Introduction to Hardware Hacking

Scott Fullam
Why Hardware Hacking?

• Hardware Hacking does not seem to get near the publicity as computer hacking
• I’d like to change reputation of hacking, hardware in particular
Hardware Hack: A Definition

• A (sometimes) clever modification or fix made to a piece of equipment that improves its performance or makes the equipment do something for which it was not originally designed.
  – The results of the hack need not be ‘useful’ in the strict sense of the word.
• The word ‘hack’ can be used as a noun or a verb.
  – Noun: “That hack you made to your toaster was great!”
  – Verb “Let’s hack your brothers TV set tonight to only tune in channel 13!”
Why is Hardware Hacking Easier than Software Hacking?

- When you buy a piece of hardware, let's say a toaster for example, you can open it up and see what is inside and see how it works.
  - Repair manuals available for many pieces of equipment
  - Your GF/SO can benefit from your hardware skills!
    - You can fix stuff in the house
    - When was the last time your GF/SO asked you to fix their copy of MS Word?
- When you buy a piece of commercial software, you cannot open it up to see how it works.
  - You are stuck with the executable file only and no source code that shows the inner workings
  - Its behavior is fixed to that which the original programmer intended.
  - You cannot examine it and change how it works.
  - Open Source software is the exception to this
About Me

• Graduated in 1990 with MS and BS in EECS from MIT
• Have been hacking since I was a kid
• Have held many interesting jobs:
  – Toy Designer
  – Digital Camera Architect
  – Startup Founder (PocketScience Inc)
  – Writer (My book)
My Book

- “Hardware Hacking Projects for Geeks”
  - Published by O’Reilly
  - Started the book 2 years ago

- Gathered together a number of hacks I put together along with a few cool ones that I found
Talk Overview

- EE Basics
  - Basic Electronic Components and what they do
- Cracking the case
  - How to open up electronics enclosures without destroying it
- Building Circuits
  - Reading schematic diagrams
  - Bread boarding
  - Soldering equipment and techniques
- Where to Get Parts
  - Online sources
  - Offline sources
- Project Walk-Throughs
  - Hacked Toaster
  - Electric Beer Mug
  - LED Flashlight conversion
- Large Scale Hack Description
  - Blinkenlights
EE Basics

• Passive and Active Parts
  – Passive Parts
    • Resistors
    • Capacitors
    • Inductors
    • Transformers
  – Active Parts
    • Transistors
    • Diodes
    • Integrated Circuits
EE Basics Cont.

- **Resistors**
  - Limits (or Resists) the flow of electrical current
  - Value of resistor measured in Ohms
  - Voltage (V), Current (I), and Resistance (R) follows the equation \( V = I \times R \).
  - An example of how a resistor can be used
    - Current limiter for LED
    - LEDs can be burned out if too much current is allowed to pass through them. If an LED is connected to a directly battery with no current limit, the LED will stop working. Add a resistor in series to limit the current to the LED to fix this problem.
EE Basics Cont.

- Capacitors
  - Stores electrical energy in the form of an electric field
  - Act like small batteries
  - Value of capacitor measured in Farads: (after Michael Farady)
  - Voltage, Current, Capacitance follow this equation: \( I = C \frac{dv}{dt} \)
  - Are sometimes polarized (they have a ‘plus’ side and a ‘minus’ side)
  - Are often used to filter noisy circuits
    - Most circuits will place many capacitors across their power supplies to decrease overall noise
EE Basics Cont.

- **Inductors**
  - Stores energy in the form of a magnetic field
  - Values specified in Henries
  - Voltage (V), Current (I), and Inductance (L) follow this equation: \( V = L \frac{di}{dt} \)
  - Often used to filter out Radio Frequency (RF) Interference
  - Used extensively in power supplies
EE Basics cont.

- Transformers
- Couples energy from one side to the other via magnetic field
- The turns ratio determines the ratio of AC voltage
- Used to isolate signals
  - A signal from one side is transferred to the other without a common ground
- Used to ‘step up’ a voltage
  - Can be used to generate large voltages
EE Basics Cont

- **Active Components**
  - Transistors
    - Act as a switch
    - Two basic types
      - BiPolar
      - Metal Oxide Semiconductor (MOS)
  - Diodes
    - One way gate
    - Light Emitting Diode
  - Integrated Circuits
    - Made from many transistors
EE Basics Cont

- Transistors
  - Electronic Switches
  - Two basic types
    - Bi-Polar
      - Current Controlled Current Switch
        - Two ‘flavors’
          - NPN
          - PNP
        - Three terminals:
          - Emitter
          - Base
          - Collector
    - MOS (Metal Oxide Semiconductor)
      - Voltage Controlled Current Switch
        - Two ‘flavors’
          - P-Channel
          - N-Channel
        - Three Terminals
          - Drain
          - Gate
          - Source
Diodes

- One way current switch
  - Three common types
    - Standard
    - Schottkey
    - Zener
  - Each has a ‘plus’ side and a ‘minus’ side
  - The side with the line on it is the ‘minus’ side
  - Current is conducted from the plus side to the minus side
  - Forward Voltage Drop of 0.6V and above

- Light Emitting Diode
  - Forward Voltage Drop of 1.7V and above
  - Available in many colors
  - Each has a ‘plus’ side and an ‘minus’ side
  - The ‘minus’ side often has a flat spot
EE Basics cont

- How to read the numbers on an IC package
- Look for manufacturers logo
- Look at first part of numeric string on part
  - Numbers and letters after the ‘dash’ are often speed grades and production date codes
- Look up numbers on the web
EE Basics Cont

Here are a few examples of well known chip companies:

- Fairchild Semiconductor
- Maxim
- Philips
- Samsung
- Toshiba
Cracking the Case

• How can you open an enclosure without destroying it?
  – Have the right tools
    • Lots of Small Screwdrivers
    • Philips and flat head
  – Know how most enclosures are fastened together.
    • Fasteners
      – Screws
      – Plastic snaps molded into the case
      – Glue
      – Double Sided Tape
Cracking the Case cont.

- **Hardware Hacking is like surgery!**
  - You wouldn’t want your doctor using an axe to perform an appendectomy… Good Tools
  - Get high quality hardened steel tools
    - The cheap stuff breaks and strips the heads off the screws
  - Torx drivers
    - Star shaped head
    - Many consumer electronics cases now use these
  - Hex Drivers
    - Hexagon shaped head
    - Also popular in consumer electronics
  - Tweezers
    - Useful for fishing out dropped screws from inside cases
    - Flat end can be used as a pry bar
  - Dental Picks
  - Razor Blades
    - I prefer Xacto style with handles
  - Collecting the tools can be an obsession of its own
    - Be the envy of the other hardware hackers by having the latest German hardened steel drivers
Cracking the Case cont.

- **Common case fasteners**
  - Screws
  - Plastic snaps molded into case
  - Glue
  - Double Sided Tape
    - The Palm V case is held together this way. You need a hair dryer to heat up the tape so that it releases to open it
- **Screws are often placed so that they cannot be seen**
  - On the bottom of the product
  - Under labels
  - Under the ‘feet’ of the product
Cracking the Case cont.

- Good ways to open up the case
  - Clear a table top
  - Place sheets of white paper under the items to be opened
    - You can see dropped screws better on the white paper
  - Make sure power has been removed from the device being taken down
    - Unplug it
    - Remove all batteries
  - Carefully remove all of the screws you can find
    - Make sure to look under all labels and feet
    - Take another piece of paper and sketch a rough outline of the case on it.
    - After each screw is removed, tape it to the diagram in its approximate location.
      - This makes it a lot easier to put them all back when you are done
Cracking the Case cont.

- Look for seams and gently pull at them
  - Don’t force it.
  - Use tweezers or a pick to open up a crack along the seam
  - Pull the two halves and feel for any resistance
    - Anywhere there is resistance, look for a screw that was not removed
    - Look for a plastic snap and pry it apart with the back of the tweezers
- Once the electronics are exposed, be careful not damage them with static electricity
  - Use a commercial static wrist strap that is plugged into a Ground point
  - If no commercial static wrist strap is available frequently touch the screw that holds the power outlet to the wall
    - Better yet, attach a wire to this screw and attach the other end of the wire to your wrist by stripping 8” of the insulation and wrapping the exposed wire around your wrist
    - Do _not_ plug the wire into any of the outlet holes.
Building Circuits

- Reading Schematic Diagrams
- Breadboarding
  - Try out the circuit before soldering
- Soldering
  - Irons
    - Lab bench style
    - Portable
    - Cordless
      - Electric
      - Gas
  - Solder
  - Perf Board
  - Tools
Building Circuits cont.

- The basics of reading a schematic diagram
Building Circuit cont.

- **Bread-boarding**
  - Utilizes a plug board and 24 gauge solid core wire
  - A way to build a circuit without soldering
  - Useful for small circuits
  - Not useful for high frequency circuits (No RF)
Building Circuits cont.

- Soldering
  - Iron
    - Electric Irons
    - Butane Irons
  - Solder
    - Tin/Lead
    - Lead Free
    - Silver
    - Tip Cleaner
      - Sponge
      - Copper sponge
  - Flux
    - Cleans surfaces to be soldered
      - Helps solder to ‘stick’
    - Rosin
    - Water Soluble
    - No Clean
  - Solder Remover
    - Solder Wick
    - Solder Sucker
Building Circuit cont

• Perf Board
  – Fiberglass board with evenly spaced metal plated holes
  – Used to build more permanent circuits

• Tools
  – Wire Strippers
  – Wire
  – Wire cutters
  – Needle Nose Pliers
Where to Get Parts

• On Line
  – Digikey: www.digikey.com
  – Mouser: www.mouser.com
  – Jameco: www.jameco.com
  – American Science and Surplus: www.sciplus.com
  – Halted on line: www.hsc.com

• Off Line
  – Frys
  – Radio Shack
  – Halted Specialties
Project Walk Throughs

- Toaster
- Beer Mug
- LED Flashlight
Toaster

- Read about Weather Toaster from a design student in the UK
  - Toaster would toast picture of the days weather on your bread in the morning
  - Thought his design was too complicated
  - Wanted to replicate the idea with less work
  - Made design trade offs
- Hacked together the basic concept in a weekend
Toaster Insides

- I modified the toasting element wiring and added a mask inside for the toasting patterns.
Self Chilling Beer Glass

- I had an extra Pentium III cooling system on hand (from some overclocking experiments)
- I wanted to keep my drink cool
- The Self Chilling Drinking Mug was born
Self Chilling Beer Mug cont.

- Need to use a metal mug
- Powered from either a 12V cigarette lighter outlet or a PC power supply
Self Chilling Beer Mug Cont

- Here are some other view of the mug
LED Flashlight

- Convert Standard flashlight to LED Flashlight
LED Flashlight cont.

- A 3 or more cell flashlight is easy to convert
- Only the bulb need be converted
BlinkenLights

- An 8 story building is turned into a giant display
- Hack developed and put on by the Chaos Computer Club of Germany
- Each window in the building is a pixel
  - An individually controlled halogen lamp is placed in front of each window
  - Over 5,000 meters of Cat5 cable is used
- The system is controlled by a Linux PC with a 192 channel parallel I/O card
- Photos courtesy of the Chaos Computer Club in Germany
Blinkenlights
Blinkenlights
BlinkenLights
A Renaissance in Hacking!

- Hardware Hacking is Easy and Fun!
- It is akin to recycling
  -- Old equipment gets reused
- You can learn something while doing it
  -- The process of deconstruction is educational
- Be careful when hacking anything that is plugged into the wall or has powerful motors in it
  -- Unplug/deactivate the equipment first
- Go Home today and Hack something!
My Garage Hacking Space

- Old Table
- Two Channel Scope
- Parts Bins
- Lots of Power Outlets
- Lots of junk to salvage parts from
- Soldering iron and tools
- Hand tools
- Desk Lamp
- Magnifying headset
Questions and Demos