Relay Attacks in Intra-handshake Attestation for Confidential Agentic AI Systems

Muhammad Usama Sardar[1,2], Viacheslav Dubeyko[3], and Jean-Marie Jacquet[4]

[1]TU Dresden, Germany

[2]Co-chair, Trusted Research Environment (TRE) Open Suite, Global Alliance for Genomics and Health (GA4GH)

[3]IBM, San Jose, CA, USA

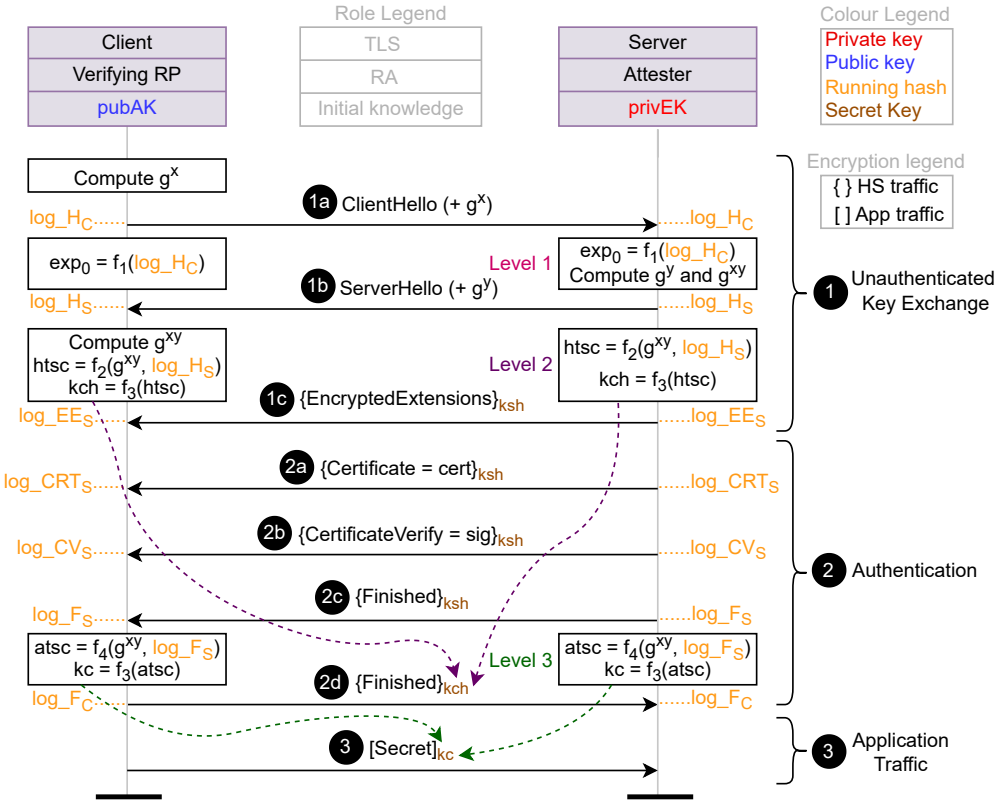
[4]Nadi Research Institute, University of Namur, Belgium

March 10, 2026

Attested TLS

- 3 ways to extend TLS with remote attestation
  - pre-handshake attestation
  - intra-handshake attestation
  - post-handshake attestation
- Paul (AD) requested an exhaustive exploration of intra-handshake attestation.
- Used state-of-the-art tool ProVerif

Devil is in the Details!



- `htsc`: used for encryption of clientFinished message (2d).
  - Irrelevant for security goals
  - Server not yet authenticated at this point
- `atsc`: used for encryption of application data (client's secret, e.g., decryption key)
  - Relevant for security goals

Potential Mechanisms for Binding (TLS Server as Attester)

S. No.	Binding material	Value of rdata field
1	Client's TLS nonce	nc
2	Client's attestation nonce	na
3	Early exporter	exp_0
4	Server's public key	pubEK
5	Client's attestation nonce and early exporter	na $\|$ exp_0
6	Client's attestation nonce and server's public key	na $\|$ pubEK
7	Nonce, server's public key, and early exporter	na $\|$ pubEK $\|$ exp_0

- Example implementations: all are vulnerable to relay attacks
  - #1: Meta's AI (even after extensive security review by *Trail of Bits* without formal methods)
    - No Evidence freshness
  - #5: draft-fossati-tls-attestation-06
  - #6: Edgeless Systems Contrast, Cocos AI and CCC PoC[1]

[1] https://github.com/CCC-Attestation/attested-tls-poc

What we learned

Intra-handshake attestation is NOT a suitable choice for standardization.

We propose post-handshake attestation (draft-fossati-seat-expat)!

Next steps: Present the results at

- LAKE WG: Monday
- SEAT WG: Tuesday
- CATALIST BoF: Wednesday
- CFRG: Thursday
- TLS WG: Friday
- Side meeting: Proposal for new RG
  - Confidential AI, Monday; 18:30 - 20 Uhr; Jiangsu and online

Links to Resources

- Wiki page
  - `github.com/EuroProofNet/ProgramVerification/wiki/AttestedTLS`
- Formal proof of insecurity of pre- and intra-handshake attestation
  - `github.com/CCC-Attestation/formal-spec-id-crisis`
- Post-handshake attestation draft
  - `datatracker.ietf.org/doc/draft-fossati-seat-expat/`
- Attestation in Arm CCA and Intel TDX
  - `github.com/CCC-Attestation/formal-spec-TEE`
- Work-in-progress Implementation
  - `https://github.com/tls-attestation/attestation-exported-authenticators`
- Security considerations of remote attestation
  - `datatracker.ietf.org/doc/draft-sardar-rats-sec-cons/`
- IETF SEAT WG
  - `datatracker.ietf.org/wg/seat/about/`
- Technical Concepts
- Validation of TLS 1.3 Key Schedule
- General Approach
- Weekly meetings: `github.com/tls-attestation#meetings`