Informatics scientists' ‘active cookies’ put bite on cyber crooks

December 7 2006

Researchers at the Indiana University School of Informatics and RSA Laboratories have written a recipe to protect Internet users from identity theft and other kinds of cyber attacks.

Whereas regular computer cookies, which are often used for authentication purposes, can easily be stolen from the computers where they belong, active cookies resist such attacks. This helps keep identifying information secret, which in turns stops cyber attacks.

Cookies are coded pieces of information stored on a user's computer. The cookies identify that computer, and therefore also its user, during the current and subsequent visits to a Web site. Active cookies can be used in exactly the same general manner, but are resistant to attacks by identity thieves and hackers.

"Normal computer cookies can be stolen in many ways," said Markus Jakobsson, associate professor of informatics and co-inventor of active cookies. "One way is for the attacker to interfere with what is called the domain lookup, a process when an Internet address, such as a well-known lending institution, is translated to an Internet Protocol address, which is the real address computers use to communicate."

This attack is called Domain Name System poisoning, commonly referred to as pharming, and it allows any users' cookies to be stolen. The attacker could simply target one of the many machines a computer interacts with when its users browse the Web, including a home router.

"But active cookies cannot be stolen like this, even if an attacker interferes with the DNS translation," said Jakobsson. "The reason is simple: Active cookies use one step that requires no translation."

Jakobsson and Sid Stamm, a computer science doctoral student at the School of Informatics, worked on the project with Ariel Juels of RSA Laboratories in Massachusetts. Jakobsson and Juels also are co-founders of RavenWhite, a private company developing cookie technology to protect users from on-line threats.

Stamm said that if an attacker successfully interferes with the translation, then the attacker still cannot obtain all the secret information he needs to impersonate the victim.

"This allows your bank to check that you are you," said Stamm, "or at least that the person who knows your username and password also uses your computer. This could really make a difference in terms of the threat of phishing."

The reason is simple: While a cyber crook might trick a user into revealing their PIN number or password, as is commonly done in some scams, it is not enough to gain access to the user's account; they would need to steal a person's personal computer where the active cookies are stored.

The researchers claim, for example, that a user's bank can put active cookies on their clients' home and work computers.

"And you can still log in if you travel, you might just have to provide some additional identifying information then, or your bank can compare your login location with the location of your last ATM withdrawal," Jakobsson said. "Or the active cookies system used by banks can flag suspicious login transactions and see whether they result in strange

transfers. Then the bank could put a hold on these transactions and verify them with their customers."

The researchers' work will be presented in February at the 14th Annual Network & Distributed System Security Symposium in San Diego, Calif.

Source: Indiana University