Contribution ID: **335**

Type: **not specified**

Attested TLS and Formalization

Friday, 20 September 2024 11:15 (15 minutes)

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 in TLS, which is named attested TLS. In this talk, we present a survey of the three approaches for this integration, namely pre-handshake attestation, post-handshake attestation and intra-handshake attestation. We also present our ongoing research on Formal Verification of the three approaches 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 TU Dresden, Arm, Bonn-Rhein-Sieg University of Applied Sciences, Barkhausen Institut, Linaro, Siemens, Huawei, and Intuit. By this talk, we hope to inspire more open-source contributors to this project.

The attendees will gain technical insights into attested TLS protocols for their use cases of attestation for confidential computing. We demonstrate to the attendees that the widely used Intel's RA-TLS protocol is vulnerable to replay attacks.

Benefits to the ecosystem

Our preliminary analysis shows that pre-handshake attestation is potentially vulnerable to replay and relay attacks. On the other hand, post-handshake attestation results in high latency. Intra-handshake attestation, offering high security via formal verification and low latency by avoiding the additional roundtrip, forms a valuable contribution to the TEE attestation ecosystem.

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

Primary author: SARDAR, Muhammad Usama (TU Dresden)

Presenter: SARDAR, Muhammad Usama (TU Dresden)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC