

Weaving a tangled 'Net

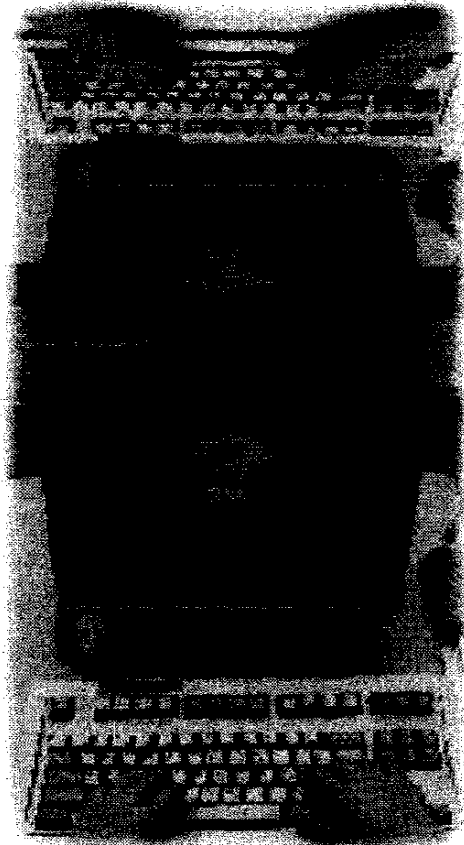
Professor's work offers warning of how Web can be used to con consumers / **Simson L. Garfinkel**

I ATTENDED A computer security workshop in New Jersey last week, and saw Princeton University professor Edward W. Felten construct a Web of deceit and intrigue.

Felten showed the audience how to use features in Netscape Navigator or Internet Explorer to construct a "mirror Web" - a twisted reflection of the Internet's World Wide Web complete with hidden tricks and traps where nothing is as it seems.

While this was an academic exercise, it demonstrated how such sites could easily be created by people with sinister intentions. The fact that the world's Web browsers are susceptible to this sort of attack should give pause to people thinking of using the Internet for commercial transactions, at least for now.

Born in Boston and educated at CalTech, Felten, 34, is a relative newcomer to the field of computer security. Last spring he and his graduate students published a series of attacks on the Java programming language, showing the system being distrib-



uted by Sun Microsystems and Netscape wasn't as secure as was widely believed. But this new attack exploits not a programming problem, but a psychological one. And while it is possible to make changes in browsers to minimize the consequences of the attack, neither Netscape nor Microsoft has shown any willingness to do

so.

The problem, explains Felten, is that programs such as Navigator ask users to make a lot of security-related decisions during a typical session on the Internet. You type a password to log in. You might type a different password to visit the Web site at The New York Times. If you download your credit-card information from a bank, you type a third password.

Unfortunately, Web browsers don't give users enough information to make the security-related decisions properly. As a result, a malicious Web site can fool users into revealing sensitive information or downloading and running a malicious program without their knowledge. Indeed, there's really no good way, with the current generation of Web browsers, for users to really believe anything they see on the screen.

Say you are surfing the Web and you click into a site that asks you for your user name and password. How do you know that the user name and password you type are really going to the computer that appears to be asking for them? You don't. Programs em-

bedded in Web sites can change what your Web browser displays. In his talk, Felten showed how to construct a mirror Web site. This is a site that appears to be housed on one computer, say WWW.MICROSOFT.COM, when in fact it is actually on another, such as WWW.MICROSOFT.COM.

Can you tell the difference between those two addresses? The second has the number zero instead of the letter "O" following the S.

Although those are different for the computer, they can be visually indistinguishable.

Using Netscape's JavaScript programming language, it's possible to reprogram your Web browser so you think it's pointing at www.microsoft.com when it's really pointing at www.attacker.org. JavaScript can change what's displayed in the Web browser's status and location fields.

The mirrored pages can be perfect replicas: You can't tell the difference, but some malicious Web site is recording everything you do and type. Or they can feed you bogus information and download programs with viruses to your hard drive.

Netscape comes with a system called public key encryption that's supposed to minimize this sort of attack. When you open up a connection to a so-called "secure" Web server, the little yellow key in the lower left-hand corner of Netscape Navigator turns blue. Unfortunately, it turns blue if you connect to *any* secure Web server. In order to figure out that you've connected to the correct one, you must use Netscape's "view document info" command. Few people do that.

One way to solve this problem would be to make Netscape al-

ways display the cryptographically verified legal name of the Web site to which you have connected. But even if that one particular nit is fixed, there are a lot of other ways to fool a user.

For example, a small program written in Java could display a window on your computer saying that your computer's dial-up connection has been lost. It could then invite you to type your user name and password to reconnect. The Java program could even play the tones that most people's modems make when they are re-establishing a connection.

Netscape tries to get around this problem by displaying the words "unsigned Java applet window" whenever a Java program tries to create its own window. Unfortunately, there are ways of getting around this.

You can find an amusing collection of other Web tricks and tangles at the DigiCrime Web site, <http://www.digicrime.com/>. For more information about Felten's work, check out Princeton's Secure Internet Programming group's Web site at <http://www.cs.princeton.edu/sip>.

Spoofing the user is a kind of 21st-century con game. But it's not an insoluble problem. Unfortunately, many institutions are jumping in to the world of Web commerce, with the idea that they're willing to take some losses in order to build up their market share. Let's hope consumers don't get hurt in the process.

Technology writer Simson L. Garfinkel can be reached at plugged-in@simson.net.