Generic Light Weight Certificate Management Protocol

By

Muhammad Asif

2008-NUST-MS-CCS-02

Thesis Supervisor

Dr. Abdul Ghafoor

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Computer and Communication Security (MS-CCS)

In

School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

Abstract

Mobile devices and digital gadgets are very popular and commonly used in daily life. Theoretically, various security solutions are designed to protect the valuable information of mobile users. But, its power, memory and processing constraints, high response time and authentication latencies are the main challenges for the researcher to develop and integrate standard security mechanisms in it. It is observed that, most of mobile users are not technical enough to configure security parameters and even already developed libraries do not support extended security features like transparent handling of certificates, verification of identities, and distribution of certificates.

In order to solve above mentioned problems, a Generic Light Weight Certificate Management Protocol (GLCMP) is designed. We adopted a holistic approach in order to solve complex certificate management task. In order to achieve desired objectives, proxy based architecture has been adopted to offload computational intensive operations from mobile devices. In GLCMP, the trust between mobile device and proxy server is developed without exchanging any secret information on network. In addition, GLCMP is designed and developed by using the concept of generic security objects. The claimed security properties (authentication, confidentiality and non-repudiation) of the protocol are formally verified by employing formal ***Z-Notation modeling.*** In Z-Notation modeling, different attacks are formalized on messages exchanged between components and discussed all possible scenarios in which an attacker can attack the protocol. After verification, it is concluded that the designed protocol resists against most of the attacks launched on registration and verification process such as impersonation, man-in-the-middle and replay. Furthermore, for the proof of the concepts, the GLCMP is implemented and evaluated based on certain parameters. Computed Authentication latency is 0.394 sec which is less than its nearest competitors NSI (4.7), PKI (5.01), and PKASSO (5.19 delegation time + 0.082 authentication times). Moreover, our design is also providing secure registration and certificate management.