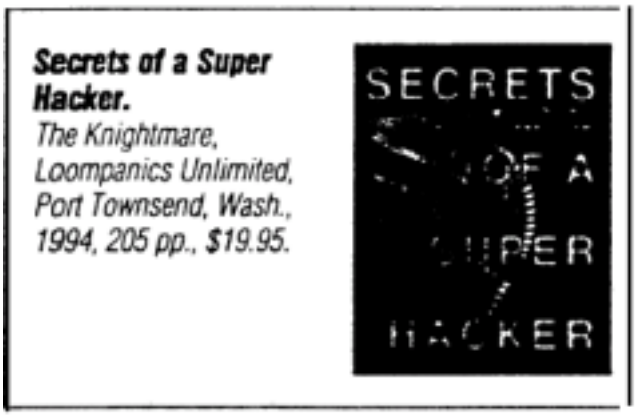
Hacker's how-to



"Code Crackers Not Crooks, Professor Says."

The headline perched atop an Associated Press story, and went on to say: "If a professor could have his way, hackers who crack top-secret computer codes would not be regarded as crooks but as eloquent manipulators of their favorite language.

For the record, I was the professor, and the sentiments expressed actually were more or less mine. In view of this history, my reading of this self-described "encyclopedic account of the methods by which security is breached and systems penetrated" might be perceived as biased.
Readers, beware.

It has not been so long since hackers were celebrated. John Badham's motion picture War Games (1983) opened the gates to many of the now-familiar stereotypes regarding hackers. Youngsters even began aspiring to hacking and phone-phreaking rather than fire-fighting or space exploration. Then followed, unsurprisingly, the demonization of the hacker.

Laws were hastily written, and hackers were apprehended and sentenced. Just recently, as I was reading this book unrelated incidents involving students from Brown University and the Massachusetts Institute of Technology MIT) brought hacking back into the news. Hacker activity on the fast-expanding Internet, meanwhile, has provoked calls for tighter rules and control of network users. If the subject matter of the book was not sensational enough already, then recent events have only elevated its profile. Youngsters, take note: computer security is a field of fast market growth and technological innovation.

The author declares a hacker to be someone "with an intense love of something, be it computers, writing, nature, or sports. A hacker is a person who, because he or she has this love, also has a deep curiosity about the subject in question.... For a computer hacker that means he respects the ability of computers to put him in contact with a universe of information and other people, and it means he respects those other people and does not intentionally use this knowledge of computers to be mischievous or destructive."

This seems so disingenuous that I cringe. It comes from the same person proclaimed on the back cover, in big, bold type, as "every security manager's worst nightmare!"

Inside, we read about "brute force attacks," which refer to "hurling passwords at a system until it cracks"; "spoofing," which is "designing dummy screens and delivering fake e-mail"; decryption of password files; and "stair-stepping," which means using a "low-level account to gain ever-higher levels of access."

We also read how to sort through trash (after scavenging, "take a shower when you get home," the author advises), and how to examine found disks and screen shots. Snooping and "shoulder surfing," in which "a hacker looms over the shoulder of a legitimate user that [sic!] logs on to a computer system," are also described. In between, the author sketchily outlines elementary notions of access control, communication software, modems and speed bar codes, computer viruses, and so on.

The main message, with which the book closes, is: "Don't get caught!" The message is amplified with a list of things to avoid, the "five ways you, the hacker, can get caught hacking: 1. by traces or technical means; 2. by being finked on; 3. by getting many agencies ganged up against you; 4. by making a mistake; or 5. by being [recognized]." If hacking merely expresses love for computers, and if hackers are so respectful, why worry about being caught?

This is a book that delivers a mixture of methods and ideas for breaking into other people's systems, and then follows that up with a code of ethics. Though this code emphasizes individual responsibility, some of its elements are controversial. To his (or her) credit, The Knightmare does address some of the big, difficult questions: access to information; the appropriate use of technology to empower people and not restrict their creativity or liberties; individual rights regarding data pertinent to people's lives; and a system of checks and balances in the digital domain, especially in the use of and commerce in databases affecting an individual's right to privacy.

"It is pointless," the author writes. "to raise the issue of 'Do you honestly think you can justify snooping with your loopy code of ethics?" A good point, and this brings up the central issue of such a book: Hacking, as the author notes, can be considered an expression of passion. But is it also exempt from moral and social constraints?

As Ken Thompson received the Turing award for his co-invention of Unix--the most hacked operating system--he made a point of explaining his attitude toward hackers: "The acts performed by these kids are vandalism at best and probably trespass and theft at worst. It is only the inadequacy of the criminal code that saves the hackers from very serious prosecution."

I wish the words were not his. Although Thompson's statement does indeed apply to many hacking cases--including most of the activities described by The Knightmare--he misses the critical point. In fact, Turing himself would have been jailed if the criminalizing of code-breaking had been applied to him. This requires elaboration, because the book I am reviewing misses this same point, too, but from the opposite direction.

In *Hackers* (Anchor Press/Doubleday, 1984), still the best book on the subject, Steven Levy noted that in the early 1960s, "a project undertaken or a product built not solely to fulfill some constructive goal, but with some wild pleasure taken in mere involvement, was called a 'hack'." Levy added that "the artistry with which one hacked was recognized to be considerable."

Programming was coming of age, and Peter Samson's code that converted Arabic into Roman numerals was one of the more celebrated hacks. At the annual MIT open house in May 1962, hackers fed into a PDP-1 minicomputer paper tape with 27 pages worth of assembly language code comprising a science fiction game written by students. Thus the interactive game was born--as a hack.

"We are prigs. We are intolerable aesthetes," wrote one hacker. The species believed in the art of programming, and their obsession was not with the "salami technique" of stealing money (briefly mentioned in the book) or with piracy. Scientific and technological motivations meshed with social and political values, some childish, others deeply visionary. There is no reason to idealize the romantic age of computation or to trivialize the driving force behind hacking, even if today's scientific and technological motivations are in fact quite different from those of the past.

The point is that there is a cognitive and an aesthetic dimension to hacking that separates it from the techniques of *phreaking* (breaking into the telephone system in order to use it for free) or cracking (hacking without respect for the computers being hacked, according to The Knightmare). Thus the author is right in asserting that hacking is not only a matter of digital technology. But after stating this in the book's opening, he or she abandons any pursuit of broader issues. Sensationalist expositions of methods (some disputable, some ingenious, none new) obscure the more fundamental question of why people hack.

The desire to understand is a basic one, and it is the downfall of all sorts of barriers to knowledge. Social, cultural, economic, and genetic codes have all been broken, leading me to believe that writing laws that criminalize hacking, without taking into account the specific nature of computer knowledge and access to it, is as ill-advised as writing a book on the so-called "secrets of a super hacker." Societies scared of hackers to the point of criminalizing them lose more than they think they gain by doing so. Gareth Branwyn, who knows quite a bit about the subject, provides good arguments along this line in the book's introduction.

The author frequently comments on obsolete statutes regarding computer crime. However, the break-in methods described are similarly anachronistic, carrying over fundamental misconceptions from previous pragmatic frameworks. As science becomes more and more computational, we need to come up with a better understanding of the nature of human activity in the Information Age. The New Frontier Foundation, mentioned in this book, is probably best equipped to help in this respect.

Nomadic computation, voice and handwriting recognition, living and working on the information grid, and virtual reality are the new territory of what hacking used to be. Unfortunately, they are not to be found in this book On the contrary, readers might wonder why The Knightmare pays so much attention to MS-DOS (Unix is mentioned, too), when so much of today's computation takes place on other platforms.

Client-server structures are quite different from old-style, centralized mainframe systems, even for a hacker bent only on "getting in." Surprisingly, the book also repeats some tired stereotypes, identifying hackers by their "thick glasses, modest height [and] fanatic taste for computers, bad movies, and pulp science fiction." It's as bad as the social engineering described by the author in absurd detail.

Media coverage of hacking has focused on penetrations of networks carrying sensitive information, intrusions into proprietary files, and piracy. It ignores intriguing or innovative ideas and broader motivations. On a smaller scale, this book does the same thing. The most that happens in this self-described super hacker's account is a penetration of a library system with dial-up access.

A computer hacker needs to understand how computers work, to study them, to learn programming. So it struck me as incredible that *Secrets of a Super Hacker* contained no technical information of which I was not already aware. Instead of holding this against the writer or publisher, I would like to turn it into a final observation.

To hack means to be on the frontier, on the border. In computer science and technology. This border is constantly being pushed back, and at a tremendous pace. In truth, a good "how to" book cannot be written on hacking, because with each new hack, a higher level of knowledge is reached that requires newer methods to surpass. To explain hacking, therefore, is to explain it away.