Contents

1 Windows access control

- Windows predominantly uses Access Control Lists. Extends the usual read, write and execute with:
  - Take ownership
  - Change permissions
  - Delete
- 32-bit access masks (cf. Unix 9-bit). A higher degree of control, with the associated complexity increase!

1.1 Access Control Matrix

Access rights are defined **individually** for each combination of **subject and object**. Quite an abstract concept, but would allow for very fine grained control. Not practical, think of the **memory required** in scaling it up!

1.2 Access Control List

Stored with an object itself, corresponding to a column of an ACM. Only need data of relevent subjects. E.g. **budget.xlsx** Alice: r,w,e Bob: r Claire: r

1.3 Access Control

- Access control in windows treats more than just files, also:
  - Registry keys
  - Active directory objects
  - Groups
- Inheritance is implemented: File can inherit ACLs from parent directories. This allows to set defaults nicely

2 Principals

Principals more broadly defined as well:

- Local users
- Domain users
- Groups
- Machines (no longer runs on behalf of the user)

Each principal has a human-readable name and security ID (SID)

2.1 Local / Domain Principals

- LSA creates local principals. principal = MACHINE\principal
- Domain principals administered on DC by domain admins. principal@domain = DOMAIN\principal.
- net user /domain, net group /domain, net localgroup /domain

2.2 Groups

- Groups are collections of SIDs (object-orientated)
- Group can itself be an SID
- Groups can thus be nested
- Groups are not nest-able on local machines
- Managed by a **domain controller** within Active Directory

3 Objects

- Objects are passive entities in access operations. In Windows:
  - Executive objects (processes, threads, etc.)
  - Private objects (files, directories)
- Securable objects have a security descriptor
  - Owner SID
  - Primary group
  - DACL - Anyone that has different access rights to the object
  - SACL - for auding purposes.
- Built-in securable objects managed by the OS
- Private objects managed by application software

4 Access Tokens

- Security credentials for a login session stored in access token
- Identifies the user, the users groups, and the users privileges
- Structure:
  - User SID
  - Groups and Alias SID
  - Privileges
  - Defaults for New Objects
  - Miscellaneous
- Token is generated during login, meaning if access is revoked, user will still be able to utilise it untill logout.

5 Subjects

- Windows subjects: Processes and threads
- New processes get a copy of the parent access token, possibly modified
- Individual access tokens are immutable, and can live beyond policy changes (TOCTTOU issue)

6 User Account Control

- After Vista, administrator users do not use an administrative access token by default
- Users **have two tokens**, one heavily restricted and used by default
- A prompt allows a user to spawn a process **with the other token**, or switch a process token

7 Domains

- Single sign-on for network resources
- Centralised security administration
- Domain Controller (DC): handles user accounts and access control, is a trusted 3rd party for authentication
- Multiple DCs allow for decentralisation by design

7.1 Interactive Logon

- The windows interactive logon allows a user to authenticate
- Windows logon begins with the Secure Attention Sequence: Ctrl + Alt + Delete. Can prevent spoofing - is tied directly to winlogon

7.1.1 Logon process

- Winlogon the process responsible for authenticating users
- Graphical Identification and Authentication (GINA)
- The Local Security Authority (LSA)
- An authentication package (NTLM and Kerberos)
- Security Account Manager (SAM)
- Since Vista, additional Credential Providers are allowed (2Factor auth, usb auth, etc.)

7.1.2 Domain logon

- Replaces NTLM with Kerberos
- Replaces SAM with an Active Directory Domain Controller
- Checks of a user are now performed on **the remote LSA**

7.2 Kerberos

- The default authentication for network logon in Windows
- Uses symmetric encryption
- Requires a trusted third party

7.2.1 Process

- Contains 2 core services: Authentication server and Ticket granting server
- Everyone will have a long term key
- When machines want to talk between each other, they obtain a key from a key granting server
- look lesson: here

7.2.2 Important features

- Including nonces / timestamps prevents replay attacks. But, clocks must be synchronised between principals
- Windows Kerberos buries domain group IDs inside tickets, for access checks
- The ticket granting ticket usually exists until log-off, or rotates daily
- A problem if user rights have been changed - TOCTTOU

Reference section

placeholder