

# **Tweaking, Bending, and Making: Stories of a Hardware Hacker**

**USENIX LISA**

**December 5, 2005**

**Joe Grand**

**Grand Idea Studio, Inc.**

**joe@grandideastudio.com**



# Brief Agenda

- Me
- Hacker v. Attacker
- What is Hardware Hacking and Reverse Engineering?
- Legal Issues
- MAKE Magazine
- Examples of Interesting Hacks



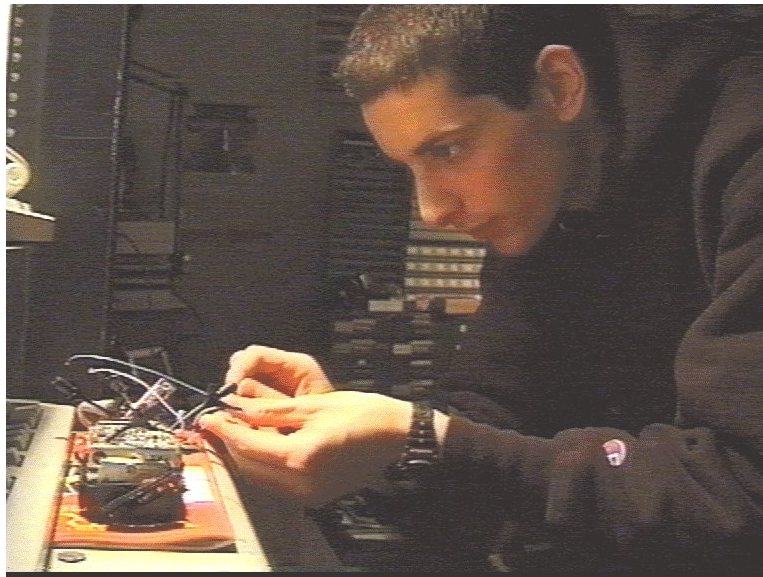
## Me (Joe)

- Been experimenting with computers and electronics since I was seven years old (1982)
- First system: Atari 400 w/ 830 Acoustic Coupler Modem
- Mostly self-taught through hands-on projects, magazines, and friends
- Formal education in EE from Boston University
- Now make a living developing new products and licensing my ideas



## Me (Joe) 2

- Obsessed inventor
- Professional hobbyist
- Mad scientist



Modifying a radio to decode mobile data terminal (MDT) information from police cars (circa 1997)



# 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 by media
- Contrary to popular belief, hacking does not have to be illegal



# A Brief History of Hardware Hacking

- 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



# 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 Jargon File v4.4.7, The Meaning of Hack, [www.catb.org/~esr/jargon/html/meaning-of-hack.html](http://www.catb.org/~esr/jargon/html/meaning-of-hack.html)
  - Dictionary.com, <http://dictionary.reference.com/search?q=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 (get your hands dirty!)



# 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

- 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 force you to waive your rights
  - Ex.: You don't actually **own** what you're reverse engineering
- I'm not a lawyer, so check with one if you have concerns



# 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, food, anything!
- Community-based sharing of hacks, projects, pictures
  - <http://www.makezine.com>
  - <http://flickr.com/groups/make/pool>



# MAKE Magazine 2

- 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 (Finally)!

- 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

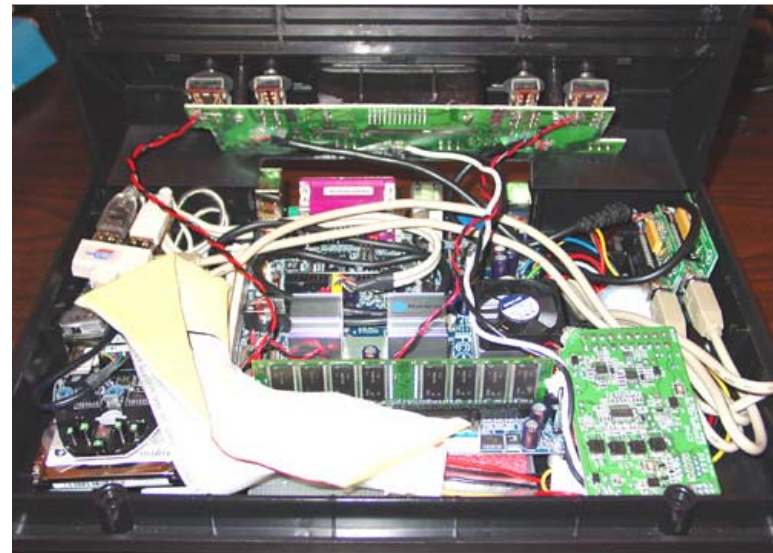
- Fully-featured PC designed into the case of an Atari 2600 (remember those?)
- Wanted a DVD/CD media station and all-purpose video game/computer emulator
- 1GHz VIA EPIA M10000 motherboard, 512MB DRAM, 60GB hard drive, CD-RW/DVD combo drive, wireless keyboard and mouse, 802.11b wireless USB adapter,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

- Disabling the Nintendo NES "Lockout Chip"
  - Patented security mechanism 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





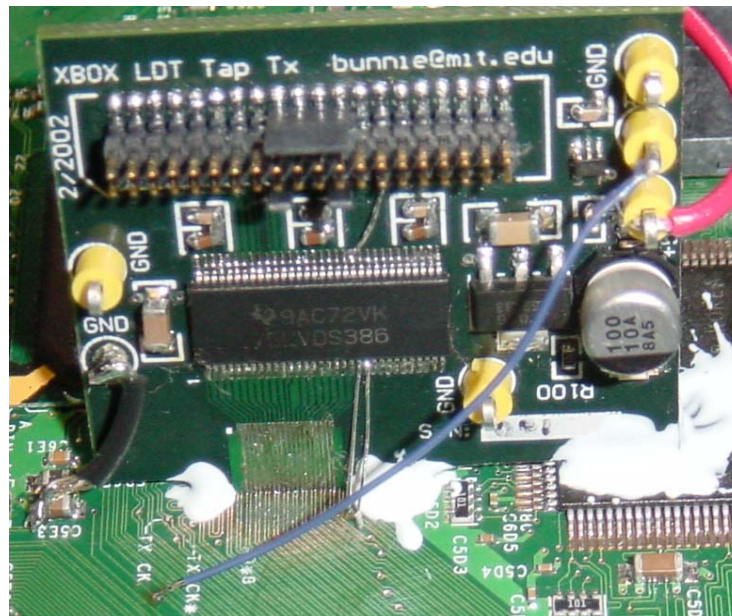
# Game Consoles: Xbox

- Andrew "bunnie" Huang's Xbox hacking
  - (He's up next!)
  - *Hacking the Xbox: An Introduction to Reverse Engineering* and [www.xenater.com/bunnie/proj/anatak/xboxmod.html](http://www.xenater.com/bunnie/proj/anatak/xboxmod.html)
  - 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

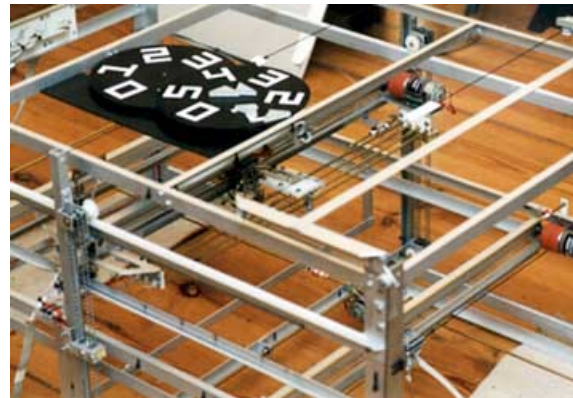


Picture: Hacking the Xbox



# Game Consoles: Pong Mechanik

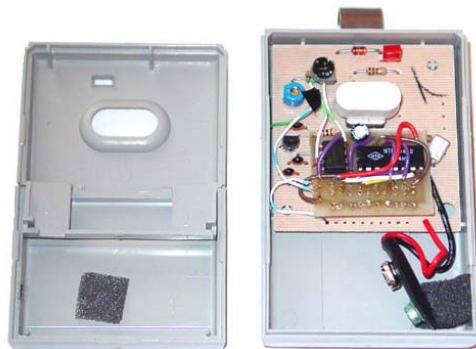
- Art project created by Niklas Roy
  - Interviewed in Make issue 1
- Completely mechanical version of Pong: Motors, relays, solenoids, strings, & pulleys!
  - [www.cyberniklas.de/pongmechanik/indexen.html](http://www.cyberniklas.de/pongmechanik/indexen.html)
- No microprocessors, semiconductors, or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





# 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>
- Underground community has created custom firmware, image dumping software, webcam, etc.



# Consumer: Dakota Single-Use Digital Camera 2

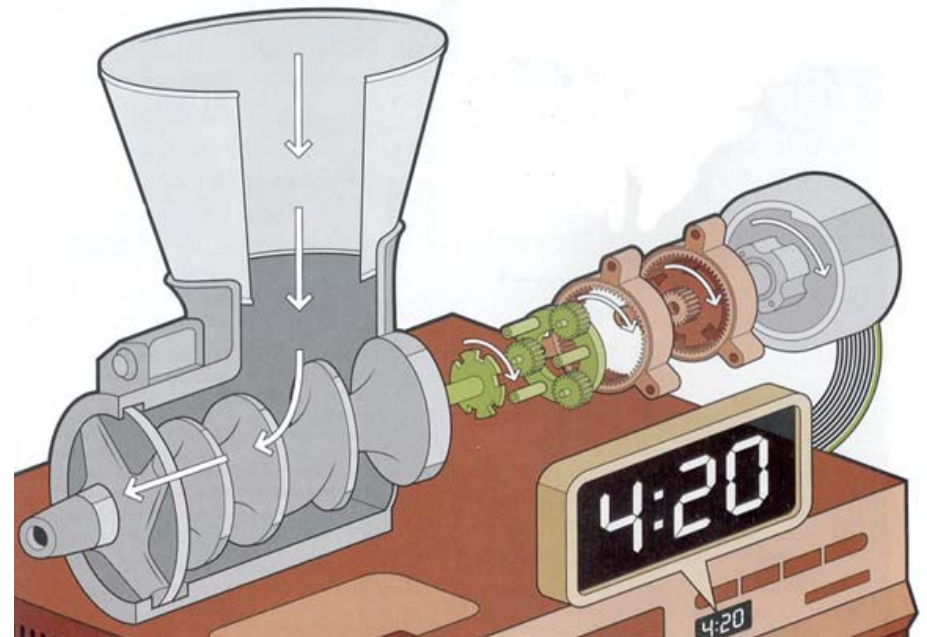


## Consumer: VCR Cat Feeder

- "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)



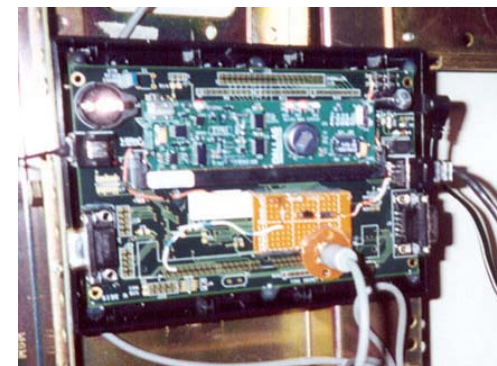
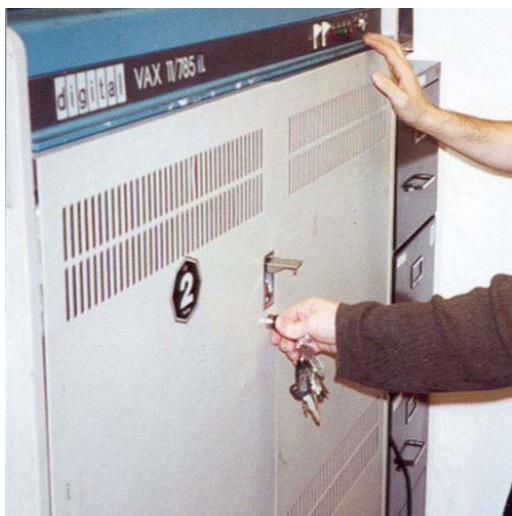
# Consumer: VCR Cat Feeder 2



Pictures: Make, issue 3

# 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

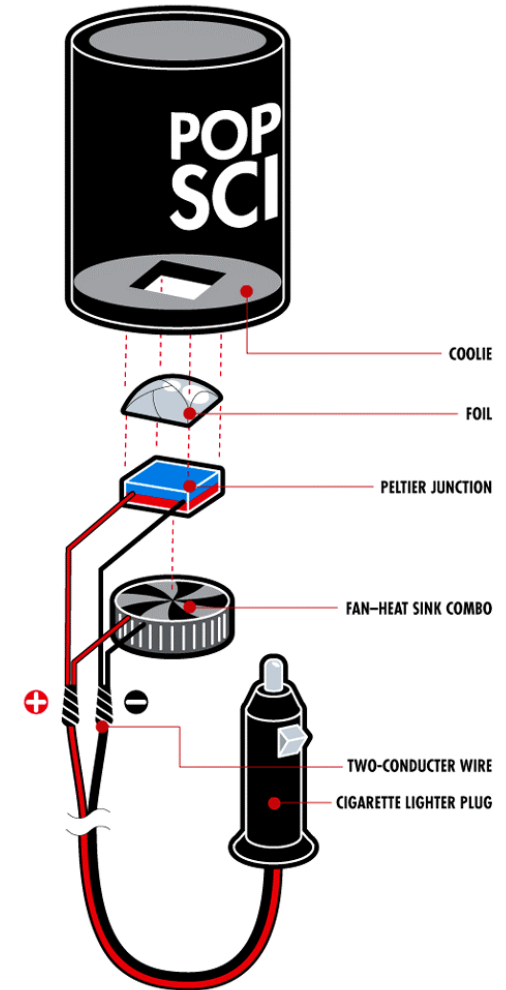


# Other: Self-Chilling Beer Mug

- Keep drink cold wherever you go!
- Uses Peltier junction (moves heat to one side, leaving the other cold)
  - [www.popsci.com/popsci/automotivetech/59ca1196aeb84010vgnvcm1000004eebccdrerd.html](http://www.popsci.com/popsci/automotivetech/59ca1196aeb84010vgnvcm1000004eebccdrerd.html)



Pictures: Scott Fullam, DefCon 12



© 2005 Grand Idea Studio, Inc.



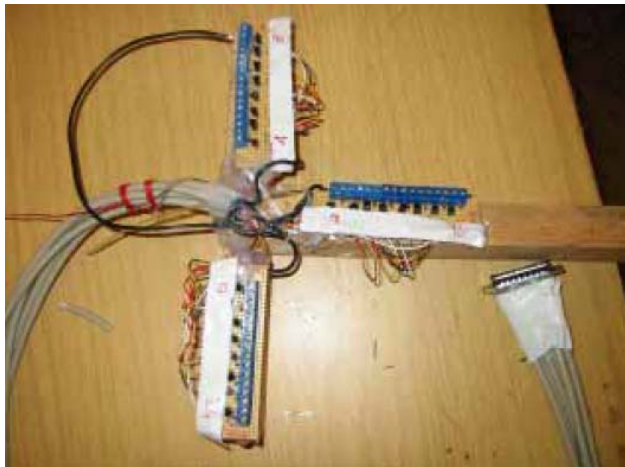
## Other: Blinkenlights

- 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.



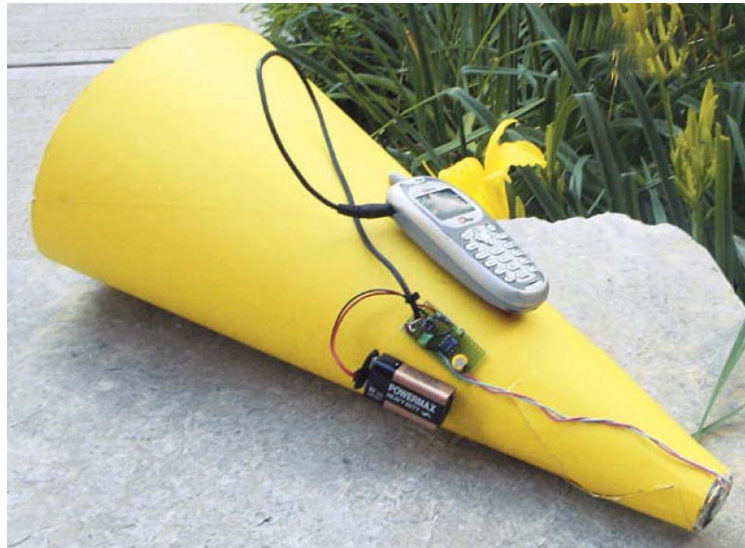


## Other: Blinkenlights 2



## 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: 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



# In Conclusion...

- Hardware hacking is making a comeback!
  - Was overshadowed for many years by network/software programming and hacking
  - Many resources, web sites, forums, magazines, and people available to learn from (see resources at the end of the presentation)
- Don't be afraid to break things and get your hands dirty!
- Have fun!



# Books and Magazines: Hardware Hacking

- Make Magazine (w/ blog updated daily), [www.makezine.com](http://www.makezine.com)
- J. Grand, et al, "Hardware Hacking: Have Fun While Voiding Your Warranty," Syngress Publishing, 2004, ISBN 1-93-226683-6.
- J. Grand, et al, "Game Console Hacking," Syngress Publishing, 2004, ISBN 1-93-183631-0.
- A. 'bunnie' Huang, "Hacking the Xbox: An Introduction to Reverse Engineering," No Starch Press, 2003, ISBN 1-59-327029-1.
- S. Fullam, "Hardware Hacking Projects for Geeks," O'Reilly Media, 2003, ISBN 0-59-600314-5.



# Books and Magazines: Hobbyist and Robotics

- Nuts & Volts Magazine, [www.nutsvolts.com](http://www.nutsvolts.com)
- Servo Magazine, [www.servomagazine.com](http://www.servomagazine.com)





# Books and Magazines: General Electrical Engineering

- Circuit Cellar Magazine, [www.circuitcellar.com](http://www.circuitcellar.com)
- EDN Magazine, [www.edn.com](http://www.edn.com)
- Horowitz and Hill, "The Art of Electronics," Cambridge University Press, 1989, ISBN 0-52-137095-7.
- K. Amdahl, "There Are No Electrons," Clearwater Publishing, 1991, ISBN 0-96-278159-2.
- M. M. Mano, "Digital Logic and Computer Design," Prentice-Hall, 1979, ISBN 0-13-214510-3.
- K. R. Fowler, "Electronic Instrument Design," Oxford University Press, 1996, ISBN 0-19-508371-7.



# Web Sites: Hardware Hacking

- hack a day, [www.hackaday.com](http://www.hackaday.com)
- I-Hacked.com: Taking Advantage of Technology, [www.i-hacked.com](http://www.i-hacked.com)
- Bill Miller's CircuitBending.com,  
<http://billtmiller.com/circuitbending>
- TiVo Techies, [www.tivotechies.com](http://www.tivotechies.com)



# Web Sites: Electrical Engineering

- Parallax, Inc., [www.parallax.com](http://www.parallax.com)
- ePanorama.net, [www.epanorama.net](http://www.epanorama.net)
- The EE Compendium: The Home of Electronic Engineering and Embedded Systems Programming, <http://ee.cleversoul.com>
- Discover Circuits, [www.discovercircuits.com](http://www.discovercircuits.com)
- WebEE: The Electrical Engineering Homepage, [www.web-ee.com](http://www.web-ee.com)
- University of Washington EE Circuits Archive, [www.ee.washington.edu/circuit\\_archive](http://www.ee.washington.edu/circuit_archive)



# Web Sites: Other

- Cambridge University Security Group - TAMPER Laboratory,  
[www.cl.cam.ac.uk/Research/Security/tamper](http://www.cl.cam.ac.uk/Research/Security/tamper)
- Molecular Expressions: Chip Shots Gallery,  
<http://microscopy.fsu.edu/chipshots/index.html>



# Distributors: Electrical Engineering

- Digi-Key, [www.digikey.com](http://www.digikey.com)
- Mouser, [www.mouser.com](http://www.mouser.com)
- Jameco, [www.jameco.com](http://www.jameco.com)
- Newark In One, [www.newarkinone.com](http://www.newarkinone.com)
- Future Electronics, [www.futureelectronics.com](http://www.futureelectronics.com)
- Radio Shack, [www.radioshack.com](http://www.radioshack.com)
- American Science & Surplus, [www.sciplus.com](http://www.sciplus.com)



# Distributors: Tools and General Hardware

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



**Thanks!**

**Joe Grand**

**Grand Idea Studio, Inc.**

**joe@grandideastudio.com**

