Contents

1 Windows

- Windows predominantly uses Access Control Lists, and has done since Windows NT
- Extends the usual read, write and execute with:
  - Take ownership
  - Change permissions
  - Delete
- 32-bit access masks (cf. Unix 9-bit)

1.1 Access Control Matrix

In principle, it would be great to store permissions in the matrix, but it's not feasable as memory would not scale

1.2 Access Control List

Stored with an object itself, corresponding to a column of an ACM. For each file we store permissions (same as in unix). **This makes it diffucult to estimate users abiltities on the system**, e.g. Which files in the system can Alice modify

2 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 like the owner of all files is the owner of AD

3 Principals

- Principals more broadly defined as well:
- Local users
- Domain users
- Groups
- Machines
- Each principal has a human-readable name and security ID (SID)

4 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

4.1 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

5 Objects

- Objects are passive entities in access operations
  - Owner SID
  - Primary group
  - DACL - discretionary access control list
  - SACL - security access control list
- In Windows:
  - Executive objects (processes, threads, etc.)
  - Private objects (files, directories)
- Securable objects have a security descriptor
  - Built-in securable objects managed by the OS
  - Private objects managed by application software

5.1 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

6 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)

6.1 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

6.2 Domains

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

7 Interacive 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**
- The logon process differs slightly for local and domain authentication

Reference section

placeholder