Co musíte vědět o šifrování

Ondřej Caletka

29. listopadu 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

Nejen, že může, ale i modifikuje

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

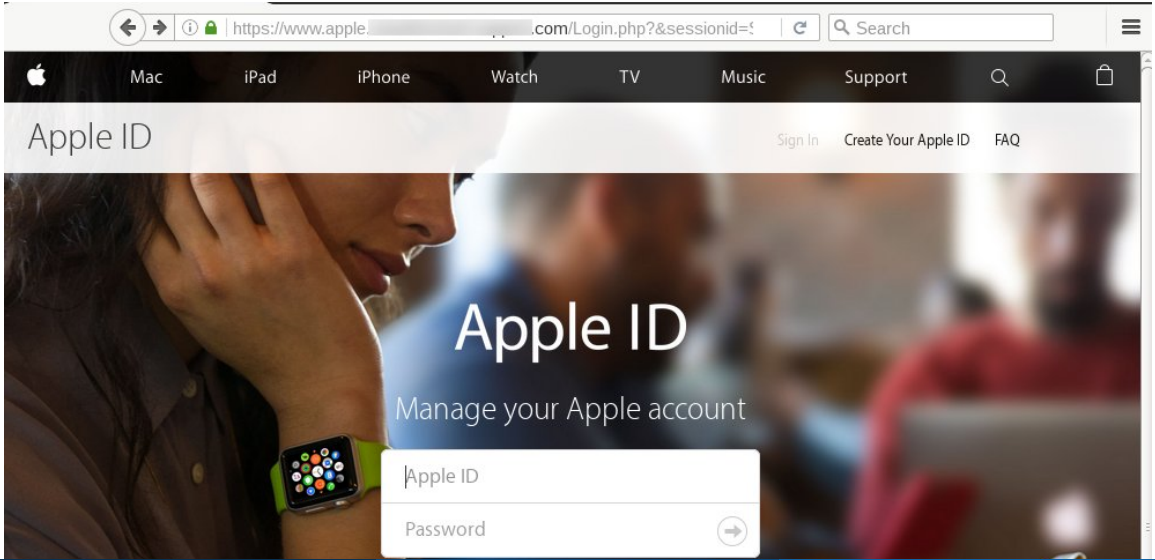
hop-by-hop zpráva se při průchodu sítí rozšifrovává a zašifrovává (typicky e-mail)

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

Šifrujeme úplně všichni

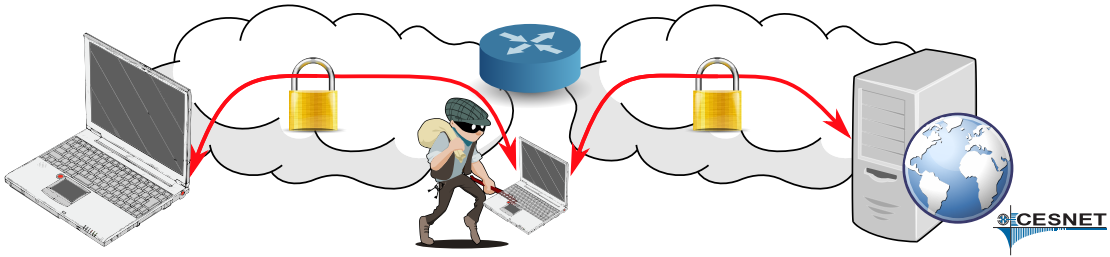
Šifrujeme úplně všichni

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* (např. PGP)
- bez autentizace lze zaútočit metodou **člověk uprostřed** (MitM)



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 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

Organzation 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

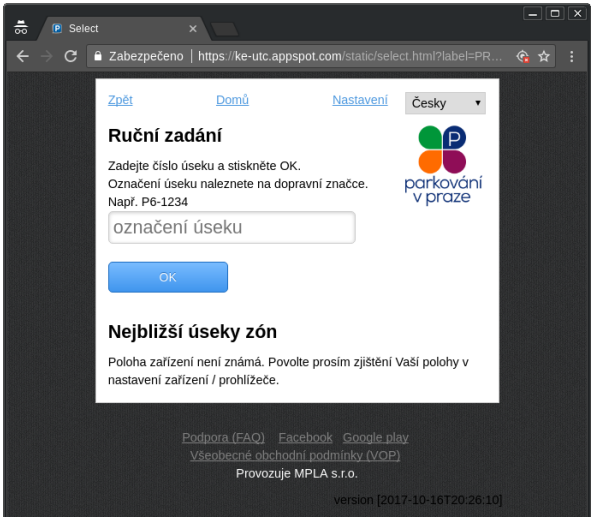
Slabiny certifikačních autorit

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

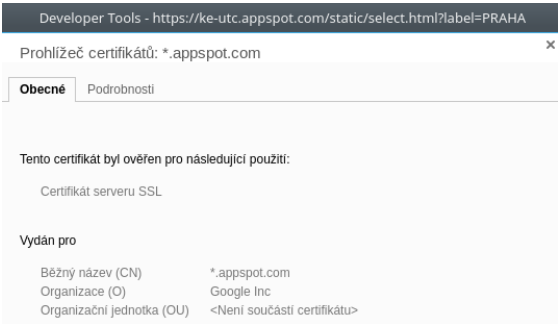
Zdroj: Jason Bourne's Passports Prop Replicas

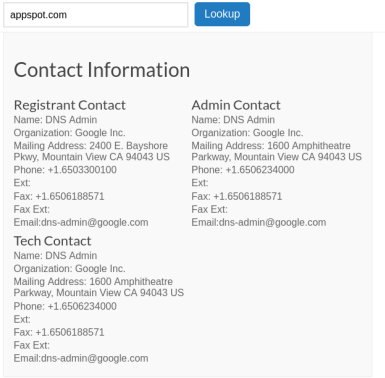
EV certifikáty v praxi

Nedůvěryhodná stránka

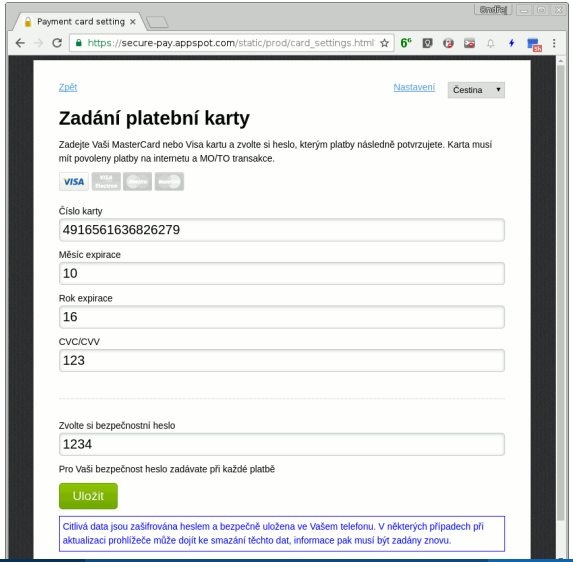


Nedůvěryhodná stránka





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
  - 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**

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 řádně ověřené šifrované spojení 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

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 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
- velmi často zasahují do komunikace

Spoiled Onions: Exposing Malicious Tor Exit Relays

Shrnutí

- nespoléhejte 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 síť používat, pořiďte VPN a nastavte automatické zapnutí VPN

Děkuji za pozornost

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

Prezentace již nyní ke stažení.