

# Počítačová bezpečnost – kreditní karty, mobily, internetové bankovníctví

PV080

Vašek Matyáš

spolupráce Jan Bouda, Marek Kumpošt

# Cíle počítačové bezpečnosti

- Zamezit zneužití počítačů (a počítačových komunikací)
- 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 zabezpečení PINem snadno odblokovat
- 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 přídatných 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.



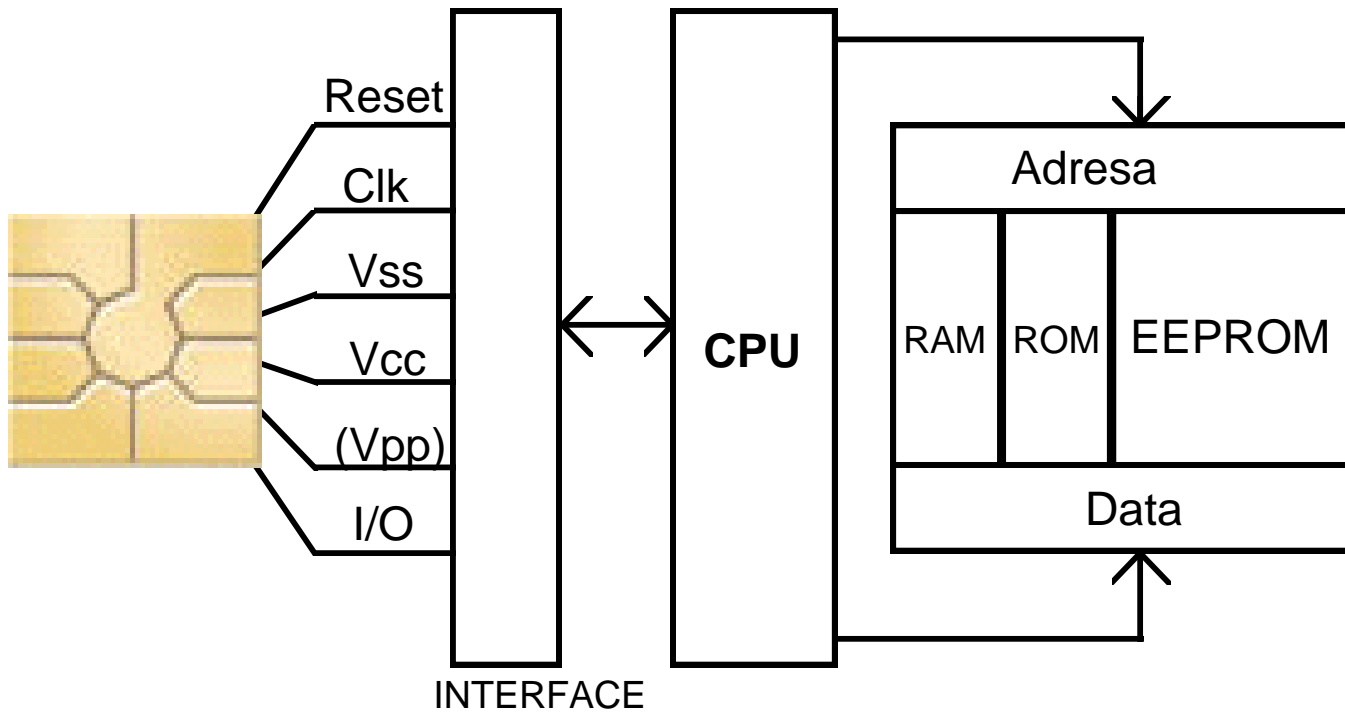
# Zneužití operátorem

- 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!
- Data retention!!!

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



# 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-paráda

Analýza 3,4 milionu PINů

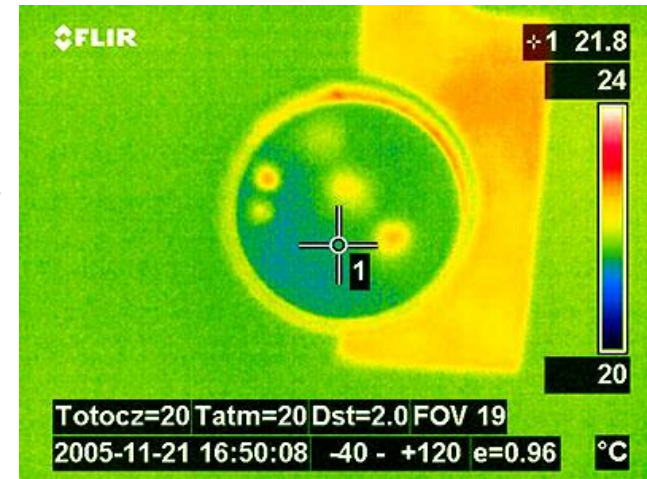
[http://www.datagenetics.com/  
blog/september32012/](http://www.datagenetics.com/blog/september32012/)

Popularita	PIN	Frekvence
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%



# PIN

- Při použití kamery citlivé na tepelné záření lze PIN odečíst z klávesnice po zadání na základě teploty kláves.
  - Lze zjistit i pořadí stisknutí 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

- Útočnickova 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 platební karty lze použít k platbám po internetu, jiné ne – nastavení parametrů (více stran)
- Obvykle lze použít embosované nebo tzv. virtuální platební karty.
- Mnoho bank své karty při vydání blokuje – 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).

# Platební 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.

# Platební karty a internet

- USA
  - Za zneužití karty nese zodpovědnost banka
  - Musí prokázat vinu klienta, pokud za zneužití karty může
- Většina EU
  - Zákazník může platbu reklamovat a banka je povinna „refundovat“ v případě delšího šetření před jeho dokončením
  - 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... ☹



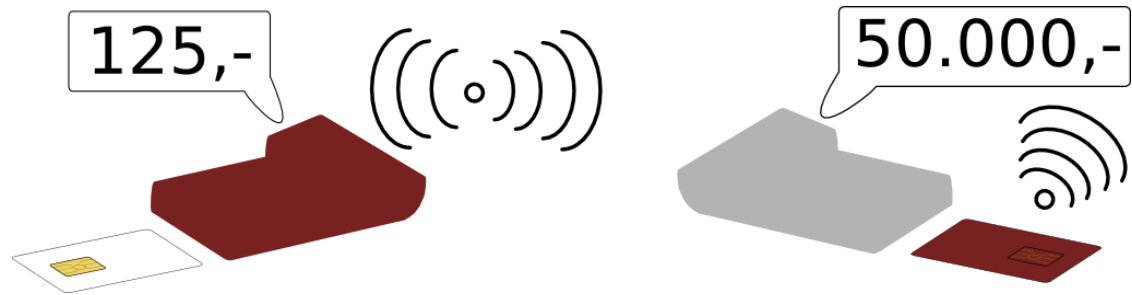
# Platební karty a internet

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

# Problémy s útoky na platby PINem

Problém nedůvěryhodného terminálu – selhání autentizace

- buď neautorizovaným přenosem



- nebo neautorizovaným zařízením mezi kartou a čtečkou:
  - device → PINpad : card authentication check OK
  - card → device → PINpad : cryptogram indicating PIN check failure
  - PINpad → bank : card auth. check OK, cryptogram with PIN check failure
  - bank → PINpad : sale is OK (signature authorization assumed)

# Internetové bankovníctví

# Nutné vybavení

- U většiny aplikací stačí běžný počítač, téměř libovolné připojení na internet a relativně moderní internetový prohlížeč.
- Pokud má k počítači přístup ještě někdo jiný, může u některých produktů internetového bankovníctví 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 (stejného pro různé operace)
  - Pro aktivní operace 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
  - Uložení (a používání) na čipové kartě je nesrovnatelně bezpečnější než ostatní zde uvedená řešení
    - Karta může provádět výpočet, nejen ukládat data

# Způsoby autentizace

- Pomocí dynamického hesla
  - Generovaného autentizačním zařízením (kalkulátorem), někdy i ve spojení s kartou (platební/bankomatovou)
  - Generovaného serverem a posílaného jiným kanálem, obvykle na mobilní telefon
    - Pozor, jiný kanál by měl být jiným kanálem až ke člověku 😊

# Možný 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.

# Pozor na autentizaci

- Man-in-the-middle = evergreen
  - Není problémem SSL, ale nepozornosti lidí a chybám uživatelského rozhraní
  - ...nebo problematické kontrole certifikátů veřejných klíčů prohlížeči nebo servery
  - ...nebo použitím oblíbené ikony u URL    
  - ...nebo zneužitím přesměrování (HTTP na HTTPS)
- Certifikáty veřejných klíčů už dnes jsou spíše atributovými certifikáty a nástroji řízení přístupu
- Problémy za úroveň technologií – přiměřená opatření, jak z právního, tak lidského pohledu

# 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

# Biometriky a ochrana soukromí

PV080

Vašek Matyáš & Zdeněk Říha

# Biometrické metody autentizace

- Metody autentizace
  - něco, co máme
    - klíč, čipová karta
  - něco, co známe
    - PIN, heslo
  - něco, co jsme
    - biometriky
- Režimy použití biometrik
  - verifikace
    - identita je známa
  - identifikace
    - identita není známa
    - identifikace je náročnější proces
    - dělení databáze (clustering)

# Biometrické metody

- Biometriky – *biologické* charakteristiky, které jsou měřitelné *automatizovanými* metodami
- Fyziologické charakteristiky (ruka, oko, tvář atd.)
- Behaviorální charakteristiky (dynamika podpisu, hlas atd.)



# Význam rozeznávání entit

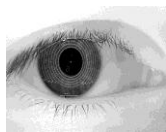
- Automatizované systémy rozeznávání (Identify Friend or Foe) jsou důležitější než v historii
- Systémy (zbraně) běžně zasahují na vzdálenost, která přesahuje možnosti vizuální identifikace.
- Vzrůst úmrtí z „přátelské palby“ z historických 10-15 % na 25 % v 1. válce v Zálivu (R Anderson, Security Engineering)

# Základní biometrické techniky

- Otisk prstu



- Vzor oční duhovky



- Vzor oční sítnice



- Srovnání obličeje



- Geometrie ruky



- Verifikace hlasu



- Dynamika podpisu



# Biometrické techniky

- Fyziologické charakteristiky
  - Ruka
    - Otisk prstu
    - Otisk dlane
    - Geometrie (tvaru) ruky
    - Žíly ruky (geometrie)
  - Oko
    - Duhovka
    - Sítnice
  - Tvář
  - Hlas
  - DNA
  - Lůžka nehtů
  - Vůně/pot
  - Tvar ucha...
- Charakteristiky chování
  - Dynamika podpisu
  - Hlas (dle podnětu)
  - Pohyby tváře
  - Dynamika chůze
  - Dynamika psaní na klávesnici

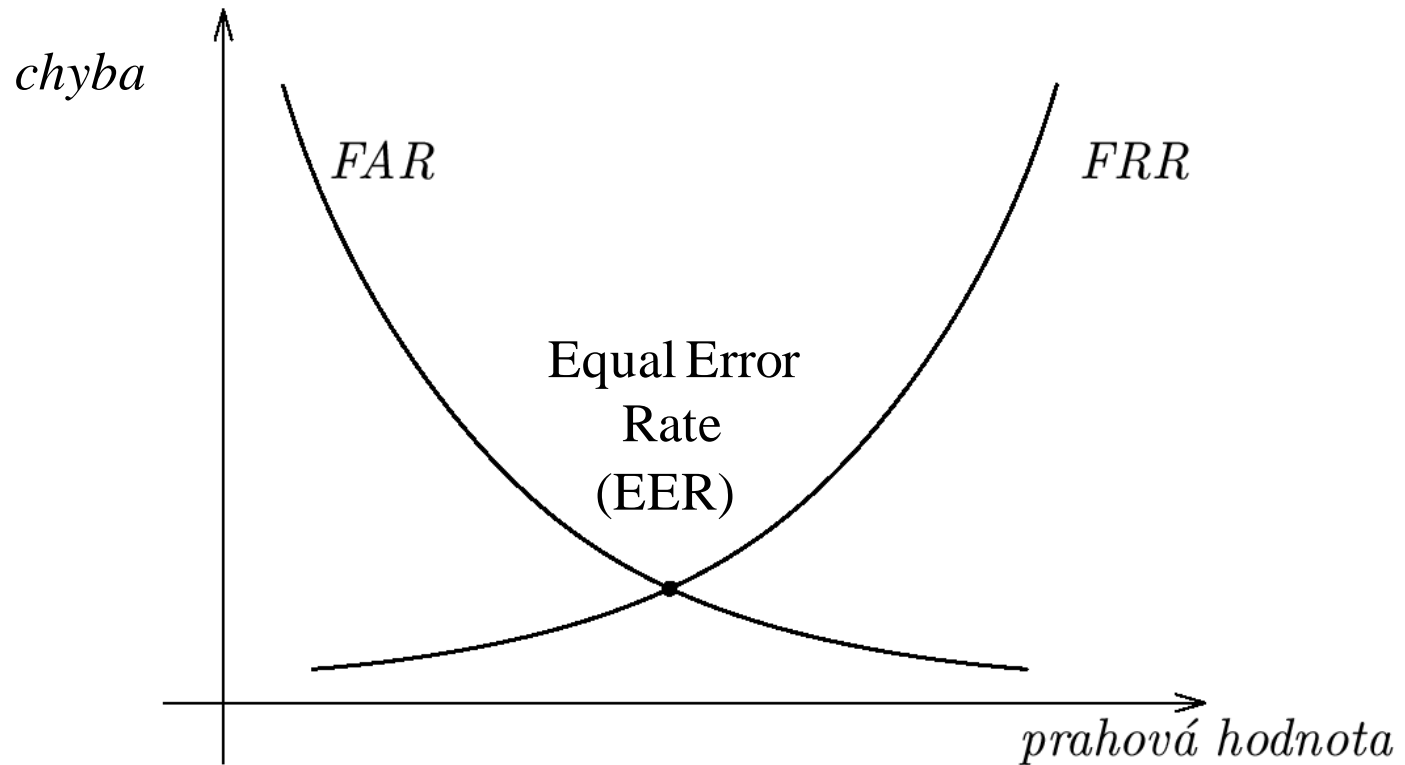
*Více v PV157*

# Specifika biometrických systémů

- Proces použití biometrik
  - registrace
    - prvotní snímání biometrických dat
  - verifikace/identifikace
    - následné snímání biometrických dat a jejich srovnání s registračním vzorkem
- Variabilita
  - biometrická data nejsou nikdy 100% shodná
  - musíme povolit určitou variabilitu mezi registračním vzorkem a později získanými biometrickými daty
    - Prahová hodnota

# Chyby biometrických systémů

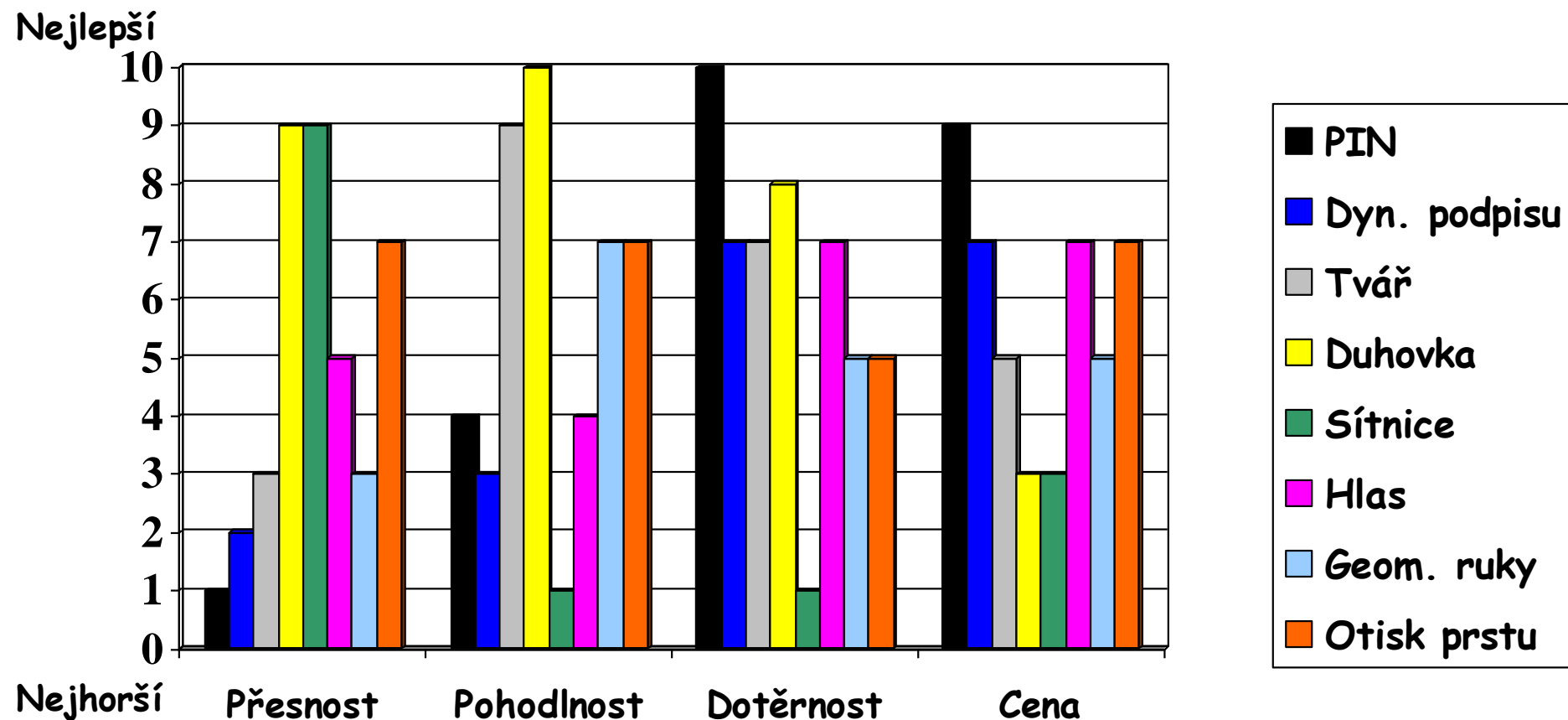
- Nesprávné přijetí  
(false acceptance)
- Nesprávné odmítnutí  
(false rejection)



- Další důležité chyby (FTE – Fail to Enroll, FTA – ...Acquire), ...

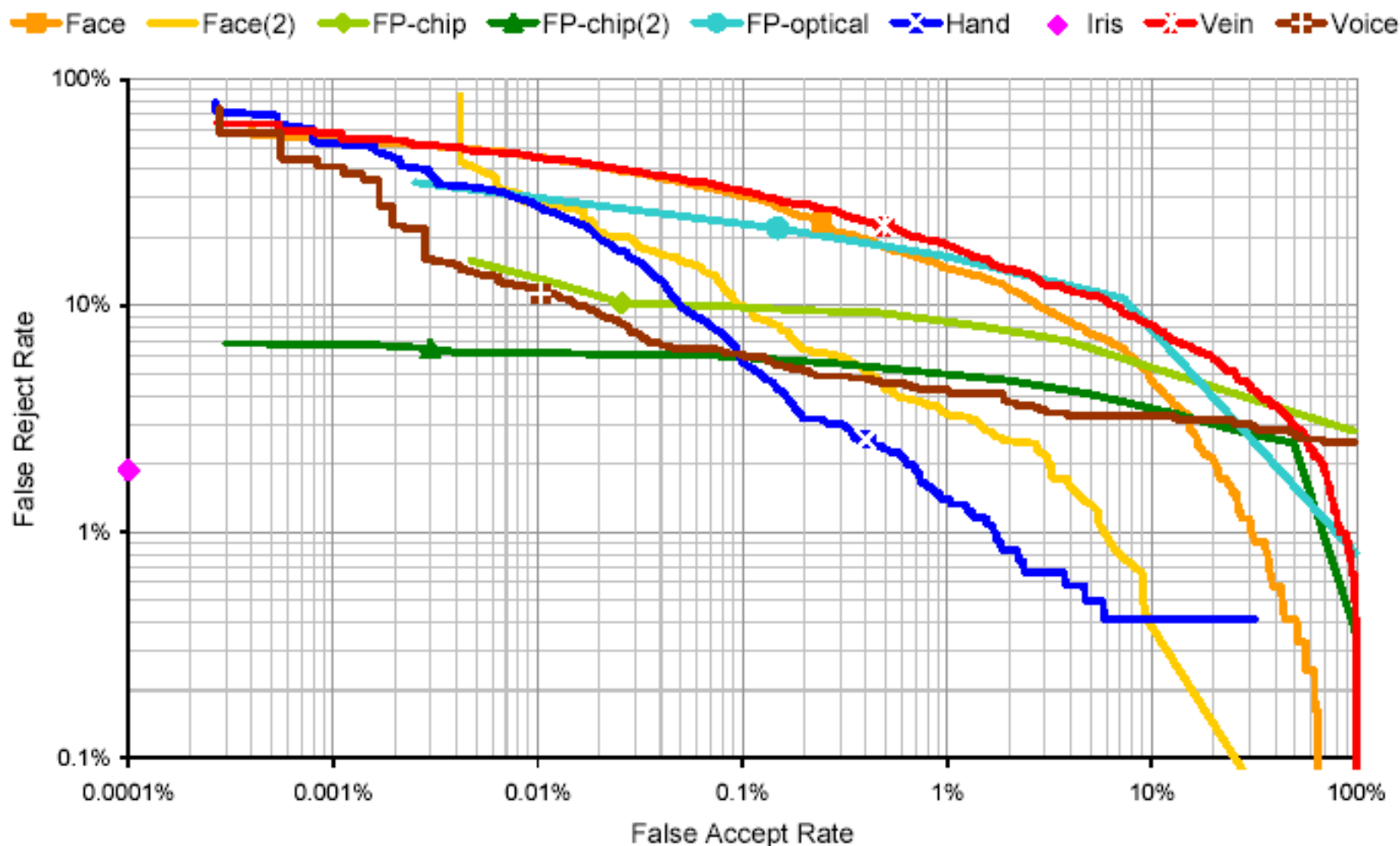
# Srovnávací přehled

(Údaje od Int'l Biometric Group & vlastní pozorování)



# Chyby biometrických systémů

- Receiver operating curve (ROC) – NPL 2001



# Chybovost systémů – realita v extrémním pohledu

- UK Passport Service (2005): Biometrics, enrolment trial, Management Summary.

	Face				Iris				Fingerprint			
	FTE	FTA	FNMR	FRR	FTE	FTA	FNMR	FRR	FTE	FTA	FNMR	FRR
Quota	0,15%	0,00%	51,57%	<b>51,64%</b>	12,30%	0,44%	1,75%	<b>14,22%</b>	0,69%	6,98%	11,70%	<b>19,24%</b>
Disabled	2,27%	0,00%	51,57%	<b>52,67%</b>	39,00%	0,68%	8,22%	<b>44,43%</b>	3,91%	3,14%	16,35%	<b>22,64%</b>



# Kroky biometrického srovnání

- 1) První měření (získání vzorku)
  - 2) Vytvoření registračního vzorku
  - 3) Uložení reg. vzorku v databázi
- 
- 4) Další měření
  - 5) *Vytvoření nového vzorku*
  - 6) Srovnání: nový – registrační
  - 7) Rozhodnutí dle prahové hodnoty

# Jedinečnost

- Záleží na velikosti skupiny, v rámci které srovnáváme!
- Tvář, hlas vs. duhovka, otisk prstu
  - Zvážení nejlepší (automatizované) dostupné srovnávací metody
    - Jsou známy problémy u některých používaných metod srovnávání DNA
  - Velikost uživatelské skupiny vs. přesnost
    - Verifikace vs. identifikace

# Problém I – Vstupní zařízení

- Důvěryhodné vstupní zařízení
  - Je vzorek od živé osoby? (problém *živosti*)
  - Je vzorek skutečně od osoby u vst. zařízení?
  - Důvěryhodnost je relativní (dle prostředí)
- Oklamání zařízení
  - Nebo komunikačního kanálu mezi zařízením a místem zpracování (počítačem)

# Problém II – Nastavení úrovně

- Je kritické a velmi závislé na druhu nasazení
- Vysoké nesprávné přijetí – aplikace s nízkou úrovní bezpečnosti
  - Neoprávnění uživatelé jsou menší zlo
- Vysoké nesprávné odmítnutí – opakované pokusy v prostředí s vysokými požadavky na bezpečnost
  - Nespokojení uživatelé jsou menší zlo

# Problém III – Logistika!?

- Administrace
  - Nároky na strojový čas
  - Problém v případě selhání/prozrazení
  - Ochrana soukromí
- Uživatelé s poškozenými/chybějícími orgány
  - Pro některé biometriky až 1-3 % uživatelů nemá (nebo má nezvratně poškozen) daný orgán

# Problém IV – vzorek

- Stálost vzorku (hlas, podpis, tvář)
- Vzorek nelze (příliš) měnit!!!
  - Jeden vzorek může být používán ve více systémech!
    - A jedině ověření hlasu lze částečně udělat jako nepřehrávatelné.
  - Zjištění vzorku by nemělo být pro bezpečnost kritické.

# Biometriky a soukromí I.

- Biometriky hodně o uživateli vypovídají 😊
  - srovnejte s jinými metodami autentizace – co ty vypovídají o uživatelích?
- Ochrana soukromí
  - Sběr některých informací
    - Otisk prstu má “stigma” vztahu k policii
    - Srovnejte např. DNA či sítnici s duhovkou či tváří

# Biometriky a soukromí II.

- DNA
  - Nepříjemné získávání vzorku
  - Dispozice k určitým chorobám ap.
- Vůně/pot
  - Lze rozpoznat některé nemoci nebo dlouhodobé zdravotní problémy
  - Vypovídá i o aktivitách v posledních desítkách hodin
- U některých typů otisků prstů je údajně statisticky větší pravděpodobnost homosexuální orientace, podobně je tomu i u některých jiných biometrik



# Biometriky a soukromí III.

- Kritická trivialita!!!
  - U dosavadních systémů lze více či méně jednoduše vystupovat pod více identitami
  - Biometriky (v ideálním případě ☺) určují identitu člověka přesně a lze tak spojovat jednotlivé jeho činy

# Další problémy – legislativa

- Již dnes velké rozdíly mezi přístupem k ochraně osobních dat mezi různými zeměmi (USA vs. EU), jaká bude situace s biometrikami?!
- Nejasná očekávání zpomalují nasazení v praxi.
  - Vnitrofiremní řešení obvykle bez problému.
  - Zákaznická řešení hledají možnost držení vlastní biometriky pouze uživateli.
- První náznaky – aktivity v rámci EU/EK

# Závěr I.

- Biometrická data nejsou tajná
  - otisky prstů zanecháme na všem, čeho se dotkneme
- Tzv. „problém živosti“
  - musíme si být jisti, že biometrická data jsou autentická
- Autentizační subsystém
  - důvěra v biometrický snímač, zabezpečená komunikace

## Závěr II.

- Biometriky jsou vnímány jako citlivé informace
- Kopírování není sice triviální, ale ani nemožné
- Bezpečnostní „klasika“: Nová ochranná opatření jsou vždy následována novými metodami útoků

# Biometriky: pohodlnost vs. bezpečnost

Vypovídající citace z licence: *„The biometric (fingerprint reader) feature in this device is not a security feature and is intended to be used for convenience only. It should not be used to access corporate networks or protect sensitive data, such as financial information. Instead, you should protect your sensitive data with another method, such as a strong password that you either memorize or store in a physically secure place.“*