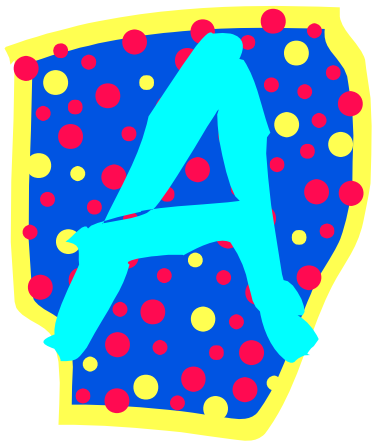
PV157 – Autentizace a řízení přístupu

Autentizace uživatelů tajnými informacemi



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.

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
  - Šifrované
  - Hašované

Šifrování hesel

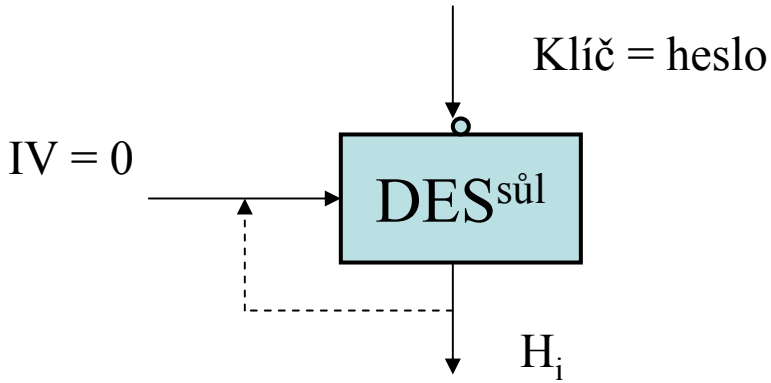
- Hesla neukládáme v otevřeném tvaru, ale šifrovaná
- Ochrana souboru s hesly se mění na ochranu šifrovacího klíče (moc jsme si nepomohli)
  - šifrovací klíč musí být přístupný autentizačnímu systému (tj. uložen na disku, v paměti apod.)
- Problémy podobné jako v případě otevřených hesel
  - důvěra v 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 = heslo (56 bitů)
    - 7-bitové znaky (osmý bit ignorován)
    - maximálně 8 znaků (další znaky ignorovány)
  - $H_{i+1}=DES^{sůl}_K(H_i)$
    - 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 ./0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz)
- 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 1sůl$haš
  - slabiny nalezené u hašovací funkce MD5 nesnižují bezpečnost ukládaných hesel
- Příklad
  - sůl je „VpFCPvjy “
  - heslo je „ahoj“
  - haš ukládáme jako „1VpFCPvjy$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 ukládají haše oba
    - to usnadňuje útoky

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, číslice 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), * see shadow, ! 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:1LxSyKziS$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

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

Čas potřebný k analýze (HAC), crypt na starém 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	4×10^6 r
10	890 r	23.000 r	5.3×10^6 r	3.8×10^8 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 ¼ 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

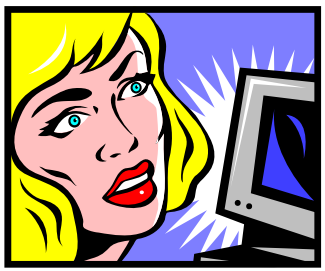
Vhodná hesla

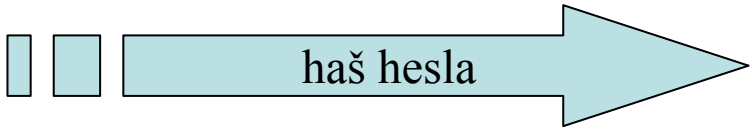
- Lehce zapamatovatelné, obtížně uhodnutelné!

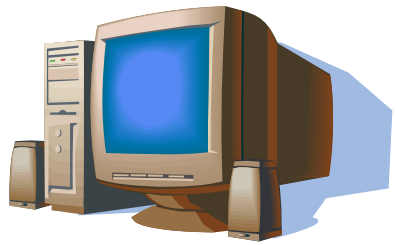
- Heslo založené na delší (lehce, s nějakou pomůckou, zapamatovatelné) frázi
  - *psmVTCOo24Z* = Polámal Se Mraveneček, Ví To Celá Obora, O Půlnoci Zavolali

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

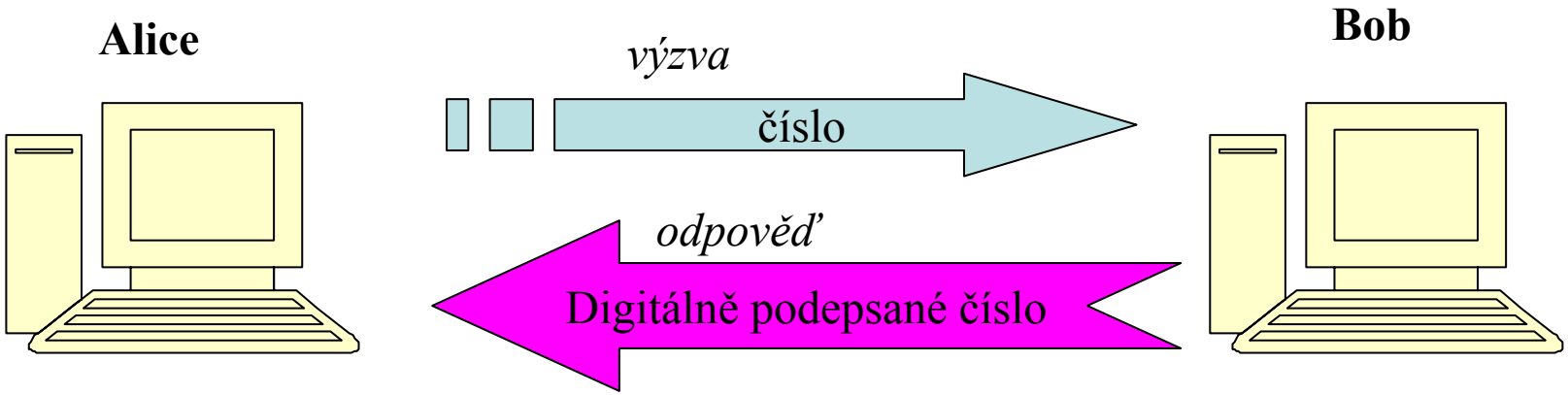






Protokoly výzva-odpověď

- 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

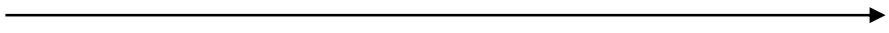
- Levnější klávesnice
- Obtížněji zapamatovatelné než hesla
- Obvykle používány s fyzickým předmětem
- Někdy lze změnit podle přání zákazníka
- Obvykle 4-8 znaků dlouhé
- Procedurální omezení proti útokům hrubou silou
  - Zabavení karty při několika (3) nesprávných PINech
  - Nutnost re-aktivace záložním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

PIN a bankovní karta

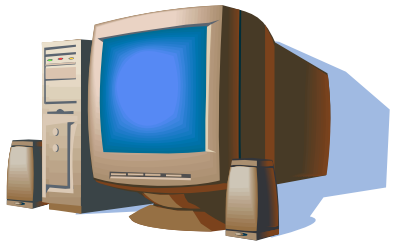
- Oba stejnou cestou, v různé dny
- Osobní převzetí – alespoň jednoho
- Vlastní výběr PINu při převzetí karty

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

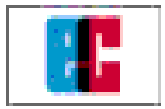
Klíčem bankomatu zašifrované číslo účtu, PIN a částka



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_{Px} 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) ☹

Experiment na FI – knihkupectví Mareček

- Čip&PIN versus podpis
  - Nejasná bezpečnost s ohledem na zneužití zlodějem
    - Zloděj (či malá skupina) pohybující se a kradoucí karty v obchodě
  - V každém případě PIN znesnadní kopírování karty
- Cíl experimentu:
  - Je pro takového zloděje jednodušší provést podvodný nákup?
  - Různé pohledy různých zainteresovaných činitelů
  - Nejsou dostupná žádná čísla z reálných experimentů

Průběh experimentu

- 32 subjektů, PIN i podpis
  - ½ PINpad s krytkou, druhá bez
  - ½ podpis vlastní, druhá cizí
- Subjekty i obchodníci nevěděli o skutečném cíli experimentu – zajištění přirozeného chování

- Omezený čas na nácvik podpisu i pro pozorovatele PINů
- Jiné aspekty (pozorování skrytou kamerou, obchodníkem atd.) nebyly zvažovány

PIN

- PINpad s krytkou
  - Pozorovatelé úspěšní v 6 ze 17 PINů (35,3 %)
    - 3 PINy zpozorovány 2 pozorovateli
    - 2 PINy zpozorovány 1 pozorovatelem
    - 1 zkonstruován ze sdílených informací
  - Celkově ze 156 číslic bylo 75 uhodnuto (48 %)
- PINpad bez krytky
  - Pozorovatelé úspěšní ve 12 z 15 PINů (80 %)
    - 3 PINy zpozorovány 3 pozorovateli
    - 4 PINy dvěma a další 3 jedním pozorovatelem
    - 2 zkonstruovány ze sdílených informací
  - Celkově ze 184 číslic bylo 129 uhodnuto (70,1 %)

Podpis

- Obchodník (klenotnicví) zjistil 12 ze 17 podvádějících
  - 5 podvádějících prošlo (29,4 %)
- Ze 12 zjištěných podvádějících
  - 8 zjištěno okamžitě po 1. podpisu (25 %)
  - 4 až po druhém podpisu (12,5 %)
- Ze 20 (15+5) „úspěšných“ zákazníků
  - 16 prošlo ihned po prvním podpisu (50 %)
  - 4 se muselo podepsat dvakrát (12,5 %)
- 8 zákazníků (25 %) se muselo podepsat dvakrát
  - Podpis byl ověřován velmi striktně (klenotníkem)!!!
  - Jeden subjekt při druhém podpisu sám vzdal ☺

Závěry

- Prozatímní – další kolo experimentu proběhlo právě minulý pátek v supermarketu
- Krytka na PINpadu je rozhodně užitečná
- Autorizace PINem není oproti pečlivé kontrole podpisu bezpečnější

- PIN v obchodě je lehčeji odpozorovatelný než v bankomatu
- Rozhodně kontrolovat a případně hlásit ztrátu karty
  - A zvolit banku, která kryje ztráty od nahlášení

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!!!

Příští přednáška je 20. 3. 2006 v 14:00

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