threatpost
The Kaspersky Lab Security News Service

Published on *threatpost* (http://threatpost.com)

Even Without Browser Flaws, Attackers Have the Upper Hand on the Web

By *Dennis Fisher*
Created *10/26/2010 - 12:59pm*

[1]TORONTO--If the spate of vulnerabilities and sophisticated attacks against browsers in the last couple of years has done nothing else, it's certainly shown just how vulnerable users are as they go about their daily business on the Web. In a talk at the SecTor conference, a researcher showed several methods for combining a variety of new and existing attacks that can not just compromise users' Web accounts but also allow attackers to use that information to extend their attacks in a number of directions.

Web-based exploits and browser attacks have become an epidemic in recent years and attackers constantly are refining their techniques, adapting the defenses that browser manufacturers and security vendors put in place. But even with all of the protections that are available, the fact remains that browsers and their components can be manipulated in a number of ways by the sites that users visit.

"The Web is a code-distribution channel. When you're running a browser, you're running someone else's code," said Samy Kamkar, an independent security researcher, in a talk at SecTor here Tuesday. Kamkar is responsible for the creation of the Evercookie [2] earlier this month.

In his presentation, Kamkar discussed techniques for attacking a user whom you know uses a particular site, such as Facebook, for example. Instead of attacking the user directly, Kamkar said it can be more effective and efficient to go after the components of the site in question. With the goal of obtaining the target's session cookie on the site in mind, Kamkar looked at the method that Facebook uses to create entropy to generate the unique session cookie for each user.

Kamkar stressed that Facebook isn't actually vulnerable to this specific attack, and is just an example.

The site uses several different components to generate the cookie, including the microsecond that the user logs in, the user's IP address and other data. Trying to brute-force the entire cookie isn't feasible, so Kamkar took each component separately and tried to identify it through various methods, thereby reducing the number of bits in the cookie that would have to be brute-

forced.

For example, to determine the time that the user logs in, he used a script that would send a chat request to the target user every second. When the user logs in, the server will respond with a message that includes the exact time of the login. That data comprises 32 bits of the cookie.

Finding the IP addres is even simpler. Kamkar said an attacker could simply send a benign link to the victim in a chat session, directing him to a site the attacker controls. The attacker could then see the victim's IP address in his server logs. That's another 32 bits of the cookie data.

The Facebook cookie also contains a random number generated by a pseudo-random number generator (PRNG) in PHP. The seed that the PRNG uses is split into halves of 32 bits each. One part of that is the exact time that the server started. By sending a huge number of requests to the remote server, Kamkar said it's possible to get the remote process to re-spawn, which will enable the attacker to make a reasonable guess at the server's start time. That gives him 12 bits of each half of the seed.

With 40 bits of the seed remaining, Kamkar said an attacker can brute force the rest of it, enabling him to predict the numbers that the PRNG will generate each time.

"Within about 500,000 requests, we can predict that cookie and log in as the target," Kamkar said. The same method can be used to gain admin access to the site, by abusing the way that sites use the PHP PRNG to generate the random URLs they send to users who have forgotten their passwords.

"If you've broken the seed, you can guess the random URL and change the admin's email to yours," he said. "The attack is dificult to execute, but it's definitely possible."

Source URL: http://threatpost.com/en_us/blogs/even-without-browser-flaws-attackers-have-upper-hand-web-102610

Links:
[1] http://threatpost.com/en_us/blogs/even-without-browser-flaws-attackers-have-upper-hand-web-102610
[2] http://threatpost.com/en_us/blogs/researchers-find-methods-kill-persistent-evercookie-101910
[3] http://www.twitter.com/home?status=Even Without Browser Flaws, Attackers Have the Upper Hand on the Web http://threatpost.com/en_us/cMG