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 úmrti 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

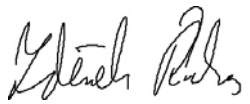
- Vzor oční sítnice

- 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

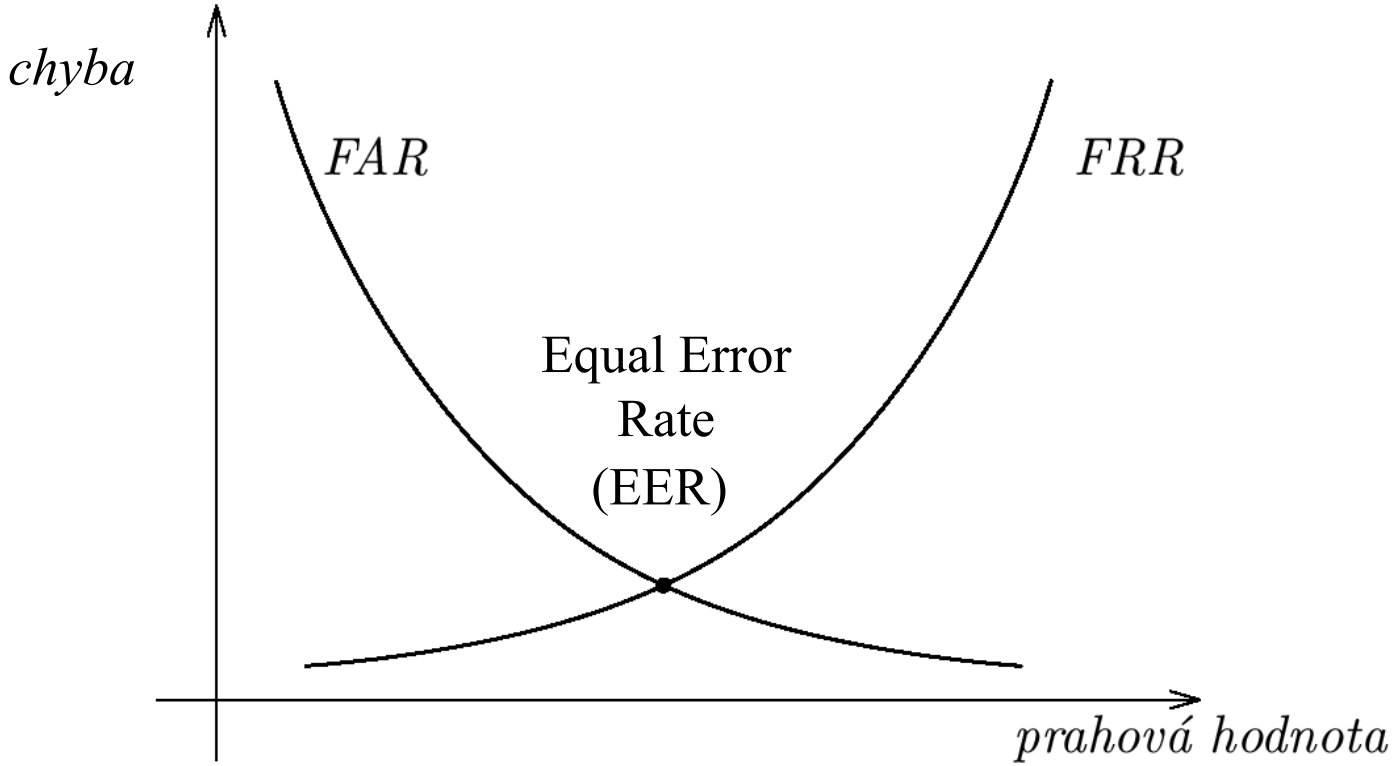
Více v PV157

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

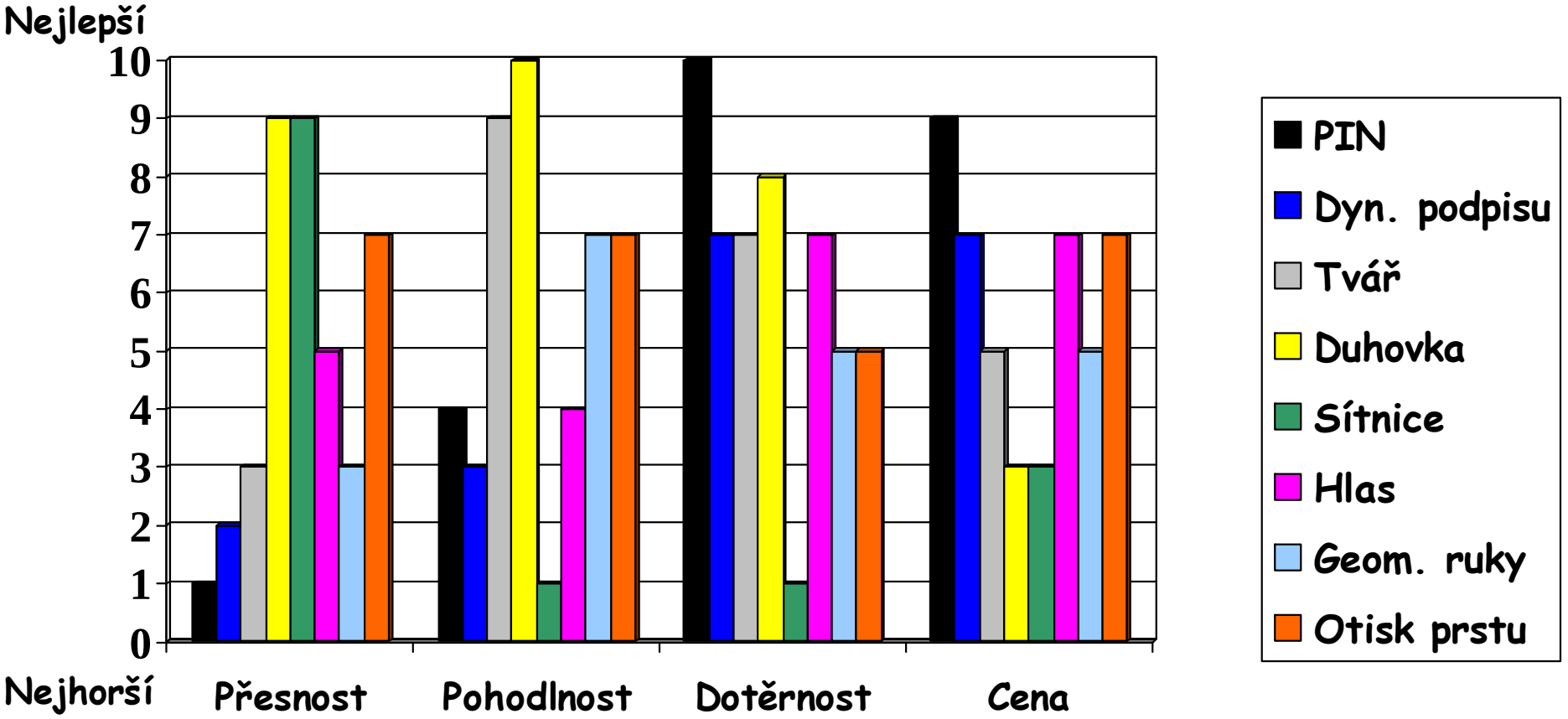
- Nesprávné přijetí (false acceptance)
- Nesprávné odmítnutí (false rejection)



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

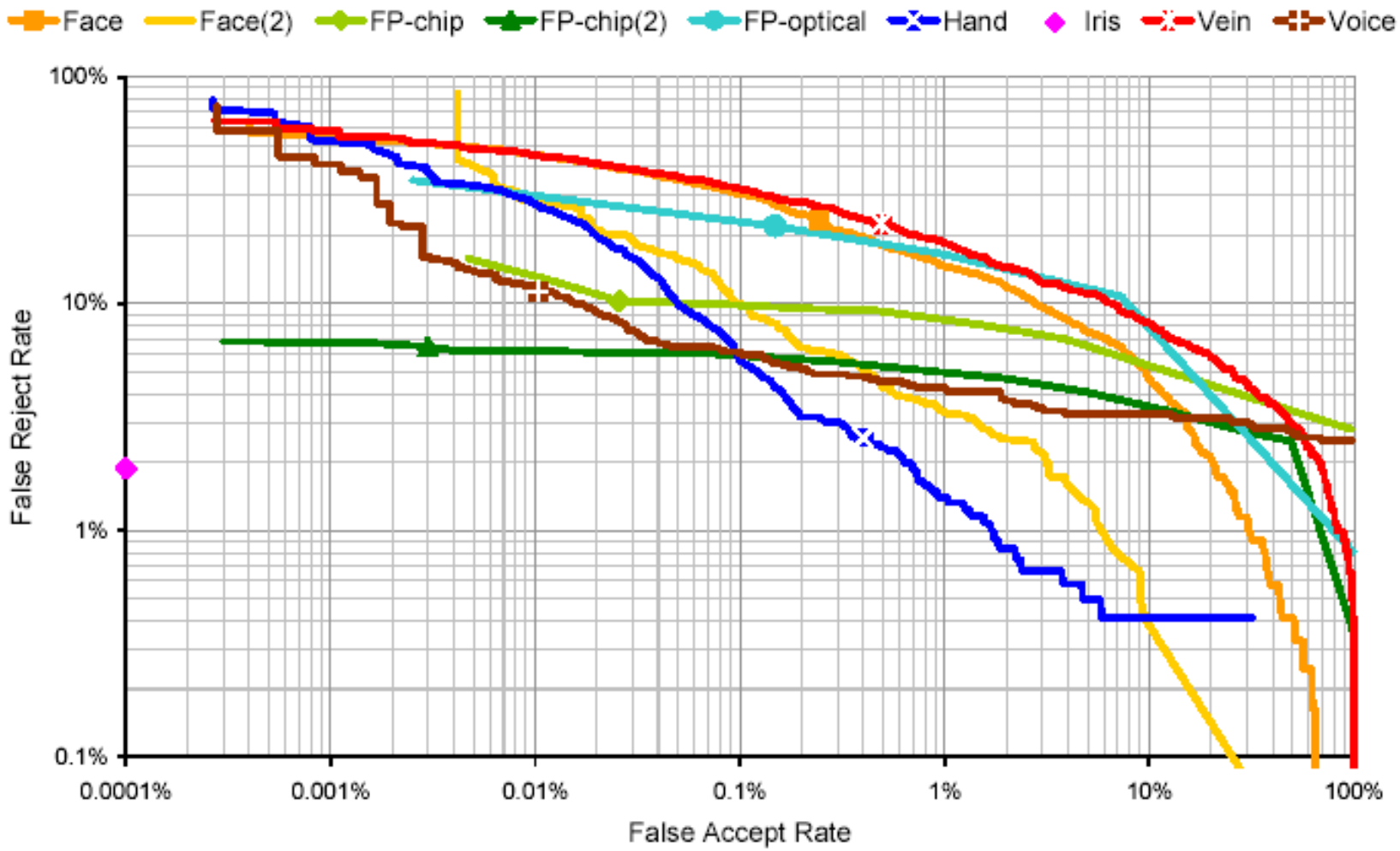
Srovnávací přehled

(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%	**51,64%**	12,30%	0,44%	1,75%	**14,22%**	0,69%	6,98%	11,70%	**19,24%**
Disabled	2,27%	0,00%	51,57%	**52,67%**	39,00%	0,68%	8,22%	**44,43%**	3,91%	3,14%	16,35%	**22,64%**

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.

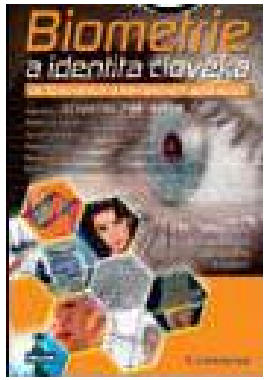
- Kritická trivialita!!!
  - U dosavadních systémů lze více či méně jednoduše vystupovat pod více identitami
  - Biometriky (v ideálním případě ☺) určují identitu člověka přesně a lze tak spojovat jednotlivé jeho činy

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.*“