

Attacking the edges of secure Internet traffic

July 30 2010, By JORDAN ROBERTSON , AP Technology Writer



A man passes a logo of the Black Hat technology conference in Las Vegas on Wednesday, July 28, 2010. (AP Photo/Isaac Brekken)

(AP) -- Researchers have uncovered new ways that criminals can spy on Internet users even if they're using secure connections to banks, online retailers or other sensitive Web sites.

The attacks demonstrated at the Black Hat conference here show how determined hackers can sniff around the edges of encrypted Internet traffic to pick up clues about what their targets are up to.

It's like tapping a [telephone conversation](#) and hearing muffled voices that hint at the tone of the conversation.

The problem lies in the way Web browsers handle Secure Sockets Layer, or SSL, encryption technology, according to Robert Hansen and Josh Sokol, who spoke to a packed room of several hundred [security](#) experts.

Encryption forms a kind of tunnel between a browser and a website's servers. It scrambles data so it's indecipherable to prying eyes.

SSL is widely used on sites trafficking in sensitive information, such as [credit card numbers](#), and its presence is shown as a padlock in the browser's address bar.

SSL is a widely attacked technology, but the approach by Hansen and Sokol wasn't to break it. They wanted to see instead what they could learn from what are essentially the breadcrumbs from people's secure Internet surfing that browsers leave behind and that skilled hackers can follow.

Their attacks would yield all sorts of information. It could be relatively minor, such as browser settings or the number of Web pages visited. It could be quite substantial, including whether someone is vulnerable to having the "cookies" that store usernames and passwords misappropriated by hackers to log into secure sites.

Hansen said all major browsers are affected by at least some of the issues.

"This points to a larger problem - we need to reconsider how we do electronic commerce," he said in an interview before the conference, an annual gathering devoted to exposing the latest computer-security vulnerabilities.

For the average Internet user, the research reinforces the importance of being careful on public Wi-Fi networks, where an attacker could plant himself in a position to look at your traffic. For the attacks to work, the attacker must first have access to the victim's network.

Hansen and Sokol outlined two dozen problems they found. They

acknowledged attacks using those weaknesses would be hard to pull off.

The vulnerabilities arise out of the fact people can surf the Internet with multiple tabs open in their browsers at the same time, and that unsecured traffic in one tab can affect secure traffic in another tab, said Hansen, chief executive of consulting firm SecTheory. Sokol is a security manager at National Instruments Corp.

Their talk isn't the first time researchers have looked at ways to scour secure [Internet traffic](#) for clues about what's happening behind the curtain of encryption. It does expand on existing research in key ways, though.

"Nobody's getting hacked with this tomorrow, but it's innovative research," said Jon Miller, an SSL expert who wasn't involved in the research.

Miller, director of Accuvant Labs, praised Hansen and Sokol for taking a different approach to attacking SSL.

"Everybody's knocking on the front door, and this is, 'let's take a look at the windows,'" he said. "I never would have thought about doing something like this in a million years. I would have thought it would be a waste of time. It's neat because it's a little different."

Another popular talk at [Black Hat](#) concerned a new attack affecting potentially millions of home routers. The attack could be used to launch the kinds of attacks described by Hansen and Sokol.

Researcher Craig Heffner examined 30 different types of home routers from companies including Actiontec Electronics Inc. and Cisco Systems Inc.'s Linksys and found that more than half of them were vulnerable to his attack.

He tricked Web browsers that use those routers into letting him access administrative menus that only the routers' owners should be able to see. Heffner said the vulnerability is in the browsers and illustrates a larger security problem involving how browsers determine that the sites they visit are trustworthy.

The caveat is he has to first trick someone into visiting a malicious site, and it helps if the victim hasn't changed the router's default password.

Still: "Once you're on the router, you're invisible - you can do all kinds of things," such as controlling where the victim goes on the Internet, Heffner said.

©2010 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Attacking the edges of secure Internet traffic (2010, July 30) retrieved 25 April 2024 from <https://phys.org/news/2010-07-edges-internet-traffic.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.