

## Biztonság az operációs rendszerekben

Biztonság és hatékonyság

Fenyegetések és típusaik

Védelmi koncepciók

Példák (UNIX, Windows 2000/XP)

## Biztonság és hatékonyság

- Biztonság és hatékonyság
- Döntésnél figyelembe veendő tényezők:
  - Rendszer fontossága
  - Szükséges biztonsági erőfeszítések mértéke
  - Biztonsági megoldások negatív hatásai
- Teljes, kizárhatatlan biztonság nem létezik
  - Egyensúlyt kell teremteni
  - Az OR-ek biztonságát folyamatosan javítják
- Belső és külső biztonság
  - Belső: az erőforrások helyes használata
  - Külső: védelem a különböző fenyegetések ellen

## Fenyegetések és típusaik

- Fizikai fenyegetések
  - Természeti csapások
  - Jogosulatlan hozzáférés
    - Betörés, beléptető rendszer kijátszása, kulcslopás stb.
- Logikai fenyegetések
  - Felhasználói felelőtlenség, tévedések
  - Szolgáltatásmegtagadás
    - Válaszidő túllépése
    - Rendelkezésre állás megszűnése
  - Jogosulatlan hozzáférés szoftvererőforrásokhoz
    - Fájlok, memória, beállítások módosítása
    - Információlopás/törlés, szerzőjog-sértés, kémkedés, vírusok, férgek, trójai falovak bejuttatása, rejtekajtók kihasználása...

## Védelmi koncepciók

- Védelmi tartomány
  - Definíció: a védett erőforrások hozzáférési privilégiumainak összessége
  - Tágabb értelemben: azonosítási és hozzáférési jogok határaival elválasztott virtuális tartomány
    - A védelmi tartományok átfedhetnek egymást
  - Cél: a lehető legszűkebb tartomány kijelölése
  - Típusok:
    - Statikus védelmi tartomány
      - Rögzített (pl. a folyamat indításakor) jogosultságok
    - Dinamikus védelmi tartomány
      - A tartományok módosíthatók, illetve lehetséges az átlépés más tartományokba (pl. futás más néven)

## Védelmi koncepciók

- Védelmi tartomány
  - Példák
    - MS-DOS: command.com
      - Mindent szabad, de: command.com és io.sys nem törölhető, eszközök (pl. PRN) nem törölhetők
    - UNIX fájlrendszer: uid és gid + jogosítványok
      - uid: felhasználó védelmi tartománya
      - gid: felhasználót tartalmazó csoport védelmi tartománya
      - jogosítvány: tartományhoz rendelt jogok (RWX)

## Védelmi koncepciók

- Hivatkozásfelügyelési koncepció  
(Security Reference Monitor concept)
  - Többfelhasználós számítógépek hozzáférés-szabályozására kidolgozott általános megoldás



## Védelmi koncepciók

- Szubjektumok (felhasználók és folyamataik) azonosítása (autentikáció)
  - Cél: szubjektum besorolása egy védelmi tartományba
  - Technikák
    - Külső
      - Mágneskártyás vagy vonalkódos beléptető rendszer
      - Kulcsalapú rendszerek
    - Belső
      - Jelszavas védelem (potenciális biztonsági rés)
      - Csak a felhasználó által ismert információ bekérése

## Védelmi koncepciók

- Objektumokhoz történő hozzáférés privilégiumai (autorizáció)

### 1) Hozzáférési mátrix

	Erőforrások (pl. fájlok, eszközök)				
	F1	F2	F3	DAT	nyomtató
U1	olvasás		írás	olvasás+írás	
U2		olvasás+írás	olvasás		nyomtatás
U3		futtatás		olvasás	nyomtatás
U4	olvasás	olvasás	olvasás		nyomtatás

műveletek

## Védelmi koncepciók

- Objektumokhoz történő hozzáférés privilégiumai (autorizáció)

### 2) Hozzáférési jogok listája (*access control list*, ACL)

A hozzáférési mátrix kitöltött elemeit az erőforrásokhoz rendeljük (általában van alapértelmezett hozzáférés is):

```
<
erőforrás1 <tartomány, művelet> <tartomány, művelet> ...
erőforrás2 <tartomány, művelet> <tartomány, művelet> ...
erőforrás3 <tartomány, művelet> <tartomány, művelet> ...
...
/>
```

Előny: az ACL jól kezelhető; elég a tartományt ismerni  
Hátrány: fájloknál hosszú lehet az ACL

## Védelmi koncepciók

- Objektumokhoz történő hozzáférés privilégiumai (autorizáció)

### 3) Jogosultsági lista (*capability list*, CL)

A hozzáférési mátrix kitöltött elemeit a tartományokhoz rendeljük:

```
<
tartomány1 <erőforrás, művelet> <erőforrás, művelet> ...
tartomány2 <erőforrás, művelet> <erőforrás, művelet> ...
tartomány3 <erőforrás, művelet> <erőforrás, művelet> ...
...
/>
```

Előny: elosztott rendszerekben is használható (az ACL nem)  
Hátrány: kevésbé szemléletes

## Védelmi koncepciók

- Objektumokhoz történő hozzáférés privilégiumai (autorizáció)

### 4) Zár-kulcs megoldás

Bizonyos hozzáférési követelményekhez kulcsokat (illetve nekik megfelelő információkat) rendelünk

Előny: rugalmas, a kulcsok átruházhatók  
Hátrány: bonyolult

## Védelmi koncepciók

- Biztonsági auditálás
  - Sikeres ÉS sikertelen hozzáférési kísérletek rögzítése
  - Biztonsági események naplózása
  - Cél: azonnali reakció (pl. rendszergazda értesítése) és/vagy utólagos intézkedések támogatása
  - Megvalósítás:
    - Naplózó komponensek
    - Auditálási politika

## Példa – UNIX rendszerek

- A szubjektumok mindig folyamatok
- „A UNIX-ban minden fájl”  $\hat{=}$  a védelmi funkciók a fájlrendszerben összpontosulnak
  - Fájlrendszer-objektumok: három védelmi tartomány
  - A jogok értelmezése objektumonként változik
    - Fájlok: R = olvasási jog, W = írási jog, X = végrehajtási jog
    - Könyvtárak: R = listázási jog, W = jog listaelemek hozzáadására/eltávolítására, X = hozzáférés a listaelemekhez
    - Példa: fájl konkrét védelmi beállításai

Tartomány:	1. tartomány (tulajdonos)	2. tartomány (tulajdonos csoport)	3. tartomány (külvilág)
Azonosító:	UID	GID	Külvilág
Védelem:	<b>RWX</b>	<b>RWX</b>	<b>R--</b>

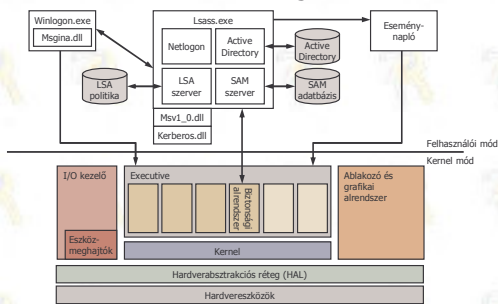
## Példa – UNIX rendszerek

- Védelmi politika
  - A folyamatoknak van valós és effektív tulajdonosa (UID) és csoportja (GID)
    - Ezzel a folyamat más nevében is működhet (setuid/setgid)
  - A hozzáférési jogokat az effektív tulajdonos jogai határozzák meg
- Védelmi politika érvényesítése
  - Folyamat effektív UID-ja = fájl UID? Ha igen  $\hat{=}$  fájl „UID” jogosultsága szerinti hozzáférés  $\hat{=}$  vége
  - Folyamat effektív GID-je = fájl GID? Ha igen  $\hat{=}$  fájl „GID” jogosultsága szerinti hozzáférés  $\hat{=}$  vége
  - A fájl „Külvilág” jogosultsága szerinti hozzáférés  $\hat{=}$  vége

Példa: ---R--RWX

## Példa – Windows 2000/XP

- A Windows 2000/XP biztonsági alrendszere



## Példa – Windows 2000/XP

- Autentikáció
  - Szubjektumok azonosítása: SID (*Security Identifier*)
    - Pl. S-1-5-21-3456738245-8534728415-112948198-8412
    - Felhasználók, csoportok, számítógépek, tartományok
  - Zseton (*token*)
    - Adott folyamat vagy szál biztonsági kontextusát azonosító objektum
    - Tartalma: egyéni és csoportazonosítók, jelzők, privilégiumok (pl. SeDebug, SeShutdown...)
  - Megszemélyesítés (*impersonation*)
    - Műveletek végrehajtása más folyamat nevében
    - Csak a megszemélyesíteni kívánt folyamat jóváhagyásával

## Példa – Windows 2000/XP

- Autorizáció
  - Jogosultságellenőrzés objektumszinten
  - Biztonsági leírók (*security descriptors*)
    - Verziószám, jelzők (pl. örökölt-e mástól)
    - Tulajdonos biztonsági azonosítója (SID)
    - Csoport biztonsági azonosítója (POSIX/UNIX kompatibilitás)
    - DACL (*discretionary access control list*) mutató
      - Mely szubjektumok milyen hozzáférési jogokkal rendelkeznek az objektumhoz
    - SACL (*system access control list*) mutató
      - Mely szubjektumok milyen műveletei során történjen az objektumra biztonsági naplózás
  - Ellenőrzés csak az első hozzáféréskor

## Példa – Windows 2000/XP

- Védelmi példa: fájl

