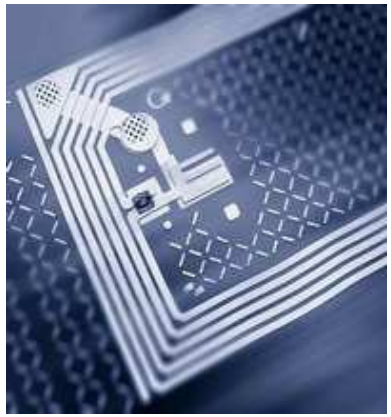
Autentizace v příkladech

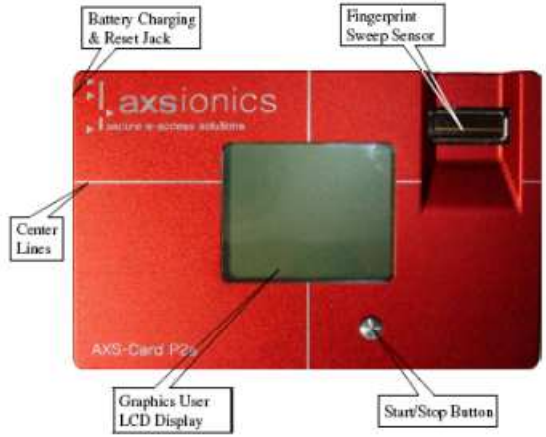


Masarykova univerzita
Fakulta informatiky

Honza Krhovják
Zdeněk Říha
Vašek Matyáš

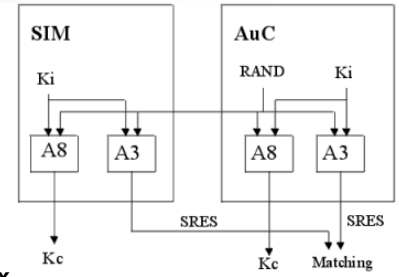
HW tokeny a jejich využití

- Uchovávání citlivých dat
  - zejména kryptografické klíče
  - údaje nezbytné pro využívání předplacených služeb
    - použití telefonní sítě, dekódování satelitního signálu
- Autentizace uživatelů
  - vstup do zabezpečené místnosti
  - přihlašování do operačního systému
  - přihlašování do GSM/UMTS sítí
  - přihlašování do e-bankovnictví
  - potvrzení finanční transakce či výběru hotovosti z bankomatu



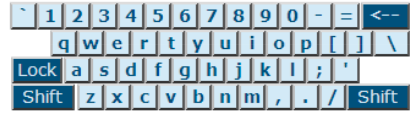
- Identifikace uživatelů
  - elektronické dokumenty (pasy, řidičské průkazy, atd.)

Autentizace do GSM sítě



- Dvoufaktorová autentizace
  - použití tokenu – Subscriber Identity Module (SIM)
    - čipová karta personalizovaná operátorem mobilní sítě
  - použití znalosti – Personal Identification Number (PIN)
    - umožňuje přístup k části dat/aplikací na čipové kartě
- Autentizace uživatele využívá sdílené tajemství
  - v každé SIM kartě je bezpečně uložen tajný symetrický klíč K_i
  - K_i uložen také v autentizačním centru (AuC) operátora
  - autentizační protokol (zjednodušeně)
    - na straně operátora vygenerováno náhodné číslo RAND
    - funkce A3 v AuC se vstupy RAND a K_i vygeneruje hodnotu SRES
      - RAND a SRES zaslána na přepínací centrum, a RAND dále do SIM
    - funkce A3 v SIM se vstupy RAND a K_i vygeneruje hodnotu SRES
      - SRES zaslána zpět na přepínací centrum ke srovnání s původní SRES

Autentizace a autorizace v e-bankovnictví



- Mnohdy pouze jednofaktorová autentizace
  - použití znalosti (tajné heslo)
  - mechanizmy zabraňující jednodušším útokům
    - testy délky a kvality hesla (v ideálním případě alespoň 10 alfanumerických a speciálních znaků)
    - virtuální klávesnice (zabraňující elementárním HW/SW keyloggerům zaznamenat stisky kláves)
    - SSL certifikáty & personalizovaný login (umožňující detekovat falešnou adresu s podvrženou přihlašovací stránkou)
- Dvoufaktorová autentizace
  - použití tokenu (čipová karta s klientským certifikátem) a znalosti (přístupový PIN)
  - použití tokenu (autentizační kalkulátor) a znalosti (přístupový PIN)
- Dodatečná autorizace citlivých operací a transakcí
  - používáno výše uvedených tokenů
  - mnohdy využíván separátní kanál (SMS zaslaná přes GSM síť)
    - využití SIM toolkitu: SMS zpráva je šifrována a chráněna přístupovým PINem

Autorizace finančních transakcí

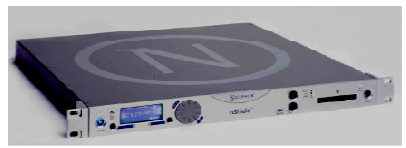
- Typicky dvoufaktorová autentizace
  - použití tokenu
    - karta s magnet. proužkem, čipová karta
  - použití biometriky nebo znalosti
    - peněžní bankomaty – PIN
    - bezhot. platba z místa prodeje – podpis nebo PIN
      - typicky závisí na typu (magnetický proužek nebo čip) i na druhu (např. MasterCard nebo VISA) karty
      - v praxi ne vždy výlučně (po PINu může být žádán i podpis)
    - bezhot. platba kartou z Internetu – CVV2/CVC/CID čísla

- Úspěšná autentizace je následována ověřením velikosti disponibilního zůstatku (je-li dostatečný, tak platba proběhne)
- Je-li autentizace neúspěšná, tak ji lze v závislosti na bezpečnostní politice vydávající banky několikrát zopakovat

Struktura bankovní sítě

- Základní terminologie
  - vydávající banka – banka kde má zákazník účet a která vydala vlastníkovi účtu kartu a PIN
  - poskytující banka – banka počátečně zodpovědná za transakci uživatele (např. provozující danou síť bankomatů či zajišťující příjem bezhotovostních plateb v místě prodeje)
- Banky vzájemně propojeny pomocí přepínačů
  - využití symetrické kryptografie (typicky 3DES)
    - potřeba předem ustavených tajných šifrovacích klíčů
- Kryptografické operace a bezpečné uložení klíčů obstarávají HW bezpečnostní moduly




Online verifikace PINu I

- Probíhá vzdáleně ve vydávající bance
  - potřeba bezpečného přenosu PINu od poskytující k vydávající bance (jiný PIN než u běžné čipové karty!)
    - banky si vzájemně nedůvěřují, nedůvěřují svým pracovníkům, a nedůvěřují ani zákazníkům
  - řeší HSM a různá administrativní/procedurální opatření
- Bankomat či platební terminál v místě prodeje je typicky bezpečné zařízení (HW bezpečnostní modul)
  - po vložení je PIN formátován do PIN-bloku
    - struktura obsahující PIN a další data zvyšující celkovou entropii
  - tento PIN-blok je odpovídajícím klíčem zašifrován a odeslán
  - na přepínačích dochází k přešifrovávání a někdy také k přeformátovávání PIN-bloku (různé sítě => různé formáty)

Online verifikace PINu II

- Originální PIN není v bance uložen
  - vygenerován v HW modulu na základě čísla účtu a bezpečně uloženého tajného PIN generujícího klíče
  - bezpečně vytištěn, zalepen do obálky, zaslán držiteli karty
- Verifikace také probíhá uvnitř HW modulu
  - přijatý PIN je dešifrován a extrahován z PIN-bloku
  - originální PIN je znovu vygenerován
  - přijatý PIN je srovnán s tímto originálním PINem
- Problém: nejednotnost standardů
  - mnoho formátů PIN-bloků, různé metody generování PINů a šifrování => špatná interoperabilita + bezpečný návrh HW modulů a jejich API se stává obtížný (ne-li nemožný)

Specifikace EMV

- Standard EMV 4.1 (Europay, MasterCard, VISA) je definován ve čtyřech samostatných dokumentech
  - aplikačně nezávislé požadavky na čipové karty a platební terminály
    - elektromechanické charakteristiky (např. rozměry čipu), přenosové protokoly, struktura souborů a příkazů, ...
  - bezpečnostní požadavky
    - mechanizmy offline autentizace dat a šifrování PINů, management kryptografických klíčů, ...
  - požadavky na jednotlivé aplikace
    - definice konkrétních APDU příkazů, ...
  - povinné, doporučené, a volitelné požadavky na platební terminály

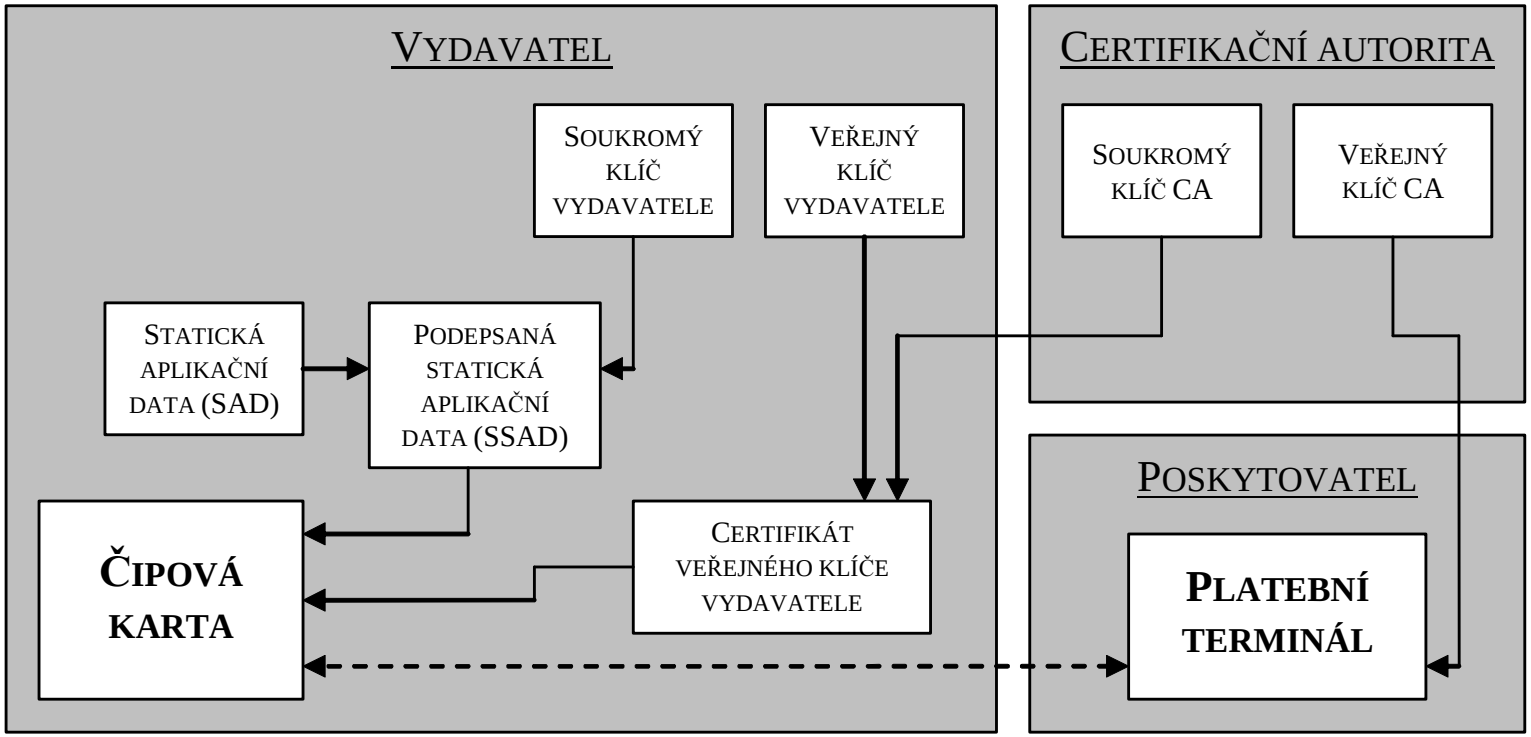
Offline autentizace dat

- Cílem je detekce falešných/padělaných karet
  - založeno na asymetrické kryptografii (RSA) a PKI
    - RSA veřejný exponent musí být vždy 3 nebo $2^{16} + 1$
  - vyžadována existence certifikační autority (CA)
    - certifikuje veřejné klíče vydávajících bank
    - každý terminál musí obsahovat veřejný klíč CA
    - musí být zajištěna integrita přenášených veřejných klíčů
- Tři základní mechanizmy
  - SDA: statická autentizace dat
  - DDA: dynamická autentizace dat
  - CDA: kombinovaná DDA a generování aplikačního kryptogramu

Statická autentizace dat I

- Základní vlastnosti SDA
  - potvrzuje pravost statických dat uložených v čipové kartě
    - detekuje neautorizovanou změnu dat po personalizaci karty
  - prováděna terminálem (čip pouze zasílá potřebná data)
- Princip a průběh SDA (obrázek na dalším slajdu)
  - veřejný klíč CA je uložen v každém terminálu
  - veřejný klíč vydávající banky je certifikován CA a uložen uvnitř čipu
  - statická aplikační data jsou podepsána soukromým klíčem vydávající banky a uložena uvnitř čipu
- Bezpečnost SDA
  - závisí na bezpečnosti soukromých RSA klíčů
  - padělání/duplikace čipových karet nevyřešena

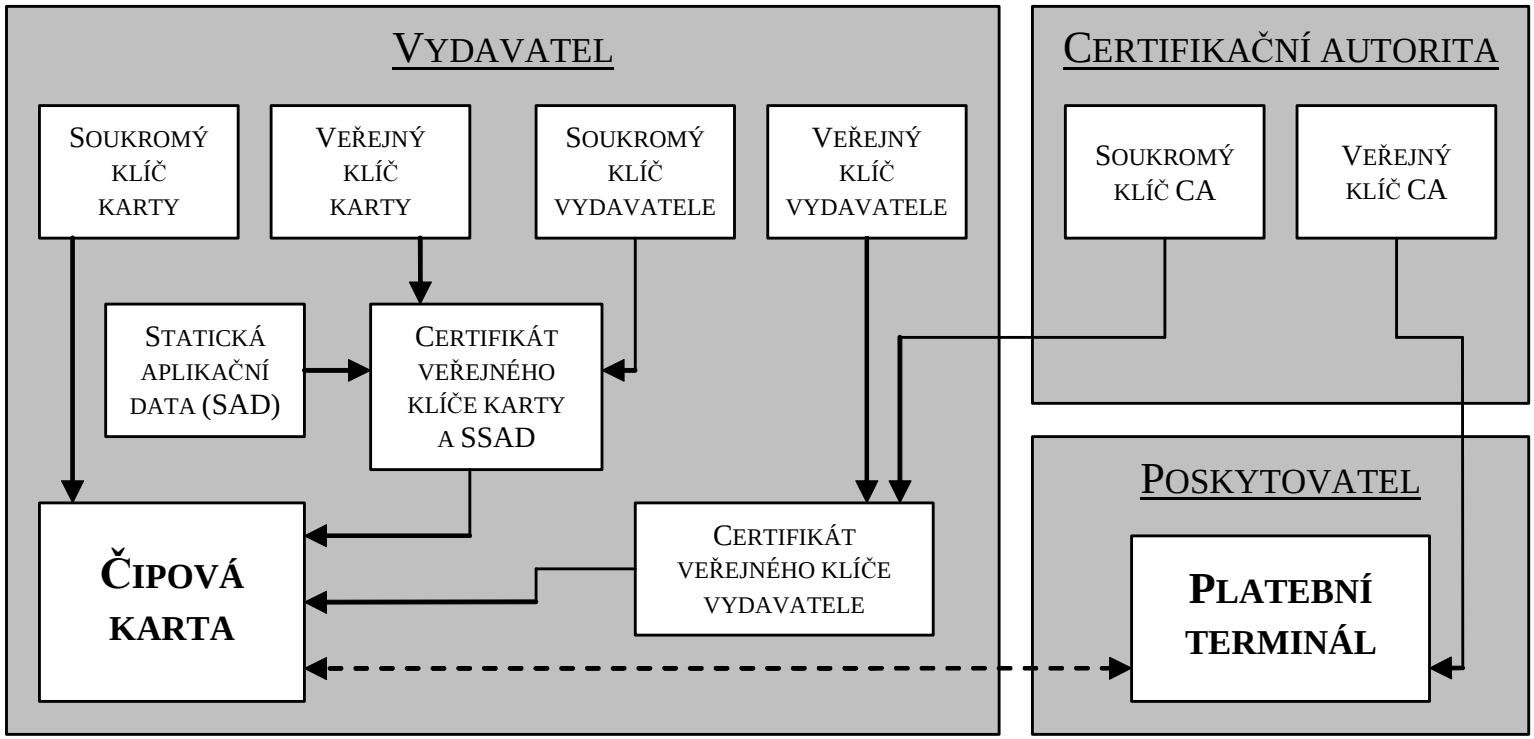
Statická autentizace dat II



Dynamická autentizace dat I

- Základní vlastnosti DDA
  - prováděna terminálem i kartou (potřeba čip s koprocesorem)
  - potvrzuje pravost statických dat uložených a generovaných v čipové kartě a dat obdržených z terminálu
    - detekuje padělané/duplikované karty
- Princip a průběh DDA (obrázek na dalším slajdu)
  - oproti SDA je v čipu uložen nový unikátní pár RSA klíčů
    - soukromý klíč je bezpečně uložen v čipu (nikdy jej neopouští)
    - veřejný klíč je podepsán a uložen společně ze stat. apl. daty
- Bezpečnost DDA
  - závisí také na bezpečnosti soukromých RSA klíčů
    - čipová karta musí být také schopna zajistit bezpečnost svého soukromého RSA klíče

Dynamická autentizace dat II



Kombinovaná DDA a ACG

- Základní vlastnosti CDA
  - prováděna terminálem i kartou společně s analýzou akcí karty (která se normálně provádí později)
- Princip a průběh CDA
  - náhodná výzva je oproti DDA součástí požadavku na získání aplikačního kryptogramu
  - je tedy i součástí podepsaného aplikačního kryptogramu
- Bezpečnost CDA
  - stejné požadavky jako v případě DDA
  - CDA navíc zabezpečuje zasílaný aplikační kryptogram
    - výhoda zejména pokud nelze garantovat bezpečnou komunikaci mezi terminálem a čipovou kartou

Dohoda autentizační metody

- Vzájemná komunikace mezi terminálem a kartou
  - Přichází na řadu ihned po offline autentizaci
  - Základní podporované metody
    - použití podpisu (ručně psaného)
    - použití PINu (online/offline, plaintext/encrypted)
    - některé kombinace (např. online => encrypted)
- Prioritně uspořádaný seznam podporovaných metod (CVM) je uložen v každé čipové kartě
  - terminál zvolí první podporovanou metodu ze seznamu
    - zvolená metoda je závislá na typu terminálu
    - jedna z metod může být „autentizace nevyžadována“
  - úspěšná verifikace PINu
    - alespoň jedna z metod úspěšně proběhla

Autorizace platby

- Autentizace založená na podpise či na online verifikaci PINu
  - stejný proces jako u karet s magnetickým proužkem
    - PIN je formátován do PIN-bloku, zašifrován, ...
  - čipové karty => ochrana proti skimmingu (zkopírování karty)
    - na kartě navíc uloženy 3 symetrické klíče (3DES, MAC)
- Autentizace založená na offline verifikaci se šifrováním PINu
  - vyžaduje nový RSA pár klíčů pro šifrování PINů
  - uložen/certifikován jako pár klíčů pro DDA (či CDA)
  - originální PIN (nutný pro verifikaci) bezpečně uložen v čipu
  - PINpad/terminál musí být fyzicky/logicky dobře zabezpečen

Automatická správa rizik

- Přichází na řadu po úspěšné autentizaci uživatele
- Ochrana proti hrozbám nedetekovatelným v offline prostředí
  - rozhoduje zda by transakce měla být:
    přijata offline, zamítnuta offline, autorizována online
- Správa rizik terminálu
  - kontrola horního limitu stanoveného obchodníkem
    - typicky při provádění několika malých oddělených transakcí
  - kontrola rychlosti oběhu peněz
    - omezení počtu po sobě jdoucích offline transakcí
  - náhodný výběr transakce pro online autorizaci
- Analýza akcí terminálu a karty
  - terminál má při zamítnutí transakce rozhodující slovo

Důsledky specifikace EMV

- Zajištění interoperability platebních systémů založených na použití kontaktních čipových karet
  - jeden standard (ideálně akceptovaný všemi stranami)
- Zavedením autorizace PINem je zodpovědnost za transakce převedena na zákazníka
  - výhodné pro banky i obchodníky – ne pro zákazníka
- Častá tvrzení o EMV a technologii Chip&PIN
  - EMV karty poskytují bezpečnější úložiště pro citlivá data
    - pokud se nepoužívá SDA
  - autentizace uživatelů pomocí PINu je bezpečnější
    - pokud je vyjednána bezp. autentizační metoda (předpokladem je dobře zajištěná integrita CVM)
  - protokol lze snadno přesměrovat (relay attack)
    - žádná ze zavedených techn. tomu nezabrání

Bližší informace na http://www.cl.cam.ac.uk/research/security/projects/banking/

Man-in-the-middle útok na EMV

- M-i-t-M útok na verifikaci PINu
  - funguje pro offline i online transakce (ověřeno v UK)
    - nezávisí na použití SDA či DDA
    - autentizační metoda „offline verifikace PINu“
  - chybí explicitní autentizace jednotlivých kroků během verifikace PINu
    - karta věří, že terminál nepodporuje PINy
    - terminál věří, že karta obdržela vždy správný PIN
      - kartě není PIN nikdy zaslán (žádný čítač se nesnižuje)
- Nefunguje pro výběry z bankomatu (odlišná „online“ verifikační metoda PINu)
- Nefunguje pro transakce prováděné přes Internet/telefon (nevyžadují PIN)

Bližší informace na http://www.cl.cam.ac.uk/research/security/banking/nopin/

Bezpečnost platebních terminálů

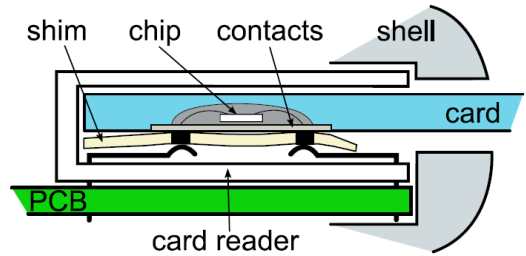
- Platební systémy v UK plně přešly na Chip&PIN
  - implementována pouze SDA (levnější karty)
  - kopie mag. proužku uložena ve veřejném certifikátu v čipu
    - mag. proužek se využívá pouze mimo UK
  - PINy zadávány uživatelem do platebních terminálů
    - terminál musí PINy dostatečně chránit
    - mají k němu volný přístup obchodníci i uživatelé
- Odolnost terminálů proti průnikům nedostatečná (i proti jednoduchým a levným útokům)
  - testovány dva modely platebních terminálů
    - Ingenico i3300 a Dione Xtreme PEDs
  - oba prošly VISA certifikací

Bližší informace na http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-711.pdf

Útoky na terminály

- Ingenico i3300
  - v zadní části terminálu přístupná nechráněná oblast
    - původně zamýšlena pro rozšíření funkcionality pomocí čipové karty (formátu SIM)
  - umožňuje snadné provléknutí drátku a napojení se na sériovou sběrnici terminálu

- Dione Xtreme
  - uvnitř terminálu umístěn nechráněný konektor
  - snadné provrtání (0.8 mm díra) a napojení se na nechráněný konektor (4 cm jehlice)
- Využití malé štěnice ve slotu pro karty
  - velmi obtížná možnost ochrany



Dopady a protiopatření

- Úspěšné odposlechnutí dat z terminálu vede k
  - získání PINu a přesné kopie mag. proužku
  - dostačující k vytvoření vlastní karty s mag. proužkem
    - lze zamezit neuložením přesné kopie mag. proužku do čipu
    - namísto CVV (crypto. checksum) je uložena hodnota iCVV
      - CVV zde nemá nic společného s CVV2 (vytištěné na kartě)
  - získání PINu zamezí až postupný přechod na DDA/CDA
- Aktivní ovlivňování terminálu
  - modifikace nepodepsaných CVM může umožnit zasílání nezašifrovaných PINů i v případě DDA/CDA
    - 8 z 15 prozkoumaných karet nemělo CVM podepsán
  - možnost plného M-i-t-M útoku proti podepsaným CVM

Platby s Chip Authentication Programme (CAP)

- Zamezení podvodů při provádění online transakcí (Internet/telefon)
  - nejrůznější útoky typu phishing a pharming
  - odcizování autentizačních dat (malware)
- Současná „řešení“ zamezují pouze offline útokům
  - zadávání jen některých znaků hesla, jednorázová hesla
  - metody náchylné na online M-i-t-M
- CAP vytváří kryptografickou vazbu mezi jednorázovým kódem a daty transakce
  - protokol převážně vychází z EMV
    - specifikace CAP ale není veřejně přístupná
  - objevují se první zranitelnosti (a útoky)

Bližší informace na http://www.cl.cam.ac.uk/research/security/banking/emvcap/

EMV/CAP a integrita

- Rozhraní dle ISO 7816 definuje jen slabou ochranu integrity příkazů zasílaných mezi platební kartou a terminálem
  - např. žádná kontrola integrity v odpovědi na příkaz GET DATA
- PIN (offline) verifikace není provázána s autorizací vykonávání APDU příkazů
  - karta umožňuje vykonávání kryptografických operací i bez zadání správného PINu
  - to (mimo jiné) umožňuje snadné provádění nejrůznějších experimentů či hledání útoků využívajících postranních kanálů
- Technické detaily (a nové postřehy) vztahující se k praktické proveditelnosti útoků na EMV/CAP lze nalézt ve slajdech Tomáše Rosy:

  http://crypto.hyperlink.cz/files/EMV_unleashed_rosa_v1.pdf

Autentizace finančních transakcí v praxi

- Chip&PIN vs. podpis
  - věříme ve zvýšení ceny nutné pro výrobu padělků
  - nebyli jsme si jisti, zda eliminuje *příležitostné* zloděje
    - zloděj (nebo malá skupina zlodějů) ukradne karty a následně padělá podpis nebo odpozoruje PIN
- Hlavní otázka
  - „Je pro zloděje jednodušší zneužít karty s technologií Chip&PIN nebo ty, co vyžadují podpis držitele?“
- Návrh a realizace experimentu
  - cílem bylo experimentálně ověřit naše domněnky

Bližší informace na http://www2.computer.org/portal/web/csdl/abs/html/mags/co/2008/02/mco2008020064.htm

Vlastní dvoufázový experiment

- První fáze „nanečisto“
  - byla provedena v částečně realistických podmínkách v univerzitní knihovně (Masarykova univerzita, FI)
    - věk nakupujících mezi 18 až 26 lety – studenti
    - čas pro nacvičení podpisu – 30 minut
    - čas pro nacvičení pozorování PINu – 2 hodiny
- Druhá fáze „naostro“
  - byla provedena v reálném obchodě
    - velký supermarket v Brně (velká fluktuace zákazníků)
    - podmínky této fáze experimentu byly stanoveny na základě zkušeností z první fáze

Příprava první fáze experimentu

- Několik místností
  - místo pro simulované nákupy – knihkupectví
  - místnost A pro lidi, kteří půjdou nakupovat
  - místnost B pro lidi, kteří provedli nákup

- Celkem se zúčastnilo cca 40 lidí
  - 32 zákazníků
  - 4 útočníci-pozorovatelé PINů
  - 3 okolostojící
  - 3 koordinátoři experimentu
  - majitel knihkupectví
    - obchodník, který běžně pracuje s plat. kartami

Normální chování nakupujících?

- Zákazníci nevěděli skutečnou podstatu experimentu
  - bylo jim řečeno, že testujeme uživatelskou přívětivost bezhotovostních plateb…
- Každý účastník vyplnil dotazník týkající se „zástěrky“
  - otázky zjišťující se časů potřebných pro autorizaci podpisem, resp. PINem…
  - …uživatelská přívětivost, zkušenosti
- Část týkající se falšování podpisu byla účastníkům sdělena po části s PINy
- Účastníkům bylo řečeno, že budou vyplňovat další dotazníky po experimentu, skutečnost ale byla jiná…

Vyhodnocení dotazníků

- Vedlejší efekt – 32 vyplněných dotazníků
- 25 z 32 účastníků využívají karty s magnetickým proužkem
- 1/2 účastníků někdy použila kartu s čipem

- Celková spokojenost (1 – nejlepší, 5 – nejhorší)
  - karty s mag. proužkem / podpis – 3,4
  - smart karty / PIN – 2,5

- Maximální únosný čas pro dokončení platební transakce (možnosti: 10, 20, … 50 sekund)
  - 21 s

- Celková úspěšnost transakcí
  - 89 % bez problémů, 7,5 % drobné problémy, 2 % velké problémy, < 2 % neúspěšné

První kolo – PINy

- Dva PINpady (viz obrázek)
  - dvě skupiny zákazníků (17/15)
  - první PINpad byl s masivním ochranným krytem
- Průběh nákupu
  1. zákazník přišel do obchodu (kde byly jiní „zákazníci“, pozorovatelé a „křoví“), vybral si a zaplatil zboží
  2. zákazník odešel z obchodu
  3. pozorovatelé nahlásili své tipy (každé číslici mohli přiřadit váhu 0–2)
  4. koordinátor měřil čas (kvůli „zástěrce“)
  5. do obchodu přišel další zákazník
- Otázka nedůvěryhodných obchodníků
  - poměrně snadné, např. CCTV namířených na PINpady

Druhé kolo – podpisy

- Dvě skupiny zákazníků
  - 15 zákazníků si kartu podepsalo svým podpisem
  - 17 zákazníků dostalo podepsanou kartu
    - V místnosti B měli 20–30 minut na nácvik
- Průběh – obchodník je zvyklý přijímat karty
  - v místnosti B zákazník dostal kartu se svým/cizím podpisem
  - obchodník ověřil podpis – identifikoval podvodníky
  - obchodník věděl, že se zákazníci budou podvádět, ale nevěděl kolik z nich to bude
- Poznámka: Zákazníci i koordinátoři se shodli, že ověřování podpisů bylo příliš důkladné – což bohužel není v běžných obchodech pravidlem

Výsledky prvního kola – PINpad1

- Pozorovatelé uspěli v 6ti ze 17ti PINů (35,3 %)
  - vzájemná spolupráce pozorovatelů
  - 5 ze 6ti PINů zcela přesně (83,3 %)
    - 3 PINy odpozorovány 2 pozorovateli
    - 2 PINy odpozorovány 1 pozorovatelem
    - 1 PIN zrekonstruován společně
- Z celkových 39 hlášených pozorování (tj. 156 číslic)
  - 75 číslic bylo pozorováno úspěšně (48 %)

Výsledky prvního kola – PINpad2

- Pozorovatelé uspěli v 12ti z 15ti PINů (80 %)
  - vzájemná spolupráce pozorovatelů
  - 10 z 12ti PINů zcela přesně (83,3 %)
    - 2 PINy odpozorovány 4 pozorovateli
    - 1 PIN odpozorován 3 pozorovateli
    - 4 PINy odpozorovány 2 pozorovateli
    - 3 PINy odpozorovány 1 pozorovatelem
    - 2 PINy zrekonstruovány
- Z celkových 46 hlášených pozorování (tj. 184 číslic)
  - 129 číslic bylo pozorováno úspěšně (70,1 %)

Výsledky druhého kola – podpisy

- Obchodník detekoval 12 ze 17ti padělaných podpisů
  - 5 cizích podpisů bylo přijato (29,4 %)
- Z 12ti detekovaných
  - 8 detekováno při prvním podepsání (25 %)
  - 4 detekování při druhém podepsání (12,5 %)
- Z 20ti (15+5) přijatých podpisů
  - 16 přijato při prvním podpisu (50 %)
  - 4 přijaty při druhém podpisu (12,5 %)
- 8 zákazníků (25 %) bylo požádáno o zopakování podpisu
  - Verifikace podpisů byla velmi důkladná!!!
  - Jeden zákazník při druhém podpisu vzdal ☺
  - Průměrná doba verifikace – 36 s

Příprava druhé fáze experimentu

- Skutečné platební karty
  - 5 pro první kolo – pozorování PINů
  - 6 pro druhé kolo – falšování podpisů
- Nutné právní kroky pro ochranu uživatelů karet
- Pouze několik lidí vědělo o experimentu
  - tým z Fakulty informatiky
  - vedoucí obchodu, bezpečnostní manažer, obsluha kamerového systému
- Nikdo z pokladních ani ostraha v obchodě o experimentu nevěděla
- Účastníci druhé fáze
  - 20 lidí (zpravidla příbuzných) se zúčastnilo jako „zákazníci“
  - celkem 15 lidí bylo „na druhé straně“…

Prostředí v obchodě

- Místnost pro instruování zákazníků
- Bylo nám umožněno použít libovolnou z určených pokladen (s ohledem na to, zda byla otevřena nebo ne)
- 1. kolo
  - tři skupiny pozorovatelů, každá pracovala nezávisle a v daném čase vždy pouze jedna skupina
  - dohled – pro případ, že by došlo k problémům a dohled na to, že je pozorován správný zákazník
- 2. kolo
  - zákazníci si nacvičili cizí podpis a provedli nákup
  - po nákupu nahlásili, zda ověření podpisu proběhlo úspěšně nebo nikoliv

Výsledky prvního kola – PINy (1)

- 13 pozorování na krytém a 7 na nekrytém PINpadu
- Pozorovatelé uspěli ve 4 z 20ti PINů (20 %)
  - Společná znalost
  - 3 PINy z krytého a jeden z nekrytého PINpadu
- 3 pozorování – správný PIN do 10ti pokusů
- 3 pozorování – správný PIN do 222 pokusů
- Z celkových 26 nahlášení 4-místného PINu (91 nahlášených číslic)
  - 38 číslic bylo odpozorováno správně (42 %)

Výsledky prvního kola – PINy (2)

	první fáze	*druhá fáze*
PIN (ochranný kryt)	6 ze 17 PINů (35%)	3 ze 13 PINů (23%)
PIN (bez krytu)	12 z 15 PINů (80%)	1 ze 7 PINů (14%)
Počet správně odpozorovaných číslic	**60%**	**42%**
Správné odpozorované číslice podle pozorovatelů		25%, 27%, **68%**

- Jedna skupina byla vysoce aktivní
  - jejím členům se dařilo často pozorovat zákazníky z výhodných pozic
  - nejlepší výsledky

Pozorování PINů v reálných podmínkách

- Úspěšnost 68 % pro třetí tým (23 z 34 číslic)
  - tento tým odpozoroval 4 PINy správně (na maximálně 3 pokusy)
- Nejlepší pozice pro pozorování je ve frontě přímo před a přímo za pozorovanou osobou
  - pozice pozorovatelů za pokladnami se ukázala jako nevýhodná
    - tito pozorovatelé předstírali činnost brigádníků
    - jejich pozorování nebylo při vyhodnocování bráno v úvahu

Výsledky druhého kola – podpisy

- 20 „zákazníků“
  - většina z nich byli pozorovatelé z prvního kola
  - 10–30 minut pro nácvik podpisu
- Druhé kolo bylo zastaveno po 17ti úspěšně ověřených podpisech
  - v průběhu kola nebyl nahlášen žádný problém při ověřování
  - nikdo nebyl požádán o zopakování podpisu
- Některé podpisy byly kontrolovány velmi zběžně nebo vůbec!
- V obchodě není stanovena hranice pro důkladnější kontrolu podpisu (např. když je částka > 1000 Kč…)

Shrnutí obou fází

- Správně odpozorované číslice PINů (60 % a 42 %)
- Ochranný kryt klávesnice je užitečný, nicméně
  - většina PINpadů jej nemá
  - slabé (málo efektivní) kryty v obchodech
  - někteří zákazníci mohou mít problémy při použití PINpadu s masivním krytem
- Skutečně znatelný rozdíl při detekci falešných podpisů (70 % vs. 0 %) – prostor pro zlepšení
- Pozorovatelé a osoby falšující podpisy byly začátečníci
  - byla to jejich první práce tohoto druhu… ☺

Názory a spekulace

- Pečlivost kontroly podpisu je odlišná
  - v různých zemích
  - v různých obchodech (v téže zemi)
- „Profesionální“ zneužití karet je mnohem důležitější než náhodné zneužití
  - platí dnes – co v budoucnosti?
- Dočasné opatření (?)
  - použití jak PINu tak podpisu
  - různé PINy pro různé typy transakcí (v závislosti na částce)

Shrnutí

- Technologie Chip&PIN nezlepší bezpečnost zákazníků oproti náhodným zlodějům
  - problémové odmítnutí falešné transakce
  - pojištění karty a ověření vlastnictví je velmi důležité
- **Dobrý** ochranný kryt PINpadu
  - pokladny v obchodech nejsou nejvhodnějším místem pro zadávání PINů
- Ověření na základě podpisu (ve standardním obchodě) je zcela nedostačující (jinak např. v klenotnictví)
- Pozorování PINů je poměrně podceňovaná oblast
  - podobně i v jiných podmínkách, např. kanceláře

Zasílání PINů poštou...

- Bezpečnost PINů zasílaných poštou
- Impulzem byla snadnost přečtení PINu z uzavřené obálky u ČS
  - 100% úspěšnost při prosvícení běžným zdrojem světla
  - šance útočníků nepozorovaně zjistit citlivé informace
- Česká spořitelna, eBanka, GE, HVB Bank
  - celkově 20 obálek (zaslané poštou, některé nedoporučeně)
- Zdroje světla
  - kapesní svítilna
  - optická myš (LED)

Bližší informace na http://www.ics.muni.cz/bulletin/articles/562.html

Česká spořitelna

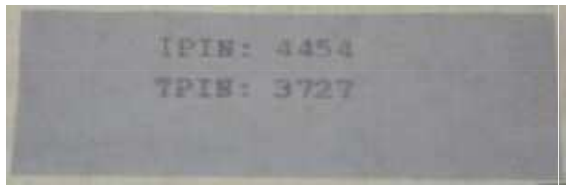
- PIN mailer využívající laserového tisku
  - v obálkách jeden list papíru s vytištěným PINem
  - prosvícení třech papírů + dvě černé krytí

- Prosvěcování bylo nejsnazší
  - nebyla nutná absolutní tma
  - i začátečník dosáhl 100% úspěchu

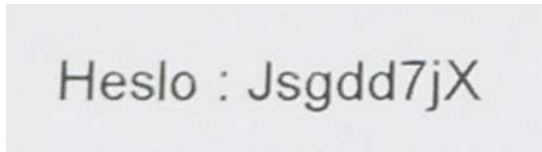
- Starší obálky – průklepový tisk
  - bez úspěchu (PIN vytištěn velmi slabě)
  - průklepový tisk => nerovnosti na obálce
    - možné řešení – umístění do další (vnější obálky)

eBanka a GE Money Bank

- PIN, přihlašovací údaje pro iBanking
- Pouze průklepový tisk (až 4 vrstvy krytí)
  - horší výsledky (1 ze 4 PINů)

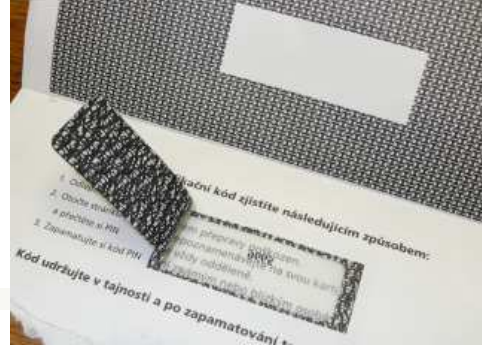


- PINy – průklepový tisk, bez úspěchu
- iBanking – laserový tisk
  - heslo vytištěno výrazně větším písmem



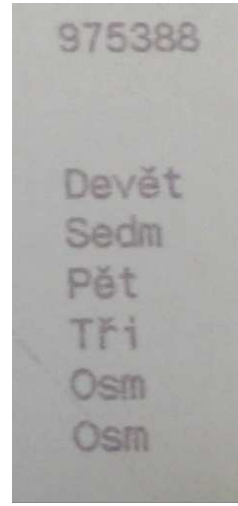
  - při prosvícení přečteno zcela bez problémů

HVB Bank



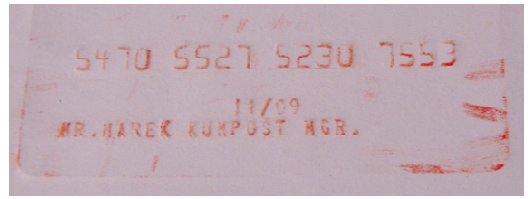
- PINy – laserový tisk, odnímatelná fólie
  - jeden PIN (ze dvou) se podařilo přečíst

- Tele-Banking – průklepový tisk, dvě krytí
  - určení pozice a délky PINu + 6 řádků textu
    - 6-ti místný PIN + číslice zapsané slovně
  - možnost zjištění PINu podle slovního zápisu nebo prvního (velkého) písmene
    - i tak je určení hodnoty PINu poměrně obtížné



Embosované karty a další pozorování

- Problém při posílání karet poštou (HVB)
  - snadno lze získat informace z obálky



  - vytvoření padělku karty
- Různé úrovně vyškolení personálu banky
  - GE – hodnota aktivačního kódu
  - HVB – změna limitů zasláním e-mailu
    - žádné ověření e-mailové adresy
- ČS – autentizační SMS zprávy
  - potvrzení převodu peněz, ale ne změn příjemců
- eBanka – social engineering např. při tel. hovoru

Shrnutí

- Banky nezareagovaly na publikované problémy PIN-mailerů
- Laserový tisk poskytuje menší ochranu
  - dobré výsledky s ostrým světlem
  - není nutná naprostá tma
- Průklepový tisk
  - dobré výsledky s kapesní svítilnou
  - nutná naprostá tma
- Počet krycích vrstev nehrál významnou roli
- Redundantní informace o PINech ulehčují útoky
- Posílání embosovaných karet poštou zcela nevhodné
- Autentizační mechanizmy nutno aplikovat na veškeré operace

Závěr

- Každý systém je bezpečný tak, jako je bezpečný jeho nejslabší článek
  - způsob generování, tisku a zasílání PINu
  - manipulace s PINem a jeho bezpečné zadávání
  - bezpečnost platebních terminálů a bankomatů
  - bezpečnost dat na platební kartě a jiných zařízeních
  - zabezpečení dat na cestě do banky a v bance
  - zabezpečení elektronického bankovnictví
  - problém nedůvěryhodných obchodníků
- Zlepšením pouze jediné části systému (např. přechodem na technologii Chip&PIN) nelze dosáhnout výrazného zvýšení celkové bezpečnosti

- Příště: Identifikace uživatelů a elektronické dokumenty
  - systémy zaváděné do praxe v současné době…

Otázky???

Děkujeme za pozornost! ☺