

Formal Proof of Insecurity of Intra-handshake Attestation and Proposal for Post-handshake Attestation

Muhammad Usama Sardar

TU Dresden, Germany

March 15, 2026

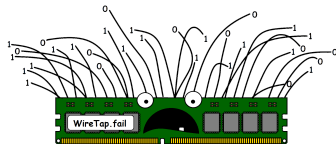
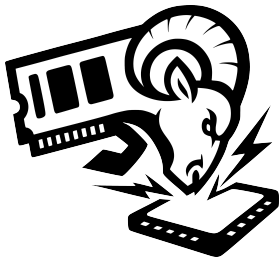
Attested TLS

- 3 ways to extend TLS with remote attestation
 - pre-handshake attestation
 - intra-handshake attestation
 - post-handshake attestation
- Formal analysis of intra-handshake attestation
 - Diversion attacks¹ (with Mariam and Tuomas)
 - Relay attacks² (with Viacheslav and Jean-Marie)
- Proposal
 - Post-handshake attestation (draft-fossati-seat-expat)
 - based on RFC9261

¹<https://github.com/CCC-Attestation/formal-spec-id-crisis>

²https://mailarchive.ietf.org/arch/msg/seat/x3eQxFjQFJLceae614_NgXnmsDY/

Diversion attacks shown to be practically feasible



Relay attacks acknowledged by Cocos AI

`https://web.archive.org/web/20260227160554/https://www.ultraviolet.rs/blog/tee-tls-privacy/`

What we are looking for?

- **Implementers** of post-handshake attestation (draft-fossati-seat-expat)
- Contributors in **formal analysis** of post-handshake attestation (draft-fossati-seat-expat)
- **Collaborators** knowledgeable in at least one of:
 - **TLS**
 - **Remote attestation**
 - **Formal methods** (Symbolic security analysis)
 - **Confidential computing**

Links to Resources

- Work-in-progress Implementation
 - <https://github.com/tls-attestation/attestation-exported-authenticators>
- 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
- 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

ACK: Co-authors (in papers/IETF drafts)

- Jean-Marie Jacquet (University of Namur)
- Ionut Mihalcea (Arm)
- Thomas Fossati (Linaro)
- Arto Niemi (Huawei)
- Hannes Tschofenig (University of Applied Sciences Bonn-Rhein-Sieg and Siemens)
- Simon Frost (Arm)
- Ned Smith (Intel)
- Carsten Weinhold (Barkhausen Institut)
- Michael Roitzsch (Barkhausen Institut)
- Yogesh Deshpande (Arm)
- Yaron Sheffer (Intuit)
- Tirumaleswar Reddy K. (Nokia)
- Henk Birkholz (Fraunhofer SIT)
- Mariam Moustafa (Aalto University)
- Tuomas Aura (Aalto University)
- Liang Xia (Huawei)
- Weiyu Jiang (Huawei)
- Jun Zhang (Huawei)
- Houda Labiod (Huawei)
- Yuning Jiang (Huawei International)
- Meiling Chen (China Mobile)
- Peter Chunchi Liu (Huawei Technologies)
- Minghui Xu (Shandong University)
- Pavel Nikonorov (GENXT)
- Viacheslav Dubeyko (IBM)

ACK: Contributors

- Eric Rescorla (Independent)
- Laurence Lundblade (Security Theory LLC)
- Göran Selander (Ericsson AB)
- Marco Tiloca (RISE AB)
- Richard Barnes (Cloudflare)
- Giridhar Mandyam (AMD)
- Christopher Patton (Cloudflare)
- Dionna Amalie Glaze (Google)
- Bob Beck (Google)
- Mike Ounsworth (Cryptic Forest Software)
- John Preuß Mattsson (Ericsson Research)
- Cedric Fournet (Microsoft)
- Thore Sommer (TU Munich)
- Nikolaus Thümmel (Scontain)
- Jonathan Hoyland (Cloudflare)
- Jo Van Bulck (KU Leuven)
- Martin Thomson (Mozilla)
- Britta Hale (Naval Postgraduate School)
- Werner Staub (CORE Association)
- Christian Simmen (DENIC)
- Dennis Jackson (Mozilla)
- Paul Wouters (Aiven)
- Matthias Wählisch (TU Dresden)
- Andrey Ruzhanskiy (Telekom MMS)
- Muuhh Ikede (Cybertrust)
- Mike Bursell (CCC)
- Ravi Sahita (Rivos)
- Samuel Ortiz (Rivos)
- Mathieu Poirier (Linaro)
- Hannes Reinecke (SUSE)
- Alexander Graf (AWS)
- Elena Reshetova (Intel)
- Jon Lange (Microsoft)
- Daniel Kiper
- David Woodhouse (AWS)
- David Kaplan (AMD)
- Tiziano Santoro (Google)
- Juho Forsén
- Ira McDonald
- Markus Rudy (Edgeless Systems)
- Ayoub Benaissa (Zama)
- Greg Kostal (Microsoft)
- Mike Stunes (Microsoft)
- David Altobelli (Microsoft)
- and many others...