Let's Encrypt & HTTPS Everywhere

by

Aaron Grothe

OLUG - April 2016

What does it take to get an SSL-Protected Site

The Usual Way

Need to generate a CSR (Certificate Signing Request)
Send it off to Thawte/Comodo/Verisign/etc - Pay them $$$ for it
Take the resulting signed response and import it into your webserver
Repeat the process every year or two forever

What does it take to get an SSL-Protected Site

The Usual Way

Or you can use a self-signed certificate

And provide browser warnings to all your users and scare some of them off

An SSL-Protected Site with Let's Encrypt

Install the Software from the Let's Encrypt website

Run it

And go

Why Does This Matter?

It removes the monetary and most of the technical issues that prevent a lot of websites from going secure
Any websites you connect to via http are vulnerable to being intercepted/modified. These classic Man-In-The-Middle attacks have been linked to a lot of issues over the years.
You have a higher chance that you are talking to the website you think you are E.g. you are talking to https://www.amazon.com vs another site impersonating it.
You make it more difficult for others to eavesdrop on your transmissions for marketing/other purposes E.g. inserting ads into the stream

Why Does it Matter? (Cont)

Privacy (on the last slide but bears repeating)

Make it harder for people/companies/governments to listen in and see what you are doing/researching

The ability to cheaply aggregate data from you is a huge source of information to companies about us

An Example

Mathletics is an e-learning site used by millions of people
It didn't use SSL and was vulnerable to snooping
Site is now moving to SSL to provide increased security
Very bad for a site holding information for children

Summary: If you ask somebody for a username/password and you're not on an https protected site, you're part of the problem

Let's Do A Demo

Hit a website that has ssl installed without a CA .crt (gpgschool.org)
Look at certificate info

Lets run letsencrypt-auto and go see what it takes

Results now are a bit different

Some Cool Things about LetsEncrypt

CA is accepted by all the major browsers (Firefox/IE/Google Chrome)
LetsEncrypt is going to be available in quite a few different systems
    Is in Ubuntu 16.04 / Debian Testing / Fedora 24
It has pretty good support for Apache / experimental support for ngnix

Some Cool Things about LetsEncrypt

Can be used to just generate a simple certificate or can be used to install a certificate and update the webserver settings
Plugin architecture
Is simply a checkbox on Dreamhost's cpanel
Big sponsors include EFF, Mozilla & Cisco
E-mails you for updates, renewals, etc.

Some Not So Cool things about LetsEncrypt

Certificates are sha-256 / RSA key size 2048 - no support for SHA-1

Can have trouble with older systems (Windows XP, some embedded systems)

Certificates are good for 90 days (need to do renewals)

Is still in beta

Some Not So Cool things about LetsEncrypt

Support for ngnix and other webservers are in development
No wildcard support currently. Can't register *.gpgschool.com
Can't generate for certain webhosts such as linode, digitalocean, aws, etc. Can use these hosts but have to point a domain to the server
Some limits to how many certs you can request a week and so on

Other Options to Let's Encrypt

CAcert.org

Another CA
Not supported by all browsers like Google Chrome
Has instructions/information for setup which can be pretty helpful
Run by donations

Other Options to Let's Encrypt

StartCom

Offers free type-1 certificates
StartCom has add on options / commercial options as well
Also not accepted automatically by all browsers

OLUG Mailing List website uses a StartCom SSL certificate

HTTPS Everywhere

HTTPS Everywhere is a browser extension for Google Chrome/Mozilla and Opera that tries to force you to connect via https to websites
Tries to force connections to stay SSL as much as possible
Some versions support SSL Observatory as well - which is a tool designed to prevent Man In The Middle attacks
Works for most sites, can cause some sites to have problems, used to be a problem with hulu.com and the ads
Uses some code from the NoScript's HTTP Strict Transport Security implementation

Summary

An encrypted web is a safer web
Let's Encrypt is going to be a part of this
There have been a couple of studies that suggest building the functionality of HTTPS Everywhere into the Android web browser
The barriers to entry aren't that high
Give it a shot, the worst you can do is to need to do it again

References

Let's Encrypt

https://letsencrypt.org

HTTPS Everywhere

https://www.eff.org/https-everywhere

References

Mathletics Security Compromise / Response

http://www.theregister.co.uk/2016/02/29/mathletics_security_complaints_parents/

CACert.org

http://www.cacert.org

References

StartCom

https://www.startssl.com

HTTPS Everywhere

https://www.eff.org/https-everywhere

References

Google Transparency Report

https://www.google.com/transparencyreport/https/grid/