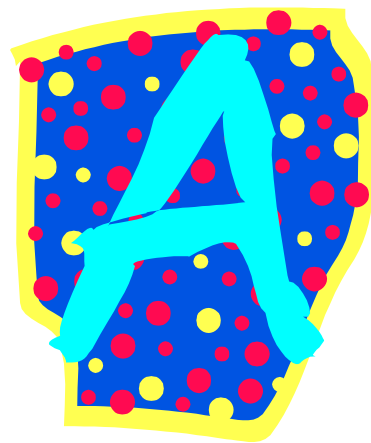


PV157 – Autentizace a řízení přístupu

# Autentizace uživatelů tajnými informacemi



# Hesla, PINy ap.

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

# Dilema

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

versus

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

# Hesla

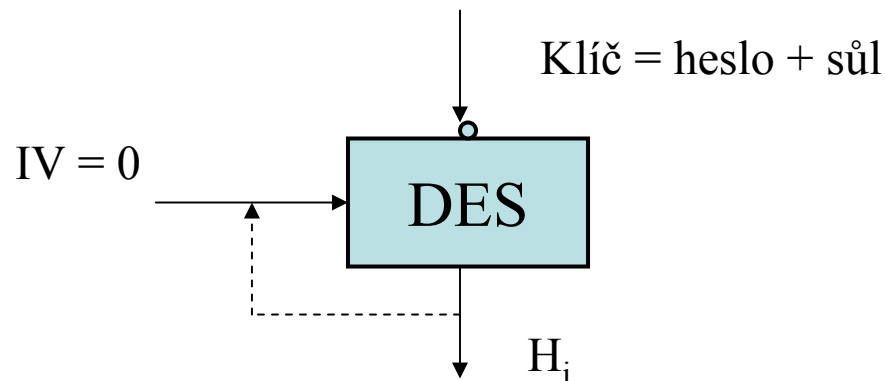
1. Skupinová (uživatelská *role*) – málo používané, bezpečnost mizivá
2. Unikátní pro danou osobu (heslo = userid)
3. *Neunikátní (používaná společně s userid)*
4. Jednorázová (ať už unikátní či nikoliv)
  - Obvykle tajná funkce/souvislost
  - Na papíře nebo pomocí speciálního zařízení

# Ukládání hesel

- V nezašifrované podobě
  - Ochrana na úrovni systému (řízení přístupu pro zápis i čtení!)
  - Absolutní důvěra v administrátora
  - Problém při zkopírování souboru
  - Raději NE
- V nečitelné podobě
  - Šifrované
  - Hašované

# Nečitelná podoba hesel

- Pomalá funkce (1x není problém, opakovaně ano)
- Nedoporučuje se ukládat zašifrovaná sama o sobě
- „Solení“
  - v tabulce hesel:  $\text{userid}$ ,  $s\hat{u}l$ ,  $f(s\hat{u}l, \text{heslo})$
  - delší efektivní heslo, také řešení pro stejná hesla



$H_i$  se použije stejným způsobem vícekrát (25)

# Nečitelná podoba hesel

- V Unixu dříve pomocí funkce crypt, postavená na DES (viz předch. slajd) pro vstup je významných jen prvních 8 znaků (!)
- Nyní s využitím hašování MD5 – významných 256 znaků

# Útoky

- Slovníkový
- Permutace písmen s několika znaky a typickými náhradami
- Slova, data, čísllice související s uživatelem
- Hrubou silou (všechny možné kombinace)



# passwd

squid:\*:23:23::/var/spool/squid:/dev/null

zriha:Cd7KKI2xoP5rs:23568:700:Zdenek Riha:/home/zriha:/bin/bash

- Obsahuje následující informace
  - account – userid
  - password
  - UID – the numerical user ID
  - GID – numerical primary group ID
  - GECOS – This field is optional...
  - directory – the user's \$HOME directory
  - shell – the program to run at login...

# shadow

squid:!!:11724:0:99999:7:::

zriha:\$1\$LxSyKziS\$D6sEAIBU2p3xbzeGqg.LK.:11760:0:99999:7:::134538348

- Obsahuje následující informace
  - Login name
  - Encrypted password
  - Days since Jan 1, 1970 that password was last changed
  - Days before password may be changed
  - Days after which password must be changed
  - Days before password is to expire that user is warned
  - Days after password expires that account is disabled
  - Days since Jan 1, 1970 that account is disabled
  - A reserved field

# Úspěšnost útoku hrubou silou

*Čas platnosti x Počet odhadů za jednotku času*

---

*Velikost abecedy* <sup>*Délka hesla*</sup>

# Čas potřebný k analýze (HAC), crypt na pomalém PC, DES 10 MB/s

n↓	c→	26 znaků	36 (alfan.)	62 (a/A,alfan)	95 (kláves.)
5		0.67 hod	3.4 h	51 h	430 h
6		17 h	120 h	130 dnů	4.7 roku
7		19 d	180 d	22 r	440 r
8		1.3 r	18 r	1.400 r	42.000 r
9		34 r	640 r	86.000 r	4 x 10 <sup>6</sup> r
10		890 r	23.000 r	5.3 x 10 <sup>6</sup> r	3.8 x 10 <sup>8</sup> r

# 1984 – Gramp & Morris

- Systém s min. 6 znaky a jedním nealfabet. znakem
- 20 nejpoužívanějších ženských jmen následovaných číslicí
- Z těchto 200 hesel bylo vždy alespoň jedno v každém z několika desítek zkoumaných systémů

# Lámání hesel

- 1979 – společnost Bell – 86% úspěšnost (!)
- 1990 – DV Klein
  - Analyzoval 13 797 souborů s hesly (Unix)
  - Asi  $\frac{1}{4}$  úspěšnost
- 1993 – ústav Bell-Northern Research 3x %

# 1993 – Zviran & Haga

- 106 studentů
- Výběr jednoho hesla a přidělení jednoho náhodného hesla
- Zapamatovat na 3 měsíce... bez používání(!)
  - Správně zapamatováno 35 % zvolených a 23 % náhodných
  - Poznamenáno 14 % zvolených a 66 % náhodných

# 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

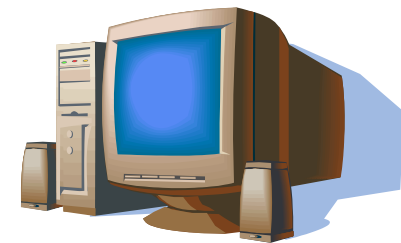
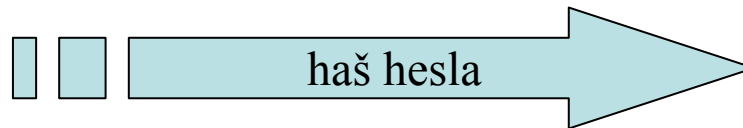
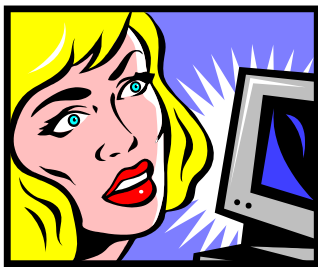


# Vhodná hesla

- Lehce zapamatovatelné, obtížně uhodnutelné!
- Heslo založené na delší (lehce, s nějakou pomůckou, zapamatovatelné) frázi
  - *psmVTCo24Z* = PolámáSe Mraveneček, Ví To  
Celá Obora, O Půlnoci Zavolali

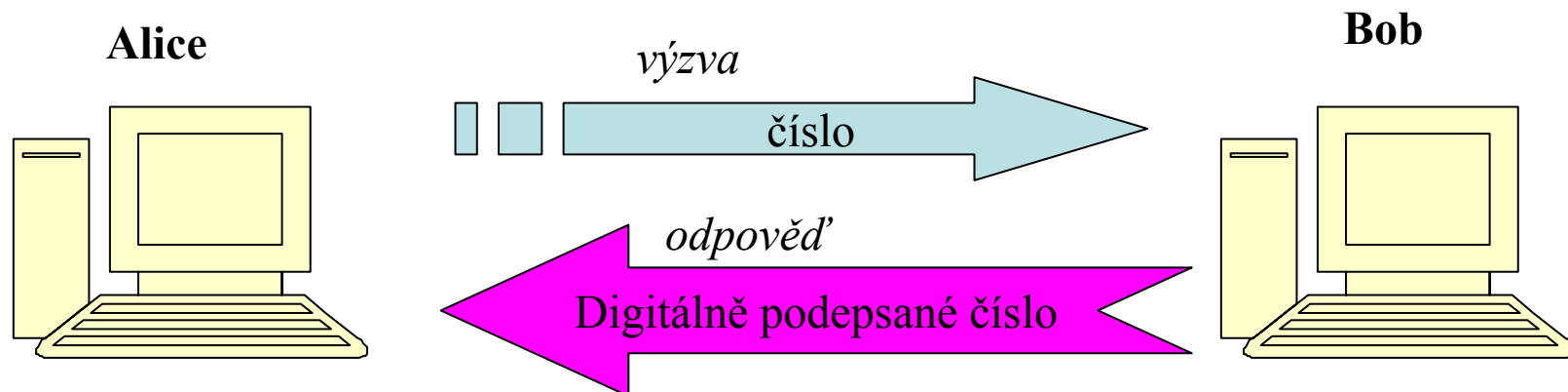
# Komunikace a autentizace heslem

- Heslo v čisté podobě je možné odposlechnout
- Při autentizaci se neposílá heslo samotné, ale pouze haš hesla
  - Kdo odposlechne haš nezíská automaticky heslo
  - Haš však lze použít pro podvodnou autentizaci



# Protokoly výzva-odpověď

- Protokoly typu výzva-odpověď (challenge-response)
  - Odposlechem výzvy i odpovědi útočník moc nezíská
  - Bob se může přesvědčit o identitě Alice, bez získání jejího tajemství



# 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 a bankovní karta

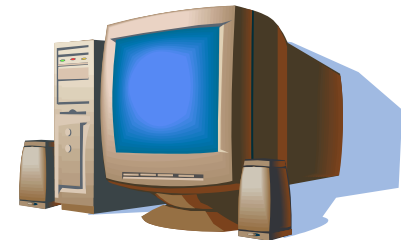
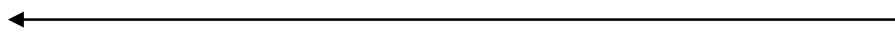
- Oba stejnou cestou, v různé dny
- Osobní převzetí – alespoň jednoho
- Vlastní výběr PINu při převzetí karty
  
- On-line verifikace (off-line se z bezpečnostních důvodů nepoužívá)




Klíčem bankomatu zašifrované číslo účtu, PIN a částka



Zašifrovaná sůl a odpověď A/N



# M. Kuhn – ec-PIN

- Publikoval koncem 90. let pravděpodobný (později potvrzen jako správný) mechanismus pro PINy v systému debetních karet EuroCheque 
- Plnou verzi příspěvku *Probability Theory for Pickpockets – ec-PIN Guessing* lze nalézt na <http://www.cl.cam.ac.uk/~mgk25/ec-pin-prob.pdf>

# PIN ve starém systému ec

- Nastaven bankou, klient si nemůže volit
- Používán německými bankami v letech 1981-1997
- Postaven na využití šifry DES (její malá síla ale není v tomto případě problém ☺ )
- Vstup: část kódu banky, číslo účtu, pořadové číslo karty

# Výpočet PINu – bankomat stejné banky

- Posledních pět číslic kódu banky, číslo účtu a pořadové číslo karty se zřetězí
- Použije se DES s klíčem banky  $K_I$
- Využije se 3. až 5. číslice výstupu
- Hexa (A-F se nahradí 0-5)
- Případná první 0 se nahradí 1



# Výpočet PINu – bankomat jiné banky

- Velmi podobně, jen místo  $K_I$  je společný klíč v systému EuroCheque  $K_{P1}$
- A podobně klíče záložní  $K_{P2}$  a  $K_{P3}$
- Vypočte se samozřejmě jiný PIN (pokud nejsou  $K_{P_x}$  a  $K_I$  shodné 😊 )
- Přidá se offset (součet mod 10), takže je třeba na magn. proužku uložit i 3x offset

# Problémy

- Společné klíče jsou známy všem bankám v systému EuroCheque
- Offsety na kartě dávají velmi cenné informace
- Pro danou kartu a z ní zjištěné informace lze určit PIN s pravděpodobností až 1/105(!)
- Pro jakoukoliv kartu a tři pokusy o zadání PINu lze „uspět“ s pravděpodobností asi 1/150

# Závěr cvičení s ec-PIN

- Úspěch (3 pokusy) s pravděpodobností asi 1/150
- Dobrý systém by měl mít 1/3000
  - Možné PINy 1000-9999 a 3 pokusy
- Daný ec-PINový systém byl horší než dobrý se 3 číslicemi (1/300) ☹

## J. Yan a kol. – práce s hesly

- Publikace ze září 2000 o práci s hesly pozorované na studentech prvního ročníku
- University of Cambridge Computer Laboratory  
Technical Report No. 500
- *The memorability and security of passwords – some empirical results*
- Dostupný na  
<http://www.cl.cam.ac.uk/TechReports/>

# 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

# 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≠A) 8,
  - Netware (a=A) 10
3. Používat nealfabetické znaky
4. Prosazovat danou politiku volby hesel nějakým mechanismem, jinak alespoň 10 % hesel bude slabých

# Otázky?

Vítány!!!

Přístí přednáška je 24. 11. 2004 v 18:00

matyas@fi.muni.cz

zriha@fi.muni.cz