Making an Arrest in Cyberspace

By Simson L. Garfinkel

ON Jan. 23, 1995, New York Times reporter John Markoff published a front-page story describing an electronic attack over the Internet. In scope, it was the electronic equivalent of the bombing of the World Trade Center.

What made this incident newsworthy was the technique, which had never been attempted before, and the apparent target: Tsutomu Shimomura, one of the leading computer security practitioners in the United States. But the real story unfolded in the following weeks, as Shimomura identified, and tracked Kevin Mitnick, the apparent attacker, and led a team of FBI agents to his den. The following day, in court, Mitnick faced Shimomura and said, "Tsutomu, I respect your skills."

The capture of Mitnick was just the beginning. By the middle of March, Markoff's agent had sold the story of Mitnick's pursuit and arrest to Hyperion; rights for the movie were sold to Miramax Films. Markoff and Shimomura then retreated to a cabin near Lake Tahoe, where the two worked fervently to create "Takedown", a fascinating behind-the-scenes account of two hackers battling it out in cyberspace.

The break-in occurred on Christmas Day, 1994, while Shimomura and Julia Menapace, a former programmer at Apple Computer, were hot-tubbing in a friend's luxurious, high-tech San Francisco apartment. Unknown to Shimomura and Menapace, while they discussed plans for a ski vacation, a computer hacker on the other side of the country had broken into the apartment's central computer and used it to launch an attack against the computers at Shimomura's home and office, 500 miles south, in San Diego.

In the weeks that followed, Shimomura discovered that the attack against him was part of a pattern of attacks against a number of top-ranked computer professionals, and perhaps more than a dozen on-line services.

Shimomura learned that the attacker was reading the electronic mail of his ski buddy, John Markoff. And he learned firsthand how ill-equipped the Federal Bureau of Investigation is to handle high-tech computer crimes.

With "Takedown", the authors are trying to follow in the tracks of Cliff Stoll's 1989 best-seller, "The Cuckoo's Egg." The parallels are certainly present: the first-hand account of California's computer counter-culture; a blossoming romance hindered by circumstances but finally strengthened by the capture of the thief; even the same literary agent, John Brockman.

But "Takedown" seems forced, a pale imitation of Stoll's book with a fundamentally less interesting villain. The narrative's technical descriptions are confusing at times, and absent at others. The book is filled with extraneous details, such as what people are wearing. An extended biography of Shimomura isn't very interesting or particularly well-written.

"Takedown's" interest lies in the high-tech tracking and trapping of Kevin Mitnick. But that story doesn't even begin until a hundred pages into the book. The first hundred pages are filled with so much background it's easy to get lost. Notably missing is action. Shimomura and Markoff never pass up the opportunity to tell the reader something, instead of taking the time to show it.

"Takedown" does a stunningly inaccurate job of reporting the major controversies about the Internet today. Richard Stallman's fight against proprietary software, the role of copyright law in stifling free speech, and the force of software patents in consolidating the computer industry are mischaracterized and dismissed as the belief that "there should be no such thing as software intellectual property rights." The authors report that the Digital Telephony Act, which President Clinton signed into law in October 1994, "had given online service and Internet providers the ability to monitor the keystrokes of people communicating over their systems. It was anathema to privacy rights groups, but an important tool that was absolutely vital for tracking intruders."

In fact, the main purpose of the Digital Telephony Act, as its name implies, was to expand the FBI's ability to wiretap telephones, not computers. The book never mentions the much publicized controversy over the Clinton administration's "clipper chip," an anti-encryption code to be required in all computer chips.

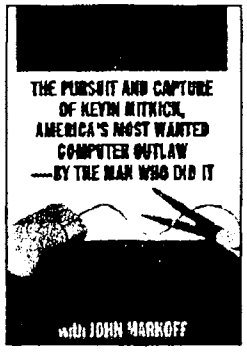
Markoff's writing, especially the sections in which he speaks to the imagined persona of Kevin Mitnick, is a pleasure to read: "Mitnick and jsz [the initials of an as yet still at large accomplice] were systematically trawling the Internet, and it appeared they were specifically targeting the computers of security experts to rifle through their mail. With the techniques they had pilfered, they subsequently attacked the computers of corporations like Apple, Motorola, Oki, and Qualcomm."

Perhaps the most revealing parts of "Takedown" are the actual transcripts between Mitnick and his more able and apparently still-unknown conspirator. The jokes about homosexuals and girls, interwoven with their comments on computer security, undercut Mitnick's supposed reputation. Instead of appearing as a technical master or cyber villain, Mitnick comes across as the dupe of jsz, the real cyber villain.

Like Mitnick himself, "Takedown" tries to do too much and ultimately fails. Devoted Markoff fans will enjoy the chase, but the catch is lacking.

■*Simson L. Garfinkel is a freelance writer who specializes in science and technology.*

BOOKS



TAKEDOWN
Tsutomu Shimomuru with John Markoff
Hyperion, 324 pp., $24.95

NEW METHODS OF DETECTION

...I quickly become bored with academic and theoretical discussions of computer security, but ...in the wake of the break-in, ...there was a chance to talk about something that was more interesting,... to use our data to describe exactly what had transpired. One of the areas of computer crime detection that is still in a relatively primitive state is methodology. For hundreds of years people have been investigating physical crimes, and while some of forensics is still a black art, there are well-established methods for investigating crime scenes and finding evidence. In the digital world, however, there is still very little in the way of formal detection methodology.

– From "Takedown"