COMMENTARY

How to Get Free HTTPS Certificates from Let's Encrypt

Mike Robinson (mcrobinson@limxr.org), Chair of the ALA's Intellectual Freedom Privacy Subcommittee and Head of Systems at the Consortium Library at the University of Alaska Anchorage

There has been a push by many organizations in recent years to move all websites from nonsecure HTTP to the more secure HTTPS protocol. HTTP is vulnerable to eavesdropping and content hijacking. HTTPS helps protect against these problems by establishing an encrypted connection between your browser and the website. There are a number of initiatives promoting the move to HTTPS:

- Federal government websites are now required to be HTTPS.
- Google now gives a ranking boost to HTTPS sites in search results.
- Firefox and Chrome now warn users that HTTP sites are insecure.
- The Freedom of the Press Foundation started the Secure the News project to track and promote the adoption of HTTPS by major news sites.
- The Electronic Frontier Foundation launched an Encrypting the Web campaign.
- The Library Digital Privacy Pledge encourages libraries and their content providers to adopt HTTPS.

Perhaps one of the most successful initiatives has been Let's Encrypt, a new certificate authority that provides both free HTTPS certificates and tools to easily install them. Let's Encrypt has a number of sponsors including the Electronic Frontier Foundation, Mozilla, Chrome, Facebook, and the American Library Association (ALA). That's right, ALA is a sponsor of this important initiative to help libraries move to HTTPS. The free tools and certificates from Let's Encrypt became available in a beta version November 2015 and moved out of beta status in April 2016. Adoption has been rapid (Aas 2017). In January 2016, they supported 240,000 active certificates, which grew to more than 28 million by January 2017, making it one of the largest certificate authorities in the world. Approximately half of the web is now on HTTPS.

Most libraries have never had HTTPS (Breeding 2016), and its time for that to change. Let's Encrypt can be used to install HTTPS on a variety of library websites and services. I have written a series of blog posts that provide step-by-step recipes of how we moved our library servers to HTTPS (Robinson 2016) last year using Let's Encrypt, including the following server types:

- Apache Web Server on CentOS 6
- IIS Web Server on Windows 2008
- Standalone EZproxy Server on CentOS 6
- Library OPAC Server—SirsiDynix Enterprise on Tomcat CentOS 5
- API Server—SirsiDynix Web Services on Tomcat CentOS 6

These recipes are for servers under the library's direct control. It was simple and straightforward for the system administrator to install the Let's Encrypt client and obtain the certificate on a variety of servers with one exception—it was tricky to install the Let's Encrypt client on the server running the aging CentOS 5 operating system because of out-of-date dependencies. Another possible issue is libraries that use EZproxy to access content from a large number of HTTPS websites. The recommended way to do this is through a wildcard HTTPS certificate, which Let's Encrypt does not yet support. Let's Encrypt does support up to one hundred domain names on a single certificate, so it can work fine for libraries with a moderate number of HTTPS resources to proxy.

Good documentation and community support exists for those that want to integrate Let's Encrypt into their products and services. More than a hundred web hosting platforms (Let's Encrypt 2015) have integrated Let's Encrypt so that certificates can be installed by customers from their control panel with just the click of a button. Vendors and content providers in the library world should begin integrating support for Let's Encrypt into their products and services.

References

Aas, Josh. 2017. "Let's Encrypt 2016 In Review." *Let's Encrypt Blog*, January 6. https://letsencrypt.org/2017/01/06/le-2016-in-review.html.

Breeding, Marshall. 2016. "Protecting Patron Privacy: Libraries are failing to use HTTPS." *American Libraries Magazine,* May 31. https://americanlibrariesmagazine.org/2016/05/31/protecting-patron-privacy/.

Let's Encrypt. 2015. "Web Hosting who support Lets Encrypt." December. https://community.letsencrypt.org/t/web-hosting-who-support-lets-encrypt/6920.

Robinson, Mike. 2016. "Let's Encrypt Cookbook for Library Servers." *Mike Robinson: UAA/APU Consortium Library* (blog), June 13. https://consortiumlibrary.org/blogs/mcrobinson/blog/2016/06/13/lets-encrypt-cookbook/.