HandsOnSecurity

Advanced Hardware Hacking with the ChipWhisperer

Course Description

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.

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 along with a UFO target board, 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, measuring power in existing systems, setting up the ChipWhisperer hardware & software, several demonstrated attacks and labs, understanding leakage detection, and analyzing your own hardware.

The training also includes updated hardware so we can target ARM devices, alongside hardware AES peripherals, and demonstrations of bootloader and lock bit attacks.

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

Course Duration

4 days

Intended Users

This course is aimed at anyone who has previously designed or reverse-engineered embedded systems. General embedded design experience is assumed - students should be familiar with UARTs, bootloaders, bus interfaces, use of microcontroller peripherals, etc. The course does not require any specific knowledge but the course content will be most valuable to someone experienced in this area.

The course targets low-level embedded systems - such as 8-bit, 16-bit, and 32-bit microcontrollers (including ARM and PowerPC). The hands-on portions will use an ARM device but the techniques are directly applicable to other microcontrollers. These techniques are most useful when attacking systems running bare-metal or a RTOS, which could include for example the bootloader mode on an automotive MCU.

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
2. Course book (including labs)
3. Students MUST bring a laptop with approximately 15GB of free space
4. VMWare image will be provided which has all tools installed

Table of Contents

Day #1-2

- **Introduction**
  - Introduction to hardware hacking
  - Software setup
  - What is “Advanced Hardware Hacking”

- **Introduction to Glitch Attacks**
  - Glitch attacks
  - Finding vulnerable parameters
  - ❖ **LAB #1: Glitch Attacks with Clock Glitching for Password Bypass**
  - ❖ **LAB #2: Glitch Attacks for Memory Dumping**

- **Finding Glitch Timing with Power Analysis**
  - Introduction to power analysis
  - ❖ **LAB #3: Finding Bootloader Lockbit Location using Power Analysis**

- **Bypassing Device Security Lockbits**
  - Introduction to device memory lockbits
  - Examples of memory lockbit types
  - ❖ **LAB #4: Bypassing Memory Lockbits using Power Analysis**

- **EM Fault Injection**
  - Introduction to EM fault injection
  - DEMO: EM fault injection platform

- **Differential Fault Analysis (DFA)**
  - Introduction to DFA
  - ❖ **LAB #5: DFA of AES**

- **Testing Real Devices**
  - Lab setup
  - Connecting to real targets
  - Finding fault injection parameters
  - Communications interfaces

Day #3-4

- **Simple Power Analysis & Finding Leakage**
  - Introduction to Simple Power Analysis (SPA)
  - **LAB #6: SPA for Password Bypass**

- **Differential Power Analysis & Leakage Detection**
  - DPA attacks on AES-128
  - Finding leakage
  - **LAB #7: AES-128 Attack**
  - **LAB #8: Finding Leakage**

- **AES-256 Bootloader Challenge**
  - Introduction to AES-256 bootloader
  - **LAB #9: AES-256 Bootloader Challenge**

- **Leakage Detection**
  - Introduction to Leakage Detection
  - **LAB #10: T-Test for Validating Devices Security**

- **Testing Real Devices**
  - Lab setup
  - Connecting to real targets
  - Introduction to attacks beyond 8-bit devices
  - Attacking hardware cryptography
  - **LAB #11: 32-bit ARM T-Table Implementation**
  - **LAB #12: Attacking Hardware Cryptography**