Identity Crisis in Attested TLS for Confidential Computing (Oral Communication)*

Muhammad Usama Sardar

TU Dresden, Germany
muhammad_usama.sardar@tu-dresden.de

Abstract. Remote attestation is increasingly being composed with different protocols to provide endpoint security. Transport Layer Security (TLS) is the most widely used among those protocols, and the composition of TLS with remote attestation is known as attested TLS protocol. Such protocols are used in security-critical applications, e.g., they serve as the backbone of an emerging computing paradigm, Confidential Computing (CC). In this work, we formalize attested TLS protocols in CC and explore the identity crisis that results from ambiguous notions of identity. We present a formal approach with a set of comprehensive security goals and a generic template for the comparison of the security strengths of attested TLS protocols. Using the approach, we discover vulnerabilities in two state-of-the-art protocols, namely Interoperable RA-TLS and TLS-attest, and propose potential solutions for the vulnerabilities.

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

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