New 'active cookie' helps protect Internet users from cyber crooks

February 17 2006

A new technique developed by an Indiana University School of Informatics scientist provides a strong shield against identity theft and cyber attacks.

Cybersecurity expert Markus Jakobsson and the start-up RavenWhite Inc., of which Jakobsson is a co-founder, have developed an "active cookie," a countermeasure designed to protect against online scams such as pharming and man-in-the-middle attacks.

Pharming is obtaining personal or private (usually financial) information through domain spoofing. Rather than spamming with malicious and mischievous e-mail requests for users to visit fake Web sites which

appear legitimate, pharming "poisons" a domain name server by planting false information in the server, resulting in a user's request being redirected elsewhere. The browser, however, tells users they are at the correct Web site.

"There are no reliable commercial tools currently available to protect users from such attacks," said Jakobsson, associate professor of informatics and associate director of the IU Center for Applied Cybersecurity Research. "We believe that active cookies can provide such protection."

RavenWhite provides a new use of cookies, which are coded pieces of information stored on a person's computer that identify that computer during the current and subsequent visits to a Web site. Active cookies can be used in some situations where traditional cookies are not practical. Jakobsson's invention helps protect against known types of pharming attacks and man-in-the-middle attacks, but also against new and threatening versions such as two new attacks discovered by Mark Meiss and Alex Tsow, both computer science doctoral students at IU.

Meiss discovered a technique that allows an attacker to hijack almost any Wi-Fi (wireless fidelity) connection with the purpose of redirecting users to incorrect sites. He recently verified that the technique works in a local hotspot, a location where Wi-Fi users pick up an active signal.

"There is no way a user can determine that this attack takes place," explained Meiss, a researcher at IU's Advanced Network Management Lab. "You can't be sure you are actually visiting your banking site, for example, even though it looks like you are. There is simply no way of telling."

Tsow discovered that consumer routers can be trivially modified to stealthily redirect users to fake sites. He showed a browser window

where he typed eBay into the address bar, but where the loaded content showed the Web page of the Anti-Phishing Working Group.

"In a real attack, the user would be taken to a site that is a true clone of the place they intended to go, but the cloned site would be operated by the attacker and would steal the user's password," said Tsow, a visiting research associate who works with Jakobsson.

Jakobsson believes these kinds of attacks pose threats that few have considered. "How can I dare to connect in a hotspot when the guy next to me may be hijacking my connection and taking me to the wrong site to steal my password?" Jakobsson asked. "And how can anybody buy hardware from sellers they don't trust? These attacks are not detectable by the ordinary Internet user."

Jakobsson cautions that consumers should not buy a router from online services if they fear the seller might really be a phisher in disguise. Apart from being a problem for online auction sites such as eBay, it is also a problem for financial service providers, whose customers are the potential victims of attacks of this type.

"Those are the organizations that would benefit most from using active cookies," Jakobsson added.

Jakobsson will discuss active cookies and other research results on identity theft and its countermeasures when he moderates a panel discussion Saturday (Feb. 18) at the annual gathering of the American Association for the Advancement of Science in St. Louis, Mo.

More details about RavenWhite can be found at www.ravenwhite.com. Information about the IU Center for Applied Cybersecurity Research is at cacr.iu.edu.

Internet-related identity theft accounted for about 9 percent of all ID thefts in the United States in 2005, according to a recent report released by Javelin Strategy and Research. The findings also show that the average loss per incident jumped to $6,432 from $2,897 in the previous year.

Consumers can find out more about how to protect themselves from identity theft at the Federal Trade Commission Web site, www.consumer.gov/idtheft

Source: Indiana University