

Extending TLS with mutual attestation for platform integrity assurance

ABSTRACT

Normally, secure communication between client-server applications is established using secure channel technologies such as Transport Layer Security (TLS). TLS is cryptographic protocol which ensures secure transmission of data and authenticity of communication at each endpoint platform. However, the protocol does not provide any trustworthiness assurance of the involved endpoint. This paper incorporates remote attestation in the TLS key exchange protocol to solve this issue. The proposed embedded attestation extension in TLS protocol will provide assurance of sender's platforms integrity to receiver, and vice versa. The CA responsibility in TLS is replaced using own Trusted Certificate Authority (TCA) in our protocol. The credibility of the proposed protocol is studied to secure against replay attack and collusion attack. The proof is performed using AVISPA with High Level Protocol Specification (HLPSL) through Dolev-Yao intruder model implementation of the proposed protocol.

Keyword: Certificate Authority (CA); Integrity; Remote attestation; SSL/TLS extension; TPM