System thwarts Internet eavesdropping

August 25 2008

The growth of shared Wi-Fi and other wireless computer networks has increased the risk of eavesdropping on Internet communications, but researchers at Carnegie Mellon University's School of Computer Science and College of Engineering have devised a low-cost system that can thwart these "Man-in-the-Middle" (MitM) attacks.

The system, called Perspectives, also can protect against attacks related to a recently disclosed software flaw in the Domain Name System (DNS), the Internet phone book used to route messages between computers.

The researchers — David Andersen, assistant professor of computer science, Adrian Perrig, associate professor of electrical and computer engineering and public policy, and Dan Wendlandt, a Ph.D. student in computer science — have incorporated Perspectives into an extension for the popular Mozilla Firefox v3 browser than can be downloaded free of charge at www.cs.cmu.edu/~perspectives/firefox.html.

Perspectives employs a set of friendly sites, or "notaries," that can aid in authenticating Web sites for financial services, online retailers and other transactions requiring secure communications. By independently querying the desired target site, the notaries can check whether each is receiving the same authentication information, called a digital certificate, in response. If one or more notaries report authentication information that is different than that received by the browser or other notaries, a computer user would have reason to suspect that an attacker has compromised the connection.

Certificate authorities, such as VeriSign, Comodo and GoDaddy, already help authenticate Web sites and reduce the risk of MitM attacks. The Perspectives system provides an extra measure of security in those cases but will be especially useful for the growing number of sites that do not use certificate authorities and instead use less expensive "self-signed" certificates.

"When Firefox users click on a Web site that uses a self-signed certificate, they get a security error message that leaves many people bewildered," Andersen said. Once Perspectives has been installed in the browser, however, it can automatically override the security error page without disturbing the user if the site appears legitimate.

The system also can detect if one of the certificate authorities may have been tricked into authenticating a bogus Web site and warn the Firefox user that the site is suspicious. "Perspectives provides an additional level of safety to browse the Internet," Perrig said. "To the security conscious user, that is a significant comfort."

Andersen said the increased use of wireless connections to the Internet has increased the risk of MitM attacks. These occur when an attacker tricks a computer user into believing that the user has established a secure link with a target site, such as a bank. In actuality, the computer user is communicating with the attacker's computer, which can eavesdrop as it relays communications between the user and the target site.

"It's very, very, very easy for someone to convince you to go through their computer" when making connections through public Wi-Fi, Andersen said. A user who thinks he is linked to an airport or coffee shop "hot spot," for instance, might actually be linked to a laptop of someone just a few seats away. "A lot of people wouldn't even know they've been attacked," he added.

Most Internet communications, such as to standard hypertext transfer protocol (HTTP) sites, are unsecured, but those involving encryption over a secured socket layer (SSL) and those using secure shell (SSH) protocol, which involves the use of a login and password, require that sites authenticate themselves with a digital certificate containing a so-called public key, which is used for encryption.

The exchange of this security information typically occurs without the computer user being aware of it. But when something isn't quite right, a dialogue box such as "Unable to verify the identity of XYZ.com as a trusted site" is displayed by the Web browser.

"Most users don't have a clue about what to do in those cases," Wendlandt said. "A lot of them just shrug and go ahead with the connection, potentially opening themselves up to attack."

A vulnerability disclosed in July in the DNS software poses a different problem for computer users, but one that also is addressed by Perspectives. The software flaw could enable an attack against an Internet Service Provider (ISP) that would cause the ISP to connect users with a malicious site instead of the legitimate site they were seeking. "With Perspectives, even if a client's ISP has fallen victim to the attack, the client will be able to detect that the public key received from the fake site is inconsistent with the results returned from the notaries," Wendlandt said.

Source: Carnegie Mellon University