A Windows új biztonsági lehetőségei

Dr. Sipos Marianna
ZMNE BJKMK

Tömeges felhasználás

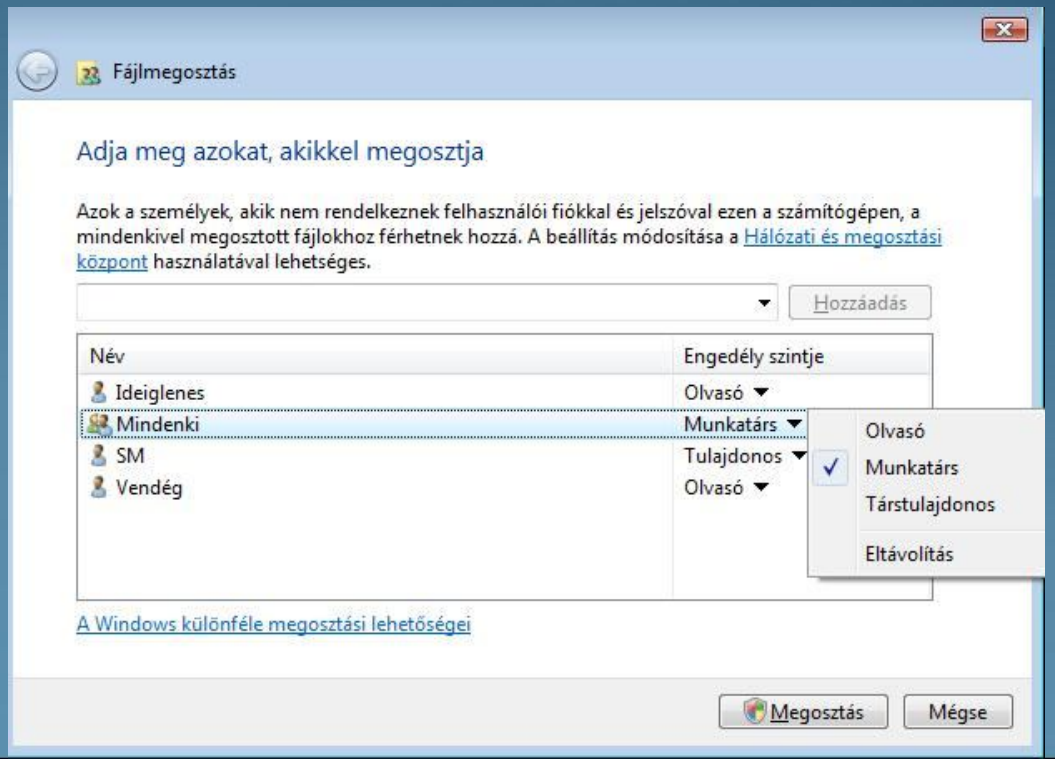
- Eredeti cél:
  - Desctop alkalmazások mindenkinek
  - Egyedi géphasználat
  - Kényelmes, felhasználóbarát felület
- Mit áldoztak fel:
  - Hozzáférés szabályozás minimális szinten.
  - Laikus felhasználók még a létező lehetőségekkel sem élnek.

  - Különböző felhasználók, akik egymás mappáihoz hozzáférnek.

Az internetelérés fejlődésével hozzáférés a hálózaton keresztül

Használt biztonsági megoldások a .NET előtt

- Nyilvános mappa
  - Alapértelmezésben más gépekről csak ez elérhető
  - Mappa megosztás lehetősége különböző jogosultságokkal



Használt biztonsági megoldások a .NET előtt

- Felhasználói jogok korlátozása
  - Többnyire a rendszer megőrzése érdekében
  - Bizonyos mappák módosításának megtiltása
  - Nincs egyénre szabás
  - Van rendszergazda és általános felhasználó.
- Már ez is mutatja a szűk lehetőségek szűkös felhasználását.

A .NET futtatókörnyezet szolgáltatásai „sokkolták” a felhasználók egy részét. A számos bírálat ellenére, talán túl gyorsan érkezett? Vagy a felhasználói tömegek nem igénylik?

A .NET Framework beépült

- Windows 3.1 a DOS alól volt indítható.
- Windows 95 / NT már önálló operációs rendszerek

- .NET Framework letölthető az XP és Windows 2000-hez
- Vista és Windows7 már tartalmazza.

- Természetesen a régi szoftverek nem készülhettek fel a .NET által később biztosított lehetőségekhez
- Természetesen régi szoftvereinket használni akarjuk.
- A .NET biztonsági lehetőségeit használva be kell állítanunk őket, vagy használatuk közben engedélyezni.

. NET Hozzáférés-szabályozás

Hálózaton vagy a számítógépen található objektumok elérésének engedélyezése felhasználók, csoportok, számítógépek részére.

- Szerep-alapú biztonság
- Kóderedet-alapú biztonság

A szabályozás elemei

- Engedélyek
- Objektumok tulajdonjoga
- Engedélyek öröklődése
- Felhasználói jogok
- Objektumok naplózása

Engedélyek

Hozzárendelhetők:

- Felhasználóhoz
- Csoporthoz
- Számítógéphez

Szabályozható objektumok

- Fájlok, mappák
- Active Directory objektumok
- Beállításjegyzék objektumok (registry)
- Rendszerobjektumok (pl. folyamatok, feladatütemező, nyomtatásvezérlés, loggolás)

Az objektum típusa határozza meg, milyen engedély adható.

Általában hozzárendelhető:

- Olvasás
- Módosítás
- Új tulajdonos engedély
- Törlés

Az NTFS-engedélyek hozzáférési korlátozásai

Speciális engedélyek	Teljes hozzáfér	Módosít	Olvas és végrehajt	Mappa tartalomlista	Olvasás	Írás
Mappa bejár, fájl végrehajt	x	x	x	x		
Mappa lista, adat olvas	x	x	x	x	x	
Attribútum olvasás	x	x	x	x	x	
Kiterj. Attribútum olvasás	x	x	x	x	x	
Fájl létrehoz, ír	x	x				x
Mappa létrehoz, adat fűz	x	x				x
Attribútum írása	x	x				x
Kiterj. Attribútum. írása	x	x				x
Almappák és fájlok törlése	x					
Törlés	x	x				
Engedély olvasása	x	x	x	x	x	x
Engedély módosítása	x					
Saját tulajdonba vétel	x					
Szinkronizálás	x	x	x	x	x	x

Szerepalapú biztonság
Role Based Security (RBS)

Felhasználókra, felhasználói csoportokra (szerepekre) vonatkozó előírások

A Windows alapértelmezett csoportjai

- Hitelesített felhasználók
- SYSTEM
- Rendszergazdák
- Felhasználók

Felhasználói fiókok felügyelete UAC (User Account Control)

- Segít megelőzni a számítógépen végzett nem engedélyezett változtatásokat.
- Az UAC előbb engedélyt kér. (Ha van az adott felhasználónak rendszergazdai jogosultsága, megkapja.) Ha nincs a felhasználónak engedélye: egy rendszergazdai jelszót kér, hisz a rendszergazdáknak is javasolt a nem rendszergazdai jogosultságokkal történő géphasználat.
- Segít megelőzni rosszindulatú szoftverek (malware), kémprogramok telepítését.

UAC üzenetek

- **A Windows a beleegyezését kéri a folytatáshoz**

  Amikor olyan Windows programot futtatunk, mely hatással van más felhasználók adataira.

- **Egy programnak engedélyre van szüksége a továbblépéshez**

  Ha a futtatni kívánt program rendelkezik digitális aláírással, mely tartalmazza a nevét és a kiadó nevét. Eldönthetjük megbízunk-e benne.

- **Egy azonosítatlan program kér hozzáférést a számítógéphez**

  Ha a futtatni kívánt program nem rendelkezik digitális aláírással, nem azonosítható. Döntsük el , hogy megbízunk-e benne.

- **Ez a program le van tiltva**

  A rendszergazda által letiltott program. Ha szüksége van rá, kérjen engedélyt a futtatáshoz.

A számítógép megóvása érdekében hozzon létre általános jogú felhasználói fiókot minden személy számára, aki a számítógépet használja.

Kóderedet-alapú biztonság

Code Access Security (CAS)

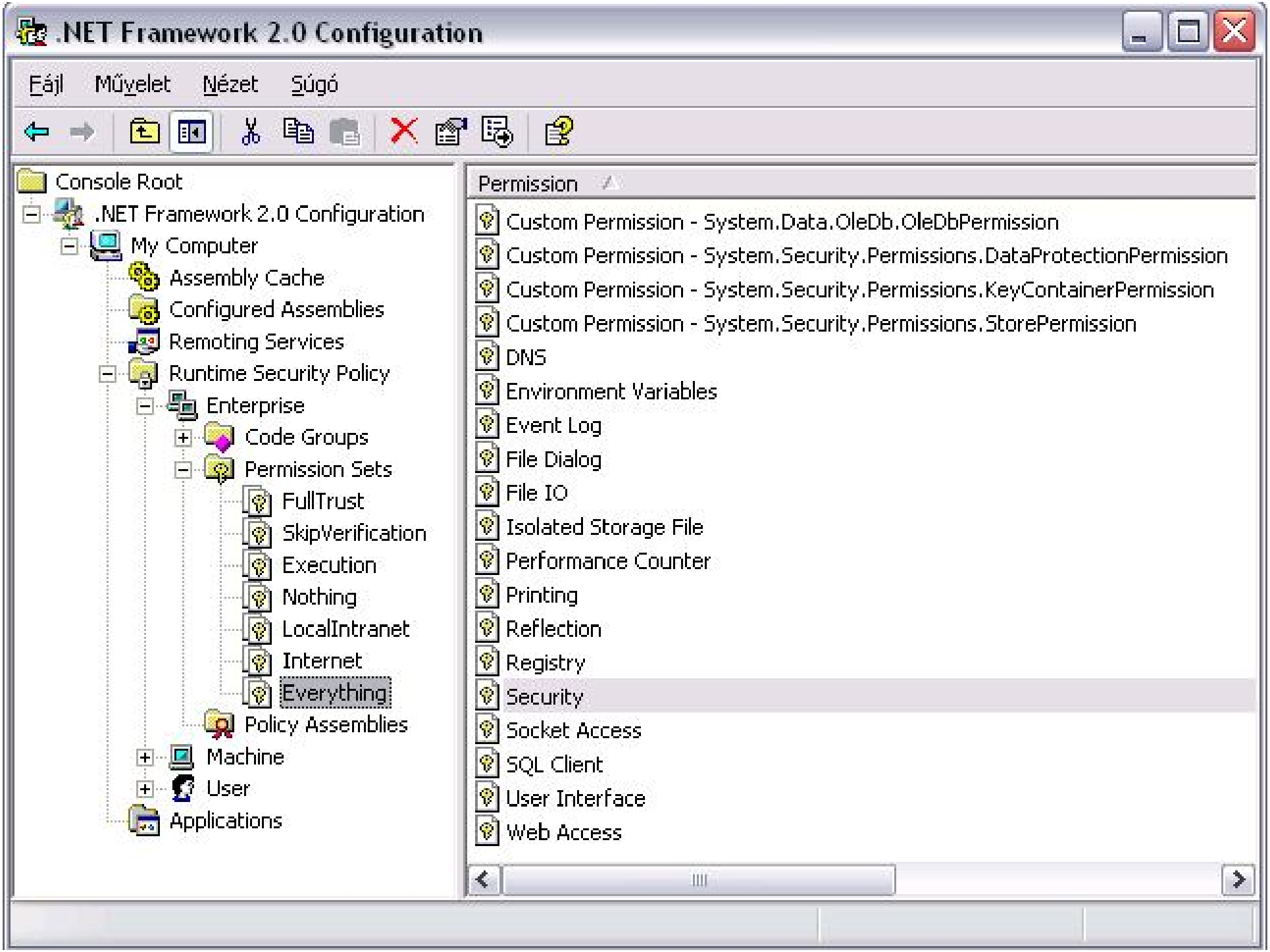
Az alkalmazás jogosultságát nézi, nem a felhasználóét. Tanúsítvány ellenőrzés.

A szerepalapú biztonsággal nem korlátozható hozzáférések is ellenőrizhetők

- Az adott alkalmazás tud vagy nem tud Web kérést küldeni az internetre.
- Egy alkalmazás kérhet vagy nem DNS-t

7 alapértelmezett engedélyhalmaz

- FullTrust: Nem ellenőrzi a CAS
- SkipVerification: Elkerülheti az ellenőrzést. Javítja a teljesítményt, feláldozza a biztonságot.
- Execution: Csak futhat.
- Nothing: Még csak nem is futhat.
- LocalIntranet
- Internet
- Everything: Összes standard, beépített engedély. Abban különbözik a FullTrust-tól, hogy a CAS ellenőrzés végrehajtódik rajta.


.NET Framework 2.0 Configuration
Fájl
Művelet
Nézet
Súgó
Console Root
.NET Framework 2.0 Configuration
My Computer
Assembly Cache
Configured Assemblies
Remoting Services
Runtime Security Policy
Enterprise
Code Groups
Permission Sets
FullTrust
SkipVerification
Execution
Nothing
LocalIntranet
Internet
Everything
Policy Assemblies
Machine
User
Applications
Permission
Custom Permission - System.Data.OleDb.OleDbPermission
Custom Permission - System.Security.Permissions.DataProtectionPermission
Custom Permission - System.Security.Permissions.KeyContainerPermission
Custom Permission - System.Security.Permissions.StorePermission
DNS
Environment Variables
Event Log
File Dialog
File IO
Isolated Storage File
Performance Counter
Printing
Reflection
Registry
Security
Socket Access
SQL Client
User Interface
Web Access

Internet / Intranet

- Internet alapértelmezett engedélyei:
  - File Dialog
  - Isolated Storage File
  - Security
  - User Interface
  - Printing
- Local Intranet zone
  - Environment Variables
  - File Dialog
  - Isolated Storage File
  - Reflection
  - Security
  - User Interface
  - DNS
  - Printing

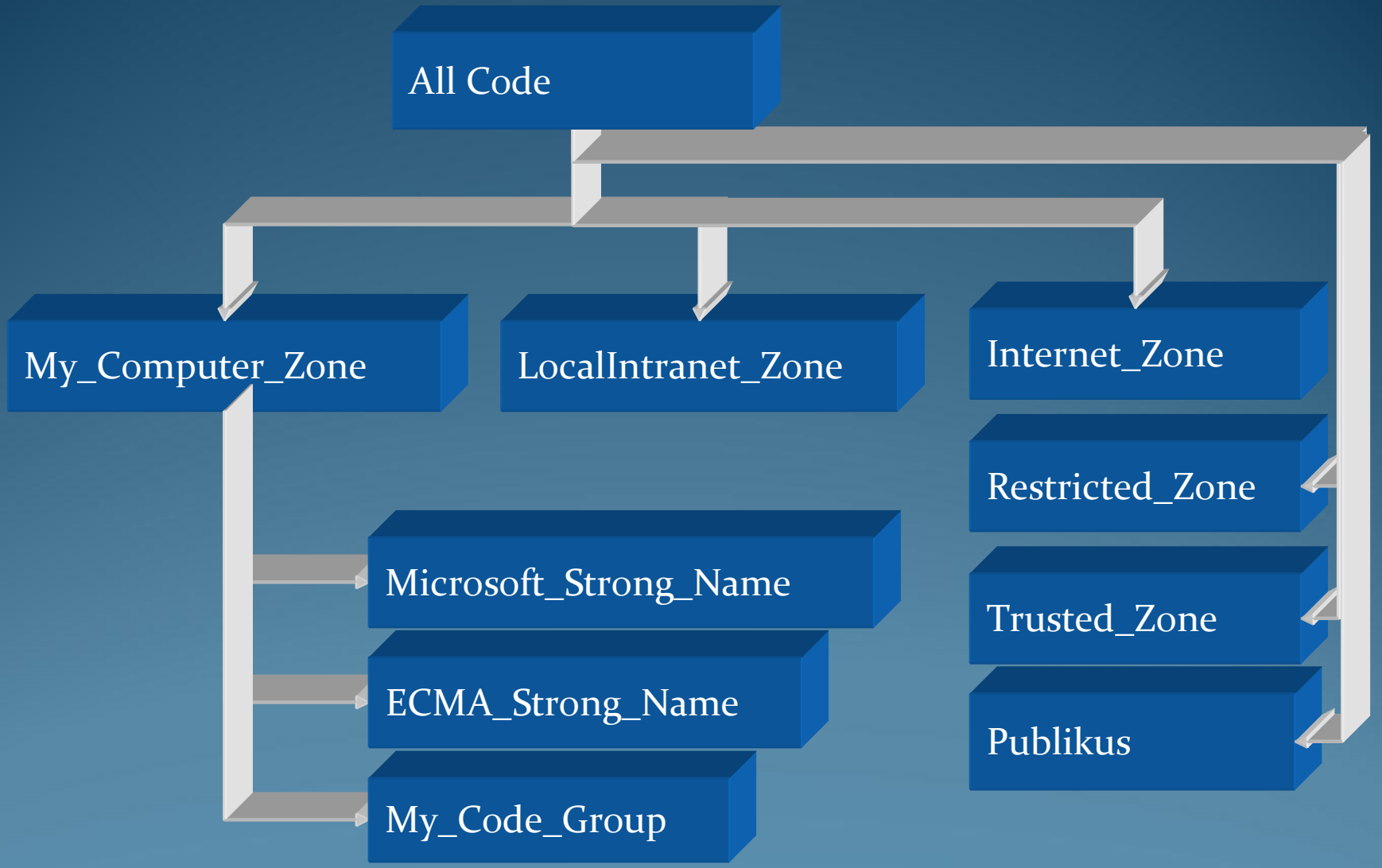
Tanúsítvány (Evidence)

- Futásidejű információ gyűjtemény egy assemblyről, hogy meghatározzuk mely kódcsoporthoz tartozik.
- Általában tartalmazza a könyvtárat vagy Web oldalt ahonnét az assembly-t futtatjuk.
- Tartalmazhat digitális aláírásokat.

Tanúsítvány típusok

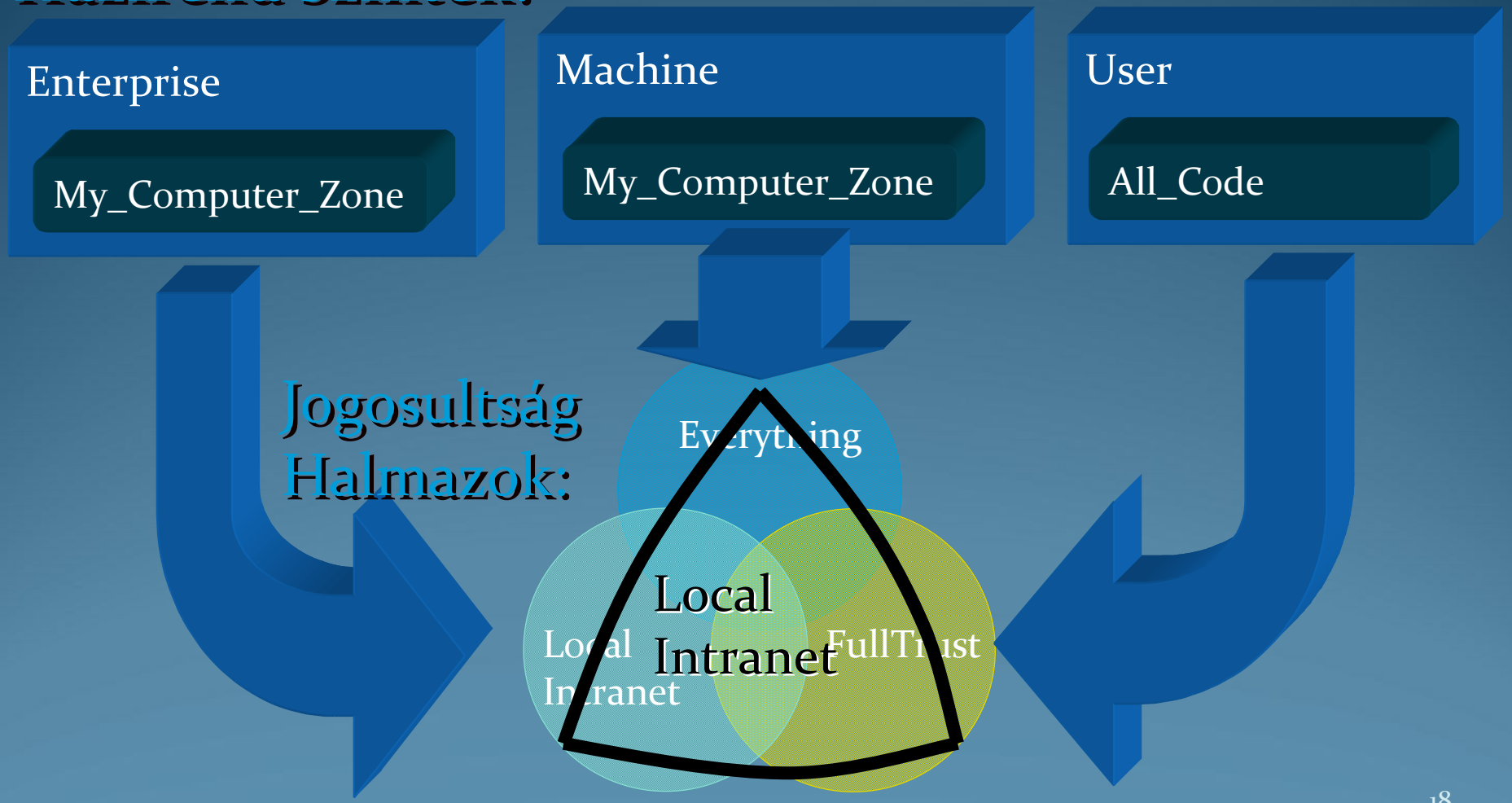
- System.Security.Policy névtér osztályai
  - Application Directory: Ahol az assembly található.
  - Hash: Az assemblyt egyedileg azonosító kriptográfiai hash-kód. Minden módosítás érvénytelenné teszi az assembly hasht.
  - Publisher: A fejlesztőt azonosító digitális aláírás. Alá kell írni az assemblyt hozzá.
  - Site: Az oldal ahonnét letöltöttük.
  - Strong Name: A kriptográfiai erős név, mely az assemlyt azonosítja. Használatához alá kell írni az assemblyt.
  - URL: Az oldal URL-je ahonnét letöltöttük.
  - Zone: A zóna amiben az assemly fut. (Internet, Intranet…).

Kódcsoportok



CAS érvényesítés a gépen futó assemblykre (My_Computer zóna)

Házirend Szintek:



Köszönöm a figyelmet!

sipos.marianna@zmne.hu

Kérdések?