Researchers find vulnerabilities in use of certificates for Web security

28 October 2015

Consumers use the Internet for banking, emailing, shopping and much more nowadays. With so much personal and private information being transmitted over the Web, Internet users must be able to rely on and trust the sites they are accessing. For security purposes, websites use certificates to establish encrypted communications. When a site becomes compromised, its certificate should be revoked.

A new study offers the first end-to-end evaluation of the Web's certificate revocation ecosystem, which includes website administrators that obtain and revoke certificates, certificate authorities that publish a list of revoked certificates, and browsers that check the revocation list to authenticate a website.

The study results reveal that website administrators are providing a large number of revoked certificates, certificate authorities are not using newer processes for distributing revocations, and Web browsers are not checking whether certificates have been revoked. The findings indicate that all participants in the revocation ecosystem must improve their performance to fulfill their responsibilities and ensure system success.

"The findings paint a bleak picture, because users put an immense amount of trust into the browsers they use and the websites they visit to do what is necessary to protect their security," says study co-author Dave Levin, an assistant research scientist at the University of Maryland Institute for Advanced Computer Studies.

The results of the study will be presented October 29, 2015 at the Association for Computing Machinery Internet Measurement Conference (ACM IMC) in Tokyo. Levin conducted the study with researchers from Stanford University, Northeastern University, Duke University and Akamai Technologies.

Secure online communication requires authentication—a user's ability to determine with whom he or she is communicating. Central to achieving authentication on the Web is a system known as the Public Key Infrastructure (PKI), which consists of certificates and encryption keys. While online use of the PKI is mostly automated, the system requires a surprising amount of human intervention to maintain the validity of the certificates.

"Revocation of certificates is critical to the security of the Web, because it is the only way to protect users from attackers who impersonate websites after a security breach, such as Heartbleed," says Levin, referencing a widespread security bug discovered in 2014.

Heartbleed allowed malicious users to capture information that would give them the opportunity to masquerade as trusted servers and potentially steal sensitive information from unsuspecting users. In a previous paper, Levin showed that few websites revoked their Heartbleed-compromised certificates and issued new ones.

"This paper builds off of my previous work on the Heartbleed vulnerability by asking: even if websites properly revoke their certificates, will browsers receive and check the certificates?" says Levin. "Unfortunately, the overwhelming answer is no."

In the current study, Levin and his colleagues investigated the performance of website administrators, certificate authorities and Web browsers in real-life scenarios.

To evaluate how well website administrators handled revocations, the team analyzed a multi-year data set that included 74 full Internet scans. The researchers found that a surprisingly large fraction of the certificates served—8 percent—had been revoked. By serving revoked certificates, website administrators introduce security holes, says Levin.

Next, the team evaluated the performance of certificate authorities, which usually distribute revocations to Web browsers through CRL files that contain lists of revoked certificates. The team found that these files can grow to large sizes, which slow down the browser and use more bandwidth when downloaded. The findings indicate that browser developers may be trading security for better performance, according to Levin. The team also found that newer techniques for distributing revocations have not been widely implemented by the certificate authorities.

Finally, the researchers investigated 30 different combinations of operating systems and Web browsers—including Chrome, Safari, Firefox and Internet Explorer—and found that none of them properly checked to see whether certificates are revoked. In addition, mobile browsers running on both iOS and Android platforms did not check for revoked certificates.

"If a browser shows the lock icon, then users believe that the page is the website it reports to be," says Levin. "And yet, our results indicate that browsers and websites are not checking the security certificates to make sure this is true."

Levin says this study will affect the fundamental assumptions about how the PKI works in practice.

"In the research space, we hope this will affect how other systems that rely on revocations are designed to better match the likely behavior of administrators," Levin says.

More information: The paper, "An End-to-End Measurement of Certificate Revocation in the Web's PKI," by Yabing Liu, Will Tome, Liang Zhang, David Choffnes, Dave Levin, Bruce Maggs, Alan Mislove, Aaron Schulman, Christo Wilson, will be presented October 29, 2015 at ACM IMC, www.cs.umd.edu/~dml/papers/revocations_imc15.pdf

Provided by University of Maryland