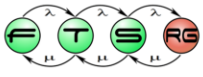
Operációs rendszerek (vimia219)

Biztonsági alrendszer a Windowsban

Micskei Zoltán

http://www.mit.bme.hu/~micskeiz



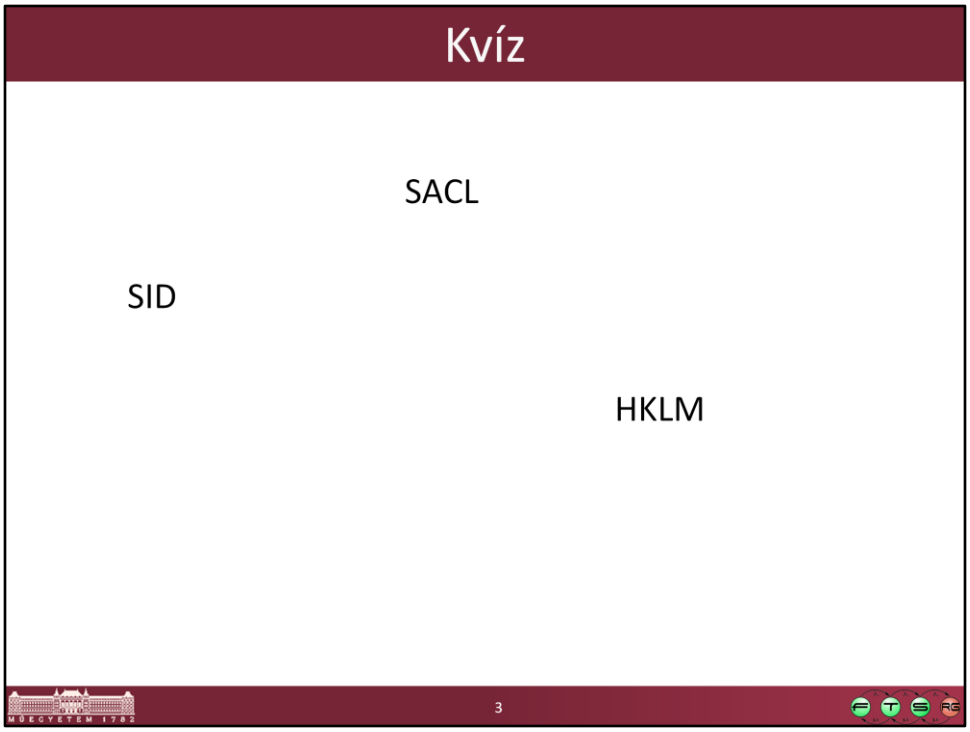
Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Utolsó módosítás: 2012. 05. 08.

Copyright Notice

- These materials are part of the *Windows Operating System Internals Curriculum Development Kit,* developed by David A. Solomon and Mark E. Russinovich with Andreas Polze
- Microsoft has licensed these materials from David Solomon Expert Seminars, Inc. for distribution to academic organizations solely for use in academic environments (and not for commercial use)
- http://www.academicresourcecenter.net/curriculum/pfv.aspx?ID=6191
-

A fóliák részben a Windows Operating System Internals Curriculum Development Kit alapján készültek.



SACL: System Access Control List
SID: Security Identifier
HKLM: HKEY_LOCAL_MACHINE

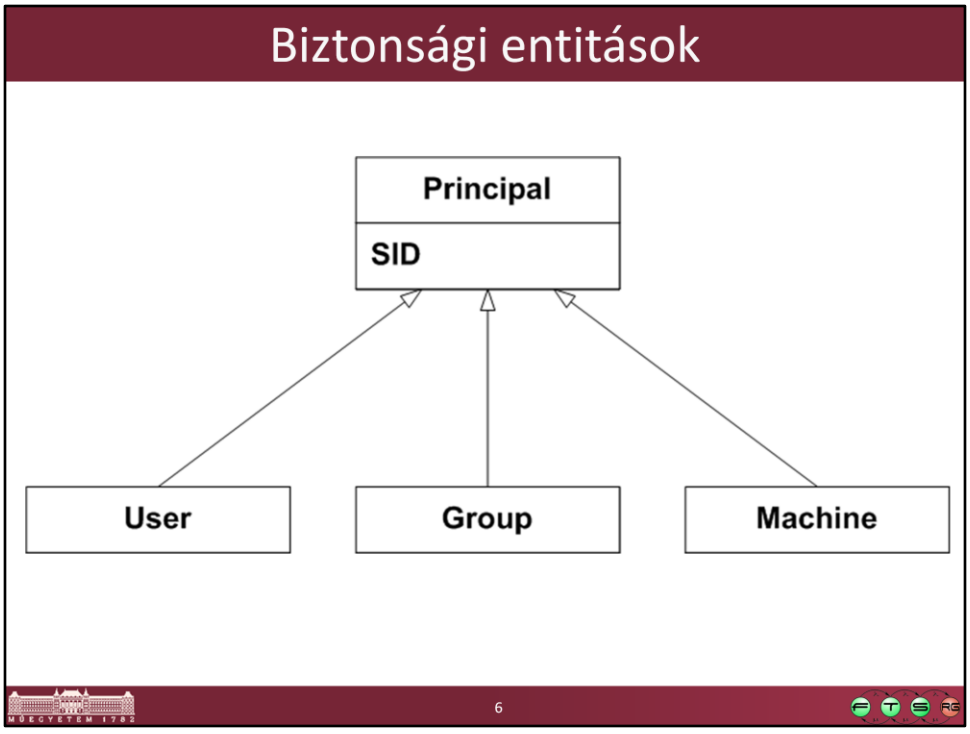
Biztonsági feladatok a Windowsban

- Hitelesítés (authentication)
  - Birtok / tudás / biometria
  - Pl. bejelentkezési képernyő, hitelesítő ablakok
- Engedélyezés (authorization)
  - Alapelv: mindig *csoportnak* osztunk jogot
  - Pl. biztonsági házirend, fájl ACL
- Auditálás
  - Biztonsági naplózás

Az authorizationnek még rengeteg egyéb fordítása van: meghatalmazás, jogosultság-ellenőrzés, felhatalmazás

Biztonsági feladatok a Windowsban

- **Hitelesítés (authentication)**
  - **Birtok / tudás / biometria**
  - **Pl. bejelentkezési képernyő, hitelesítő ablakok**
- Engedélyezés (authorization)
  - Alapelv: mindig *csoportnak* osztunk jogot
  - Pl. biztonsági házirend, fájl ACL
- Auditálás
  - Biztonsági naplózás



Principal: A biztonsági rendszer által kezelt entitások összefoglaló neve.

Csoportokat az egyszerűbb, átláthatóbb adminisztrálás érdekében érdemes létrehozni; a biztonsági beállításokat mindig csoportokra adjuk meg, és felhasználókat pedig csak eltávolítjuk vagy hozzáadjuk a megfelelő csoporthoz.

A biztonsági rendszerben a számítógépet is reprezentálja egy felhasználó, az NT AUTHORITY\System (a Szolgáltatások résznél Local System néven hivatkoztunk rá).

Security Identifier (SID)

- Felhasználó / számítógép azonosítója
- Pl. gép SID-je:

`S-1-5-21-2052111302-1677128483-839522115`

- Felhasználók, csoportok:
  - <Gép SID>-<RID>
  - RID: relative identifier
- Jól ismert SID-ek
  - Everyone: S-1-1-0
  - Administrator: S-1-5-domain-500
- Vista: szolgáltatások is kapnak SID-et

Well-known security identifiers in Windows operating systems
http://support.microsoft.com/kb/243330

Miért jó a SID alapú és nem login név alapú azonosítás
- login átnevezhető
- SID gépspecifikus, így két ugyanolyan nevű, de külön gépen létrehozott felhasználó is megkülönböztethető

DEMO Security identifier (SID)

- `psgetsid.exe gepnev`
- `psgetsid.exe rendszergazda`
- `psgetsid.exe <felhasznalo>`

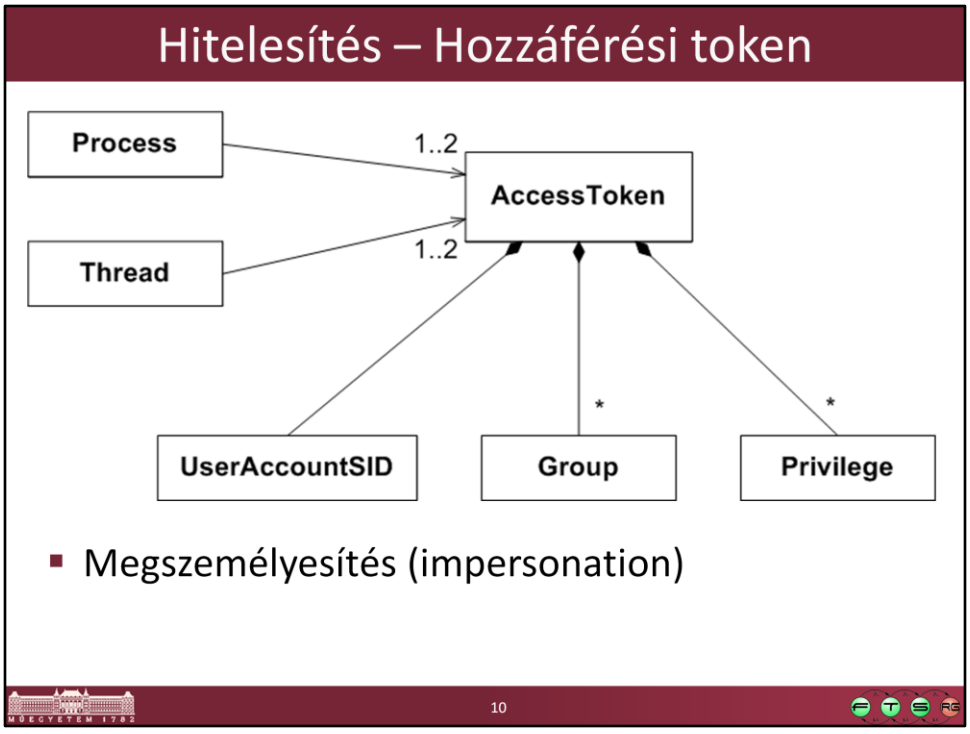
psgetsid: sysinternals csomag része, http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

Hitelesítés

- Belépés
  - Winlogon saját ablakán keresztül
  - Secure Attention Sequence: Ctrl + Alt + Del
- Jelszavak tárolása:
  - Hash a registry-ben
- Hálózati azonosítás
  - NTLM: NT LAN Manager
  - Kerberos: Windows 2000 óta, tartományi (domain) környezetben

Miért pont a Ctrl + Alt + Del: ez volt egy jól megjegyezhető, nem foglalt billentyűkombináció

Why is Control-Alt-Delete the secure attention sequence (SAS)?
(http://blogs.msdn.com/larryosterman/archive/2005/01/24/359850.aspx)

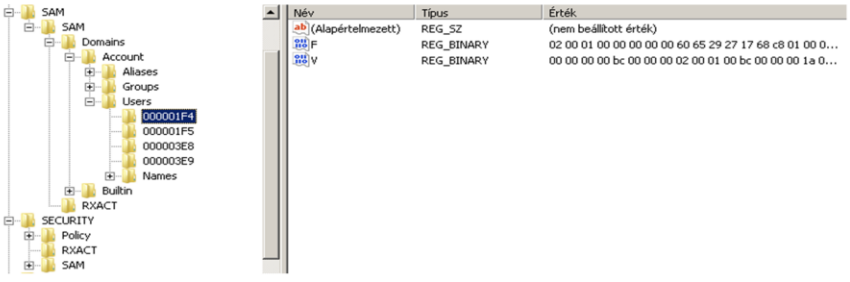


A belépéskor hozzárendelődik egy hozzáférési token a felhasználóhoz, és a későbbi műveletek során az ebben tároltakat ellenőrzi a rendszer.

Ideiglenesen egy folyamat vagy szál kaphat másik hozzáférési tokent, mint az őt futtató felhasználóé. Például egy fájlszerver végrehajtó szála átveszi a hívót reprezentáló tokent a kérés végrehajtásához (így a hívó jogosultságaival hajtja végre a kérést).

DEMO Security Account Manager DB

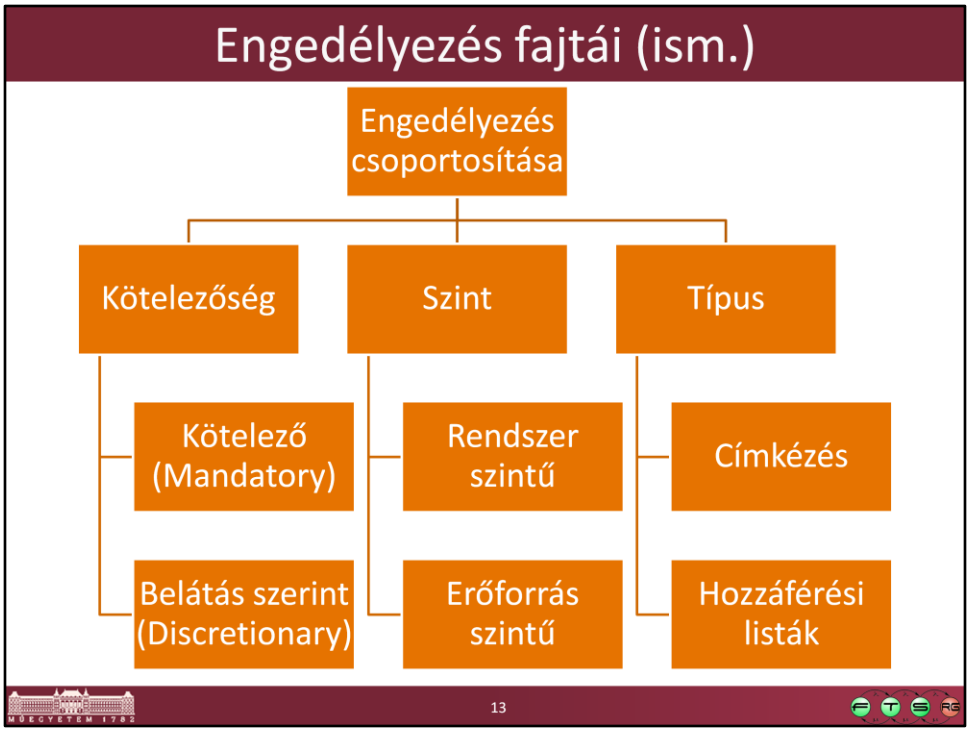
- rendszerleíró adatbázis (registry)
  - HKEY_LOCAL_MACHINE\SAM
- megnézés: `psexec -i -s regedit.exe`



A SAM-ot még a Rendszergazda se tudja megnézni.
A jelszavak hash-e tárolódik itt.

Biztonsági feladatok a Windowsban

- Hitelesítés (authentication)
  - Birtok / tudás / biometria
  - Pl. Bejelentkezési képernyő, hitelesítő ablakok
- **Engedélyezés (authorization)**
  - **Alapelv: mindig *csoportnak* osztunk jogot**
  - **Pl. Biztonsági házirend, fájl ACL**
- Auditálás
  - Biztonsági naplózás

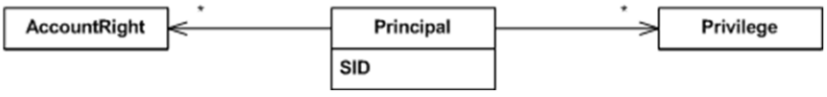


A csoportosítás esetleges, rengeteg egyéb szempont van természetesen.

Engedélyezési lehetőségek a Windowsban

- **Rendszerszintű jogosultságok**
- Discretionary Access Control
- Mandatory Integrity Control

Rendszerszintű felhatalmazás



- **Jogosultság** (privilege)
  - operációs rendszer szintű jog
  - Pl.: számítógép leállítása, eszközmeghajtó betöltése
  - Név: SeShutdownPrivilege, SeLoadDriverPrivilege
- **Fiók jog** (account right)
  - ki hogyan léphet be / nem léphet be
  - Pl.: interaktív, hálózaton keresztül…

Privilege Constants
http://msdn.microsoft.com/en-us/library/bb530716(VS.85).aspx

Account Rights Constants
http://msdn.microsoft.com/en-us/library/bb545671(VS.85).aspx

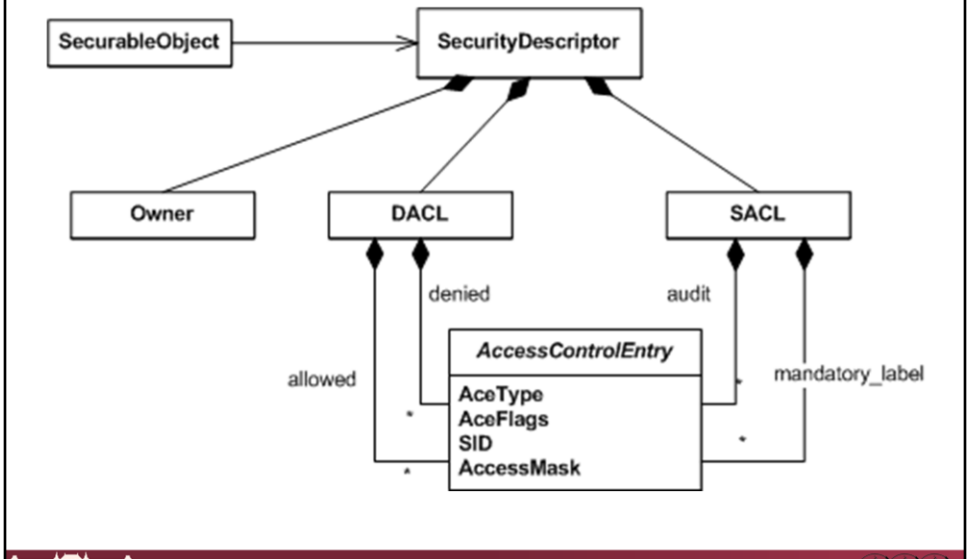
DEMO Jogosultságok: Helyi biztonsági házirend

- Jogosultságok
  - `whomai /priv`
  - Helyi házirend: Felhasználói jogok kiosztása
- Helyi biztonsági házirend további elemei
  - Jelszóházirend
  - Fiókzárolás
  - Biztonsági beállítások

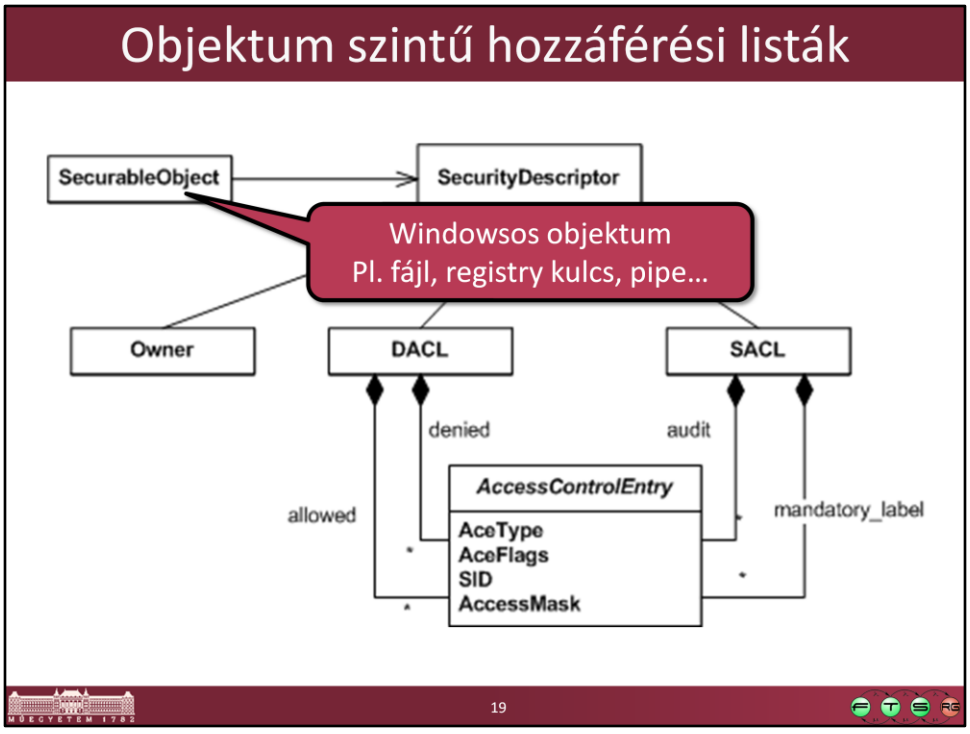
Engedélyezési lehetőségek a Windowsban

- Rendszerszintű jogosultságok
- **Discretionary Access Control**
  - belátás szerinti, erőforrás szintű, hozzáférési lista
- Mandatory Integrity Control

Objektum szintű hozzáférési listák



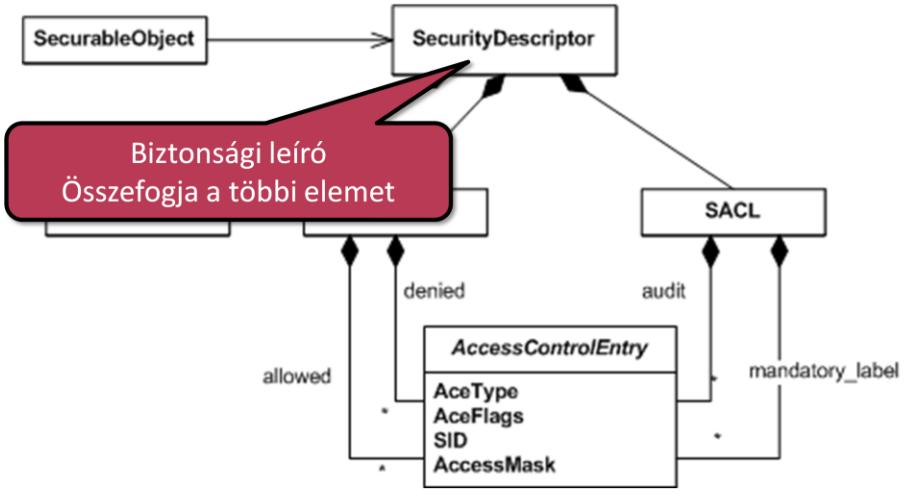
Az ábra csak a legfontosabbakat tartalmazza, teljes lista:
http://msdn.microsoft.com/en-us/library/aa379561(VS.85).aspx



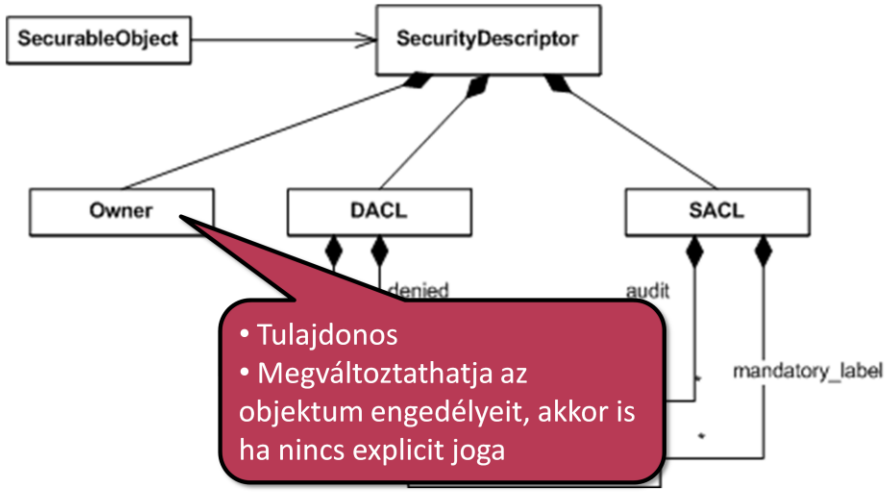
Közös hozzáférési modell a legtöbb windowsos objektumhoz, mindegyikhez ugyanolyan biztonsági leíró rendelhető, csak majd mások lesznek a speciális jogok.

Securable Objects
http://msdn.microsoft.com/en-us/library/aa379557(VS.85).aspx

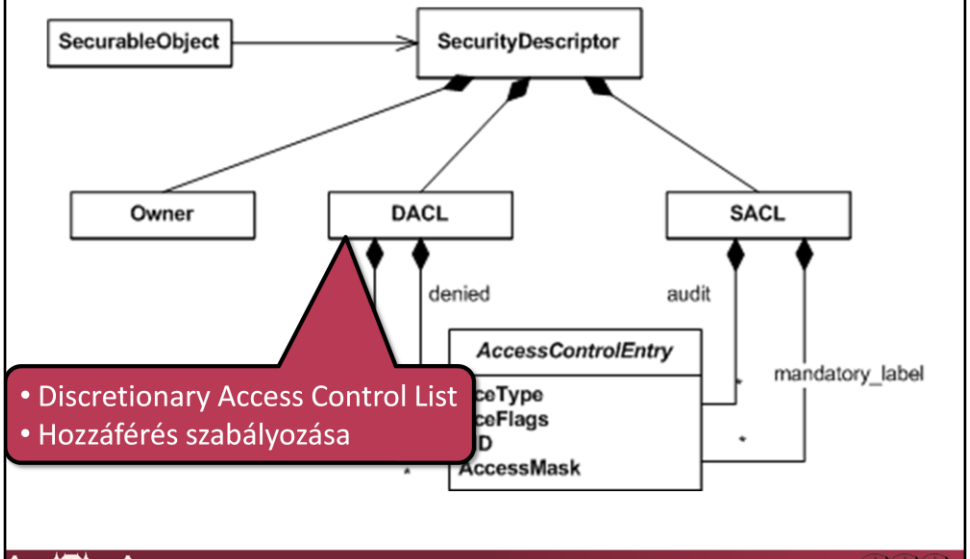
Objektum szintű hozzáférési listák

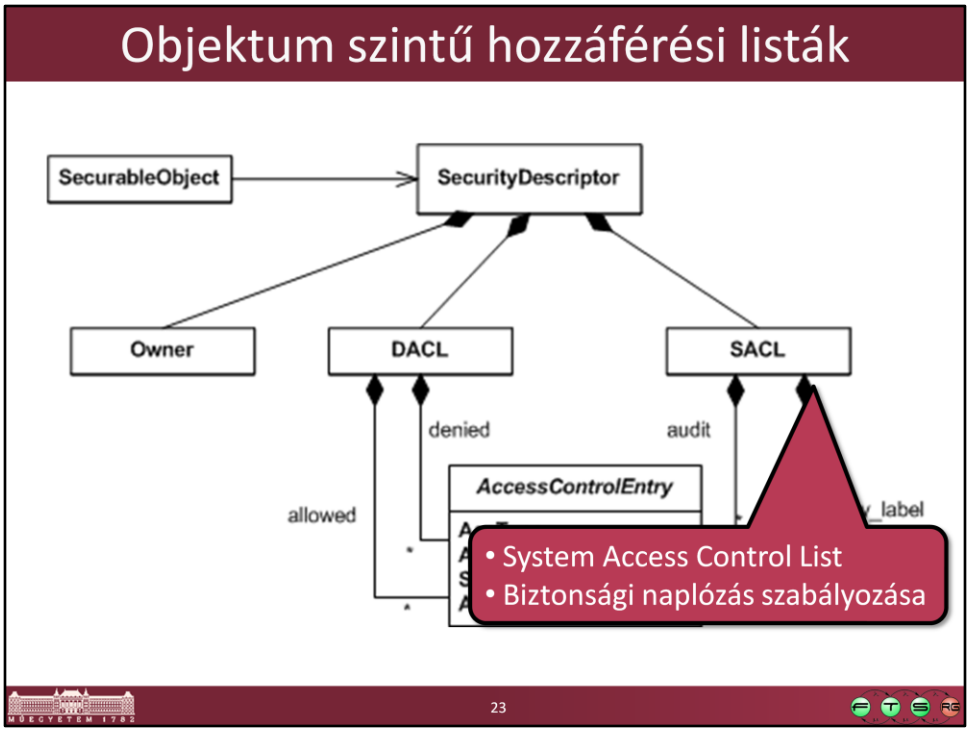


Objektum szintű hozzáférési listák



Objektum szintű hozzáférési listák





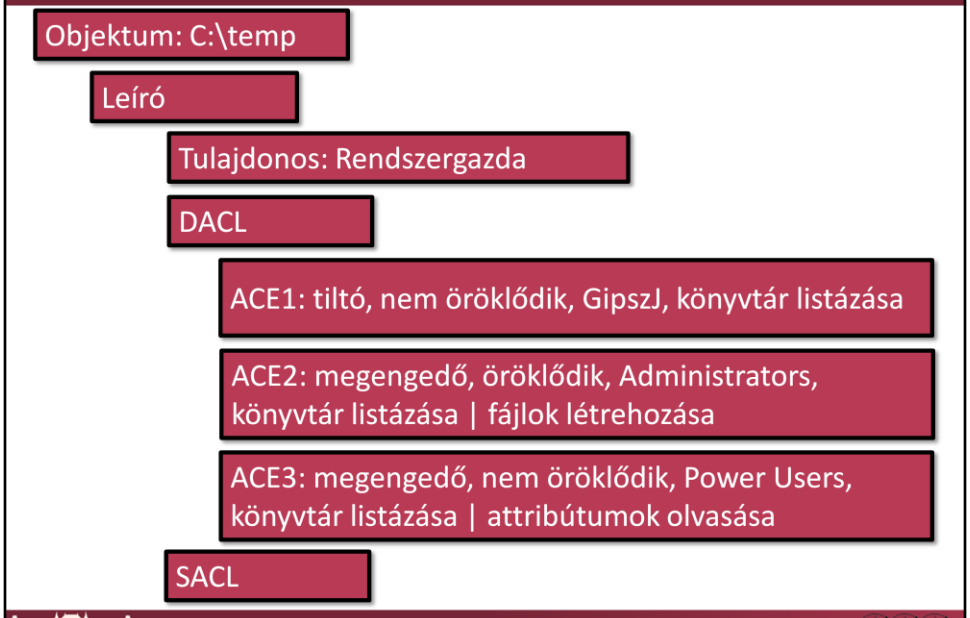
(Ez nem a felhatalmazás feladatát látja el, hanem azt szabályozza, hogy kinek milyen művelete esetén kell naplózni az adott műveletet.)

Objektum szintű hozzáférési listák

- Típus
  - megengedő, tiltó, audit
- Flag
  - Pl. öröklődés
- SID
  - kire vonatkozik
- Maszk
  - végrehajtás | törlés | tulajdonos írása…

ACCESS_MASK Data Type
http://msdn.microsoft.com/en-us/library/aa374892(VS.85).aspx

Hozzáférés-vezérlési listák - példa



Hozzáférés-vezérlési listák

- Öröklődés flag
  - Konténer típusú objektumnál (pl. könyvtár)
  - Gyerek objektum megkapja azt az ACE-t
- Kiértékelés menete
  - Egy SID-re több ACE is érvényes lehet
  - ACE-kból kapott engedélyek UNIÓJA számít
  - Kivéve a tiltást, az mindig magasabb prioritású

DEMO Engedélyezés – Fájl hozzáférési listák

- Csoport, felhasználó – elemi engedélyek
- Öröklődés
  - Öröklés korlátozása
- Tulajdonba vétel
- Eredő engedély
  - Unió (csoportokból és felhasználótól), kivéve
  - Tiltás mindig érvényesül
- Hibaelhárítás: Process Monitor

•Előadók és Hallgatók csoport, gipszj felhasználó mindkettőnek tagja
•Könyvtárszerkezet:
- Opre – Hallgatók csoport olvasás jog, öröklődik
  - Eloadasok – Előadók csoport módosítás jog, öröklődik

• Hozzunk létre egy fájlt az Eloadasok könyvtárban, és nézzük meg, hogy gipszj-nek milyen effektív joga van rá. Itt látszik, hogy az egyes egyszerű jogok (Teljes hozzáférés, Módosítás, Olvasás & Végrehajtás, Könyvtár tartalmának listázása, Írás, Olvasás) milyen elemi engedélyekből állnak össze.
• Adjuk hozzá a fájlhoz gipszj-t: tiltsuk meg az írást. Így is nézzük meg az effektív jogokat.

Engedélyezési lehetőségek a Windowsban

- Rendszerszintű jogosultságok
- Discretionary Access Control
- **Mandatory Integrity Control**
  - kötelező, erőforrás szintű, címkézés

DEMO Mandatory Integrity Control

- Vista funkció
- Folyamatok megkülönböztetése: védelem az általunk indított, nem megbízható folyamatok ellen
- Alapból minden fájlnak Medium címkéje van
- Internet Explorer használja:
  - IE folyamata Low integritási szint (lásd Process Explorer, Integrity Level oszlop)
- `icacls /setintegritylevel H|M|L`
  - „No write up” kipróbálása

Windows Vista Integrity Mechanism Technical Reference,
http://msdn.microsoft.com/en-us/library/bb625964.aspx

Rendszergazda cmd-ből:

```
echo „High integrity information, only restricted modification” >> high.txt
icacls high.txt /setingegritylevel H
icacls high.txt
        ‘ kimenet:
        C:\temp>icacls high.txt
                high.txt BUILTIN\Rendszergazdák:(I)(F)
                NT AUTHORITY\SYSTEM:(I)(F)
                BUILTIN\Felhasználók:(I)(RX)
                NT AUTHORITY\Hitelesített felhasználók:(I)(M)
                Kötelező címke\Magas kötelező szint:(NW)

‘ alacsony integritású cmd indítása
psexec –l cmd.exe
```

Alacsony integritású cmd-ből:

echo „módosítás” >>high.txt

A hozzáférés megtagadva.

(Integritási címke megváltoztatásához SeRelabelPrivilege jogosultság kell.)

Biztonsági feladatok a Windowsban

- Hitelesítés (authentication)
  - Birtok / tudás / biometria
  - Pl. Bejelentkezési képernyő, hitelesítő ablakok
- Engedélyezés (authorization)
  - Alapelv: mindig *csoportnak* osztunk jogot
  - Pl. Biztonsági házirend, fájl ACL
- **Auditálás**
  - **Biztonsági naplózás**

Eseménynapló

- Rendszer és alkalmazás üzenetek
- Bejegyzés:
  - Típus, idő, forrás, ID, leírás
- Napló felülírása:
  - Ciklikus, időnként, soha

DEMO Auditálás

- Naplózási házirend
- Biztonsági eseménynapló tartalma
- Jogok, pl. SeSecurityPrivilege használata

Biztonsági napló eseménye:
- házirendben megadjuk, hogy a sikertelen belépéseket naplózza
- RunAs paranccsal próbálunk indítani valamit, és hibás jelszót adunk meg

Pl. „Manage auditing and security log (SeSecurityPrivilege): Allows a user to specify object access auditing options for individual resources such as files, Active Directory objects, and registry keys. Object access auditing is not actually performed unless you have enabled it in Audit Policy (under Security Settings , Local Policies). A user who has this privilege also can view and clear the security log from Event Viewer.
By default, this privilege is assigned to Administrators.”

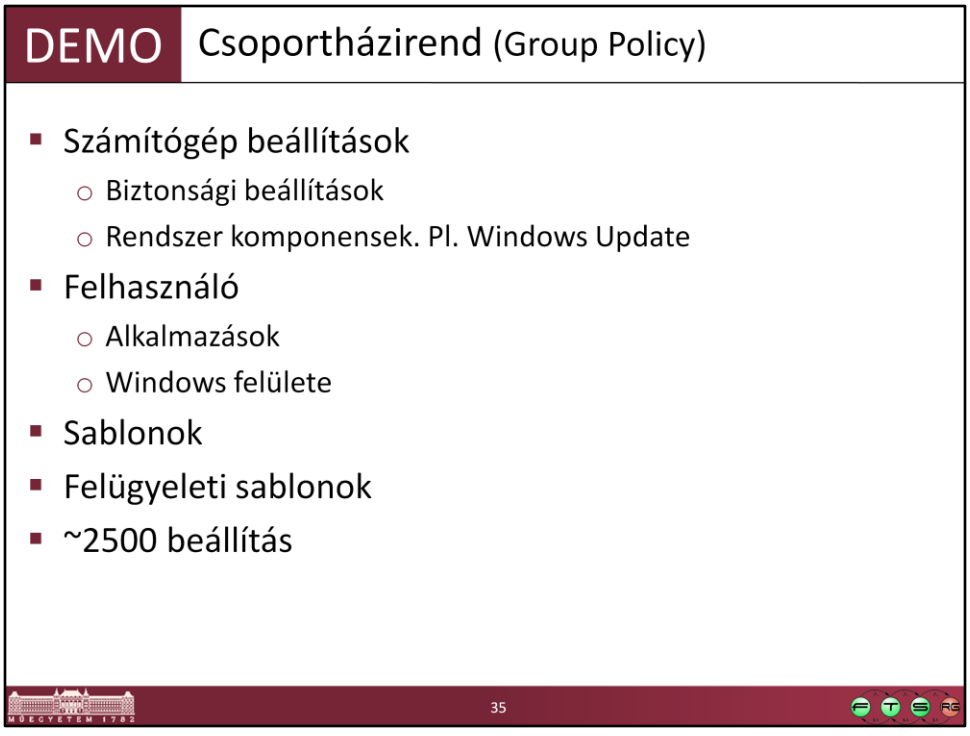
Egyéb biztonsági funkciók

- Letöltött fájlok blokkolása (Properties / Unblock)
- RunAs parancs
- User Account Control (UAC)

Egyéb funkciók, amiről érdemes tudni.

DEMO User Account Control, Runas

- Adminisztrátor felhasználó veszélyei
- Korlátozott felhasználóval dolgozni
  - Windows XP alatt kényelmetlen volt
  - Run as… és runas parancs
  - Ha nincs Run as..: bal SHIFT + jobb gomb
- Vistaban tervezéskor figyeltek rá: UAC



Ez nem kifejezetten biztonság, inkább menedzselhetőség. Az operációs rendszer és a programok beállításait szabályozhatjuk központilag, egy helyről. Tartományi környezet esetén akár több száz gép és több ezer felhasználó esetén lehet ugyanúgy egy helyről szabályozni a beállításokat.

Group Policy Settings Reference Windows Vista (http://www.microsoft.com/downloads/details.aspx?FamilyID=41dc179b-3328-4350-ade1-c0d9289f09ef&DisplayLang=en): XLS táblázat az összes csoportházirend beállítási opcióról

Összefoglalás

- Hitelesítés
  - felhasználók tárolása, azonosítása, SID
- Engedélyezés
  - Fajtái, jogosultságok, ACL-ek
- Naplózás
  - Eseménynapló, házirendek

További információ

- Mérés laboratórium 4. segédlet
  - http://www.mit.bme.hu/oktatas/targyak/vimia315/jegyzet/
    Windows segédlet