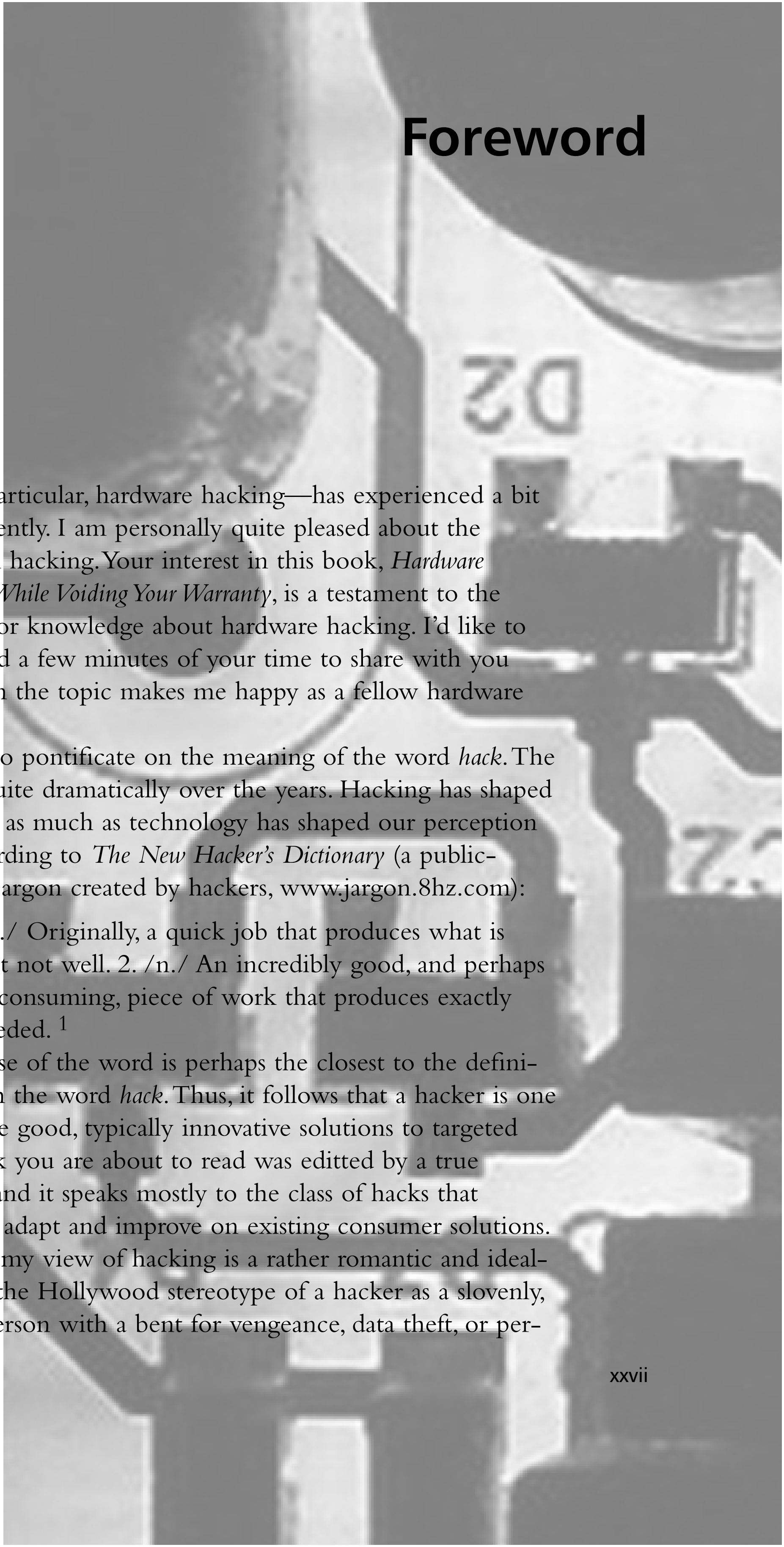

Foreword

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 perhaps 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 professional-grade FPGA design tools for *free*.The motivating theory for this development is that FPGA manufacturers could "hook" more designers into a particular brand or architecture if an effective and powerful set of design tools were made freely available. Stiff competition and hungry manufacturers helped ensure that a very featureful set of tools found their way into the market at a very low barrier of entry.

The significance of easy and affordable FPGA development systems cannot be understated. FPGAs have the effect of transforming the traditional solder-and-wires world of hardware hacking into the much more accessible and more widely understood code-and-compile world. A single hardware hacker working alone or in a small group can realistically build a complex microprocessor using FPGAs.This kind of activity was unheard of before the advent of FPGAs. Also, the availability of "programming languages" for hardware that could be translated into FPGA configurations meant that software hackers could cross over into hardware hacking without much formal training in traditional hardware design and assembly.

I can relate a personal example of the positive impact of the economic slowdown on hobbyists and hackers. During the buildup to the dot-com bust, it was literally impossible to buy high-quality tantalum and ceramic capacitors of the type used in compact/mobile switching power supplies. Chronic shortages due to explosive demand for portable and mobile electronic technologies meant that hackers had to compete toe-to-toe with large OEMs for pricing and component availability. I remember back around 2000 looking for samples of the AVX TPS "low-ESR" capacitors for a demonstration project I was building. I swept through every distributor I knew of, and all of them were posting lead times of months, with minimum buy quantities in the thousands. Ultimately, I had to do a minor last-minute redesign of the circuit just before sending the board for fabrication to compensate for the lack of high-quality capacitance. In contrast, just last month I cranked out a design that used an AVX TPS capacitor, and multiple hacker-friendly (i.e., high in-stock availability, credit card payment terms, and low minimum buy restrictions) distributors posted thousands of parts in their inventories. It certainly was pleasant to be able to access, with great ease, the same quality of components that the "big boys" use.

Although the confluence of recent macro-economic events set the stage for hardware hacking to regain popularity, this alone is not enough.

Remember, hacking is a fundamentally grass-roots activity, and it does not happen on a large scale unless there is some kind of social drive to motivate people into action.

A small part of the renewed social awareness in hardware hacking may be due to the desire of young hackers to extend themselves and carve a new niche for themselves. The software hacking world is now more structured, and new hackers joining one of the major software hacking establishments feel more like cogs rather than inspired inventors. Change and new ideas are not always so welcome from so-called "n00bs," and some budding hackers may be turned off by the intense flame wars that are sometimes triggered by a newbie suggestion or mistake.

However, this kind of sociopathy is probably not the real drive behind the renaissance of hardware hacking. I feel that the larger impetus is the recent pertinence of reverse-engineering consumer hardware. Rather than looking to hardware hackers for new product innovation, the public is looking to hardware hackers for the extension and liberation of existing solutions. This trend is a result of the tension between corporate motivations and the public's desires. Corporations are motivated by profit; thus, accessories are expensive, feature sets are artificially limited to create price discrimination, and lately, hardware vendors are locking their products to particular brands of consumable goods via embedded security or ID chips. On the other hand, consumers desire featureful, inexpensive products that deliver exactly what the they need, with no hidden costs or accessories required.

The status quo going into the new millennium was a competitive hardware market. However, the introduction of hardware-locked goods, especially combined with the power of the DMCA, has created a series of mini-monopolies. Hardware locking enables manufacturers to create vertically controlled mini-monopolies that break the free market model. Given the increasing complexity of hardware, consumers have few advocates that can cogently combat such corporate advances. Some advocacy groups work through political and legislative means, but legal processes are slow relative to the rate at which hardware locking can damage a market.

A new law protecting consumers may take years to draft and pass; on the other hand, a determined corporation can radically change a vertical market segment within a single year. For example, a printer manufacturer can realistically deploy crypto-locks on all its ink-consuming products within the span of a single product family generation, typically under two years. This would mean that the market for third-party ink suppliers would dry up in the same amount of time. The companies that provide consumers with choice and prices that reflect a competitive market would be long out of business before legislators were even aware of the problem. By the time reactive legislation was passed, the economies of scale would have been tipped grossly in favor of the OEM ink supplier, and such reactive legislation could have little practical impact on the market.

Since hackers are by definition a grass-roots group, the hacker's interests in these issues are inherently aligned with those of the general public. As a result, hackers are becoming the natural stop-gap consumer advocates in hot-button technological issues. These hackers sometimes operate above ground, and they sometimes operate like vigilante groups, breaking the most obnoxious hardware-locking schemes and "liberating" hardware to the public. Some may not agree with my viewpoint, but I find it hard to believe that monopoly prices, narrow selection, and a lack of market competition can be construed as positive developments for consumers. I believe that the majority of hackers are at least partially motivated by a desire to contribute to some larger cause, and preserving the technological balance of power against corporate monopoly tactics may be a rallying point for hardware hackers.

The publicity surrounding the DMCA has served to increase the public's awareness of the potential shifting of power from free-market consumer economics to corporate-driven mini-monopolies. It has also sparked a renewed interest in hacking. This interest meets a newly fertile technology scene, enriched by the availability of affordable hardware-hacking tools and services enabled by the economic slowdown in technology. Hopefully, this renewed interest in hardware hacking will not only result in a better-informed general public that is better capable of defending itself in the technology marketplace, it will also result in a new round of innovative products and companies in the vein of HP and Apple Computer. I personally hope that you find this topic enjoyable, and I look forward to hearing more about your adventures and exploits in hardware hacking.

Happy hacking!

—Andrew "bunnie" Huang,
Author of *Hacking the Xbox: An Introduction to Reverse Engineering*
and hardware hacker