San Jose Mercury News, February 12, 1996

Beware: Net addresses hijacked

BY SIMSON L. GARFINKEL
Special to the Mercury News

A prankster changed the name of computer security expert Tsutomu Shimomura's Web home page.

COMPUTER pranksters have graduated from forging electronic-mail messages to hijacking entire Internet addresses.

Even technically challenged cyberthieves can send messages or rob companies of their "domain names," which are the computer addresses used by people and corporations on the World Wide Web. The situation has led to calls for increased use of digital signatures on e-mail messages and a stricter authentication process before Internet addresses can be changed.

The lack of authentication recently became a problem for computer security expert Tsutomu Shimomura. Last month, Shimomura published "Takedown: The Pursuit And Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw — By the Man Who Did It."

To help publicize the book, Shimomura built a "home page" on the World Wide Web that offered additional information, sound clips from several harassing phone calls that were left on his voice-mail system and transcripts from several "chat" sessions allegedly involving Mitnick, in which he bragged about his hacker skills.

But last week Shimomura's Web site was taken down after a computer prankster persuaded Net-

See ADDRESSES, Page 6E

Hijackers change Net domain names

Pranks prompt calls for digital IDs, tougher verification procedures

■ ADDRESSES

from Page 1E

work Solutions Inc. — the unofficial gatekeeper for Internet addresses — to change the name *takedown.com* to *takendown.com*.

Network Solutions is the company that runs the telephone book of cyberspace. In Shimomura's case, NSI's computers play a key role in routing inquiries and messages. By changing the record in NSI's computers, the attacker effectively kicked Shimomura's computer off the Internet. Although Shimomura's Web page was still at the original address, anyone who tried to access it was sent to the prankster's home page.

"It's pretty juvenile," Shimomura told the Wall Street Journal last week. On Friday, Shimomura was reportedly sick in bed with a high fever and unavailable for comment.

How to send forged e-mail

It turns out that it is relatively easy to send forged electronic mail on the Internet today. Using programs such as the Netscape Navigator, all a potential forger has to do is change the name and return mail address. Thus, anybody with a copy of Netscape Navigator can transmit messages that look as if they were written by a boss or co-worker. In the case of *takedown.com*, the attacker presumably sent a message that appeared to come from Shimomura.

"I am aware that it occurred," said Dave Graves, Internet business manager for Network Solutions. "We have an ongoing internal investigation as we speak. The only thing that I know for sure is that it was not the result of a hacker attack. Nobody penetrated our system."

> **"The only thing that I know for sure is that it was not the result of a hacker attack. Nobody penetrated our system."**
>
> *— Dave Graves, Internet business manager for Network Solutions, about the changing of Shimomura's home page*

Instead, what probably happened was that somebody on the Internet sent a forged piece of electronic mail to Network Solutions' Internet Network Information Center, or InterNIC, which followed the standard procedure for changing an Internet address.

Network Solutions receives roughly 3,000 of these requests each week, Graves said. For the most part, the requests are processed automatically by its computer — no questions asked. But the automatic process can create problems. According to Mark Kosters, a software engineer with Network Solutions, as many as 30 of those change requests each week may be fraudulent.

Most are probably done as pranks, experts said, although increasingly people are changing addresses as a way to harm a person or company financially. Some want to try to steal someone else's business.

Legal issues

Mike Godwin, staff attorney for the Electronic Frontier Foundation, said it isn't clear whether it is against the law to change someone's Internet address without that person's permission.

"There's no particular fraud statute associated with domain names," said Godwin, whose group tracks cyberspace issues. "However, general fraud statutes

might apply, at either the state or federal level. Generally, if you make material misrepresentations to someone in order to get something from them, it is considered a fraud."

To help weed out fraudulent changes, Graves said, Network Solutions will accept a change to a domain name only if it is sent by a previously agreed-upon representative. Change requests that don't come from the right e-mail address are handled manually.

"We have a letter that we will send to the domain name holder," Graves said. "We will send it by fax or Federal Express or postal mail."

Unfortunately, the name of each site's authorized contact is *readily available on the Internet* itself. As a result, some bogus requests get through and are processed automatically.

"Our domain, 'colossus.net,' was stolen twice by a third party," said Eric Klien, president of Colossus Inc., an Internet service provider in Chicago that had its domain name switched twice last December. "(We) complained a lot to InterNIC. They immediately corrected the problem each time."

What happened in the Colossus case, said Graves, is that two partners who had created Colossus had a falling out.

"These two individuals wanted control of the Colossus domain name," he said. "We found ourselves in the position where we were receiving conflicting information from two different individuals, each with the apparent authority to legally bind the company."

"InterNIC's security is so weak that I could move IBM's domain tomorrow to my site," Klien said.

No special protection

Graves agreed, saying that Network Solutions does not grant special protections for high-profile names such as *ibm.com*, *aol.com* or *compuserve.com*. "We treat all of our customers equally."

And Graves does not plan to give these names special protection. Instead, Network Solutions is working on a new system called "Guardian," which will authenticate all change requests using public key cryptography. Public key cryptography is a code that allows Internet users to send private information that cannot be read by anyone other than the intended recipient.

Although cryptography, the science of making secret codes of *messages, is normally used to* "encrypt" mail so that it cannot be read by anyone other than the intended recipient, it can also be used to create a "digital signature." The digital signature is placed at the bottom of an electronic-mail message, which certifies the author of the message, and allows the recipient to determine if the message has been modified since it was signed.

Graves said that the registration process will be analogous to a company putting a person's name and signature on a bank signature card.

"If one of the people on your signature card cleans you out of your money, it is your fault and not the bank's," he said.