UNIVERSITÀ POLITECNICA DELLE MARCHE

DII DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Avviso di Seminario

Corso di Laurea Magistrale in Ingegneria Elettronica
Nell'ambito dell'insegnamento Cybersecurity for Networks

Lunedì 13 Maggio dalle 11:30 alle 13:30
AULA 160/2

FIRME DIGITALI A SOGLIA

RELATORE: Michele Battagliola
Dipartimento di Ingegneria dell'Informazione
Università Politecnica delle Marche

Abstract. La crescente diffusione delle tecnologie distribuite ha causato un forte interesse per i protocolli di firma a soglia, che ha raggiunto l'apice con la recente "First Call for Multi-Party Threshold Schemes" del NIST. Una firma a soglia (t, n) consente di distribuire il protocollo di firma tra n utenti, in modo tale che qualsiasi sottoinsieme di dimensione almeno t di essi possa firmare, mentre qualsiasi sottoinsieme con meno utenti non possa farlo. Di solito, la sicurezza di una firma digitale viene dimostrata attraverso una dimostrazione "ad hoc", che riduce la sicurezza della firma alla soluzione di un problema matematico difficile.

Dopo una breve introduzione sulle firme a soglia, il seminario presenterà la Trasformata Distribuita di Fiat-Shamir, una nuova euristica per semplificare la progettazione e la dimostrazione di firme a soglia. Fin dalla sua introduzione, la Trasformata di Fiat-Shamir è stata il modo più diffuso per progettare schemi di firma digitale. Si trasporta la trasformata di Fiat-Shamir nel mondo della multi party computation, costruendo un framework che mira a essere un modo alternativo e più semplice per progettare firme digitali a soglia. Si introduce il concetto di schema di identificazione a soglia e di sigma protocol a soglia e si mostrano le condizioni necessarie e sufficienti per dimostrare la sicurezza degli schemi di firma a soglia da essi derivati. Verrà mostrata anche un'applicazione pratica del framework presentato, fornendo una dimostrazione di sicurezza alternativa per Sparkle, una recente firma a soglia di Schnorr.

Bio: Laureato magistrale in Matematica, curriculum di Crittografia e Teoria dei codici, Michele Battagliola sta conseguendo il Dottorato in Matematica presso l'Università di Trento. Attualmente ricopre la posizione di assegnista di ricerca all'Università Politecnica delle Marche nell'ambito del Progetto PRIN 2022 "Post quantum Identification and eNcryption primiTives: dEsign and Realization".

Per informazioni: Prof. Marco Baldi (m.baldi@univpm.it)