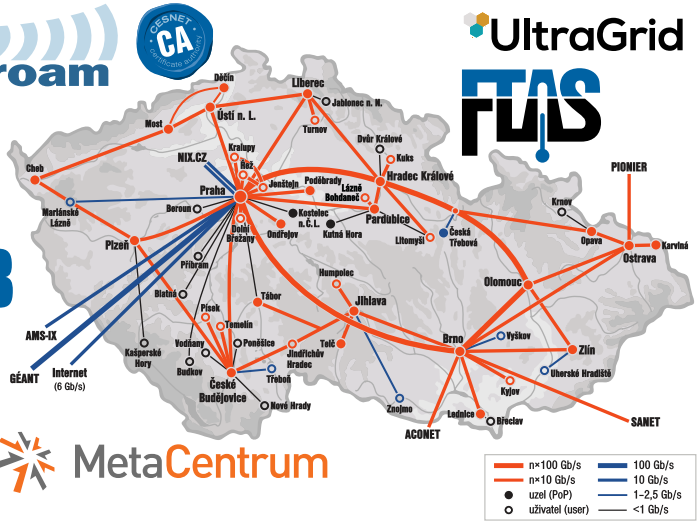
Pojďme šifrovat!

aneb ACME, továrna na certifikáty

Ondřej Caletka

11. října 2015

O sdružení CESNET



n×100 Gb/s — 100 Gb/s
n×10 Gb/s — 10 Gb/s
uzel (PoP) — 1–2,5 Gb/s
uživatel (user) — <1 Gb/s

Obsah

V minulosti od Electronic Frontier Foundation

- SSL observatory
  - sken certifikátů na portu tcp/443 celého IPv4 prostoru
  - odhalena tisícovka *důvěryhodných* autorit
  - odhaleny zásadní přešlapy certifikačních autorit
- přesvědčování hlavních poskytovatelů obsahu o nutnosti šifrování
  - přinejnemším jako alternativu
- rozšíření HTTPS everywhere pro prohlížeče

HTTPS by mělo být všude

- stále panuje představa, že HTTPS je jen pro bankovnictví nebo přihlašování
- dokumentované případy přidávání supercookies či exploitů do HTTP komunikace
- je obtížné rozlišovat citlivá a necitlivá data
  - citlivý může být i seznam hesel hledaných na wikipedii, popř. seznam článků čtených na zpravodajském serveru
- minimální overhead šifrování na dnešním hardwaru
- HTTP/2 resp. SPDY je dostupné jen se šifrováním
  - především kvůli transparentním proxy serverům

http://www.root.cz/clanky/https-by-melo-byt-vsude

CESNET

Konfigurace TLS je obtížná

1. vygenerovat klíče a žádost
2. najít a často i zaplatit certifikační autoritu
3. nainstalovat certifikát
4. nastavit bezpečně další volby
5. hlídat konec platnosti
6. celý postup opakovat každé 1 – 3 roky

Blokování smíšeného obsahu

- prohlížeče do HTTPS stránky nenačtou HTTP objekty
- problém při migraci HTTP webu na HTTPS
- dá se řešit přepsáním absolutních odkazů z `http://` na `//`
- k přepisu dochází jako vedlejší efekt zavedení HSTS, popř. HPKP hlaviček
- nová hlavička pro automatický přepis na místo blokování: `Content-Security-Policy: upgrade-insecure-requests`

Projekt Let’s Encrypt

- společný projekt EFF, Mozilla, University of Michigan a dalších
- cílem je eliminovat problémy při zavádení TLS
- transparentně, plně automaticky a zdarma

Součásti Let’s Encrypt

boulder	automatická certifikační autorita
ACME	protokol pro automatizaci vydávání certifikátů
letsencrypt	ACME klient s automatickou konfigurací TLS software

Autorita Let’s Encrypt

Autorita Let’s Encrypt

- plně automatizovaná certifikační autorita
- vydává pouze DV certifkáty pro TLS
- transparetní provoz
  - všechny certifikáty zveřejněné
  - sériová čísla tvoří posloupnost
  - zveřejněné logy průběhu žádostí a validace
- open-source software v jazyce Go

Validace držení domény

- vystavením souboru na určené cestě HTTPS / HTTP serveru
- vystavením certifikátu na určené jméno (DVSNI)
- vystavením DNS TXT záznamu s určeným obsahem
- důkazem **držení privátního klíče stávajícího certifikátu**
  - pro domény, které mají v době žádosti platný certifikát od jiné autority
  - zabraňuje vylákání certifikátů např. únosem IP adres
  - riziko *lock-out* při ztrátě privátního klíče

Platnost a revokace

- certifikáty *pravděpodobně* s platností 3 měsíce
- revokace zdarma a automatizovaně
- možnost získat certifikát na více jmen (multi SAN)
- wildcard certifikáty *zatím* nedostupné
  - obvykle nejsou potřeba
  - obtížná validace pomocí HTTPS
  - protokol ACME na ně zatím není připraven

Automatic Certificate Management Environment

Tradiční postup získání certifikátu

1. zřídit uživatelský účet
2. požádat o validaci domény
3. splnit podmínky validace
4. odeslat žádost o certifikát
5. vyčkat na vydání certifikátu
6. stahnout certifikát
7. nakonfigurovat TLS software

Všechny tyto kroky vyžadují manuální práci operátora.

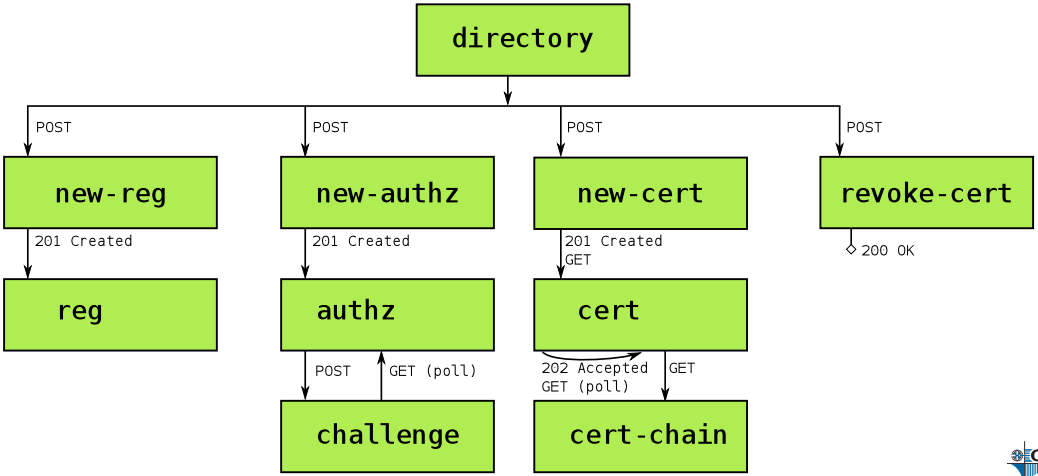
Protokol ACME

- draft stejnojmenné pracovní skupiny IETF
- používá JSON nad HTTPS
- autentizace serveru (CA) pomocí TLS
- autentizace klienta pomocí JOSE (JWS)
- požadavek na *HTTP Public Key Pinning* hlavičky
- ochrana proti opakování HTTP hlavičkou `Replay-Nonce`

JSON Object Signing and Encryption

- pracovní skupina IETF s cílem vytvořit standard pro šifrování a autentizaci JSON dokumentů
- definuje standardní JSON struktury
  - JWK JSON Web Key
  - JWS JSON Web Signature
  - JWE JSON Web Encryption
  - JWA JSON Web Algorithms
- v poli `payload` je base64 kódovaná zpráva, často JSON

Komunikace v ACME



Registrace účtu

- klient vygeneruje pár klíčů
- odešle prázdnou zprávu s volitelnými kontaktními informacemi
- autorita odpoví registračním objektem
- klient může požádat o klíč pro obnovu
  - umožňuje vyměnit pár klíčů pro daný účet, příp. obnovit účet při ztrátě privátního klíče
  - klíč pro obnovu je získán ECDH algoritmem z náhodného tajemství klienta i autority

Zádost o validaci

- klient požádá o validaci dané domény
- autorita oveří požadavek, vytvoří objekt žádosti a specifikuje validační výzvy
- klient splní výzvu a odešle zprávu
- autorita provede validaci a změní objekt validace podle výsledku

Validace metodou SimpleHTTP

- autorita vygeneruje náhodný token
- klient připraví odpověď obsahující token
- tuto odpověď vystaví na HTTP(S) serveru validované domény, na cestě `/.well-known/acme-challenge/<token>`
  - se správným MIME typem `application/jose+json`
  - v případě HTTPS na certifikátu nezáleží
- stejnou odpověď pošle ACME autoritě, ta na jejím základě spustí ověření

Validace metodou DVSNI

- autorita vygeneruje náhodný token
- klient připraví odpověď obsahující token
- vytvoří SHA-256 otisk podpisu odpovědi
- vygeneruje self-signed certifikát na jméno `<otisk podpisu>.acme.invalid`
- nastaví na HTTPS serveru nový virtuální server na uvedené jméno, kam nakonfiguruje vygenerovaný certifikát
- odešle odpověď ACME autoritě, ta naváže spojení na HTTPS server se SNI hlavičkou obsahující speciální jméno
- validace bude úspěšná, pokud autorita dostane certifikát vystavený na dané jméno

Validace metodou DNS

- autorita vygeneruje náhodný token
- klient připraví odpověď obsahující token
- podpis odpovědi vystaví jako TXT záznam na adrese `_acme-challenge.<validovaná doména>`
- odešle odpověď ACME autoritě

Validace důkazem držení privátního klíče

- autorita vytvoří seznam akceptovaných certifikátů
- klient vytvoří zprávu obsahující validované doménové jméno a veřejný klíč ACME účtu
- zpráva je podepsána privátním klíčem jednoho z akceptovaných certifikátů
- validační zpráva nemusí obsahovat `Replay-token` – je možné vytvořit ji off-line, např. při převodu domény

Vydání a revokace certifikátu

Vydání certifikátu

- klient vygeneruje standardní CSR žádost, podepíše svým ACME klíčem a předá autoritě
- autorita odpoví URL certifikátu, kterou klient dotazuje
- autorita může certifikát sama obnovovat bez přičinění klienta

Revokace certifikátu

- klient podepíše certifikát svým ACME klíčem a předá autoritě
- autorita certifikát revokuje

Objevená zranitelnost znovupoužití podpisů

$$signature = function(message, privatekey) \quad (1)$$

- při validaci autorita ověřuje podpis JOSE zprávy
- útočník může vytvořit svou vlastní validační zprávu
- následně vypočítá privátní klíč tak, aby podpis odpovídal
- provede obnovu účtu, použije nově vypočítaný klíč
- odešle vlastní zprávu podepsanou novým klíčem – hodnota podpisu se bude rovnat hodnotě podpisu oběti

Řešeno v novém návrhu kontrolou veřejného klíče signatáře.

ACME klient `letsencrypt`

ACME klient `letsencrypt`

- klientská utilita pro komunikaci s ACME-kompatibilními autoritami
- open-source software v jazyce Python 2.7
- kompletní správa životního cyklu TLS certifikátů
- modulární architektura, připravené moduly pro Apache a NGINX
- kromě získání certifikátu jsou i bezpečně nakonfigurovány TLS volby
  - s volitelným přesměrováním HTTP na HTTPS a HSTS
  - při spuštění *snad i* s hlavičkou `Content-Security-Policy: upgrade-insecure-requests`

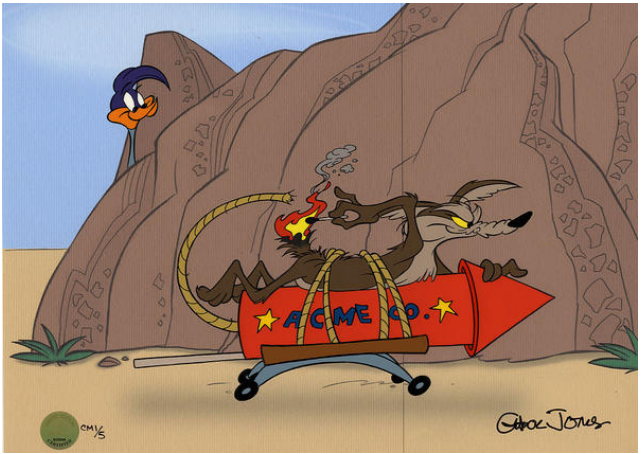
Možnosti ručního získání certifikátu

- vestavený HTTPS server v `letsencrypt`
  - provede důkaz, pokud provozujete jiný server než Apache/NGINX
  - je však nutné na okamžik zastavit ostatní servery na portu 443
- kompletně manuální validace metodou SimpleHTTP
  - utilita vás vyzve k vystavení daného souboru na web serveru
  - po vystavení důkaz ověří nejprve `letsencrypt`, pak požádá autoritu
  - v tomto režimu nemusí `letsencrypt` běžet na serveru, pro který je získáván certifikát

Ukázka letsencrypt v praxi

https://youtu.be/Gas_sSB-5SU

```
# ./venv/bin/letsencrypt -vv --redirect run
```



Nedostatky vývojové verze

- IPv4-only
  - validace IPv6-only doménového jména selže `Host not found`
  - žádost a validaci domény hostované na IPv6-only DNS serverech selže na interní chybu
- parsování příkazového řádku neodpovídá dokumentaci
  - záleží na pořadí parametrů
  - správné je jiné než uvedené v nápovědě ☺
- špatně ošetřené chybové stavy
- velmi omezená dokumentace
  - bez zmínky o automatickém udržování certifikátů

Závěr

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
http://Ondřej.Caletka.cz

- !SECURITY Fest! 21. října
- poslední exkurze v 15:00
- soutěž o ceny na stánku

FAQ

Vztah Let’s Encrypt a DANE

DNS-based Authentication of Named Entities

- použití DNSSEC pro pinning TLS certifikátů
- teoreticky nahradí DV certifikáty
- zcela jiný bezpečnostní model
- naráží na rozbitost DNS v koncových sítích

Let’s Encrypt

- tradiční CA, jen s novým přístupem
- automatizace pomůže i zavedeným autoritám
- ideální pro kombinaci s DANE

HTTP Strict Transport Security

- speciální HTTP hlavička, platná pouze na HTTPS spojení s validním certifikátem
- sdělí prohlížeči, že všechny další požadavky k tomuto serveru mají jít výhradně prostřednictvím `https`
- odkazy na `http://` jsou automaticky přepisovány v prohlížeči
- selhání TLS validace nemůže uživatel obejít
- dlouhá životnost hlavičky (typ. půl roku), možnost editace životnosti pouze majitelem, platnost i na subdomény
- některé adresy mají HSTS předinstalováno ve zdrojovém kódu prohlížeče

`https://tools.ietf.org/html/rfc6797`

CESNET