Towards Formal Verification of Attested TLS: Potential Replay Attacks on RA-TLS*

Muhammad Usama Sardar[1], Arto Niemi[2], Hannes Tschofenig[3] and Thomas Fossati[4]

[1] TU Dresden, Germany
muhammad_usama.sardar@tu-dresden.de
[2] Huawei Technologies, Helsinki, Finland
arto.niemi@huawei.com
[3] University of Applied Sciences Bonn-Rhein-Sieg and Siemens, Germany
Hannes.Tschofenig@siemens.com
[4] Linaro, Lausanne, Switzerland
thomas.fossati@linaro.org

Abstract. Transport Layer Security (TLS) is a widely used protocol for secure channel establishment. However, it lacks any inherent mechanism for validating the security state of the endpoint software and its platform. To overcome this limitation, there have been recent proposals to combine remote attestation and TLS, named as attested TLS. The most common attested TLS protocol for confidential computing is Intel's RA-TLS, which is used in multiple open-source industrial projects. By using the state-of-the-art symbolic security analysis tool ProVerif, we found a potential issue in RA-TLS, namely attestation evidence can be replayed from an old session without the verifier noticing. We finally reflect on the challenges and lessons learned in the formalization process, including the discovery of crucial issues in the earlier formalization of TLS.

Keywords: Formal analysis · Transport Layer Security (TLS) · Remote Attestation (RA) · Symbolic Security Analysis · ProVerif.

* funded by DFG grant 389792660 as part of TRR 248 – CPEC.