Současné problémy certifikačních autorit

Petr Krčmář

9. října 2016

Prezentace už teď na webu

https://www.petrkrcmar.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?


https://www.root.cz


https://www.root.cz


I'm Green!
I'm Green!
I'm Green!

Problém: důvěryhodné předání klíče

- šifrovat asymetrickou šifrou umíme
- autentizace stejně důležitá jako silná šifra
- jinak hrozí útok man-in-the-middle
- problém důvěryhodného předání veřejného klíče
- protistrana je pro nás neznámá
- nastupují autority: důvěryhodní prostředníci
- ověří žadatele, vystaví certifikát
- certifikát je **veřejný dokument**

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
- většina delegovaných – reálně desítky firem

Svět není ideální

- v ideálním světě neexistují neoprávněně vydané certifikáty
- technická chyba, omyl, útok, státní zájmy
- autority jsou „univerzálně“ důvěryhodné
- kterákoliv může vydat důvěryhodný certifikát
- hříšníci: DigiNotar, Thawte, Symantec, WoSign...
- řetěz je silný jako nejslabší článek
- = tempo neudává nejlepší autorita, ale nejhorší
- jedno shnilé jablko zničí celý košík

Současná kauza WoSign

- antedatované certifikáty s SHA-1
- stejné sériové číslo
- validace na libovolném TCP portu
- vydání certifikátu k nadřazené doméně
- vydání certifikátu bez žádosti
- chyby v API StartSSL (vlastněná také WoSign)
- výběr kořenů + možnost volby URL pro výzvu
- navíc netransparentnost, špatná komunikace
- WoSign odmítla revokovat certifikáty
- = vážný problém pro celé PKI

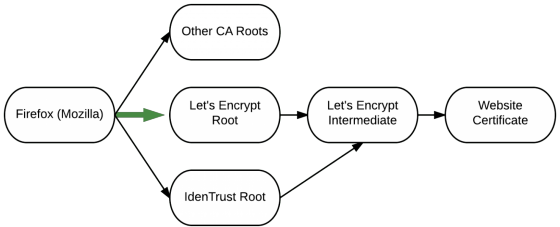

SECURITY WILL
RETURN IN
5 MINUTES
FAIL

Cross-signing

- vystavení mezilehlého z různých kořenů
- nestačí odebrat důvěru jedné autoritě
- řetězec důvěry může začít jinde
- problém třeba u WoSign – ochrana před znedůvěryhodněním
- mezilehlý od StartCom, Unizeto a USERTRUST

Cross-signing

- vystavení mezilehlého z různých kořenů
- nestačí odebrat důvěru jedné autoritě
- řetězec důvěry může začít jinde
- problém třeba u WoSign – ochrana před znedůvěryhodněním
- mezilehlý od StartCom, Unizeto a USERTRUST



Problém: DV certifikáty

- automatizovaná validace
- neodlišitelné od OV (poznáte EV?)
- velmi snadno získatelné
- nevymyslel to Let’s Encrypt, vydává je kdekdo
- stačí vystavit soubor nebo přijmout mail
- řada služeb umožňuje vystavovat soubory na své doméně
- Google Drive, Dropbox, GitHub, Amazon…
- neprovozujete něco podobného?

Řešení: lepší ochrana

- nenechat vystavovat soubory na /.well-known/
- rezervovat mailové adresy admin, administrator, webmaster, hostmaster, postmaster
- chránit některé typy záznamů: TXT a CAA (RFC 6844)

Řešení: lepší ochrana

- nenechat vystavovat soubory na /.well-known/
- rezervovat mailové adresy admin, administrator, webmaster, hostmaster, postmaster
- chránit některé typy záznamů: TXT a CAA (RFC 6844)

```
comodo.com.  IN CAA 0 issue "comodoca.com"
comodo.com.  IN CAA 0 iodef "mailto:sslabuse@comodoca.com"
```

Ale...

- doopravdy to nezabrání autoritě vystavit certifikát
- můžou se objevit další chyby
- jedna pochybná autorita rozbíjí princip
- útočník si vybere nejméně důvěryhodnou autoritu

Problém: chybějící přesměrování z HTTP

- snadný vektor útoku
- přesměrování z HTTP na HTTPS probíhá nešifrovaně
- útočník může vložit vlastní přesměrování
- nebo přesměrování neposlat a ovlivnit spojení
- nepozorný uživatel nic nepozná

Řešení: hlavička HSTS

- HTTP Strict Transport Security (HSTS)
- hlavička v HTTP odpovědi (RFC 6797)
- tento web musí mít vždy důvěryhodný certifikát
- prohlížeč sám přepíše http:// na https://
- TOFU = Trust On First Use

Řešení: hlavička HSTS

- HTTP Strict Transport Security (HSTS)
- hlavička v HTTP odpovědi (RFC 6797)
- tento web musí mít vždy důvěryhodný certifikát
- prohlížeč sám přepíše http:// na https://
- TOFU = Trust On First Use

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

Řešení: hlavička HSTS

- HTTP Strict Transport Security (HSTS)
- hlavička v HTTP odpovědi (RFC 6797)
- tento web musí mít vždy důvěryhodný certifikát
- prohlížeč sám přepíše http:// na https://
- TOFU = Trust On First Use

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

- možno i HSTS preload
- chrome://net-internals/#hsts
- rozšíření HTTPS Everywhere

Ale…

- problém TOFU
- náchylné k útokům na systémové hodiny (NTP)
- preload neškáluje (už teď přes 11K položek)
- neřeší přímo problém autorit – jakýkoliv cert vyhoví
- nelze se jednoduše zbavit (!) – opatrně při nasazení
- může sloužit jako supercookie (i v anonymním režimu)

Problém: svázání klíče s webem

- klíč je přenášen jen v certifikátu
- web není nijak vázán na autoritu
- k vystavení certifikátu donutím jinou autoritu
- můžu podvrhnout vlastní šifrovací klíče
- hodila by se další vazba klíče ke zdroji

Řešení: hlavička HPKP

- HTTP Public Key Pinning (HPKP)
- hlavička obsahující hashe klíčů (RFC 7469)
- klient se je naučí a očekává je
- možno více klíčů, ale minimálně dva
- jeden **musí** ležet v cestě, druhý **nesmí**
- alespoň jeden je vždy záložní

Řešení: hlavička HPKP

- HTTP Public Key Pinning (HPKP)
- hlavička obsahující hashe klíčů (RFC 7469)
- klient se je naučí a očekává je
- možno více klíčů, ale minimálně dva
- jeden **musí** ležet v cestě, druhý **nesmí**
- alespoň jeden je vždy záložní

```
Public-Key-Pins: max-age=5184000;
  pin-sha256="WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=";
  pin-sha256="RRM1dGqnDFsCJXBTHky16vi1obOlCgFFn/yOhI/y+ho=";
  pin-sha256="k2v657xBsOVe1PQRwOsHsw3bsGT2VzIqz5K+59sNQws=";
  pin-sha256="K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q=";
  pin-sha256="IQBnNBEiFuhj+8x6X8XLgh01V9Ic5/V3IRQLNFFc7v4=";
  pin-sha256="iie1VXtL7HzAMF+/PVPR9xzT80kQxdZeJ+zduCB3uj0=";
  pin-sha256="LvRiGEjRqfzurezaWuj8Wie2gyHMrW5Q06LspMnox7A=";
  includeSubDomains
```

Ale…

- opět TOFU
- pozor na chyby – ztrátu klíčů
- autorita může změnit politiku a vyměnit mezilehlý klíč
- nepodporuje MSIE/Edge
- podle Netcraftu používá jen 0,09 % webů
- velmi mladý standard (duben 2015)

Problém: potřebuji zneplatnit certifikát

- CRL – Certificate Revocation List
- seznamy revokovaných certifikátů včetně data
- generují se jednou za pár dnů
- klient je stahuje a kešuje zhruba týden
- cesta musí být součástí certifikátu
- klient musí seznamy stahovat
- neškáluje to – problém mobilních klientů
- co když je zdroj nedostupný? (soft/hard fail)

Řešení: OCSP

- Online Certificate Status Protocol
- zapojení OCSP responderu, který vrací info o stavu
- „razítko“ potvrzující platnost certifikátu
- varianty „good“, „revoked“, „unknown“
- součástí podepsané odpovědi je i časové omezení
- informace je platná obvykle jeden až dva dny
- je platná i offline – je možné ji kešovat
- možno mít samostatnou subautoritu pro OCSP

Ale…

- poměrně náročná komunikace (pro každý certifikát v řetězci)
- unikají informace o tom, kdo se kam připojuje
- co když je zdroj nedostupný?
- možno vyřešit pomocí OCSP stapling – posílá server
- útočník s privátním klíčem může na cestě OCSP blokovat
- v certifikátu může být příznak „MustStaple“
- pak musí server s certifikátem předat i OCSP razítko
- Chrome nepodporuje OCSP od roku 2012

Problém: Nemůžeme zrušit PKI?

- můžeme vymyslet jiný kanál pro důvěryhodný přenos klíče
- musel by mít podobné vlasnosti, ale zavrhnout autority
- ideální stav = já sám jsem autoritou
- můžu sám vystavovat bod důvěry
- je možné nezávislým kanálem ověřit můj klíč

Řešení: DANE/TLSA

- DNS-based Authentication of Named Entities (DANE)
- přidává TLSA záznam do DNS (RFC 6698)
- podobné jako HPKP, ale v doméně
- záznamy jsou podepsané DNSSEC
- nezávislý kanál pro ověření klíče
- ověření proběhne ještě před TLS (odpadá TOFU)
- umí vložit nový bod důvěry nebo přímo koncový otisk

Řešení: DANE/TLSA

- DNS-based Authentication of Named Entities (DANE)
- přidává TLSA záznam do DNS (RFC 6698)
- podobné jako HPKP, ale v doméně
- záznamy jsou podepsané DNSSEC
- nezávislý kanál pro ověření klíče
- ověření proběhne ještě před TLS (odpadá TOFU)
- umí vložit nový bod důvěry nebo přímo koncový otisk

```
$ dig +short _443._tcp.www.linuxdays.cz tlsa
3 1 1 7FA66F6694BC634F8A5068F19FBF02B7069E8F6A9818A9236BBCE9A4 B4CB4C61
3 1 1 C97E2059C469CB20AA321F7A20C195A536E91E11DC91CA3B9AD3646D A1385ED1
```

Ale...

- problémem je podpora DNSSEC
- validuje asi třetina uživatelů (APNIC)
- ale velká část vzdáleně třeba u Google (10 %)
- musela by se dotáhnout na koncovou stanici
- další problém – v řadě sítí je rozbité DNS
- nelze se tedy spolehnout výhradně na DANE
- skončíme ve slepé uličce bez potvrzených klíčů
- proto prohlížeče nepodporují – bohužel
- DNS over TLS, dns.google.com (JSON)
- dobrá podpora v mailových serverech

PKI se jen tak nezbavíme

- PKI je všude, je to kritická infrastruktura
- spoléhají na něj weby, služby, API a další
- bohužel se jej asi rychle nezbavíme
- lepíme díry po kolena ve vodě
- ale snažíme se plout dál...

PKI se jen tak nezbavíme

- PKI je všude, je to kritická infrastruktura
- spoléhají na něj weby, služby, API a další
- bohužel se jej asi rychle nezbavíme
- lepíme díry po kolena ve vodě
- ale snažíme se plout dál...

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz