Buyer Beware: Online Shopping Hazards Exposed By Computer Scientist

February 21 2006

Consumers who shop online may be risking their privacy with every purchase, contends University of Massachusetts Amherst computer scientist Kevin Fu. His research suggests that a confluence of factors, including the widespread use of cookies and demand for quick and easy transactions, results in Web sites that are often insecure.

“Much Web security rests on illusion and hope,” says Fu, who discussed how Web sites leak private information on Saturday, Feb. 18 at the American Association for the Advancement of Science meeting in St. Louis.

Most Web users have heard of cookies, the small chunks of information that a Web server sends to a browser to identify the user at a later date. Cookies are stored on the browser computer’s hard drive and each time a user revisits a site the cookie is sent back to the server, telling it, “Hi, it’s me again.”

“Cookies are insecure, no matter what you do,” says Fu. While they aren’t that dangerous when used for things like storing preferences on personalized Web pages (they are how Yahoo remembers that a user wants science headlines displayed, for example) they are also employed to authenticate users who are shopping online. It’s these so-called “authentication cookies” that are often exploitable, says Fu.

Cookies work by replaying the same information. While they may be associated with a password to start, the cookie is how a site remembers a

user, and allows them to skip a log-in page. So someone who has accessed a series of cookies on a hard drive can look for a pattern and then backtrack to come up with the algorithm that generated them. “It’s the kind of thing a bored teenager could do in a few hours,” says Fu.

Cookies aren’t the only problem, says Fu. Every Web site has its own method of authenticating users, and there is no set standard for Web site security—even that little padlock icon doesn’t mean much, he says. Many sites use what Fu calls “home-brew cryptography,” a security system that’s set up by someone lacking the expertise to do so. In recent years some companies have begun selling off-the-shelf encryption toolkits. These can be more secure, says Fu, but many are “just smoke and mirrors.”

Unless a security system has “open design,” meaning how it works is public information, it probably isn’t worth much, says Fu. The best log-in methods don’t employ cookies, but use what’s known as client certificates in SSL or “secure socket layer.” These are akin to a signet ring, says Fu. The user authenticates who they are by stamping the wax with their seal. They never actually send the ring itself to the site—which is what cookies do. These systems are often used at universities, allowing students to access grades online, for example.

Why aren’t client certificates used elsewhere? They are cumbersome, says Fu, and retailers want to offer quick, easy shopping. Cookies get the most sales in the shortest time, and if no one is attacking, they work just fine. Being able to order something quickly provides short-term fulfillment, and the long-term cost to privacy isn’t very tangible.

There are steps that companies can take to prevent attackers from breaking their authentication schemes, says Fu. Prohibiting guessable passwords, for example, or only using temporary cookies that expire when the user exits the browser. A cryptographic system with a public

protocol that can be reviewed for flaws will likely be more secure than a system with a private one.

Fu does shop online. “There isn’t much of an alternative for consumers. Even if you shop by phone, the attendant often enters your data on the same Web page you are trying to avoid,” he says. A CEO, a doctor or someone with access to the records of others should especially care about secure log-ins.

“There’s a lot of legacy to this, too,” he adds, “The set-up is too entrenched at this point—too many hours and too much money would be required to change things. But the company that figures out how to do so will be very successful.”

Source: University of Massachusetts Amherst