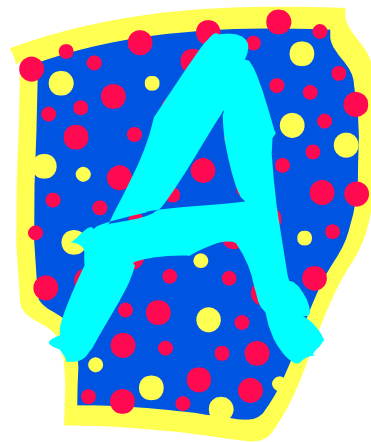


PV157 – Autentizace a řízení přístupu

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.

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

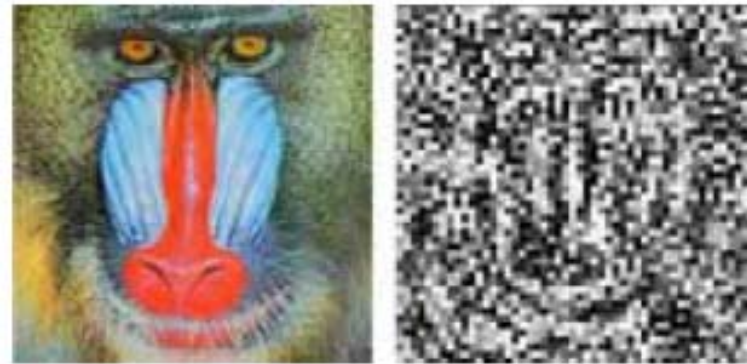
Tajné informace

- 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

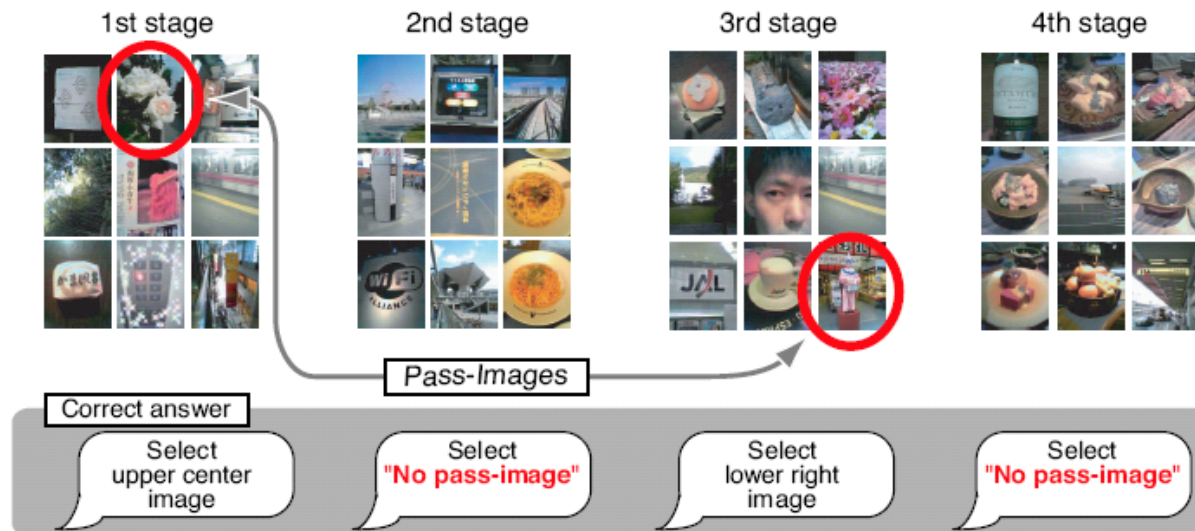
Autentizace obrazovou informací (1)

- 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 (rastovaná 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 nejružnějších obrázků a ten musí identifikovat obrázky ze své skupiny (systém Déjà Vu)
 - jedno odkoukání nestačí

Autentizace obrazovou informací (2)

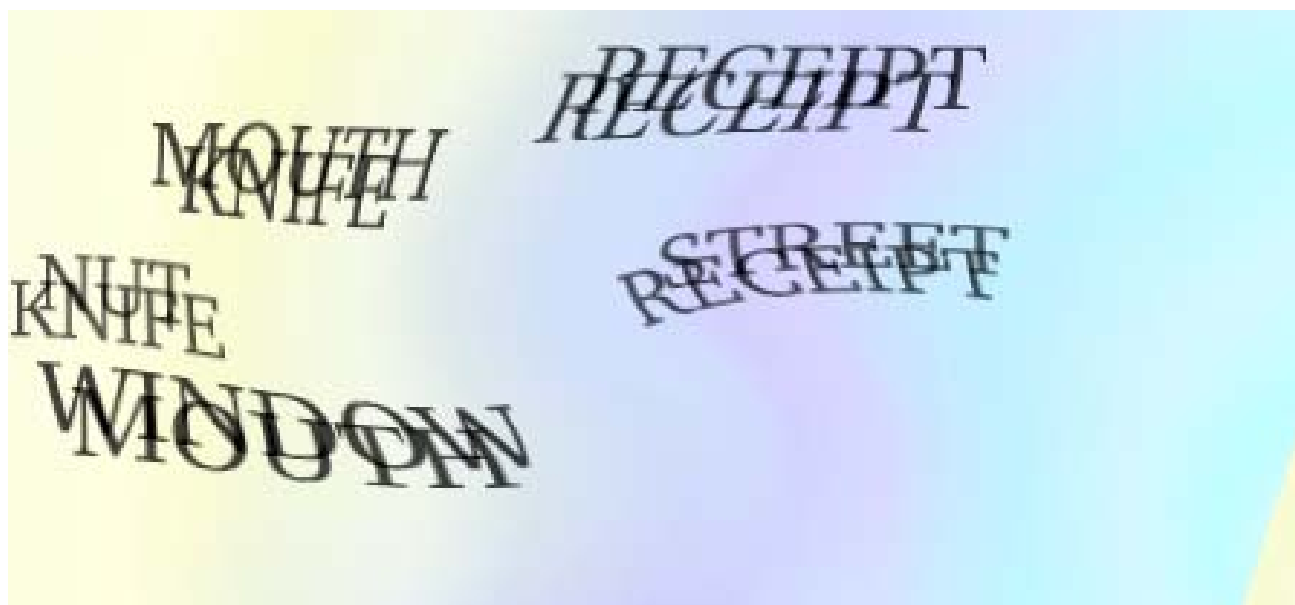


Verification stage



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
- Více v kopii článku „Lze rozeznat...“ (časopis DSM), v ISu
- Pokud 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

Ukládání hesel

- V otevřeném tvaru
 - Ochrana na úrovni systému (řízení přístupu pro zápis i čtení!)
 - Absolutní důvěra v administrátora
 - Problém při zkopírování souboru
 - Raději NE
- V nečitelné podobě
 - Šifrovaná
 - Hašovaná

Šifrování hesel

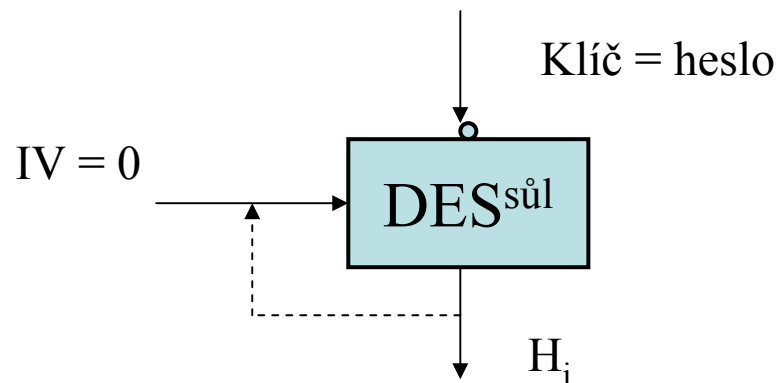
- Hesla neukládáme v otevřeném tvaru, ale šifrovaná
- Ochrana souboru s hesly se mění na ochranu šifrovacího klíče (moc jsme si nepomohli)
 - šifrovací klíč musí být přístupný autentizačnímu systému (tj. uložen na disku, v paměti apod.)
- Problémy podobné jako v případě otevřených hesel
 - důvěra v administrátora
 - problémy v případě kompromitace šifrovacího klíče
- Šifrování využíváme v situaci, kdy chceme mít přístup k otevřenému tvaru hesla
 - např. autentizační protokol nepřenáší heslo jako takové, ale pouze odvozenou informaci

Hašování hesel

- Neukládáme hesla jako taková, ale pouze výsledek hašovací funkce
 - velice se nám hodí jednosměrnost funkce
 - ikdyž se útočník dostane k haši hesla, nezískává automaticky heslo
- Pomalá funkce (1x není problém, opakovaně ano)
 - pro ztížení útoků, kdy k haši hledáme odpovídající heslo
- „Solení“
 - haš není jen funkcí hesla, ale ještě dodatečné náhodné informace (soli)
 - v tabulce hesel musíme ukládat i sůl: $userid, sůl, f(sůl, heslo)$
 - delší efektivní heslo
 - řešení pro stejná hesla (stejná hesla s různou solí budou mít různé haše)

Hašování hesel v UNIXu I

- Funkce „crypt“ – hašovací funkce vytvořená z upraveného šifrovacího algoritmu DES
 - $IV = H_0 = 0$ (64-bitový blok ze samých nul)
 - $K = \text{heslo}$ (56 bitů)
 - 7-bitové znaky (osmý bit ignorován)
 - maximálně 8 znaků (další znaky ignorovány)
 - $H_{i+1} = \text{DES}^{\text{sůl}}_K(H_i)$
 - algoritmus DES je modifikován podle hodnoty soli
 - H_{25} je výsledný haš



H_i se použije stejným způsobem vícekrát (25)

Hašování hesel v UNIXu II

- U funkce crypt je významných jen 8 znaků hesla!
- Ukládáme 2 znaky soli a 11 znaků haše
 - 64 bitů dat uložených jako tisknutelné ASCII znaky
 - 6 bitů/znak (z abecedy
./0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZab
cdefghijklmnopqrstuvwxyz)
- Příklad:
 - sůl je „WQ“
 - heslo je „ahoj“
 - haš ukládáme jako „WQefQg9O93d7I “
- Funkce crypt již není považována za bezpečnou a proto se již nepoužívá

Hašování hesel v UNIXu III

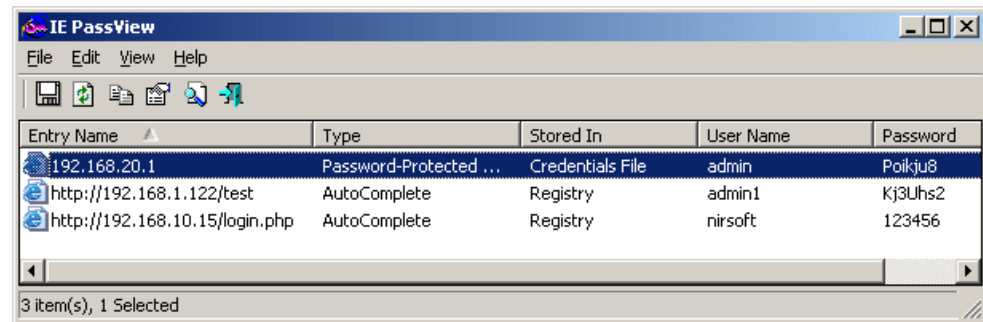
- Nyní se místo hašovací funkce crypt používá hašovací funkce založená na MD5
 - sůl až 8 znaků
 - u hesla je významných 256 znaků
 - ukládáme ve tvaru \$1\$sůl\$haš
 - slabiny nalezené u hašovací funkce MD5 nesnižují bezpečnost ukládaných hesel
- Příklad
 - sůl je „VpFCPvjy“
 - heslo je „ahoj“
 - haš ukládáme jako „\$1\$VpFCPvjy\$DV6ArxpPf7M4mWYJ9v6U2.“

Ukládání hesel ve Windows

- Lze se rozhodnout mezi hašovací funkcí nebo šifrovací funkcí (reversibilní šifrování)
 - default je hašování
- Hašovací funkce
 - LM (Lan Manager) hash
 - starší, není dostatečně bezpečné
 - nerozlišuje velikost písmen (konverze do uppercase)
 - maximálně 14 znaků hesla, hesla delší než 7 znaků se rozdělují na 2 poloviny (to značně usnadňuje útoky)
 - NTLM
 - novější; bezpečnější ale ne ideální
 - založena na MD4 hašování hesla v UNICODE
 - z důvodu kompatibility se staršími systémy se ukládaly haše oba
 - to usnadňuje útoky
 - až od Windows Vista je třeba LM (pro kompatibilitu s win 95 a 98) explicitně povolit

Ukládání hesel v aplikacích

- Pro autentizace vůči této aplikaci
 - stejné metody jako u operačních systémů
- Uložené autentizační údaje pro autentizaci vůči jiným systémům
 - pro pohodlí uživatele
 - není bezpečné
 - ukládáme
 - heslo v otevřeném tvaru
 - heslo zakódované (base64 apod.)
 - heslo zašifrované, šifrovací klíč uložen v aplikaci, její konfiguraci apod.



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 (salt+hash), “x” see shadow, “!” or “*” account locked
 - 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
 - Hashed 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

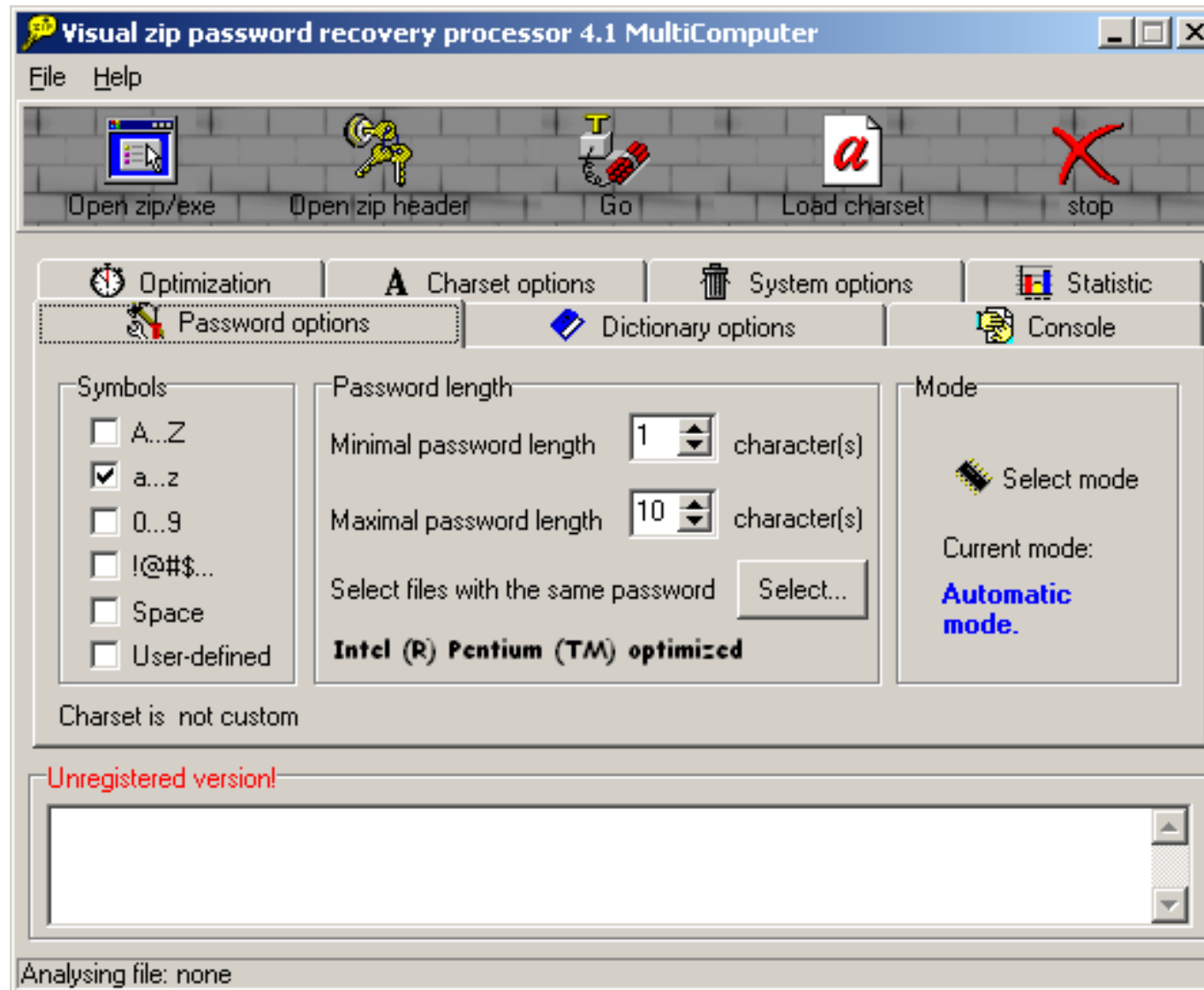
Čas platnosti x Počet odhadů za jednotku času

Velikost abecedy ^{*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



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

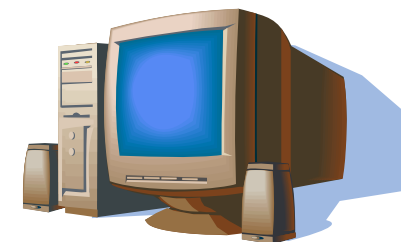
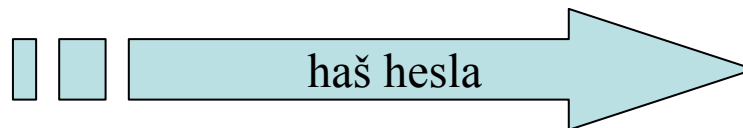
- MojeHeslo09 v září a MojeHeslo10 v říjnu
- Jiné než předchozí – uživatelé zjistí délku záznamu historie hesel a „vyčerpají“ ho:
Heslo123 → qwre321 → jr7*&d → Heslo123
- Zákaz změn po nějakou dobu má za následek problém v případě prozrazení hesla

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

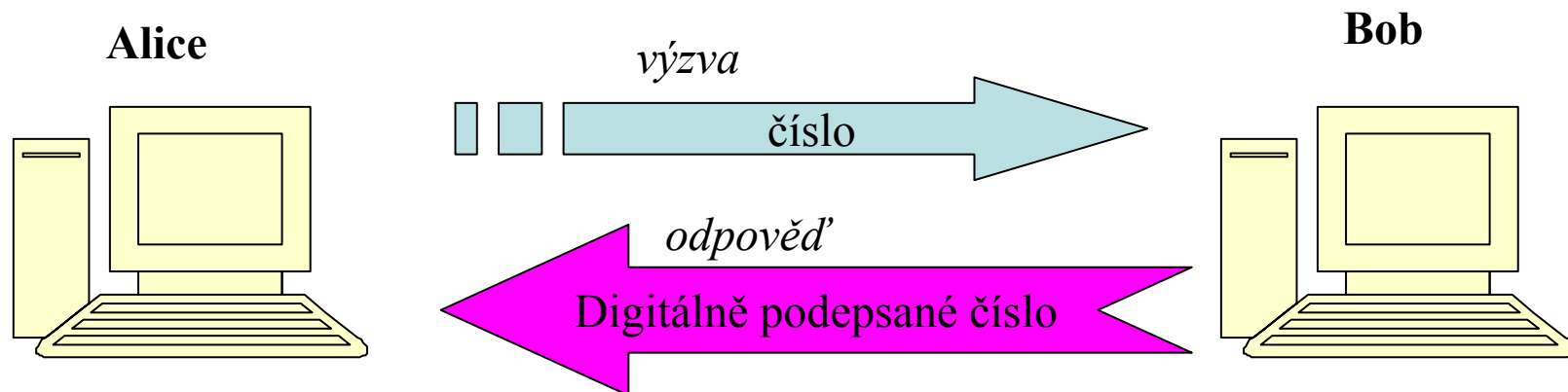
Komunikace a autentizace heslem

- 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

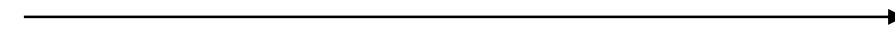
PIN a bankovní karta

- Oba stejnou cestou, v různé dny
- Osobní převzetí – alespoň jednoho
- Vlastní výběr PINu při převzetí karty

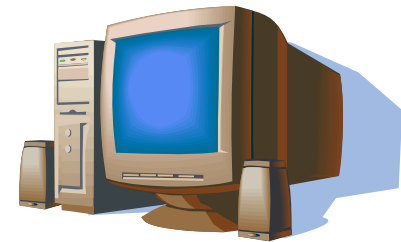
- On-line verifikace (off-line se z bezpečnostních důvodů nepoužívá)




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) ☹

Autentizace finančních transakcí



- Chip&PIN vs. podpis
 - Věříme ve zvýšení ceny nutné pro výrobu padělků
 - Nebyli jsme si jisti, zda eliminuje *příležitostné* zloděje
 - Zloděj (nebo malá skupina zlodějů) ukradne karty a následně padělá podpis, nebo odpozoruje PIN a pak ukradne karty
- Hlavní otázky
 - Je pro zloděje jednodušší zneužít karty s technologií Chip&PIN nebo ty, co vyžadují podpis držitele?
 - Různé pohledy různých subjektů
- Experiment bude představen později v semestru...

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

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 $a \neq A$) minimálně 8 znaků
3. Používat nealfabetické znaky
4. Prosazovat danou politiku volby hesel nějakým mechanismem, jinak alespoň 10 % hesel bude slabých

Otázky?

Vítány!!!

Příští přednáška je 8. 3. 2011 v 10:00

matyas@fi.muni.cz

zriha@fi.muni.cz

