Komu to věříme? Pohled mezi důvěryhodné certifikační autority

Petr Krčmář

2. března 2019

Prezentace už teď na webu

https://www.petrkrcmar.cz

Co je to HTTPS?

- přenos protokolu HTTP v šifrovaném TLS tunelu
- provoz běží po TCP portu 443
- data jsou přenášena šifrovaně a autentizovaně
- pro sestavení kanálu se používá asymetrická kryptografie
- k potvrzení identity se využívají **certifikáty**
- pro šifrování se používá symetrická kryptografie

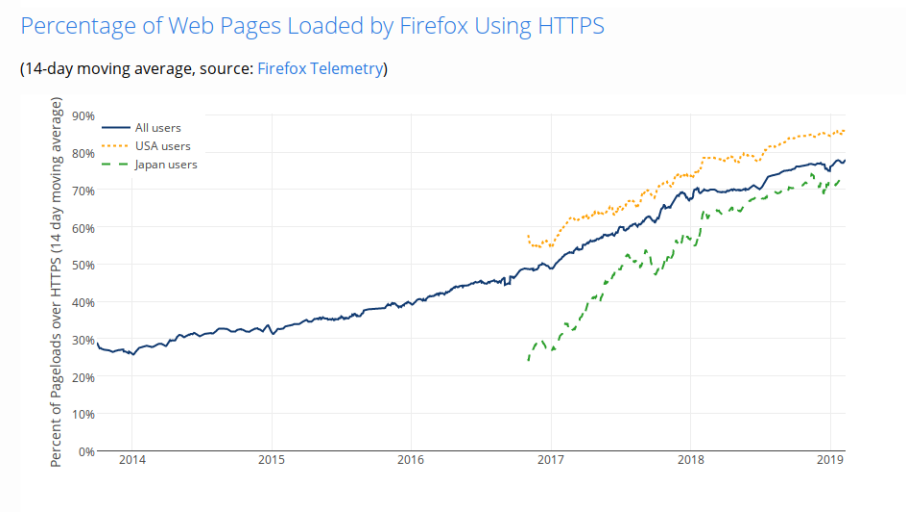
Před čím chrání HTTPS?

- před síťovými útoky (věříte zdejší Wi-Fi?)
- před odposlechem komunikace (RFC 7258 – odposlech je útok)
- před man-in-the-middle – víme, s kým komunikujeme
- před blokováním části obsahu (Wikipedie)
- před pozměňováním dat během přenosu
- před vkládáním supercookies, malware, trackovacích kódů
- před únikem osobních údajů – nechcete e-shop bez HTTPS
- před únosemu session cookie – při přihlašování

Zařízení značky Sandvine (dnes Procera)
(Root.cz: Vlády přesměrovávají uživatele na software doplněný o malware)

Před čím HTTPS nechrání?

- před únikem informací o doméně (DNS, SNI)
- před sběrem metainformací (netflow, IP…)
- před phishingovými weby
- před blokováním provozu na síťové vrstvě
- před útokem na legitimního provozovatele webu (XSS, SQL…)
- před zlými úmysly autora webu



- 78 % stránek načteno po HTTPS, v USA dokonce 85 %
- před rokem 70 a 78 %, před dvěma 50 a 60 %

Problém: důvěryhodné předání klíče

- šifrovat bezpečně asymetrickou šifrou umíme
- protistrana je pro nás ale neznámá
- autentizace stejně důležitá jako silná šifra
- bez ní se kdokoliv může vydávat za kohokoliv
- problém důvěryhodného předání veřejného klíče
- nastupují autority: důvěryhodní prostředníci
- ověří žadatele, vystaví certifikát


EVROPSKÁ UNIE
ČESKÁ REPUBLIKA
CESTOVNÍ
PAS
EVROPSKÁ UNIE
ČESKÁ REPUBLIKA
CESTOVNÍ
PAS
EVROPSKÁ UNIE
ČESKÁ REPUBLIKA
CESTOVNÍ
PAS
EVROPSKÁ UNIE
ČESKÁ REPUBLIKA
CESTOVNÍ
PAS

Certifikát je internetový pas

- pas propojuje fotografii obličeje se jménem
- certifikát propojuje doménové jméno s veřejným klíčem
- server se prokazuje: toto je potvrzení o mém klíči
- pas vystavují jen důvěryhodné státy
- certifikáty vystavují důvěryhodné autority
- celník ověří totožnost na základě dokumentu známého státu
- prohlížeč ověří identitu na základě dokumentu známé autority
- důvěryhodné autority a jejich klíče jsou předinstalované v software
- to celé ↑ se jmenuje PKI (Public Key Infrastructure)

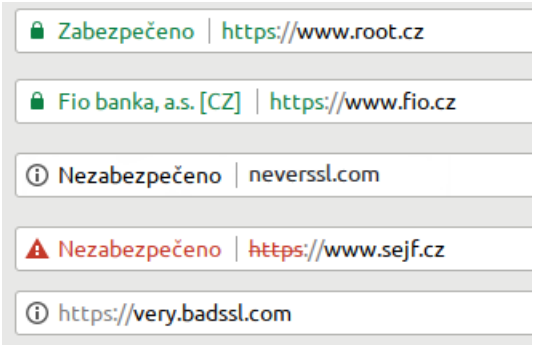
Co je to certifikát?

- **veřejný** dokument, který obsahuje hlavně:
  - jméno autority
  - doménová jména
  - veřejný klíč žadatele
  - datum platnosti
  - podpis autority
  - a další
- elektronický podpis = nezfalšovatelné
- ověříme pomocí známého veřejného klíče v software
- certifikát **není tajemstvím**, chráníme privátní klíč

Tři druhy certifikátů

- **EV** – Extended Validation
  - velmi drahý, důkladné ověření identity žadatele
  - signalizace zeleným názvem vedle adresy
  - nesmí obsahovat wildcard (hvězdičku)
  - nemůžou vydávat všechny autority
- **OV** – Organzation Validation
  - levnější varianta, zběžné prověření idenity žadatele
  - v prohlížeči nemá speciální označení
- **DV** – Domain control Validation
  - velmi levné vystavení, lze automatizovat
  - jen kontrola doménového jména
  - není nijak svázán s identitou žadatele
  - nejběžnější typ certifikátu
- max. platnost všech je 825 dnů (přibližně 27 měsíců)

ROOT.CZ vpsFree.cz


Zabezpečeno | https://www.root.cz
Fio banka, a.s. [CZ] | https://www.fio.cz
Nezabezpečeno | neverssl.com
Nezabezpečeno | https://www.sejf.cz
https://very.badssl.com

Řetězec důvěry

- software zná kořenové certifikáty s veřejným klíčem autority
- od serveru dostane řetězec – delegace pravomocí autority
- certifikáty se musí vzájemně potvrzovat
- konečný certifikát potvrzuje identitu žadatele (serveru)
- zároveň obsahuje veřejný klíč
- identita je potvrzena, klíč předán protistraně
- komunikace může začít

Kdo je to certifikační autorita?

- splňuje bezpečnostní podmínky CAB Fóra
- má hardware a procesy podle doporučení
- zveřejní všechny potřebné informace
- podá žádost k zařazení mezi důvěryhodné
- projde auditem od certifikovaného auditora
  - opakuje se nejméně jednou ročně
- proces trvá minimálně dva roky
- výsledkem je vložení kořenových certifikátů do úložišť

Komu jsme se rozhodli věřit?

Kolik jich je?

Datum	Počet CA
23. 1. 2019	135
5. 12. 2018	128
17. 10. 2018	129
20. 6. 2018	132
7. 3. 2018	133
17. 1. 2018	138
20. 9. 2017	143
7. 6. 2017	155
18. 1. 2017	158
2. 11. 2016	158

Kde se dají najít?

- ve zdrojových kódech prohlížečů
- v instalacích prohlížečů
- … `/nss/lib/ckfw/builtins/certdata.txt`
- k extrakci lze použít existující utility
  - `mk-ca-bundle`
  - `firefox-db2pem.sh`

Kdo je provozuje?

- každá autorita má v popisku provozovatele (0=)
- položek je sice 135, ale **unikátních je 70**
- mají více kořenových certifikátů
  - Amazon Root CA 1, 2, 3, 4
  - GTS Root R1, R2, R3, R4
  - TrustCor RootCert CA-1, CA-2, ECA-1
  - vlastně je jich ještě méně
- je tam několik semi-duplicit
  - Comodo CA vs. COMODO CA
  - SECOM Trust.net vs. SECOM Trust Systems
  - ...
- celkem existuje 58 organizací provozujících CA

Kdo je provozuje?

- AC Camerfirma S.A.
- ACCV
- Actalis S.p.A.
- AddTrust AB
- AffirmTrust
- Agencia Catalana de Certificacio (NIF Q-0801176-I)
- Amazon
- AS Sertifitseerimiskeskus
- Atos
- Baltimore
- Buypass AS-983163327
- Certinomis
- Certplus
- certSIGN
- Comodo CA Limited
- COMODO CA Limited
- Cybertrust, Inc
- Deutsche Telekom AG
- Dhimyotis
- DigiCert Inc
- Digital Signature Trust Co.
- Disig a.s.
- D-Trust GmbH
- Entrust, Inc.
- Entrust.net
- E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
- FNMT-RCM
- GeoTrust Inc.
- GlobalSign
- GlobalSign nv-s
- GoDaddy.com, Inc.
- Google Trust Services LLC
- Government Root Certification Authority
- GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.
- Hellenic Academic and Research Institutions Cert. Authority
- Hongkong Post
- China Financial Certification Authority
- Chunghwa Telecom Co., Ltd.
- IdenTrust
- Internet Security Research Group
- IZENPE S.A.
- Japan Certification Services, Inc.
- Krajowa Izba Rozliczeniowa S.A.
- LuxTrust S.A.
- Microsec Ltd.
- NetLock Kft.
- Network Solutions L.L.C.
- QuoVadis Limited
- SECOM Trust.net
- SECOM Trust Systems CO.,LTD.
- SecureTrust Corporation
- Sonera
- SSL Corporation
- Staat der Nederlanden
- Starfield Technologies, Inc.
- SwissSign AG
- TAIWAN-CA
- TeliaSonera
- thawte, Inc.
- The Go Daddy Group, Inc.
- The USERTRUST Network
- TrustCor Systems S. de R.L.
- Trustis Limited
- T-Systems Enterprise Services GmbH
- Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK
- UniTrust
- Unizeto Technologies S.A.
- VeriSign, Inc.
- WISeKey
- XRamp Security Services Inc

Kdo je vlastní?

- AC Camerfirma, S.A.
- Actalis
- Amazon Trust Services
- Asseco Data Systems S.A.
- Atos
- Autoridad de Certificacion Firmaprofesional
- Buypass
- Certinomis / Docapost
- certSIGN
- Consorci Administració Oberta de Catalunya
- Cybertrust Japan / JCSI
- Dhimyotis / Certigna
- DigiCert
- Disig, a.s.
- DocuSign
- D-TRUST
- Entrust
- E-Tugra
- Global Digital Cybersecurity Authority
- GlobalSign
- GoDaddy
- Google Trust Services LLC (GTS)
- Government of Hong Kong
- Government of Spain
- Government of Taiwan
- Government of The Netherlands
- Government of Turkey
- HARICA
- China Financial Certification Authority (CFCA)
- Chunghwa Telecom
- IdenTrust Services, LLC
- Internet Security Research Group (ISRG)
- Izenpe S.A.
- Krajowa Izba Rozliczeniowa S.A. (KIR)
- LuxTrust
- Microsec Ltd.
- NetLock Ltd.
- QuoVadis
- SECOM Trust Systems CO., LTD.
- Sectigo
- SecureTrust
- Shanghai Electronic Certification Authority
- SK ID Solutions AS
- SSL.com
- Swisscom (Switzerland) Ltd
- SwissSign AG
- Taiwan-CA Inc.
- Telia Company
- TrustCor Systems
- Trustis

Odkud jsou

- po ručním vyřezení všech duplicit

Stát	Počet CA
US	19
ES	5
DE	4
CN	3
FR	3
TW	3
TR	2

- jedna
  - BE, BM, EE, FI, HK, IE, IT, LU, NL, NO, PA, RO, SE, SK, EU
- dvě
  - GB, GR, HU, CH, JP, PL, TR

Paretův princip v praxi

Autorita	Podíl certifikátů
IdenTrust	49,1 %
Sectigo	27,3 %
DigiCert	11,8 %
GoDaddy	6,8 %
GlobalSign	2,8 %

- Sectigo vlastní AddTrust, Comodo a UserTrust
- zbytek pod 1 %
- zdroj: statistiky W3Techs

Státem provozované autority

- Mozilla pro ně má speciální politiku
- v současné době je provozuje sedm států
  - Francie
  - Hong Kong
  - Japonsko
  - Španělsko
  - Nizozemsko
  - Tchaj-wan
  - Turecko
- to jsou ale jen přiznané
- řada veřejných organizací: CNNIC, CATCert, TurkTrust…
- hodně závisí na definici „vládní CA“

Všechny autority můžou všechno

- existuje rozšíření Name Constrains
- omezuje autoritu na subdomény
- používá ale jen turecká vládní autorita TUBITAK
- vazbu na ccTLD totiž nelze vynutit
- řadě států a federací se navíc překrývají jurisdikce
- většina autorit potřebuje vystavovat na generické domény
  - například na .gov, .org, .edu…
- u nás třeba datoveschranky.info
- navíc registr domén už teď může podvádět
  - má moc nad validačními údaji
  - může si nechat vystavit certifikát od libovolné CA

Musíme jim věřit?

- od konce dubna 2018 povinné používat Certificate Transparency
  - veřejné logy pro ukládání certifikátů
  - lze do nich jen přidávat (Merklův hashový strom)
  - definováno v RFC 6962
- prohlížeče vyžadují dodání potvrzení o uložení v CT
- vyhledávat je možné v crt.sh
- existují automatické hlídače nově vystavených certifikátů
  - každý může hlídat své domény nebo jakékoliv cizí

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz