



SAPIENZA
UNIVERSITÀ DI ROMA

***Effetti dell'hardware nella valutazione di
funzioni di sicurezza comunque
realizzate (HW, FW, SW)***

Dipartimento di Ingegneria Elettronica (DIE)

Università di Roma "La Sapienza"

Relatore

Prof. Alessandro Trifiletti

Dottorando

Francesco Trotta

Ambito di ricerca

- Attacchi a funzioni di sicurezza basati su vulnerabilità dell'hardware (*hardware attacks*) che supporta la loro realizzazione e relative contromisure
 - Anticipazione tramite *studio/simulazione*
 - Verifica in *laboratorio*
- Alcuni attacchi all'hardware (*side channel attacks*) si basano su osservazione del comportamento fisico del dispositivo che realizza la funzione di sicurezza

Side Channel Attacks(I)

- Categoria di attacchi che, utilizzando varie tecniche di inferenza statistica, producono una stima del valore dei segreti utilizzati in una funzione di sicurezza sulla base dell'osservazione di grandezze fisiche (p.es., inferenza sulla chiave di un cifrario a blocchi a partire dalla potenza consumata dal dispositivo)

Side Channel Attacks(II)

- Esempi di grandezze fisiche osservabili (la cui misurazione produce *tracce*)
 - Potenza dissipata (*power attacks*)
 - Potenza irradiata (*electromagnetic attacks*)
 - Tempo di esecuzione (*timing attacks*)
- Esempi di tecniche di inferenza statistica (basate su opportune collezioni di tracce)
 - Analisi differenziale
 - Analisi a correlazione

Laboratorio

- Tra le attività principali: Sperimentazione degli attacchi di interesse in laboratorio opportunamente attrezzato (parzialmente disponibile al DIE)
 - Hardware standard (p.es., Oscilloscopio, Schede di acquisizione, ...)
 - Hardware dedicato (p.es., Schede di test, ...)
 - Software standard (p.es., *LabVIEW*, ...)
 - Software dedicato (p.es., Driver per Schede di test/acquisizione dati, ...)

Alcune attività rilevanti

- Tecniche per l'osservazione congiunta di grandezze fisiche rilevanti (p.es., potenza consumata e irradiata)
- Tecniche convenienti per la misura delle grandezze di interesse (p.es., misura di potenza irradiata con dispositivo all'interno di una gabbia di Faraday)



SAPIENZA
UNIVERSITÀ DI ROMA

Grazie per l'attenzione!