PV157 – Autentizace a řízení přístupu

Biometrická autentizace uživatelů I.

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)

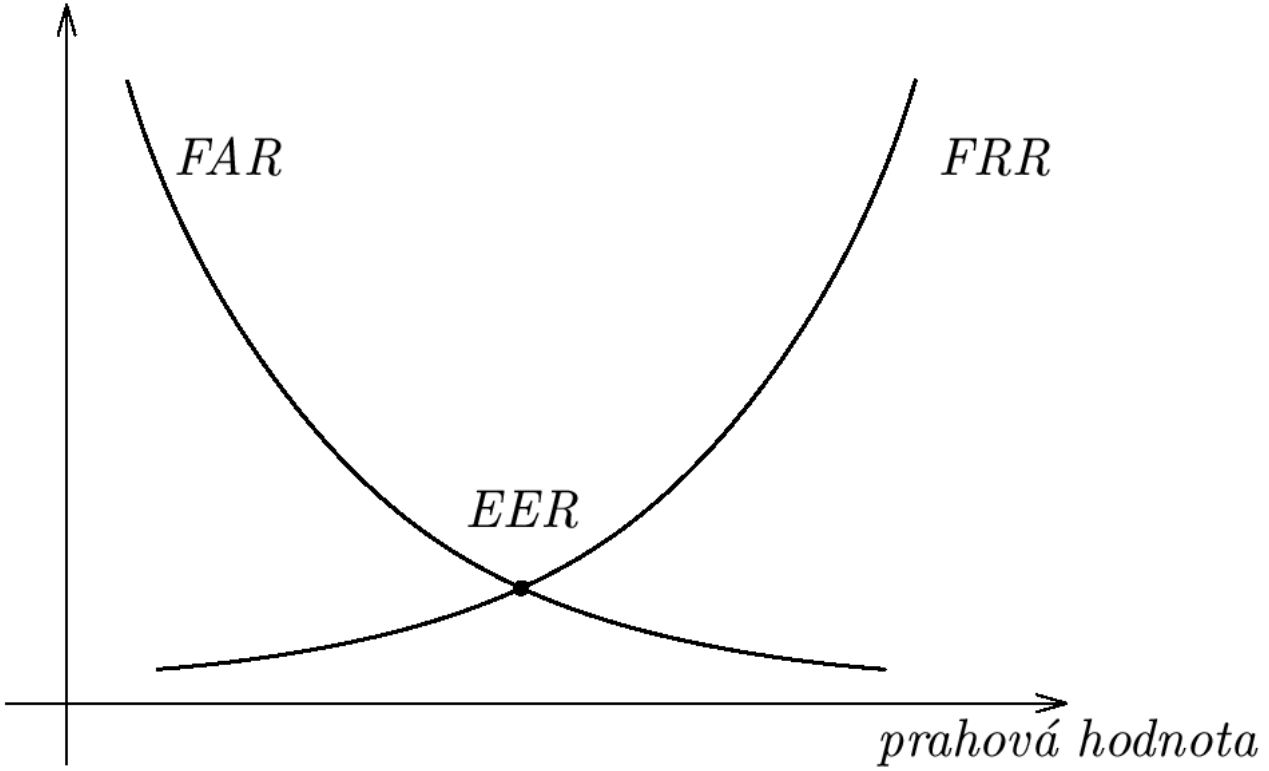
- Fáze registrace
  - prvotní získání biometrických dat
    - kvalita těchto dat je velmi důležitá
  - vytvoření registračního vzorku
    - získání důležitých charakteristik
  - uložení registračního vzorku
    - karta, snímač, pracovní stanice, server

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

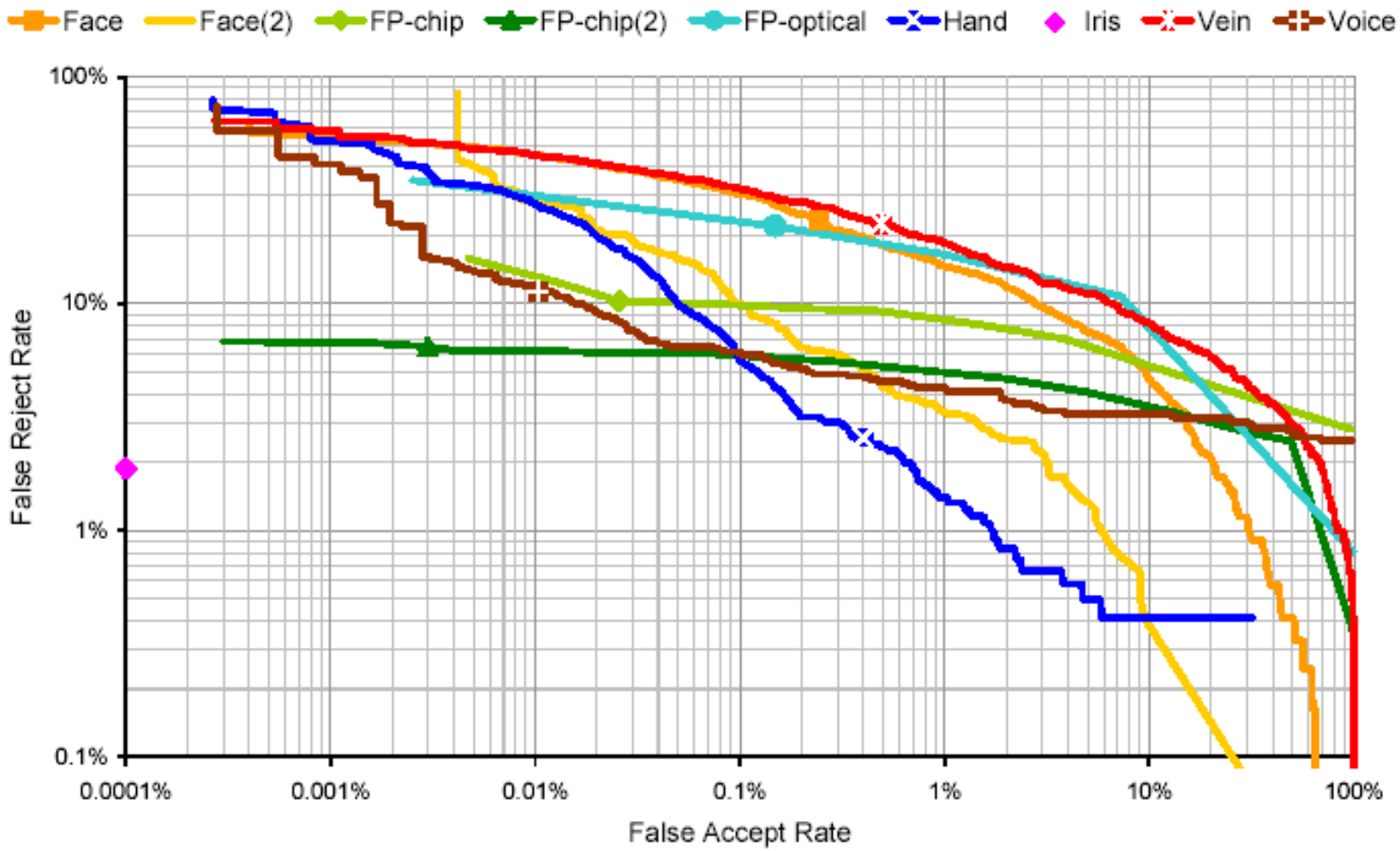
Chyby biometrických systémů

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

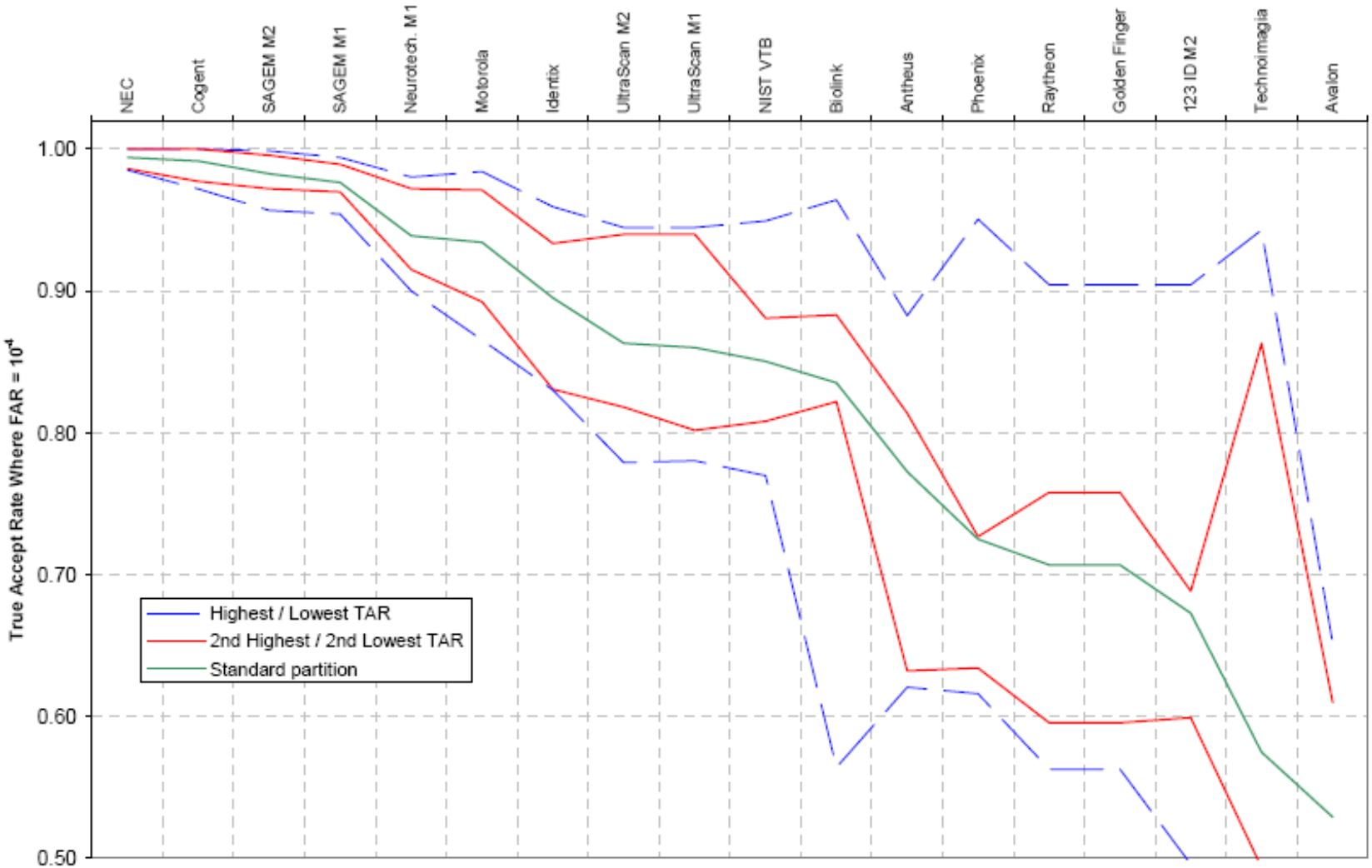


Chyby biometrických systémů

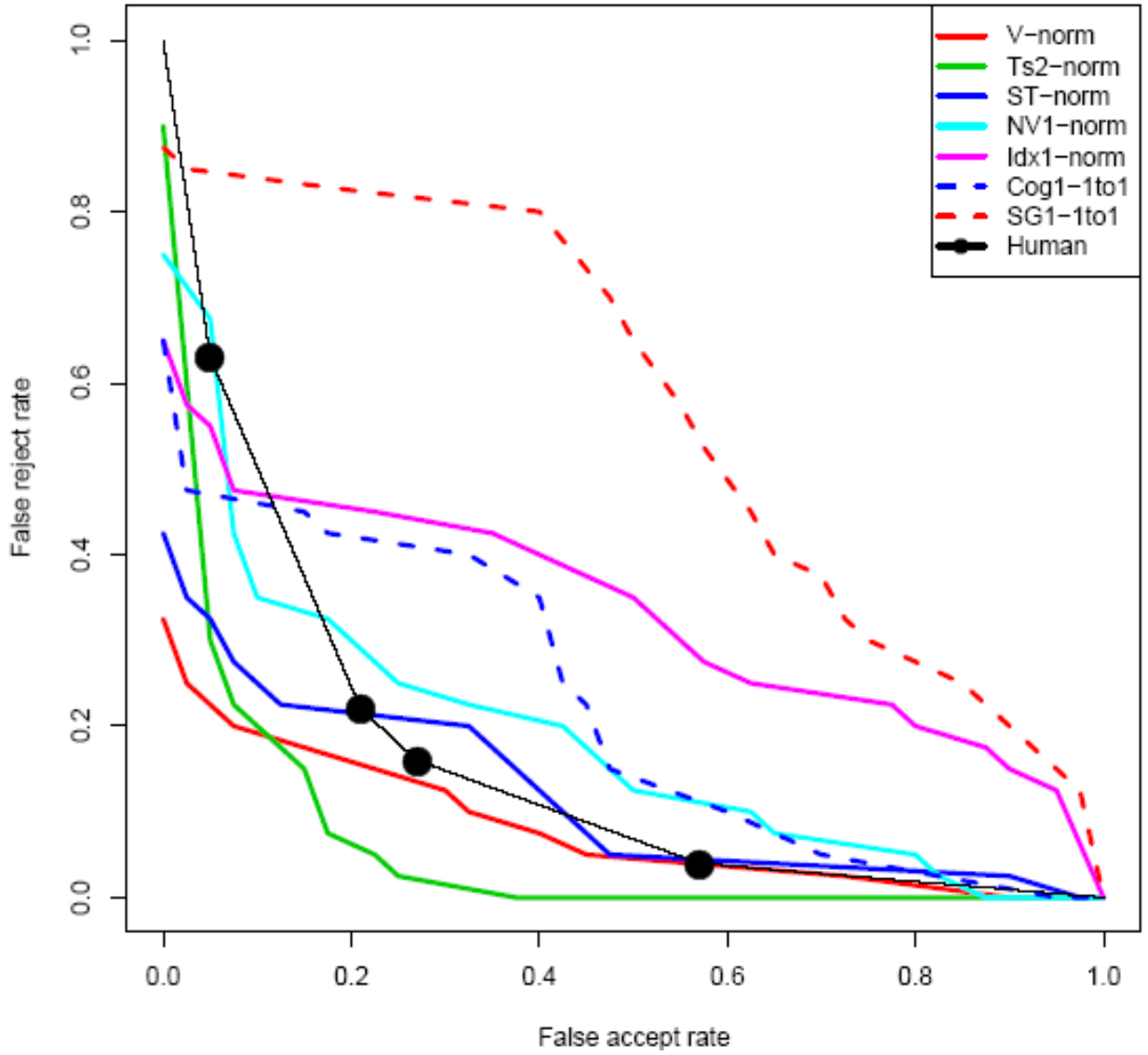
- Receiver operating curve (ROC) – NPL 2001



NIST FpVTE 2003



NIST FRVT 2006



UK Passport Service: Biometrics Enrolment trial 2005

- verifikace (registrace)
  - rozpoznání obličeje
    - pro běžné uživatele: 69% úspěšnost (100%)
    - pro postižené: 48% úspěšnost (98%)
  - oční duhovka
    - pro běžné uživatele: 96 % úspěšnost (90%)
    - pro postižené: 91 % úspěšnost (61%)
  - otisk prstu
    - pro běžné uživatele: 81% úspěšnost (100%)
    - pro postižené: 80 % úspěšnost (96%)

Chybovost

- Chybovost biometrických systémů závisí na řadě faktorů
  - typ snímače, používání různých typů snímačů
  - prostředí ((ne)možnost přizpůsobit prostředí, vnitřní, venkovní prostory, zdroje světla…)
  - nastavení (počet pokusů, omezení kvality vzorků,…)
  - uživatelé
    - trénovaní/nováčci
    - úředníci/dělníci/horníci…
    - jejich motivace
- Samotné FAR, FRR bez znalosti detailů testování nám mnoho nepomůže (a nemusí být srovnatelné)

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

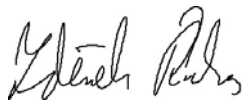
- Vzor oční sítnice

- Srovnání obličeje

- Geometrie ruky

- Verifikace hlasu

- Dynamika podpisu



- Dynamika psaní na klávesnici

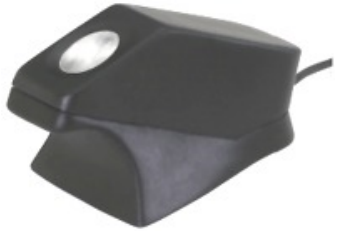
heslo

Otisky prstů

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

Snímače otisků prstů

- optické



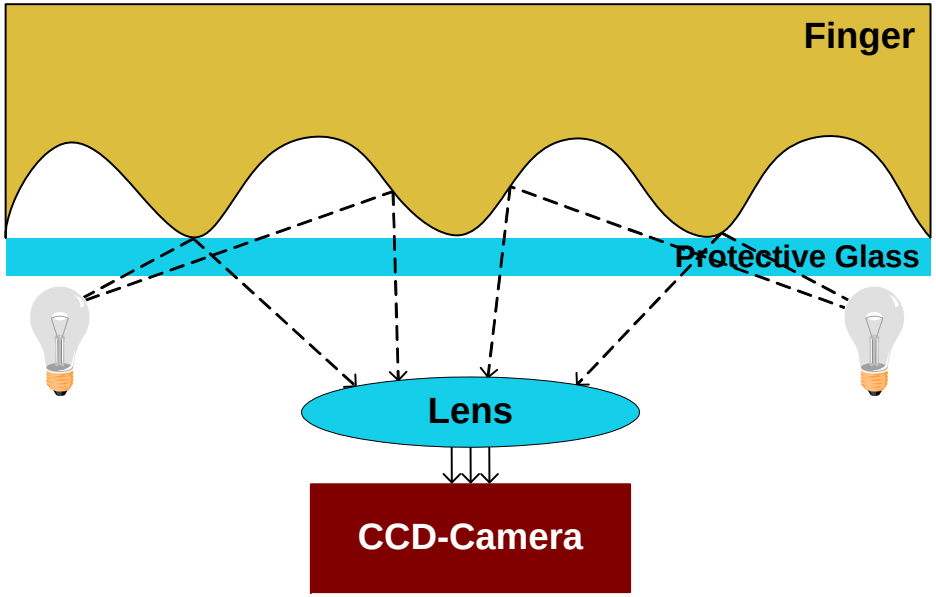
- silikonové (kapacitní)

- i elektrooptické
- ultrazvukové

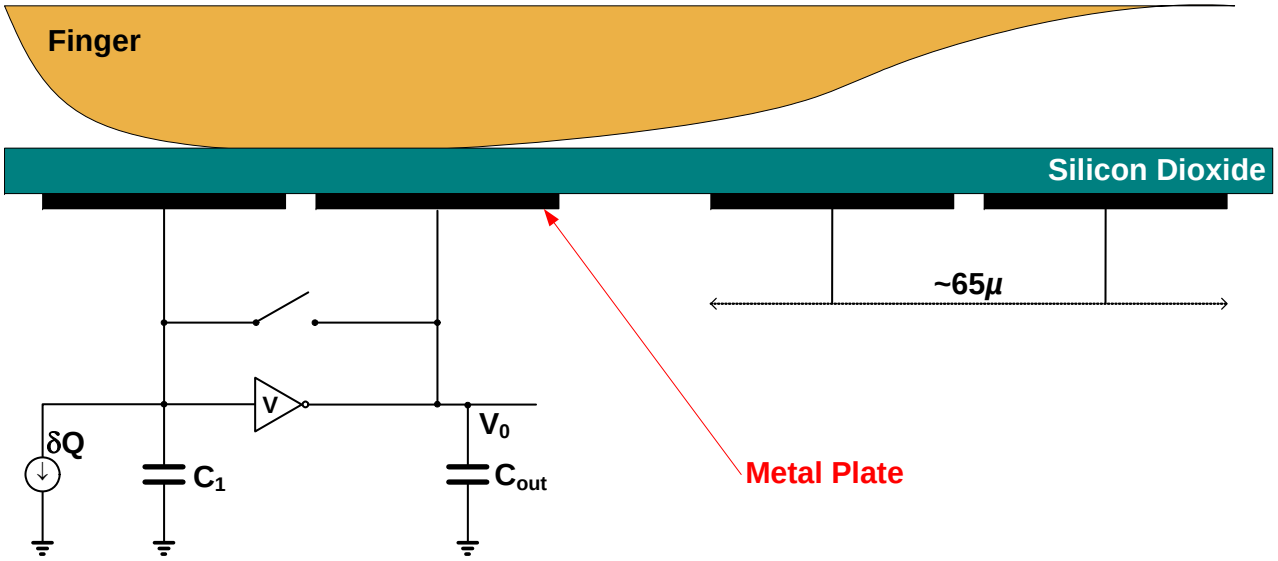
- tepelné
- tlakové

Díky M. Drahanskému za několik následujících slajdů!

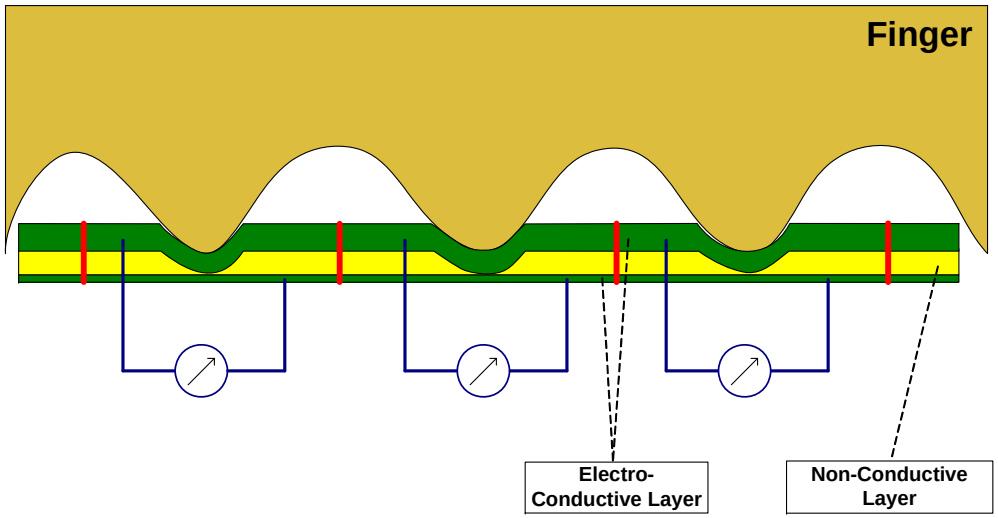
Princip optického snímače



Princip kapacitního snímače

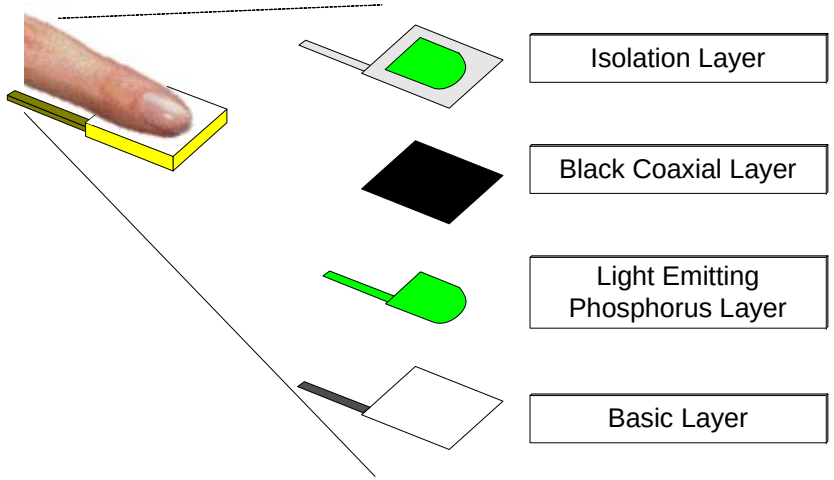


Snímač tlakový



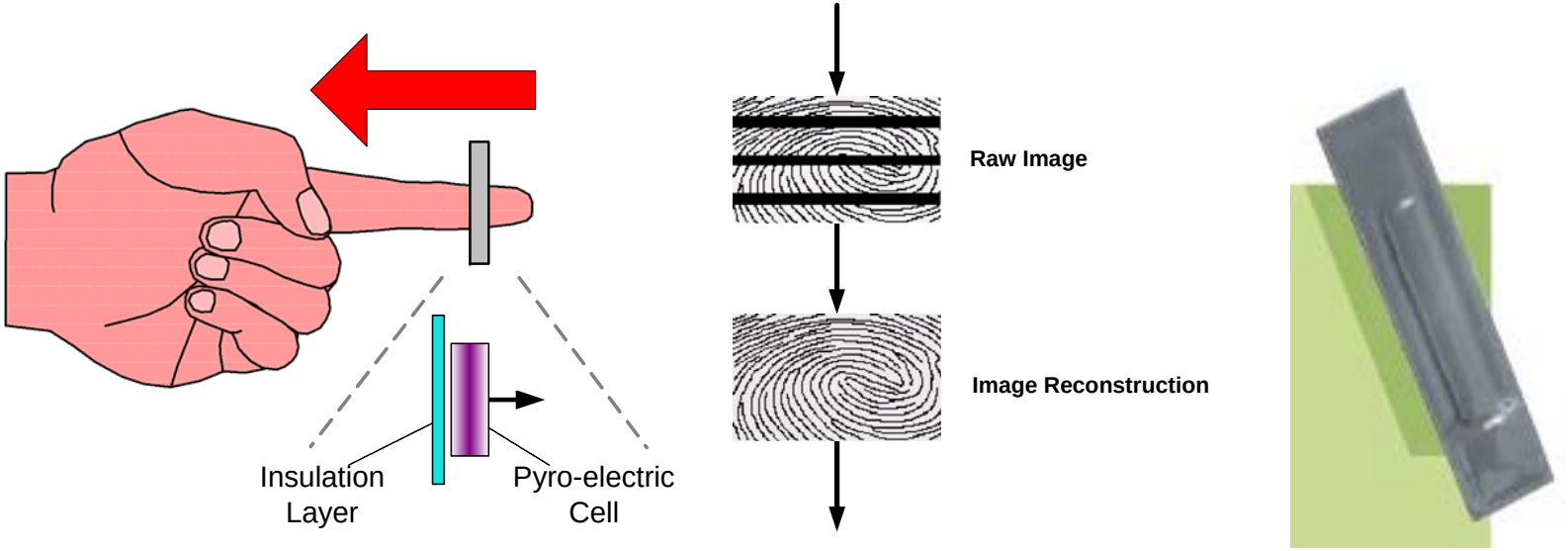
BMF

elektrooptický

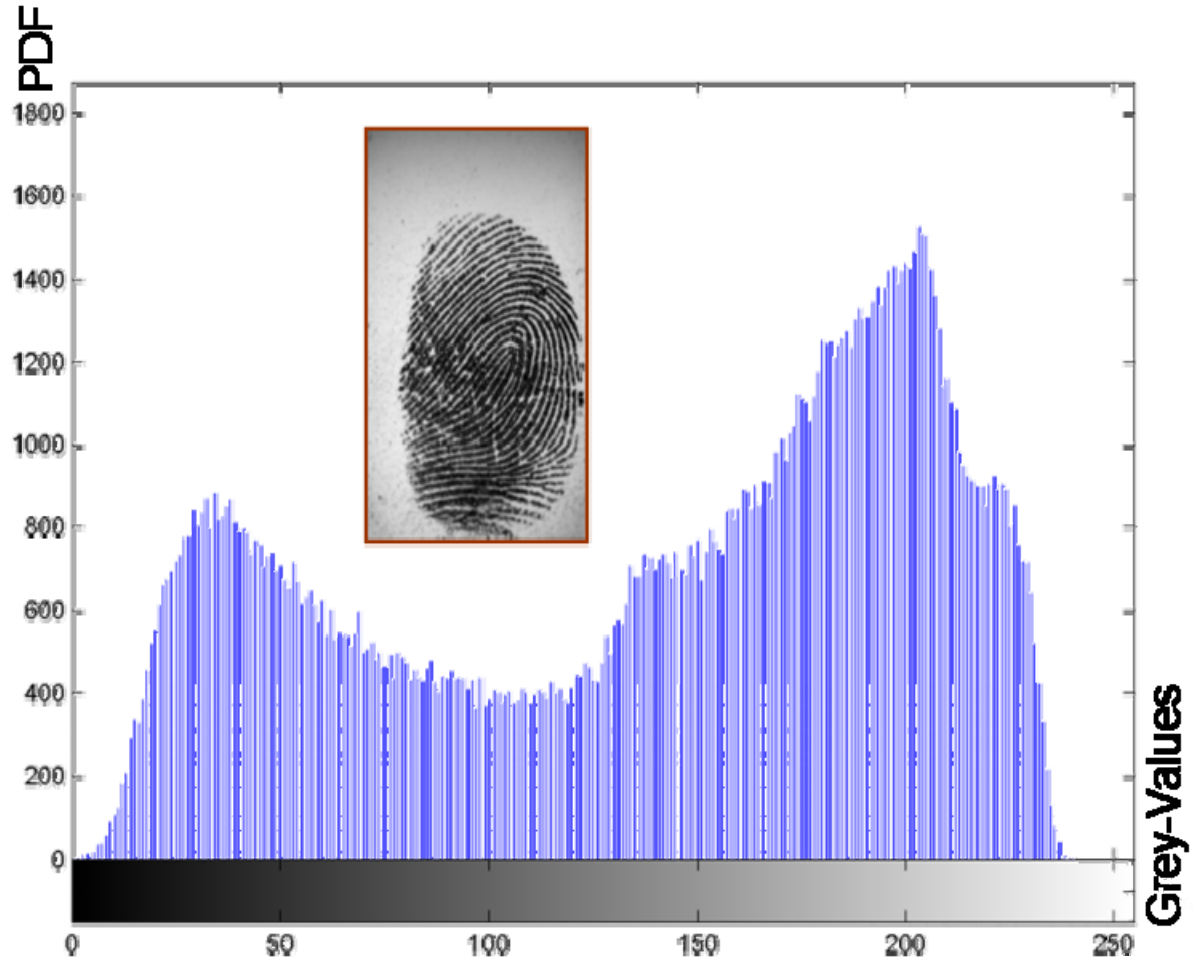


AuthentTec

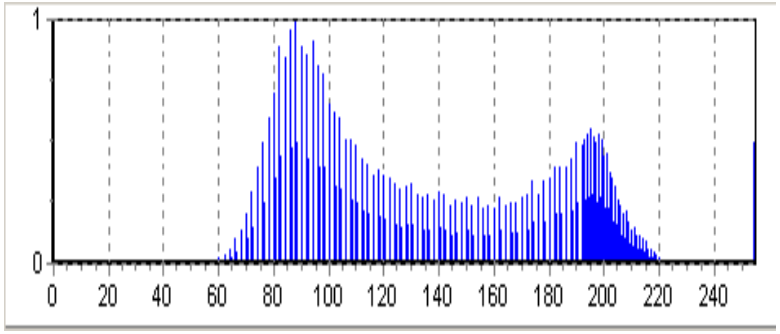
Tepelný snímač

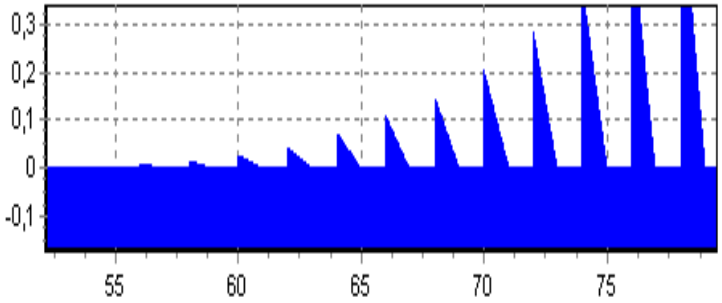


Kvalita obrazu – histogram otisku



Zvláštnosti sejmutého obrazu – příklady Suprema SFM 3050, Suprema SFM 3020



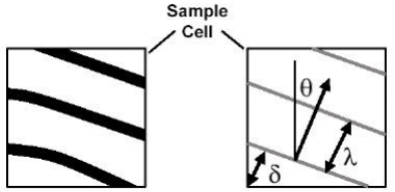


Markanty otisků prstů

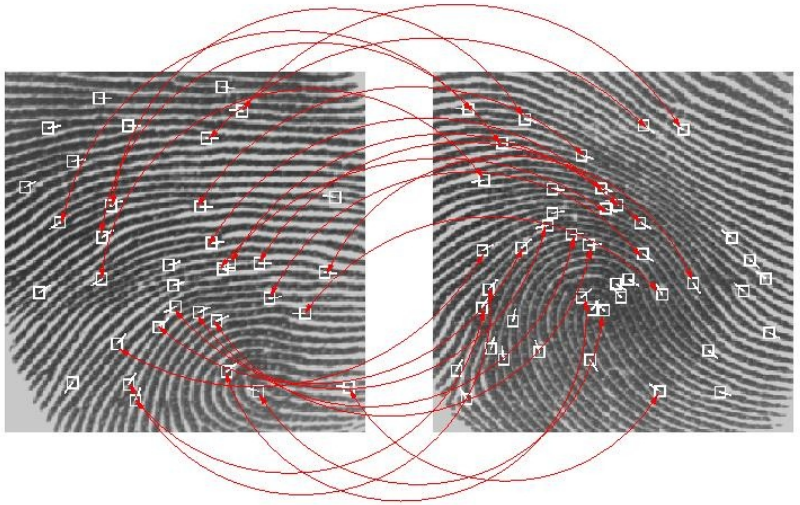
Otisky prstů

- Zpracování otisků prstů
  - „markanty otisků“ (ISO/IEC 19794-4)
  - spektrální srovnání (ISO/IEC 19794-3)

Zdroj: Digital Persona, Inc.



- Srovnání otisků prstů
- Rychlost
  - jedno srovnání 1ms až 2s
- Přesnost
  - FAR pod 0,01 %
    při FRR asi 5%



Geometrie ruky

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

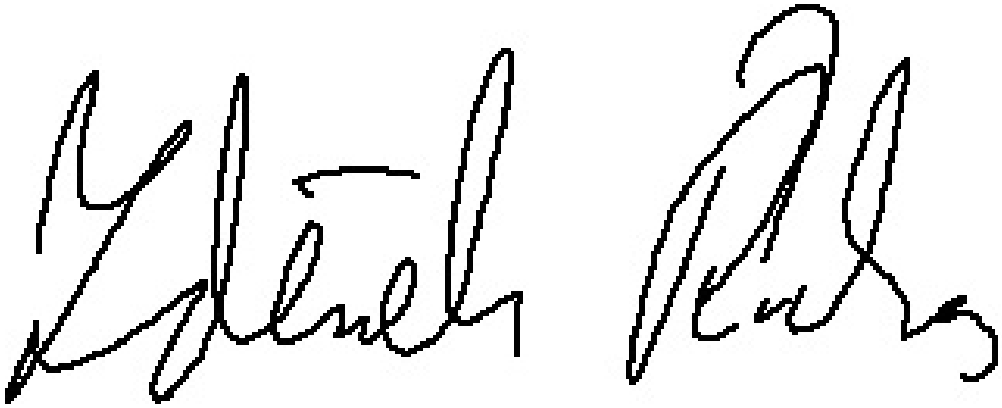
Geometrie ruky

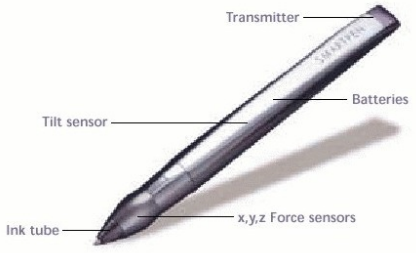
- Rychlost
  - verifikace asi během 1 s
- Přesnost
  - málo přesné, tvar ruky není jedinečný
  - nevhodné pro identifikaci
  - pouze omezeně vhodné pro verifikaci
  - FAR i FRR kolem 3 - 5 %
- Použito při kontrole vstupu do olympijské vesnice na Olympijských hrách v Atlantě v roce 1996

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 až 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

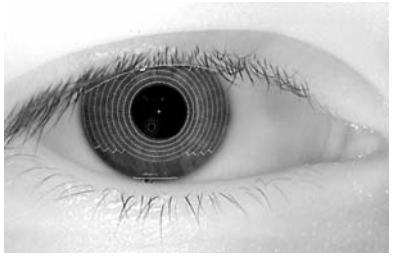
- Založeno na způsobu psaní na klávesnici
  - měří se čas stlačení klávesy a čas mezi stisky kláves
  - nevyžaduje speciální HW
  - algoritmy pracují na principu srovnávání vzorů (pattern matching) nebo neuronových sítí (neural networks – problém přidání dalšího uživatele)
  - možnost kontinuální autentizace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

Oční duhovka

- Srovnává se jedinečný vzor oční duhovky

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

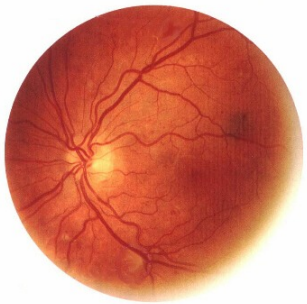
- Iriscode
  - 256 bajtů popisujících vzor duhovky



- 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

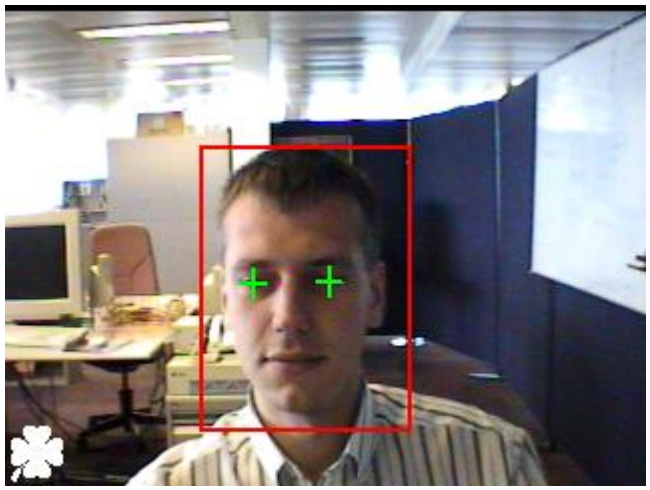


- Pro snímání se používá infračervený zdroj světla

- 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 procent
  - Přesnost se výrazně zlepšila v posledních 5 letech
  - Obličej člověka se mění v čase
  - Účes, brýle, náušnice
  - Problém osvětlení a pozadí

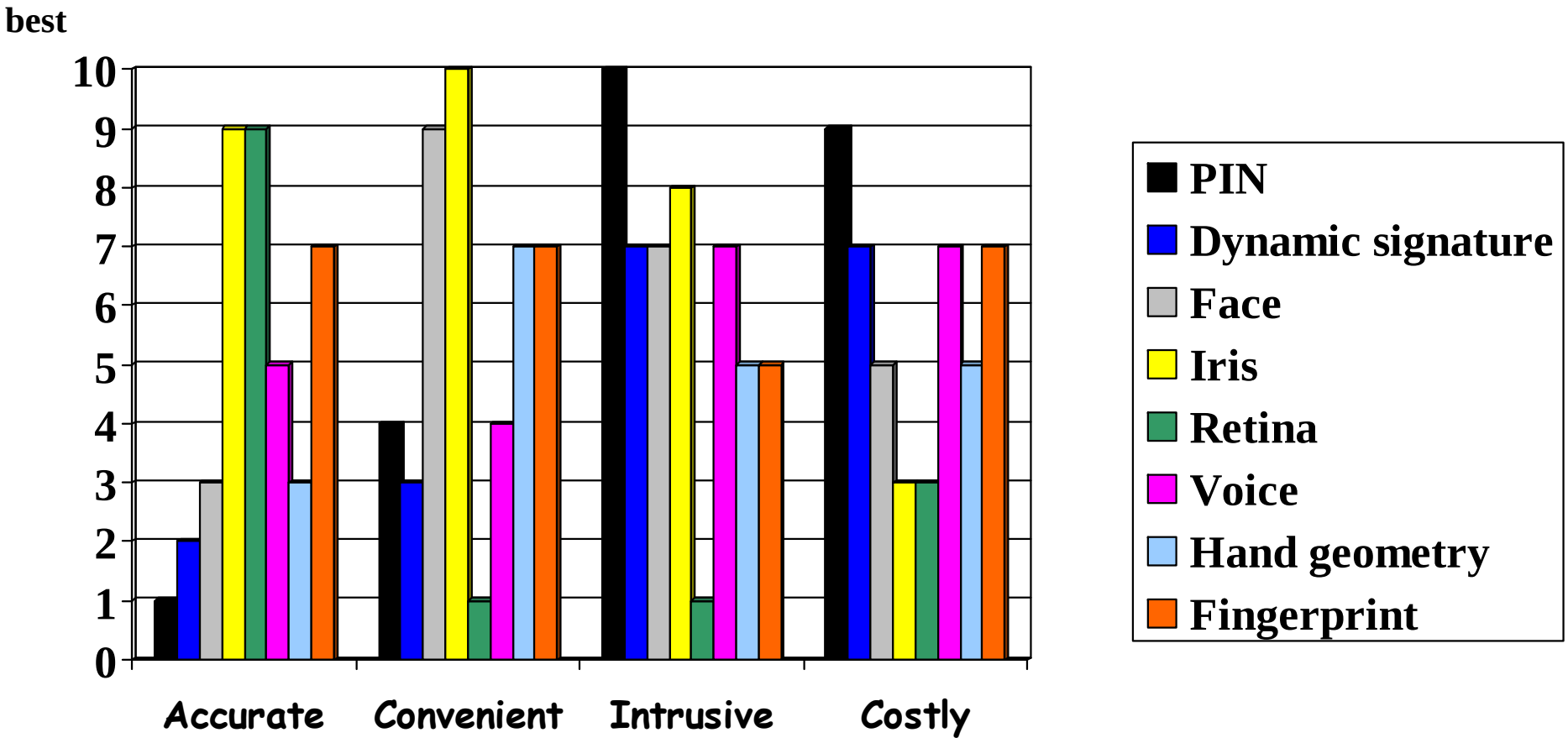


Kvalita snímku (ISO 19794-5)

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

DNA jako biometrika?

Počet vzorků	Pravděpod. náhodné shody	Doba analýzy (minuty)
1	10^{-18}, 16 znaků	345
10	10^{-18}, 16 znaků	450
90 poloautom.	10^{-18}, 16 znaků	830
90 plně autom.	10^{-18}, 16 znaků	190
1 plně autom.	10^{-10}, 8 znaků	93

Sériová analýza znaků (brzy)

1. znak	60 minut	10^{-2}
2. znak	60 minut	10^{-3}
3. znak …	60 minut	10^{-5}

Multiplexování (za X let)

3 znaky	60 minut	10^{-5}
další 3…	60 minut	10^{-7}
další 3…	60 minut	10^{-10}

Polosemestrální písemka (I)

- 19. 4. 2011
  - Dvě skupiny od 10:00 a 10:50 – rozpis v ISu
  - Body jsou kladné i záporné
  - Záporné bodování je vyšší a nižší
    - Podle toho jak špatně je dané odpověď
  - Volné otázky u polosemestrální písemky nebudou
  - Celkem asi 30 bodů, což je 30 % celkového počtu bodů pro hodnocení zkoušky
  - Kdo bude nemocný nebo jinak omluven v ISu bude mít přepočítané body z finální písemky
    - Tj. náhradní termín polosemestrálky není

Polosemestrální písemka (II)

- Organizační pokyny
  - Přijďte včas (čas nás tlačí)
  - S sebou jen ISIC a pero (případně náhradní pero)
  - Čekejte u spodního vchodu do D3, seřaďte se přibližně podle abecedy
  - Odchod bude probíhat horním vchodem

Příklad otázky

Jak zajistíme integritu veřejného klíče
 :c1 Pomocí párového privátního klíče
 :c2 Pomocí klíčované hašovací funkce
 :c3 Pomocí certifikátu veřejného klíče
 :c4 Částečným utajením veřejného klíče
 :c5 Utajením soukromé části veřejného klíče
:c1 -3
:c2 -2
:c3 ok 4
:c4 -3
:c4 -4

Otázky?

Vítány!!!

PÍSEMKA 19. 4. 2011 10:0x-10:3x, 10:5x-11:2x

Příští přednáška 12. 4. 2011 v 10:00

matyas@fi.muni.cz

zriha@fi.muni.cz

PV157 – Autentizace a řízení přístupu

Biometrická autentizace uživatelů II.

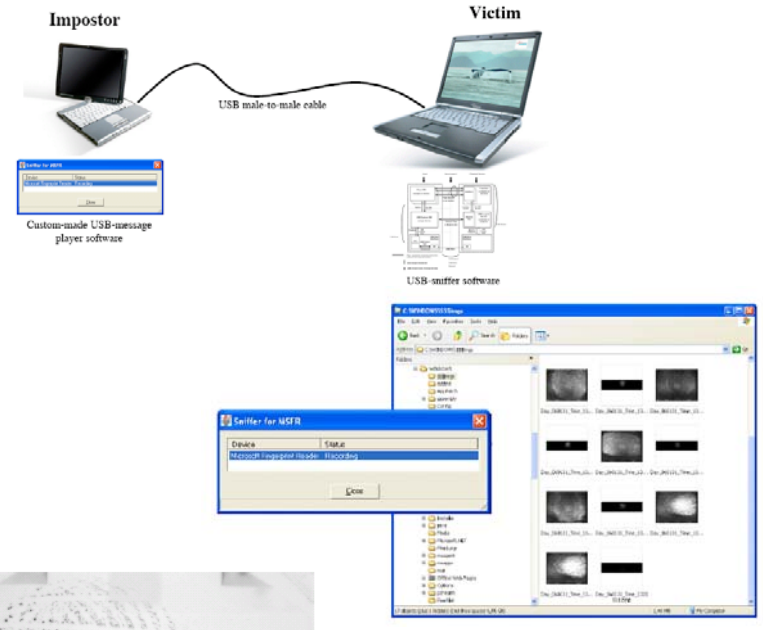
Příklad běžného komerčního zařízení!

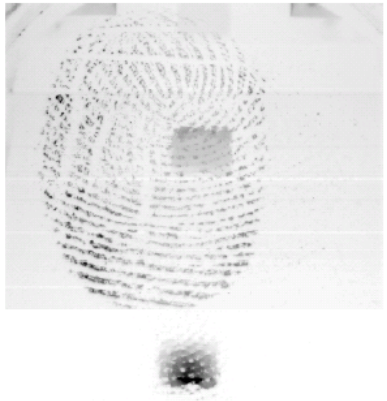
- The biometric (fingerprint reader) feature in this device is not a security feature and is intended to be used for convenience only. It should not be used to access corporate networks or protect sensitive data, such as financial information. Instead, you should protect your sensitive data with another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

- Zařízení opravdu není příliš bezpečné…
- http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Kiviharju/bh-eu-06-kiviarju.pdf

Příklad běžného komerčního zařízení (2)

- Zařízení není autentizováno, lze jej nahradit útočníkovým zařízením (např. notebookem)
- Přenášená data nejsou šifrována (jedná se o odlehčené zařízení DigitalPersona UareU s vypnutým šifrováním), odposlechem USB je možné získat otisky prstů
- Obrana vůči podstrčeným datům je realizována kontrolním součtem určité oblasti otisku





Fingerprint, and its "checksum"

Komerční versus forenzní

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

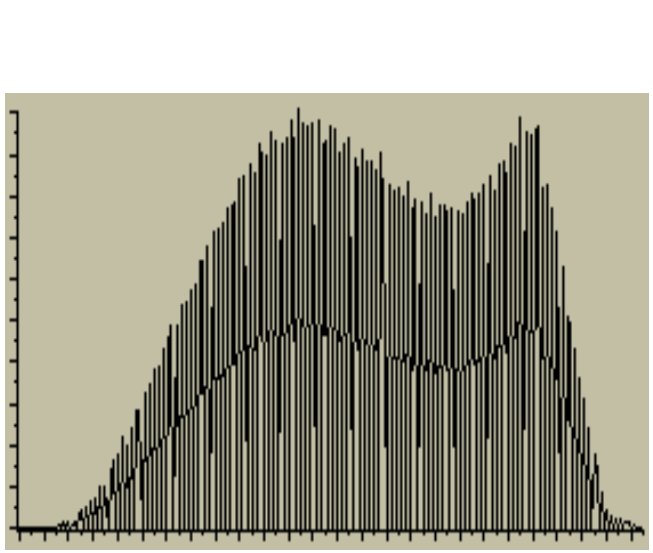
- Vyšší přesnost
- Nutné manuální intervence profesionálů
- Registraci není možné opakovat
- Uchováváme zpracované charakteristiky i původní biometrické vzorky

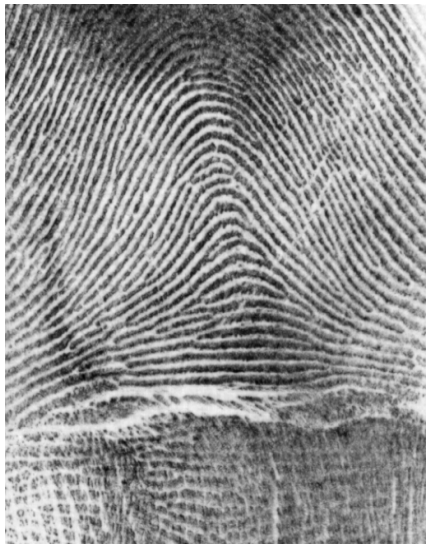
Komerční versus forenzní II.

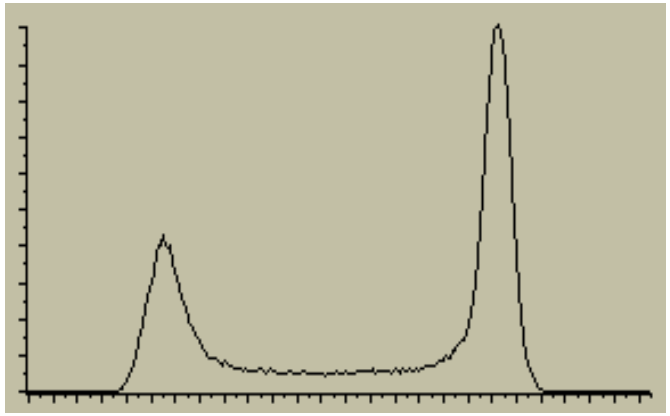
- Výsledek autentizace v sekundách
- Nízká až střední znalost systému nutná (pro používání)
- Miniaturizace
- Cena hraje důležitou roli a je relativně nízká

- 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.

Kvalita forenzních a běžných systémů







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)

Testování živosti

- Obvykle má jako dopady
  - Zvětšení senzoru/zařízení
  - Vyšší náklady na vývoj a výrobu
  - Zvýšený počet nesprávných odmítnutí

- Řada metod je patentovaných
- Žádná metoda neposkytuje 100% ochranu (bezpečnostní „klasika“ – každé řešení lze obelstít, záleží „jen“ na ceně útoku – a znalost principu testu tuto cenu výrazně snižuje!)

Tsutomu Matsumoto 2002 (1)

How to make a mold

Put the plastic into hot water to soften it.

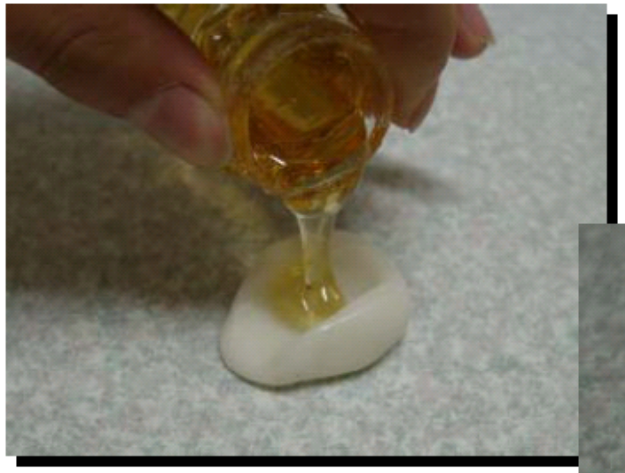
Press a live finger against it.

The mold

It takes around 10 minutes.

Tsutomu Matsumoto 2002 (2)

How to make a gummy finger



Pour the liquid into the mold.

Put it into a refrigerator to cool.

The gummy finger

It takes around 10 minutes.

Tsutomu Matsumoto 2002 (3)

Captured images with the device C (an optical sensor).

(a) Live Finger (b) Silicone Finger (c) Gummy Finger

Captured images with the device H (a capacitive sensor).

(a) Live Finger (b) Gummy Finger

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“

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 + biometrické 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 3. 5. 2011 v 10:00

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