

# Co musíte vědět o šifrování

Ondřej Caletka



31. října 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

A man with a receding hairline, wearing a dark suit, white shirt, and dark tie, is looking down. A white speech bubble with a black outline is positioned above him, containing the text 'A vy už jste někdy šifroval?'. The background is a blue patterned wall.

A vy už jste  
někdy šifroval?

**Ondřej Závodský** náměstek pro hazard a majetek státu, MF

# 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**
- u kvalitního šifrování není k dispozici *výjimka pro veřejnou moc* ani nikoho jiného

## 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 šifrovacího kanálu
- nejčastěji pomocí **Infrastruktury veřejného klíče (PKI)**
- méně často také *TOFU* (např. SSH), či *síť důvěry (WOT)* (např. PGP)



- 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**

**privátní klíč** tajné číslo, umožňující rozšifrovat zprávu a vytvořit elektronický podpis

**veřejný klíč** číslo, umožňující zašifrovat zprávu a ověřit elektronický podpis

**certifikát** podepsaný veřejný dokument, obsahující veřejný klíč, identifikaci subjektu a omezení využití certifikátu

**self-signed** certifikát podepsaný stejným klíčem, jehož veřejnou část certifikuje. **nedůvěryhodný**

**pevný bod důvěry** certifikát, jehož věrohodnost byla ověřena jiným způsobem a je považován za důvěryhodný

# Co autority ověřují

- že entita držící certifikát opravdu existuje a žádá vydání certifikátu
  - s důkladným prověřením (Extended Validation, €€€)
  - se zběžným prověřením (Organization Validation, €€)
- že majitel certifikátu mohl v době jeho vydání ovládat doménové jméno, případně e-mailovou adresu, pro kterou byl certifikát vydán (Domain Validation, €)
  - držitele doménového jména lze dohledat v doménových registrech

# Slabiny certifikačních autorit

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



Zdroj: Jason Bourne's Passports Prop Replicas

# Jak to má vypadat

🔒 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]

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

### 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

### 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

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>

# Nedůvěryhodná platební brána

Payment card setting x

← → ↻ [https://secure-pay.appspot.com/static/prod/card\\_settings.html](https://secure-pay.appspot.com/static/prod/card_settings.html) ☆ 6°

[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.

VISA  VISA Electron  MasterCard  American Express

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...

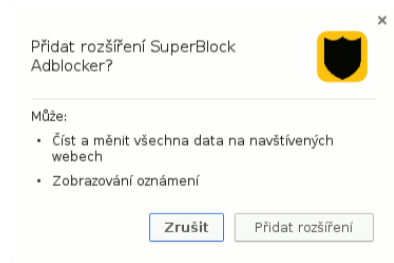
- data vidíme pouze my a ten, jehož certifikát vidíme
- nikdo další data neviděl
- nikdo další nemohl komunikaci pozměnit

## Šifrování negarantuje, že...

- protistrana použije data pouze k danému účelu
- náš počítač před zašifrováním data nepozmění

# Man-in-the-browser

- častý útok, prováděný pomocí zlomyslných rozšíření
- pozmění viditelný i neviditelný obsah stránky
- může odesílat stisknuté klávesy
- může přidat věrohodnou výzvu k instalaci nové bankovní aplikace
- **adresní řádek přitom ukazuje správnou adresu!**



# Šifrování by mělo být všude

- původní myšlenka: šifrování jen pro banky
- později: ...a stránky, kam se uživatel přihlašuje
- dnes: ...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 šifrované spojení s ověřením certifikátu zcela bezpečné

## Internetová kavárna

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

# Problém nešifrovaných Wi-Fi sítí

- nulová autentizace provozovatele sítě
- zařízení sítě **aktivně vyhledává**
- útočník dokáže síť vyrobit na míru danému klientovi
- bezpečné jen pro šifrovaný provoz
- typický útok: načítání reklam v mobilních aplikacích a hrách
- stejnou zranitelností trpí i šifrované sítě s veřejně známým heslem, ale útočit na nešifrované je jednodušší

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

# Použití veřejných VPN

- Virtuální privátní síť představuje šifrovaný tunel, kterým proudí veškerý provoz
- např. 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
- často zasahují do komunikace

- nespolehejte jen na techniku
- naučte se rozlišovat EV certifikáty (zelený pruh) a ostatní
- pokud si nejste jisti, 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 spojení

Děkuji za pozornost

Ondřej Caletka

Ondrej.Caletka@cesnet.cz

<https://Ondrej.Caletka.cz>



Prezentace již nyní ke stažení.