Autentizace uživatelů

Kamil Malinka
malinka@fit.vutbr.cz
Fakulta informačních technologií

Důležité termíny

- **Termín vnitrosemestrální písemky**
  - 3.11. - 7.00 v místnosti P381.
  - Na vypracování písemky budete mít 45 minut. Písemka bude písemná a otázky budou pokrývat problematiku probranou během předcházejících přednášek (tedy přednáška 1 až 6 včetně). Po skončení písemky bude dále pokračovat přednáška.
  - Upozorňuji, že opravný termín nebude. Vypíšu pouze náhradní termín a to pouze pro studenty, kteří se prokáží neschopenkou s datem termínu písemky.

- Veškeré informace týkající se cvičení z KIB naleznete na http://www.kumpost.net/kib/

Tři základní přístupy

- něco co víš
- něco co máš
- něco co jsi

Hesla, PINy…

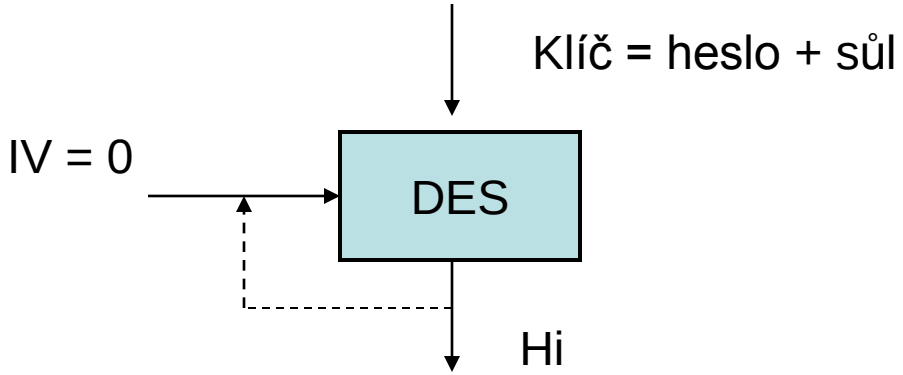
- Cílem je, aby autentizace uživatele byla:
  - jednoduchá pro *oprávněné* uživatele
    - limitem je lidská paměť – krátká, jednoduchá hesla
  - obtížná pro ***ne****oprávněné* uživatele
    - nutno zabránit slovníkovému útoku, hádání => dlouhá, těžko zapamatovatelná hesla
- dalším krokem je řízení přístupu
- nutno pokrýt 3 okruhy problémů:
  - uložení vzorů
  - korektní verifikační proces
  - kvalita autentizační informace

Ukládání hesel

- v čisté formě
  - ochrana na úrovni OS (řízení přístupu pro zápis a čtení)
  - absolutní důvěra v administrátora
  - co se stane, pokud je soubor zkopírován
    - **raději NE**
- v nečitelné formě
  - šifrované
  - hashované

Šifrování hesel

- pomalejší (problém při velké zátěži systému)
- nedoporučuje se šifrovat „pouze“ hesla
- technika „solení“
  - tabulka hesel: user ID, sůl, f(sůl, heslo)
  - zisk delších efektivnějších hesel
  - řešení kolizí



1984 – Gramp & Morris

- hlavní bezpečnostní problém systémů založených na heslech – uživatelé
- systémy s alespoň 6 znakovými hesly, aspoň 1 znak nealfabetický
- studie útoku:
  - jednoduchý slovníkový útok
  - 20 nejčastějších ženských jmen následovaných číslem => 200 hesel
  - alespoň jedno heslo nalezeno v každém systému
- lámání hesel
  - 1979 Bellova společnost – úspěšnost 6/7
  - 1990 DV Klein – analýza 13797 soborů s hesly (/etc/passwd) úspěšnost 1/4

Zvýšení složitosti hesel

- **Pravidelná změna hesla**
  - MyPasswd09 in Sept, MyPasswd10 in Oct
  - jiná varianta – uživatelé zjistí délku historie a vrátí se k původnímu heslu
    - passwd123 → qwre21 → jr7*&d → passwd123
- **Vstupní fráze**
- heslo je odvozeno z delší fráze (úryvek knihy, báseň…)
  - *psmVTCOo24Z* = Polámal Se Mraveneček, Ví To Celá Obora, O Půlnoci Zavolali

Osobní identifikační čísla - PIN

- levná klávesnice/PINpad
- těžší na zapamatování – v porovnání s hesly
- obvykle s fyzickým předmětem – token
- možnost změny PINu uživatelem
- obvyklá délka PINu je 4-8 číslic
- procedurální omezení proti útoku hrubou silou
  - zablokování karty po několika (2-3) špatných pokusech
  - reaktivace pomocí záložního PINu (delší, obvykle uschován v psané formě) - PUK

Závěr k heslům

- náhodně generovaná hesla –obtížně zapamatovatelná
- hesla založená na frázích jsou obtížněji uhodnutelná
- hesla z frází se lépe pamatují v porovnání s jednoduchými hesly
- školení uživatelů nemá **žádný** vliv na jejich chování – bezpečnost hesel

Autentizační tokeny

- ekonomické dilema
  - poměr ceny výroby ku ceně padělání
  - produkce ve velkých sériích (nejnižší možná cena)
  - vylepšování tokenu na nejnižší možnou ještě bezpečnou úroveň
  - př: čipové karty – ochrana proti útokům skrytými kanály

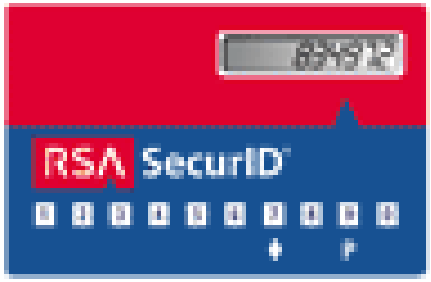
Cena padělání

- běžné ekonomické pravidla ALE
  - rozdíl mezi vytvořením jednoho nebo mnoha padělků (např. dekodéry satelitních televizních kanálů) – vysoké náklady jsou pokryty následným ziskem
  - čas potřebný na výrobu padělku
  - počet originálních tokenů potřebných k vytvoření padělku
  - možnost potrestání útočníků (další navýšení ceny útoku)

    - to vše ovlivňuje ceny, rizika a benefity ☺

Nejčastější tokeny

- Karty
  - s magnetickým páskem
  - smart-karty (čip)
    - kontaktní/bezkontaktní
    - vlastník čtečky/verifikátor
- Autentizační kalkulátory
  - s tajemstvím
  - časově synchronizované
  - vstup/výstup rozhraní



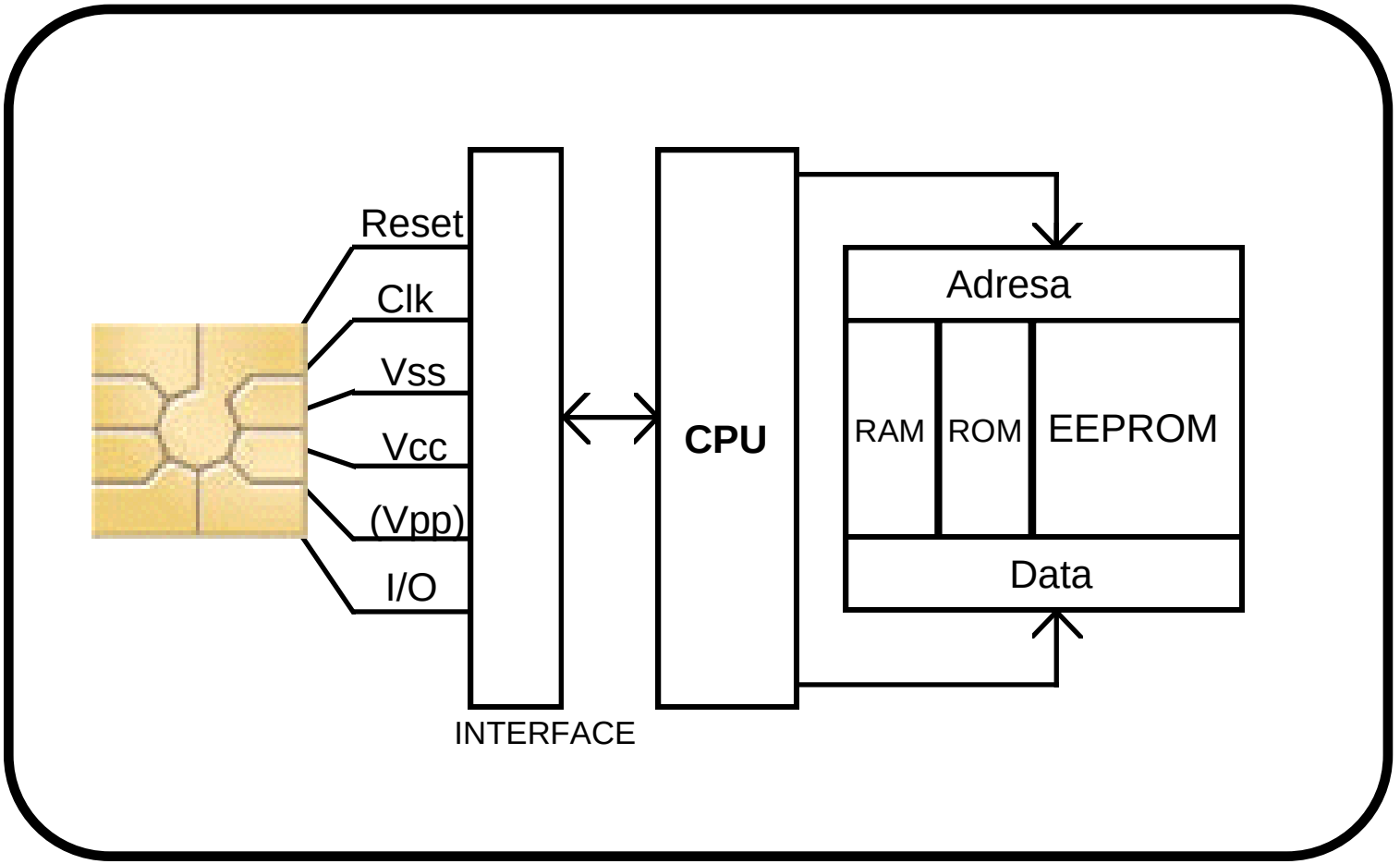
Smart karty

- paměťové karty (*čipové karty*)
- paměťové s logikou (zabezpečené PINem, čítačem, atd..)
- procesorové karty (*smart karty*)
- kontaktní – čtečka slouží jako zdroj komunikace a napájení
- bezkontaktní
  - nemožnost použít externí zdroj energie – limity použití
  - možnost operace s kartou bez vědomí uživatele
  - vhodné pro fyzické řízení přístupu

Procesorové karty

- obvykle nazývány jako smart karty
- několik typů pamětí
  - RAM (Random Access Memory) – pár KB
  - ROM (Read Only Memory) – desítky - 10^2 KB – OS
  - EEPROM (Electrically Erasable Programmable Read Only Memory) – desítky KB
- Podporují nejrůznější složitosti výpočtů, ideálně dokonce náročné kryptografické operace

Kontaktní smart karty



Autentizační kalkulátory

- vyžadují speciální infrastrukturu
- běžně využívají protokoly výzva-odpověď
  - odpověď je odvozena z výzvy a tajné informace uložené v HW
  - výměna informací (vstup/výstup)
    - manuální (keypad, displej)
    - automatická (optika, čárové kódy, infrared)
- PIN - standard

Časově synchronizované tokeny

- část autentizačních tokenů
  - ne vždy – RSA SecurID
- hodnota je platná pouze v daném momentu
  - hodnota je unikátní pro každý token
  - hodnota se mění s časem (předdefinované časové okno)
  - stejná hodnota je vypočítána autentizačním serverem
- Problém synchronizace
  - otázka časového okna (přes, po)
  - čítač záznamu na serveru

Souhrn

- pro
  - token může obsahovat relativně velké množství dalších informací
  - je obtížné jej zkopírovat
  - je snadné zjistit ztrátu
  - je možné s nimi implementovat bezpečné autentizační protokoly
- proti
  - potřeba speciálních čtecích zařízení nebo tréninku uživatelů
  - žádný token – žádná autentizace
  - složitost musí být dostatečná, aby odolala útokům
  - může se pokazit, přestat fungovat – relativně obtížné zjistit

Tří faktorová autentizace

- maximum v oblasti autentizace
- užití každé ze tří základních skupin autentizace

- token- smart karta
- PIN/heslo – pod kontrolou autentizačního serveru
- biometrika zpracovaná tokenem

Biometrická autentizace

- autentizační metody založené na 3 přístupech
  - něco máme (klíč, kartu)
  - něco víme (PIN, heslo)
  - **něco co jsme (biometriky)**

- ***Biometriky*** – „*automatizované* metody identifikace nebo autentizace založené na měřitelných fyziologických nebo behaviorálních charakteristikách lidského těla“

Specifika biometrik

- metodika
  - registrace
    - prvotní odběr vzorku biometrických dat
  - verifikace/identifikace
    - následné odebírání vzorků a jejich porovnání s původním registračním vzorkem
- variabilita
  - biometrická data nejsou nikdy 100% identické
  - musíme připustit určitou míru variability (práh) mezi registračním vzorkem a dalšími vzorky

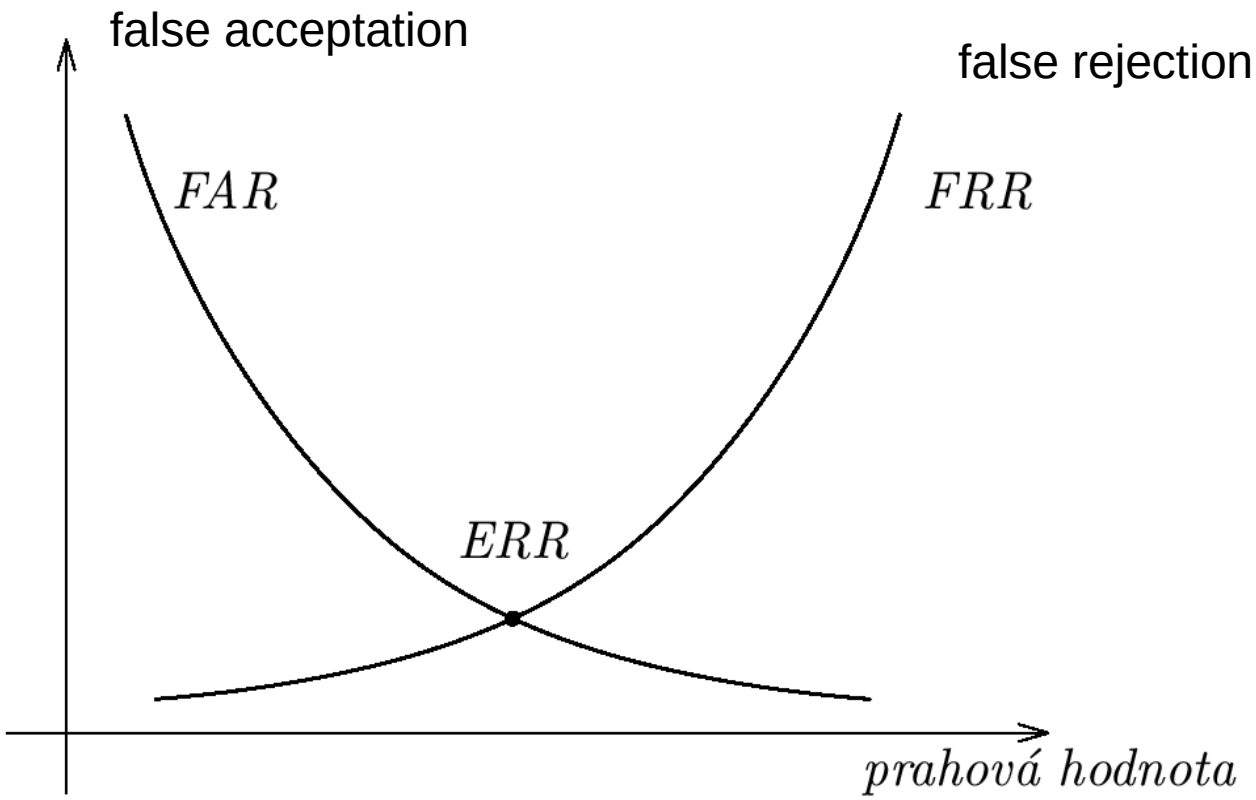
Biometrická autentizace Model I

- registrační fáze
  - prvotní odběr vzorku biometrických dat
    - kvalita této fáze ovlivňuje četnost chyb v autentizační fázi
  - vytvoření registračního vzorku
    - extrakce důležitých charakteristik
  - uložení registračního vzorku
    - karta, čtečka, pracovní stanice, server

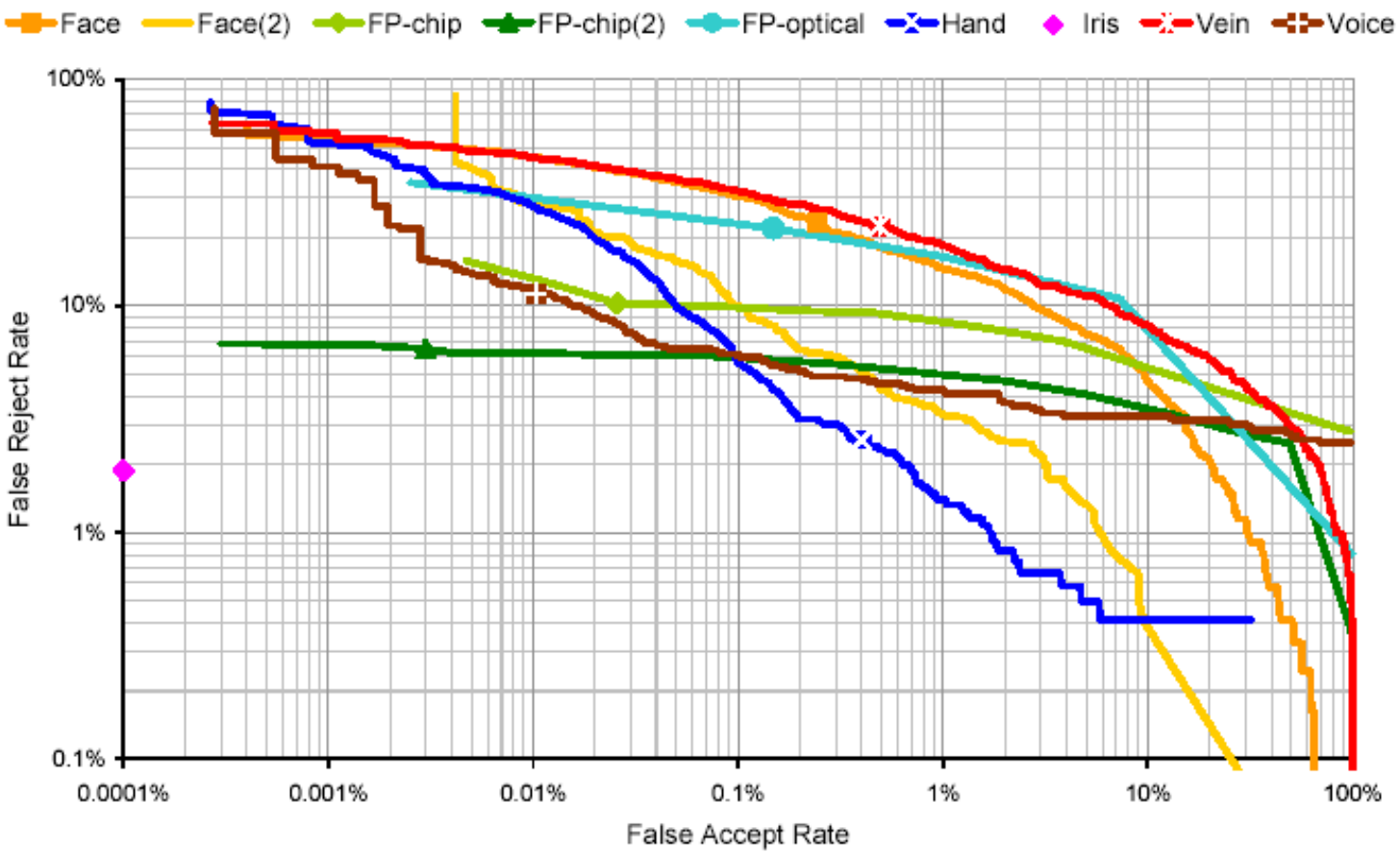
Biometrická autentizace Model II

- identifikační/autentizační fáze
  - snímání biometrických dat
    - plně automatické, bezobslužné
  - extrakce charakteristik
    - k dispozici je pouze jeden snímek
  - porovnání aktuální charakteristiky s registračním snímkem
  - úroveň korelace / shody
  - závěrečné ano/ne

Četnost chyb



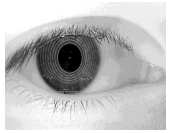
- Receiver operating curve (ROC)



Biometrické technologie

- otisky prstů

- duhovka



- sítnice

- rozpoznávání obličeje

- geometrie ruky

- rozpoznávání hlasu

- dynamika podpisu

- dynamika psaná na klávesnici

heslo

Otisky prstů

- jedna z nejstarších metod
- snímání otisků
  - s použitím inkoust
  - bez inkoustu

čtečky otisků prstů

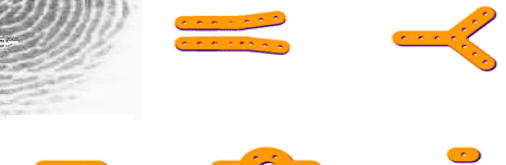
- optické

- silikonové (kapacitní)

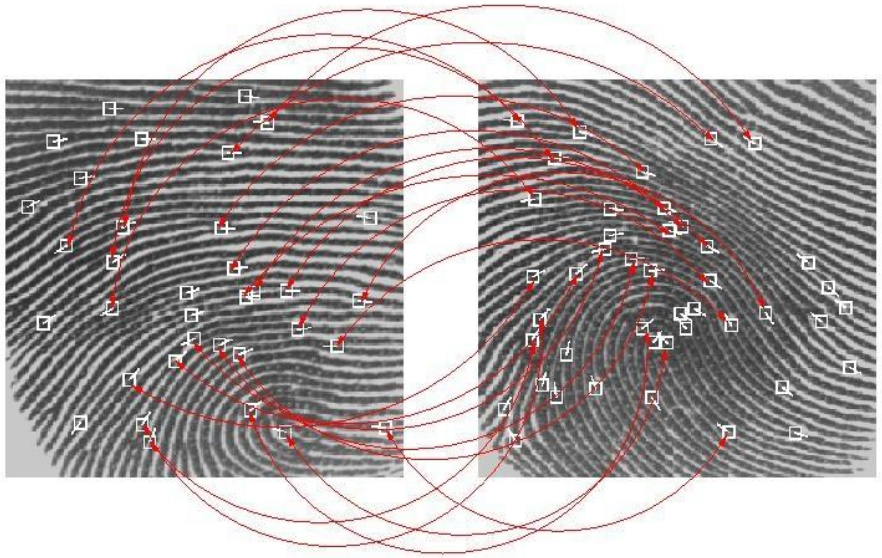
- ultrazvukové

Otisky prstů

- zpracování otisků
  - „miniatury“
- porovnání otisků
- rychlost
  - jedno porovnání od 5ms do 2s
- přesnost
  - FAR pod 0,1 %
    FRR okolo 5%



Zdroj: Digital Persona, Inc.



Geometrie ruky

- skenování geometrie, obrysu ruky
- není unikátní (na rozdíl od např. otisku prstu)

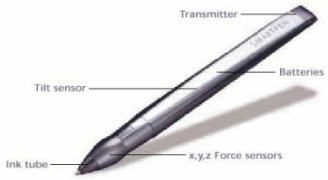
- možnost zachycení 3D snímku
  (velikost okolo 9B)

Geometrie ruky

- rychlost – verifikace okolo 1 s
- přesnost
  - relativně nízká, geometrie není unikátní
  - nevhodná pro identifikaci
  - omezené užití pro verifikaci
  - FAR a FRR okolo 10 %
- použito pro řízení přístupu do olympijské vesnice v Atlantě 1996

Dynamika podpisu

- více než podpis je důležitý způsob jakým je tvořen
- vstupní zařízení
  - tablet
  - speciální čtečka ve formě tužky

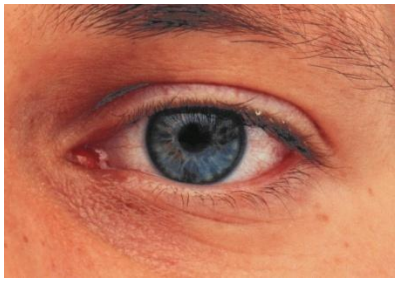


Dynamika podpisu

- velikost charakteristiky
  - okolo 20 kB (spočítána z 3 až 10 podpisů)
- rychlost
  - verifikace okolo 1 s
- přesnost
  - velmi nízká, nedostatečná pro většinu aplikací
  - FAR a FRR v desítkách procent

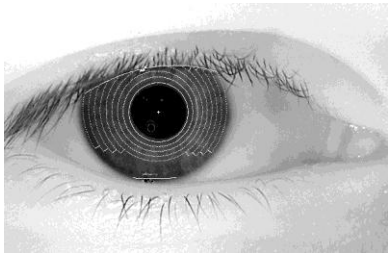
Duhovka

- obraz duhovky (unikátní)



- skenování
  - B/W kamera ze vzdálenosti 10 cm

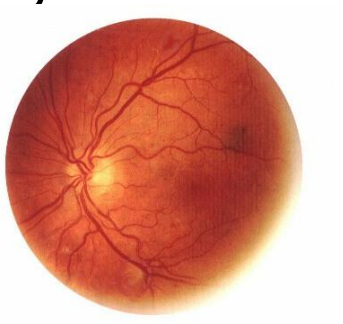
- Iriscode
  - 256 B charakteristika



- rychlost
  - miliony srovnání za sekundu
- přesnost
  - velmi dobrá, vhodná pro identifikaci
  - FAR (téměř) nulová, FRR okolo 3 %

Sítnice

- obrázky sítnicových kapilár

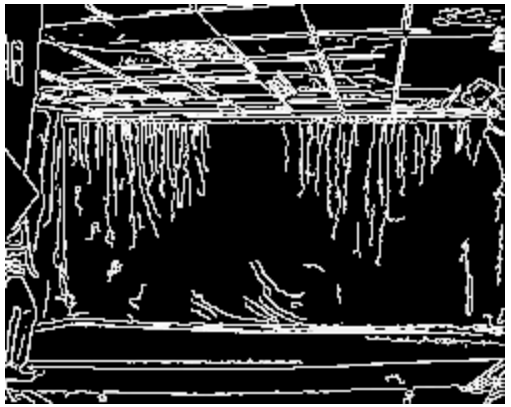


- skenování pomocí laserového paprsku

- velikost charakteristiky
  - 96B
- přesnost
  - velmi vysoká
  - nízké FAR, ne tak dobré FRR
- uživatelská přívětivost
  - skenování není moc příjemné

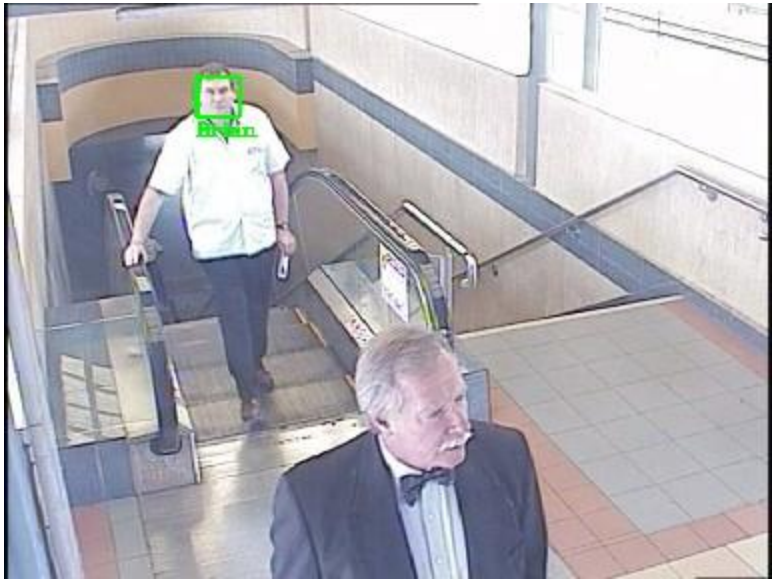
Chůze

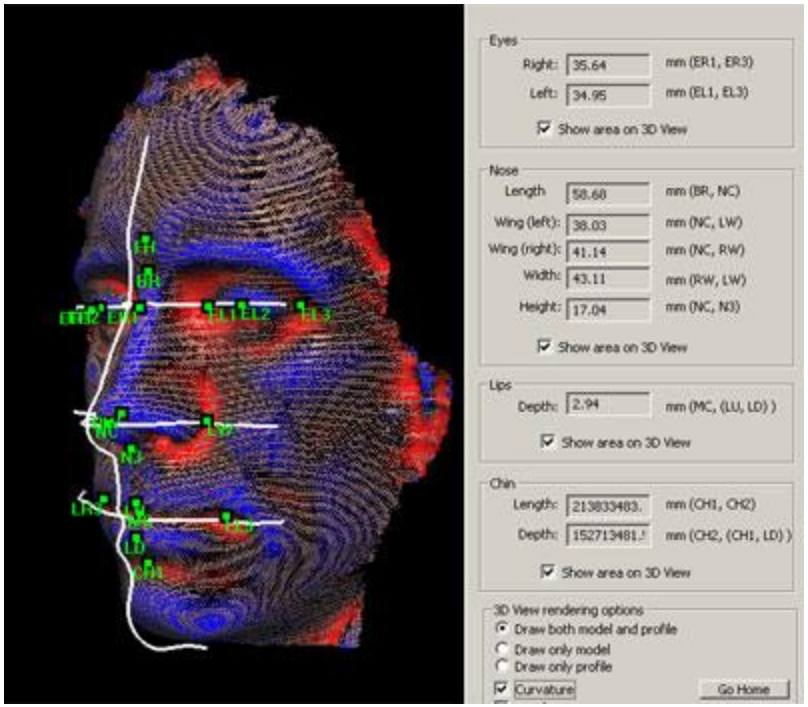
- výzkum řízen tématem terorismu
- historické zázemí
  - Leonardo da Vinci…
  - literatura…
- relativně nová metoda



Obličej

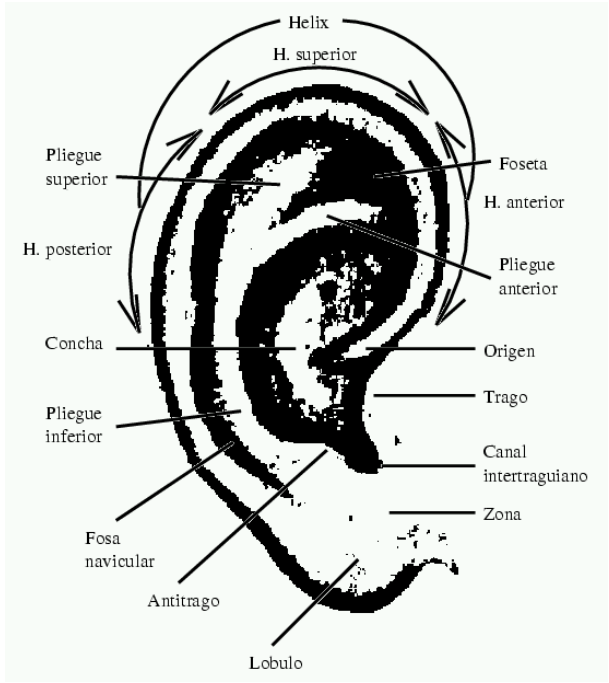
- 2D vs. 3D
- identifikace v davu (sportovní akce…)
- záznamy z kamer
- …

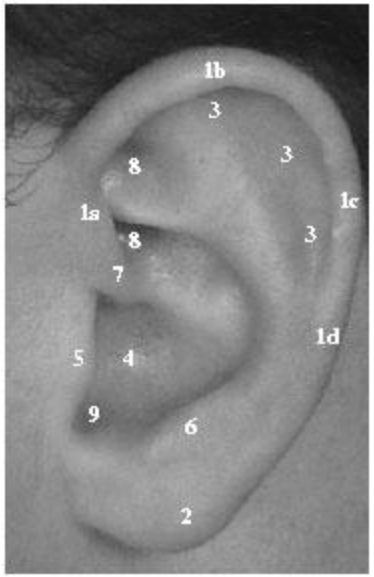


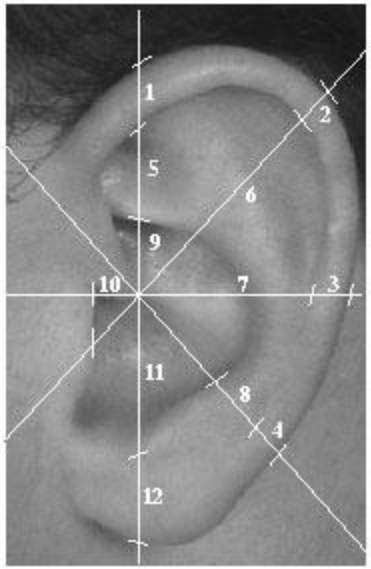


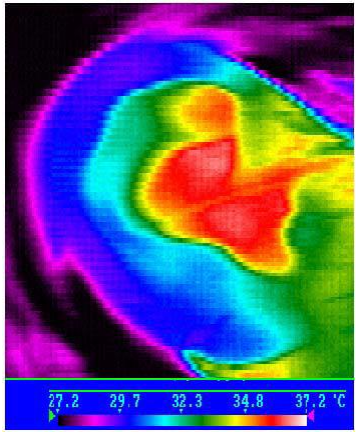
Ucho

- Stejně unikátní jako otisk prstu

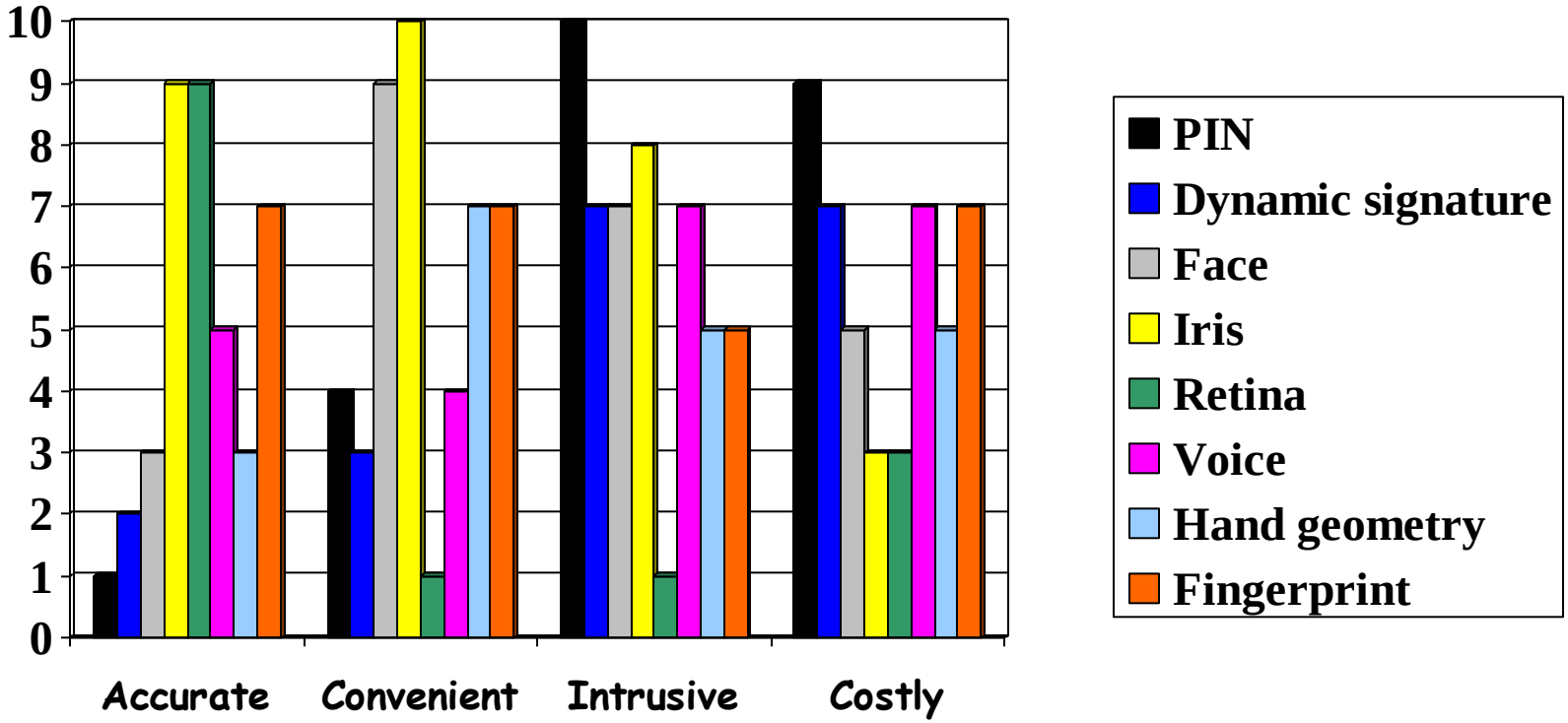








Souhrnné srovnání



Komerční vs. forenzní

- nízká přesnost
- plně automatické, příslušenství k PC
- registraci je možné zopakovat
- ukládány pouze charakteristiky

- vyšší přesnost
- manuální zpracování odborníkem
- registrace je věcí jednoho pokusu
- jsou ukládány i originální biometrická data

Komerční vs. forenzní II.

- autentizace během vteřin
- uživatelé nepotřebují téměř žádné znalosti o systému
- miniaturizace
- cena je tlačena konkurencí stále níž

- identifikace trvá i několik dní
- je třeba uživatelů s přesnými a důkladnými znalostmi systému a problematiky
- velikost je naprosto nepodstatná
- relativně drahé, cena není nejdůležitějším faktorem

Biometriky a kryptografie

- biometriky nejsou soukromé!!!
- generování kvalitních kryptografických klíčů z biometrických údajů je více méně nepoužitelné
  - atraktivní design – klíč vždy když je potřeba

  ale

  - prostor klíčů je dost omezený
  - co bude tajemství a kde bude uloženené?
  - co v případě kompromitace klíče?
  - nevratné změny vzoru, změna skenovací technologie…

Nové trendy

- řešení zkreslení charakteristik
- zvětšení prostoru charakteristik záměrnou deformaci vzorku
- nové biometriky
  - DNA
  - tlukot srdce, EEG

  ….