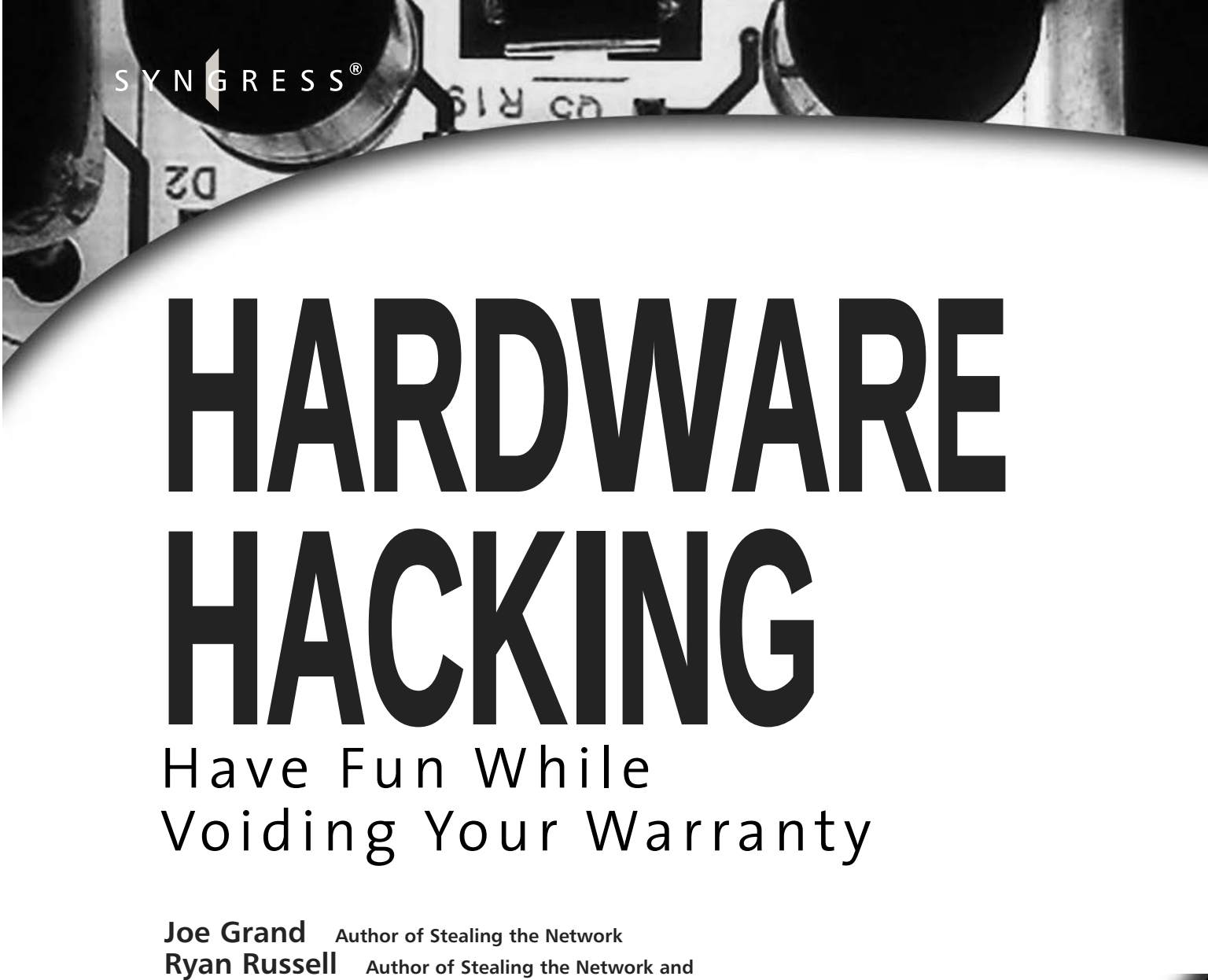
HARDWARE HACKING

Have Fun While Voiding Your Warranty

SYNGRESS®



SYNGRESS®

HARDWARE HACKING

Have Fun While Voiding Your Warranty

Joe Grand Author of Stealing the Network
Ryan Russell Author of Stealing the Network and Hack Proofing Your Network, Second Edition

And featuring Kevin D. Mitnick Technical Reviewer

Foreword by Andrew "bunnie" Huang

Lee Barken **Marcus R. Brown** **Job de Haas** **Deborah Kaplan**
Bobby Kinstle **Tom Owad** **Albert Yarusso**

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	B7NMW3V9KM
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Hardware Hacking: Have Fun While Voiding Your Warranty

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0
ISBN: 1-932266-83-6

Technical Editor: Joe Grand
Technical Reviewer: Kevin D. Mitnick
Acquisitions Editor: Catherine B. Nolan
Page Layout and Art: Patricia Lupien
Cover Designer: Michael Kavish
Copy Editor: Darlene Bordwell
Indexer: J. Edmund Rush
Editorial Assistant: Michael Rubin

Distributed by O'Reilly & Associates in the United States and Jaguar Book Group in Canada.

Acknowledgments

We would like to acknowledge the following people for their kindness and support in making this book possible.

To Jeff Moss and Ping Look of Black Hat for being great friends and supporters of Syngress.

A special thanks to Kevin Mitnick for sharing his invaluable expertise and knowledge, and to Darci Wood for her support of this book and the Syngress publishing program.

Syngress books are now distributed in the United States by O'Reilly & Associates, Inc. The enthusiasm and work ethic at ORA is incredible and we would like to thank everyone there for their time and effort in bringing Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Lynn Schwartz, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Valerie Dow, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, and Mark Jacobsen.

The incredibly hard working team at Elsevier Science, including Jonathan Bunkell, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, and Rosie Moss for making certain that our vision remains worldwide in scope.

David Buckland, Wendi Wong, Daniel Loh, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, and Joseph Chan of STP Distributors for the enthusiasm with which they receive our books.

Kwon Sung June at Acorn Publishing for his support.

Jackie Gross, Gayle Voycey, Alexia Penny, Anik Robitaille, Craig Siddall, Darlene Morrow, Iolanda Miller, Jane Mackay, and Marie Skelly at Jackie Gross & Associates for all their help and enthusiasm representing our product in Canada.

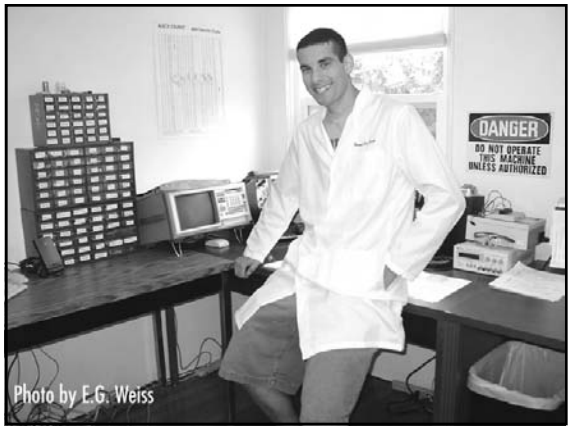
Lois Fraser, Connie McMenemy, Shannon Russell, and the rest of the great folks at Jaguar Book Group for their help with distribution of Syngress books in Canada.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Geoff Ebbs, Hedley Partis, Bec Lowe, and Mark Langley of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji Tonga, Solomon Islands, and the Cook Islands.

Winston Lim of Global Publishing for his help and support with distribution of Syngress books in the Philippines.

To all the folks at Malloy who have made things easy for us and especially to Beth Drake and Joe Upton.

Technical Editor & Contributor



Joe Grand; Grand Idea Studio, Inc. Joe Grand is the President and CEO of Grand Idea Studio, a product design and development firm that brings unique inventions to market through intellectual property licensing. Many of his creations, including consumer electronics, medical products, video games and toys, are sold worldwide.

A recognized name in computer security and electrical engineering, Joe's pioneering research on product design and analysis, mobile devices, and digital forensics is published in various industry journals. He is a co-author of *Hack Proofing Your Network, Second Edition* (Syngress Publishing, ISBN 1-928994-70-9) and *Stealing The Network: How to Own the Box* (Syngress, ISBN 1-931836-87-6).

Joe has testified before the United States Senate Governmental Affairs Committee on the state of government and homeland computer security, and is a former member of the legendary hacker think-tank, L0pht Heavy Industries. He has presented his work at numerous academic, industry, and private forums, including the United States Naval Post Graduate School Center for INFOSEC Studies and Research, the United States Air Force Office of Special Investigations, the USENIX Security Symposium, and the IBM Thomas J. Watson Research Center. Joe holds a BSCE from Boston University.

Joe is the author of Chapter 1 "Tools of the Warranty Voiding Trade," Chapter 2 "Electric Engineering Basics," Chapter 3 "Declawing Your CueCat," and Chapter 13 "Upgrading Memory on Palm Devices."

Contributors

Lee Barken (CISSP, CCNA, MCP, CPA) is the co-director of the Strategic Technologies and Research (STAR) Center at San Diego State University. He has worked as an IT consultant and network security specialist for Ernst & Young's Information Technology Risk Management (ITRM) practice and KPMG's Risk and Advisory Services (RAS) practice. Lee is the co-founder of the San Diego Wireless Users Group and writes and speaks on the topic of wireless LAN technology and security. He is the technical editor for *Mobile Business Advisor Magazine*, and the author of *How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN* (ISBN: 0-13-140206-4).

"Let's be grateful for those who give us happiness; they are the charming gardeners who make our soul bloom." —Marcel Proust

With deepest appreciation for my charming gardeners, a special thank you to my love Stephanie, my mom and dad, Frieda and Israel, my brothers, Derren and Martin, my sister Randi and her husband Scott, my Uncle Harry and my Grandmother Sophie. Thank you for your support and love.

Lee is the author of Chapter 10 "Wireless 802.11 Hacks."

Marcus R. Brown is a software engineer at Budcat Creations. His work includes writing low-level drivers and system-level programming such as resource management, file loading, and audio streaming. He is currently working on an unannounced title for the PlayStation 2 and Xbox. Marcus lives in Las Vegas, Nevada.

Marcus is the author of Chapter 9 "Hacking the PlayStation 2."

Job de Haas is Managing Director of ITSX BV, a Dutch company located in Amsterdam. ITSX BV provides security testing services in the broadest sense. Job is involved in testing, researching, and breaking security aspects of the latest technologies for corporate clients. In assignments for telecommunication operators and mobile phone manufacturers, Job gained experience with the internal operations of modern phones.

Job holds a master's degree in electrical engineering from Delft Technical University. He previously held positions at the Dutch Aerospace Agency (NLR) as a robotics researcher and at Digicash BV as a developer of cryptographic applications. He lives in Amsterdam, The Netherlands.

Job is the author of Chapter 12 "Can You Hear Me Now? Nokia 6210 Mobile Phone Modifications."

Deborah Kaplan (PCP) is an independent consultant focusing on revision control systems, system administration tools, release engineering, and open-source software. Deborah has developed enterprise-wide technology infrastructure, integrating telecommunications with heterogeneous Windows and UNIX environments. She specializes in building tools that automate repetitive tasks and monitor systems for performance tuning.

Deborah holds a bachelor's degree from Haverford College and a master's degree from Simmons.

Deborah is the author of Chapter 14 "Operating Systems Overview" and Chapter 15 "Coding 101."

Bobby Kinstle works in the Reliability Engineering department at Apple Computer, Inc. where he performs destructive simulations of extreme use and abuse of the products. His specialties are performing voltage and frequency margin analysis as well as detailed thermal performance studies. He also performs environmental testing, mechanical shock and vibration, and repetitive stress testing. Bobby also designed and built the lab's test network of over 600-switched Ethernet ports with 4-gigabit fiber optic backbones and NetBoot servers as well as the department data center. When projects are slow Bobby teaches Mac OS X Server training classes within the company.

Bobby is the author of Chapter 4 "Terabyte FireWire Hard Drive Case Mod" and a co-author of Chapter 5 "Macintosh Hacks."

Tom Owad is the owner and Web master of Applefritter, www.applefritter.com, a community where the artist and the engineer meet. Applefritter provides its members with discussion boards for the exchange of ideas and hosts countless member-contributed hardware hacks and other projects. Tom is pursuing a Bachelor's Degree in Computer Science and International Affairs from Lafayette College, Pennsylvania.

Tom is a co-author of Chapter 5 "Macintosh Hacks."

Ryan Russell has worked in the IT field for over 13 years, focusing on information security for the last seven. He was the primary author of *Hack Proofing Your Network, Second Edition* (Syngress Publishing, ISBN 1-928994-70-9) and *Stealing the Network: How to Own the Box*, Syngress Publishing (ISBN: 1-931836-87-6, and is a frequent technical editor for the Hack Proofing series of books. He is also a technical advisor to Syngress Publishing's *Snort 2.0 Intrusion Detection* (ISBN: 1-931836-74-4). Ryan founded the `vuln-dev` mailing list, and moderated it for three years under the alias "Blue Boar." He is a frequent lecturer at security conferences, and can often be found participating in security mailing lists and website discussions. Ryan is the Director of Software Engineering for AnchorIS.com, where he's developing the anti-worm product, Enforcer. One of Ryan's favorite activities is disassembling worms.

Ryan is the author of Chapter 6 "Home Theater PCs."

Albert Yarusso is a principle of Austin Systems (www.austinsystems.com), an Austin, Texas-based firm that specializes in web design programming and hosting services. Albert's background consists of a wide range of projects as a software developer, with his most recent experience focused in the game industry. Albert previously worked for Looking Glass Technologies and more recently for Ion Storm Austin, where he helped create the highly acclaimed PC game "Deus Ex."

Albert co-founded AtariAge (www.atariage.com) in 2001, a comprehensive website devoted to preserving the history of Atari's rich legacy of video game consoles and computers, which has become one of the busiest destinations on the web for classic gaming fans. In 2003, Albert helped bring the first annual Austin Gaming Expo (www.austingamingexpo.com) to Austin, an extremely successful event that drew over 2,000 visitors in its first year.

Albert is the author of Chapter 7 "Hack Your Atari 2600 and 7800," Chapter 8 "Hack Your Atari 5200 and 8-Bit Computer," and Chapter 11 "Hacking the iPod."

Foreword Contributor

Andrew "bunnie" Huang (PhD) is a staff engineer with Luxtera, and a part-time research staff with the California Institute of Technology. He also heads up a private consultancy firm, Xenatera LLC. bunnie is the author of *Hacking the Xbox*. bunnie has a broad background in electronics and firmware that comes in handy for various hardware hacking and reverse engineering projects. bunnie holds a PhD, M.Eng, and SB from the Massachusetts Institute of Technology, and is a member of the IEEE. He lives in San Diego, CA, with his fiancée, Nicole Justis.

Technical Reviewer

Kevin D. Mitnick is a security consultant to corporations worldwide and a cofounder of Defensive Thinking, a Las Vegas-based consulting firm (www.defensivethinking.com). He has testified before the Senate Committee on Governmental Affairs on the need for legislation to ensure the security of the government's information systems. His articles have appeared in major new magazines and trade journals, and he has appeared on Court TV, *Good Morning America*, *60 Minutes*, CNN's *Burden of Proof* and *Headline News*, and has been a keynote speaker at numerous industry events. He has also hosted a weekly radio show on KFI AM 640, Los Angeles. Kevin is also author of the best-selling book, *The Art of Deception: Controlling the Human Element of Security*.

Contents

Foreword

Hacking—and in particular, hardware hacking—has experienced a bit of a renaissance recently. I am personally quite pleased about the increased interest in hacking. Your interest in this book, *Hardware Hacking: Have Fun While Voiding Your Warranty*, is a testament to the increased demand for knowledge about hardware hacking. I'd like to take a few pages and a few minutes of your time to share with you why your interest in the topic makes me happy as a fellow hardware hacker.

First allow me to pontificate on the meaning of the word *hack*. The term has evolved quite dramatically over the years. Hacking has shaped technology perhaps as much as technology has shaped our perception of the hacker. According to *The New Hacker's Dictionary* (a public-domain lexicon of jargon created by hackers, www.jargon.8hz.com):

> hack: 1. /n./ Originally, a quick job that produces what is needed, but not well. 2. /n./ An incredibly good, and perhaps very time-consuming, piece of work that produces exactly what is needed. [1]

The second sense of the word is perhaps the closest to the definition I associate with the word *hack*. Thus, it follows that a hacker is one who labors to create good, typically innovative solutions to targeted problems. This book you are about to read was editted by a true hacker, Joe Grand, and it speaks mostly to the class of hacks that address the need to adapt and improve on existing consumer solutions.

As you can see, my view of hacking is a rather romantic and idealized one. I eschew the Hollywood stereotype of a hacker as a slovenly, socially maladept person with a bent for vengeance, data theft, or per-

haps a penchant to blithely play a game of deploy-the-nuke inside NORAD's computers. Although there are certainly such elements in today's hacker culture, I prefer to focus on promoting the more socially redeeming aspects of hacking. I believe that hacking is rooted in a desire to play with and understand technology, a modern manifestation of the values of exploration, passion, and hard work that date back to the first explorers and settlers of this country. Furthermore, hacking is a kind of grass-roots technology movement, in contrast to the kinds of technology movements that are forwarded by corporations and governments. As a result, hackers tend to play the part of proxy for the masses when it comes to sorting out the interplay of technology, society, and business. As technology continues to infuse our daily lives, it is becoming more important for society to bring its representatives to the technology direction table.

It is interesting and perhaps informative to see how hardware hacking has evolved over the years. In the early days of electronics, common hobbyists—hackers of sorts, but the term wasn't coined back then—could cobble together unique, useful, and sometimes outright impressive pieces of hardware that could match commercially available products in both performance and quality. In fact, some of the projects that hackers labored over in their garages went on to form the roots of today's technology.

Roll the calendar back to 1938: A young Bill Hewlett and Dave Packard get together and invent, in their garage, a high-quality piece of audio test equipment, the HP200A resistance-capacitance audio oscillator. Hewlett and Packard continued on to found the company we know today, and its rich history of engineer-friendly products helped forge the technology base we now enjoy. Most people are familiar with HP as a manufacturer of computers and printers, but HP's richest contributions to technology have been through enabling technologies, such as the tools engineers require to do their jobs. I myself use an HP48GX calculator, and I have an HP1650B logic analyzer on my desk, on top of my old HP8410C network analyzer.

Another well-recognized example of a company and technology with roots in the hacker community is Apple Computer. Roll back to 1976: Steve Wozniak debuts the Apple I at the Homebrew Computer Club in Palo Alto, California. The Apple I was designed over a period of years as a hobby machine, a true product of the hacking culture. Wozniak joined

forces with Steve Jobs, and the two went on to found the Apple Computer that brought us the Apple II and the now ubiquitous Macintosh computer.

The gritty grass-roots hacking culture in the early days of electronics technology served as a kind of incubator for innovation that has resulted in many of the products we enjoy today. Hewlett and Packard, Jobs and Wozniak are just two examples of the influence of the hacker spirit on our society. The basic values of hacking—creating a good thing that is exactly what is needed at a particular time—are a good match with innovation. Furthermore, hackers' independently motivated nature means that thousands of ideas are tested and built by hackers in the absence of venture capital or the risk constraints of investors. Hackers play an important part in the growth of technology, so I am always pleased to see a greater interest and awareness of hacking in the general public.

Recently, hacking has taken on more of a software-oriented bent. This is due in part to the steady pace of hardware improvement guaranteed by Moore's Law. Hardware hacking is a time-consuming labor of love, and it is discouraging to know that almost any hack you can think of to double a computer's performance will be obsolete within 12 months. It is much more rewarding to work in the instant-gratification world of software and let the performance of your programs ride the Moore's Law wave.

Another factor working against hardware hackers is the barrier of entry that was created by the higher levels of integration that naturally followed as a result of Moore's Law. The hackability of the desktop PC met a turning point in the evolution of the IBM PC-XT to the IBM PC-AT. The IBM PC-XT motherboard was chiefly composed of chips that were essentially naked logic gates. This was very hacker-friendly, since most of the core functionality was exposed at a human-friendly scale. The IBM PC-AT, on the other hand, was one of the first desktop computers to use VLSI chips for the processor support logic. I remember my first look at the PC-AT motherboard: I was hoping to be able to read the board like a book, with all the logic gates' part numbers gleaming in their fresh white silkscreen against the matte epoxy bodies of chips. What I saw instead was a closed book; there were perhaps three or four curious, high pin-count chips with part numbers and a manufacturer's logo I had never seen before. These chips were proprietary, and any hope of a deeper level of understanding or hardware exploration seemed to be dashed.

I think perhaps a lot of prospective hardware hackers felt the same way around then, because since then hacking has taken on a distinct software-oriented slant. Some of the most famous hackers today are renowned for their software contributions. Richard Stallman and Linus Torvalds are perhaps household names among the technological elite due to their fantastic contributions to free software through GNU and Linux. The best part about software hacking is its very low barrier of entry. Any willing youth with access to a computer and an Internet connection can plug into any of the various free software efforts and make a contribution to the technology collective. All the tools required to generate high-quality code are virtually free, and aside from the time investment, it costs nothing to use them. On the other hand, hardware hacking has a very real entry cost associated with the activity; there is a bare minimum set of tools that are needed on a daily basis, and an unfortunately large and diverse assortment of expensive, specialized tools is required to accomplish specific jobs. Furthermore, producing a hardware hack typically requires real materials in addition to time and energy, thereby placing creative and/or bold (read: risky) hardware-hacking projects beyond the financial horizon of most young folk. Given that human nature is to follow the path of least resistance, it is no surprise that hacking today is primarily a software affair.

In a twist of fate, recent macro-economic and social trends have worked to reverse the trend and bring more people into hardware hacking. The detritus of the dot-com bubble created fertile soil for sprouting hardware hackers. An overall reduction in demand for components, design, and manufacturing services has resulted from the economic slowdown. High-quality, used test equipment is trickling down into the ranks of hackers, either snatched off the shelf of dead companies or snapped up for pennies on the dollar at auction. Scrap components are also finding their way into distribution, driving down component prices. Combined with an overall soft demand situation, individual hackers are able to command the same level of service and component choice as large corporations. Furthermore, fabrication and assembly services have been forced to drive their prices down, to the point where hardware hackers could purchase high-tech, custom-built multilayer boards for under $50 per board.

Hardware design tool vendors also experienced a corresponding price adjustment due to the economic slowdown. Perhaps the most significant recent technological change for hardware hackers is the introduction of pro-