Co musíte vědět o šifrování

Ondřej Caletka

31. října 2017

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


24
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

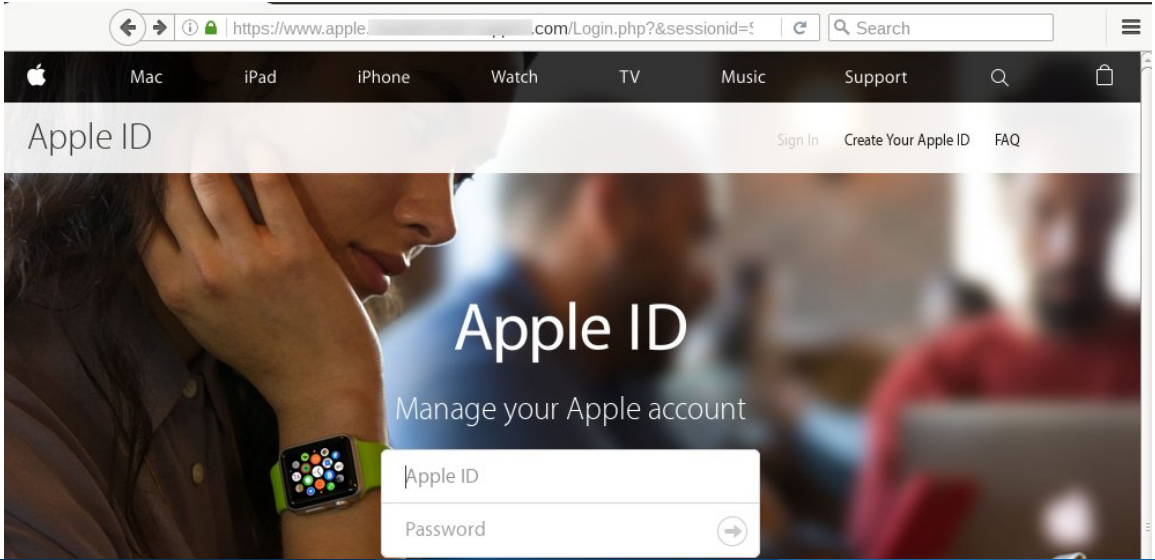
hop-by-hop zpráva se při průchodu sítí rozšifrovává a zašifrovává (typicky e-mail)

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

Šifrujeme úplně všichni

Šifrujeme úplně všichni

Jenom šifrovat nestačí



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)

Infrastruktura veřejného klíče

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

Pojmy z oblasti PKI

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

CESNET

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

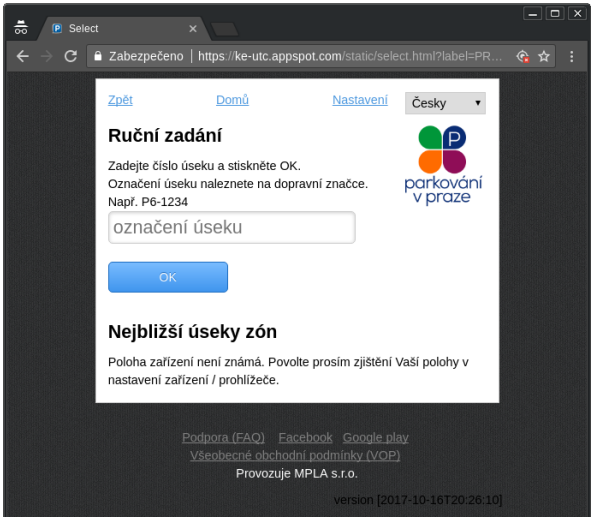
Slabiny certifikačních autorit

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

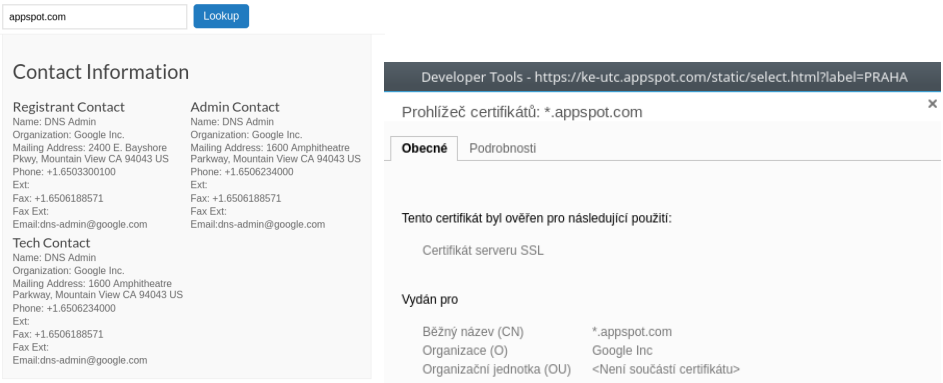
Zdroj: Jason Bourne's Passports Prop Replicas

Jak to má vypadat

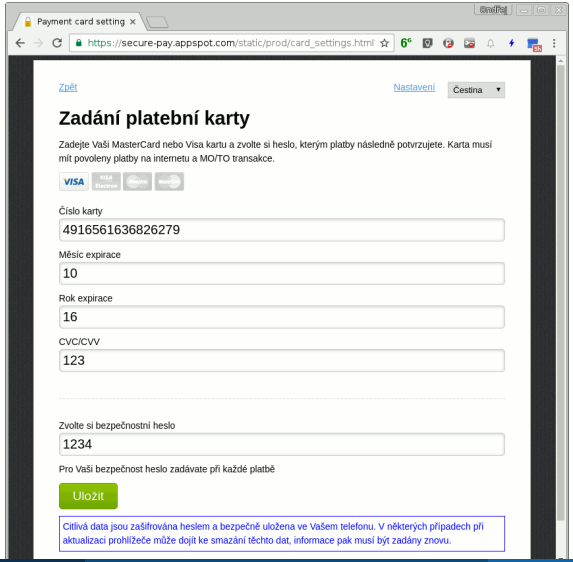
Nedůvěryhodná stránka



Nedůvěryhodná stránka



Nedůvěryhodná platební brána



Šifrování garantuje, že...

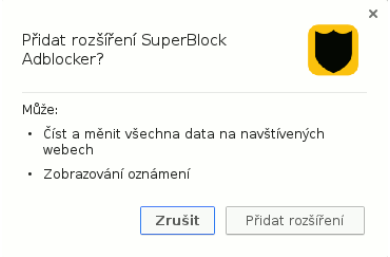
- data vidíme pouze my a ten, jehož certifikát vidíme
- nikdo další data neviděl
- nikdo další nemohl komunikaci pozměnit

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**

Známé 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 naší 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 veškrou 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

Spoiled Onions: Exposing Malicious Tor Exit Relays

Shrnutí

- nespoléhejte 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 síť používat, pořiďte VPN a nastavte automatické spojení

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://Ondřej.Caletka.cz

Prezentace již nyní ke stažení.