Performance analysis for extended TLS with mutual attestation for platform integrity assurance

ABSTRACT

A web service is a web-based application connected via the internet connectivity. The common web-based applications are deployed using web browsers and web servers. However, the security of Web Service is a major concern issues since it is not widely studied and integrated in the design stage of Web Service standard. They are add-on modules rather a well-defined solutions in standards. So, various web services security solutions have been defined in order to protect interaction over a network. Remote attestation is an authentication technique proposed by the Trusted Computing Group (TCG) which enables the verification of the trusted environment of platforms and assuring the information is accurate. To incorporate this method in web services framework in order to guarantee the trustworthiness and security of web-based applications, a new framework called TrustWeb is proposed. The TrustWeb framework integrates the remote attestation into SSL/TLS protocol to provide integrity information of the involved endpoint platforms. The framework enhances TLS protocol with mutual attestation mechanism which can help to address the weaknesses of transferring sensitive computations, and a practical way to solve the remote trust issue at the client-server environment. In this paper, we describe the work of designing and building a framework prototype in which attestation mechanism is integrated into the Mozilla Firefox browser and Apache web server. We also present framework solution to show improvement in the efficiency level.

Keyword: Web service; TLS protocol; Network security; Attestations; TrustWeb