Let’s Encrypt – nahoďte šifrování na webu

Petr Krčmář

5. března 2016

Prezentace už teď na webu

https://www.petrkrcmar.cz

ROOT.CZ vpsFree.cz

Proč nasazovat HTTPS?

- HTTPS není jen pro banky a mail
- autenticita přenášených dat
- odposlech je považován za útok (RFC 7258)
- pozměňování přenosů, supercookies, malware
- ochrana osobních údajů
- zabránění únosu session cookie
- možnost nasazení HTTP/2 – výkon

Proč nasazovat HTTPS?

- HTTPS není jen pro banky a mail
- autenticita přenášených dat
- odposlech je považován za útok (RFC 7258)
- pozměňování přenosů, supercookies, malware
- ochrana osobních údajů
- zabránění únosu session cookie
- možnost nasazení HTTP/2 – výkon
- SSH je normální, proč používat telnet?

Problém: důvěryhodné předání klíče

- autentizace stejně důležitá jako silná šifra
- problém důvěryhodného předání veřejného klíče
- nastupují autority: důvěryhodní prostředníci
- ověří žadatele, vystaví certifikát
- veřejný dokument, který obsahuje hlavně:
  - jméno autority
  - doménová jména
  - veřejný klíč žadatele
  - podpis autority
  - a další

Řetězec důvěry

- software zná kořenové certifikáty
- od serveru dostane řetězec
- certifikáty se musí vzájemně potvrzovat
- konečný certifikát potvrzuje identitu
- zároveň obsahuje veřejný klíč
- identita je potvrzena, klíč předán
- komunikace může začít
- existuje asi 1000 důvěryhodných CA

Největší překážky v nasazení

- generování klíčů a žádostí
- hledání autority
- cena certifikátu a vůbec nutnost zaplatit
- složité kolečko s ověřováním
- nutnost hlídat si platnost
- po roce až třech nutno opakovat
- = moc práce, kašlu na to

Let’s Encrypt

- projekt EFF, Mozilla Foundation, Akamai a Cisco Systems
- plus další partneři
- certifikační autorita
- představena v listopadu 2014
- veřejná beta běží od prosince 2015

Vlastnosti LE

Let’s Encrypt to chce dělat:

- **Zdarma** – stačí vlastnit doménu/ovládat server
- **Automaticky** – vše vyřídí stroje mezi sebou
- **Průhledně** – vystavení i revokace jsou zveřejněny
- **Otevřeně** – protokol i software jsou otevřené

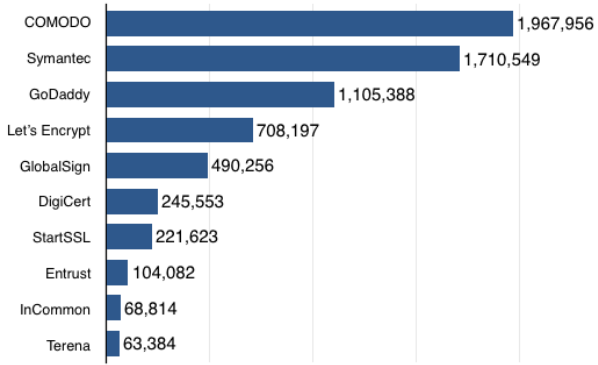
Vlastnosti LE

Let’s Encrypt to chce dělat:

- **Zdarma** – stačí vlastnit doménu/ovládat server
- **Automaticky** – vše vyřídí stroje mezi sebou
- **Průhledně** – vystavení i revokace jsou zveřejněny
- **Otevřeně** – protokol i software jsou otevřené

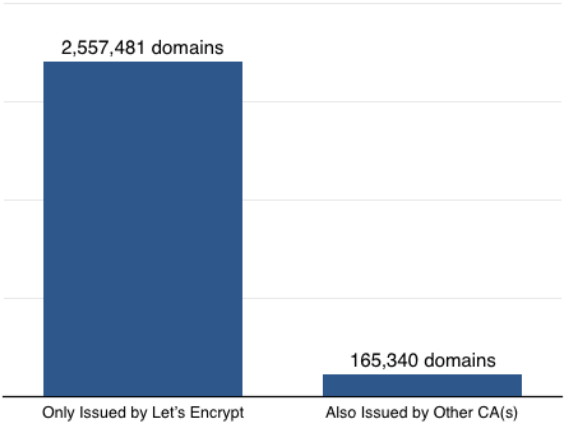
... a autority nebudou mít co žrát!

Počet vystavených certifikátů



(J.C.Jones, 16. února 2016)

Počet zabezpečených domén

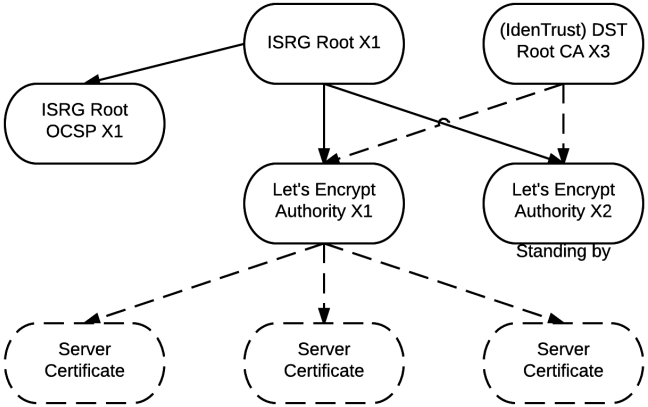


(J.C.Jones, 19. února 2016)

Technickou řečí

- protokol ACME
  - Automated Certificate Management Environment
  - JSON nad HTTPS
- automatické utility
- ověření pomocí výzev v /.well-known/
- nebo DNS _acme-challenge.<doménové jméno> TXT ”hex řetězec”
- vygenerujete klíč, dostanete certifikát a chain
- kořen není v prohlížečích – zatím
- cross-sign IdenTrust („DST Root CA X3“ Root CA)
- výchozí utilita konfiguruje web server
- existuje celá řada dalších implementací

Cross-signing



Vlastnosti certifikátů

- pouze DV certifikáty
- nevystavují wildcard (hvězdička)
- platnost 3 měsíce
- možnost SAN (Subject Alternative Name)
- limit je 100 jmen v certifikátu
- možnost kdykoliv obnovit
- možnost revokace (pokud máte klíče)
- všechny žádosti i certifikáty jsou veřejné

Pozor na rate limiting

- 100 jmen v certifikátu
- 5 žádostí v jedné doméně (SLD) za týden
- 500 registrací z jedné IP za 3 hodiny
- 300 nedokončených žádostí za týden – pro vývojáře
- existuje testovací (staging) prostředí bez limitů

Kompatibilita s klienty

- Funguje to:
  - Android >= 2.3.6 (asi 2%)
  - iOS >= 3.1
  - Windows >= Vista
  - všechny současné distribuce
  - Firefox a Thunderbird >= 2.0 (od roku 2008)
  - Chrome
- Nefunguje to:
  - Pidgin (mají ticket 16835)
  - Java (nemá „DST Root CA X3“)
  - Blackberry OS 10, 7 a 6
  - Windows XP (ani SP3)

Proč Windows XP

- zastaralé CryptoAPI (používá IE, Chrome, Safari…)
- před SP3 neumí SHA256, SP3 neumí SNI a hlavně…
- nerozumí namespaces (Name Constraint) – RFC 5280
- mezilehlý cert IdenTrust zakazuje doménu .mil
- je kritický – neznámý – zamítne se
- Firefox má vlastní validační kód
- do 22. března to chtějí opravit

Ukázka Name Constraint

```
$ openssl x509 -noout -text < intermed.pem
…
        X509v3 Name Constraints:
            Excluded:
             DNS:.mil
…
```

Klienti

- letsencrypt – oficiální klient, maximální automatika
- letsencrypt-nosudo – jednodušší a malý (jeden soubor)
- letsencrypt_simpleclient – knihovna v Pythonu
- acme-tiny – jen 200 řádků kódu
- simp_le – jednoduchý, bezestavový, trochu automatický
- tyhle jsou v Pythonu ↑
- existují v PHP, Go, Ruby, .NET
- dokonce i ve webovém prohlížeči
- viz gethttpsforfree.com

(Zdroj)

Praktická ukázka nasazení

- použijeme simp_le u samostatného uživatele
- předkonfigurovaný Nginx – cesta pro /.well-known/
- máme samostatný adresář s identitou
- poté jen spustíme jeden příkaz

Spuštění skriptu

```
./simp_le.py -d debian-linux.cz:/home/letsencrypt/webroot/ \
-d www.debian-linux.cz:/home/letsencrypt/webroot/ \
-d forum.debian-linux.cz:/home/letsencrypt/webroot/ \
-f account_key.json -f key.pem -f fullchain.pem \
--reuse_key
```

- při opakování se jen zkontroluje platnost (30 dnů)
- pak už stačí jen ukázat web serveru cert a klíč

Čím to otestovat?

- SSL Labs Test – velmi podrobný test
- SSL Decoder – vypíše všechny detaily o certifikátech
- Symantec CryptoReport – protokoly, chyby, díry
- GeoCerts SSL Checker – ukazuje řetězec
- COMODO SSL Analyzer – a ještě jeden
- gcr-viewer v balíčku gnome-keyring

```
openssl s_client -showcerts -connect www.root.cz:443 < \
/dev/null | openssl x509 -outform DER > cert.der
```

Pár technických poznámek

- TLSA – není problém, klíč se nemusí měnit
- HSTS preload – také není problém
- LE neumí (do dubna opraví) IPv6 – problém u (Neběží.cz)
- mezilehlý jen RSA (kořen samozřejmě taky) – do dubna ECDSA
- pozor na posílání řetězce (mezilehlý)

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz