SECURITY darkREADING
Protect The Business Enable Access

SSL Still Mostly Misunderstood

Even many IT professionals don't understand what Secure Sockets Layer does and doesn't do, leaving them vulnerable, new survey shows

By Kelly Jackson Higgins, DarkReading
Oct. 7, 2009
URL:http://www.darkreading.com/story/showArticle.jhtml?articleID=220301548

Most users ensure their Web sessions are using Secure Sockets Layer (SSL) before entering their credit card information, but less than half do so when typing their passwords onto a Web page, according to a new survey.

Just what SSL does and doesn't do isn't clear to many users, and the way Websites implement it doesn't help: "The biggest issue is the general population doesn't know what SSL is, why they're using it, and it's ingrained in them that it always makes them secure, which is not always the case," says Tyler Reguly, senior security engineer for nCircle, who surveyed a cross-section of users -- technical and nontechnical -- and shared the results of his findings today during a panel presentation about SSL at the SecTor Conference in Toronto.

Reguly's survey found that while 83 percent of users check they're using an SSL-secured session before entering their credit card information on a Website, only 41 percent do so when typing in their passwords. "It's scary that people care so little about their passwords than they do about their credit card numbers," he says. "You see surveys saying that anywhere from 30 to 60 percent of users are using the same password everywhere, so they're probably using it for online banking, too."

It has been a rough year for SSL, with the groundbreaking man-in-the-middle hack by researcher Moxie Marlinspike, which dupes a user into thinking he's in an HTTPS session when in reality he has been taken elsewhere by the attacker, as well as a demonstration by researcher Mike Zusman showing how several certificate authorities (CAs) themselves are vulnerable to attacks when issuing SSL certificates. And Dan Kaminsky at Black Hat USA exposed critical flaws in X.509 certificate technology used in SSL.

Zusman, who spoke on Reguly's panel along with Robert "RSnake" Hansen of SecTheory and Jay Graver, lead engineer at nCircle Network Security, says it's not just the general consumer population who doesn't understand SSL, which encrypts a Web session and authenticates the identity of a Website. "It's still a challenge in the infosec community. I was doing a penetration test with a team last week, and the development team asked why we found all these vulnerabilities in their product when they were using SSL," he says.

More than half of the respondents don't know what Extended Validation SSL (EVSSL) is and how it differs from SSL, while 36 percent say they do. Interestingly, most of them are aware that SSL traffic can be sniffed without their knowledge.

Even so, nearly one-third say the only purpose of SSL is to encrypt their traffic so it can't be sniffed.

Reguly and Zusman say aside from a need for better user education about SSL, much of the problem lays with how Web developers deploy SSL. One respondent, for example, said SSL would be more effective if an