Let's Encrypt

The Free CA for Web Site Encryption

Lee Lammert
St. Louis Linux User's Group
18 February 2016

ACRONYMS

- SSL (Secure Sockets Layer) – old name for the main TCP security layer
- TLS (Transport Layer Security) – current name
- HTTPS (HTTP Secure) – HTTP plus TLS X.509 (format for TLS certs)
- PKI (Public Key Infrastructure) – infrastructure for distributing crypto keys

WHY TLS?

- Not just for financial data or website logins
- Wide area networks are inherently untrustworthy
- Plain HTTP offers no defense

Risks - Attacks

- Sidejacking
- Location tracking
- Reader privacy
- Content-based censorship
- ISP header or advertisement injection

Issues

- Lower performance
- Inhibits load balancing
- Certificate cost
- Time consuming, error-prone, and complex to install and renew certificates

Current solutions

- Self-signed Certificates
  - Must be accepted in browser
  - Ignore signer for other ops
- Low-cost certificates
  - No validation other than domain ownership
  - No traceability

Let's Encrypt

- Initially, a collaboration among EFF, University of Michigan, and Mozilla
- Fully-automated Certificate Authority
- Publicly trusted in all major web browsers

Let's Encrypt

- Certificate authority [CA] entered public beta on December 3, 2015
- Free, automated X.509 certificates for Transport Layer Security encryption (TLS)
- Expires in 90 days
- Renewal easily automated

Validation

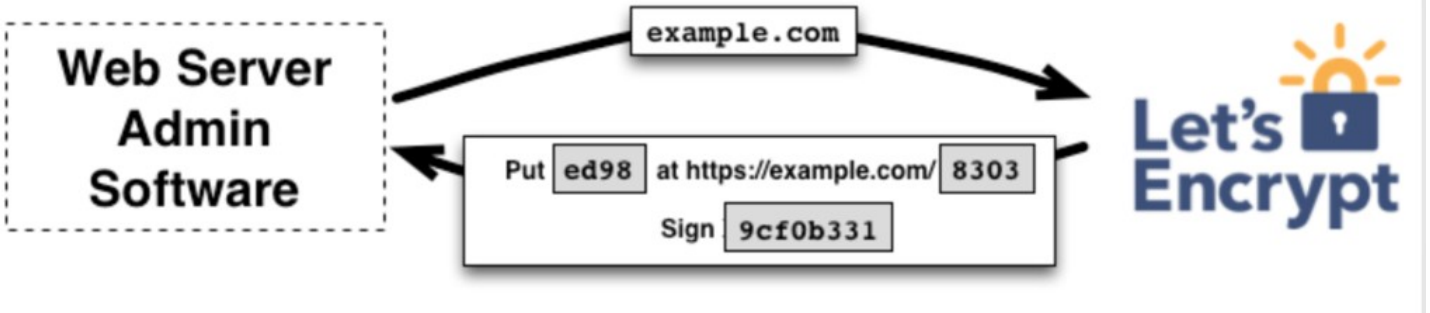
- Free certificates attest only that the applicant controls the domain
- Green Lock Symbol
- OV and EV are out of scope for now

Publicly Trusted

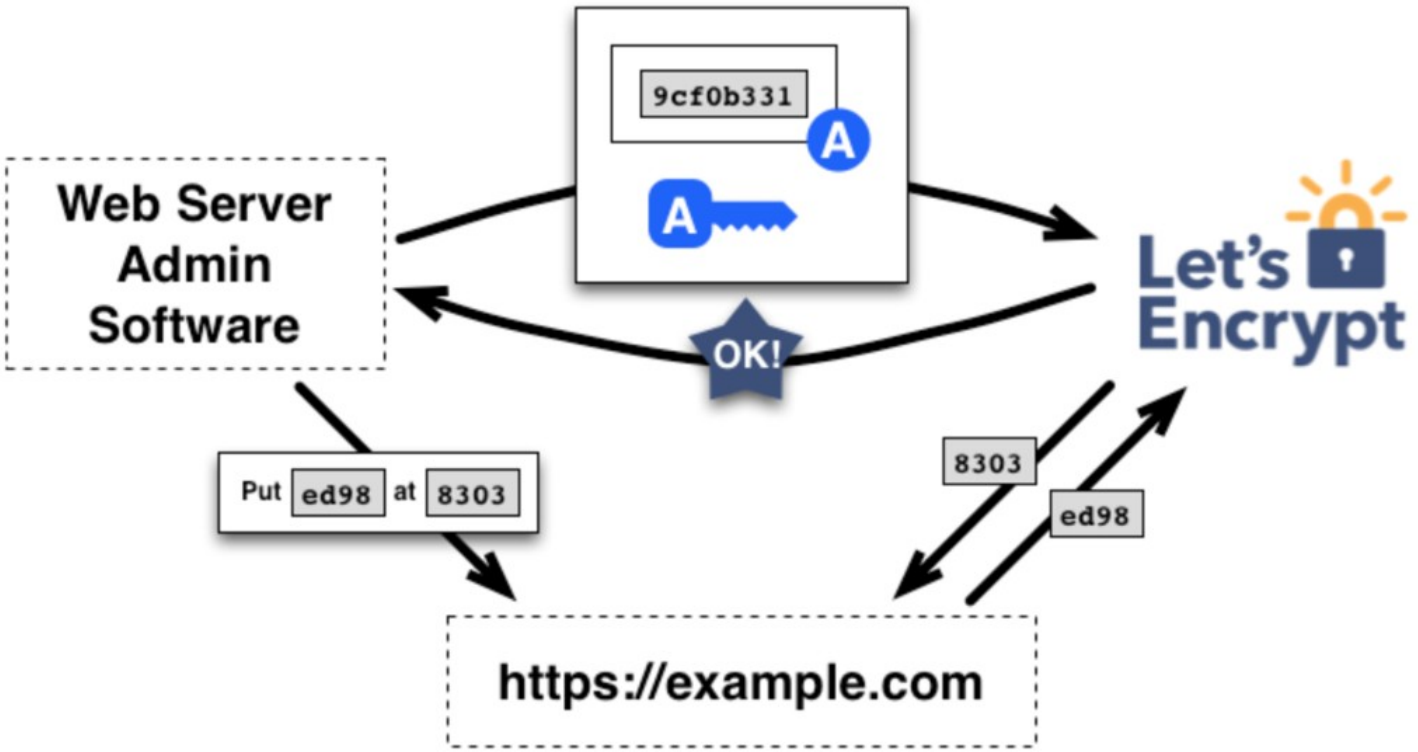
- Complies with WebTrust audit requirements
- Open Source software and specs
- Open Audits / Publication
- Browser root programs
- Cross-signatures from IdenTrust

Registration

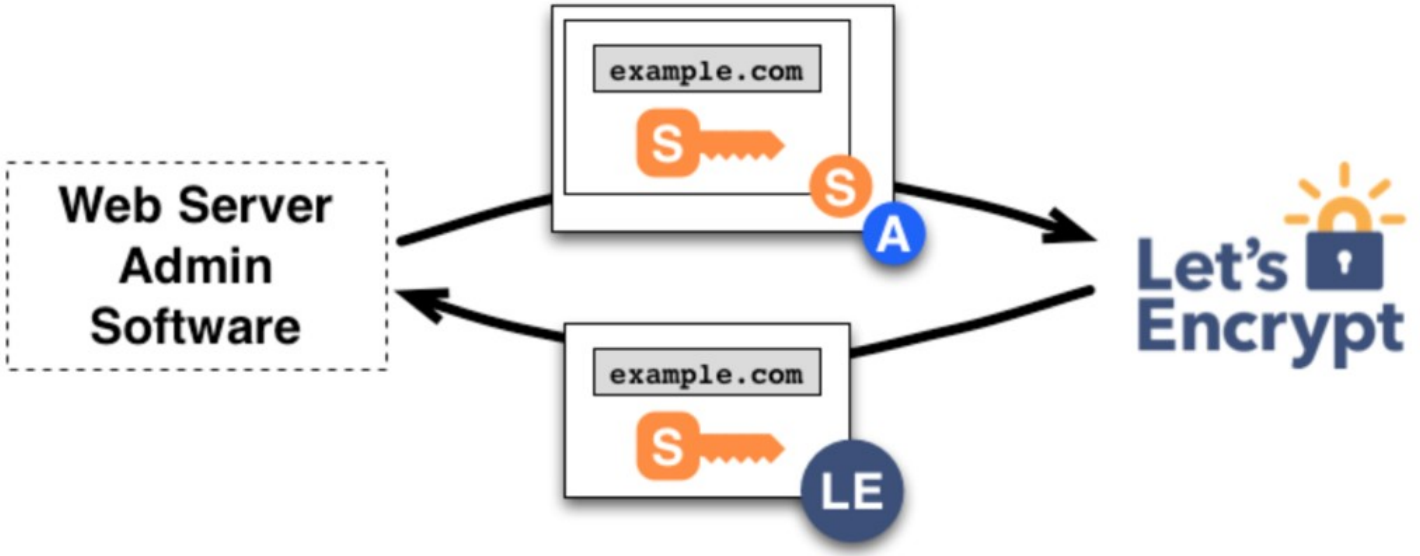
- For *open* web site (i.e. no authentication)



Validation


9cf0b331
A
A
Web Server
Admin
Software
OK!
Let's
Encrypt
Put
ed98
at
8303
8303
ed98
https://example.com

Issuance


Web Server
Admin
Software
example.com
S
S
A
example.com
S
LE
Let's
Encrypt

Process

- For a simple site, as easy as:
  - sudo apt-get install lets-encrypt
  - sudo lets-encrypt
- The lets-encrypt client will not only obtain, but also deploy, the new cert in less than one minute

Authenticated Sites

- Let's Encrypt client cannot automate process due to authentication requirement
- *standalone* method used, where the client supplies a server to respond to the handshake

Examples

- https://oc.omnitec.net
- https://nagios.omnitec.net

Credits

- Let's Encrypt @GatorLug
  J.C. Jones <jcjones@letsencrypt.org>