Let's Encrypt certificate authority to launch 2015

November 19 2014, by Nancy Owano

Web encryption for free—tough deal to turn down? After all the instances of cyberattacks, snoopers and sophisticated surveillance, encryption technology has become especially appreciated and familiar to many people. In a bid to alleviate the expense and complexities of encryption, the Electronic Frontier Foundation has joined Mozilla, Cisco, Akamai, IdenTrust, and researchers at the University of Michigan for Let's Encrypt, to launch in summer 2015 as a certificate authority to encrypt the entire web.

The Let's Encrypt CA will automatically issue and manage free certificates for any website that needs them. Free, as opposed to expensive, certificates will in turn encourage small businesses and web sites in adopting the technology. As of now, you cannot assume you are getting a secure HTTPS connection when logging on to a website from a cafe or transportation terminal. Actually, wrote Frederic Lardinois of TechCrunch, "most smaller websites don't offer these kind of secure connections because getting the kind of digital public-key certificate that makes HTTPS connections work involves a rather annoying and manual process. They also typically don't come cheap."

Peter Eckersley, The EFF's technology projects director, announced the move on Tuesday. "Switching a webserver from HTTP to HTTPS with this CA will be as easy as issuing one command, or clicking one button," he said. Here are some of the factors that inspired the launch: The HTTP protocol has been hugely successful but inherently insecure, said Eckersley. Users have been vulnerable to such events as account hijacking and identity theft; surveillance and tracking; injection of malicious scripts into pages; and censorship that targets keywords or specific pages on sites. "The HTTPS protocol, though it is not yet flawless, is a vast improvement on all of these fronts, and we need to move to a future where every website is HTTPS by default." Moving over to HTTPS, however, has not been trivial.

Ars Technica quoted Eckersley on Tuesday: "The unfortunate truth is that there are a lot of obscure and head-spinning technical details that need to be gotten right for a top-notch HTTPS deployment," he said. "With Let's Encrypt, we are going to automate as much of that as we possibly can."

Addressing complexity, the effort it takes for a web developer to enable encryption for the first time is anywhere from one to three hours. With Let's Encrypt, the time will be cut down to 20 to 30 seconds. Another

advantage of the project is that it will employ Internet-wide datasets of certificates such as EFF's Decentralized SSL Observatory, the University of Michigan's scans.io and Google's Certificate Transparency logs, for higher-security decisions about when a certificate is safe to issue. (Google's Certificate Transparency project fixes structural flaws in the SSL certificate system, the main cryptographic system that underlies HTTPS connections. Certificate Transparency makes it possible to detect SSL certificates that have been mistakenly issued by a certificate authority or maliciously acquired from an otherwise unimpeachable certificate authority. It also makes it possible to identify certificate authorities that have gone rogue and are maliciously issuing certificates.)

The Let's Encrypt CA will be operated by an organization called the Internet Security Research Group (ISRG).

More information: — www.eff.org/deeplinks/2014/11/ … y-encrypt-entire-web

— letsencrypt.org/