Mozilla says HTTPS is the way forward for the Web

May 4 2015, by Nancy Owano

Credit: Wikipedia

The web developer community can hear a rallying cry loud and clear :Let's hear it for web security. Mozilla, the group behind the browser Firefox, is turning up the volume by saying enough's enough with non-secure HTTP. The Foundation has taken a move in order to protect users from snoopers.

HTTP stands for hypertext transfer protocol, used for web data exchange. Mozilla is instead opting for the encrypted version, HTTPS, providing better security.

A security lead and his colleague at Mozilla said a beginning step in that direction should be, according to their draft document, to make it less appealing to deploy new things over non-secure HTTP, so as to create incentives for HTTPS adoption. *Fortune* carried a link to the draft document titled "Insecure HTTP Deprecation Plan."

Fortune said about 30 percent of Internet traffic in North America is protected with HTTPS encryption but Sandvine, a networking equipment company in Canada, has a report that over half the world's traffic will be secured by encryption by the end of the year.

In a blog post on April 30 titled "Deprecating Non-Secure HTTP," Mozilla announced its intent to phase it out. Certainly Mozilla is not alone in calling out the need for encryption. "In recent months," wrote Richard Barnes, Firefox Security Lead in the blog post, "there have been statements from IETF, IAB (even the other IAB), W3C, and the US Government calling for universal use of encryption by Internet applications, which in the case of the web means HTTPS."

Moving forward, Mozilla has a two-step plan: Set a date after which all new features will be available only to secure websites and gradually phase out access to browser features for non-secure websites, especially features that pose risks to users' security and privacy.

At the same time, the Mozilla move "still allows for usage of the 'http' URI scheme in legacy content. With HSTS and the upgrade-insecure-requests CSP attribute, the 'http' scheme can be automatically translated to 'https' by the browser, and thus run securely."

To be sure, some web developers will want to know just how the move will affect their unencrypted sites and when. In a FAQ document, Mozilla's answer is "Transitioning the web to HTTPS is going to take some time. The first thing we're going to do is require HTTPS for new features." They also explained that in the long run, any changes such as removing or limiting features currently available to unencrypted sites "will be announced well ahead of any change, so you'll have time to update your site either to not rely on those features or, we hope, to move to HTTPS."

Also, anticipating there will be those who say "But there's nothing secret on my site! Why should I bother with encryption?" Mozilla's answer is, "HTTPS isn't just about encryption. It also provides integrity, so your site can't be modified, and authentication, so users know they're connecting to you and not some attacker."

More information: Mozilla blog: blog.mozilla.org/security/2015 … ing-non-secure-http/