



Hands-On Hardware Hacking and Reverse Engineering Two Day Agenda

Document Revision: 1.4

Last updated: February 17, 2011

(Times for each section are approximate)

1. Introduction to Hardware Hacking (1 hour)

- 1.1. What is Hardware Hacking and Reverse Engineering?
- 1.2. Hardware Hacking Methodology: How to Approach the Problem
- 1.3. Legal Issues
- 1.4. Hack Examples

2. Tools of the Warranty Voiding Trade (0.5 hours)

- 2.1. Basic Tools
- 2.2. General Hardware Hacking
- 2.3. Advanced Projects

3. Electrical Engineering Fundamentals (1 hour)

- 3.1. Voltage, Current, and Resistance
- 3.2. Basic Device Theory

4. Soldering and Desoldering (1.5 hours)

- 4.1. Hands-on: Through-hole devices
- 4.2. Hands-on: Surface mount devices

5. Schematics and Circuit Boards (1 hour)

- 5.1. Reading and Drawing Schematics
- 5.2. Printed Circuit Boards (PCBs)
- 5.3. Design Tools
- 5.4. Modifying Circuit Boards
 - 5.4.1. Hands-on: Trace cutting

6. Embedded Security (0.5 hours)

- 6.1. General Security Concepts
- 6.2. Hardware Security Myths and Common Problems
- 6.3. Types of Attacks and Attackers
- 6.4. Goals of an Attack
- 6.5. Anti-Tamper Mechanisms

7. Opening Product Housings (0.25 hours)

- 7.1. The Basics
- 7.2. Security Bits and One-Way Screws
- 7.3. Epoxy Encapsulation Removal

8. Hardware Reverse Engineering (3 hours)

- 8.1. Component Identification and Package Marking Information
- 8.2. Finding Data Sheets
- 8.3. Probing Boards and Tracing Signals
 - 8.3.1. Design-for-Manufacturability and Test
 - 8.3.2. Hands-on: Experiments with the Multimeter
 - 8.3.3. Hands-on: Learning to use the Parallax USB Oscilloscope

9. Memory and Programmable Logic (1 hour)

- 9.1. General Concepts and Security Issues
- 9.2. Hands-On: Reading Serial EEPROM devices

10. External Interfaces (0.5 hours)

- 10.1. General External Interfaces
- 10.2. JTAG (IEEE 1149.1)
- 10.3. Backdoors

11. Advanced Techniques (0.5 hours)

- 11.1. Emissions and Side-Channel Attacks
- 11.2. Chip Decapping and Die Analysis

12. Hands-On Hardware Hacking Challenge (Remaining time)

In this challenge, the students apply the knowledge they've learned throughout the course to defeat the security mechanisms of a custom-designed circuit board.