Advanced Hardware Attacks: Side Channel Analysis, Fault Injection and Their Countermeasures (3 days)

Course Description

This 3-days course takes you through Side-Channel Power Analysis, Fault Injection Attacks and their countermeasures on embedded systems. This course concentrates on embedded systems such as found in many IoT devices, automotive, military and industrial. Such systems contain microcontrollers, microprocessors, ASSPs and FPGAs.

Results of such attacks include recovering encryption keys with DPA, bypassing security checks, bypassing password checks, and more. Students leave the course with the most up-to-date knowledge of the attacks and their countermeasures.

Side-Channel Power Analysis - that freaky method of extracting secret keys from embedded systems that doesn't rely on exploits or coding errors. It can be used to read out an AES-128 key in less than 60 seconds from a standard implementation on a small microcontroller. Are your products vulnerable to such an attack?

Fault Injection Attacks - can you even trust your hardware? This training will cover fault injection attacks (also known as glitch attacks) on embedded systems. These attacks allow you to entirely bypass security mechanisms, dump memory over communication interfaces, and wreak havoc for fun and profit.

Countermeasures - Understanding how to implement advanced attacks is only one side of the story.

This extended version of the training includes additional training material on software and hardware countermeasures against Side Channel Analysis and Fault Injection Attacks.

Easy to grasp examples example vulnerable implementations are discussed along with industry best practices to counter and mitigate the advanced hardware attacks that were discussed during the first part of the training.

During the three-day course, topics covered will include: theory behind side-channel power analysis (SPA, DPA, CPA, TVLA), measuring power in existing systems, understanding leakage detection, Fault Injection techniques, and their countermeasures.

Course Duration

3 days

Intended Users

The course is suited for both Software and Hardware Engineers. However, it is recommended that students should have a general background in embedded design or minimum hardware knowledge.

Previous Knowledge

None

Course Material

Slides & Documentation used during the class (not open source, non-distributable)

Class Outline

Day #1

- What is Advanced Hardware Hacking, What Can We Attack?
- Side Channel Analysis
- Power Analysis Attacks Theory
- Simple Power Analysis (SPA)
- Leakage Detection

Day #2

- Differential Power Analysis (DPA)
- Correlation Power Analysis (CPA)
- Introduction to Fault Injection Attacks
- Clock Glitching
- Voltage Glitching
- Laser Fault Injection
- Electromagnetic Fault Injection

Day #3

- Introduction to SW / HW Countermeasures
- Side Channel Analysis SW Countermeasures
- Side Channel Analysis HAW Countermeasures
- Fault Injection SW Countermeasures
- Fault Injection HW Countermeasures
- What's Next