Hands-On Hardware Hacking and Reverse Engineering Training Course Agenda

Last updated: February 20, 2017

This two-day course teaches hardware hacking and reverse engineering techniques commonly used against electronic products and embedded systems. It provides students with the resources and skills they need to confidently approach hardware hacking and to come up with creative solutions for their own particular engagements. No prior electronics experience is required. Additional information is available at www.grandideastudio.com/portfolio/hardware-hacking-training/.

A. Hardware Hacking Overview

B. Information Gathering

C. Product Teardown

1. Opening housings
2. Anti-tamper mechanisms
   2.1. Defeating encapsulation
   2.2. Hands-on exercise: Epoxy removal
3. Component identification
   3.1. Discrete components
   3.2. Integrated circuits
   3.3. Finding and reading data sheets
4. Schematics and PCBs (Printed Circuit Boards)
   4.1. Creating and reading schematics
   4.2. PCB construction/fabrication
   4.3. Hands-on exercise: PCB modifications
   4.4. PCB deconstruction techniques

D. Soldering and Desoldering

1. Tips/techniques
2. Hands-on exercise: Soldering
3. Hands-on exercise: Desoldering
4. How to work with difficult package types

E. Buses and Interfaces

1. Identifying interfaces
2. Determining pin function
    2.1. Hands-on exercise: Initial measurements w/ multimeter
3. Hands-on exercise: Create a block diagram of target system
4. Signal monitoring/analysis
    4.1. Tools/techniques
    4.2. Hands-on exercise: Signal monitoring w/ logic analyzer
    4.3. Serial/UART interfaces
    4.4. Hands-on exercise: Digital decoding w/ logic analyzer
    4.5. Wireless/RF overview

F. Signal/Data Manipulation

1. Tools/techniques
2. Debug interfaces
    2.1. Vendor-specific
    2.2. JTAG (IEEE 1149.1)
3. Glitching/fault injection

G. Memory and Firmware

1. Memory types/technologies
2. Retrieving contents from memory
    2.1. Hands-on exercise: Data extraction/modification
3. Security considerations
4. Firmware analysis/disassembly

H. Other Attack Vectors

I. Hardware Hacking Challenge

Apply the knowledge and skills learned in the course to reverse engineer and defeat the security mechanism of a custom electronic product.