A Free Certificate Authority to Encrypt the Entire Web

Seth Schoen
Senior Staff Technologist,
EFF

Acronyms

- SSL (Secure Sockets Layer) – the old name for the main security layer for TCP
- TLS (Transport Layer Security) – the modern name for SSL
- HTTPS (HTTP Secure) – HTTP plus TLS
- X.509 – the format used by TLS certs
- PKI (Public Key Infrastructure) – an infrastructure for distributing crypto keys
- CA (Certificate Authority) – an entity that issues digital certificates in a PKI

Importance of TLS

- Still occasionally dealing with the idea that it's only needed for *financial data*
- … more often these days, the idea that it's only needed for *logins*

- We need to articulate a stronger vision that *networks are untrustworthy and communications need to be protected*
- Networks are routinely attacking us and plain HTTP offers no defense

Just a few examples

- Sidejacking and location tracking
- Integrity of software downloads
- Reader privacy (although size of documents is still an enormous problem)
- Content-based censorship prevention
- Protection against ad injection, tracking-header-injection and even malware injection at ISP

Barriers to adoption

- Perception that TLS is slow (especially for session establishment) or is very computationally intensive
- Difficulty integrating into some server and data center designs (like load balancing)
- *Cost and effort of obtaining and managing PKI certificates*
- Even a skilled person who understands PKI conceptually may take ~1 hour to get and deploy a cert … and then it may

Let's Encrypt

- Initially, a collaboration among EFF, University of Michigan, and Mozilla
  - to create a fully automated CA to issue certificates to any site for any purpose, quickly and at no charge
  - Aiming to be cheaper, easier, *and* more secure than existing CAs
- Thanks to partners including Akamai, Cisco, and IdenTrust, we have *publicly trusted* certificates accepted by browsers

Cross-signing

- Root CAs can and do delegate their authority to intermediate CAs — currently hundreds of named entities
- Browsers then *automatically trust* these intermediates; end-entity certs are almost always signed by intermediates, not roots
- Our CA is now cross-signed by IdenTrust; mainstream browsers trust us *today*; browser users don't have to install our CA's root certificate

Let's Encrypt concept

- Lowest level of validation for PKIX certificates is DV (Domain Validation) — verification by the CA that the applicant *controls the domain name* (or a server that the domain name is pointed at)
- Explicitly doesn't confirm the real-world identity of the applicant
- Very low marginal cost for each issuance!
- We can *replace the certificate authority with a very small shell script*

Let's Encrypt concept

- OK, there's actually a lot of engineering work plus work to comply with industry standards (Baseline Requirements and WebTrust audit), and so that “shell script” grew in size

- But DV certificate issuance can be fully automated in the common case, and that's what we're doing!

Let's Encrypt concept

- Client (user's web server) connects to server (Let's Encrypt CA) using a client application (that may be bundled with the OS or offered by a hosting or platform provider)

- We're developing a protocol called ACME (Automated Certificate Management Environment) to handle conversations about cert issuance

Let's Encrypt concept

- Client claims to control a particular name or names, and asks for a cert for them
- Server issues one or more *challenges* to ask the client to prove its control (and/or possibly prove control of other cryptographic keys)
- Client satisfies these challenges and server verifies this automatically, then issues cert and sends it over

ACME

- A JSON-based protocol for talking about certificate issuance and revocation, primarily invented by Richard Barnes
- Handling each step in our DV issuance process
- Centrally, challenging clients to prove that they control specific domains

Let's Encrypt status

- We're incorporated as the Internet Security Research Group (ISRG), a U.S. 501(c)(3) nonprofit, to operate the Let's Encrypt CA
- We built infrastructure, passed WebTrust PITRA audit, got cross-signature, and are in beta test now (issued 7,020 certs as of Nov. 7, when I wrote this slide)
- We welcome testing and collaboration to improve our client and service and integrate with more platforms

DVSNI

- One validation method we've developed that's stronger than existing manual DV challenges used by some CAs today
- Basically, the verifier asks the applicant to put up a self-signed cert containing certain server-provided information
- Then the verifier connects and negotiates a TLS session and checks that the cert does contain that information
- Proves *control of the web server itself*

Convenience

- We anticipate people who administer their own web servers will run something like

```
sudo apt-get install letsencrypt

sudo letsencrypt
```

  and the client will not only *obtain*, but also *deploy*, the new cert in less than a minute
- We're working on a client that will parse and write Apache and Nginx configs, and autorenew expiring certs

Safety

- We care a lot about avoiding misissuance and plan to adopt technologies to stop it
- We are publishing all certs in Google's Certificate Transparency system
- We're planning to prevent issuance for a domain that already has a valid cert unless the applicant can prove control of its subject key
- We can also have mechanisms for domains to ask us never to issue for

Wider integration

- We'd like to be integrated on every server OS or web server and every hosting and application platform
- The ACME protocol is in a standardization process at IETF and will be an open standard
- You can use the protocol to request certs from us without using our client software
- Contractual relationship isn't required, though we welcome new sponsors

Help!

- Please join the beta test program
  - Fill out a form with your domain names + e-mail address, then wait for e-mail confirmation
- Try out our service and report client or service bugs, and optionally send us patches
- Beta certs are fully “real” and mainstream browsers accept them now

Help!

- Integrating our client in your favorite OS or with your favorite web server
  - Or other server (ESMTP, IMAP, XMPP...)
- Packaging our client
- Integrating our client with your favorite hosting environment, CDN
- Testing our client (+ renewal) in your environment
- Translating our client

Help!

- Auditing our client or server
- Writing more tests
- Documenting our client (man pages, FAQ, introduction, explaining PKI, what key/cert/chain are)
- Documenting renewal and making sure it makes sense
- Getting more people interesting in shipping or integrating our client

Thanks!

You can contact me with any questions:

Seth Schoen <schoen@eff.org>
FD9A6AA2 8193A9F0 3D4BF4AD C11B36DC 9C7DD150

https://letsencrypt.org/

https://community.letsencrypt.org/ (for questions)

https://github.com/letsencrypt