27 Settembre 2018
Sala Conferenze “Emilio Gatti”
DEIB, Politecnico di Milano
ore: 14.00-18.00

Sicurezza hardware nei sistemi digitali

Abstract

La sicurezza dei sistemi digitali, a livello hardware (microelettronico circuitale), vale a dire di processore, sistema di memoria e sistemi di comunicazione, sta crescendo in importanza. Le tecnologie, più o meno invasive, che permettono di simulare, sondare e perfino perturbare i sistemi digitali, diventano sempre più sofisticate e precise: simulazione del comportamento e della struttura a livello logico, elettrico, termico, radio e ottico; profilazione della potenza consumata o irradiata, ispezione del dispositivo a frequenza radio e ottica; manomissione tramite iniezione di disturbi temporanei e guasti permanenti; per finire con “reverse engineering” (ricostruzione) più o meno accurato, o addirittura “editing” (modifica) del circuito. I metodi di attacco proliferano, e di necessità sempre più funzioni di sicurezza hardware vengono inserite nei moderni sistemi integrati. Questo seminario presenta lo stato dell’arte in materia, illustrandone concetti, tecnologie e soluzioni, e dando qualche esempio, nei campi tecnologici e applicativi principali: microprocessori, sistemi di memoria e “Internet of Things” (IoT). Il seminario è rivolto principalmente a ingegneri professionisti e a studenti in ingegneria delle tecnologie dell’informazione e della comunicazione (ICT), pertanto è opportuna una conoscenza base dei sistemi digitali, ma non richiede competenze specifiche.

Programma

Chairs: Luca Breveglieri (Polimi - DEIB), Giuseppe Gattavari (AEIT - AMES), Mariagiovanna Sami (Accademia delle Scienze)

- 14.00-14.30: Domenico Squillace (Technical Relations Executive IBM Italia – Presidente UNINFO)

Sicurezza informatica: da che cosa ci dobbiamo difendere e come? (Quadro di riferimento applicativo e normative con un occhio su IoT)

Intervento di inquadramento generale sulle problematiche e soluzioni per sicurezza nelle applicazioni e normative (con qualche attenzione a IoT).

- 14.30-15.00: Guido Bertoni (Security Patterns)

La sicurezza hardware nei moderni circuiti integrati: attacchi e prevenzione

Molti circuiti integrati (microchip), specialmente processori e memorie, presentano funzionalità di sicurezza. Se ne trovano sia nei microcontrollori per uso industriale sia nei microprocessori per uso generale (server di rete, computer da tavolo e sistemi mobili). La richiesta di sicurezza è in aumento costante e anche prodotti economici devono disporre di funzioni (primitive) di sicurezza. Tali primitive sono blocchi hardware funzionali base per costruire un sistema sicuro. In questo tutorial, si mostrerà quali sono e a che cosa servono, in relazione agli attacchi che mirano a prevenire. Se da una parte si riscontra un aumento dell’offerta di sicurezza, dall’altra gli attacchi diventano sempre più raffinati e potenti, grazie alla notevole varietà di tecnologie che permettono di simulare, sondare o perturbare sistemi digitali di ogni tipo. Trovare il giusto equilibrio tra sicurezza e costo dipende fortemente dall’applicazione e dalla tipologia di dati trattati.

- 15.00-15.30: Francesco Regazzoni (Università della Svizzera Italiana - Alari)

Funzioni di sicurezza nelle architetture di microprocessore

Istruzioni dedicate e meccanismi vari per la sicurezza sono state e saranno sempre più incluse nei microprocessori moderni. Le istruzioni dedicate servono principalmente ad accelerate il calcolo di algoritmi crittografici eseguiti in software, mentre i meccanismi a supporto della sicurezza servono a creare "enclavi" sicure, a cifrare la memoria e a realizzare la cosiddetta "root-of-trust". Questo tutorial introduce le funzionalità di sicurezza presenti nei microprocessori maggiormente utilizzati e illustra alcuni problemi di sicurezza che si presentano nelle architetture di processore.

- 15.30-16.00: **Intervallo**

- 16.00-16.30: Paolo Amato (Micron)

Problemi e soluzioni di sicurezza nelle memorie tradizionali ed emergenti

La memoria diventa sempre più una componente chiave per un sistema digitale sicuro. Diminuendo costantemente la dimensione della cella di memoria RAM dinamica (DRAM), e aumentando la densità di memoria, emergono fenomeni di inaffidabilità e fragilità che mettono a rischio il funzionamento corretto della memoria, e che dunque possono causare qualche vulnerabilità o falla sfruttabile praticamente contro la sicurezza del sistema. Un esempio notevole è il cosiddetto attacco "RowHammer" o "martellamento" della cella di memoria. Guardando più avanti, si intravvedono questioni di sicurezza e privatezza perfino più impegnative e di lungo termine, che potrebbero scaturire dall'entrata in uso progressiva di tecnologie di memoria RAM non-volatile (NVM – Non-Volatile Memory), come per esempio la tecnologia PCM (Phase-Change Memory), e anche altre. Infatti, da un lato la memoria RAM non volatile può arricchire la gerarchia di memoria aumentandone capacità e persistenza, tutte proprietà molto desiderabili, senza comprometterne la latenza. Dall'altro lato, avere tutta la memoria RAM persistente (o parte di essa) significa che i dati in elaborazione saranno esposti ad attacchi per tempi prolungati, rispetto alla memoria tradizionale. In questo tutorial, si illustreranno tali rischi, e i metodi e le tecnologie allo studio per eliminarli o quanto meno mitigarli.

- 16.30-17.00: Marco Macchetti (Kudelski Group)

Problemi e soluzioni di sicurezza hardware per Internet of Things (IoT)

Si stima che entro il 2025 il numero di dispositivi digitali in rete supererà 75 miliardi. La crescita rapida di questa "Internet of Things" (IoT) lancia una sfida enorme alla sicurezza dei dati e alla loro protezione. Oggigiorno, molto spesso i circuiti integrati offrono alcune funzioni (primitive) di sicurezza hardware, che vanno da un ambiente di esecuzione sicuro (Trusted Execution Environment), al bootstrap sicuro del sistema operativo, a un file system (sistema di archiviazione) sicuro, ad altre ancora. Il consenso sulla necessità di avere sicurezza a livello hardware è ampio, tuttavia al tempo stesso la politica aggressiva di prezzo basso praticata da numerosi produttori spinge progettisti e fabbricanti di circuiti integrati a trovare modi innovativi per garantire sicurezza a costo limitato. In questo tutorial si illustreranno alcune delle funzionalità di sicurezza hardware più all'avanguardia disponibili sul mercato, o prossime ad esserlo. Per esempio, verranno presentate la tecnologia PUF (Physically Unclonable Function) e la tecnologia "Secure Elements and integrated SIMs" (iUICCs). Siffatte tecnologie avanzate, combinate con protocolli e librerie funzionali di comunicazione sicura progettati specificamente per dispositivi con basso consumo di potenza, come per esempio la tecnologia NB-IoT (NarrowBand Internet of Things), dovrebbero assicurare o almeno facilitare la realizzazione estensiva di sicurezza in ambito IoT, a prezzo ragionevole e con complessità limitata.

- 17.00-18.00: Casi applicativi a cura di AEIT