Bezpečnostní mechanismy

Hardwarové prostředky kontroly přístupu osob

- Identifikační karty
  - informace umožňující identifikaci uživatele
  - PIN – Personal Identification Number
  - úroveň oprávnění
  - informace o povolených úkonech
  - povolení vstupu do určitých oblastí

Principy identifikačních karet

- Karta s čárovým kódem
  - nositel ident. informací je sekvence mezer a čar
  - levná implementace a nízká technická náročnost
  - vysoké riziko padělání
  - nízká celková úroveň zabezpečení systému

Principy identifikačních karet

- Magnetické karty
  - nosič informací – magnetický pásek
  - opakovaný záznam různých informací
  - vysoká životnost
  - riziko možného vymazání a vložení nových informací

Principy identifikačních karet

- Indukční a radiofrekvenční karty
  - přenos informací pomocí radiových vln
  - čtecí jednotka může přijímat údaje z větší vzdálenosti
  - dražší implementace
  - vyšší úroveň zabezpečení než u předchozích dvou typů

Principy identifikačních karet

- Optické karty
  - čtecí zařízení může rozeznat písmo, popř. optické prvky na kartě
  - zařízení na bázi skeneru nebo CCD kamery
  - zabezpečení srovnatelné s indukčními/radiofrekvenčními kartami
  - finančně náročnější

Principy identifikačních karet

- Čipové karty
  - většinou programovatelné smart karty, umožňující zápis do paměti čipu (na rozdíl od čipových PROM karet – pouze čtení)
  - možnost aktualizace ident. údajů
  - obsahují množství typů informací (ident. údaje, přístupová práva, šifrovací klíče, atd.)
  - složitější implementace, vyšší hardwarové požadavky a finanční nároky
  - široké možnosti využití a nejvyšší úroveň bezpečnosti = preference čipových karet před ostatními

Bezpečnostní karty

- přídavný HW, který se vkládá do některého ze slotů motherboardů
- při startu BIOS přebírá bezp. mechanismus karty kontrolu nad systémem dle zadaných pravidel
- výhoda: k inicializaci dochází před startem OS = znesnadnění útoku
- chrání pouze jeden počítač, vysoké finanční náklady
- někdy je součástí tzv. touch memory systém (přiložení přívěsku ke čtečce)

Bezpečnostní karty umožňují:

- šifrování dat, ukládaných na různá média
- řízení přístupu k sériovým a paralelním portům
- kontrolu přístupu k pevným diskům či jiným záznamovým médiím
- uzamykání klávesnice či dalších komponent
- statistické zpracování provozu systému apod.

Hardwarový zámek

- jednoznačně překonaná hardwarová ochrana systému
- prakticky žádný význam vzhledem k příliš málo variacím vyráběných zámků
- jednoduché přemostění příslušných kontaktů na motherboardu vyřadilo zámek z činnosti

Biometrické systémy

- Biometrika – věda, zabývající se autentizací měřením fyziologických nebo behaviorálních charakteristik osob
- Multifaktorová autentizace
  - informace, kterou osoba zná (heslo)
  - předmět, který má osoba v držení (token)
  - biometrické vlastnosti osoby

Biometrika

	Neměnnost	Jedinečnost	Invazivita	Reprodukovatelnost
Hlas	*	**	*	***
Ruční písmo	**	**	*	**
Otisk prstu	**	**	*	**
Obličej	*	*	*	***
Sítnice oka	***	***	***	?
Duhovka oka	***	***	***	?

Přesnost měření - biometrika

- dosahuje se pouze pravděpodobnostních výsledků
- měření neprobíhá za ideálních podmínek – hluk, akustika, jiné psací potřeby apod.
- možnost neoprávněného přijetí X neoprávněného odmítnutí ?!?!
- => nastavení dle míry zabezpečení

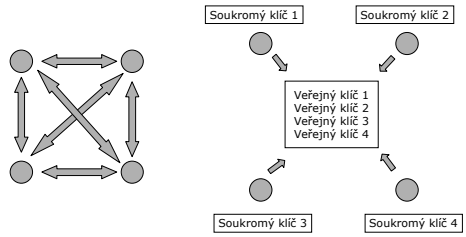
Biometrické systémy ze sociálního a kulturního hlediska

- Snímání oční rohovky může být sociálně akceptovatelné při řešení přístupu do vysoce chráněných vládních či armádních komplexů
- ale při placení v supermarketu???
- Zkoumání lidského hlasu -vykřikování určitých slov na veřejnosti ???
- Biometrika kromě technických problémů naráží na kulturní a sociální překážky.

Kryptologie a kryptografie

- **Kryptologie** je vědní obor zabývající se tvorbou, používáním a luštěním čili prolamováním šifer.
- Kryptologie zahrnuje kryptografii a kryptoanalýzu.
- **Kryptografie** je věda o tvorbě šifer, kdy informace mají abecedně číslicový charakter.

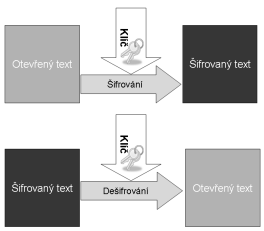
Symetrická a asymetrická kryptografie



Symetrická kryptografie

- V počátcích byly šifrovací algoritmy založeny na symetrickém klíči – jeden tajný klíč
- Proudové šifry zpracovávají otevřený text po jednotlivých bitech
- Blokové šifry rozdělí otevřený text na bloky stejné velikosti a doplní vhodným způsobem poslední blok na stejnou velikost
- Blok o 64 bitech, AES používá 128 bitů

Symetrická kryptografie



DES (Data Encryption Standard)

- Symetrická šifra vyvinutá v 70. letech
- V roce 1977 byla zvolena za standard (FIPS 46) pro šifrování dat v civilních státních organizacích v USA a následně se rozšířila i do soukromého sektoru.
- 56 bit klíč
- Šifru lze prolomit útokem hrubou silou za méně než 24 hodin.
- Nástupce byl 3DES - trojnásobná aplikace šifry DES (168 bit klíč) – oproti AES pomalejší

AES (Advanced Encryption Standard)

- Nástupce DESu
- Symetrická bloková šifra
- Vyvinuta americkou vládou jako standard pro šifrování svých dokumentů
- Velikost klíče může být 128, 192 nebo 256 bitů
- Šifruje data postupně v blocích s pevnou délkou 128 bitů
- Vysoká rychlost šifrování
- Nejlepší a dosud nepřekonaná symetrická šifra

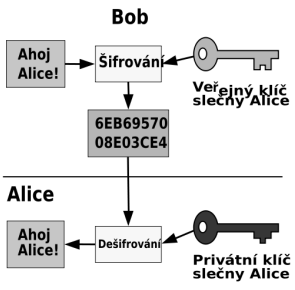
Twofish

- Symetrická bloková šifra
- 128-bitová délka bloku a 256-bitová délka
- Vyvinutá Brucem Schneierem
- Jde o nepatentovanou otevřenou šifru pro volné použití.

Asymetrická kryptografie

- asymetrické algoritmy – dvojice klíčů (pár klíčů, key pair) – soukromý či privátní klíč a veřejný klíč = snazší správa klíčů
- pomocí veřejného klíče odesílatel zprávu zašifruje a příjemce pomocí soukromého klíče rozšifruje (pomocí veřejného klíče nelze rozšifrovat)
- založeno na tzv. jednocestných funkcích

Asymetrická kryptografie



RSA (iniciály autorů Rivest, Shamir, Adleman)

- Šifra s veřejným klíčem
- Jedná se o první algoritmus, který je vhodný jak pro podepisování, tak šifrování.
- Používá se i dnes, přičemž při dostatečné délce klíče je považován za bezpečný.

Šifrování nebo podepisování?

- šifrování mění data, aby nebyla čitelná neoprávněnou osobou
- podepisování – zajištění nepopiratelnosti a integrity
- nepopiratelnost = nelze popřít, osoba zprávu podepsala (obdoba písemného podpisu)
- integrita = od podpisu nedošlo ke změně dat