**Focus especially on recent changes made to enhance security within the OS and the effects these have on application developers.**

**Remember to consider low-level security of features within the OS such as related built-in encryption techniques/tools (e.g., File Vault in macOS ).**

**In the end, briefly compare the listed techniques/tools with similar techniques in an alternative OS.**

1) A high-level description of the security features of an OS file system (15% of the assessment component mark). (WORDS: 225) 3 or 4?

2) A detailed description of how your selected OS supports and provides the listed security features. This should be based on the official documents and includes the timeline that tells from which version the mentioned features were added to the selected OS (30%). (WORDS: 450)

3) A comparison of the listed features in your selected OS with an alternative OS (15%). (WORDS: 225)

4) The effects that the listed security features have on application developers (20%). (WORDS: 300)

5) A conclusion section that includes recommendations for improving the security of OS File Systems and personal reflection(15%). (WORDS: 225)

6) References (using Harvard or Numerical style of referencing) and proper citation(5%).

Upload to github

1. Excellent: Provides an excellent overview of the report and it covers all the essential features, concise, and brief.

Description of Security Features - (WORDS: 225) ¼ = 60

* Security Descriptor - Holds metadata about all the access rights of a windows object in  a data structure. Such entries in the structure include “Owner”, “Primary Group”, “Global Flags”, “DACL”, “SACL”.

<https://learn.microsoft.com/en-us/windows/win32/adschema/a-ntsecuritydescriptor>

* File System Privileges - Limit how users and groups can interact with folders and files. This is done by allocating rights, making interactions managed.

<https://learn.microsoft.com/en-us/iis/web-hosting/configuring-servers-in-the-windows-web-platform/configuring-share-and-ntfs-permissions>

* Auditing - This enables administrators to keep track of particular security events so that the log can be examined afterwards to conduct post-mortem analysis of a broken system.

<https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/auditing>

* Access Control List - Allows you to choose the access type, specify the groups and users whose access you want to limit or enable, and configure permissions on a file or folder.

<https://learn.microsoft.com/en-us/windows/win32/secauthz/access-control-lists>

* BitLocker Drive Encryption - This allows critical system data and other data saved on NTFS volumes to be further secured, aiding in preventing unauthorised users from accessing system files.

<https://learn.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview#increased-security>

* Controlled folder access -  Protects your critical data from dangers, by comparing apps to a database of well-known, trustworthy apps. Thus only allowing trusted apps to access the file system..

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide>

* User Account Control - UAC ensures that all processes and apps always operate in the context of a non-administrator account unless a system administrator explicitly grants administrator-level access.

<https://learn.microsoft.com/en-gb/windows/security/identity-protection/user-account-control/how-user-account-control-works>