Università degli Studi di Salerno

Dottorato di Ricerca in Informatica e Ingegneria dell'Informazione

Ciclo 31 – a.a 2017/2018

ABSTRACT PH.D. THESIS

Improvement in the management of cryptographic keys in a HSM and proposal of an Outdoor Position Certification Authority

Marco MANNETTA

SUPERVISOR: **Prof. Roberto DE PRISCO**

PHD PROGRAM DIRECTOR: **Prof. Pasquale CHIACCHIO**

Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica Applicata

Dipartimento di Informatica

Abstract

The following doctoral thesis comprises two distinct sections, both describing a specific applied research concerning the macro-theme of computer security. The first section describes a proposal for the improvement and optimization of the storage space required for the management of cryptographic keys within a Hardware Security Module (**HSM**), whereas the second section outlines the design of an Outdoor Position Certification Authority (**OPCA**), a distributed client-server architecture aimed for the validation and certification of the positioning of a mobile device.

A **Hardware Security Module** is a special device designed for cryptographic operations and cryptographic keys management. The latter keys are stored into the HSM and never exposed outside the device. All the operations carried out through the keys are performed inside the HSM so the operations result is indeed the only external outcome produced by the HSM. In order for the HSM to store all the keys that have to be managed, plenty of storage space is required. The biggest data centres, handling millions of cryptographic keys, need to host a large number of HSMs. The related costs are proportional to the number of HSMs used. These costs include: hardware, energy consumption, network hosting, network speed, management, etc. In this thesis, there can be found two methods to save the space useful for the storage of the keys in a HSM, so to reduce the number of HSMs needed and all related costs. While reducing costs on storage, expenses related to computation time will increase.

The outlined **Outdoor Position Certification Authority** represents the project and design of a certification authority whose purpose is to certify the positioning of a mobile device equipped with a *GNSS (Global Navigation Satellite System)* receiver. In general, a GNSS receiver is capable of acquiring radio signals (low-level data) and navigation messages (high-level data) in the outdoor environments coming from different constellations of global/regional satellite

navigation systems and satellite-based augmentation system (SBAS). To date, these data are not reliable from a security point of view, because they can be easily forged by malicious attackers through specialized spoofing techniques. An OPCA defines a client/server architecture through which a user can certify his position by sending to one or more remote servers the geo-localization information required for its verification. Once the truthfulness and reliability of the data received have been verified, the OPCA will issue and then send to the client a digitally signed document having legal force and certifying the position of the user in a given moment. The use of this service will concern different and multiple scenarios and the devices requiring it will extensively grow in number thanks to the spread of the Internet of Things (IoT).
Here are some possible scenarios: remote digital signing of a document for users located in a specific place; certification of the geographical position of a user in a given moment; certification of geographical position related to the delivery of valuable goods; certification of geographical position in case of critical events, such as rescue operations, police actions, etc.

The first section of this thesis has been carried out based on two scientific publications. The first one, entitled *"Reducing Costs in HSM-Based Data Centres"*, is a conference publication presented during the *"International Conference on Green, Pervasive, and Cloud Computing 2017 (GPC 2017) at Cetara (SA)"*. This paper offers a first experimental evaluation of what will be found in the next pages and referred to as "**Enhanced HSM (EHSM)"**. The second paper is a journal version, published in the *"Journal of High Speed Networks (JHSN) - IOS Press"*. In this publication, an alternative approach has been illustrated in relation to the issue of space storage in the key management of a HSM.

The second section of the thesis is based on an *International Patent* registered at the *European Patent Organization (EPO),* its official number being *EP 18724344.9,* and on a related paper, being completed, entitled *"Design of an Outdoor Position Certification Authority"*.