

Co musíte vědět o šifrování

Ondřej Caletka



29. listopadu 2017



Uvedené dílo podléhá licenci Creative Commons Uvedte autora 3.0 Česko.

Internet jako nepřátelské prostředí

- mnoho uzlů
- předávání zpráv předem neznámou cestou
- každý uzel může **nahlížet do zpráv**
- každý uzel může zprávy **nedetekovatelně modifikovat**

Nesvěřujte Internetu nic, co byste nenapsali na zadní stranu pohlednice.

- ze starodávné příručky o internetu

Nejen, že může, ale i modifikuje

Pozor! Státní hranice! Vstup zakázán!

Pokusili jste se navštívit zahraniční stránku!

Dnes na to stačí jeden klik, ale před rokem 1989 bylo složité podívat se za hranice. Svěvolné opuštění republiky se trestalo odnětím svobody až na pět let. Pokud vás přímo při pokusu nezastřelila pohraniční stráž.

Svoboda není samozřejmost.

Proto si i my 17. listopadu připomínáme výročí Sametové revoluce a jsme rádi, že vám v Česku i na Slovensku můžeme přinášet svobodnou komunikaci s celým světem.

[Více informací o 17. listopadu](#)

[Chci svobodně pokračovat](#)

O₂

Šifrování jako záchrana

- utajení zprávy před přenosem
- obsah zprávy vidí jen koncové strany šifrování
- ostatní neznají obsah, nemohou zprávu modifikovat
- stále mají **přístup k metadatům komunikace**

hop-by-hop vs. end-to-end

hop-by-hop zpráva se při průchodu sítí rozšifrovává a zašifrovává (typicky e-mail)

end-to-end zpráva se jednou zašifruje u původce a rozšifruje až u příjemce (typicky HTTPS)

Šifrujeme úplně všichni

 <https://www.cesnet.cz>

Šifrujeme úplně všichni



<https://www.cesnet.cz>



Jenom šifrovat nestačí

Mac iPad iPhone Watch TV Music Support

Apple ID Sign In Create Your Apple ID FAQ

Apple ID

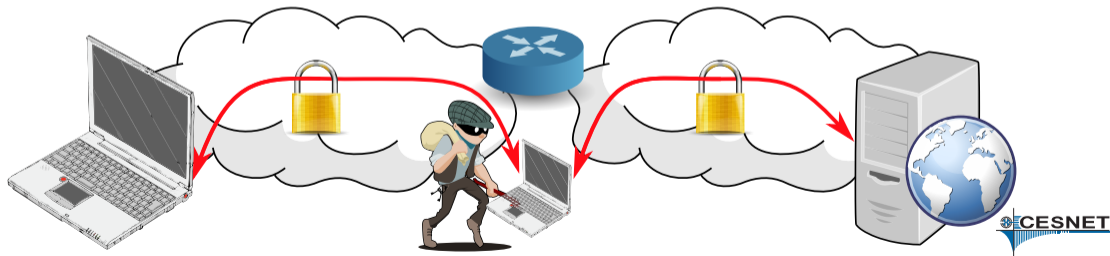
Manage your Apple account

Apple ID

Password

Kdo je na druhé straně?

- nedílnou součástí je *autentizace* – určení, kdo je na druhé straně šifrovaného kanálu
- nejčastěji pomocí **Infrastruktury veřejného klíče (PKI)**
- méně často také *TOFU* (např. SSH), či *síť důvěry* (např. PGP)
- bez autentizace lze zaútočit metodou **člověk uprostřed** (MitM)



- řeší problém důvěryhodného ověření identity protistrany
- **certifikát = průkaz totožnosti** vystavený důvěryhodnou autoritou
- svazuje virtuální identitu (šifrovací klíč) s reálnou identitou (jméno a příjmení, adresa, doménové jméno,...)
- zapečetěný elektronickým podpisem autority
- důvěryhodné autority **jsou předinstalovány v počítači**

Jak probíhá ověření

Cestovní pas

- 1 cestující předloží cestovní pas a své biometrické údaje
- 2 ověříme shodu biometrických údajů
- 3 ověříme pravost dokumentu
- 4 ověříme, že vydavatel je na seznamu uznávaných vydavatelů
- 5 známe identitu cestujícího

Certifikát

- 1 protistrana předloží certifikát a důkaz vlastnictví privátního klíče
- 2 ověříme důkaz vlastnictví
- 3 ověříme podpis certifikační autority
- 4 ověříme, že autorita je na seznamu důvěryhodných
- 5 známe identitu protistrany

Co se dozvíme z certifikátu

Různé úrovně ověření

Extended Validation (EV, €€€)

důkladné prověření identity žadatele

Organization Validation (OV, €€)

zběžné prověření identity žadatele

Domain control Validation (DV, €)

kontrola ovládání doménového jména, pro které je vydán

- počítače automaticky kontrolují shodu doménového jména v certifikátu se jménem, ke kterému se připojují
- použití EV certifikátu je obvykle signalizováno zelenou barvou a viditelným zobrazením držitele certifikátu
- ostatní položky nejsou automaticky analyzovány



Slabiny certifikačních autorit

- možnost vydání certifikátu neoprávněnému držiteli
- záruky především právní, méně už technické
- minimum odhalených případů



Zdroj: Jason Bourne's Passports Prop Replicas

EV certifikáty v praxi

🔒 Apple Inc. [US] | <https://appleid.apple.com/#!/&page=signin>

🔒 Alza.cz a.s. [CZ] | <https://www.alza.cz>

🔒 CZC.cz s.r.o. [CZ] | <https://www.czc.cz>

🔒 Úřad vlády České republiky [CZ] | <https://vlada.cz>

🔒 mBank S.A. [PL] | <https://www.mbank.cz/informace-k-produktum/info/>

🔒 Fio banka, a.s. [CZ] | <https://www.fio.cz/ib2/login>

🔒 Ceskoslovenska obchodni banka, a.s. [CZ] | <https://www.postovnisporitelna.cz>

🔒 Česká spořitelna, a.s. [CZ] | <https://www.servis24.cz/ebanking-s24/ib/base/usr/aut/login?execution=e1s1>

Nedůvěryhodná stránka

Select

Zabezpečeno | https://ke-utc.appspot.com/static/select.html?label=PR...

[Zpět](#) [Domů](#) [Nastavení](#) Česky

Ruční zadání

Zadejte číslo úseku a stiskněte OK.
Označení úseku naleznete na dopravní značce.
Např. P6-1234

OK

Nejbližší úseky zón

Poloha zařízení není známa. Povolte prosím zjištění Vaší polohy v nastavení zařízení / prohlížeče.

[Podpora \(FAQ\)](#) [Facebook](#) [Google play](#)
[Všeobecné obchodní podmínky \(VOP\)](#)
Provozuje MPLA s.r.o.

version [2017-10-16T20:26:10]

Developer Tools - <https://ke-utc.appspot.com/static/select.html?label=PRAHA>

Prohlížeč certifikátů: *.appspot.com ✕

Obecné Podrobnosti

Tento certifikát byl ověřen pro následující použití:

Certifikát serveru SSL

Vydán pro

Běžný název (CN)	*.appspot.com
Organizace (O)	Google Inc
Organizační jednotka (OU)	<Není součástí certifikátu>

appspot.com

Lookup

Contact Information

Registrant Contact

Name: DNS Admin
Organization: Google Inc.
Mailing Address: 2400 E. Bayshore Pkwy, Mountain View CA 94043 US
Phone: +1.6503300100
Ext:
Fax: +1.6506188571
Fax Ext:
Email: dns-admin@google.com

Admin Contact

Name: DNS Admin
Organization: Google Inc.
Mailing Address: 1600 Amphitheatre Parkway, Mountain View CA 94043 US
Phone: +1.6506234000
Ext:
Fax: +1.6506188571
Fax Ext:
Email: dns-admin@google.com

Tech Contact

Name: DNS Admin
Organization: Google Inc.
Mailing Address: 1600 Amphitheatre Parkway, Mountain View CA 94043 US
Phone: +1.6506234000
Ext:
Fax: +1.6506188571
Fax Ext:
Email: dns-admin@google.com

Nedůvěryhodná platební brána

Payment card setting x

https://secure-pay.appspot.com/static/prod/card_settings.html

[Zpět](#) [Nastavení](#) Cestina ▾

Zadání platební karty

Zadejte Vaši MasterCard nebo Visa kartu a zvolte si heslo, kterým platby následně potvrzujete. Karta musí mít povoleny platby na internetu a MO/TO transakce.

Číslo karty

Měsíc expirace

Rok expirace

CVC/CVV

Zvolte si bezpečnostní heslo

Pro Vaši bezpečnost heslo zadáváte při každé platbě

Citlivá data jsou zašifrována heslem a bezpečně uložena ve Vašem telefonu. V některých případech při aktualizaci prohlížeče může dojít ke smazání těchto dat, informace pak musí být zadány znovu.

Šifrování garantuje, že...

- data vidíme pouze my a ten, jehož certifikát vidíme
- nikdo další data neviděl
- nikdo další nemohl komunikaci pozměnit

Šifrování negarantuje, že...

- protistrana použije data pouze k danému účelu
- náš počítač před zašifrováním data nepozmění
 - problém zlomyslných rozšíření prohlížečů

Šifrování by mělo být všude

- šifrování je jen pro banky

Šifrování by mělo být všude

- šifrování je jen pro banky
- ...a stránky, kam se uživatel přihlašuje

Šifrování by mělo být všude

- šifrování je jen pro banky
- ...a stránky, kam se uživatel přihlašuje
- ...a všechny ostatní stránky

Šifrování by mělo být všude

- šifrování je jen pro banky
- ...a stránky, kam se uživatel přihlašuje
- ...a všechny ostatní stránky
- hlavním důvodem je **autenticita přenášených dat**

Znamé případy zásahů do komunikace

- vkládání/náhrada reklam
- vkládání sledovacích kódů
- vkládání kódu **zneužívajícího známé slabiny**

Wi-Fi nebo internetová kavárna?

Wi-Fi

- snadná možnost pozměňování komunikace
- nemožné nedetekovaně vstoupit do šifrovaného spojení
- pro řádně ověřené šifrované spojení zcela bezpečné

Internetová kavárna

- počítač mimo naši kontrolu
- může být napaden nejrůznějším malwarem
- může zaznamenávat stisky kláves
- nelze důvěřovat ničemu, co počítač zobrazuje

Nikdy **neukládejte nešifrované sítě** do seznamu známých sítí!

- nulová autentizace provozovatele sítě
- zařízení sítě **aktivně vyhledává**
- útočník dokáže síť vyrobit na míru danému zařízení
- možnost kompromitace slabin manipulací *nešifrovaného* provozu
 - v kombinaci se zastaralými zařízeními bez bezpečnostních záplat

Použití veřejných VPN

- virtuální privátní síť představuje šifrovaný tunel, kterým proudí veškerý provoz
- vhodné pro nešifrovaná spojení na nešifrované Wi-Fi
- poskytovatel VPN vidí veškerou komunikaci
- poskytovatel dokáže spárovat provoz s konkrétním uživatelem

Tor

- speciální VPN, která data šifruje **několikanásobně** a posílá různými směry
- často zneužívána k trestné činnosti
- výstupní uzly vidí všechna data nešifrovaně
- velmi často zasahují do komunikace

- nespolehejte jen na techniku
- sledujte EV certifikáty (zelený pruh)
- konzultujte s registry nebo odborníky
- nepište svá hesla do cizích počítačů
- pravidelně mažte uložené nešifrované sítě
- jste-li nuceni nešifrovanou sítí používat, pořídte VPN a nastavte automatické zapnutí VPN

Děkuji za pozornost

Ondřej Caletka

Ondrej.Caletka@cesnet.cz

<https://Ondrej.Caletka.cz>

