THE LINUX FOUNDATION

CASE STUDY

Making Internet Security Accessible to Everyone

ABOUT LET'S ENCRYPT

Let's Encrypt is a free, automated and open certificate authority, run for the public's benefit and operated by The Linux Foundation. The objective of Let's Encrypt and the ACME protocol is to make it possible to set up an HTTPS server and have it automatically obtain a browser-trusted certificate, without any human intervention. This is accomplished by running a certificate management agent on the web server. There are two steps to this process. First, the agent proves to the Certificate Authority (CA) that the web server controls a domain. Then, the agent can request, renew, and revoke certificates for that domain. Let's Encrypt provides the system that allows for this to happen seamlessly and automatically with the goal of creating a more secure Internet.

Letsencrypt.org

HIGHLIGHTS

- Despite growing concern for data security, most transactions and websites are not secure
- Let's Encrypt enables free and automated installation of security certificates
- By end of 6-month beta period, Let's Encrypt had issued 1.7 million certificates for more than 3.8 million websites

The Challenge

Vital personal and business information flows over the Internet more frequently than ever, and we don't always know when it's happening. HTTPS has been around for a long time but according to Firefox telemetry only ~40% of websites and ~65% of transactions used HTTPS at the end of 2015. Those numbers should both be 100% if the web is to provide the level of privacy and security that people expect, and Let's Encrypt is leading the way.

It's clear at this point that encrypting is something all of us should be doing. In essence everyone should use TLS (the successor to SSL) everywhere to protect themselves. Every browser in every device supports it. Every server in every data center supports it. However, until Let's Encrypt there was a challenge and a significant cost to administering server certificates.

Let's Encrypt is a free certificate authority, built on a foundation of cooperation and openness, that lets everyone be up and running with basic server certificates for their domains through a simple one-click process.

The anchor for any TLS-protected communication is a public-key certificate which demonstrates that the server you're actually talking to is the server you intended to talk to. For many server operators, getting even a basic server certificate is just too much of a hassle. The application process can be confusing. It usually costs money. It's tricky to install correctly. It's difficult to update.

The Let's Encrypt client goes further than most other clients in terms of end-to-end automation and extensibility, both getting certificates and in many cases installing them. This is an important strategy since major servers don't yet have

built-in support, and the team supporting Let's Encrypt want to make sure it's given a proper chance to thrive. The Electronic Frontier Foundation (EFF) has led development of the Let's Encrypt client from the beginning, and they are well-qualified to continue pursuing this strategy.

The Approach

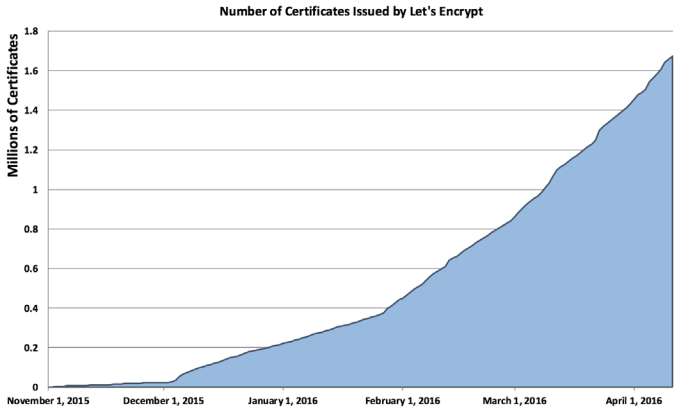
Mozilla Corporation, Cisco Systems, Inc., Akamai Technologies, Electronic Frontier Foundation, IdenTrust, Inc., and researchers at the University of Michigan started working through the Internet Security Research Group ("ISRG") to deliver this much-needed infrastructure in 2014. The Linux Foundation is providing the infrastructure and operational support of Let's Encrypt using their collaborative model for open source projects.

The key principles behind Let's Encrypt are:

- **Free:** Anyone who owns a domain can get a certificate validated for that domain at zero cost.
- **Automatic:** The entire enrollment process for certificates occurs painlessly during the server's native installation or configuration process, while renewal occurs automatically in the background.
- **Secure:** Let's Encrypt serves as a platform for implementing modern security techniques and best practices.
- **Transparent:** All records of certificate issuance and revocation are available to anyone who wishes to inspect them. Twice annually a Legal Transparency report will be published to ensure users have visibility regarding legal requests.
- **Open:** The automated issuance and renewal protocol is an open standard and as much of the software as possible will be open source.
- **Cooperative:** Much like the underlying Internet protocols themselves, Let's Encrypt is a joint effort to benefit the entire community, beyond the control of any one organization.

The Results

In November 2014 Let's Encrypt was launched and in September 2015 Let's Encrypt entered their beta period. By March of 2016 Let's Encrypt had issued its millionth certificate and had secured over 2.4 million domains. Through April 1, 2016 when the their beta ended Let's Encrypt issued 1.7 million certificates for more than 3.8 million websites.



Since leaving beta, support for the effort has also grown. Cisco and Akamai have renewed their Platinum sponsorships with 3-year commitments. Facebook has joined as a Gold sponsor along with IdenTrust, Internet Society and Gemalto. HP Enterprise, Fastly, Shopfiy, Automattic, and ReliableSite.net and many others have joined the ranks of over 20 silver sponsors.

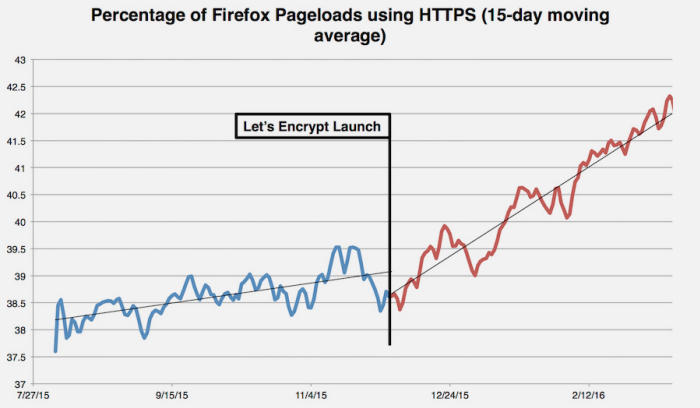
> "Encryption by default is critical to privacy and security, and by working with Let's Encrypt Gemalto is helping to deliver trust for the digital services that billions of people use every day."
>
> *- Todd Moore, Vice President of Encryption Product Management, Gemalto*

THE LINUX FOUNDATION

CASE STUDY

Let's Encrypt has received a considerable boost from industry endorsement, with major hosting companies like OVH, Wordpress.com, Gandi, Dreamhost, and Digital Ocean helping many sites move to HTTPS with Let's Encrypt.

Based on numbers Mozilla gathers from Firefox users, encrypted sites now account for more than 42 percent of page visits, compared with 38.5 percent just before Let's Encrypt launched.



In April, Wordpress.com started providing free HTTPS for all custom domains hosted on WordPress.com which helps protect users in various ways, including defending against surveillance of content and communications, cookie theft, account hijacking, and other web security flaws.

Bitly, the URL shortening service, serves approximately twelve billion clicks a month, helping users with shorter links get to the places online that they want to go. Until May of 2016 none of those URLs were generated securely via HTTPS URLs. As Bitly rolls out phase 2 of their plan to offer secure URLs with Let's Encrypt, will bring HTTPS to the ubiquitous Bit.ly domain and be available to every user of the Bitly platform.

> "Cisco is committed to improving the security of the Internet, not only for our customers and partners, but for everyone else as well. Let's Encrypt has been doing impressive work toward that goal. Our support of this community towards real-time, on-demand certificates will make the Internet more secure."
>
> *- David Ward, CTO of Engineering and Chief Architect at Cisco*

The project's aim is for HTTPS to become the default on the web, and the success so far gives the community confidence that it will get there - and much faster than anyone predicted. Let's Encrypt is growing at a current rate of more than 100,000 certificates per week which is creating a rapid increase in the security and safety of online web users.

For more information on Let's Encrypt visit letsencrypt.org
For more information on projects hosted at The Linux Foundation, visit linuxfoundation.org/projects