How Let's Encrypt doubled the internet's percentage of secure websites in four years

November 13 2019

Credit: CC0 Public Domain

The percentage of websites protected with HTTPS secure encryption —indicated by the lock icon in the address bar of most browsers—has jumped from just over 40% in 2016 to 80% today.

That's largely due to the efforts of Let's Encrypt, a nonprofit certificate authority co-founded in 2013 by J. Alex Halderman, a University of Michigan professor of computer science and engineering.

By offering a free service, Let's Encrypt has turned the implementation of HTTPS from a costly, complicated process to an easy step that's within reach for all websites. The certificate authority is now the world's largest, providing more HTTPS certificates than all other certificate authorities combined.

Halderman and his collaborators at Let's Encrypt—the Electronic Frontier Foundation, Mozilla, Cisco and Stanford University—have published a paper detailing how the project came to fruition. They hope it serves as a model for streamlining other aspects of the internet infrastructure we all rely on every day.

What exactly is an HTTPS certificate authority?

Halderman: HTTPS is the protocol that web browsers use to talk to web servers over an encrypted connection. It provides confidentiality by preventing eavesdroppers from making sense of the data. It provides integrity by preventing malicious networks from changing the data. And it provides authentication by ensuring that you're talking to the server shown in the browser's address bar rather than an imposter. That last part is essential. If HTTPS didn't have authentication, an attacker could

redirect the connection to a server they controlled and read or alter the data.

Authentication is also the tricky part, and that's where certificate authorities come in. They're a small group of organizations that web browsers trust to vouch for the identity of servers. To implement HTTPS, a website first has to prove to a certificate authority that it really is the server at a particular internet domain. Then the certificate authority issues the site a digitally signed certificate, which works like a driver's license to let browsers confirm its identity.

Why is encryption important on websites that don't handle sensitive information?

Halderman: When HTTPS was invented in the 1990s, it was intended mostly for credit card transactions and online banking. But since then, the internet has become a much more dangerous place. Edward Snowden showed us that governments were surveilling traffic on a global scale. We've also seen instances where governments and others have changed internet traffic to attack the user's computer, or to use their computer to attack third parties.

So today, encryption is important not just for financial transactions but for all online communications. That's why it's important to make it accessible to every website operator, and Let's Encrypt is doing just that. It has been particularly good at driving HTTPS adoption on smaller websites that don't have the resources to get a certificate through the traditional process.

Why has HTTPS been so difficult to implement?

Halderman: Traditionally, implementing HTTPS has required website

operators to choose a certificate authority, prove their identity to them, pay as much as a few hundred dollars for a certificate, wait for it to arrive, then follow a complicated series of steps to install it. You have to repeat the process every year or two, and if you don't do it on time, your website might go down. So a lot of websites, particularly smaller ones, just left their sites unencrypted.

Let's Encrypt is a different kind of certificate authority that provides free certificates through an automated process that often only takes one click, and sometimes it's an automatic part of website setup. That has driven a huge increase in the number of secured sites.

How can Let's Encrypt provide certificates for free?

Halderman: First, Let's Encrypt is nonprofit and is funded mostly by donations from large tech companies. That's different from most certificate authorities. Secondly, and maybe counterintuitively, making certificates free dramatically reduces the cost of issuing them. Payment is a big source of friction that makes the process much harder to automate.

So once you remove that friction, certificates become much simpler to issue. Once we simplified the process, we were able to automate it by building a software system called the ACME protocol. ACME lowers the cost of each certificate Let's Encrypt issues to a fraction of a cent.

Why is your team's first paper about Let's Encrypt coming out four years after its launch?

Halderman: Because creating a new kind of certificate authority that gives out free certificates was a crazy idea. If we had written the paper before we built it, it wouldn't have gotten published. We had to prove

that the economics would work, and there was no way to do that except to just build it.

Four years later, Let's Encrypt has been wildly successful. And I hope this paper, which looks back at how we built it and measures it impact on the web, can help spread some of the lessons we've learned to help other parts of the internet infrastructure work better.

What are some of those lessons and how can they help in other areas?

Halderman: Part of what makes Let's Encrypt work is that it's a neutral party operating in the public interest rather than a product of any one large tech company. That makes it something everyone can trust and that no one company has an overriding stake in.

There are other places where authentication and cooperation are necessary. For example, ISPs often work together on routing protocols that direct information around the internet. But that process itself is not encrypted and is subject to attack. That's a place where a model similar to Let's Encrypt could work well.

You mentioned that Let's Encrypt was a crazy idea in 2013. Today, it doesn't seem so crazy. How do you get from "crazy idea" to "why didn't I think of that?"

Halderman: By looking beyond the usual academic measures of success like number of papers or commercial startups. We can do that at Michigan because real-world impact is in the DNA of the College of Engineering. And to be honest, I don't think there are many other universities where this could have happened.

When we started this project, we knew that it wasn't going to become a traditional academic paper anytime soon. But people here saw that it was likely to be valuable to the world, and they supported the work—everyone from the colleagues who tenured me to the thesis committee for the Ph.D. student who helped design ACME. That support was what enabled us to drive the project all the way to success.

The paper, Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web, will be presented Nov. 14 at the ACM Conference on Computer and Communications Security in London.

Provided by University of Michigan