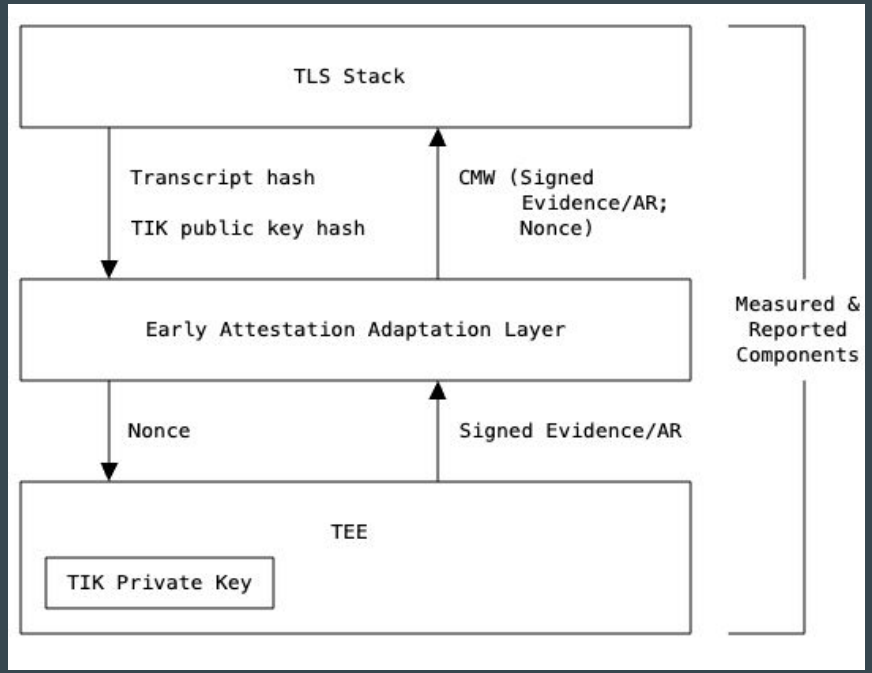
- Now completely separate from the TLS key schedule
- Role: binds the attestation to the specific TLS handshake, including the attester's PKI identity
- Binder inputs: message transcript, attester's public key
  - Transcript is roughly modeled on the *handshake_context* (TLS Sec. 4.4)
- Used as a nonce when signing the Evidence or AR

```
c_attest_base = Derive-Secret(0, "c attestation base",
                              ClientHello...Server-Finished)
s_attest_base = Derive-Secret(0, "s attestation base",
                              ClientHello...EncryptedExtensions)

c_attest_binder = HKDF-Expand-Label(c_attest_base, "attestation",
                                    TLS_Client_Public_Key, Hash.length)
s_attest_binder = HKDF-Expand-Label(s_attest_base, "attestation",
                                    TLS_Server_Public_Key, Hash.length)
```

Architectural Considerations (new Sec. 5.3)

- The solution needs to accommodate different architectural choices:
  - TLS stack within the TEE vs. one that's outside the TEE but still measured
  - Separate Verifier on RP side vs. collocated verification
- The Adaptation Layer can be part of the TLS stack or the TEE, per specific deployment
- RATS "conceptual message" notion allows the peers to be agnostic of attestation details
  - The RP does not need to parse Evidence from the CMW to appraise it!



Reattestation

- Draft -03 does not propose a solution, rather it presents 3 options:

  a. Extended Key Update
  b. No explicit reattestation, simply re-establish the connection
  c. Post-handshake using *CertificateUpdate*

- For *client-side* attestation we could use post handshake client authentication (RFC 8446, Sec. 4.6.2) - not yet in the draft

Next Steps

- The draft is now within SEAT charter and (as far as we're aware) covers all use cases
- We are requesting the working group to adopt it

Backup

Security Properties

- Replay attack: reuse of an old attestation
  - Prevented by using message transcript in the Binder
  - Both client and server Binders include entropy from both peers
  - Note: for complete attestation freshness, the TEE has to rerun the measurement, which is out of scope for SEAT

- Diversion attacks: TLS is terminated on a rogue server and attestation is compromised (Sec. 8.1 of Identity Crisis)
  - TLS stack in the TEE: the attacker may be able to present attestation but cannot present a valid TLS certificate
  - The paper discusses an ephemeral key; we are only using the TLS identity key which the rogue server does not know

Security Properties - Cont.

- Relay attacks: TLS terminated on a rogue server that has a valid certificate and (ab)uses a genuine TEE for attestation
  - Note: the paper referenced from the FOSDEM presentation is not openly available
- Can be addressed through architecture or by enhancing the Evidence

- Architecture: ensure the TEE does not receive an opaque nonce as input; it receives the transcript hash and TLS public key and derives Binder/nonce
  - The public key must be validated against the TLS private key that the TEE manages
  - In other words, the Adaptation Layer has to be part of the TEE, TEE and AL key handling must be reviewed/endorsed, and the TEE should maintain the TLS private key

- An alternative WIP suggests to include PoP of the TLS key inside the evidence (EAT)