CRIME attack is shown to decrypt HTTPS web sessions

September 14 2012, by Nancy Owano

(Phys.org)—The fun of acronyms is reflected in coming up with CRIME, which stands for Compression Ratio Info-leak Made Easy. What it translates into, though, is not much fun. Two security researchers have developed the CRIME attack that can successfully decrypt session cookies from HTTPS (Hypertext Transfer Protocol Secure) connections. This, in theory, would be a serious weakness that would enable the hijacking of a user's session cookie while the user is still authenticated to a website. Encryption protocols are the Internet's fundamental safety cushion, the basic level of trust, in encrypting traffic that flows over open networks. They cryptographically confirm websites are really operated by those sites rather than cyber-criminals and spies.

Security researchers Juliano Rizzo and Thai Duong devised a technique that can attack web sessions that are protected by the Secure Sockets Layer and Transport Layer Security protocols, only when they use certain data-compression schemes. These are compression schemes that reduce network congestion or the time it takes for webpages to load.

Security experts have noted that a downside of compression is that it leaks clues about encrypted contents. For the attack to work, a computer user's client and server hosting the targeted website need to support the vulnerable SSL/TLS features. According to reports, Internet Explorer was never vulnerable because it never supported SPDY or the TLS compression scheme known as Deflate. Apple's Safari browser doesn't support SPDY, but its use of compression is unknown.

Google and Mozilla released patches after the weaknesses were reported by the researchers. A video taken by Rizzo and Duong shows Github.com, Dropbox.com, and Stripe.com, when visited with Chrome, succumbing to the CRIME attack, but those sites had disabled compression and are no longer vulnerable. Mozilla and Google have prepared patches that block the attack.

Rizzo and Duong will take their demo of CRIME to the Buenos Aires, Argentina, security conference, Ekoparty, on September 21. Their attack technique no longer works on the most popular browsers to connect to HTTPS-protected websites, but security watchers believe this is a most useful reminder that the science of encrypton protection knows no rest.

Their CRIME exploit is the type of attack that would be a large-scale attack by geopolitical antagonists. In turn, security watchers reasons are paying attention to the researchers' CRIME technique.

More information: www.ekoparty.org/2012/juliano-rizzo.php

Citation: CRIME attack is shown to decrypt HTTPS web sessions (2012, September 14) retrieved 25 April 2024 from https://phys.org/news/2012-09-crime-shown-decrypt-https-web.html