PAINE23 - Workshop

Embedded System Security Assurance: Unveiling Vulnerabilities through Side-Channel Analysis and Fault Injection

eShard

Embedded System Security Assurance: Unveiling Vulnerabilities through Side-Channel Analysis and Fault Injection

Abstract: Join our PAINE workshop for a deep dive into embedded system security assurance. Through the lens of side-channel analysis and strategic fault injection, unravel the intricacies of chips: smartcards, microcontrollers, SoCs and FPGA. Through guided and practical Jupyter notebooks, we'll explore a systematic methodology for acquisition, alteration, analysis and interpretation of chip activities to gain insight and discover vulnerabilities. Applied on multiple implementations of the AES-128 cryptographic primitive (full software vs. hardware assisted vs. full hardware), the techniques and tools extend beyond the presented use-cases.

Note: No software download nor installation is required for the present workshop.

However, for those who are interested, the possibility to explore the tool used for the presented investigations can be offered. A free cloud instance can be set for two weeks.
Side Channel Attacks content and traces as well as tutorials will be shared.
Contact fabien.bouffard@eshard.com