Certificate Transparency

povinně zveřejněné certifikáty

Petr Krčmář

19. dubna 2018

Prezentace už teď na webu

www.petrkrcmar.cz

ROOT.CZ vpsFree.cz

Funguje PKI (?)

- funguje naprosto skvěle!

Funguje PKI (?)

- funguje naprosto skvěle!
- až na případy, kdy to selhává

Funguje PKI (?)

- funguje naprosto skvěle!
- až na případy, kdy to selhává
- autority jsou „univerzálně důvěryhodné“
- kdokoliv vystavuje cokoliv
- DigiNotar, Thawte, Symantec, WoSign…
- technická chyba, omyl, útok, státní zájmy
- řetěz je silný jako nejslabší článek
  - bezpečnost neurčuje nejlepší, ale nejhorší
  - jedno shnilé jablko zničí celý košík

Provozovatelé se bojí

- provozovatelé služeb se bojí
- PKI je jedinou ochranou
- robustní, ale stojí na bezpečnosti autorit
- pokud selže, může se kdokoliv vydávat za kohokoliv
- typicky Google, Microsoft, Apple, GitHub…
- ukradení přihlašovacích údajů, odposlech
- vkládání vlastních informací
- platný certifikát = internetová identita
- trvá dlouho problém odhalit a vyřešit

ROOT.CZ vpsFree.cz

Řešení = transparentnost

- donutit autority zveřejňovat všechny certifikáty
- možnost monitoringu i zpětného auditu
- pokud někdo vydá neoprávněně, můžu reagovat
- spustím poplach, můžu revokovat
- mám přehled o všech vydaných certifikátech
- autority se dostávají pod veřejnou kontrolu
- hlídám své domény, kdokoliv hlídá cokoliv

Certificate Transparency

- veřejné logy pro ukládání certifikátů
- lze do nich jen přidávat (Merklův hashový strom)
- kdokoliv je může mirrorovat a prohledávat v nich
- kdokoliv může přidávat certifikáty
- kvůli ochraně ale pouze od uznávaných CA
- odstranění certifikátu je detekovatelné
- není možné antedatovat certifikáty
- definováno v RFC 6962

Historie a budoucnost

- první log spustil Google v březnu 2013
- v září 2013 začala první CA vkládat (DigiCert)
- od 1. ledna 2015 vyžaduje Chrome pro EV
  - přítomnost alespoň ve dvou lozích
- od 1. června 2016 vyžaduje u všech od Symantec
- od 30. dubna 2018 bude **vyžadováno u všech**
- (původně to měl být už říjen 2017)
- Let’s Encrypt posílá od začátku
- Firefox oznámil podporu, ale bez termínů

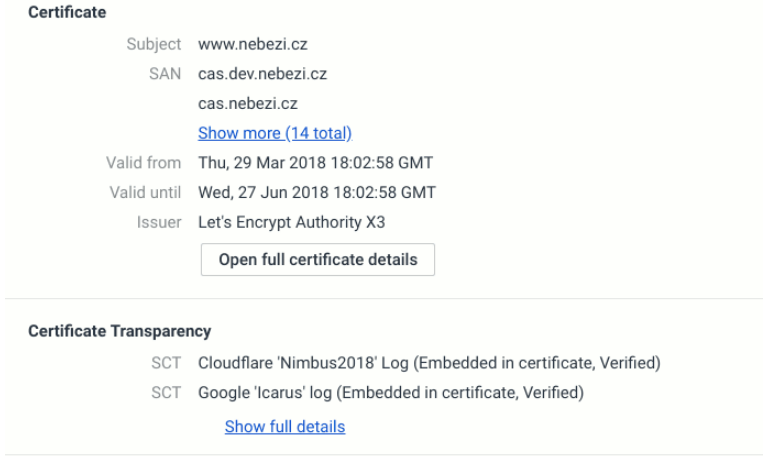
ROOT.CZ vpsFree.cz

Jak autority donutit

- bude fungovat, jen když to budou dělat všichni
- musí existovat donucovací mechanismus
- je zabudován do prohlížeče
- prohlížeč zkontroluje že je certifikát v logu
- (kromě data platnosti, domény a podobně)
- jen takový certifikát bude důvěryhodný
- technicky se vynutí zveřejňování certifikátů

Klient se neptá

- klienti se sami ptát nebudou
- to by neškálovalo a unikaly by informace
- důkazní břemeno je na serveru (uživateli certifikátu)
- ten musí doložit, že je certifikát v logu
- ideálně ho vloží už CA, ale může i sám
- log vydává Signed Certificate Timestamp (SCT)
  - příslib budoucího zařazení certifikátu do stromu
  - server musí klientovi doručit i SCT
- Let’s Encrypt doručuje SCT od 29. března 2018


Certificate
Subject www.nebezi.cz
SAN cas.dev.nebezi.cz
cas.nebezi.cz
Show more (14 total)
Valid from Thu, 29 Mar 2018 18:02:58 GMT
Valid until Wed, 27 Jun 2018 18:02:58 GMT
Issuer Let's Encrypt Authority X3
Open full certificate details
Certificate Transparency
SCT Cloudflare 'Nimbus2018' Log (Embedded in certificate, Verified)
SCT Google 'Icarus' log (Embedded in certificate, Verified)
Show full details

Tři způsoby doručení

1. OCSP stapling
   - složité a nespolehlivé (umí prohlížeč OCSP?)
   - server i autorita musí spolupracovat
   - autorita získá SCT a vloží do OSCP responderů
   - server musí podporovat stapling
   - s OCSP zprávou předává i SCT

Tři způsoby doručení

1. OCSP stapling
   - složité a nespolehlivé (umí prohlížeč OCSP?)
   - server i autorita musí spolupracovat
   - autorita získá SCT a vloží do OSCP responderů
   - server musí podporovat stapling
   - s OCSP zprávou předává i SCT
2. rozšíření TLS
   - server pošle certifikát a získá SCT
   - změní konfiguraci web serveru (podpora?)
   - rozšíření TLS signed_certificate_timestamp

Tři způsoby doručení

1. OCSP stapling
   - složité a nespolehlivé (umí prohlížeč OCSP?)
   - server i autorita musí spolupracovat
   - autorita získá SCT a vloží do OSCP responderů
   - server musí podporovat stapling
   - s OCSP zprávou předává i SCT
2. rozšíření TLS
   - server pošle certifikát a získá SCT
   - změní konfiguraci web serveru (podpora?)
   - rozšíření TLS signed_certificate_timestamp
3. rozšíření certifikátu
   - nulová zátěž na provozovatele serveru
   - vše zařídí CA, pošle do logu, získá SCT
   - SCT je pak přímo součástí certifikátu

ROOT.CZ vpsFree.cz

Současný stav logů

- v tuto chvíli je v Chrome uznáváno 15 logů
- Certly, DigiCert, Izenpe, Google (4)…
- jsou různé velké (statisíce až desetimiliony certů)
- infrastruktura se bude časem zahušťovat
- Google nabízí i webové rozhraní
- případně vyhledávače třetích stran jako crt.sh
- další info na www.certificate-transparency.org

Kde to uvidím?

- Chrome devtools → Security → Main origin
- chrome://net-internals „signed_cert…“
- na webu crt.sh
- Certspotter služba, GitHub
- pomocí řady nástrojů a knihoven
- OpenSSL má od verze 1.0.2 podporu pro SCT
- Facebook má vlastní monitoring posílající maily

ROOT.CZ vpsFree.cz

Co bude dál?

- od 30. dubna 2018 bude **povinné**
- vznik dalších logů
- vznik mnoha dalších monitorů
- vznik dalších nástrojů

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz