RATLS: Integrating Transport Layer Security with Remote Attestation

Carsten Weinhold, Michael Roitzsch
Barkhausen Institut, Dresden, Germany Robert Walther

Technische Universität Dresden, Dresden, Germany

Transport Layer Security (TLS) is the state-of-the-art protocol for secure communication channels between two machines. It uses encryption and message authentication to ensure confidentiality and integrity for all information transmitted over the channel. TLS also offers authentication to ensure that only the "right" communication partners can successfully establish a TLS connection. The authentication method used by TLS requires that users trust the party operating the remote computer to keep this computer secure. If Alice wants to exchange data via TLS with a computer operated by Bob, she usually has to make two assumptions: 1) Bob keeps secret the cryptographic keys required for TLS authentication and 2) the software running on Bob's computer does what he claims (e.g. not leak data received from Alice).

Unfortunately, TLS alone cannot provide verifiable evidence that assumptions 1) and 2) actually apply. However, in certain highly critical use cases, such proof is desirable. For example, Alice may want the assurance that her valuable scientific data will only be processed by a specific, trusted analysis program that runs on the cloud server Bob rented to her. And in an Internet of Things (IoT) scenario, life could be at stake if an attacker manages to manipulate the firmware of an IoT device. Therefore, technical measures are needed to reduce confidence in the operator of a remote computer or the environment that surrounds it.

Remote Attestation is a cryptographic protocol that solves the two trust issues described above. First, it is based on a hardware root-of-trust, which is intended to protect cryptographic secrets. Second, it provides verifiable proof that the software running on another computer is in a known-good state.

Despite the clear security advantages, remote attestation is complicated for application developers to deploy. There is no standardized protocol suite, but various root-of-trust implementations come with their own protocol and software development kit. In this talk, we present RATLS [1], which intends to simplify the use of attestation by integrating it into the widely used TLS protocol. We have developed RATLS as an auxiliary library for the widely used OpenSSL implementation. The design of RATLS is also independent of the underlying hardware trust root. In this talk, we describe a RATLS plugin that works with the widely used TPM v2.0.

References

[1] Robert Walther, Carsten Weinhold, Michael Roitzsch. RATLS: Integrating Transport Layer Security with Remote Attestation. 4th Workshop on Cloud Security and Privacy (Cloud S&P). Springer, June 2022.