Elektronická bezpečnost – kreditní karty, mobily, internetové bankovnictví

PV080

Vašek Matyáš
spolupráce Jan Bouda, Marek Kumpošt

Co je to elektronická bezpečnost?

- Bezpečnost při používání elektronických zařízení obecně
  - Počítačová bezpečnost
  - Mobilní telefony
  - Kreditní karty
  - Internetové bankovnictví
- Nejedná se o bezpečnost práce, ale o omezení rizik plynoucích ze zneužití daného zařízení

Cíle elektronické bezpečnosti

- Zamezit zneužití elektronických zařízení
- Nalézt osobu pokoušející se o zneužití
- Minimalizovat škody způsobené zneužitím
- ...

Autentizace entit (uživatelů)

Autentizace entit

- Elektronická zařízení musí navzájem prokazovat svou identitu
- Kreditní karta prokazuje svou identitu bankomatu
- Mobilní telefon (SIM karta) prokazuje svou identitu přijímající radiostanici mobilního operátora

Metody autentizace osob

- Znalost nějakého tajemství
  - PIN kreditní karty
  - Heslo pro telefonního bankéře
- Fyzická vlastnost (biometrika)
  - Otisk prstu
  - Sítnice oka
  - Hlas

Metody autentizace osob

- Vlastnictví nějakého předmětu (tokenu)
  - Vlastnictví kreditní karty
  - Vlastnictví SIM karty v mobilu
  - Vlastnictví klíče ke dveřím
- Kombinace předchozích
  - Kreditní karta a PIN
  - Občanský průkaz = token, fotka = biometrika

Metody autentizace

- SIM karta v mobilu je elektronické zařízení
- Moderní kreditní karty jsou elektronická zařízení
- Hlavním problémem autentizace je, aby se ten komu se prokazujete nemohl později vydávat za vás
- Někdo může proces autentizace pozorovat, nahrávat, odposlouchávat

Metody autentizace

- Při vsunutí (staré) kreditní karty do bankomatu zloději používali zařízení, které přečetlo magnetický pásek a umožnilo jim vytvořit kopii
- Nad bankomaty může být umístěna malá kamera, která nahraje zadávání PINu
- Zloděj takto získá kopii karty a PIN

Typy autentizace elektronických zařízení

- Pomocí hesla
  - Ověřující může ukrást identitu
- Pomocí důkazu nulového rozšíření znalostí
  - Osoba prokazuje, že zná řešení nějakého problému. Prokazování probíhá tak, že ověřovatel je na konci přesvědčen, že osoba dané tajemství zná, ale ověřovatel ani v budoucnu nebude schopen přesvědčit další osobu, že tajemství zná.

Mobilní telefony

Krádež mobilního telefonu

- Ukradený telefon lze i při zabezpečením PINem snadno odbklokovat
- Najít člověka, který jej odblokuje je snadné a tedy i levné (cca 500 Kč u nelegálního odblokování PINu)
- Odblokování SIM karty je velmi nepravděpodobné
- Její používání po krádeži je nebezpečné

Krádež mobilního telefonu

- Mobilní telefon s ukradenou SIM kartou lze identifikovat, lokalizovat a následně zaměřit
- Zneužití údajů uložených v ukradeném telefonu
  - Telefonní seznam
  - Osobní plán
  - Záznamy o bankovních převodech
  - Audio, video, fotky, ...
  - Vydírání, krádeže, …

Zneužití bezdrátového přenosu

- Odposlech telefonního hovoru
  - Šifrování v GSM má velmi nízkou bezpečnost
  - Do standardu byly (úmyslně?) zavedeny chyby, které měly zmást konkurenční telefonní společnosti.
  - V mnoha zemích (USA, Turecko, …) se šifrování nepoužívá vůbec.
  - Lze odposlechnout díky jednoduchému zařízení.

Zneužití bezdrátového přenosu

- Zneužití identity volaného
  - Poškození pověsti
  - Získání obchodních výhod
- Volání „na cizí účet“
- Přes relativní snadnost vyžadují tyto útoky jisté technické znalosti
- Přechod na standard 3GSM – navržen kvalitně

Zneužití přídavných zařízení

- Bluetooth
  - Handsfree, synchronizace s počítačem a PocketPC
  - Návrh obsahuje mnoho bezpečnostních chyb
  - Zařízení v mobilech mají udávaný dosah 10m
  - Bluetooth puška dokáže odposlech na 1 km

Zneužití operátorem

- Operátor může sledovat všechny hovory
  - Někteří zaměstnanci operátora mohou být schopni sledovat všechny hovory
- Záznam zvuku je zatím naštěstí relativně náročný na kapacitu úložných zařízení a obtížně se automatizuje jeho zpracování.
- SMS zprávy zaberou málo místa a snadno se automaticky vyhodnocují.

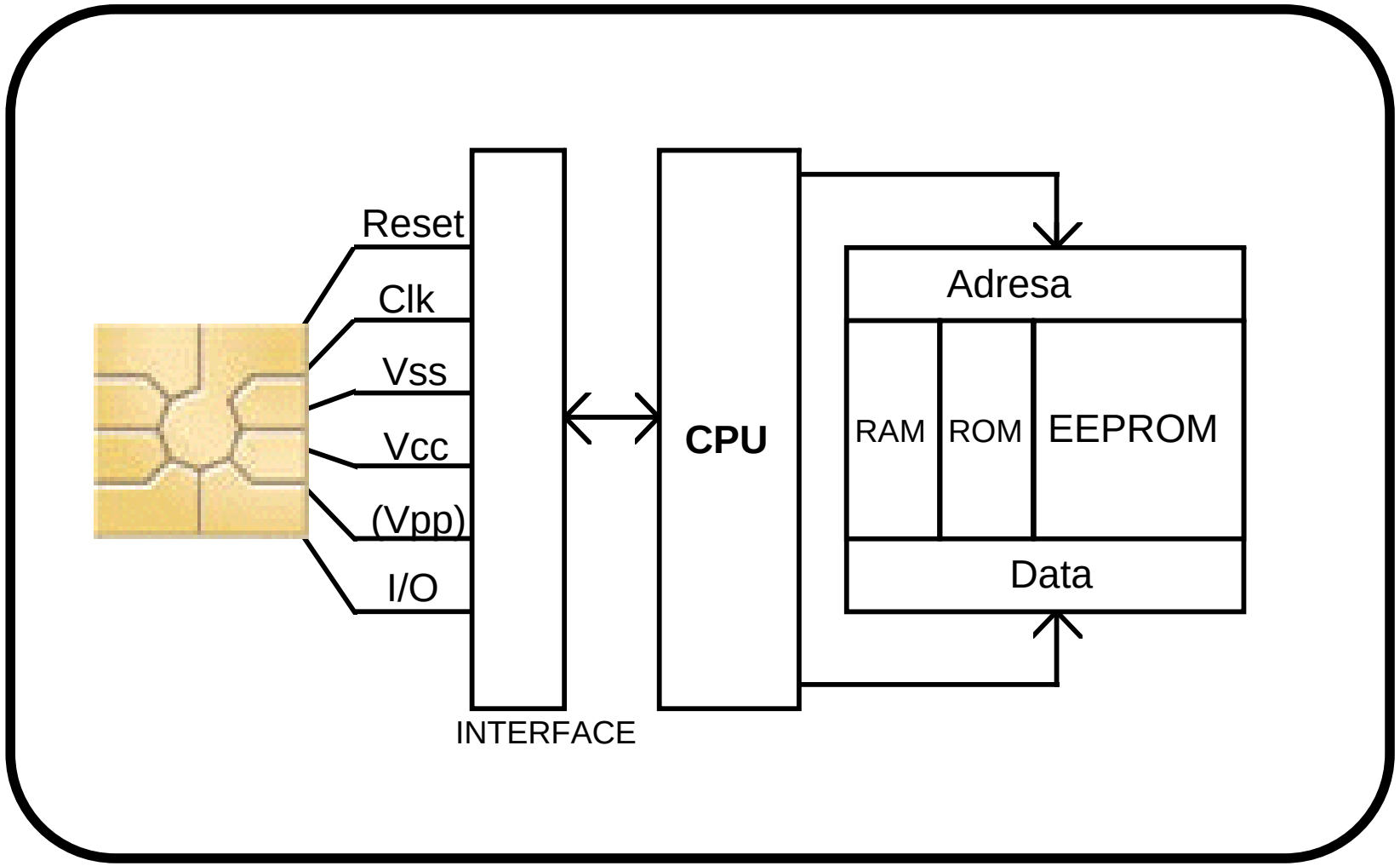
Zneužití operátorem

- SMS posílané z mobilu na mobil nebo z internetu při udání čísla odesilatele mohou být a někdy také jsou ukládány!
- Mohou být poskytnuty legálně na základě žádosti soudu, nebo nelegálně zneužity zaměstnancem – prodány třetí osobě.
- Je možné sledovat polohu mobilních telefonů!
- Použito při vyšetřování útoků v Londýně.

Platební karty

Princip uložení údajů

- Historický – psané údaje na embosované kartě
  - U ‘terminálu’ se údaje přetiskly na papír a poté použily při účtování platby
- Magnetický proužek
  - Obsahuje údaje o kartě, případně majiteli
  - Upravená čtečka je schopna údaje zkopírovat a později lze snadno vytvořit kopii


Reset
Clk
Vss
Vcc
(Vpp)
I/O
INTERFACE
CPU
Adresa
RAM
ROM
EEPROM
Data

Princip uložení údajů

- Karty s čipem
  - Čip neposkytuje bankomatu své kompletní údaje, je schopen provádět výpočet a může se autentizovat pokročilými kryptografickými technikami
  - Bez technicky velmi náročného rozebrání čipu a jeho analýzy není možné vytvořit jeho kopii
  - Jiné útoky, které nevyžadují kopii čipu existují

Princip uložení údajů

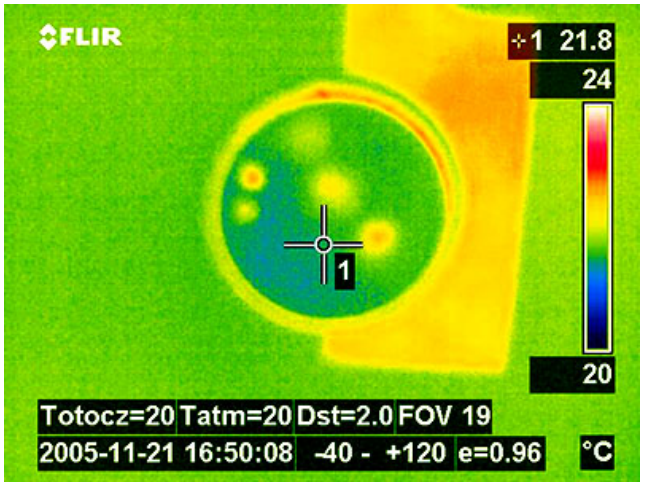
- Ne všechny bankomaty a terminály čip používají!
- Karty s čipem mají i magnetický proužek kvůli zpětné kompatibilitě.
- Dají se zkopírovat (bez čipu) a použít na terminálech nevyžadujících čip.

PIN

- Pro ztížení použití kopie karty nebo použití ukradené karty je u některých karet vyžadován PIN.
- PIN lze snímat kamerou umístěnou na horní stěně bankomatu.
- Nestačí jen zakrýt prsty, k určení PINu stačí vidět pohyb ruky!

PIN

- Při použití kamery citlivé na tepelné záření lze PIN odečíst z klávesnice po zadání na základě teploty kláves.
  - Lze zjistit i pořadí stištění kláves
  - V praxi závisí na okolní teplotě



- PIN lze odpozorovat při zadávání u bankomatu, obchodního terminálu, …
- Pokus na FI MU – získáno přes 35 % PINů u PINpadu s krytem, 80 % u PINpadu bez krytu

Jak obtížné je odpozorovat PIN?

- Několik tajných studií, veřejnosti výsledky zamlčovány
- Experiment – dvě fáze
- První fáze „nanečisto“
  - Byla provedena v částečně realistických podmínkách v knihkupectví FI
    - věk nakupujících mezi 18 až 26 lety – studenti
    - čas pro nacvičení podpisu – 30 minut, pozorování PINu – 2 hod

- Druhá fáze
  - Byla provedena v reálném obchodě
    - velký supermarket v Brně
    - podmínky stanoveny na základě zkušeností z první fáze
- Detaily v přednáškách PV157

Shrnutí experimentu

- 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
- Správně odpozorované číslice PINu (60 % a 42 %)
- Značný 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… ☺

„Okrajové“ postřehy

- Útočníkova nejlepší pozice pro pozorování PINu je ve frontě přímo před a přímo za pozorovanou osobou

- Pečlivost kontroly podpisu je odlišná
  - V různých zemích
  - V různých obchodech (v téže zemi)

- Dočasné opatření (?)
  - Použití jak PINu tak podpisu – se skutečnou kontrolou
  - Různé PINy pro různé typy transakcí (v závislosti na částce)

Platební karty a platby po internetu

Platební karty a internet

- Některé kreditní karty lze použít k platbám po internetu
- Obvykle lze použít embosované nebo tzv. virtuální platební karty.
- Mnoho bank své karty při vydání bloku – nedají se na internetu použít. Na žádost je lze odblokovat.
- K platbě na internetu obvykle stačí zadat číslo karty, jméno a datum platnosti, případně nějaký kód (jiný než do bankomatu – z druhé strany karty).

Kreditní karty a internet

- Každý obchodník, kterému tyto údaje poskytnete, je může použít k zaplacení také.
- Tyto údaje si obchodníci ukládají.
- Mohou je zneužít jejich zaměstnanci
- Tyto údaje může někdo odposlechnout
- Pokud vám banka tvrdí, že používá zabezpečený přenos a nemůže se nic stát – tak LŽE.

Kreditní karty a internet

- USA a částečně i Západní Evropa
  - Za zneužití karty nese obvykle zodpovědnost banka
  - Zákazník může platbu reklamovat a banka je povinna vzít ji bez dalšího šetření na sebe
  - Zákazník má spoluúčast max. cca 2000 Kč
- České banky
  - Zneužití (téměř vždy) platí zákazník
    - Banka mu tvrdí, že celý systém je bezpečný
    - „Řešením“ je pojistka, ale obvykle placená klientem
  - Změna v listopadu 2010 – vynucená legislativou EU
    - Limit zvlášť na každou transakci
    - Důkazní břímě na žalující straně... ☹

Platební karty a internet

- Celý systém funguje, protože ztráty způsobené zneužitím jsou nižší než zisky z tohoto systému.

Internetové bankovnictví

Co je internetové bankovnictví?

- Umožňuje provádět bankovní operace bez návštěvy banky
- Možnosti a bezpečnost se u jednotlivých bank liší
- Výpis z účtu, převod na jiný účet, výpis z karty, zadání/zrušení inkasa, nákup podílových listů, převod na termínované vklady, …

Nutné vybavení

- U většiny aplikací stačí běžný počítač, téměř libovolné připojení na internet a relativně moderní internetový prohlížeč.
- Pozor, pokud má k počítači přístup ještě někdo jiný, může u některých produktů internetového bankovnictví získat přístup k vašemu účtu
  - Jedná se ale o velmi odbornou a časově náročnou operaci

Způsoby autentizace

- Je nutno systému prokázat svou identitu
- Pomocí hesla
  - Zastaralé, žádná rozumná banka už toto řešení nemůže používat
  - Kdokoliv kdo získá heslo (odposlechne, získá od pracovníka banky, …) může používat váš účet

Způsoby autentizace

- Osobní klíč (názvy se podle banky různí)
  - Obvykle se jedná o tajný klíč pro asymetrickou kryptografii
  - Je uložen na CD, USB disku, SD-kartě nebo čipové kartě
  - Poskytuje rozumnou úroveň bezpečnosti, pokud je tento systém bankou rozumně implementován (není tomu tak u několika českých bank)
  - Uložení (a používání) na čipové kartě je nesrovnatelně bezpečnější než ostatní zde uvedená řešení

Průběh autentizace

- V prohlížeči si otevřete stránku pro přihlášení do banky
- Prohlížeč stáhne na váš počítač aplikaci, která bude dále s bankou komunikovat
  - Toto je obvykle nejméně bezpečný bod!
  - Musí být **spolehlivě** zajištěno, že místo originální aplikace vám nebyla ‘podstrčena’ jiná

Průběh autentizace

  - To lze zajistit buď tak, že si aplikaci vyzvednete v bance na CD a z internetu ji nestahujete, nebo musí být aplikace podepsána klíčem, který JE ULOŽEN VE VAŠEM POČÍTAČI
  - U nejmenované banky bylo ještě nedávno podepsání provedeno klíčem, který není v počítači uložen, je poslán s aplikací.
- Stažená aplikace si od vás vyžádá heslo, kterým je certifikát na CD zašifrován.

Heslo na čipové kartě

- Pokud je heslo dobře uloženo na čipové kartě, nemá k němu aplikace přímo přístup.
- Nebezpečí ze strany podvržené aplikace a nedůvěryhodného počítače je podstatně menší.

Autentizační ‘kalkulačka’

- Bezpečnost je srovnatelná s čipovými kartami.
- Vzdálený počítač vám pošle tzv. výzvu
- Tu zadáte do své ‘kalkulačky’ a na displeji se objeví odpověď, kterou zadáte do počítače
- Celá komunikace je téměř na úrovni zero-knowledge

Shrnutí

- Je potřeba uvážit samostatně jakou bezpečnost poskytuje daný produkt konkrétní banky
- Nemůžete spoléhat na informace pracovníků u přepážek – jsou pouze minimálně proškoleni a to většinou tak, aby říkali, že je vše bezpečné.
- Nejvyšší bezpečnost může poskytnout osobní klíč uložený na čipové kartě a autentizační ‘kalkulačka’ – tyto ale samy o sobě nejsou garancí bezpečnosti