Obrázky: M.C. Escher,
i dále v přednášce

Identita

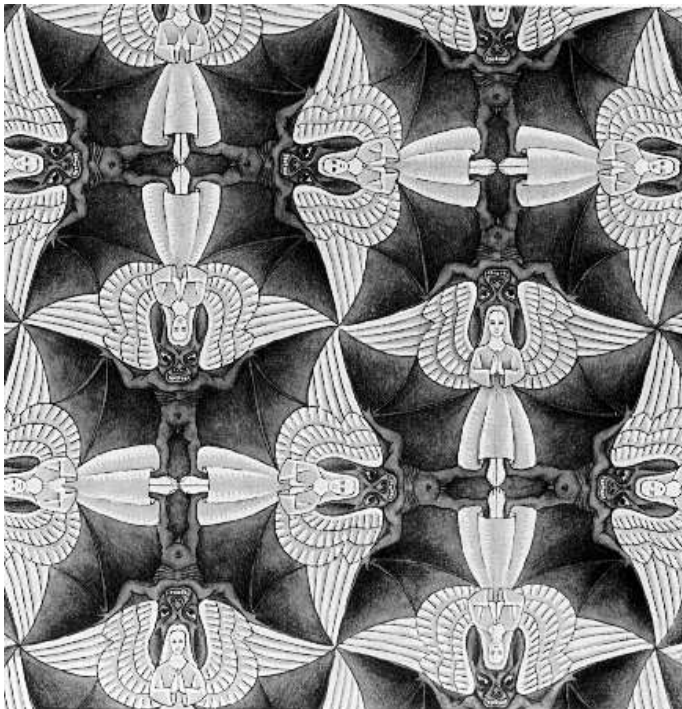
v počítačových a komunikačních systémech

Vašek Matyáš

Fakulta informatiky Masarykovy univerzity

Agenda

- Úvod, terminologie, základní problémy
- Autentizace v počítačových systémech
- Hesla a PINy
- Tokeny
- Biometriky



Jak rosteme…

- Každý rok přidáváme
  - Téměř 260 milionů nových „standardních“ počítačů
  - …přes 70 milionů aut
    - Průměrné auto má dnes asi 50 procesorů
  - …asi 2 miliardy nových mobilů
  - …9 miliard čipových karet (přes 90 % s procesory)
  - …přidejte PDA, e-pasy a jiné RFID čipy, senzorové uzly, vlaky, letadla, lodě, domácí spotřebiče…
- Uživatelé služeb mobilní telefonie – 7+ miliardy (2015)
  - 1 miliarda v roce 2002
  - GSM sítě fungují ve více zemích a teritoriích než je jich v OSN (193 vs. 238)

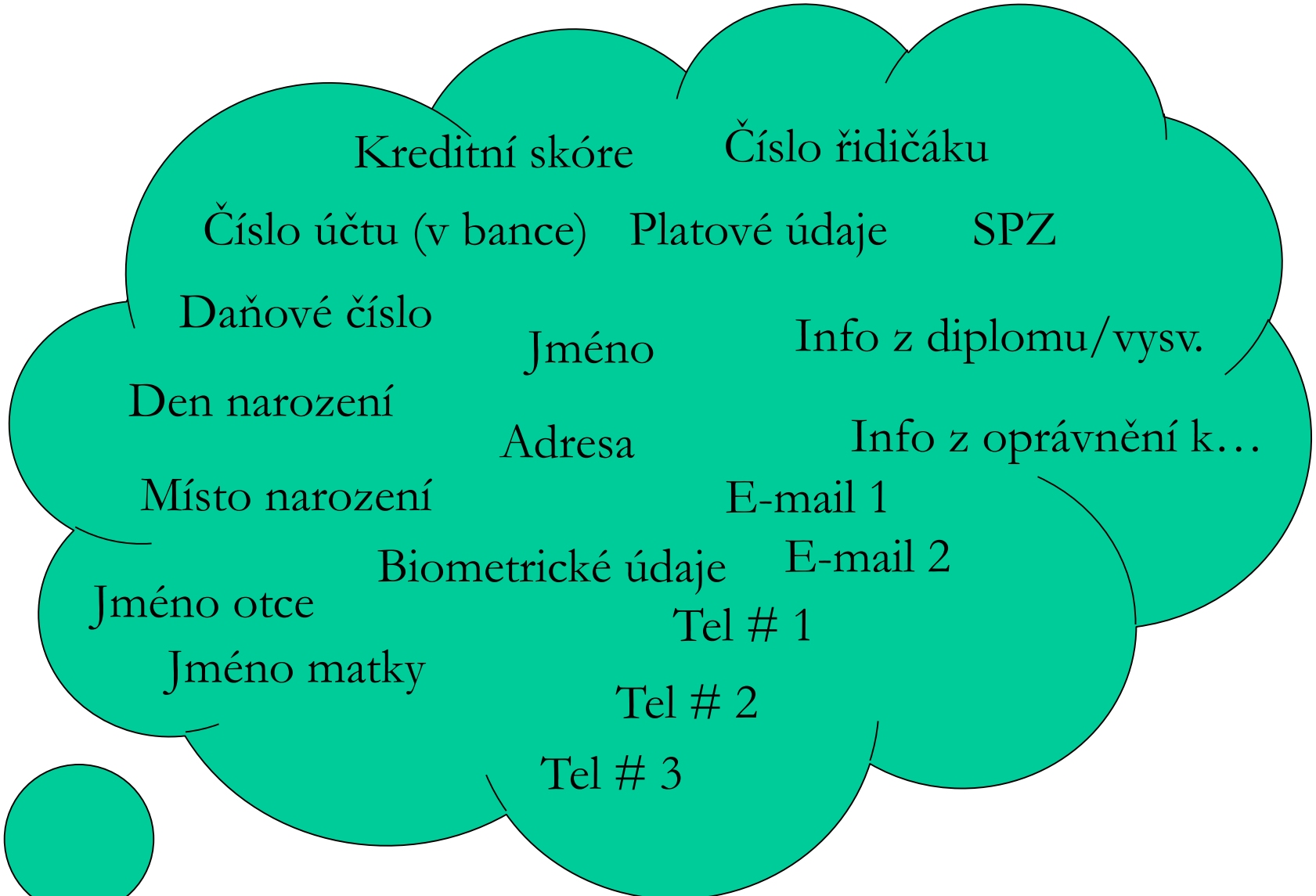
Osobní identita

  - Biologická
  - Fyziologická
  - Sociální
- Kriminologie předpokládá, že během života člověka se identita nemění
- Identifikace
  - Interní
  - Externí
- Potřeba lepší identifikace – příjmení, identifikační čísla…
  - Šangaj má 8 mil. lidí se 408 příjmeními, celá Čína 3 100 příjmení a čínských Top 5 (Zhang, Wang, Li, Zhao, Chen) používá 350 milionů lidí

Identita

- Libovolná podmnožina atributů určitého jedince, která tohoto jedince jednoznačně určuje v jakékoliv množině jedinců.
  - Tzn. není jedna identita, ale několik.
  - *Částečná identita* se pak vztahuje k určitému kontextu či roli, tzn. i k omezené množině jedinců.
    - Pak může být i pseudonym za určitých okolností identifikátorem pro částečnou identitu.

Různé části identity



Pseudonym

- Z řeckého *pseudonumon* – falešně pojmenovaný
  - tzn. používající jiné než „skutečné jméno“
- Pozor – „skutečné jméno“ (např. dané oficiálními státními dokumenty) se během života mění
  - Mimo „obvyklých“ změn i otázky písma/abecedy
  - Jako pseudonym lze pak označit každé pojmenování (identifikátor)

Pseudonymita

- Bytí pseudonymním je stav používání pseudonymu jako identifikátoru (ID).

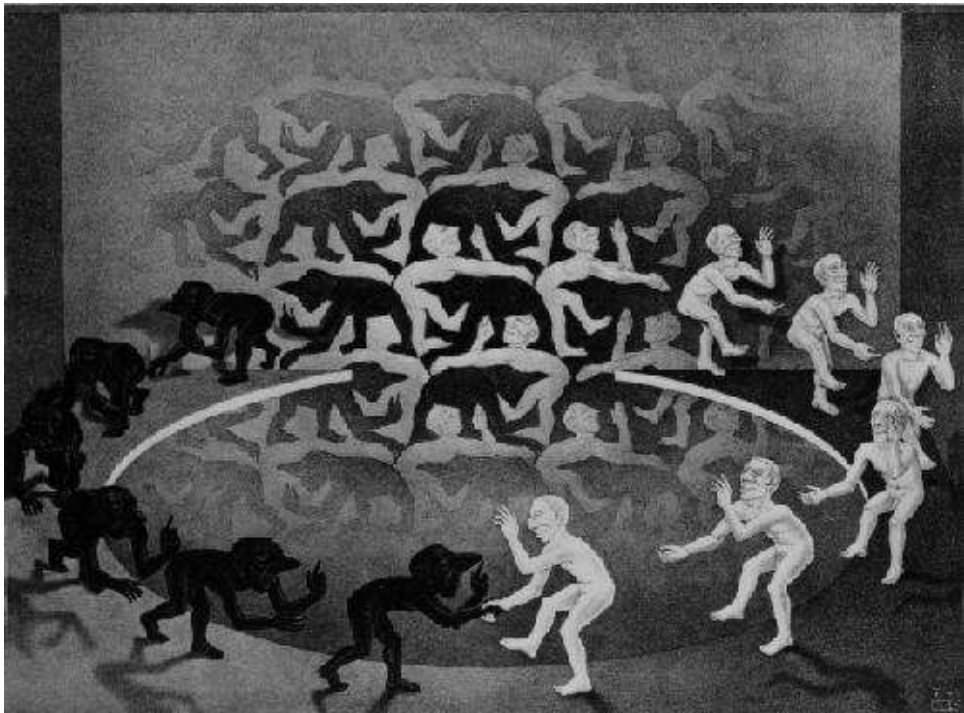
- Digitální pseudonym – řetězec bitů, který je
  - unikátní jako ID (s velmi velkou pravděpodobností) a
  - použitelný pro autentizaci jeho vlastníka a předmětů zájmu (např. odeslaných zpráv)

Poznámky k pseudonymitě

- Anonymita a prokazatelná zodpovědnost (accountability) jsou dva extrémy
- V praxi obvykle vhodná pseudonymita
  - Ovlivňuje spojitelnost mezi předměty zájmu a uživateli
- Opakované použití pseudonymu může uživateli umožnit ustavení reputace (důvěryhodnosti)
- Uživatelé používají větší počet pseudonymů
  - Odhalují spojitost mezi nimi jen v případě potřeby (zisku výhod, času, peněz...)

Agenda

- Úvod, terminologie, základní problémy
- Autentizace v počítačových systémech
- Hesla a PINy
- Tokeny
- Biometriky



3 zásadní pojmy

- ***Autentizace*** – proces ověření (a tím i ustavení) identity (s požadovanou mírou záruky).
- ***Identifikace*** – rozpoznání určité entity (systémem) v dané množině entit.
- ***Autorizace*** – udělení určitých práv a určení povolených aktivit.

Authentizace v časech kritických…

- *Gileád dobyl na Efrajimovi jordánské brody. Když nyní řekl někdo z efrajimských uprchlíků: „Rád bych se přebrodil," zeptali se ho gileádští muži: „Jsi Efratejec?" Jestliže odvětil: „Nejsem," vyzvali ho: „Tak řekni šibbolet! On však řekl: „Sibbolet a nedokázal to přesně vyslovit. Tu ho popadli a zabili při jordánských brodech. Toho času padlo z Efrajima čtyřicet dva tisíce mužů. (Soudců 12:5-6)*
- Automatizované systémy rozeznávání (Identify Friend or Foe) jsou důležitější než v historii
- Systémy (zbraně) dnes 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)

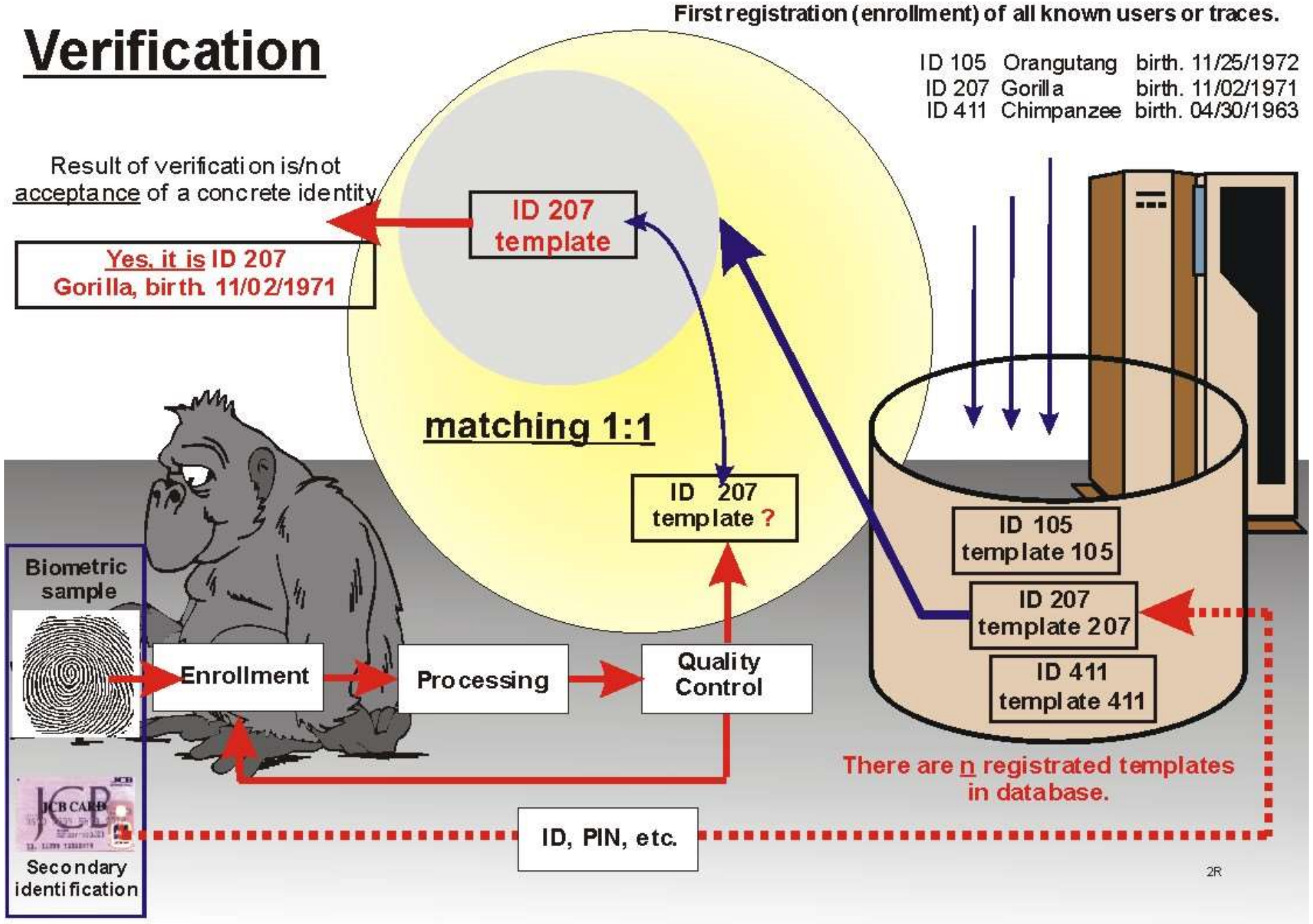
Metody autentizace osob

- Znalost nějakého tajemství
  - PIN kreditní karty
  - Heslo pro telefonního bankéře
- Fyzická vlastnost (biometrika)
  - Otisk prstu
  - Sítnice oka
  - Hlas
- Držení určitého předmětu
  - Čipová karta
  - Telefon

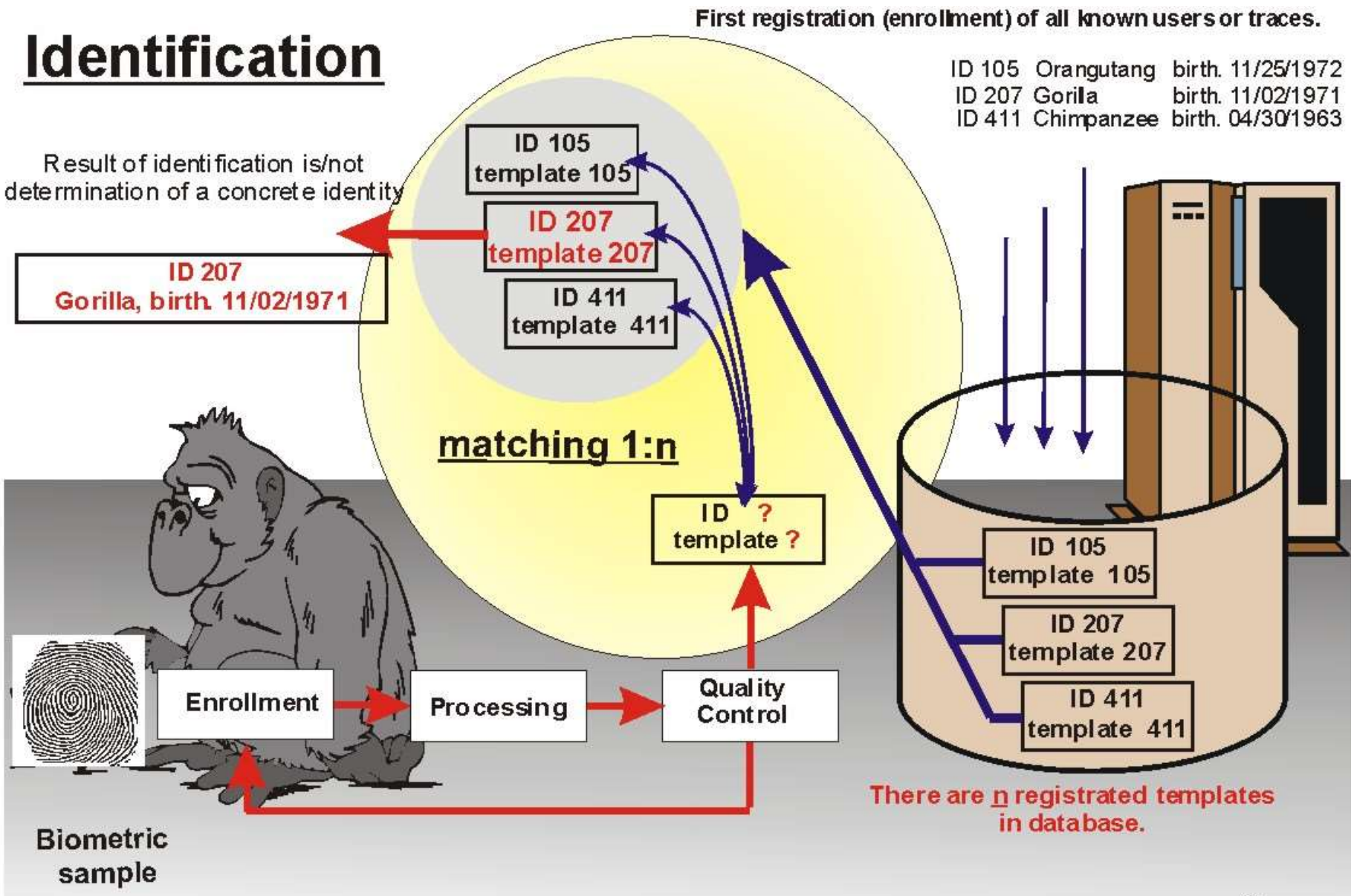
Autentizace a identifikace uživatele

- *Autentizace (verifikace)* – subjekt předkládá tvrzení o své identitě – 1:1
- *Identifikace* (*vyhledání*) – subjekt identitu nepředkládá. Systém prochází všechny (relevantní) záznamy v databázi, aby našel patřičnou shodu a identitu subjektu sám rozpoznal – 1:n
- Následující ilustrace od Romana Raka...

Verification

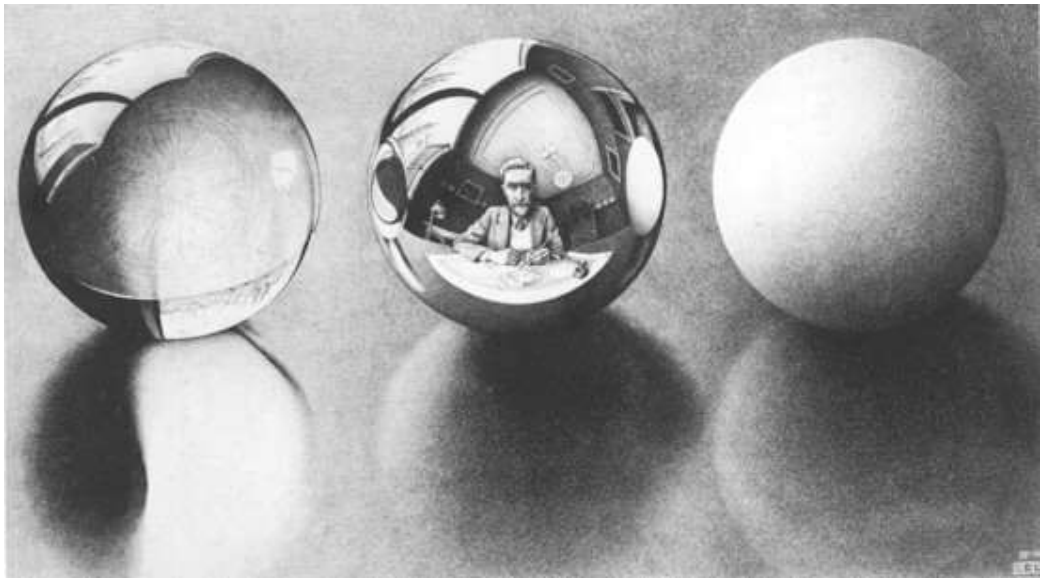


Identification



Agenda

- Úvod, terminologie, základní problémy
- Autentizace v počítačových systémech
- Hesla a PINy
- Tokeny
- Biometriky



Hesla, PINy ap.

- Cílem je autentizace (ověření identity) uživatele
  - Co nejjednodušeji pro autorizované uživatele
  - Co nejkomplikovaněji pro neautorizované uživatele
- V návaznosti pak nastupuje řízení přístupu
- Je potřeba řešit otázky
  - ukládání,
  - průběhu kontroly,
  - „kvality“ hesel a PINů.

Autentizace tajnou informací

- Aby autentizace tajnou informací byla bezpečná je nutné dodržet
  - informace musí být opravdu tajná, tj. nikdo jiný než oprávněný uživatel by ji neměl znát
    - Ne jméno psa, jména rodičů, datum narození, adresa…
  - autentizační informace by měla být vybrána z velkého prostoru možných hodnot
    - Ne jednopísmenné heslo…
  - pravděpodobnost všech hodnot z prostoru by měla být pokud možno stejná
  - pokud dojde ke kompromitaci autentizační informace, musí být možné nastavit novou jinou autentizační informaci

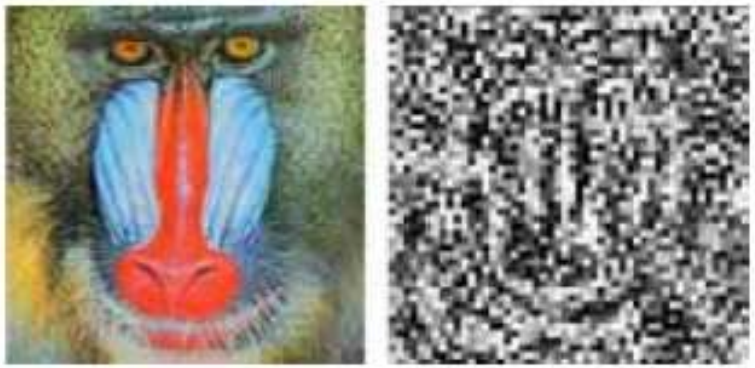
Tajné informace

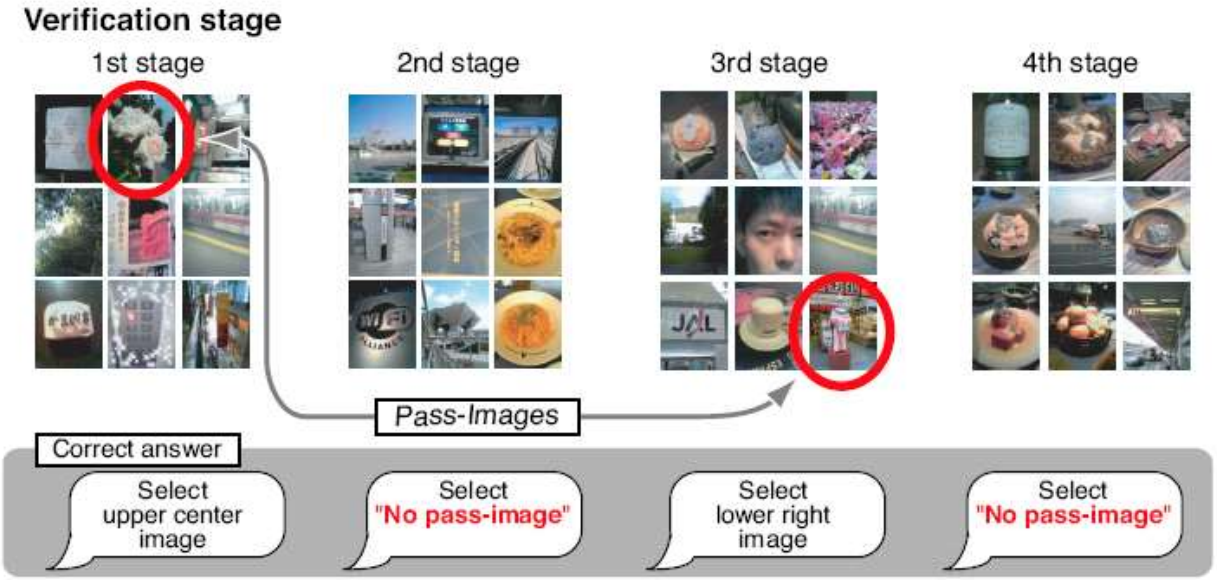
- Klasicky si představíme textové informace
  - PIN
  - hesla
  - passphrase
- Existují ale i alternativní systémy
  - např. identifikace obrazové informace
- Kombinace s biometrickými systémy
  - uživatel si pomyslí heslo, měříme aktivitu mozku

Autentizace obrazovou informací (1)

- Vybírá se jeden obrázek z několika možných
  - např. konkrétní fixní/smluvený obrázek – to je obdobou textového hesla, ale lidé si lépe pamatují vizuální informaci než textová hesla
    - lze snadno odkoukat správný obrázek
  - např. je smluven konkrétní fixní obrázek jako autentizační informace, ale při autentizaci se neukáže přímo tento obrázek, ale jen něho značně znehodnocená (rastrovaná černobílá) verze (všechny nabízené obrázky jsou takové)
    - obdobné jako výše, ale pro útočníka neznajícího původní obrázek je obtížné zapamatovat si degradovaný snímek
  - např. autentizační informací je skupina obrázků, uživateli je představena řada nejrůznějších obrázků a ten musí identifikovat obrázky ze své skupiny (systém Déjà Vu)
    - jedno odkoukání nestačí

Autentizace obrazovou informací (2)





Odlišení člověka od počítače (CAPTCHA)

- Neautentizuje konkrétního člověka, ale odlišuje člověka od počítače
- Obvykle založeno na zpracování (rozpoznání) vizuálních informací
- Používá se proti hromadnému zneužívání služeb automatizovanými programy
- Reálně není obtížné obejít automatizovanými postupy (SW)
- Pokusy s audiem aj. zatím s nezajímavými výsledky (bezpečnost a někdy i použitelnost)

Hesla — Dilema

- **Lidská paměť** (co nejkratší / nejjednodušší)
  - zapamatování

versus

- **Bezpečnost** (co nejdelší / nejsložitější)
  - uhodnutí / odpozorování ap.

Hesla

1. Skupinová (uživatelská *role*) – málo používané, bezpečnost mizivá
2. Unikátní pro danou osobu (heslo = userid)
3. *Neunikátní (používaná společně s userid)*
4. Jednorázová (ať už unikátní či nikoliv)
   - Obvykle tajná funkce/souvislost
   - Na papíře nebo pomocí speciálního zařízení

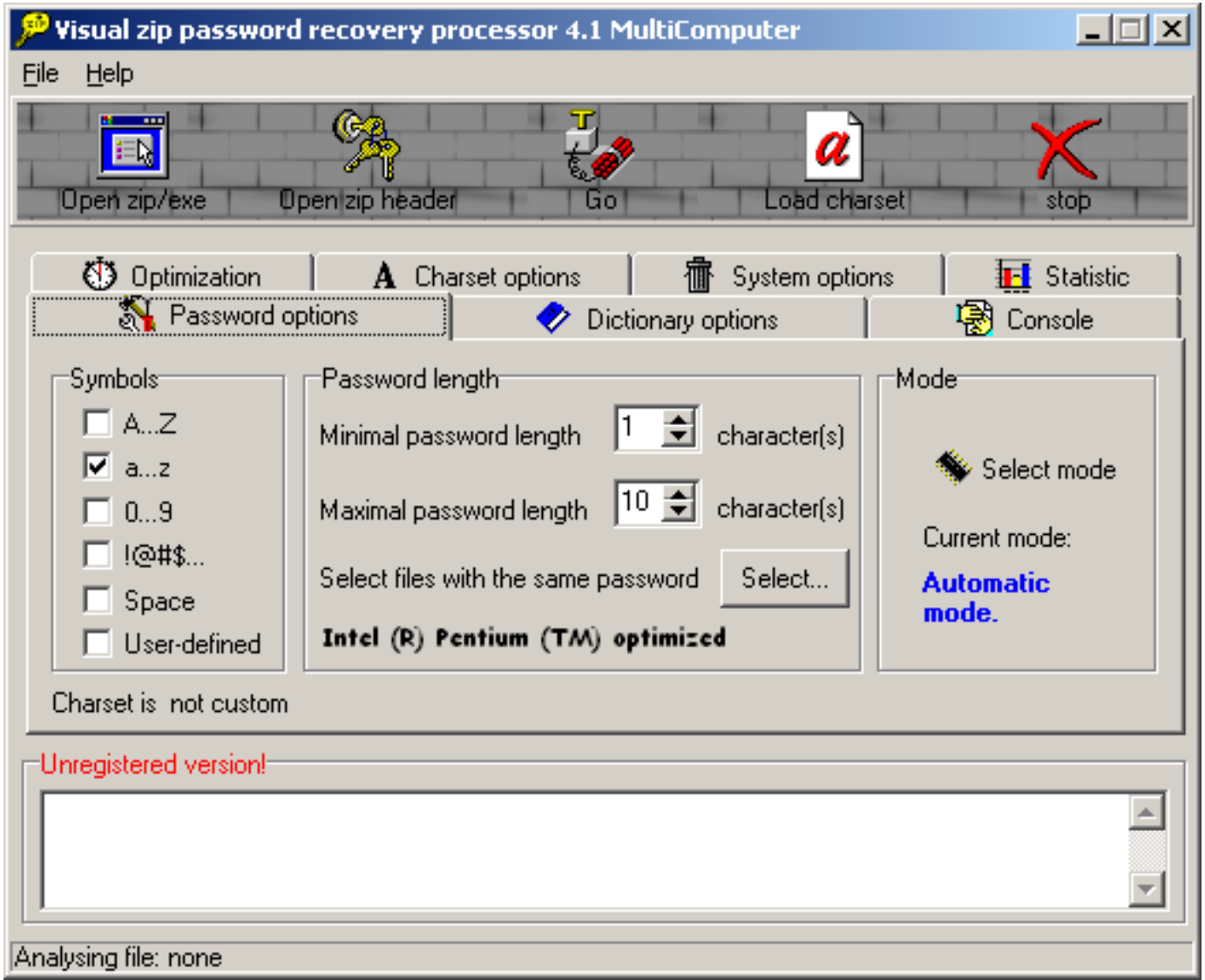
Úspěšnost útoku hrubou silou

$$\frac{\textit{Čas platnosti} \times \textit{Počet odhadů za jednotku času}}{\textit{Velikost abecedy}^{\textit{Délka hesla}}}$$

Čas potřebný k analýze NTLM hašů (na běžném počítači)

n↓ c→	26 znaků	36 (alfan.)	62 (a/A,alfan)	95 (kláves.)
5	15 s	1,3 min	19,9 min	2,8 h
6	6,69 min	47,2 min	20,5 h	11 d
7	3 h	1,2 d	55 d	3,1 r
8	3,26 d	44 d	9,6 r	290 r
9	84,8 d	4,5 r	590 r	28000 r
10	7,1 r	180 r	42000 r	3000000 r

Lámání hesel v praxi



Problémy při vyžadovaných změnách hesel

- MojeHeslo09 v září a MojeHeslo10 v říjnu
- Jiné než předchozí – uživatelé zjistí délku záznamu historie hesel a „vyčerpají“ ho: Heslo123 → qwre321 → jr7*&d → Heslo123
- Zákaz změn po nějakou dobu má za následek problém v případě prozrazení hesla

Vhodná hesla

- Lehce zapamatovatelné, obtížně uhodnutelné!

- Heslo založené na delší (lehce, s nějakou pomůckou, zapamatovatelné) frázi
  - *psmVTCOo24Z* = Polámal Se Mraveneček, Ví To Celá Obora, O Půlnoci Zavolali

J. Yan a kol. – práce s hesly

- University of Cambridge Computer Laboratory Technical Report No. 500
- *The memorability and security of passwords – some empirical results*

Pokusní králíci (vědomě)

- 400 studentů prvního ročníku (přírodověd.)
- *Nezainteresovaná skupina* – jediná neprošla školením
- *Kontrolní skupina* – heslo s alespoň 8 znaky a jedním nealfabetickým
- *Náhodná skupina* – náhodné heslo (A-Z, 1-9)
- *Skupina vstupní fráze* – heslo založené na delší (lehce zapamatovatelné) frázi

Provedené útoky na uložená hesla

- Slovníkový
- Permutační – na základě slovníkového, permutace s 0-3 číslicemi a záměnami (I – 1, S – 5 ap.)
- Uživatelské informace (userid, jméno atd.)
- Hrubou silou (do 6 znaků)

Výsledky útoků

- *Nezainteresovaná skupina* – 33 % a 2 hrubou silou
- *Kontrolní skupina* – 32 % a 3 hrubou silou
- *Náhodná skupina* – 8 % a 3 hrubou silou
- *Skupina vstupní fráze* – 6 % a 3 hrubou silou

Dále…

- E-mailový průzkum mezi uživateli
  - Obtížnost na zapamatování
  - Jak dlouho měli na papíru psanou kopii hesla
- Záznam o resetu hesla administrátory pro zapomenutá hesla

Závěry

- Náhodně vybraná hesla se obtížně pamatují
- Hesla založená na frázích jsou obtížněji uhodnutelná než naivně zvolená hesla
- Náhodná hesla nejsou lepší než ta založená na frázích
- Hesla založená na frázích se nepamatují hůře než naivně zvolená hesla
- Školení uživatelů nemá za následek výrazný posun v bezpečnosti hesel

Doporučení

1. Používat fráze
2. Myslet na délku
   - Unix a Windows (kde a≠A) minimálně 8 znaků
3. Používat nealfabetické znaky
4. Prosazovat danou politiku volby hesel nějakým mechanismem, jinak alespoň 10 % hesel bude slabých

PIN (Personal Identification Number)

- Levnější klávesnice
- Obtížněji zapamatovatelné než hesla
- Obvykle používány s fyzickým předmětem
- Někdy lze změnit podle přání zákazníka
- Obvykle 4-8 znaků dlouhé
- Procedurální omezení proti útokům hrubou silou
  - Zabavení karty při několika (3) nesprávných PINech
  - Nutnost re-aktivace záložním (delším) PINem po několika nesprávných PINech

PIN-paráda

Analýza 3,4 milionu PINů

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 stištění kláves
  - V praxi závisí na okolní teplotě

- PIN lze odpozorovat při zadávání u bankomatu, obchodního terminálu, …

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

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… ☺

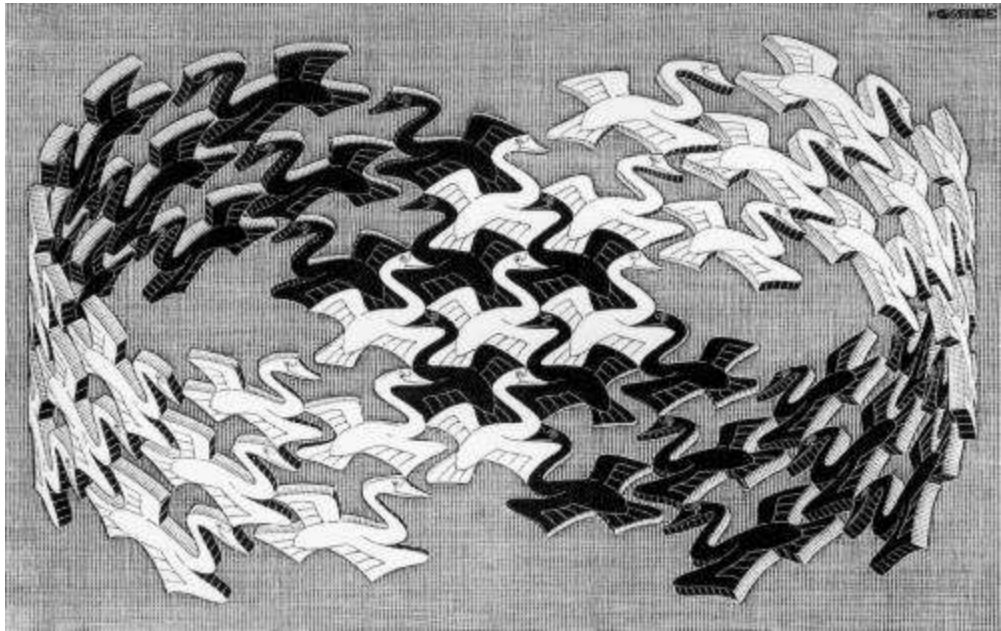
„Okrajové“ postřehy

- Útočníkova 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)

Agenda

- Úvod, terminologie, základní problémy
- Autentizace v počítačových systémech
- Hesla a PINy
- Tokeny
- Biometriky



Metody autentizace uživatele

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

- Třífaktorová autentizace
  - Token – čipová karta
  - PIN / heslo
  - Biometrika (např. načtená a zpracovaná přímo tokenem)

Token / Předmět

- *Něco, co uživatel má...*

- Předmět, token

- Token (angl.)
  - Projev, znamení, upomínka, památka
  - Známka pravosti
  - *By the token...* Na důkaz toho
  - *Token money...* Bankovky kryté zlatem

Z historie

- Amulet
- Pečeť
- Bankovka se specifickým číslem nebo specificky roztržená bankovka

- Klíč!
- Peníze

Tokeny

- Jako u tajných informací je cílem autentizace (ověření identity) uživatele
  - co nejsnáze pro autorizované uživatele;
  - co nejkomplikovaněji pro neautorizované uživatele.
- Je potřeba řešit mj. otázky
  - obtížnosti vytvoření a kopírování,
  - průběhu kontroly,
  - práce s tokeny v „neočekávaných případech“,
    - např. co se má stát, je-li karta vyjmuta ze čtečky.

Dilema

- **Cena výroby** jednoho kusu při výrobě mnohakusové série (co nejmenší cena)

versus

- **Cena padělání** jednoho kusu za účelem vniknutí do systému (co největší cena)
  - Přestává platit v případech, kdy se vyplatí produkce mnohakusové série (padělků)

Cena výroby

- Ekonomická „klasika“
- V přepočtu na kus klesá při výrobě větších sérií
  - Může být důležité pro uživatele prvních sérií, kdy následně cena výroby klesá a tím i bariéra pro ty, kdo zvažují padělání

Cena padělání

- Platí to, co pro cenu výroby, ale navíc
  - Je důležité to, zda (potenciální) útočník získá stejně výrobou jednoho nebo více padělků či nikoliv – motivace útočníka
  - Jak dlouho (a případně kolik) musí mít k dispozici původní(ch) token(ů)
  - Zda existuje legislativní postih padělání jako takového (bez ohledu na útok na systém)

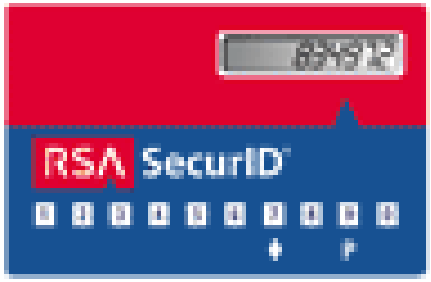
Další omezení

- Prevence
  - Dostupnost vybavení
  - Modifikace běžně dostupného vybavení, např. barevné kopírky
    - Nekopírují přesně určité barvy
    - Také vnášejí svůj identifikátor do obrazu
  - Kontrola a licence živností atd.
- Utajení určitých informací (k používání nebo vlastní konstrukci tokenu)

Nejčastější tokeny v IT/IS

- Karty
  - S magnetickým proužkem
  - Čipové
    - Kontaktní / bezkontaktní
    - Čtečka na straně dotazovatele / kontrolovaného (mobil)

- Autentizační kalkulátory
  - S tajnou informací
  - S hodinami
  - Způsob vstupu/výstupu



Čipové karty

- Co umí?
  - Paměťové (*chipcard*)
  - Paměťové se speciální logikou (ochrana PINem, čítače atd.)
  - Procesorové (*smartcard*)
- Jak s nimi komunikovat?
  - Kontaktní – nutný kontakt se čtečkou (zdroj energie)
  - Bezkontaktní
    - Operace mohou být prováděny bez vědomí uživatele
    - Vhodné pro fyzickou kontrolu přístupu ap.
    - Omezený zdroj energie => procesory s extremně nízkou spotřebou => nižší výkon a omezená funkčnost
    - Existují i bezkontaktní Javakarty
    - Elektronické pasy jsou výkonné bezkontaktní karty

Podoby čipové karty

- Obvyklá karta – bankomatová ap.

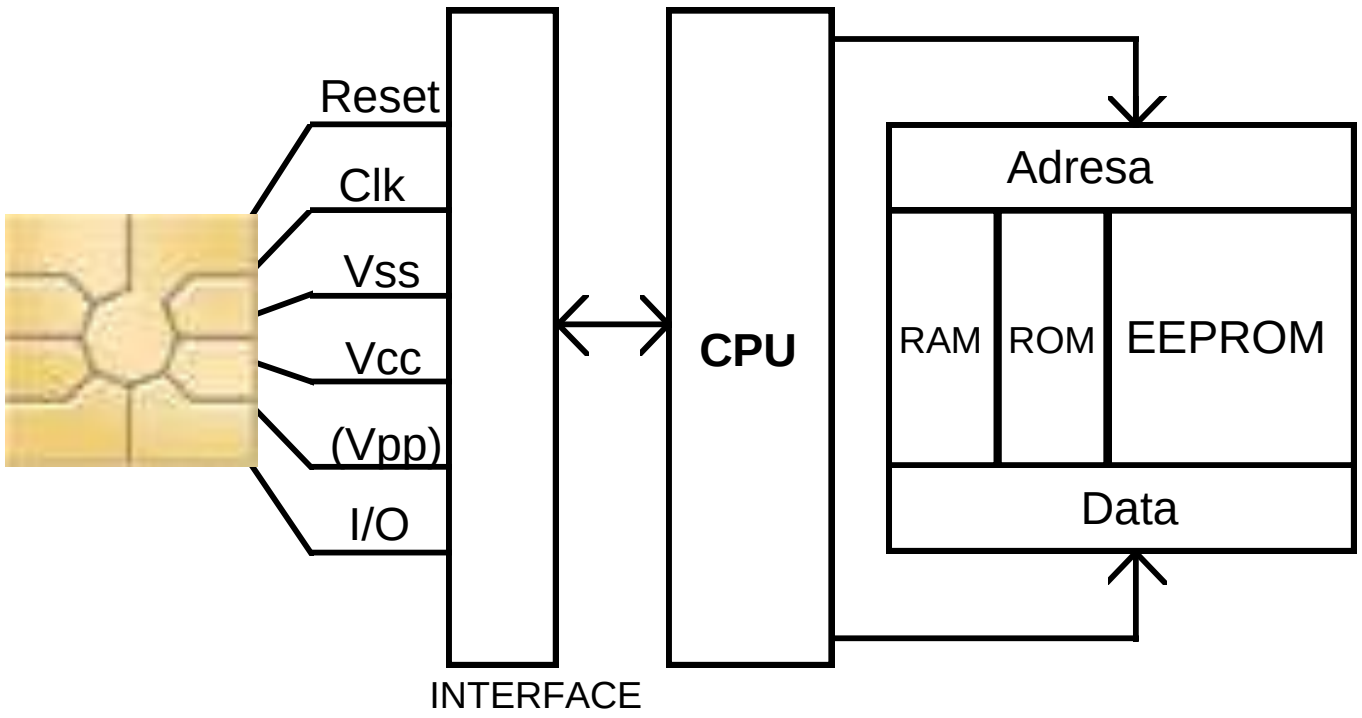
- SIM karta (telefony GSM)
- USB token

Čipová karta s procesorem

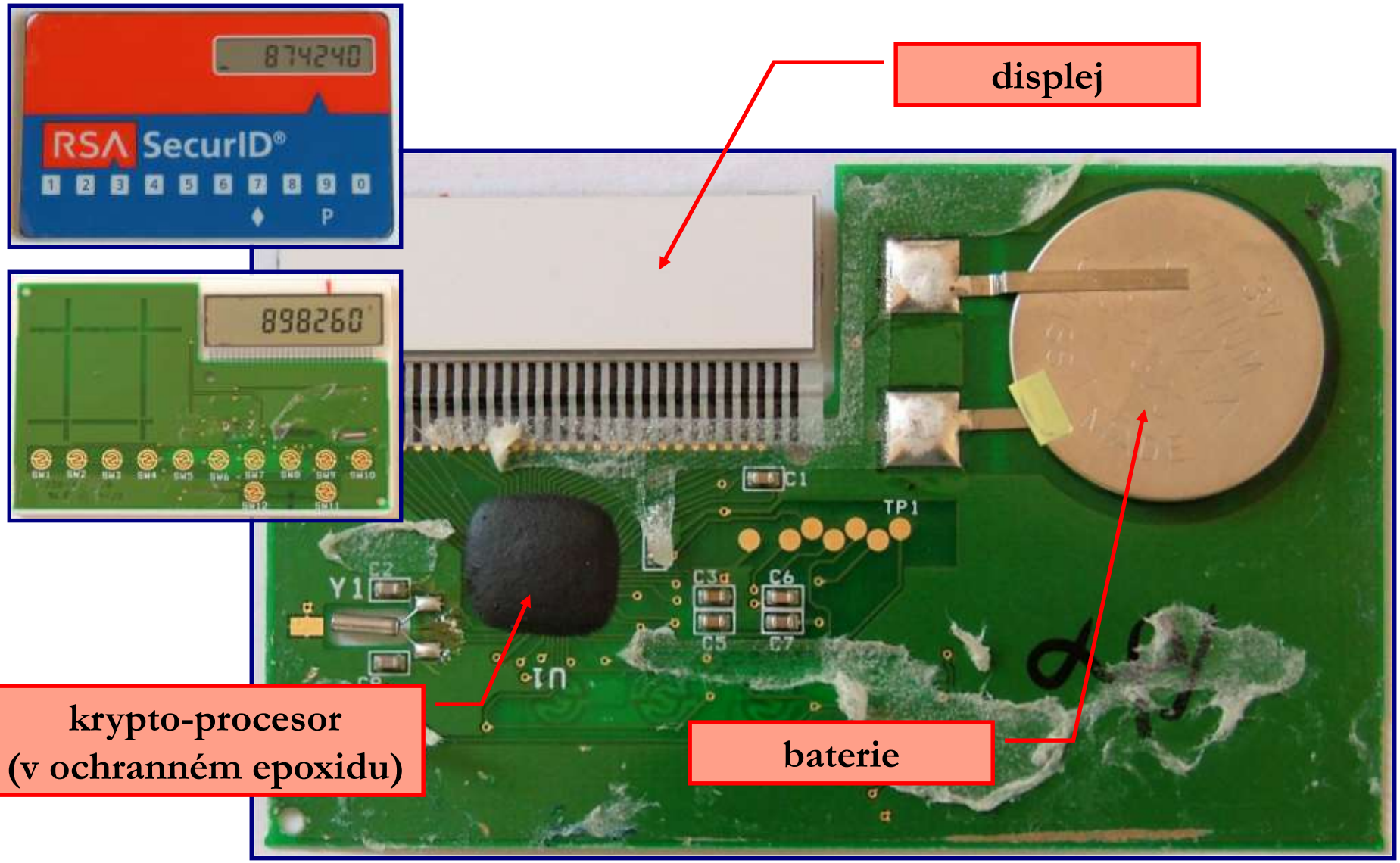
- Dále jen „čipová karta“
- A samozřejmě i s pamětí
  - RAM (Random Access Memory) – x KB
  - ROM (Read Only Memory) – x.10-10^2 KB – OS ap.
  - EEPROM (Electrically Erasable Programmable Read Only Memory) – x.10 KB

- Různá složitost výpočtů, ideálně i náročné kryptografické operace

Kontaktní procesorová čipová karta

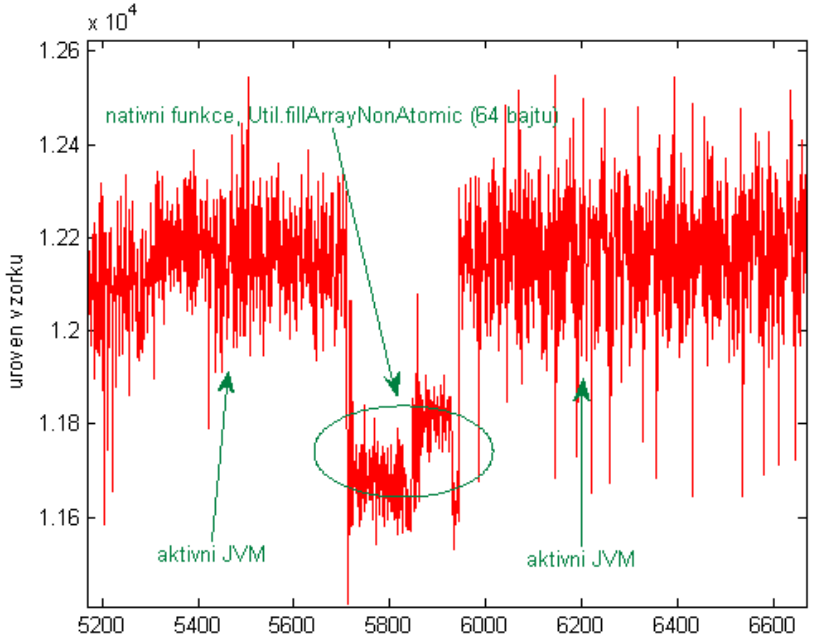


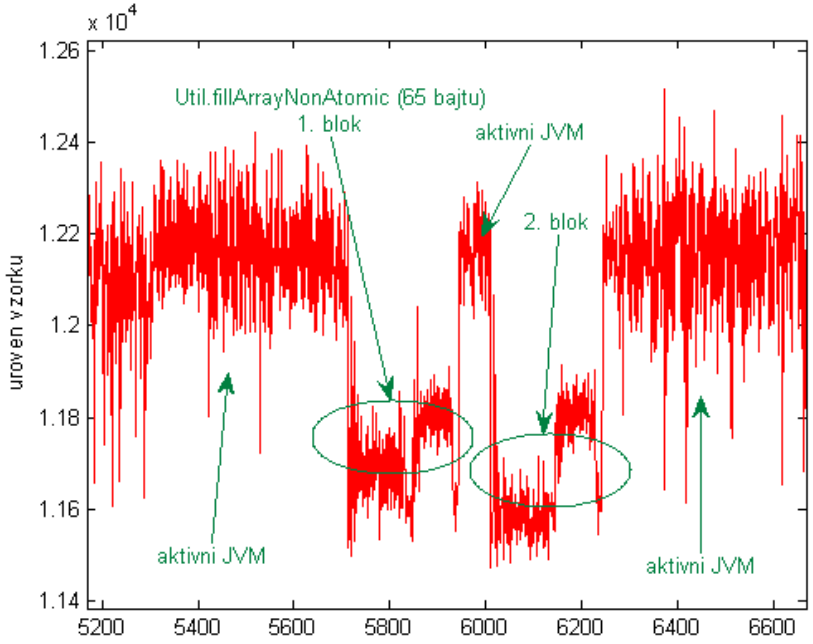
RSA SecurID – odstranění krytu



Příklad časové analýzy

- Velikost pole zapisovaného do paměti
  - karta zapisuje po 64 bajtech
  - výrazný rozdíl mezi zápisem 64 a 65 bajtů (trvá déle)

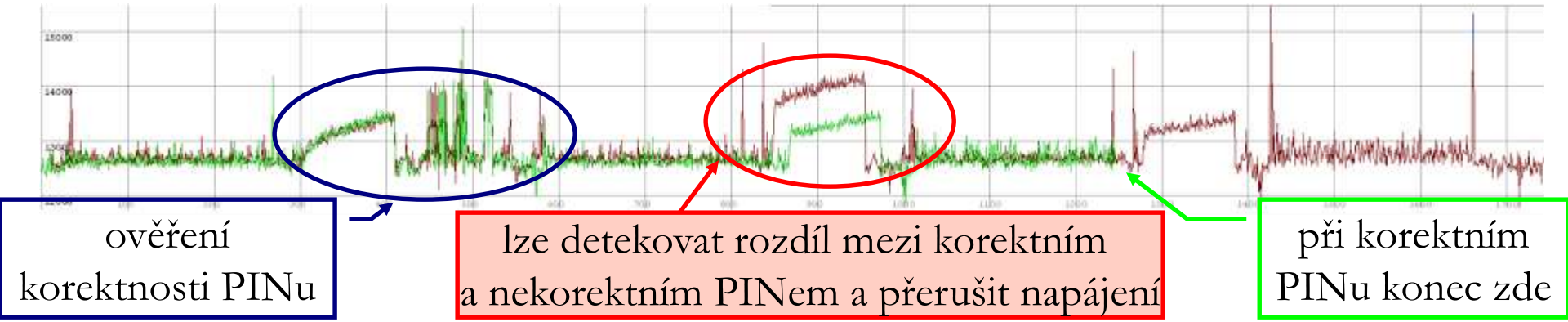




Příklad SPA: verifikace PINu

- sniž čítač-ověř-[zvyš čítač]

- zranitelná implementace: ověř-[zvyš/sniž čítač]

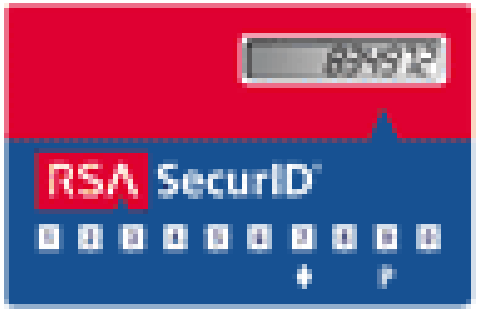


Indukce chyb během výpočtu

- Cílem útoku je pomocí náhlých změn operačních podmínek vyvolat změnu hodnoty v paměti, registru apod.
- Záměrem je obejít určitou instrukci či změnit data v registrech či na sběrnici.
- Lze takto obejít správnou autentizaci, kontrolu přístupových práv, modifikovat počet cyklů algoritmu.
- Mezi ovlivnitelné prvky okolí patří např.:
  - napájecí napětí
  - hodinový signál, reset signál
  - elektrické pole
  - teplota

Autentizační kalkulátory

- Obvykle využívají protokol výzva-odpověď
  - Odpověď je funkcí tajné informace – klíče a výzvy
- Přenos informací (vstup / výstup)
  - Manuální (klávesnice, displej)
  - Automatický (optika, čárový kód, infrared)
- PIN – standardní (někdy i nouzový)



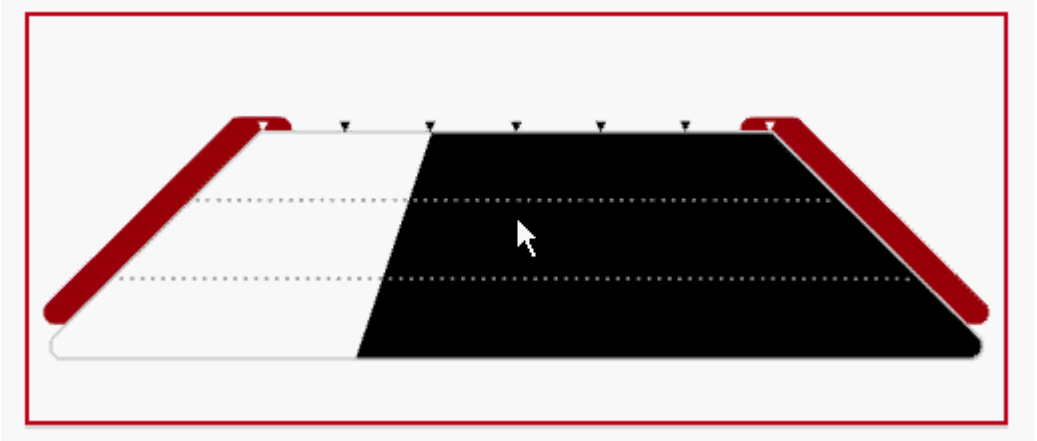
Příklad: Autorizace bankovní transakce

- Příklad reálného využití AK
- Nutnost přepisu řady údajů do kalkulátoru

- **Postup pro vygenerování autentizačního čísla z kalkulátoru:**
  - Zapněte kalkulátor, zadejte Váš PIN, který jste si zvolili pro používání autentizačního kalkulátoru.
  - Stiskněte na autentizačním kalkulátoru tlačítko Enter.
  - Stiskněte dvakrát tlačítko S (na displeji se objeví položka "Platba") a stiskněte Enter.
  - Zadejte částku v měně transakce bez haléřů a stiskněte Enter.
  - Zadejte předčíslí čísla účtu příjemce (pokud není předčíslí definováno zadejte 0) a stiskněte Enter.
  - Zadejte číslo účtu příjemce a stiskněte Enter.
  - Zadejte kód banky příjemce a stiskněte Enter.
- **V tuto chvíli došlo k vygenerování desetimístného autentizačního čísla, které zadejte do pole "Autentizační kód". Po zadání tohoto autentizačního kódu můžete transakci odeslat ke zpracování do banky.**

Příklad: Autentizační kalkulátor

- Autentizační kalkukátor může být uživatelsky přívětivý
  - Autentizace biometrikou
  - Snímač flicker kódu z obrazovky



Tokeny založené na hodinách

- Bývají součástí autentizačních kalkulátorů
  - Ale ne vždy – viz nejrozšířenější RSA SecurID
- V daném okamžiku dávají správnou hodnotu
  - Jedinečnou pro daný přístroj
  - Platnou pouze po určitou dobu (časový rámec)
  - Tuto hodnotu umí spočítat i autentizační server
- Je potřeba řešit otázku ztráty synchronizace hodin
  - Otázka platnosti časových rámců před a po
  - Záznam v čítači na serveru

Příklad – bezkontaktní karta

- Autentizace bývá obvykle založena pouze na ověření sériového čísla karty (to karta na požádání sdělí)
  - Bezpečnost staví na obtížnosti výroby karty (zařízení) se stejnou funkčností
  - Pozor – zařízení útočníka nemusí být nutně stejně velké jako původní karta!

Demonstrace útoků

Problém nedůvěryhodného terminálu – selhání autentizace

- buď neautorizovaným přenosem signálu

- 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)

Obecné výhody tokenů

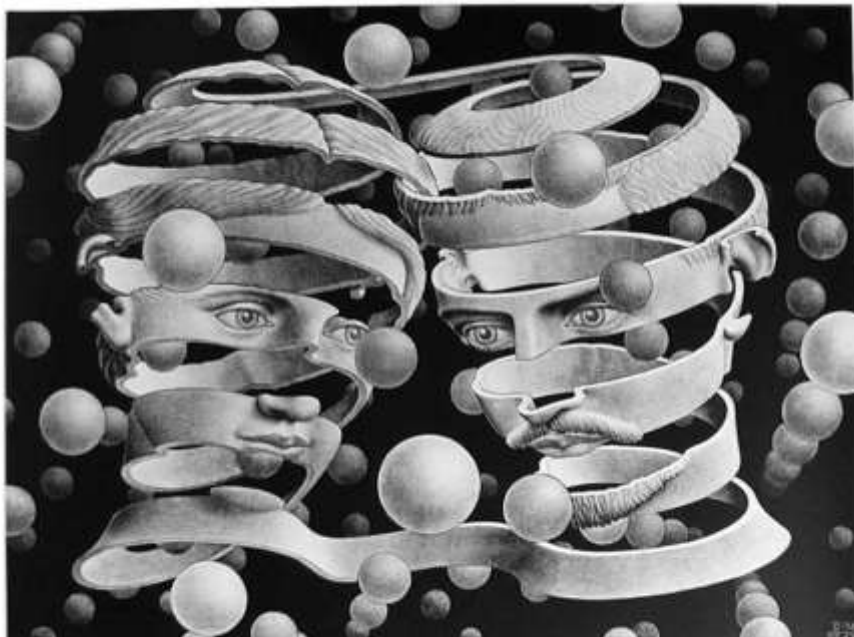
- Rychle se zjistí jejich ztráta
- Nejsou jednoduše kopírovatelné
- Tokeny samy o sobě mohou být schopny zpracovávat nebo přenášet další informace

Obecné nevýhody tokenů

- Ke kontrole je potřeba obvykle speciální čtečka, zařízení nebo vycvičená osoba
- Bez tokenu není autorizovaný uživatel rozeznán
- Token musí být dostatečně složitý, aby se zvýšila obtížnost kopírování
- Může se polámat, přestat fungovat, což nemusí být vždy jednoduše detekovatelné uživatelem

Agenda

- Úvod, terminologie, základní problémy
- Autentizace v počítačových systémech
- Hesla a PINy
- Tokeny
- Biometriky



Biometrické metody

- Biometriky – *biologické* charakteristiky, které jsou měřitelné *automatizovanými* metodami

- Fyziologické charakteristiky (ruka, oko, tvář atd.)
- Behaviorální charakteristiky (dynamika podpisu, hlas atd.)

Základní biometrické techniky

- Otisk prstu

- Vzor oční duhovky

- Vzor oční sítnice

- Srovnání obličeje

- Geometrie ruky

- Verifikace hlasu

- Dynamika podpisu

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}

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).

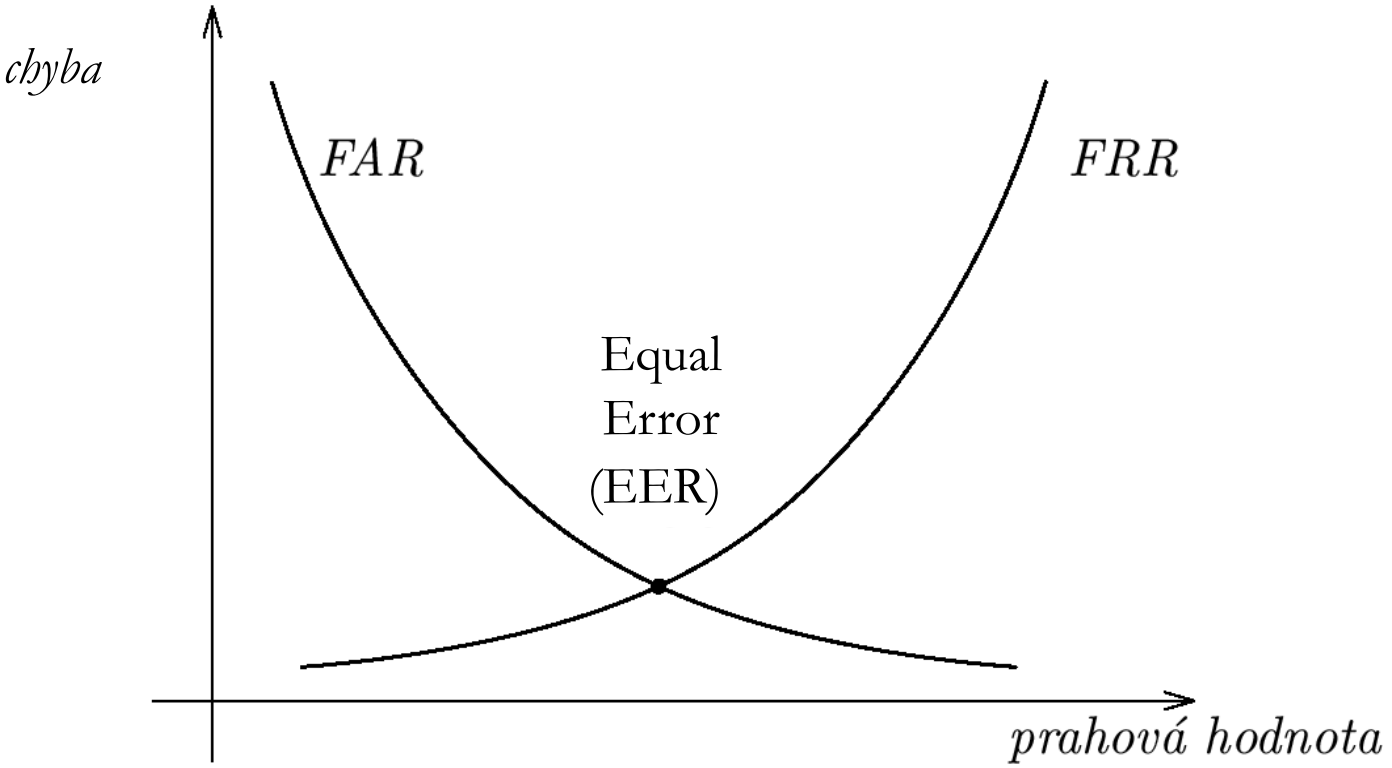
(a) Live Finger (b) Gummy Finger

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

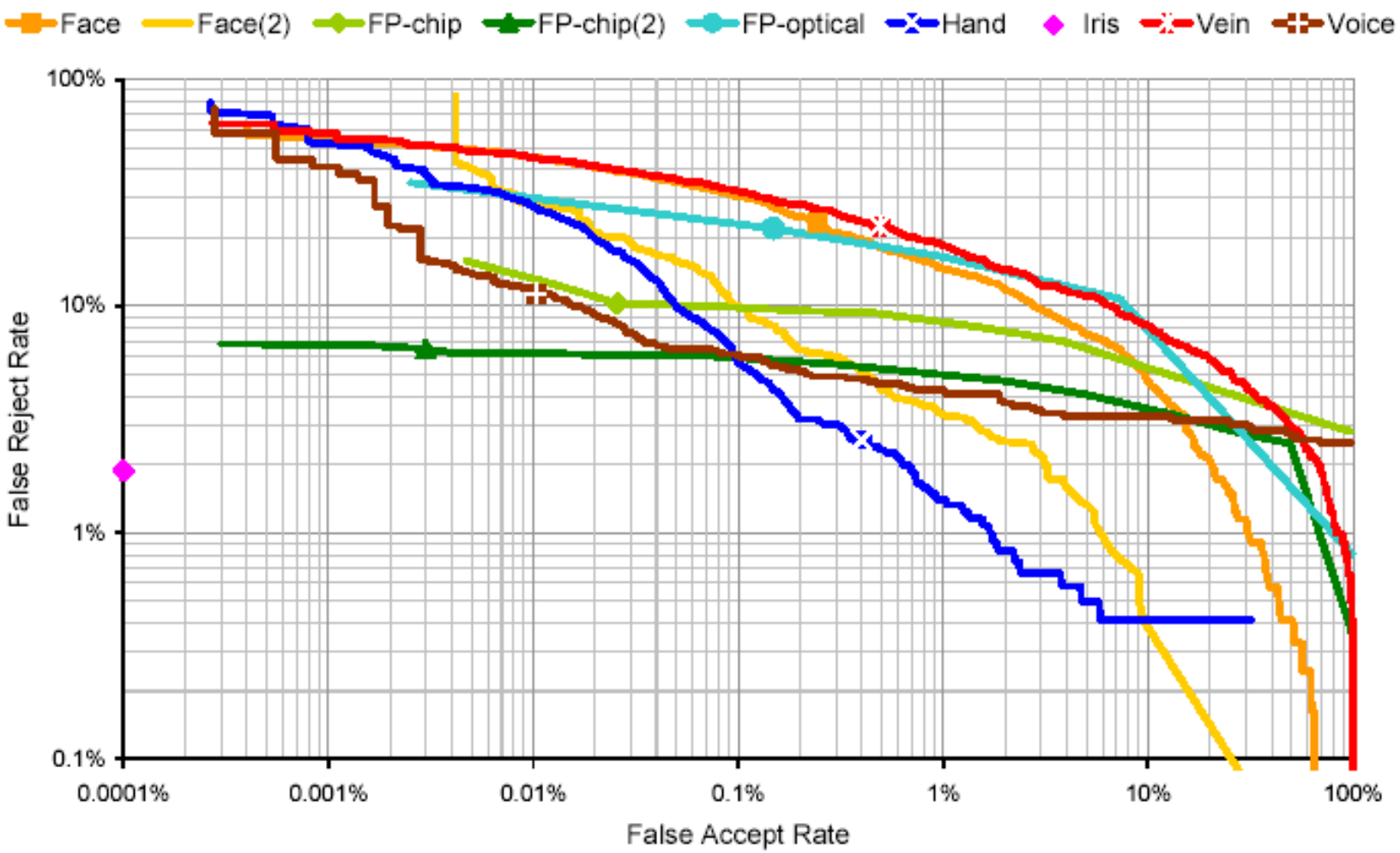
- Nesprávné přijetí (false acceptance)
- Nesprávné odmítnutí (false rejection)



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

Chyby biometrických systémů

- Receiver operating curve (ROC) – NPL 2001



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

- 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

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

Komerční versus forenzní

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

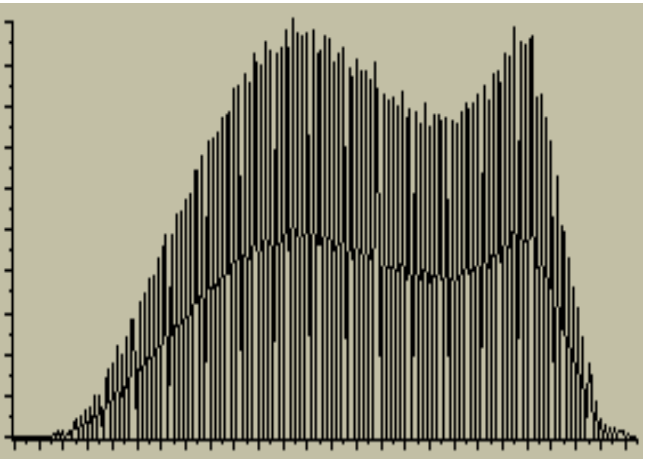
- Vyšší přesnost
- Nutné manuální intervence profesionálů
- Registraci není možné opakovat
- Uchováváme zpracované charakteristiky i původní biometrické vzorky

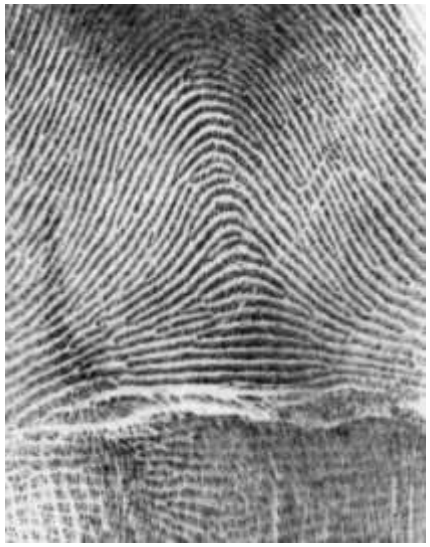
Komerční versus forenzní II.

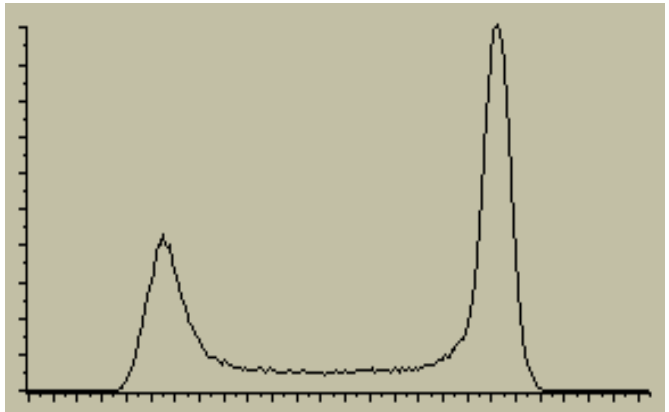
- Výsledek autentizace v sekundách
- Nízká až střední znalost systému nutná (pro používání)
- Miniaturizace
- Cena hraje důležitou roli a je relativně nízká

- 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

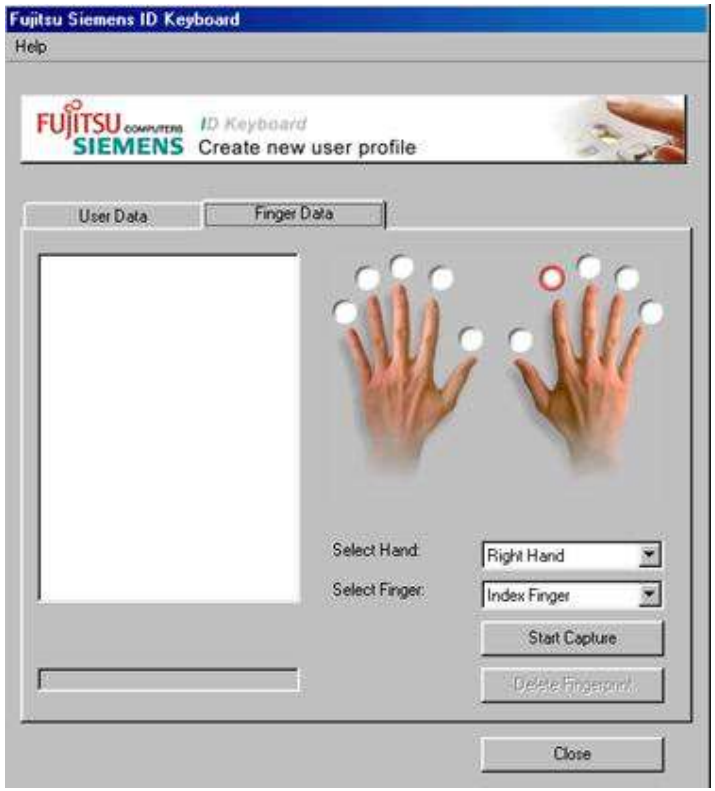






Výhody biometrik

- 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)



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

Otázky?

Vítány!!!

matyas@fi.muni.cz