HandsOnSecurity

Advanced Hardware Attacks with the ChipWhisperer® Hands-On Side Channel Analysis, Fault Injection and Their Countermeasures (4 days)

Course Description

This 4-days course takes you through Side-Channel Power Analysis, and Fault Injection Attacks and their countermeasures on embedded systems (32-bit Arm Cortex M3/M4 as well as 8-bit XMEGA). This course concentrates on low-level embedded systems such as found in many IoT devices, as well as boot ROM and similar code. However, the techniques are directly applicable to other microcontrollers/Microprocessors and even FPGAs.

Results of such attacks include recovering encryption keys with DPA, bypassing security checks, bypassing password checks, and more. Students leave the course with a ChipWhisperer setup they keep, meaning they can continue to experiment with the provided material, and then apply it to their own targets after the course has completed.

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? This course is loaded with hands-on examples to teach you not only about the attacks and theories, but how to apply them.

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 with the ChipWhisperer® 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 demonstrated during the first part of the training.

The course uses the open-source ChipWhisperer project (www.chipwhisperer.com) for both hardware & software tools, meaning attendees can immediately take the knowledge learned in this course and apply it in real life. The course includes a ChipWhisperer-Lite or Nano, so students walk away with the hands-on hardware used during the lab.

During the four-day course, topics covered will include: theory behind side-channel power analysis (SPA, DPA, CPA, TVLA), measuring power in existing systems, setting up the ChipWhisperer hardware & software, understanding leakage detection, the theory and practice of Fault Injection techniques, countermeasures, and analyzing your own hardware. Using many hands-on labs, students will use the ChipWhisperer hardware to walk through attacks on software AES, hardware AES, password checks, RSA, and more.

Side Channel Power Analysis & Fault Injection have never been more accessible and testing your products has never been this inexpensive or easy.

Course Duration

4 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

Students are expected to be familiar with both C and Python (in-depth experience is not required, but knowledge of general syntax and how to build programs in both).

Course Material

1. Hardware: ChipWhisperer Lite/Nano (kept by the participant once class is done)
2. Slides & Documentation used during the class (not open source, non-distributable)
3. VMWare image & Software Tools (all tools are open source, distributable)
4. Example capture traces (distributable)

What Students Should Bring

Students MUST bring a laptop with approximately 32GB of free space. A variety of (Python-based) tools will be installed and used, which can run on Linux & Windows. To simplify the class, a VMWare image will be provided which has all tools installed, but students are free to directly install the tools on their own computer.

Students are encouraged to bring a computer with VMWare Workstation or VirtualBox already installed to reduce setup time. They can alternatively install ChipWhisperer® directly on their system.

Class Outline

Day #1

- **What is Advanced Hardware Hacking, What Can We Attack?**
- **Side Channel Analysis**
- **Introduction to the ChipWhisperer® Platform**
- **Power Analysis Attacks Theory**
- **Simple Power Analysis (SPA)**

❖ **Hands-On Labs**

- Firmware Build Setup
- Instruction Differences
- Password Bypass
- Breaking RSA
- Measuring Signal-to-Noise Ratio of Target
- Timing Analysis with Power for Password Bypass

Day #2

- **Leakage Detection**
- **Differential Power Analysis (DPA)**
- **Correlation Power Analysis (CPA)**

❖ **Hands-On Labs**

  - ○ Hamming Weight Measurement
  - ○ Large-Hamming Weight Swings
  - ○ Performing TVLA Testing for Crypto Validation
  - ○ using ChipWhisperer Analyzer for Correlation Power Analysis Attack
  - ○ Manual Correlation Power Analysis Attack
  - ○ Resynchronization Data Traces
  - ○ Attacking 32-bit AES

Day #3

- **Introduction to Fault Injection Attacks**
- **Clock Glitching**
- **Voltage Glitching**
- **Laser Fault Injection**
- **Electromagnetic Fault Injection**

❖ **Hands-On Labs**

  - ○ Clock Glitch Attacks
  - ○ Vcc Glitch Attacks
  - ○ Glitch Buffer Attacks
  - ○ AES Differential Fault Analysis Attack
  - ○ RSA Fault Attack

Day #4

- 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