Sami Laiho

Senior Technical Fellow, MVP

Adminize.com / Win-fu.com

sami@adminize.com @samilaiho

BLOG.WIN-FU.COM

How Windows Security Really Works?

Configuration Manager

Sami Laiho

Senior Technical Fellow
adminize.com

- IT Admin since 1996
- MCT since 2001 (MCT Regional Lead – Finland)
- MVP in Windows OS since 2011
- Specializes in and trains:
  - Troubleshooting
  - Security
  - Centralized Management
  - Active Directory
  - Hacking
  - Penetration testing
  - Social Engineering
- Trophies:
  - Ignite 2015 – Best male presenter ;) (#2 out of 1000 speakers)
  - TechEd Europe 2014 – Best session
  - TechEd North America 2014 - Best session, Best speaker
  - TechEd Australia 2013 - Best session, Best speaker
  - TechEd Europe 2013 - Best Session by an external speaker

Ratings

- Windows NT needs to work in a way to achieve different US standards
- Trusted Computer System Evaluation Criteria
  - The National Computer Security Center (NCSC) - part of NSA/DoD
  - http://csrc.nist.gov/publications/history/dod85.pdf
  - *1983 – referred to as the ”Orange book”*
- *The Common Criteria*
  - *1996 by* United States, United Kingdom, Germany, France, Canada, and the Netherlands

TABLE 6-1 TCSEC Rating Levels

Rating	Description
A1	Verified Design
B3	Security Domains
B2	Structured Protection
B1	Labeled Security Protection
C2	Controlled Access Protection
C1	Discretionary Access Protection (obsolete)
D	Minimal Protection

Security System Components

- **Security reference monitor (SRM)**
  - **Part of NTOSKRNL.exe that creates ad Access Token**
- **Local Security Authority subsystem (LSASS)**
  - **Responsible for the local policies and authenticating users**
  - **Windows 10 might move part of these to LSAISO**
- **LSASS policy database**
  - **HKLM\Security**
- **Security Accounts Manager (SAM)**
  - **Local accounts**
- **SAM database**
  - **Database for the previous**
- **Active Directory**
  - **Directory Service for Windows environments**

Security System Components

- **Authentication packages**
  - **LSASS DLL that check the passwords**
- **Interactive logon manager (Winlogon)**
  - **Logs users in**
- **Logon user interface (LogonUI)**
  - **Gathers the logon input with a credential provider**
- **Credential providers (CPs)**
  - **COM-object used to gather logon information**
- **Network logon service (Netlogon)**
  - **Communicates with the DC to create a Secure Channel for example**
- **Kernel Security Device Driver (KSecDD)**
  - **ALPC-calls with user mdoe**
- **AppLocker**
  - **White- and Blacklists for applications**

Protecting Objects

- SID
- Security Principal
- Access Token
- Security Descriptor
- Access Method Mask
- Integrity Levels
- Privileges
- User rights / Account rights

SID

- Security identifier
- Wellknown or ”unique”
  - Unique sids are never reused
- Most SID’s have a computer or domain specific part and a RID
  - RID’s start from 1000 so you can count the number of users created on a computer by Number=RID-1000+1
- Tools
  - Whoami /all
  - PSGETSID
- Format: S-R-I-S…
  - R=Revision level
  - I=48-bit authority identifier
  - S=variable number of sub-authority identifiers
  - The last part is the Relative Identifier (RID)

Well-known SIDs

- https://msdn.microsoft.com/en-us/library/cc980032.aspx

Some SID patterns

- Session ID: S-1-5-5-0-RID
- Service ID: S-1-5-80-SRVNAMEHASH
- Machine SID: S-1-5-21-x-y-z
- Local user SID: S-1-5-21-x-y-z-RID
- Mandatory Integrity Levels: S-1-16-x

Security Principal

- Someone who has a SID
- Object for permissions
- Users, Groups, Services, AD objects
  - Users are, Contacts aren’t
  - Security groups have SID’s, Distribution groups don’t

Access Token

- The ”keys”
- Parts
  - SID
  - SID’s of groups
    - One represents the Integrity Level
    - (Primary group for POSIX)
  - Privileges
  - Session ID
  - Claims
  - Default max size of tokens in Windows 8 increased to 48k
- Updated during logon
- Flag that tells if this is a primary or impersonation token
- Process ID that caused the creation of the token
- If the user has a ”super-power” or is part of a ”super-group” it will have two tokens
  - Normal
  - Restricted

Viewing an access token

- Whoami /all
- Process Explorer
- Debugger: **!token** *address*

Security Descriptor

- The ”Lock”
- Parts:
  - DACL – Discretionary Access Control List
    - Who can do what in what circumstances
  - SACL
    - Who should be audited for doing something
    - Integrity Level
    - Privilege required to edit
  - OWNER
    - User or groups who owns the resource
    - Creator by default
- Types:
  - Absolute or Self-Relative (not that important honestly)
- Control Bits: Inheritance level and some extra info
- To view in debugger:
  - !sd address & -8 (x86)
  - !sd address & -10 (x64)

Access Control Entries

- In DACL and SACL
- Contains
  - SID of trustee
  - Access Mask →
  - Inheritance mask

GR → Generic_Read
GW → Generic_Write
GE → Generic_Execute
GA → Generic_ALL
AS → Right to access SACL

String Security Descriptors

- "O:AOG:DAD:(A;;RPWPCCDCLCSWRCWDWOGA;;;S-1-0-0)”
- https://msdn.microsoft.com/en-us/library/windows/desktop/aa379570(v=vs.85).aspx

Privileges

- Control access to System resources and system-related tasks
  - ”Read the eventlogs”
  - ”Backup files”
  - Change the SACL
- Given through User Rights Assignment and some through Security Options
- Added to Access Token
  - Can be enabled or disabled
- Names: https://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx

Demo

Privilileges Beat Permissions

User Rights / Account Rights

- ”Allow Logon locally”, ”Deny logon locally” etc.
- Almost like privileges
  - Control access to securable objects
- Monitored by Local Security Authority
- Not added to tokens

Integrity Levels

- Since Windows Vista Mandatory Integrity Control has been one of most important parts of Windows Security
- Very poorly documented and spoken about
- Mandatory = Can’t be overriden
- Access control by trustworthiness of apps and the level of criticality of objects
- Based on the work by Kenneth J. Biba in 1975
  - https://en.wikipedia.org/wiki/Biba_Model
  - In general, preservation of data *integrity* has three goals:
    - Prevent data modification by unauthorized parties
    - Prevent unauthorized data modification by authorized parties
    - Maintain internal and external consistency (i.e. data reflects the real world)

Mandatory Integrity Control

- Trustworthiness is derived automatically
- Biba:
  - “Subject at a given level of integrity must not write to any object at a higher level of integrity (*no write up)”*
  - “Subject at a given level of integrity must not read an object at a lower integrity level (*no read down*)”
- Windows implementation:
  - **No Write Up** implemented – Lower integrity level process can’t write to higher level object
  - **No Read Down** not implemented
  - **No Read Up** implemented for reading process memory only, not objects

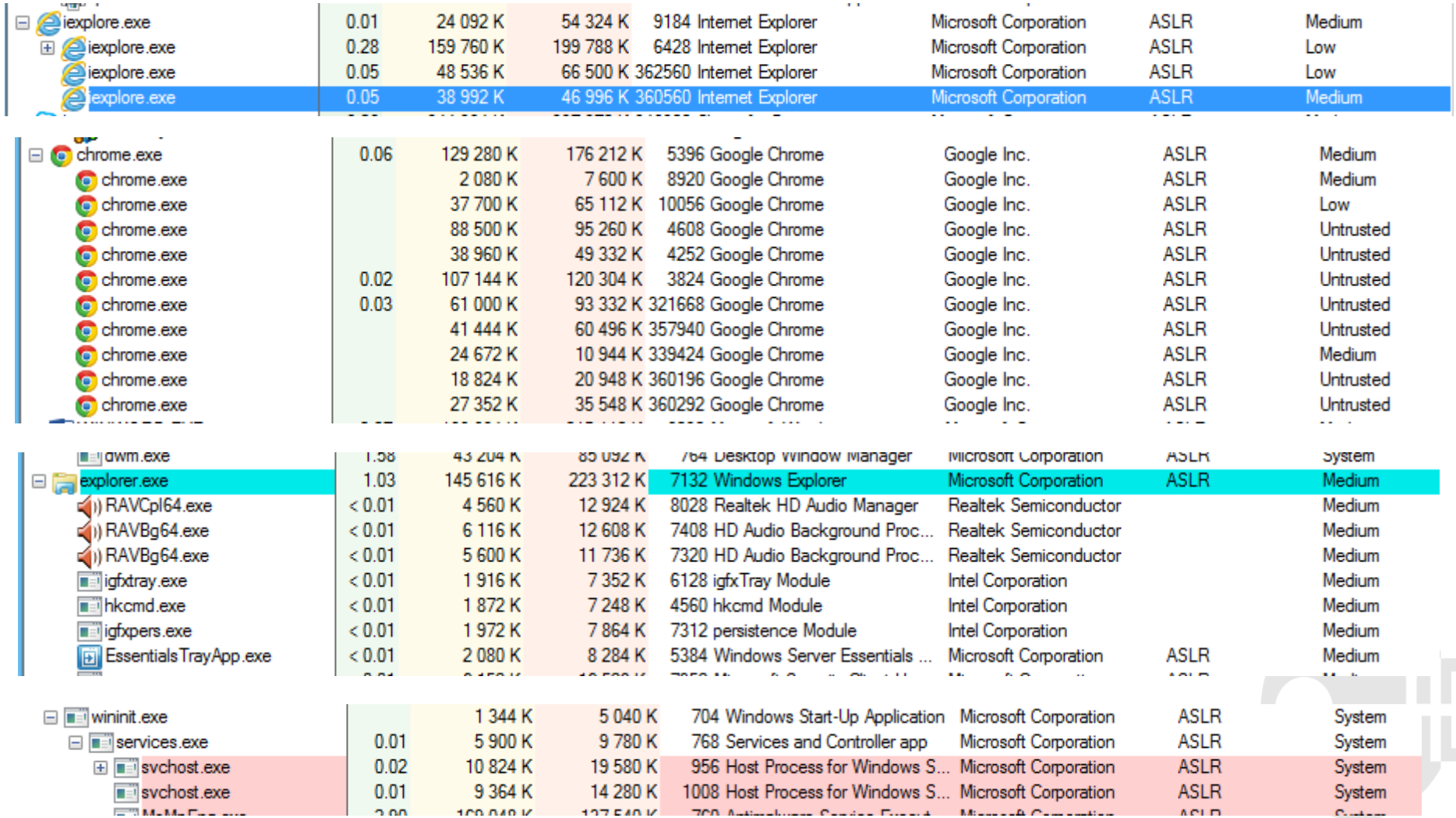
Integrity Levels

- Protected Access
  - Not currently in use
- System
  - LocalSystem account
- High
  - LocalService and NetworkService
  - Elevated admins
- Medium-High
  - Used by on-screen accessibility apps like on screen keyboard
- Medium
  - Authenticated user
  - Admin non-elevated
  - Explorer.exe
  - Trusted Internet Explorer
- Low
  - Everyone (World)
  - Untrusted Internet Explorer
- Untrusted
  - Anonymous Logins

Integrity Levels

- Identified by SIDs
  - Subjects denoted by a SID in their Access Token
  - Objects denoted by IL ACE in SACL
    - If not explicit then implicit Medium is the default
    - Objects created by Medium or higher are marked as Medium
    - Objects created by Low processes are marked as Low

Integrity level examples



iexplore.exe	0.01	24 092 K	54 324 K	9184 Internet Explorer	Microsoft Corporation	ASLR	Medium
iexplore.exe	0.28	159 760 K	199 788 K	6428 Internet Explorer	Microsoft Corporation	ASLR	Low
iexplore.exe	0.05	48 536 K	66 500 K	362560 Internet Explorer	Microsoft Corporation	ASLR	Low
iexplore.exe	0.05	38 992 K	46 996 K	360560 Internet Explorer	Microsoft Corporation	ASLR	Medium
chrome.exe	0.06	129 280 K	176 212 K	5396 Google Chrome	Google Inc.	ASLR	Medium
chrome.exe		2 080 K	7 600 K	8920 Google Chrome	Google Inc.	ASLR	Medium
chrome.exe		37 700 K	65 112 K	10056 Google Chrome	Google Inc.	ASLR	Low
chrome.exe		88 500 K	95 260 K	4608 Google Chrome	Google Inc.	ASLR	Untrusted
chrome.exe		38 960 K	49 332 K	4252 Google Chrome	Google Inc.	ASLR	Untrusted
chrome.exe	0.02	107 144 K	120 304 K	3824 Google Chrome	Google Inc.	ASLR	Untrusted
chrome.exe	0.03	61 000 K	93 332 K	321668 Google Chrome	Google Inc.	ASLR	Untrusted
chrome.exe		41 444 K	60 496 K	357940 Google Chrome	Google Inc.	ASLR	Untrusted
chrome.exe		24 672 K	10 944 K	339424 Google Chrome	Google Inc.	ASLR	Medium
chrome.exe		18 824 K	20 948 K	360196 Google Chrome	Google Inc.	ASLR	Untrusted
chrome.exe		27 352 K	35 548 K	360292 Google Chrome	Google Inc.	ASLR	Untrusted
dwm.exe	1.58	43 204 K	85 092 K	764 Desktop Window Manager	Microsoft Corporation	ASLR	System
explorer.exe	1.03	145 616 K	223 312 K	7132 Windows Explorer	Microsoft Corporation	ASLR	Medium
RAVCpl64.exe	< 0.01	4 560 K	12 924 K	8028 Realtek HD Audio Manager	Realtek Semiconductor		Medium
RAVBg64.exe	< 0.01	6 116 K	12 608 K	7408 HD Audio Background Proc...	Realtek Semiconductor		Medium
RAVBg64.exe	< 0.01	5 600 K	11 736 K	7320 HD Audio Background Proc...	Realtek Semiconductor		Medium
igfxtray.exe	< 0.01	1 916 K	7 352 K	6128 igfxTray Module	Intel Corporation		Medium
hkcmd.exe	< 0.01	1 872 K	7 248 K	4560 hkcmd Module	Intel Corporation		Medium
igfxpers.exe	< 0.01	1 972 K	7 864 K	7312 persistence Module	Intel Corporation		Medium
EssentialsTrayApp.exe	< 0.01	2 080 K	8 284 K	5384 Windows Server Essentials ...	Microsoft Corporation	ASLR	Medium
wininit.exe		1 344 K	5 040 K	704 Windows Start-Up Application	Microsoft Corporation	ASLR	System
services.exe	0.01	5 900 K	9 780 K	768 Services and Controller app	Microsoft Corporation	ASLR	System
svchost.exe	0.02	10 824 K	19 580 K	956 Host Process for Windows S...	Microsoft Corporation	ASLR	System
svchost.exe	0.01	9 364 K	14 280 K	1008 Host Process for Windows S...	Microsoft Corporation	ASLR	System

Tools

- INBOX
  - Whoami /all (or /groups)
  - Icacls.exe
  - Reg.exe
- From Sysinternals
  - Procexp.exe
- From Mark Minasi
  - ChML
  - RegIL

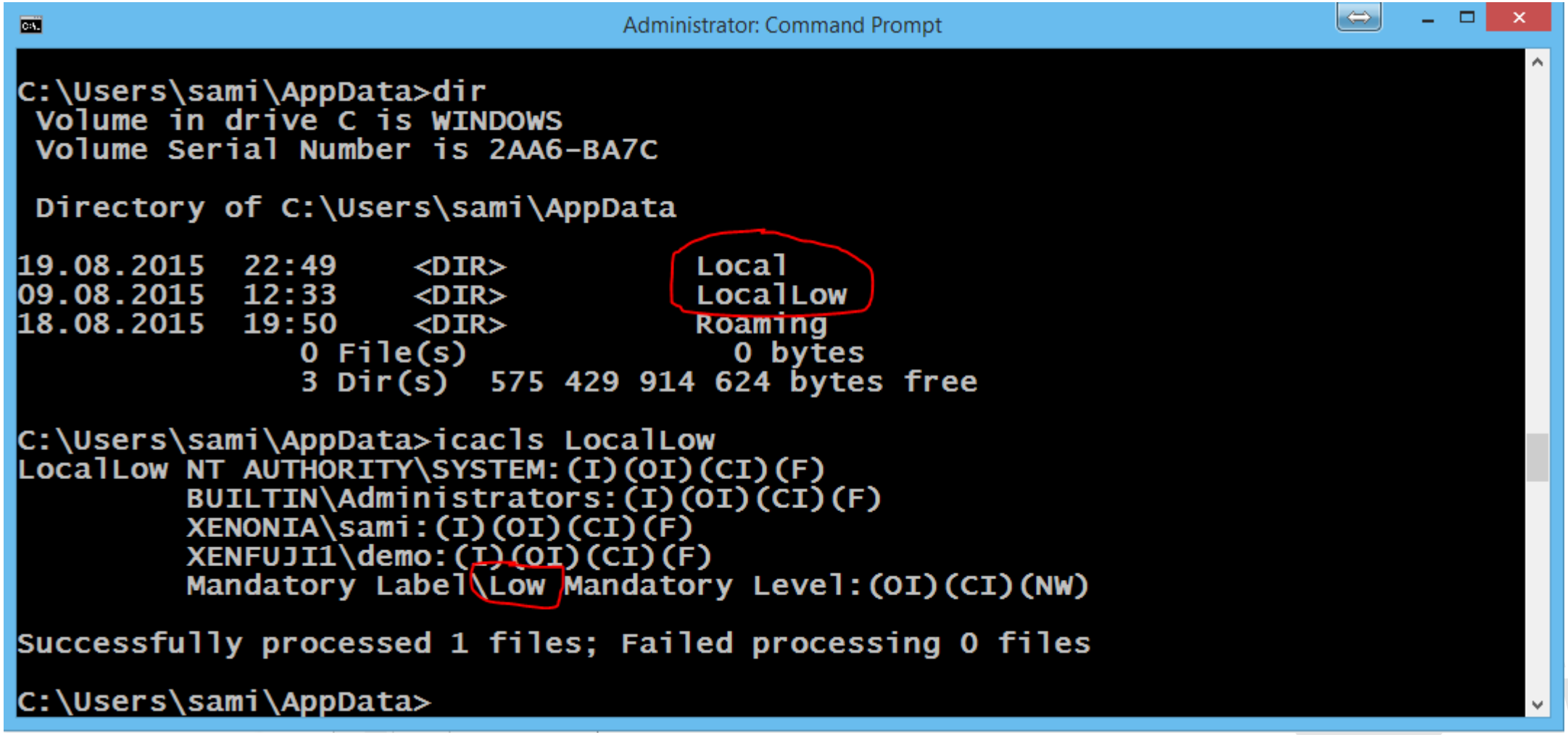
IL Access Checks

- For Write access
  - IL is always checked before DACL → It always wins DACL
  - Requestor IL must be >= Object IL
- For Read access
  - By default there are no IL checks for reading objects
  - For Processes requestor IL must >= process IL

MIC and IE

- Protected Mode IE runs at Low IL
- For Trusted Sites IE process runs at Medium IL
- IE started by an elevated admin runs at Medium IL
- IE Helper process runs at Medium IL
  - Starts the other processes
  - For example allows for file saving to a users profile

User Profiles



Processes

- Process defaults
  - Anonymous Users → Untrusted
  - Limited users and unelevated admins → Medium
  - Elevated Admins → High
  - System → System

User Interface Privilege Isolation (UIPI)

- Less trusted processes can send only query messages to the windows or more trusted processes
  - Can send WM_GETTEXT, WM_DRAWCLIPBOARD, etc…
- Can’t send input to higher IL window
  - SendMessage
- Some apps need to ”bypass” this rule
  - On Screen Keyboard runs at Medium-High IL

Security auditing

- Auditing events are logged in the security log
  - Only Admins can view by default
  - Clearing of the log is always logged
- Audit policy states what categories are to be audited
  - Basic Audit Policy
    - All Windows versions supported
  - Advanced Audit Policy
    - Vista and up
    - More precise
    - Wins if competing with Basic (kind of… Don’t use both!)
    - Can be user-specific or systemwide
  - Object access can be audited globally or based on SACL of objects
- Tools: Security templates, GPO, LocalGPO.exe, auditpol.exe

Demo

Auditing

User Account Control and Virtualization

If you belong to a SuperGroup these get converted to Deny SIDs in your restricted token:

- Built-In Administrators
- Certificate Administrators
- Domain Administrators
- Enterprise Administrators
- Policy Administrators
- Schema Administrators
- Domain Controllers
- Enterprise Read-Only Domain Controllers
- Read-Only Domain Controllers
- Account Operators
- Backup Operators
- Cryptographic Operators
- Network Configuration Operators
- Print Operators
- System Operators
- RAS Servers
- Power Users
- Pre-Windows 2000 Compatible Access

User Account Control and Virtualization

Or you have a superpower they are removed from your restricted token:

- SeBackupPrivilege
- SeCreateTokenPrivilege
- SeDebugPrivilege
- SeImpersonatePrivilege
- SeLabelPrivilege
- SeLoadDriverPrivilege
- SeRestorePrivilege
- SeTakeOwnershipPrivilege
- SeTcbPrivilege

UAC elevation

- UAC will ask you for elevation if it detects that it should
  - AppCompat database
  - Heuristic installer detection
  - Manifest asks for it
  - You choose Run as Administrator
- UAC will not ask for elevation if something would fail otherwise!!
- Consent.exe asks for elevation consent or authentication
  - By default on the Secure Desktop
  - Child of AppInfo-service

Demo

UAC – the Good and the Bad

Pass-The-Hash

- Shouldn’t be a problem
  - No two computer can have the local admin with the same password
  - Domain Admins are not allowed to log on to workstations
- Differences between Windows 7, 8.1 and 10

Well-known SIDs

- New ”Pseudo Groups” in Windows 8.1 (FINALLY!!!)
  - LOCAL_ACCOUNT
    - S-1-5-113
  - LOCAL_ACCOUNT_AND_MEMBER_OF_ADMINISTRATORS_GROUP
    - S-1-5-114

Security in the Future

- Disk encryption
- No admin rights
- Whitelisting is the way to go
- Signing solves a lot

Contact

- sami@adminize.com
- Twitter: @samilaiho
- Blog: http://blog.win-fu.com/
- Free newsletter: http://eepurl.com/F-GOj
- Websites:
  - www.adminize.com
  - www.win-fu.com
  - www.wioski.com
  - www.samilaiho.com
- Video-based training:
  - Later: http://www.pluralsight.com/
  - NOW: http://dojo.win-fu.com/

Nächster Event: Freitag 17. Juni Digicomp Bern
(begrenzte Anzahl Teilnehmer möglich)