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, and also how to mitigate them with various techniques.

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 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, 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, 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

Any software or hardware engineer can attend this training. No hardware background is required!

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/Microprocessors.

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
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

- Power & Noise
- Dealing with noise
- Signal Noise Ratio (SNR)
- Using SCA to Attack Cryptography
- Power Analysis in Real-Life
- ChipWhisperer Capture Setup
- Synchronized vs Non-Synchronized Clock
- Advantages of Synchronous Sampling

❖ **Lab #3: Power Acquisition Basics: Measuring SNR of Target**

- What is Simple Power Analysis (SPA)?
- SPA Attack Requirements
- SPA as Pattern Recognition
- Examples
- RSA Refresher
- Using SPA to break RSA

❖ **Lab #4: Simple Power Analysis for Password Bypass**

- What is Differential Power Analysis (DPA)?
- DPA Attack Requirements
- A Typical DPA Attack Flow (MGPC)
- AEA Refresher
- Attacking AES with DPA
- DPA Tips & Tricks

❖ **Lab #5: DPA: Hamming Weight Measurement**

❖ **Lab #6: DPA: Large Hardware Swings**

❖ **Lab #7: DPA: AES Attack**

- What is Correlation Power Analysis (CPA)?
- CPA Attack Requirements
- CPA Attack Example

❖ **Lab #8: CPA: Using ChipWhisperer**

❖ **Lab #9: CPA: Manual Attack**

❖ **Lab #10: CPA; Resynchronizing Data Traces**

❖ **Lab #11: CPA: Attacking AES on 32-bit MCU**

- Power Analysis Mitigation Overview
- Power Analysis Mitigation Strategy
- Approached to Mitigate Power Analysis

- Implementing Power Analysis Mitigation
- Mitigation Tradeoff
- Chip-Level Mitigations
- Program-Level Mitigations
- SCA Attacks & Mitigation Assessment
- Evaluation Methods
- GSR and TVLA
- ❖ **Lab #12: Test Vector Leakage Assessment for Crypto Validation**

Day #3-4

- **Module III – Advanced Side Channel Attacks**
  - Bootloader AES 256 Attack
  - Template Attacks
  - ❖ **Lab #13: Breaking AES-256 Bootloader**
  - ❖ **Lab #14: Template Attacks with Hardware Assumption**

- **Module IV - Fault Injection**
  - What is Fault Injection?
  - Fault Injection Attack Requirements
  - Fault Injection Techniques
  - What is Glitching Attack?
  - Implication of Glitching on Security
  - Advantages of Glitching Attacks
  - Effective Glitching Attacks
  - Fault Injection Attack Workflow
  - Voltage Glitching Attacks
  - How Do Voltage Glitching Attacks Work?
  - Voltage Glitching Setup
  - How Voltage Glitching is Generated
  - Clock Glitching Attacks
  - How Clock Glitching is Generated
  - ChipWhisperer ADC Clock Setup
  - ❖ **Lab #15: Introduction to Clock Clock Glitch Attacks**
  - ❖ **Lab #16: Introduction to Vcc Glitching Attacks**
  - ❖ **Lab #17: Glitch Buffer Attacks**
  - ❖ **Lab #18: AES Differential Fault Analysis Attacks**

❖ **Lab #19: RSA Fault Attack**

- Fault Injection Mitigation
- Fault Tolerance
- Passive Tamper Detection
- Active Tamper Detection

- What Next?
- Developing Your Own Attacks with th ChipWhisperer