Architecturally-defined Attestation, Attested TLS and Open Challenges

Muhammad Usama Sardar[*]

Based on joint works with Arto Niemi, Hannes Tschofenig, Thomas Fossati, Simon Frost, Ned Smith, Mariam Moustafa, Tuomas Aura, Yaron Sheffer, Ionut Mihalcea, Jean-Marie Jacquet and Henk Birkholz

[*]TU Dresden, Germany

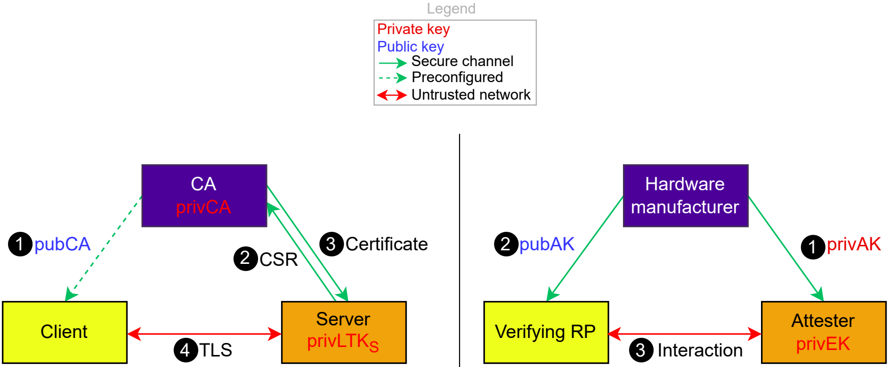
April 8, 2025

Outline

1. Attested TLS

2. Open Problems

TLS vs. Architecturally-defined Attestation



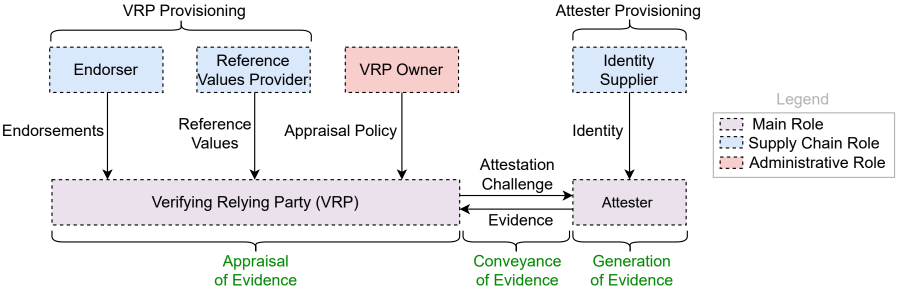
- CA as Trust Anchor

- HW manufacturer as Trust Anchor

$$Cert = sign(privCA, ID \parallel pubLTK)$$

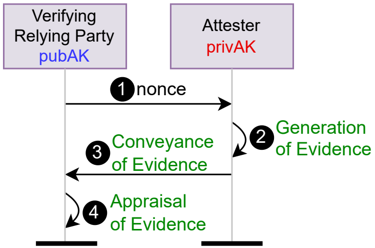
$$Evidence = sign(privAK, m \parallel pubEK)$$

Architecturally-defined Attestation: Architecture Perspective

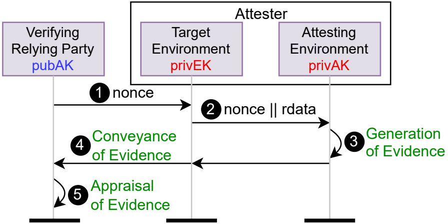


Architecturally-defined Attestation: Protocol Perspective

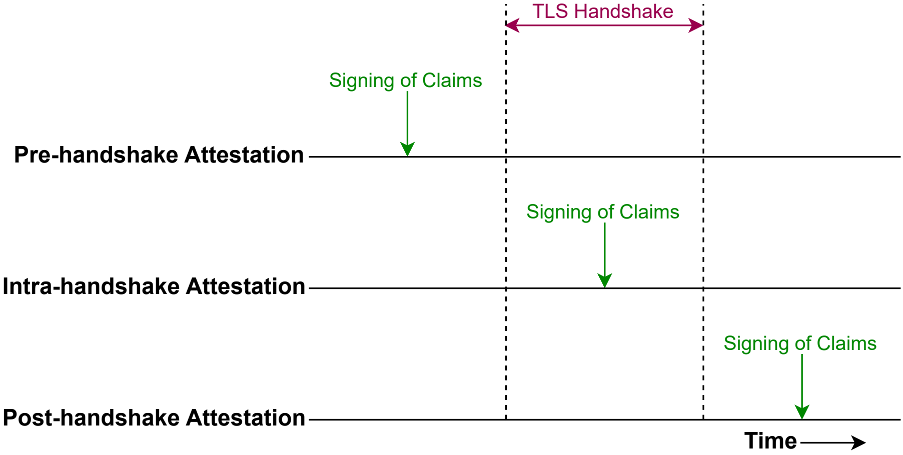
- Integrated Attester



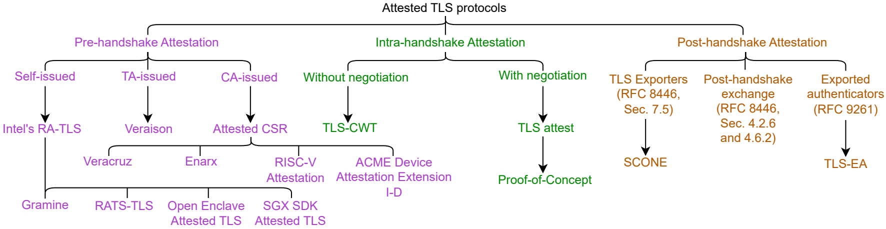
- Attester with separate env.



Attested TLS

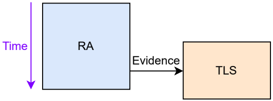

TLS Handshake
Signing of Claims
Pre-handshake Attestation
Signing of Claims
Intra-handshake Attestation
Signing of Claims
Post-handshake Attestation
Time

Main Design Options

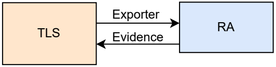

Attested TLS protocols
Pre-handshake Attestation
Intra-handshake Attestation
Post-handshake Attestation
Self-issued
TA-issued
CA-issued
Without negotiation
With negotiation
TLS Exporters (RFC 8446, Sec. 7.5)
Post-handshake exchange (RFC 8446, Sec. 4.2.6 and 4.6.2)
Exported authenticators (RFC 9261)
Intel's RA-TLS
Veraison
Attested CSR
TLS-CWT
TLS attest
SCONE
TLS-EA
Veracruz
Enarx
RISC-V Attestation
ACME Device Attestation Extension I-D
Proof-of-Concept
Gramine
RATS-TLS
Open Enclave Attested TLS
SGX SDK Attested TLS

Channel Bindings

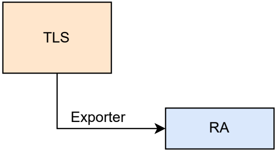
- Pre-HS



- Intra-HS



- Post-HS



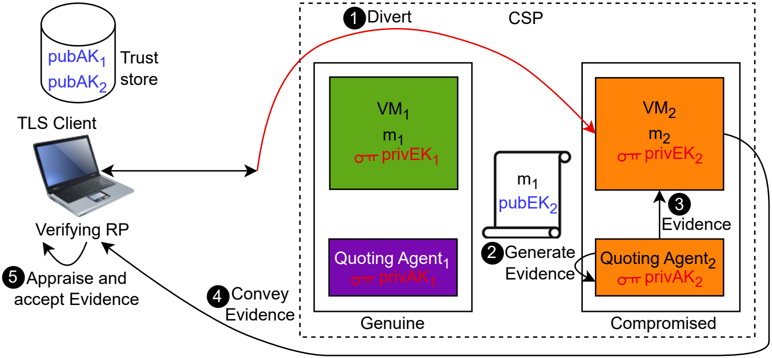
Outline

1. Attested TLS

2. Open Problems

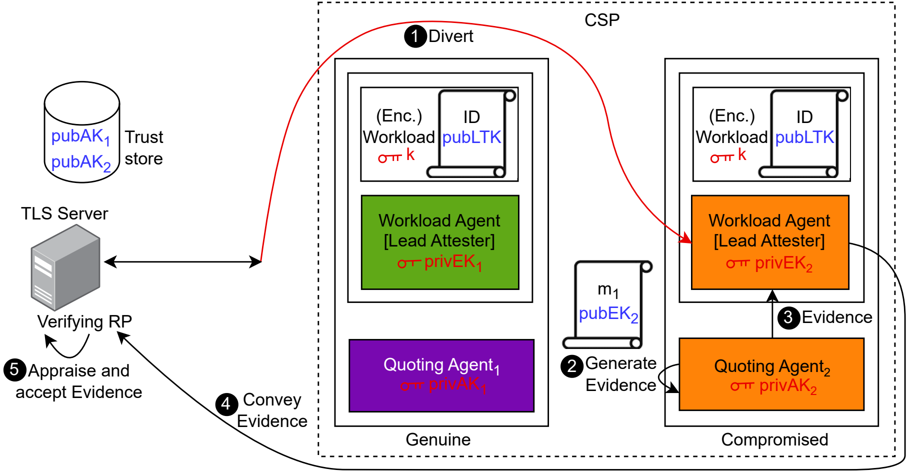
A Diversion Attack Within CSP

- AK of a specific machine may be compromised. (e.g., $privAK_2$)
  - Transient execution attacks, as demonstrated by Foreshadow[1]
- VM_2 impersonates VM_1



[1] Van Bulck, Minkin, Weisse, Genkin, Kasikci, Piessens, Silberstein, Wenisch, Yarom, and Strackx, "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution", 2018.

B How to Provision ID and LTK?



- CSP gets the key k

Questions for Discussion

- Threat model: CSP as fully untrusted vs. “Honest but curious”? [Fritz]

Questions for Discussion

- Threat model: CSP as fully untrusted vs. “Honest but curious”? [Fritz]
- Equivalence class? [Keith]

Questions for Discussion

- Threat model: CSP as fully untrusted vs. “Honest but curious”? [Fritz]
- Equivalence class? [Keith]
- Temporal: How has pubAK become untrusted? [Jim]