Formal Analysis of Attested TLS for Confidential Computing

Muhammad Usama Sardar

TU Dresden, Germany

November 3, 2024

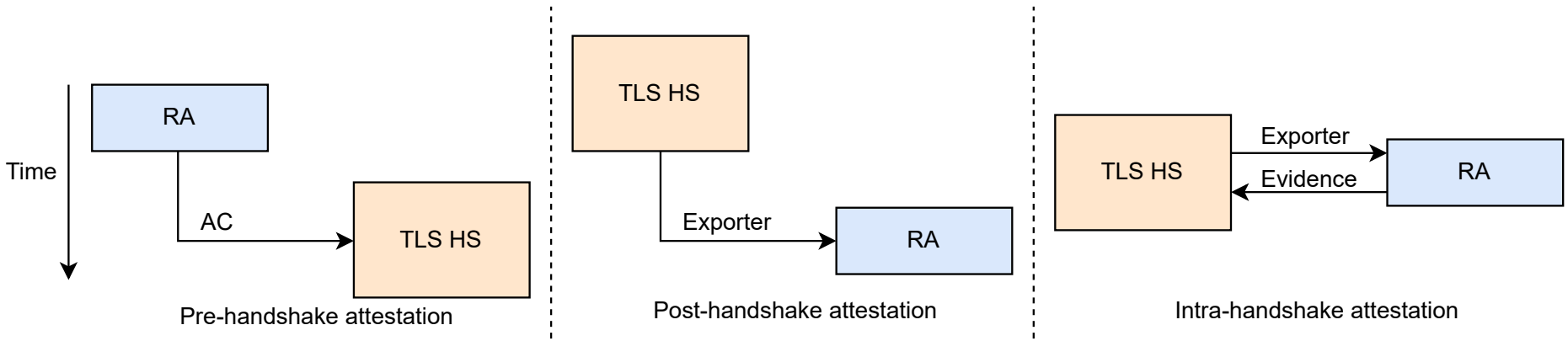
Attested TLS

- TLS 1.3[1]
  - Good for network security
  - Not good for endpoint security
- Use case: Confidential Computing

[1] https://datatracker.ietf.org/doc/html/rfc8446

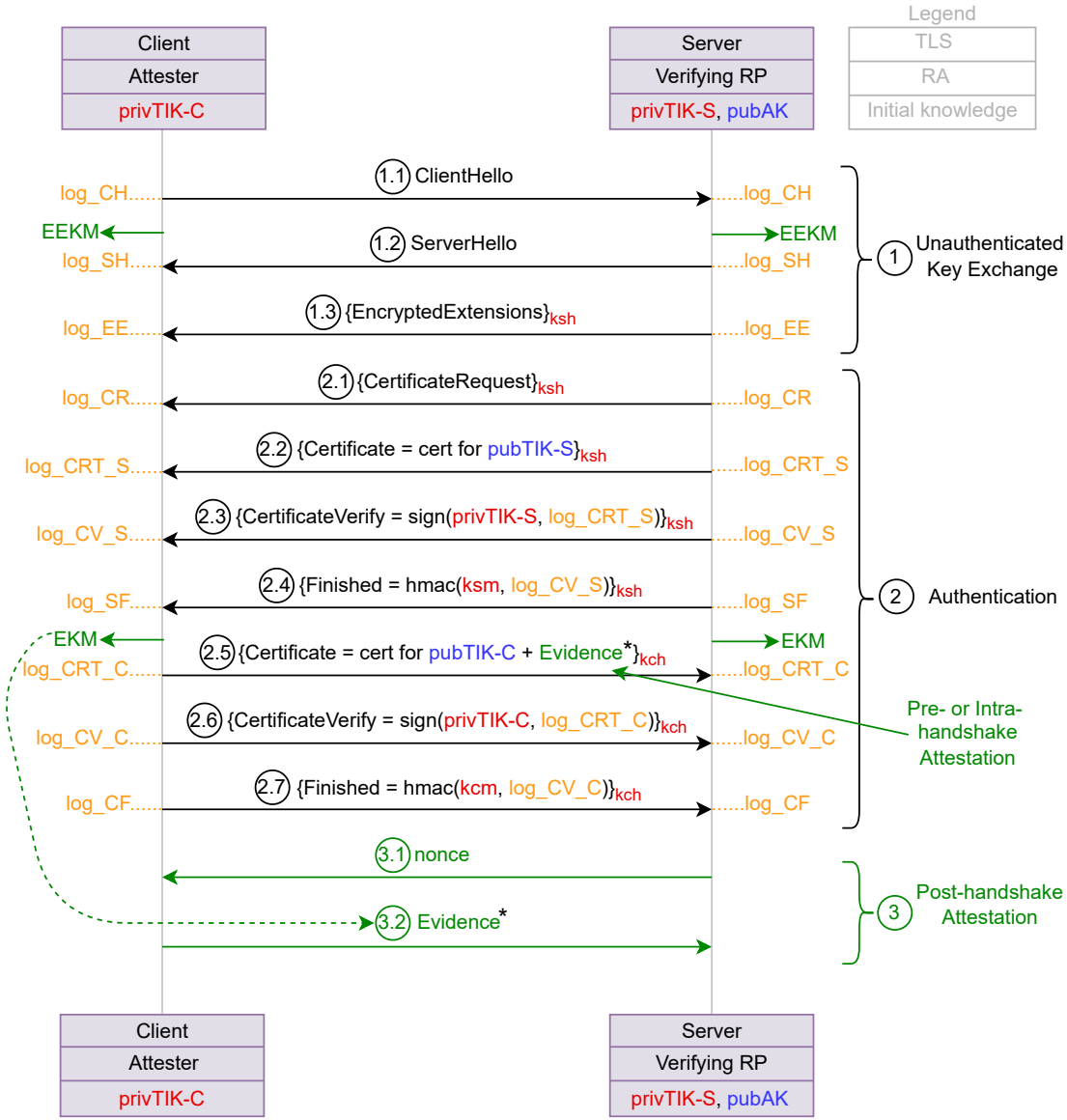
Attested TLS

- TLS 1.3[1]
  - Good for network security
  - Not good for endpoint security
- Use case: Confidential Computing



[1] https://datatracker.ietf.org/doc/html/rfc8446

Generic Protocol (Client as Attester)



What's done: Pre-handshake attestation (Intel's RA-TLS)

- Intel neither specified protocol nor properties
- RATS WG is too vague and incomplete about security considerations
  - RATS Architecture[2], e.g., errata[3]
  - Interaction models[4], e.g., issue[5]
- Tool: ProVerif

Property	Without `privEK` leak	With `privEK` leak
Freshness of evidence	× (1.7 s)	× (6 min 56 s)
Server authentication	✓ (4.6 s)	× (2 min 08 s)

Table: Verification results and times for RA-TLS protocol

[2] `https://datatracker.ietf.org/doc/html/rfc9334`

[3] `https://www.rfc-editor.org/errata_search.php?rfc=9334`

[4] `https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/11/`

[5] `https://github.com/ietf-rats-wg/draft-ietf-rats-reference-interaction-models/issues/58`

What we are looking for?

- Seek collaborators knowledgeable in at least one of:
  - TLS
  - Remote attestation
  - Formal methods (Symbolic security analysis)
  - Confidential computing

  and interested in precisely specifying further properties of attested TLS

- Side meetings
  - Basic attested TLS tutorial: Tuesday 9:30-11:30, Wicklow Hall 2A
  - Advanced attested TLS tutorial: Wednesday 9:30-11:30, Wicklow Hall 2A

Pointers to resources

- Pre-handshake attestation[6]
- Intra-handshake attestation[7]
- Post-handshake attestation: Sec. 4 in this paper[8]
- Remote Attestation for Confidential Computing[9]
- Repo for attestation[10]
- Some recent slides and videos[11]
- Slides from side-meeting at IETF 120[12]
- #attested-tls on IETF slack

---

[6] https://www.researchgate.net/publication/385384309_Towards_Validation_of_TLS_13_Formal_Model_and_Vulnerabilities_in_Intel's_RA-TLS_Protocol

[7] https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/

[8] https://www.researchgate.net/publication/367284929_SoK_Attestation_in_Confidential_Computing

[9] https://www.researchgate.net/publication/375592777_Formal_Specification_and_Verification_of_Architecturally-defined_Attestation_Mechanisms_in_Arm_CCA_and_Intel_TDX

[10] https://github.com/CCC-Attestation/formal-spec-TEE

[11] https://github.com/CCC-Attestation/formal-spec-KBS

[12] https://www.researchgate.net/publication/382489639_Presentation_Interactive_Tutorial_Attested_TLS_and_Formalization