Let's Encrypt

PC-Treff-BB

Roland Egeler

Zielgruppe

- Betreiber von Webservern mit verschlüsselter Kommunikation
  - Webseite
  - Mailserver
  - Spieleserver
  - ...
- Eigentümer von Domains
- Computererfahrene Privatleute (Blogger...)
- Durchschnittliche Internetbenutzer eher nicht

Verschlüsselung für alle

- Englisch: „Let's encrypt!“
- Deutsch: „Lasst uns verschlüsseln!“

- Verschlüsselungsinitiative
- Zertifizierungsstelle

- Internet Security Research Group (ISRG)
- https://letsencrypt.org

ISRG

- Gemeinnützige Organisation
- Sponsoren
  - EFF (Electronic Frontier Foundation)
  - Mozilla
  - Google Chrome
  - Akamai (CDN)
  - Cisco
  - u.v.a.m.

Motivation

- Möglichst allen Netzwerkverkehr im Internet verschlüsseln
- Zertifikate leicht zu bekommen
- Automatisierung
- Leichte Einbindung in Infrastruktur
- Kostenlos
- Abhören erschweren bzw. verteuern (Geheimdienste)

Motivation für Privatanwender

- Nicht öffentlich einsehbare eigene Webseiten
- Private Daten sollen nicht in Suchmaschinen landen
- Webseiten per Benutzername und Passwort absichern
- Ohne Zertifikate nur http möglich
- Bei http werden Benutzername und Passwort im Klartext übertragen
- Weitere zu vermeidende Protokolle:
  - telnet, ftp, smtp, pop3, imap...

Motivation für Privatanwender

- Bei Klartextpasswörtern sehr einfache „Man in the middle“-Attacke möglich
- Situation häufiger als gedacht
- Mobilgeräte in fremdem WLAN
- WiFi-Geräte verbinden sich mit jedem Access Point, der eine bekannte SSID und das passende Passwort hat
- Https verhindert einfache Attacken
- Geheimdienste können hier vielleicht mehr
- Sichere Algorithmen und Schlüssellängen beachten

Motivation für Privatanwender

- Eigenen Mailserver sicher betreiben
- Unabhängigkeit vom Provider
- Kontrolle über E-Mails
- Eigenes Backup
- Bei großen Mails nicht auf Versendung warten
- Siehe auch PC-Treff Vortrag vom April 2011

Unterstützte Protokolle

- Alles, was TLS (SSL) benutzt
  - https (Webserver)
  - imaps (Mailserver)
  - pop3s (Mails abholen)
  - smtps (Mails verschicken)
  - sips (IP-Telefonie)
  - ssh (An Rechner anmelden)
  - scp (Daten zwischen Rechnern austauschen)
  - OpenVPN (Virtuelles privates Netzwerk)
  - ...

Zertifikate

- Selbst Zertifikat erstellen ist einfach
- Mittels „openssl“ (Open Source)
- Zertifikatstyp „X.509“
- Verschlüsselung ist sicher
- Problem „Vertrauen“: Zertifikat wird vom Aussteller selbst beglaubigt
- Browser und Mailprogramme werfen bei selbst unterschriebenen Zertifikaten Fehler
- Wenn der Benutzer dem Zertifikat vertraut, verschwinden die Fehlermeldungen
- Nutzer muss selbst handeln, sperrig

Zertifikate

- „Offizielle“ Zertifikate werden von externen Zertifizierungsstellen unterzeichnet (beglaubigt)
- CA (Certification Authority: Bsp: Comodo, Symantec, GoDaddy, GlobalSign > 88%)
- Kostet normalerweise Geld
- Stammzertifikat muss im Browser hinterlegt sein, sonst wie selbstausgestellt
- Vorteil ISRG: Mit Mozilla und Chrome sind schon die meisten Browser im Boot
- Stammzertifikat wird mit ausgeliefert

Zertifikate

- Vertrauensstufen von Zertifikaten
  - DV (Domain Validation)
  - OV (Organisation Validation)
  - EV (Extended Validation)
- Vorteil EV: Browser hebt EV-Zertifikate in Addresszeile hervor
- Siehe z.B. Banken

Stufen der Vertrauenswürdigkeit

- DV
  - Domain Validation: Der Antragsteller muss nur beweisen, dass er die Domain unter Kontrolle hat
- OV
  - Organisation Validation: Der Antragsteller muss sicherstellen, dass er der beantragenden Organisation angehört
- EV
  - Extended Validation: Die Zertifizierungsstelle überprüft, ob der Antragsteller das Recht besitzt, die Domain zu verwenden

Challenge Verfahren

- Let's Encrypt stellt nur DV-Zertifikate aus
- Vorgehensweise zum Beweis der Kontrolle
  - Der Antragsteller fordert Zertifikat an
  - Let's Encrypt fordert ihn auf, unter einem bestimmten Pfad in der Domain eine Datei mit einem bestimmten Namen und einem bestimmten Inhalt bereitzulegen.
  - Wenn Let's Encrypt genau diese Daten findet, wird das Zertifikat ausgestellt und bereitgestellt.

Manuelle Vorgehensweise

- Benutzung von Befehlen auf der Kommandozeile
- Installation der Software z.B. von github oder über Paketverwaltung der Distribution
- Best Practice:
  - Eigenen Server stoppen
  - Software startet eigenen Webserver und beantwortet Challenge selbsttätig
  - Ergebnis: Zertifikate auf der Platte
  - Zertifikate händisch installieren
  - Eigenen Server wieder starten

Alternative Vorgehensweise

- Alternative:
  - Eigenen Server laufen lassen
  - Challenge händisch auf dem Webserver einrichten
  - Vorteil: Challenge kann auch über https ablaufen
  - Ergebnis: Zertifikate auf der Platte
  - Zertifikate händisch installieren
  - Eigenen Server neu starten

Automatische Vorgehensweise

- Regelmäßiges Auffrischen per Skript
  - Per Eintrag in die Crontab
  - 0 0 1 */2 * /opt/letsencrypt/letsencrypt-auto certonly --config /opt/letsencrypt/cli.ini --webroot -w /var/www/html/ -d beispiel-de-domain.de -d www.beispiel-de-domain.de
  - Inhalt cli.ini:
  - agree-tos
  - renew-by-default = True

Beispiel

- ./letsencrypt-auto certonly --standalone -d beispiel-de-domain.de -d www.beispiel-de-domain.de
  - --standalone: Starte eigenen Server
  - certonly: Nur Zertifikate, keine automatische Änderung der Serverkonfiguration
- Problem: Für eigenen Webserver werden root-Rechte benötigt
- Man muss aus dem Netz geladene Software mit hohen Rechten starten
- Paranoia...

Aktualität der Beispiele

- Die Entwicklung von Let's Encrypt schreitet rasch voran
- Bisher wurde jedesmal bei Erneuerung der Zertifikate die Software neu geladen
- Neuer Befehl namens „certbot“
- Skripte und Parameter möglicherweise jetzt anders
- Manual lesen hilft

Gültigkeitsdauer

- Von Let's Encrypt ausgestellte Zertifikate sind im Moment nur 90 Tage gültig
- Bei automatischer Erneuerung kein Problem
- Bei händischer Erneuerung eventuell Termindruck
- Bei Erstbeantragung wurde Mailadresse hinterlegt
- Es werden Erinnerungsmails verschickt (dreistufig)

Wildcard-Zertifikate

- Let's Encrypt plant ab Anfang 2018 Wildcard-Zertifikate
- Beispiel: *.beispiel-de-domain.de
- Zertifikat wäre gültig für alle denkbaren Subdomains
  - www.beispiel-de-domain.de
  - news.beispiel-de-domain.de
  - beispiel.beispiel-de-domain.de
  - ...

Quellen

- https://letsencrypt.org
- https://de.wikipedia.org/wiki/Let's_Encrypt
- https://de.wikipedia.org/wiki/Extended-Validation-Zertifikat
- https://willy-tech.de/ssl-zertifikat-mit-lets-encrypt-erstellen/
- https://www.digitalocean.com/community/tutorials/how-to-use-certbot-standalone-mode-to-retrieve-let-s-encrypt-ssl-certificates
- https://dominicpratt.de/lets-encrypt-nutzen-eine-anleitung/

Vielen Dank!