PV157 – Autentizace a řízení přístupu

Biometrická autentizace uživatelů

Biometrické metody autentizace

- Metody autentizace
  - něco, co máme (klíč, čipová karta)
  - něco, co známe (PIN, heslo)
  - něco, co jsme (biometriky)

- Biometriky – „*automatizované* metody identifikace nebo ověření identity na základě *měřitelných* fyziologických nebo behaviorálních (založených na chování) vlastností člověka“

Režimy použití biometrik

- Verifikace
  - 1:1
  - identita je známa (ověření této identity)
- Identifikace
  - 1:n
  - identita není známa (nutné projít celou databázi registrovaných osob)
  - identifikace je náročnější proces
  - dělení databáze (clustering)

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

Model biometrické autentizace (1)

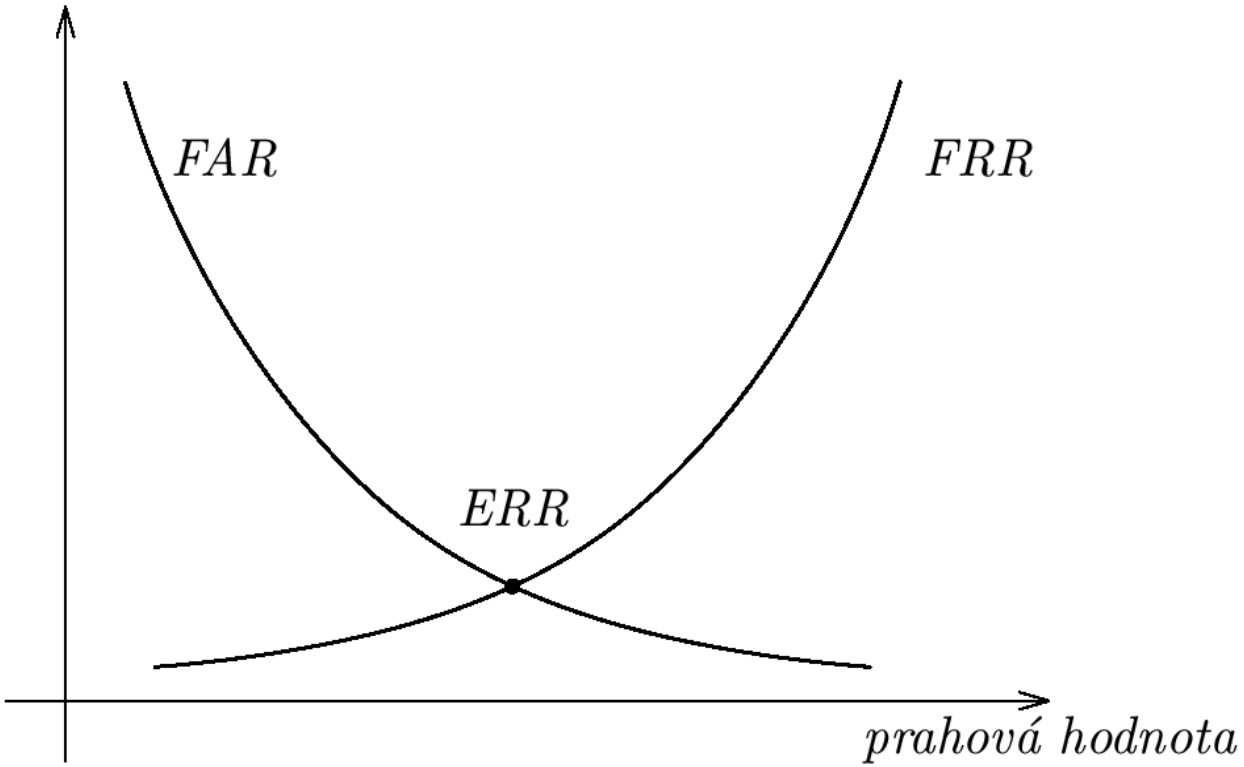
- Fáze registrace
  - prvotní získání biometrických dat
    - kvalita těchto dat je velmi důležitá
  - vytvoření registračního vzorku
    - získání důležitých charakteristik
  - uložení registračního vzorku
    - karta, snímač, pracovní stanice, server

Model biometrické autentizace (2)

- Fáze identifikace / autentizace
  - získání biometrických dat
    - plně automatické, bez obsluhy
  - vytvoření charakteristik
    - pouze jeden vzorek k dispozici
  - srovnání charakteristik
    - míra shody registračního vzorku s aktuálními daty
  - finální rozhodnutí ano/ne

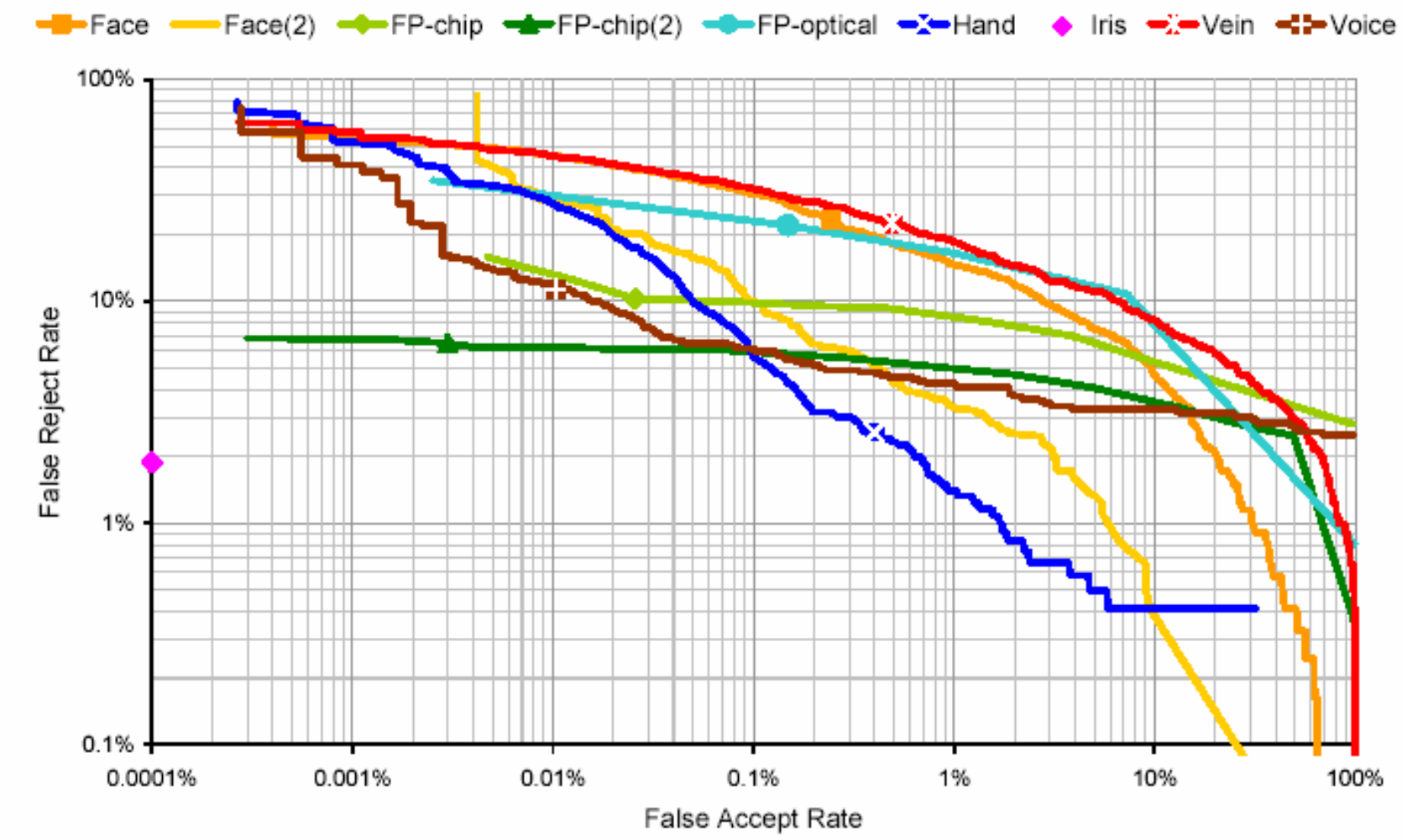
Chyby biometrických systémů

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



Chyby biometrických systémů

- Receiver operating curve (ROC)



Biometrické technologie

- Založené na
  - *Fyziologických* charakteristikách (otisk prstu, geometrie ruky) – též nazývané *statické*
  - *Behaviorálních* charakteristikách (podpis, hlas) – je vyžadována akce uživatele – též nazývané *dynamické*
- Charakteristiky
  - Genotypické – geneticky založené (např. DNA)
  - Fenotypické – ovlivněné prostředím, vývojem (např. otisk prstu)

Biometrické technologie

- Otisk prstu

- Vzor oční duhovky

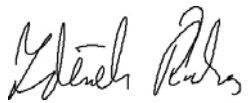
- Vzor oční sítnice

- Srovnání obličeje

- Geometrie ruky

- Verifikace hlasu

- Dynamika podpisu



- Dynamika psaní na klávesnici

heslo

Otisky prstů

- Jedna z nejstarších metod
- Získání otisku prstu
  - za použití inkoustu
  - bez použití inkoustu

Snímače otisků prstů

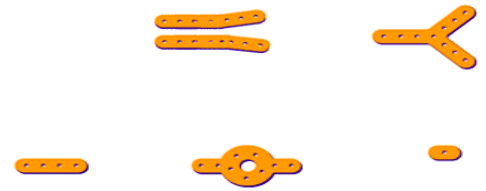
- optické

- silikonové (kapacitní)

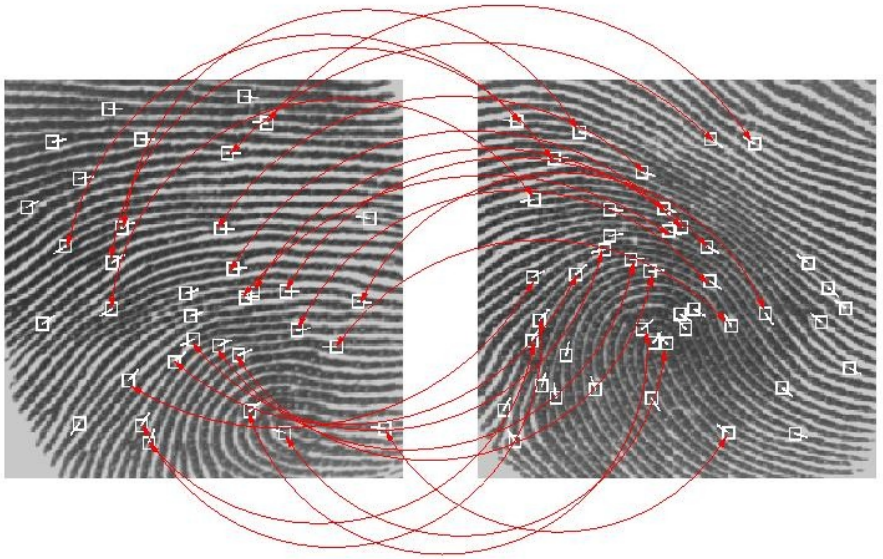
- ultrazvukové

Otisky prstů

- Zpracování otisků prstů
  - „podrobnosti otisků“
- Srovnání otisků prstů
- Rychlost
  - jedno srovnání 5ms až 2s
- Přesnost
  - FAR pod 0,1 %
    při FRR asi 5%



Zdroj: Digital Persona, Inc.



Geometrie ruky

- Snímá se tvar ruky
- Ten ovšem není jedinečný (např. ve srovnání s otisky prstů)
- Snímače snímají 3D (velikost šablony pouze 9 bajtů)

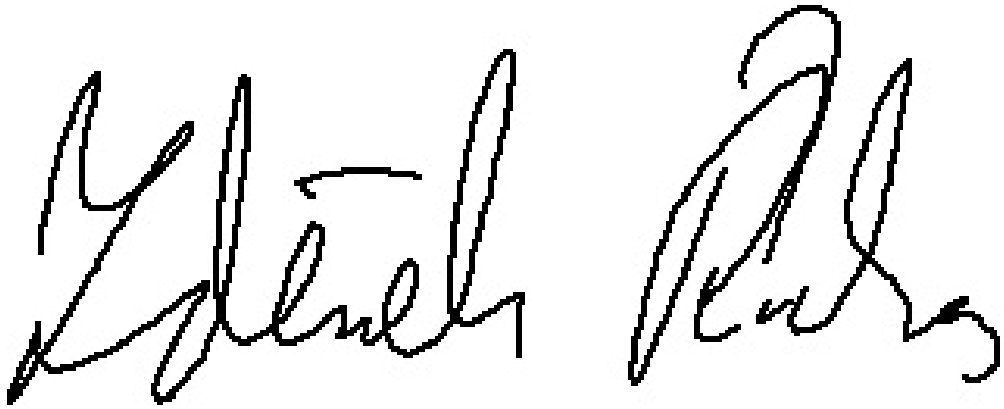
Geometrie ruky

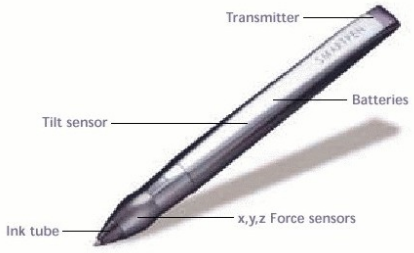
- Rychlost
  - verifikace asi během 1 s
- Přesnost
  - málo přesné, tvar ruky není jedinečný
  - nevhodné pro identifikaci
  - pouze omezeně vhodné pro verifikaci
  - FAR i FRR přes 10 %
- Použito při kontrole vstupu do olympijské vesnice na Olympijských hrách v Atlantě v roce 1996

Dynamika podpisu

- Důležitý je nejen výsledný podpis, ale i způsob (dynamika) jeho psaní

- Vstupní zařízení
  - tablet
  - speciální snímač





Dynamika podpisu

- Velikost šablony
  - kolem 20 kB (vytvořeno ze 3 až 10 podpisů)
- Rychlost
  - verifikace asi během 1 s
- Přesnost
  - velmi malá, nedostatečná pro většinu aplikací
  - FAR i FRR několik desítek procent
  - často důraz pouze na dynamickou komponentu psaní bez ohledu na výsledný podpis

Verifikace hlasu

- Založeno
  - na charakteristikách hlasu daných hlasovým ústrojím člověka
- Snímání
  - běžný mikrofon
  - telefon

Verifikace hlasu

- Rychlost
  - docela rychlé
- Přesnost
  - za ideálních podmínek FAR i FRR pod 2 %
  - reálné výsledky velmi ovlivněny šumem linky a šumem z okolí

Dynamika psaní na klávesnici

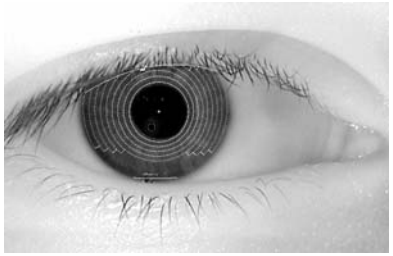
- Založeno na způsobu psaní na klávesnici
  - měří se čas stlačení klávesy a čas mezi stisky kláves
  - nevyžaduje speciální HW
  - algoritmy pracují na principu srovnávání vzorů (pattern matching) nebo neuronových sítí (neural networks – problém přidání dalšího uživatele)
  - možnost kontinuální autentizace uživatele

Oční duhovka

- Srovnává se jedinečný vzor oční duhovky

- Snímání oční duhovky
  - černobílá kamera ve vzdálenosti x.10 cm

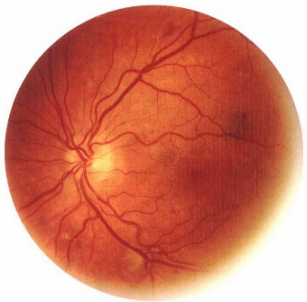
- Iriscode
  - 256 bajtů popisujících vzor duhovky



- Rychlost
  - miliony srovnání za sekundu
- Přesnost
  - velmi přesné, vhodné i pro identifikaci
  - FAR (téměř) nulové při FRR kolem 3 %

Oční sítnice

- Srovnává se vzor cév na oční sítnici

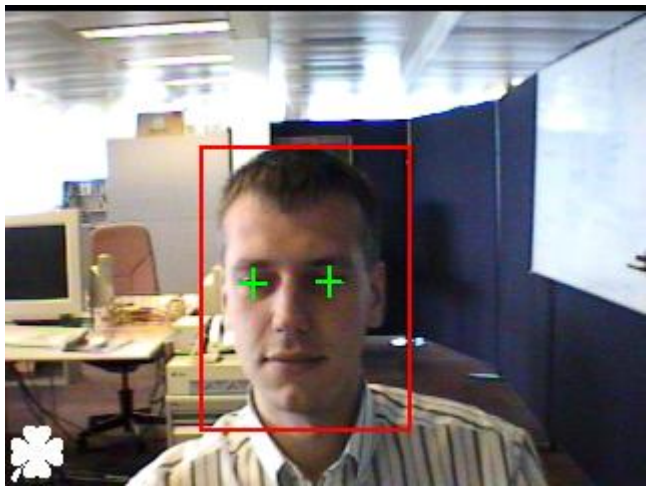


- Pro snímání se používá infračervený laserový paprsek

- Velikost výsledného záznamu
  - 96 bajtů
- Přesnost
  - velmi přesné
  - velmi nízké FAR, avšak relativně vysoké FRR
- Příjemnost
  - snímání není uživatelsky příjemné

Rozpoznání obličeje

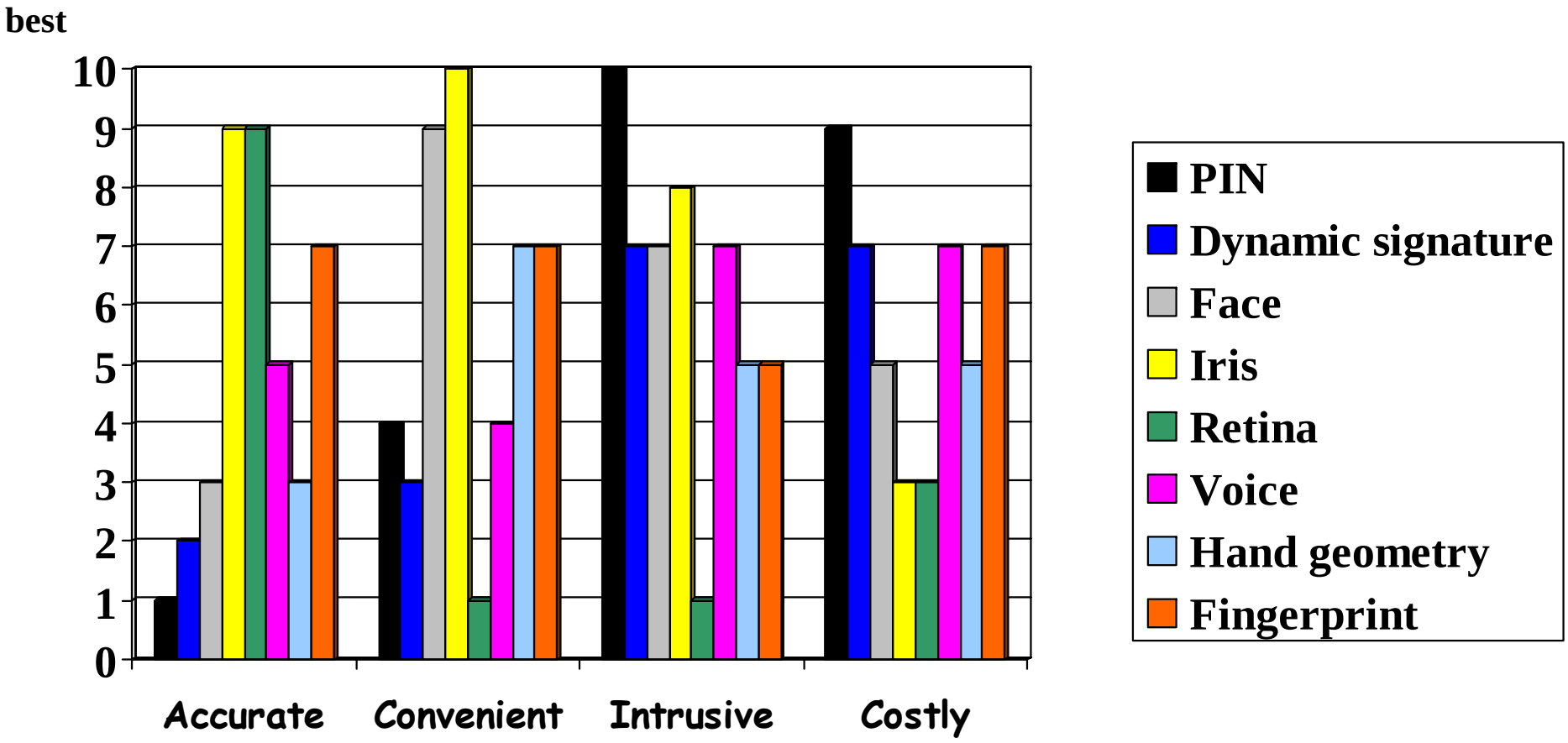
- Rozpoznání obličeje
  - Detekce obličeje
  - Srovnání obličeje
- Rychlost
  - Velice výpočetně náročné
  - Verifikace až několik sec
- Přesnost
  - FRR i FAR několik desítek procent
  - Obličej člověka se mění v čase
  - Účes, Brýle, Náušnice



Biometriky – neúplný přehled

- Fyziologické charakteristiky
  - Ruka
    - Otisk prstu
    - Otisk dlaně
    - 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

Srovnání – autentizace a biometriky



Nejslibnější technologie

- Otisk prstu
  + hodně produktů a aktivit v oblasti výzkumu a vývoje
  + cena a velikost obecně přijatelné již dnes
  - možnost podvodů

- Duhovka
  + vynikající přesnost – identifikace i v obrovských skupinách lidí
  - možnost podvodů; nová technologie (patentový monopol)

- Ověření mluvčího
  + kontinuální verifikace a možnost ověření výzva-odpověď
  - změna charakteristik a vývoj řeči

Komerční versus forenzní

- Nízká přesnost
- Plně automatizované, počítačové periferie
- Nedostatečně kvalitní registrační vzorky můžeme získat znovu.
- Ukládáme pouze zpracované charakteristiky

- Vyšší přesnost
- Nutné manuální intervence profesionálů
- Registraci není možné opakovat
- Uchováváme zpracované charakteristiky i původní biometrické vzorky

Komerční versus forenzní II.

- Výsledek autentizace v sekundách
- Nízká až střední znalost systému nutná (pro používání)
- Miniaturizace
- Cena hraje důležitou roli a je relativně nízká

- Získání výsledků může trvat i dny
- Pro používání je nutná odborná znalost systému a principu na němž je založen
- Velikost zařízení je nedůležitá
- Vysoká cena; není to však nejdůležitější faktor.

Výhody biometrik

- Autentizace/identifikace uživatele
- Nemůžeme ztratit, zapomenout nebo předat jiné osobě
- Rychlé a (relativně) přesné výsledky
- Nižší cena údržby než u tokenů (a často i hesel)

Praktické problémy I

- Důvěryhodné vstupní zařízení (živost)
  - Pochází vzorek od živé osoby?
  - A pochází skutečně od osoby, která jej podává?
- Vysoké FAR – aplikace s nízkou úrovní bezp.
- Vysoké FRR – nespokojení uživatelé.
- Uživatelé s poškozenými/chybějícími orgány (FTE – fail to enroll, FTA – fail to acquire)

Praktické problémy II.

- Správa charakteristik
- Omezení při použití charakteristik
  - Jedna charakteristika může být použita ve více systémech!
  - Zveřejnění nesmí ohrozit bezpečnost!
- Záležitosti s ochranou soukromí a uživatelskou přívětivostí pro uživatele.
- Legislativa a omezení.

Hlavní poznatky

- Biometriky mohou být velmi citlivé informace
- Biometriky nejsou tajné
- Kopírování nemusí být triviální, ale není obtížné
- Spolehlivost: nemohou být zapomenuty
- Nová ochranná opatření mají za následek nové druhy útoků – bezpečnostní „klasika“

Jsou tedy biometriky přínosem?

- Uživatelská přívětivost
- Bezpečnost (současných implementací) musí být zlepšena

Digitální podpis a autentizace

Uživatel — Počítač — Data

Digitální podpis v teorii

Tajný klíč + Dokument = Podpis

Veřejný klíč + Podpis + Dokument = Ano / Ne

Digitální podpis v realitě

- Veřejný klíč – kritický pro ověření podpisu, používány certifikáty veřejných klíčů (PKI).
- Privátní klíč – musí být udržován tajný, jinak další osoby mohou vytvářet „cizí“ podpis.
  - Digitální podpis využívá omezeného přístupu k privátnímu klíči
- Ve skutečnosti nepodepisuje člověk, ale počítač!!!

Ochrana soukromého klíče

- Uložen v počítači, čipové kartě …
- Obvykle zašifrován/blokován
  - Pro přístup ke klíči je nutné zadat PIN/heslo a/nebo vložit čipovou kartu
  - Při vytváření podpisu (a jiném použití) – trojský kůň nebo administrator může k soukromému klíči získat přístup!!!

Biometriky a kryptografie

- Biometriky nejsou tajné!!!
- Generování kvalitních kryptografických klíčů z biometrik je víceméně nesmyslné
  - Sice atraktivní návrh – klíč jen v okamžiku potřeby ap.
  - Ale prostor všech možných klíčů je omezený
  - Co bude tajné a když to „přidáme“, tak kam to uložíme?
  - A co v případě prozrazení klíče, nevratné změny vzorku, změny snímací technologie...

Úloha biometrik

- Biometriky mohou výhodně chránit přístup k tajnému klíči (nejlépe ještě s tajnou informací)
- Biometriky autentizují uživatele, nikoliv počítače nebo data, zprávy...
- Podepisovací čip + biometrický senzor + biometrický porovnání = … zářné zítřky? ☺

Závěry

- Mnohé biometrické technologie jsou použitelné v praxi. Nikdy ale nejsou 100% bezchybné.
- Použití biometrických technologií nemusí automaticky znamenat zvýšení bezpečnosti systému.
- Výhodné je použití biometrik jako *doplňkové* metody.

Otázky?

Vítány!!!

Příští přednáška 8. 12. 2003 v 18:00

matyas@fi.muni.cz
zriha@fi.muni.cz