Dejte mi práva na...

ACL a řízení přístupu ve Windows
skrz naskrz

Patrik Malina
patrikmalina.eu

O čem bude řeč

- Co je a jak vypadá ACL
- Kde všude jsou ACL
- Co vypadá jako ACL, ale není ACL
- Mechanismy uplatnění ACL
- Nástroje pro správu ACL
  - Grafika
  - Příkazové rozhraní
  - Automatizace pomocí skriptů
- Jak na správu ACL prakticky

O čem bude řeč

- Konkrétní správa
  - Souborový systém
  - Sdílení
  - Active Directory
  - Služby
  - Tiskárny
  - Registry
  - Exchange 2003
  - Exchange 2007
  - IIS
  - ...
  - MS Office Sharepoint

O čem bude řeč

- **Co je a jak vypadá ACL**
- Kde všude jsou ACL
- Co vypadá jako ACL, ale není ACL
- Mechanismy uplatnění ACL
- Nástroje pro správu ACL
  - Grafika
  - Příkazové rozhraní
  - Automatizace pomocí skriptů
- Jak na správu ACL prakticky

Co je ACL

- Principiálně
  - Mechanismus řízení přístupu ke zdrojům
    - Seznam „vyvolených“ – identity s oprávněním k přístupu, případně s bližším určením
- Technologicky
  - Seznam logicky přiřazený zdroji
    - Tabulka v paměti používaná vlákny procesu
    - Binární struktura s SID a přístupovou „maskou“

Co je ACL

- Z pohledu OS
  - Řízení přístupu vláken na objekty
    - Vlákno (thread) – základní jednotka „běhu“ v systému
      - Dědí identitu od procesu
    - Obecný zabezpečitelný objekt s potřebnými popisnými informacemi
      - NTFS
      - Tiskárny
      - …

Co je ACL

- Z pohledu programátora v OS
  - ACL je
    - Univerzální mechanismus na různorodých objektech
    - Je zprostředkován a zapouzdřen prostřednictvím Windows API

```
Private Declare Function RegGetKeySecurity Lib "advapi32.dll„
```


Co je ACL

- Z pohledu skriptujícího administrátora
  - ACL je
    - Kolekce objektů použitelná pomocí metod a vlastností
    - Rozhraní dosažitelné použitím příslušných knihoven
      - NTFS – ADsSecurity.dll
      - Exchange 2003 – CDOEX.dll

Jak vypadá ACL

- Pohled z různých výšek

Poctivý „oknař“

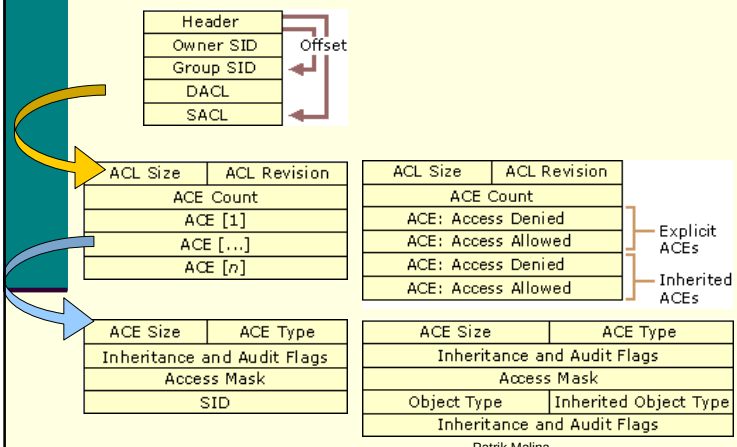
Umírněný inovátor

Skriptař a shellman

Aplikační programátor

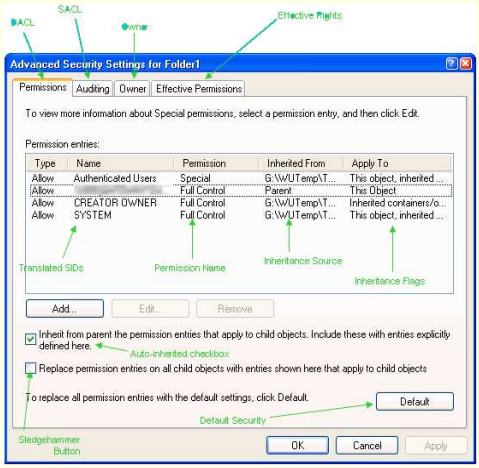
Jak vypadá ACL

- Pohled schematický



Jak vypadá ACL

- Pohled „pro lidi“
  - Editory ACL
    - Určeny pro běžnou, „nahodilou“ správu



Jak vypadá ACL

- Ještě pořád text…
  - **S**ecurity **D**escriptor **D**efinition **L**anguage
    - Textový řetězec jako varianta zápisu
      - Powershell: Get-Acl | fl
      - Security templates

```
"c:\windows\system32", 2,
"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"


"w32time", 3,
"D:(A;;CCLCSWLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPL
O;;;IU)(A;;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

Jak vypadá ACL

- Už jen bity a bajty…
  - Struktura ACL
    - zahrnuje masku přístupu (access mask)
      - 4bajtové číslo
      - Jednotlivé bity pracují jako řídící příznaky
      - Je spojena s konkrétním SID
      - Je spojena s příznakem:
        - Deny
        - Allow
        - Audit

O čem bude řeč

- Co je a jak vypadá ACL
- **Kde všude jsou ACL**
- Co vypadá jako ACL, ale není ACL
- Mechanismy uplatnění ACL
- Nástroje pro správu ACL
  - Grafika
  - Příkazové rozhraní
  - Automatizace pomocí skriptů
- Jak na správu ACL prakticky

Kde všude jsou ACL

- Souborový systém NTFS
  - Dva typy objektů
  - Uplatnění hierarchie a dědičnosti
  - Problém zachování při přenosu souborů
  - „Klasické“ řízení přístupu
- Registry
  - Hierarchie klíčů
  - Řízení přístupu k hodnotám

Kde všude jsou ACL

- Sdílení (shares)
  - „Vykopávka“ služby LanMan
  - Slabá granularita
  - Řízení síťového přístupu
- Tiskárny
  - Kontrola připojení ke službě
  - Pozor na souvislost se službou spooler

Kde všude jsou ACL

- Služby (services)
  - Řízení činnosti služby
  - Žádná hierarchie
  - Dostatečné možnosti
    - Start, stop, pause
    - Change startup type
    - Read/Query
  - Bez výchozí grafické konfigurace
    - Security templates
    - Příkazový řádek, skripty

Kde všude jsou ACL

- WMI
  - Řízení přístupu ke službě Mgmt
  - Hierarchie dle WMI „namespaces“
  - Vymezení možnosti inventarizace sítě
- IIS Metabase
  - „Další“ konfigurační databáze
  - Významem odpovídá zhruba registry
  - Hierarchie, dědičnost
  - MetaACL.exe

Kde všude jsou ACL

- Active Directory
  - Propracovaný model zabezpečení
    - Hierarchické uspořádání
    - Možnost nastavení na úroveň atributu či jejich skupin
    - Dědičnost
    - Pomocné nástroje – Delegation wizard

Kde všude jsou ACL

- Poštovní schránky (Exchange)
  - Kombinované řízení
    - „Přístupový“ záznam uživatele – v AD
    - ACL na schránce – mail store
    - Nebezpečí narušení synchronizace
      - Opatrně při skriptování

Kde všude jsou ACL

- Objekty jádra Windows
  - Speciální objekty nízké systémové úrovně
  - Určeny k pokročilému programování
  - Při běžné správě bezvýznamné

O čem bude řeč

- Co je a jak vypadá ACL
- Kde všude jsou ACL
- **Co vypadá jako ACL, ale není ACL**
- Mechanismy uplatnění ACL
- Nástroje pro správu ACL
  - Grafika
  - Příkazové rozhraní
  - Automatizace pomocí skriptů
- Jak na správu ACL prakticky

Co vypadá, ale není ACL

- Poštovní schránky (Exchange)
  - Právo Send On Behalf
    - Ve skutečnosti příznak (atribut) v Active Directory (LDAP) – „publicDelegates“

Co vypadá, ale není ACL

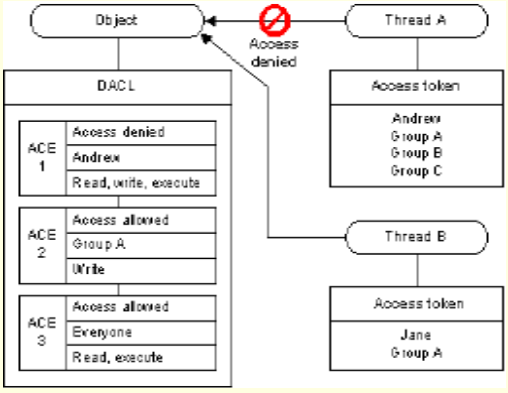
- MS Office Sharepoint
  - Velmi propracovaný systém
  - Přístupová práva řešena na aplikační úrovni
  - Záznamy o přístupu v databázi SQL
  - Vlastní systém skupin a dědění
  - Vztah k aplikačním objektům (sites, webparts…)

O čem bude řeč

- Co je a jak vypadá ACL
- Kde všude jsou ACL
- Co vypadá jako ACL, ale není ACL
- **Mechanismy uplatnění ACL**
- Nástroje pro správu ACL
  - Grafika
  - Příkazové rozhraní
  - Automatizace pomocí skriptů
- Jak na správu ACL prakticky

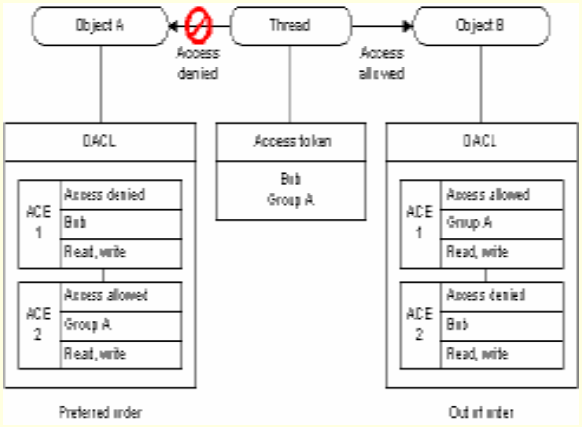
Mechanismy uplatnění ACL

- Jak pracuje DACL – přednost



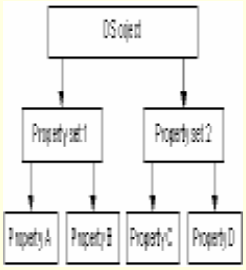
Mechanismy uplatnění ACL

- Jak pracuje DACL – pořadí



Mechanismy uplatnění ACL

- Jak pracuje DACL – objekt DS a properties

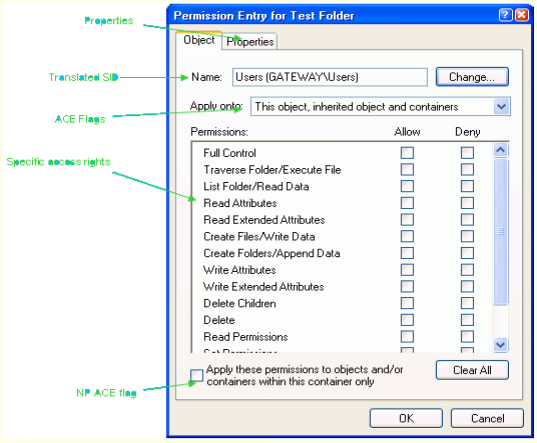


O čem bude řeč

- Co je a jak vypadá ACL
- Kde všude jsou ACL
- Co vypadá jako ACL, ale není ACL
- Mechanismy uplatnění ACL
- **Nástroje pro správu ACL**
  - Grafika
  - Příkazové rozhraní
  - Automatizace pomocí skriptů
- Jak na správu ACL prakticky

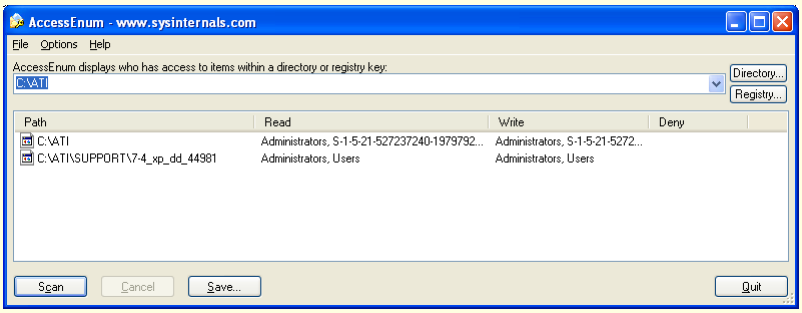
Nástroje pro správu ACL

- Grafika – Windows



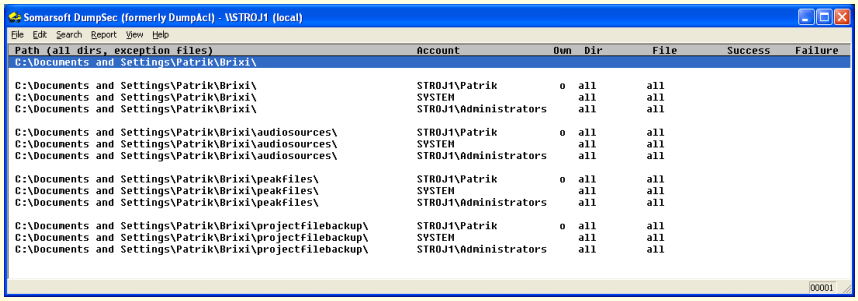
Nástroje pro správu ACL

- Grafika – Sysinternals
  - AccessEnum



Nástroje pro správu ACL

- Grafika – SomarSoft
  - DumpSec
    - http://www.somarsoft.com/



Nástroje pro správu ACL

- Příkazové rozhraní – MS
  - NTFS – nastavení
    - Cacls.exe
    - XCacls.exe
    - ICacls.exe

```
xcacls c:\temp

xcacls *.* /g Uzivatel:rwed;rw /e

xcacls *.* /g Uzivatel:r;trw /e

xcacls "F:\Directory" /e /g "Domain Users":R /y
```


Nástroje pro správu ACL

- Příkazové rozhraní – MS
  - NTFS – přenos
    - Robocopy

```
robocopy \\zdroj \\cil /MIR /COPY:DATSOU /V /LOG:C:\robocopy.log /Tee

/COPY:copyflag[s] : What to COPY (default is /COPY:DAT).
                    (copyflags : D=Data, A=Attributes, T=Timestamps).
                    (S=Security=NTFS ACLs, O=Owner info, U=aUditing
info).

/SEC : Copy files with SECurity (equivalent to /COPY:DATS).
```

Nástroje pro správu ACL

- Příkazové rozhraní – MS
  - Různé typy objektů
    - SubInACL
      - Univerzální robustní nástroj
      - Velmi pokročilé možnosti
      - Komplikovanější syntax
      - Výborná podpora pro migrace a záměny identit

Nástroje pro správu ACL

- Příkazové rozhraní – MS
  - Různé typy objektů – SubInACL

```
subinacl /file c:\temp /display

subinacl /service CPUCooLServer Service /display

subinacl /file C:\TEST.TXT /owner=DOMAIN1\USER1

subinacl /subdirectory C:\*.* /changedomain=domain1=domain2
```

Nástroje pro správu ACL

- Příkazové rozhraní – MS
  - Active Directory
    - DSacls.exe
      - Univerzální nástroj
      - Nesnadná syntax
      - dsacls <somedn> /I:T /G "<somedomain\somegroup>:CA;Reset Password;"

Nástroje pro správu ACL

- Příkazové rozhraní – MS
  - Active Directory
    - Acldiag.exe
      - Možnost nápravy po změnách – kontrola oproti schématu
      - Acldiag <DN> /schema
        Dsacls <DN> /s

Nástroje pro správu ACL

- Příkazové rozhraní – MS
  - MS Exchange 2007
    - Založeno na Powershellu

```
Add-MailboxPermission „Schranka1" -AccessRights FullAccess -
user „Uzivatel01„
```

```
Add-ADPermission „Schranka01" -User „Uzivatel01" –AccessRights
extendedright -ExtendedRights "send as"
```


Nástroje pro správu ACL

- Příkazové rozhraní – neMS
  - SetACL
    - Nastavení, záloha ACL
    - Pro řadu typů objektů
    - Velmi pokročilé možnosti
    - Přehledná syntax
    - Objektový model – přístup přes COM (WSH)
    - Dobrá nápověda

Nástroje pro správu ACL

- Příkazové rozhraní – neMS
  - SetACL – příklady

```
SetACL.exe -on "\\server1\share1\my dir" -ot file -actn ace
           -ace "n:domain1\user1;p:change"
           -ace "n:S-1-5-32-544;p:full;s:y"
           -ace "n:domain2\user2;p:full;m:aud_fail;w:sacl"
           -actn clear -clr "dacl,sacl"
           -actn rstchldrn -rst "dacl,sacl"

psexec \\server -c c:\setacl -on "MyService" -ot srv -actn ace
–ace "n:user;p:start_stop„
```


Nástroje pro správu ACL

- Příkazové rozhraní – neMS
  - Sysinternals – AccessChk
    - http://technet.microsoft.com/en-us/sysinternals/bb664922.aspx

```
7# C:\accesschk.exe "patrik" c: -q
RW C:\Documents and Settings\Patrik\.GalleryRemote
RW C:\Documents and Settings\Patrik\.SygateTmpYY
…
16# C:\accesschk.exe -k hklm\software -q | more
HKLM\software
  R  BUILTIN\Users
  RW BUILTIN\Power Users
  RW BUILTIN\Administrators
…
```

Nástroje pro správu ACL

- Příkazové rozhraní – neMS
  - Joeware.net – ADFind
    - http://www.joeware.net/freetools/tools/adfind/index.htm

```
adfind -default -f "(objectcategory=organizationalunit)" -sc
sdfilterns:FC -elapsed

dn:OU=Exchange,DC=joe,DC=com
>nTSecurityDescriptor: [DACL] ALLOW;;(FC);;;JOE\Domain Admins
>nTSecurityDescriptor: [DACL] ALLOW;;(FC);;;NT AUTHORITY\SYSTEM
>nTSecurityDescriptor: [DACL] ALLOW;(CONT
INHERIT)(INHERITED);(FC);;;JOE\Enterprise Admins
```


Nástroje pro správu ACL

- Skripty – obecně
  - Objektové rozhraní – ADSI
    - ADsSecurity.dll
    - Poměrně komplexní a komplikované
    - Dosti riskantní při chybách
  - Objektové rozhraní – Exchange
    - Cdoexm.dll
    - Podobné jako u ADSI

Nástroje pro správu ACL

- Skripty – obecně
  - Powershell
    - Čtení a zápis ACL pomocí cmdletů
    - Práce s ACL pomocí tříd .NET Frameworku
    - Přímočaré, dobře uchopitelné

Nástroje pro správu ACL

- Skripty – prakticky
  - XCacls.vbs
    - Předchůdce XCacls.exe
    - Dobrá ukázka postupů a technik
    - Hotový použitelný nástroj

Nástroje pro správu ACL

- Skripty – prakticky
  - Čistý skript WSH (mailbox)

```
AddAce dacl, sTrustee, 131073, _
       ADS_ACETYPE_ACCESS_ALLOWED, 2, 0, 0, 0

Function AddAce(dacl, TrusteeName, gAccessMask, gAceType, gAceFlags, gFlags,
gObjectType, gInheritedObjectType)

' Add the modified DACL to the security descriptor.
oSecurityDescriptor.DiscretionaryAcl = dacl

objUser.MailboxRights = oSecurityDescriptor ' Save new SD onto the user.

objUser.SetInfo
' Commit changes from the property cache to the information store.
```


Nástroje pro správu ACL

- Skripty – prakticky
  - Kombinace WSH a jiných nástrojů
    - Volání ze skriptů WSH (např. Vbs)

```
'strCurrentFolder = "patrik"
'strDomainName = "patrik-wkst"
…
strSetaclCommand = "setacl.exe
-on """ & strStorage & "\" & strCurrentFolder & """
-ot file -actn ace
-ace ""n:" & strDomainName & "\" & strCurrentFolder & ";p:full;i:so,sc;m:grant""
-actn setowner -ownr ""n:" & strDomainName & "\" & strCurrentFolder & """ -actn
setprot -op ""dacl:np"" -actn rstchldrn -rst ""dacl"""

objShell.Run (strSetaclCommand)
```

Nástroje pro správu ACL

- Skripty – prakticky
  - Powershell
    - Přenos ACL
      - Get-Acl test.txt | Set-Acl test2.txt
    - Tvorba ACE
      - $acl = Get-Acl c:\temp
        $permission = “domain\user”,”FullControl”,”Allow”
        $accessRule = New-Object `
        System.Security.AccessControl.FileSystemAccessRule $permission
        $acl.SetAccessRule($accessRule)
        $acl | Set-Acl c:\temp

Nástroje pro správu ACL

- Skripty – prakticky
  - Powershell
    - ACL důkladněji
      - $acl = get-acl test.txt
      - $acl | Get-Member

Zdroje informací

- Knihy
  - Microsoft Windows Internals
    - http://www.microsoft.com/mspress/books/6710.aspx

Zdroje informací

Internet

- Technet
  - Access Control
    - http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/w2rkbook/DistSystems.mspx?mfr=true
- Technet
  - New ACLs Improve Security in Windows Vista
    - http://technet.microsoft.com/en-us/magazine/cc138011.aspx
- MSDN
  - ACL overview
    - http://msdn.microsoft.com/en-us/library/ms229742.aspx

Zdroje informací

Internet

- The Code Project
  - The Windows Access Control Model Part 1
    - http://www.codeproject.com/KB/winsdk/accessctrl1.aspx
- TechTasks Code Center
  - Display object ACL (Perl)
    - http://techtasks.com/code/viewbookcode/1881
    - http://techtasks.com/code

Dotazy

- … a diskuse

Další informace

- Autor
  - http://www.patrikmalina.eu/
- Blog
  - http://patrikmalina.cz