Let's Encrypt

Rod Bruce and Alex Lazar

2018 LibTech Conference

March 14, 2018

Why use HTTPS?

- HTTPS is a secure protocol for transferring encrypted web traffic
- Using HTTPS increases privacy of all information transferred
- Using HTTPS reduces risk of exploits and compromising data
- HTTPS is highly important when using insecure networks (e.g., public Wi-Fi)
- Non-HTTPS web traffic is like sending a postcard in the open

How does HTTPS work?

- HTTPS protocol uses encryption to secure information during transfer
- Transport Layer Security is the underlying secure protocol
- Public and private keys are used for session encryption
- Servers are authenticated using server certificates
- Server certificates are issued by Certificate Authorities

Certificate Authorities

- Certificate Authorities (CAs) issue digital server certificates
- CAs act as trusted third parties to guarantee ownership of private keys
- CAs are validated and included in browsers by browser vendors
- Most CAs are for-profit companies like Symantec, Comodo, GoDaddy
- Typical server certificates cost money and require manual installation

Let’s Encrypt

- Let’s Encrypt is a relatively new certificate authority
- Let’s Encrypt is a non-profit and they issue certificates for free
- Mozilla, Cisco, Akamai, EFF and ALA are among backers
- Let’s Encrypt certificates are designed for complete automation
- Let’s Encrypt uses an open protocol to handle installation and renewal

Reasons to use Let's Encrypt

- Cost savings – the certificates are free
- It has a collaborative nature and isn't controlled by any one organization
- Highly secure, by virtue of using open standards
- Easy to use and fully automated on supported platforms
- It is one of the most trustworthy CAs on the market today

Reasons to avoid Let's Encrypt

- Your platform and server type are not natively supported
- You need Organization Validation or Extended Validation certificates
- You don't have shell access to the server
- You don't have system administrator skills or expertise available
- Certificate cost is not an issue for your budget

Supported platforms and servers

- Uses a tool called Certbot for automatic installation and renewal
- Full automation available for Linux and Unix-like operating systems
- Natively supports Apache, Nginx, Haproxy, Plesk
- Possible to install manually or automatically on other platforms
- Would need to write custom scripts or use third-party contributed tools

Additional considerations

- Let's Encrypt certificates are valid for 90 days
- They recommend renewing automatically every 60 days
- Limit of 20 certificates per domain per week (up to 100 names per domain)
- Let's Encrypt wildcard certificates require domain control validation
- Let's Encrypt certificates are public

Indemnification

- Most CA user agreements include an indemnification clause
- US State/Local laws may forbid entering into contracts with indemnification
- Special contracts between US States and CAs not always negotiated
- Let's Encrypt has a provision specifically for US State/Local governments
- The indemnification clause does not apply where prohibited by law

Summary

- Let’s Encrypt offers free certificates and complete automation
- Native support is available for Linux and Unix-like operating systems
- Works well for Apache, Nginx and some hosted services
- Third-party tools are available for systems that are not natively supported
- Frequent renewal requirement makes non-automated use impractical