

Hands-On Hardware Hacking

Designed for O'Reilly's Maker Faire

Copyright © 2006 Grand Idea Studio, Inc.
All Rights Reserved

Document Revision: 1.1
Last updated: April 12, 2006

Class Syllabus

Abstract

Hardware hacking. Mods. Tweaks. Though the terminology is new, the concepts are not: A gearhead in the 1950s adding a custom paint job and turbo-charged engine to his Chevy Fleetline, a '70s teen converting his ordinary bedroom into a "disco palace of love," complete with strobe lights and a high-fidelity eight-track system, or a technogeek today bypassing the cryptographic authentication routines of the Microsoft Xbox to allow him to play homebrew games written by hobbyists. Building on an existing idea to create something better. Making products do things they were never intended to do. Reverse engineering products to defeat protection and security mechanisms. These types of self-expression can be found throughout recorded history.

This workshop, designed specifically for O'Reilly's Maker Faire, consists of lecture and hand-on laboratory components, each lasting 90 minutes. We'll guide you through an introduction to hardware hacking, explore the basic electronics fundamentals, and then dive into the step-by-step processes of successful circuit modifications and hardware hacking. Whether you're a beginner hobbyist with no electronics experience or a self-proclaimed "gadget geek," you're sure to learn something. And, you'll most definitely have fun in the process.

Learning Objectives

- Understand the mindset of a hardware hacker and why he does what he does
- Familiarity with basic electronic components and theories
- Become confident that you can open a piece of hardware without breaking it (and maybe how to fix it if you do!)
- Solder and assemble your own electronic game (with components and a circuit board provided in kit form)

Materials

Each student will be presented with the following resources to be used throughout the workshop:

- Electronics measurement tools, including a multimeter and soldering iron
- Safety equipment
- All other necessary tools, components, and circuit boards

Following completion of the workshop, each student will leave with a custom electronic game that they built on their own (using components and a circuit board provided in kit form).

Instructor Biography

Joe Grand is the President of Grand Idea Studio, Inc., a San Diego-based product research, development, and licensing firm, where he specializes in the design of consumer electronics, video game accessories, and toys. An avid inventor and hardware hacker, Joe has been creating and modifying electronics since he was seven years old. He is the author of the books *Hardware Hacking: Have Fun While Voiding Your Warranty* and *Game Console Hacking*, and is on the technical advisory board of *MAKE Magazine*.

Joe is also a globally recognized figure in computer security. He has testified before the United States Senate Governmental Affairs Committee and is a former member of the legendary hacker collective L0pht Heavy Industries. Joe holds a Bachelor of Science degree in Computer Engineering from Boston University. You may reach him at joe@grandideastudio.com.

Part I: Lecture

1. Introduction to Hardware Hacking

- 1.1. Hacker v. Attacker
- 1.2. What are Hardware Hacking and Reverse Engineering?
- 1.3. A Brief History of Hardware Hacking
- 1.4. Challenges and Trends
- 1.5. Hardware Hacking Methodology: How to Approach the Problem
- 1.6. Examples of Interesting Hacks

2. Tools of the Warranty Voiding Trade

- 2.1. The Essential Tools
- 2.2. Basic Hardware Hacking
- 2.3. Advanced Projects and Reverse Engineering
- 2.4. Tools Provided in this Course

3. Electrical Engineering Fundamentals

- 3.1. Bits, Bytes, and Nibbles
- 3.2. Voltage, Current, and Resistance
 - 3.2.1. Voltage
 - 3.2.2. Current
 - 3.2.3. Power
 - 3.2.4. Direct Current (DC) and Alternating Current (AC)
 - 3.2.5. Resistance
 - 3.2.6. Ohm's Law
- 3.3. Basic Device Theory
 - 3.3.1. Switches
 - 3.3.2. Resistors and Potentiometers
 - 3.3.3. Capacitors
 - 3.3.4. Inductors
 - 3.3.5. Diodes and LEDs
 - 3.3.6. Transistors
 - 3.3.7. Integrated Circuits (ICs)
 - 3.3.8. Digital Logic
 - 3.3.9. Microcontrollers
 - 3.3.10. Memory (RAM, ROM, EEPROM, Flash)
 - 3.3.11. Programmable Logic (ASICs, FPGAs)
- 3.4. Reading and Drawing Schematics
 - 3.4.1. Reading Schematics
 - 3.4.2. Common Schematic Symbols
 - 3.4.3. Package Marking Information

Part II: Lab

4. Opening Products

- 4.1. The Basics
- 4.2. Step-by-Step
- 4.3. Security Bits and One-Way Screws
- 4.4. Identifying Components

5. Building and Modifying Circuits

- 5.1. Prototyping and Breadboarding
- 5.2. Custom Printed Circuit Boards

6. Hands-on Exercises

- 6.1. Cutting a Trace
- 6.2. Soldering (Thru-Hole)
- 6.3. Desoldering (Thru-Hole)
- 6.4. Building Your Own Electronic Game