Università degli Studi di Salerno

Dottorato di Ricerca in Informatica e Ingegneria dell'Informazione

Ciclo 31 – a.a 2017/2018

ABSTRACT TESI DI DOTTORATO

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

Il tema generale può essere riassunto in "**Crittografia e Sicurezza**". All'interno di questo macro tema vengono collocati due specifici filoni di **ricerca** applicata.

Il primo argomento di ricerca applicata riguarda la sperimentazione di un ***"Enhanced Hardware Security Module – EHSM"*** per la generazione e la gestione delle chiavi crittografiche. Con la parola "*Enhanced"* si intende indicare una versione migliorata di un HSM classico riguardo l'*ottimazione dello spazio di archiviazione* delle chiavi crittografiche e i relativi *costi di gestione* in grandi data center. Un EHSM è una innovazione, variante specifica di un HSM classico, concepita per specifici contesti, nei quali l'obiettivo primario è *abbattere i costi di management* attraverso una significativa riduzione dello spazio di archiviazione da utilizzare, che si materializza in un *numero minore di HSM da acquistare*, un conseguente *abbattimento dei costi di manutenzione* e un *abbassamento dei costi energetici*. In un EHSM la chiavi crittografiche non sono più generate e memorizzate in un database cifrato, ma vengono create *"on the fly"* ad ogni specifica richiesta utente attraverso *algoritmi crittografici di generazione dei numeri pseudo-causali*, *random function* e utilizzo di strutture dati specifiche come i *Merkle Tree (o Hash Tree)*.

Il secondo filone di ricerca applicata riguarda il "*posizionamento sicuro*" ed è orientato verso l'ideazione e la sperimentazione di un'"***Autorità di Certificazione della Posizione Outdoor - OPCA***". Scopo di tale autorità è fornire lato server un servizio di certificazione a valore legale della posizione globale di un utente che, in un determinato istante, ne fa richiesta tramite un dispositivo mobile abilitato al servizio. Il servizio è orientato alla geolocalizzazione *outdoor* e sfrutta i segnali radio generati dal sistema GNSS (*Global Navigation Satellite System*). Per certificare la posizione dell'utente la OPCA richiede l'invio di diverse tipologie di informazioni lato client relative ai segnali radio acquisiti dai diversi sistemi di localizzazione satellitari globali, quali i *dati elaborati di alto*

livello relativi ai messaggi di navigazione (struttura del pacchetto dati e relativi messaggi di navigazione – data frame) e i *dati grezzi non elaborati di basso livello* (portante, fase, effetto doppler, potenza e rapporto segnale/rumore del segnale radio, valori e fase del codice pseudo-range, etc.). Il server confronterà tali dati con quelli in suo possesso (acquisiti attraverso le proprie antenne GNSS, elaborati e storicizzati lato server ad intervalli regolari all'interno di una specifica finestra temporale) e potrà identificare eventuali discrepanze ed anomalie frutto di tentativi di frode (*spoofing*). Se tutte le verifiche avranno esito positivo, la OPCA certificherà la posizione dell'utente fornendo al client un *report di geolocalizzazione firmato digitalmente a valore legale e marcato digitalmente*, attestante la posizione dell'utente in quel determinato momento. La versione attuale della OPCA utilizza il solo sistema GNSS per la certificazione della posizione utente, ma in futuro è previsto un'estensione e potenziamento del servizio (in termini di copertura, efficienza e precisione) attraverso la raccolta ed analisi di dati di geolocalizzazione derivati da altri sistemi di comunicazione, come quelli generati dalle *Base Station* della rete cellulare, dalle *reti WIFI* (per la localizzazione *indoor*) ed eventuali sensori presenti sul dispositivo mobile dell'utente (altimetro, magnetometro, giroscopio …).