UNIVERSITÀ DI PISA

HARDWARE AND EMBEDDED SECURITY

SERGIO SAPONARA

Anno accademico	2022/23
CdS	CYBERSECURITY
Codice	930II
CFU	9

Moduli	Settore/i	Tipo	Ore	Docente/i
HARDWARE AND EMBEDDED SECURITY	ING-INF/01	LEZIONI	72	LUCA CROCETTI DANIELE ROSSI SERGIO SAPONARA

Obiettivi di apprendimento

Conoscenze
Il corso Hardware and Embedded Security (9 CFU, 72 ore di lezioni frontali) si propone di fornire le competenze richieste per analizzare, progettare e verificare soluzioni HW o HW / SW dedicate in sistemi embedded (ad es. moduli di sicurezza hardware integrati in processori GPP) per diverse funzioni crittografiche per crittografia / decrittografia, firma/verifica, HW trojans, counterfiting e side channel attacks, rilevamento di anomalie / intrusioni.
Il corso presenterà anche esempi applicativi di sicurezza HW e sicurezza embedded a casi di studio per applicazioni IoT, Automotive o Industria 4.0.

Modalità di verifica delle conoscenze
Esame orale (con almeno 1 domanda per ciascuna delle 2 parti) piu discussione della relaizone di un progettino assegnato a gruppi di studenti (e.g. 1 o 2 studenti per gruppo) dal docente durante il corso

Capacità
Verifica sia delle capacità tecniche acquisite (hard skills) che di quelle
legati ad aspetti relazionali, di lavoro in team, di presentazione risultati ottenuti (soft skills)

Modalità di verifica delle capacità
Esame orale (con almeno 1 domanda per ciascuna delle 2 parti) piu discussione della relaizone di un progettino assegnato a gruppi di studenti (e.g. 1 o 2 studenti per gruppo) dal docente durante il corso

Prerequisiti (conoscenze iniziali)
basi di elettroncia digitale aqcuisite o nella lautrea triennale o nel corso di omogeinizzazione al 1 semestre del Prof. Saletti

Programma (contenuti dell'insegnamento)
Più in dettaglio il programma del corso tratterà i seguenti argomenti con due parti: la prima parte più correlata alla sicurezza integrata a livello hardware digitale e SW di basso livello, mentre il la seconda parte più incentrato sulla sicurezza hardware considerando gli aspetti tecnologici Sicurezza integrata a livello di hardware digitale e SW di basso livello [40 ore]: -Introduzione al corso, docenti, tipologia di esame, nozioni di base richieste per seguire il corso [2 ore] - Co-design HW / SW per la sicurezza informatica e confronto tra soluzioni basate su SW e soluzioni basate su HW in termini di efficienza energetica, capacità operativa in tempo reale, flessibilità, costi e dimensioni [5 ore]. - Analisi di acceleratori crittografici incorporati nei processori General Purpose (es.HSM- Moduli di sicurezza hardware su piattaforme Intel e / o ARM e / o Aurix) [6 ore] Esempi di acceleratori HW per la sicurezza informatica per la crittografia asimmetrica e simmetrica e per la firma (ad esempio coprocessori per AES, SHA, ECC) e l'evoluzione verso il post-quantum crittografia [16 ore] - Soluzioni integrate per rilevamento di anomalie / intrusioni [8 ore] - Esempi di applicazione della sicurezza embedded (hardware digitale e livelli SW di basso livello) all'IoT e case study automobilistici [3 ore] Sicurezza hardware considerando gli aspetti tecnologici [32 ore]: - Correlazioni tra problemi di sicurezza e safety in HW [5 ore]. - Tecnologie e architetture per l'archiviazione sicura di dati/chiavi, HW trojans e HW counterfieting [8 ore] - Tendenze tecnologiche per la generazione su chip di dati casuali, funzioni fisicamente non clonabili (PUF), generazione di numeri casuali HW (ad es. TRNG) [8 ore] - Attacchi di cybersecurity “side-channel” a livello fisico [8 ore] - Esempi di applicazione della sicurezza HW considerando aspetti tecnologici per IoT, Automotive o Case study in Industria 4.0 [3 ore]

Bibliografia e materiale didattico

testo
J. Szefer, “Principles of Secure Processor Architecture Design”, Morgan & Claypool publisher, 2018
Materiale fornito dal docente (slides, appunti,..)

Indicazioni per non frequentanti

Possibilità di accedere al materiale didattico e alle registrazioni delle lezioni su canale TEAMS del corso

Modalità d'esame

Esame orale (con almeno 1 domanda per ciascuna delle 2 parti) piu discussione della relaizone di un progettino assegnato a gruppi di studenti (e.g. 1 o 2 studenti per gruppo) dal docente durante il corso

Ultimo aggiornamento 29/07/2022 10:37