COMP7024- Operating Systems Security and Development

Coursework- Part 1: Security of an OS- File System Security

Nowadays, and since its debut, Windows has been leading the rankings for most powerful and used commercial operating system. A key factor of this is that the data is organised and can be easily manipulated, due to the file system that is build in the software. In this report I will deep dive into the security features with focus to the file system.

1 ) As outlined above, Windows is operating on global level which means that from local laptop system to large corporation networks take advantage of the power that it brings. This establishes the need of organising and controlling the access to different users when it comes to a networkable usage. Defining operational access to commands such as: Read, Write, Delete, Append, is a must in order for the administrator to keep track on how the files are used by the users and not to have a user with access that is not needed for them. On later stages, when an issue occurs, the administrator could pull audit findings to track and monitor the behavior of given user or in general. This is especially important when it comes to legal documents and financial transactions. Furthermore, backing up and secure removal of data should be ensured as if the user deletes by mistake documents, the file system should be able to recover the documents. However, if the user really wants to remove the file from the software, then the system should ensure that the data is erased and cannot be recovered. In case of an attack on the system or the erasing process, the file system should have put in place an encryption mechanism to prevent malicious activities to all files and folders written on the software.

Organising and controlling access; auditing; backing up/removal; encryption

To demonstrate how Windows OS implements security features listed above, I will begin with the core, thus organising the files. Move up to structuring the access controls and controlling users’ activity. Will further deep dive into encryption of the files and end up with specific requirements on the back-up policy and removal. Auditing the logs, would be the final touch where we can extract data for the users and the actions taken for audit purpose and analysis.

1. Organising files

Originally files in the system are orchanised in a hierarchical way with the help of NTFS which first was implemented back in 1993 with the Windows NT 3.1 [1]. However, the newest technology that Microsoft has introduced almost 10 years ago (ReFS), is offering greater data integrity and resilience, designed to handle large sum of files and work with them efficiently. Using B+ trees algorithm to structure all metadata and file data, which is further pushed to a database table. All items components are limited to 64-bit number therefore the maximum file size is 35 petabytes in comparison to NTFS’s 256 terabytes. [2] The Resilient File System was first added to Windows Server 2012 [3] and the performance is taken out of the roof. Reason being the core concept of dividing the volume into tiers where each tier has own drive and resilience types, further allowing each tier to make the decision to optimize either the capacity or the performance of the operations. [4] This is pre-configured so for example given operations such as ‘write’ is operated by one tier (performance tier) and the left-overs will be moved to the other tier in real time (capacity tier).

1. Structuring and Controlling accesses

Once the structure of the files and the network of devices/accounts is done, next step is to consider accesses and having the ability of control over. Windows OS uses ACL (access-control-list) which outlines the accesses given to the user by defining specific rules. [5] This technique is tested and implemented firstly back in 1984 by Multics OS. Nowadays, almost all operating systems take advantage of the idea. Windows OS uses the list by creating entries inside based on their category. Two types of lists exist DACL (Discretionary ACL) and SACL (System ACL) , one describes the access policy and the other the auditing policy of the security descriptors respectively [6][7]. The list is created and begins with zero entries, meaning that the targeted object will not let any user as the user is not presented in the ACL. Most common ACE is to grant world access to the object by using SID (SeWorldSid). For each new entry:   
call BuildExplicitAccessWithName function, grant the relevant EXPLICIT\_ACCESS that describes the needed access, select the ACL and select the array of EXPLICIT\_ACCESS created in the previous step to add those accesses to the list. [8]

1. Encryption
2. Back-up and removal policy
3. Audit

2) - This is usually done in ACL (access-control list) that outlines the access given to the user by defining specific rules. -> Organising access

- NTFS provides auditing capabilities that allow administrators to track and monitor file and folder access. The audit logs record details such as who accessed the file or folder, what action was taken, and when the action occurred. -> Auditing

-User Account Control (UAC) is a security feature that helps prevent unauthorized changes to the system. UAC prompts the user or administrator for permission before allowing any program or user to perform actions that require elevated privileges. -> Control

- BitLocker is a built-in encryption feature that can encrypt the entire drive or specific files and folders. -> Encryption

- The following features are unavailable on ReFS at this time: NOT included in ReFS Encryption : [Resilient File System (ReFS) overview | Microsoft Learn](https://learn.microsoft.com/en-us/windows-server/storage/refs/refs-overview)

Encryption: NTFS supports file encryption using the built-in encryption feature called Encrypting File System (EFS). EFS uses a public key infrastructure (PKI) to encrypt and decrypt files, ensuring that only authorized users can access the encrypted data -> Enctryption

5) – Recommendation – Change encryption methods in given time period

- recommendation – implement role bases for the users (for example: designer- have access to separate disk space in the network where all designers are working on the same project and have exact same accesses. When a new joiner comes in, then only give the role as designer)

References

[1] [NTFS - Wikipedia](https://en.wikipedia.org/wiki/NTFS#:~:text=New%20Technology%20File%20System%20(NTFS,Linux%20and%20BSD%20as%20well.) – NTFS was introduced back in 1993 with Windows NT 3.1

[2] [Resilient File System (ReFS) overview | Microsoft Learn](https://learn.microsoft.com/en-us/windows-server/storage/refs/refs-overview) – Limits

[3] [Resilient File System (ReFS) overview | Microsoft Learn](https://learn.microsoft.com/en-us/windows-server/storage/refs/refs-overview) – ReFS first implemented with Windows Server 2012

[4] [Resilient File System (ReFS) overview | Microsoft Learn](https://learn.microsoft.com/en-us/windows-server/storage/refs/refs-overview) – Performance

[5] [Security descriptors in file systems - Windows drivers | Microsoft Learn](https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/security-descriptors) – Use of ACLs and ACEs

[6] [Security descriptors in file systems - Windows drivers | Microsoft Learn](https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/security-descriptors) – List Types : DACL and CACL

[7] [Access Control List - Windows drivers | Microsoft Learn](https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/access-control-list) – Deep dive in methodology

[8] [Creating or Modifying an ACL - Win32 apps | Microsoft Learn](https://learn.microsoft.com/en-us/windows/win32/secauthz/creating-or-modifying-an-acl) – ACL steps