MI-SP-SP-3 (MI-BPR.16) (přednáška 7 a 8)

Úrovně bezpečnostních oprávnění. Běh programu při nízkých oprávněních.

ACL - access control list

→ obsahuje ACE (entry) - každá identifikuje entitu (SID) a přístupová práva

- securable objects (každý objekt, který se dá zabezpečit)

- jen některé FS umí ACL : NTFS
- pořadí pravidel je důležité!
  - jde se od objektu do příček, zamítnutí se kontroluje první

POSIX: getfacl, setfacl

- rozšíření standardního modelu práv

  user : name : rwx

  group : name : rwx

Access Token - popisuje bezpečnostní kontext procesu nebo vlákna

- každý uživatel musí po přihlášení svůj token → jím spuštěné procesy mají svůj primární token
  - všechny se spouští s určitým hlavním tokem
  - dá se vynutit i spuštění s jiným tokenem (mají to kvůli běhu služby OS)

→ omezený token ← odebrání některých práv

- OS používá SID uložené v tokenu při spouštění procesu

- každý program má dělat jen to, co má a nic víc → vzdát se ostatních práv
- pokud potřebujeme větší oprávnění, můžeme ji spustit v procesu vedle
  → výrazně větší napadnutelnost

proč potřebují vyšší práva:

- kvůli ACL: zápis na místo, kam může pouze administrátor, zápis do registrů HKEY_LOCAL_MACHINE
  → nejsou místa kam mohou zapisovat všichni (i registry), rozvolnění ACL
- kvůli právům: → lepší přidat uživatele do skupiny než ho nechat dělat administrátorem

⊳ kvůli LSA secrets (Local System Authority)

- uživatel musí být ve skupině administrátorů

→ skutečně toto potřebujeme

- každé ACE by mělo být odůvodněné → ostatní odstranit

- zjistím co všechno používám a ke všemu definuji úroveň přístupu potřebnou

→ měnit za běhu

- zjistit všechna SID v tokenu a odstranit nepotřebná

→ omezení tokenu

UAC - User Account Control

- pro každého uživatele je při přihlášení vytvořený token

→ pro administrátory druhý se zeslabenými právy - to spustí explorer.exe

→ možná elevace na administrátora

prompt for consent / prompt for credentials (consent.exe)

Application Information service - spustí consent.exe a kontroluje výsledek

- ten kontroluje co je soubor zač

+ elevuje práva automaticky pro některé Microsoft soubory

- spustí prompt v zabezpečeném okně

→ pokud je souhlas udělen, je do procesu zkopírován plnohodnotný token z procesu

Virtualizace pro starší aplikace

→ povolí některé věci ve vlastním virtuálním prostoru