Hardware Hacking, Tweaking, and Bending: Making Technology Do Things It Was Never Intended To Do

University of Advancing Technology
November 2, 2005

Joe Grand
Grand Idea Studio, Inc.
joe@grandideastudio.com
Introduction to Hardware Hacking

- Hacker v. Attacker
- What is Hardware Hacking and Reverse Engineering?
- Legal Issues
- A Brief History of Hardware Hacking
- Challenges and Trends
- Examples of Interesting Hacks
Hacker v. Attacker

- Hacker: Somebody involved in the exploration of technology
- Attacker: Malicious goals of theft or illegitimately breaking into a system
- Terms often confused and hyped (intentionally?) by media
- Contrary to popular belief, hacking does not have to be illegal
What is Hardware Hacking?

- Doing something with a piece of hardware that has never been done before
  - Personalization and customization (e.g., "hot rodding for geeks")
  - Adding functionality
  - Capacity or performance increase
  - Defeating protection and security mechanisms (not for profit)
- Creating something extraordinary
- Harming nobody in the process
What is Hardware Hacking? 2

- Some attempts at defining "hack":
  - The MIT Gallery of Hacks (Building Hacking), http://hacks.mit.edu/Hacks/Gallery.html

- It's a noun and a verb!
  - Noun: "That Furby hack was really cool."
  - Verb: "Let's hack the Atari Flashback 2 to play actual game cartridges."
What is Reverse Engineering?

- The art of learning from practical examples
- Examining products or technologies to see how they work
  - Ex.: Opening a product and creating a schematic based on the circuit board layout
- Often a subset of hardware hacking
Why Hardware Hacking?

- Curiosity and fun
  - To see how things work
- Improvement and innovation
  - Make products better/cooler (build a better mousetrap)
  - Some products are sold to you intentionally limited or "crippled"
- Education
  - Learn by doing
- Grass-roots technology development
  - Sow a thousand seeds and see what blooms
Why Hardware Hacking? 2

- **Consumer protection**
  - I don't trust glossy marketing brochures...do you?
- **Security competency**
  - Test hardware security schemes and look for failures/weaknesses
  - People generally trust hardware devices as "secure"
- **Good for the environment?**
  - Old/obsolete hardware gets reused instead of brought to the landfill
Legal Issues

- I am not a lawyer!

- Thin line between good and evil
  - Recent laws (DMCA) have worked to prevent reverse engineering by enabling large corporations to flex their muscle against potential threats
  - However, there is legal precedent that explicitly protects certain types of reverse engineering

- "Shrink wrap" or explicit agreements used to waive your rights
  - Ex.: You don't actually own what you're reverse engineering
Legal Issues 2

- Reverse engineering a patented product does not grant you a license to use it
  - Patents contain a full disclosure of the technology, anyway
- Cannot copy or use a copyrighted work
- Trade secrets (confidential, but not legally protected) are fair game
- Check with a lawyer if you have any questions!
A Brief History of Hardware Hacking

- Hacking is not just about breaking and tweaking - it's also about creating!
- Arguably dates back 200 years
  - Charles Babbage's Difference Engine (early 1800s)
  - William Crooke's discovery of the electron (mid 1800s)
- Hardware hackers you might have heard of:
  - Benjamin Franklin, Thomas Edison, Alexander Graham Bell, Bill Hewlett and Dave Packard, Steve(s) Jobs and Wozniak
- Early hardware hacking included:
  - Wireless telegraphy, vacuum tubes, radio, television, transistors, computers
The Technology Divide

- Differential between mass production and hobbyist capabilities
The Technology Divide 2

- Differential between mass production and hobbyist capabilities

Advent of integrated circuits

Advent of FPGAs, rapid prototyping
The Technology Divide 3

- Differential between mass production and hobbyist capabilities

Diagram:
- Advent of integrated circuits
- Advent of FPGAs, rapid prototyping
- Slowing of Moore’s Law (exaggerated)
- Further advances (FIBs, cheap protos)
- Reducing technology gap
Evolution of the Technology Divide

- In the beginning (1940s-1960s)
  - Production and hobbyist technology the same
  - Your own two eyes, a soldering iron, and some discrete components

Evolution of the Technology Divide 2

- ICs lead the way to greater integration (1970s-1980s)

Picture: [Applefritter.com](http://www.applefritter.com/pictures/images/apple1platine.jpg)
In the 1970s-1980s, most boards used SSI/MSI chips:
- SSI (Small Scale Integration) = <10 gates
- MSI (Medium Scale Integration) = 10-100 gates
- LSI (Large Scale Integration) = 100-1000 gates
- VLSI (Very Large Scale Integration) = >10000 gates

At SSI and MSI level, most logic functions visible to the "naked eye"
Evolution of the Technology Divide 4

- Early 1990s
  - Mass-market adoption of technology drives integration
  - Fine-pitch surface mount technology, increasing integration, and escalating clock speeds
  - Hardware hacking stagnates as interest in software/network hacking increases
  - Hardware hacking now requires high-end test equipment, microscopes, soldering irons
Evolution of the Technology Divide 5

- **Late 1990s**
  - BGA technology widely deployed
    - Die connections ("pins") located underneath device package
    - Working with BGAs inaccessible to hobbyists
    - Requires sophisticated soldering and rework equipment
    - Inspection and repairing of ball/solder joints expensive
  - High board clock speeds obsolete cheap test equipment
    - Low-cost oscilloscopes have ~100 MHz bandwidth
    - Motherboards hit 133 MHz signaling in late 1990s (now over 400 MHz!)
Evolution of the Technology Divide 6

- Early 1990s v. Late 1990s: Do more with less!
Evolution of the Technology Divide 7

- Cross section of modern circuit board showing hidden BGA connections and buried traces

Picture: Hacking the Xbox
Hardware Hacking Challenges

- Advances in chip packaging
  - Ultra-fine pitch and chip-scale packaging (e.g., BGA, COB, CIB)
  - Not as easy to access pins/connections to probe
  - Discrete components can now easily be inhaled

- Highly-integrated chips (sub-micron)
  - Difficult, but not impossible, to probe and modify
  - Building a full-custom chip as a hobby project is still too expensive (> $100K)
Hardware Hacking Challenges 2

- **Cost of equipment**
  - Advanced tools still beyond the reach of average hobbyist (probing, decapping, SEMs, etc.)
  - "State of the art" defined by what hackers can find in the trash and at flea markets

- **Societal pressures**
  - Hardware hacking is practically becoming mainstream, but "hacker" is still a naughty word
Emerging Trends

- Economic downturn of early 2000 is a blessing to hardware hackers
  - Growth of technology slows down
  - Price competition bring rapid PCB prototyping prices into the < $100 range
  - Excess inventory drives down component costs
  - IC analysis services become affordable for the mere mortal
Emerging Trends 2

- Hardware hacking is making a comeback!
  - Was overshadowed for many years by network/software programming and hacking
  - Many resources, web sites, forums, magazines, people available to learn from
Make Magazine

- Full-color, quarterly hybrid magazine/book (also known as a *mook*) published by O'Reilly
- Launched January 2005, already 80,000 paid subscribers
- Focused on all aspects of the do-it-yourself ethos
  - Electronics, Mechanical, Metal, Wood Working, Food, Anything!
- Community-based sharing of hacks, projects, pictures
  - [http://www.makezine.com](http://www.makezine.com)
  - [http://flickr.com/groups/make/pool](http://flickr.com/groups/make/pool)
Even the media likes it!
- "It's the kind of magazine that would impress MacGyver" -- Marcus Chan, San Francisco Chronicle
- "This is Popular Mechanics for the modern age with a 1968 James Brown attitude." -- Wayne Bedsoe, Knoxville News Sentinel
- "If you're the type who views the warnings not to pry open your computer as more a challenge than admonition, MAKE is for you." -- Rolling Stone
Hacks!

- Case Modifications
- Game Consoles
- Consumer Products
- Other Technologies
- ...Only a tiny sampling of the thousands of amazing hacks out there (and the ones I think are particularly cool)!
Case Mods: Atari 2600PC

- Fully-featured PC designed into the case of an Atari 2600 (remember those?)
- Wanted a DVD/CD media station and all-purpose video game/computer emulator
- 1GHz VIA EPIA M10000 motherboard, 512MB DRAM, 60GB hard drive, CD-RW/DVD combo drive, wireless keyboard and mouse, 802.11b wireless USB adapter, 2 Stelladaptor Atari controller-to-USB interfaces
Case Mods: Atari 2600PC 2

- Game Console Hacking and Make issue 2
Case Mods: Millennium Falcon Xbox

- Stripped down Xbox retrofitted into an original 1979 Star Wars Millennium Falcon
  - www.darkops.co.uk

- Xbox w/ 4 gamepad ports, 6 fan "hyper drive" cooling system, concealed DVD drive
Game Consoles: Retro/Classic

- Thriving homebrew game development community
  - Ex.: www.atariage.com

- Primarily driven by nostalgia and the desire to use old technology to create new things

- Excellent way to learn about electronics and programming
  - The challenge is in overcoming constraints of these early systems (ex.: limited ROM, RAM, and processor power, necessary low-level hardware interaction, etc.)
Game Consoles: Retro/Classic 2

- Custom circuit boards to build actual cartridges for retro systems (Atari 2600, Atari 5200, Atari 8-bit, Colecovision)
  - www.pixelspast.com
Disabling the Nintendo NES "Lockout Chip"

- Security mechanisms used by Nintendo to maintain exclusivity on cartridge manufacturing and to control game distribution
- Lockout chip inside the NES communicates with an identical chip inside the cartridge (e.g., as a "lock" and "key")
- Can be disabled with a simple trace cut and additional wire
- Hack allows foreign games and unlicensed third-party games to be played on the console
- *Game Console Hacking*, chapter 7
Game Consoles: Retro/Classic 4

- Cut this pin
- Jumper
Game Consoles: Xbox

- Andrew "bunnie" Huang's Xbox hacking
  - Custom-built tap circuit used to intercept data transfer over Xbox's HyperTransport bus
  - Able to retrieve symmetric encryption key used for protection of a secret boot loader
  - Allowed him to execute untrusted/unauthorized code on the system
Game Consoles: Xbox 2

- Tap board uses single LVDS-to-CMOS logic converter (TI SN75LVDS386) interfaced to a Xilinx Virtex-E FPGA
Game Consoles: Gran Turismo 4 Steering Wheel Mount

- Woodworking skills > Paying $ for expensive gaming chair
  - $18 in parts + time + fun v. $199
  - http://berserk.org/gt4
Game Consoles: Pong Mechanik

- Art project created by Niklas Roy
  - Interviewed in Make issue 1
- Completely mechanical version of Pong: Motors, relays, solenoids, strings, & pulleys!
  - www.cyberniklas.de/pongmechanik/indexen.html
- No microprocessors, semiconductors, or other electronic components
Consumer: VaxBar

- Built in January 2001
- Simple access control system to prevent unauthorized employees from eating our snacks!
- Original DEC VAX 11/785 housing w/ custom-designed Java-based web server and iButton authentication
Consumer: Universal Garage Door Opener

- Replaced DIP switches with timer and counter to automatically cycle through all $2^{10}$ (1024) possible combinations.
- Built in July 1994 as a hobbyist project.
  - **Still** works on many garage door types that use a selectable "security code".
  - Who changes their garage door systems that often?
Consumer: Dakota Single-Use Digital Camera

- One of the few low-cost, single-use digital cameras (~$10.99 at Ritz or Wolf Camera)
- Intended to be used like a disposable camera
  - Sticker on unit says "Camera does not connect to home computers."
- Quickly hacked to convert to regular, multi-use camera via USB
  - [http://cexx.org/dakota](http://cexx.org/dakota)
- Underground community has created custom firmware, image dumping software, webcam, etc.
Consumer: Dakota Single-Use Digital Camera 2

Pictures: Make, issue 3
Consumer: VCR Cat Feeder

- "Liberate a motor from an old VHS deck, attach it to a food chopper, and program the deck's recording timer to fill Fluffy's bowl on schedule."  
  - http://makezine.com/03/catfeeder

- Any old VCR has a programmable timer that connects to a motor for recording TV shows
- Hack the VCR so the motor operates a food delivery mechanism instead of the video head
- One of many curiously insane hacks created by James Larsson (he's also created a clock by measuring decay rates of a prawn sandwich)
Consumer: VCR Cat Feeder 2

Pictures: Make, issue 3
Wireless:
Dell TrueMobile 1184

- One of many broadband access point/routers
- Port scan reveals open ports 80, 333, 1863, 1864, 4443, 5190, 5566
- Device based on vLinux distribution
  - www.onsoftwarei.com/product_vlinux.htm
  - *Hardware Hacking: Have Fun While Voiding Your Warranty*, chapter 10
Wireless: Dell TrueMobile 1184 2

- Can `telnet` into port 333 with default password to gain complete control of the device
  - username: root, password: admin
- No special hardware tools or reprogramming is necessary
- Many devices running Linux which can make hacking/experimentation easier
  - www.linuxdevices.com
  - www.ucdot.org
- Linksys WRT54G is another good one for hacking: Open source firmware, etc.
Wireless: Can Antenna (Cantenna)

- What better way than to use your empty Pringles can or coffee can as a WiFi antenna?  
  - www.turnpoint.net/wireless/has.html
- Perfect for increasing network range or for "wardriving"
- Many variations exist...
Other: Self-Chilling Beer Mug

- Keep drink cold wherever you go!
- Uses Peltier junction (moves heat to one side, leaving the other cold)
  - [www.popsci.com/popsci/automotivetec h/59ca1196aeb84010vgnvcm1000004eeceb ccdrcrd.html](http://www.popsci.com/popsci/automotivetec h/59ca1196aeb84010vgnvcm1000004eeceb ccdrcrd.html)

Pictures: Scott Fullam, DefCon 12
Other: Blinkenlights

- Eight floors of a building turned into a huge interactive display
  - 144 lamps behind front windows
  - Each lamp computer-controlled to form 18x8 pixel monochrome matrix
  - Linux PC w/ 192-channel Parallel I/O card
    - [www.blinkenlights.de](http://www.blinkenlights.de)

- Created by the Chaos Computer Club to celebrate its 20th anniversary (Sept. 2001)

- Followed up by the "Arcade" project in Paris 2002
  - 20x26 pixel greyscale matrix
  - Play Tetris, Pong, Breakout, Pac Man, etc.
Other: Blinkenlights 2

Pictures: Chaos Computer Club
Other: Anonymous Megaphone

- "Bring anonymous voices into public spaces, stage an anonymous protest, or speak to the masses without revealing your identity."
  - [http://makezine.com/04/diy_megaphone/](http://makezine.com/04/diy_megaphone/)

- Cellphone (auto answer) -> Audio amplifier -> Paper cone

Picture: Make, issue 4
Other: Joe's Random Hacks

- Laser Listener: Window Vibration Audio Reconstruction Project (left)
- Joystick-Controlled Pneumatic Cannon (right)
Other: Technology as Artwork

- Lichtenberg Lightning Frame (left)
- Tank Searchlight Lamp (right)
Other: Technology as Artwork 2

- Solder Stencil End Table (left)
- Macintosh Aquarium (right)
Other: Technology as Artwork 3

- Hard Drive Coffee Table
Thanks & Have Fun!

Joe Grand
Grand Idea Studio, Inc.
joe@grandideastudio.com
Books and Magazines: Hardware Hacking

- Make Magazine (w/ blog updated daily), www.makezine.com
Books and Magazines: Hobbyist and Robotics

Books and Magazines: General Electrical Engineering

- Circuit Cellar Magazine, www.circuitcellar.com
Web Sites: Hardware Hacking

- hack a day, www.hackaday.com
- TiVo Techies, www.tivotechies.com
Web Sites: Electrical Engineering

- Parallax, Inc., www.parallax.com
- ePanorama.net, www.epanorama.net
- Discover Circuits, www.discovercircuits.com
Web Sites: Other

Distributors: Electrical Engineering

- Digi-Key, www.digikey.com
- Mouser, www.mouser.com
- Jameco, www.jameco.com
- Newark In One, www.newarkinone.com
- Future Electronics, www.futureelectronics.com
- Radio Shack, www.radioshack.com
Distributors: Tools and General Hardware

- Contact East/Jensen Tools, www.contacteast.com
- Test Equity, www.testequity.com
- The Home Depot, www.homedepot.com
- Lowe's, www.lowes.com
- Hobby Lobby, www.hobbylobby.com
- McMaster-Carr, www.mcmaster.com