Bezpečné placení na Internetu

Ondřej Caletka

5. prosince 2016

Bezpečné placení

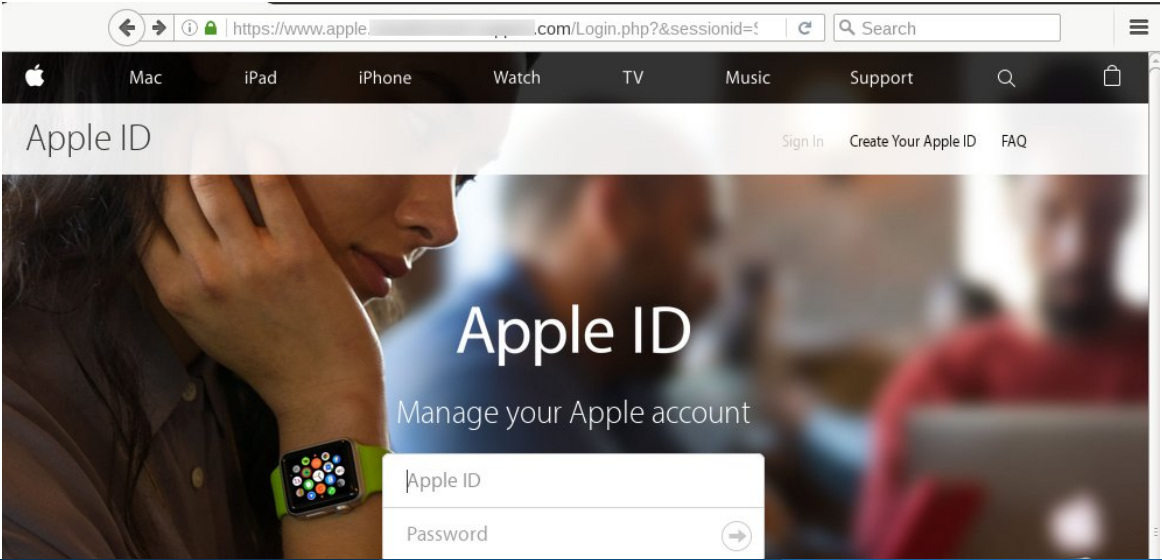
- internetové bankovnictví
- mobilní bankovnictví
- platební karty
- mikroplatební systémy


ČT 24
A vy už jste někdy šifroval?
Ondřej Závodský
náměstek pro hazard a majetek státu, MF

Šifrujeme úplně všichni

Šifrujeme úplně všichni

Jenom šifrovat nestačí



Jak to má vypadat

Šifrování garantuje, že...

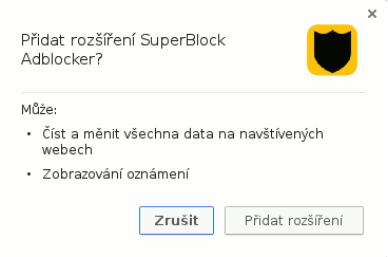
- data vidíme pouze my a ten, jehož certifikát vidíme
- nikdo další data neviděl
- nikdo další nemohl komunikaci pozměnit

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!**



Vícefaktorová autentizace

- nejčastěji SMS zprávou
- měla by obsahovat podstatné informace o transakci, **ne jenom kód**

Typické zneužití

- počítač uživatele je napaden malwarem
- malware zjistí jméno a heslo k internetovému bankovnictví
- malware zobrazí falešnou výzvu banky k instalaci nové bezpečnostní aplikace do telefonu
- tato aplikace přeposílá všechny přijaté SMS zprávy útočníkovi

Mobilní banka

- kumulace obou faktorů do jediného zařízení
- ověřování pomocí SMS nedává smysl
- obrovské množství známých chyb mobilních OS
- laxní přístup výrobců k pravidelnému záplatování
- rozumně nastavený limit je nutnost

Platební karty

- různé technologie
  - embosované číslo karty, samopropisovací papír
  - magnetický proužek
  - kontaktní čip
  - bezkontaktní čip
  - tokenizace
- různé druhy ověření držitele
  - žádné
  - PIN (vlastně PAN)
  - podpis
- off-line nebo on-line autorizace
- použití bez fyzické přítomnosti karty (MO/TO/eCommerce)

Bezkontaktní ano, či ne?

- o čistě kontaktní kartu je třeba explicitně žádat
- vždy je ale možné přerušit drátek antény
- riziko zneužití na dálku spíše teoretické
- snadné zneužití na podlimitní transakce při odcizení
- mnoho míst přijímá pouze bezkontaktní platby (např. MHD Plzeň, Ostrava, Liberec, Praha)
- důležité správně nastavit limity

http://www.mesec.cz/clanky/ne-bezpecne-bezkontaktni-karty-ukradli-jsme-desitky-tisic/

Emulace karty mobilním telefonem

- bezpečnější než fyzická bezkontaktní karta
- původní řešení s kartou jako aplikací na SIM kartě
  - neúspěšné
  - vyžadovalo správnou kombinaci karty, operátora a mobilního telefonu
  - postupně opouštěné (dnes už jen Fio)
- řešení založené na *Host Card Emulation*
  - kryptografické funkce přesunuty do cloudu
  - tokenizace – unikátní tajemství pro každou transakci
  - funkce i bez trvalého připojení k internetu
  - dostupné i u nás (ČSOB NaNákupy, mojeMobilní karta)
  - obdobně též v Apple Pay

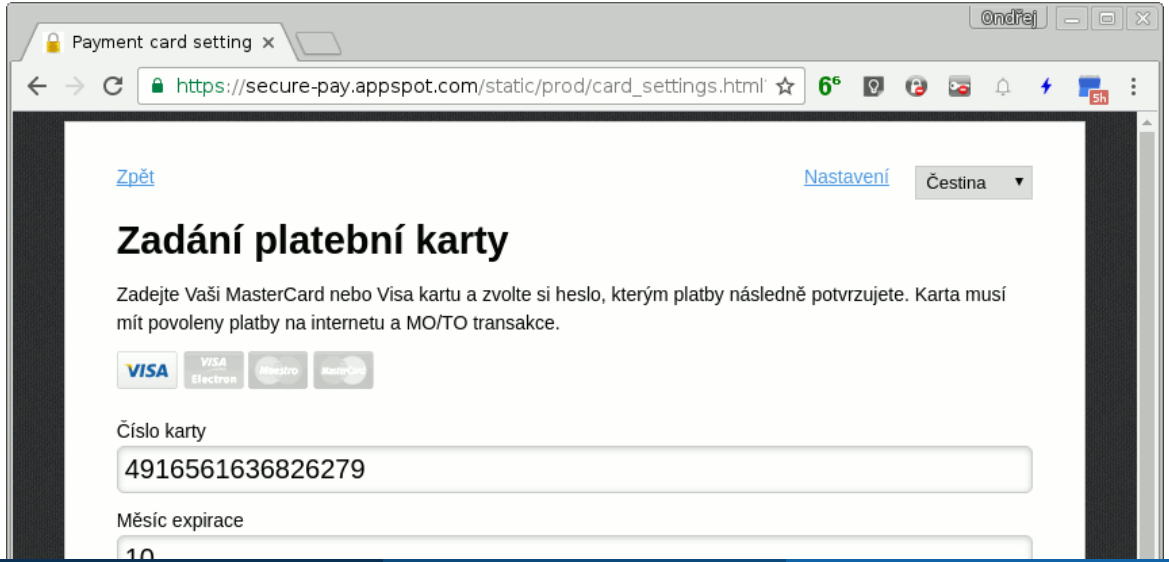
Bezpečnostní model platebních karet

- snaha o použitelnost na úkor bezpečnosti
- bezpečnost je především v dohledatelnosti a revokovatelnosti transakcí
- držitel karty
  - může reklamovat libovolnou transakci
  - má problém s prokázáním neprovedení transakce
  - pojištění zneužití karty mají různé podmínky (např. se vztahují pouze na ztrátu karty)
- příjemce platby
  - musí na požádání prokázat, že dodal zboží/službu držiteli karty
  - jinak musí vrátit peníze

Platba na internetu

- dnes v naprosté většina speciální kategorie *eCommerce* transakce
- možno nastavit samostatný limit
- bez fyzické přítomnosti se nikdy nepoužívá PIN
- dodatečné zabezpečení pomocí 3-D Secure
  - během platby je zákazník přesměrován na stránky vydavatele karty
  - vydavatel provede dodatečné ověření (typicky SMS)
  - pouze pro zapojené banky a platební brány
- nutno důsledně prověřit autenticitu platební brány
  - pozor na automatické ukládání karty v prohlížeči, v platební bráně, nebo přímo u obchodníka

Nedůvěryhodné platební brány



Sociální inženýrství

Falešné inzeráty a předplacené karty

1. Mallory si pořídí anonymní předplacenou kartu
2. Mallory ji aktivuje pomocí anonymní předplacené SIM karty
3. Mallory podá falešný inzerát na libovolné zboží
4. Alice odpoví na inzerát Mallory
5. Mallory požádá Alici o platbu předem, předá číslo účtu a variabilní symbol
6. Alice převodem dobije předplacenou kartu
7. Mallory ihned vybere hotovost z bankomatu a zmizí

http://www.mesec.cz/clanky/blesk-penezenka-laka-podvodniky-na-aukcnich-a-bazarovych-webech/

Social MitM

1. Bob nabízí prodej virtuálního zboží (např. Bitcoinů)
2. Mallory podá falešný inzerát na libovolné zboží
3. Alice odpoví na inzerát Mallory
4. Mallory objedná u Boba zboží
5. Mallory požádá Alici o platbu předem, předá platební údaje získané od Boba
6. Alice zaplatí přímo na účet Boba
7. Mallory přijme zboží od Boba a zmizí
8. Alice dohledá Boba a požaduje po něm vrácení peněz

http://www.lupa.cz/clanky/frantisek-fuka-prodal-jsem-bitcoiny-obvinili-me-z-podvodu/

Romance scam

- získání tzv. *bílých koňů* pro jinou trestnou činnost
- odpovídá na inzeráty v internetových seznamkách
- umělý ideální partner, *láska na první e-mail*
- je někde daleko v zahraničí, ale „brzy“ se vrátí
- nechce peníze, ale potřebuje účet u české banky
- přemluví oběť k otevření účtu na její jméno a předání karty a přihlašovacích údajů
- takový účet pak slouží pro *fyzikalizaci* ukradených virtuálních peněz

Spear phishing

- adresné oslovení na základě úniku dat
- oslovení přátel ze sociálních sítí
- požadavek na půjčení malého obnosu
- odkaz na falešnou platební bránu, o které kamarád tvrdí, že je přece bezpečná a známá

Další možnost: zneužití autorizačních zpráv

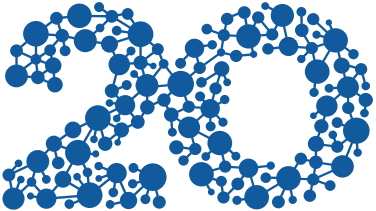
„Nejde mi poslat ověřovací kód na můj telefon. Můžu ho nechat poslat na tvůj? Přepošleš mi ho?“

Závěr

- bezpečné IT potřebujeme všichni, každý máme cenná data
- nikdy neuškodí dát číslo účtu nebo telefonní číslo do vyhledávače
- že vám píše osobně člověk kterého znáte, nemusí nutně znamenat, že je to on
- **hlavně nevypínat rozum!**

Děkuji za pozornost

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



1996–2016
CESNET
SPOLUPRÁCE
VÝZKUM
KOMUNITA