

Certificate Transparency

povinně zveřejněné certifikáty

Petr Krčmář



5. listopadu 2017



Uvedené dílo (s výjimkou obrázků) podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

Prezentace už teď na webu

www.petrkrcmar.cz

CA v(e fakt malé) kostce

- problém bezpečného předání veřejného klíče
- komunikujeme se správnou protistranou?
- autorita je důvěryhodný prostředník
 - vystaví digitálně podepsaný dokument
 - certifikát = veřejný doklad vystavený CA
 - propojuje doménové jméno s veřejným klíčem
 - klient dostává certifikát při spojení
 - může ověřit, že má správný klíč
- celé se to jmenuje PKI

Funguje to (?)

- tohle celé funguje skvěle

Funguje to (?)

- tohle celé funguje skvěle
- až na případy, kdy to selhává

Funguje to (?)

- tohle celé funguje 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

Různé způsoby vylepšení

- letité snahy PKI vylepšit
- HPKP – pinování klíče, Chrome opouští
- OCSP – rychlejší revokace klíče
- CAA – DNS záznam svazující doménu a autoritu
- řada projektu sbírajících certifikáty
- všechno jsou jen berličky
- stále existuje riziko neoprávněného vydání
- trvá dlouho takový problém odhalit a vyřešit

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 (Merklov 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
- monitor – kontroluje logy a hledá problémy
- auditor – kontroluje konkrétní certifikát (prohlížeč)
- 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 dubna 2018 bude **vyžadováno u všech**
- původně to měl být už říjen 2017
- Firefox oznámil podporu, ale bez termínů

Jak authority 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

Odesílání do logu

- POST `https://<log server>/ct/v1/add-chain`
- vstup v JSON, certifikáty BASE64 v DER
- první musí jít koncový certifikát
- pak mezilehlý nebo kořen
- server odpoví pomocí SCT
- takto je možné (doporučeno) oslovit více logů
- i pokud daný log certifikát viděl, vystaví SCT
- SCT má do 100 bytů, používá se ECDSA
- žádná velká zátěž na servery

- verze standardu (v1)
- Log ID - veřejný klíč logu (bod důvěry)
- časová značka - nesmí být například v budoucnosti
- podpis - ECDSA s SHA256
 - struktura podepisovaných dat je složitější
 - samozřejmě je v ní i logovaný certifikát!
- SCT patří ke konkrétnímu certifikátu
- klient rekonstruuje celý záznam a ověřuje podpis

Příklad SCT v certifikátu

CT Precertificate SCTs:

Signed Certificate Timestamp:

Version : v1 (0x0)
Log ID : DD:EB:1D:2B:7A:0D:4F:A6:20:8B:81:AD:81:68:70:7E:
2E:8E:9D:01:D5:5C:88:8D:3D:11:C4:CD:B6:EC:BE:CC
Timestamp : Mar 15 15:50:02.152 2017 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:46:02:21:00:8C:CD:48:E9:CA:EC:66:A0:7E:31:3B:
02:E0:50:81:10:E6:F7:24:A2:0A:AE:C4:D4:6D:0D:02:
AD:10:C0:2E:73:02:21:00:8F:A0:A9:FD:13:36:A0:00:
48:D0:BE:7E:CA:C6:39:AC:9A:47:99:6C:E5:60:9C:2D:
2E:EF:EC:9C:D1:4F:6A:E2

Signed Certificate Timestamp:

Version : v1 (0x0)
Log ID : A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:
3C:35:98:04:F9:1B:DF:B8:E3:77:CD:0E:C8:0D:DC:10
Timestamp : Mar 15 15:50:02.179 2017 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:46:02:21:00:FF:76:7D:B2:5F:C6:9C:40:B0:D7:77:
0B:50:74:83:A2:EA:3D:54:BF:EC:13:0C:A8:EE:1B:0D:
37:62:E5:60:48:02:21:00:94:F3:A4:F3:CD:8A:2E:38:
F7:A0:E4:BE:42:C0:2F:B3:EB:8B:79:C7:DE:4E:98:AA:
08:3C:FC:AE:AE:8E:43:1D

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
- změni 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 OCSP 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

Jak najít „brejle bez brejlí“?

- jak vydat certifikát s důkazem o vydání?

Jak najít „brejle bez brejlí“?

- jak vydat certifikát s důkazem o vydání?
- vytvoří se „precertifikát“
- je stejný jako konečný certifikát
- vydává ho běžná autorita nebo speciální podřízená
- obsahuje ale „jedovaté rozšíření“
 - bit znemožňující běžnou validaci klienty
- precertifikát ukazuje **záměr** vytvořit certifikát
- POST `https://<log server>/ct/v1/add-pre-chain`
- log zkontroluje celý řetězec důvěry, vydá SCT
- při vydání se zanedbá podpis certifikátu a jed
- autorita přidá SCT do certifikátu a znovu podepíše

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

Funguje to?

- už teď jsou výsledky
- Symantec vystavil google.com
- 2500 certifikátů na neexistující domény
- odhaleny problémy autority WoSign

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

Má to i nevýhody

- další komplikovaná infrastruktura
- prozrazujete interní domény
 - řešení: wildcard certifikáty, vlastní CA
- navrhuje se několik možností redigování
- návrh: požádáte o zakrytí části jména
 - log zveřejní zahašovanou část jména
- návrh: zveřejníte jen mezilehlý certifikát
 - v něm deklarujete, že další certy nejsou v logu
- stále nevíme, zda něco z toho bude akceptováno

Co bude dál?

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

Otázky?



Petr Krčmář
petr.krcmar@iinfo.cz