Contribution ID: **416** Type: **not specified**

Standardization of Attested TLS Protocols

Friday 12 December 2025 12:00 (30 minutes)

Summary

This talk is a follow-up of LPC'24, where the community had diverse opinions on the suitable approach of attested TLS protocols for confidential computing. Meanwhile, we have defended our position (cf. expat BoF) to standardize the protocol in the IETF, and a new Working Group named Secure Evidence and Attestation Transport (SEAT) has been formed to exclusively tackle this specific problem. We would like to present updates to the work since last year (candidate draft for standardization) and gather feedback from the community on the desired security goals, so that it can be accommodated in the standardization.

Background

Transport Layer Security (TLS) is a widely used protocol for secure channel establishment. However, it lacks an inherent mechanism for validating the security state of the workload and its platform. To address this, remote attestation can be integrated into TLS, which is named attested TLS protocol. At LPC'24, we presented an overview of the three approaches for this integration, namely pre-handshake attestation, intra-handshake attestation, and post-handshake attestation. We also presented insights from the Formal Verification using the state-of-the-art symbolic security analysis tool ProVerif to provide high confidence for use in security-critical applications.

Current project partners include Arm, Linaro, Siemens, Huawei, Intuit, Axis, Bonn-Rhein-Sieg University of Applied Sciences, and Barkhausen Institut. By this talk, we hope to inspire more open-source contributors to this project.

The attendees will gain technical insights into the latest developments of standardization of attested TLS protocols in the IETF and will be able to provide feedback on the requirements for their use cases of attestation for confidential computing.

Benefits to the ecosystem

Our thorough analysis shows that pre-handshake attestation is potentially vulnerable to replay, relay, and diversion attacks. On the other hand, intra-handshake attestation is potentially vulnerable to relay and diversion attacks. While post-handshake attestation results in slightly high latency, it offers better security properties than the other two options, forming a valuable contribution to the TEE attestation ecosystem.

In a nutshell, to provide more robust security guarantees, applications can replace standard TLS with attested TLS.

Background readings

- Technical Concepts
- Validation of TLS 1.3 Key Schedule
- General Approach

Primary author: SARDAR, Muhammad Usama (TU Dresden)

Presenter: SARDAR, Muhammad Usama (TU Dresden)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC