**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 to users or groups for a windows object in a data structure (Ashcraft, 2020). **X**
* File System Permissions - Limit how users and groups can interact with folders and files. This is done by allocating rights, making interactions managed (Oliver, 2022). **X DELETE!**

* Auditing - This enables administrators to track what files or folders users have accessed and the actions that have been performed on them. The log can be examined to conduct a post-mortem analysis of a potential compromised system (Hollasch, 2021). **YES**

* Access Control List – Administrators can manage who has access to files or directories by using ACLs. Each file or folder has its own ACL, which lists the users or groups and the level of access they are permitted to (Ashcraft, 2023). **YES**

* BitLocker Drive Encryption – This provides whole-disk or volume encryption and authentication features to conceal and protect a hard drive’s contents from any unauthorized access. This is typically useful for portable electronic devices that may be stolen/lost (Gerend, 2021). **YES**

* Controlled folder access - When an app wants to access the file system, the app is compared to a database of well-known trustworthy apps. Thus, mitigates malicious apps from accessing the file system (Vangel-MSFT, 2023). **YES**

* 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 (Matarazzo, 2022). **YES**

A detailed description of how your selected OS **supports** and **provides** the listed security features. Include **timeline** that tells from which **version the mentioned features were added** to the selected OS. (450 WORDS 64 each)

* Security Descriptor – Window provides a data structure consisting of a security identifier of the object owner, an optional security identifier for the object’s default group, a system access control list that details the auditing policy and a discretionary access control list that details the access policy. This supports the user with information about permissions and control over who has access to an object in the file system (Ashcraft, 2020). 1999
* File System Permissions – Windows provides users with the ability define the degree of access for users and groups on files, with standard permissions including full control, modify, read, and execute, list folder contents, read and write. This supports the user by specifying what users can do with files/folders, enabling supervision of interactions of the file system (Oliver, 2022). 1997
* Auditing – Windows provides a log of the specific events and behaviours that the user has chosen. This supports the user as when a file system becomes comprised, the log provides details which can entail how the system has become compromised. This can be used to fix the vulnerability that the file system acquires (Hollasch, 2021). **2000**
* Access Control List – Windows provides a list made up of access control entries that the user can add to or remove. This supports the user by allowing them to create and specify generic or specified access control entries detailing the access rights which include allowed, denied, or audited for a selected trustee (Ashcraft, 2023). 1998
* BitLocker Drive Encryption – Windows provides the user with the ability to strongly encrypt their most sensitive information on their file system. This supports the user from any malicious intent from other users that may be for example trying to access system files that user passwords are dependent on (Gerend, 2021). **2006**
* Controlled folder access – Windows provides regulations on only allowing trusted apps the ability of accessing protected folders. Windows supports the user with a list of apps that are deemed trusted by their prevalence and reputation, with the ability of the user adding and removing apps. Overall securing file systems from unauthorized apps (Vangel-MSFT, 2023). 2006
* User Account Control – Windows provides a measurement of trust for applications which are marked by integrity levels which include low, medium, high and system. With applications that have a low integrity level being unable to change data in applications that have a high integrity level. This supports the user by limiting applications to a standard privilege until an administrator provides a password to authorize an increase in access. Overall managing applications receiving administrator access, preventing malware from compromising the file system (Matarazzo, 2022). 2006

Timeline

A **comparison** of the **listed features** in your selected OS with an **alternative OS** (15%). (WORDS: 225) 7 security features 32 words each

Windows – Security descriptor Apple –

* Security Descriptors – Windows has security descriptors that detail the access rights for user. Mac OS has headers at the beginning of all objects containing details about the object, \*\*
* File System Permissions – Both systems provide the feature of permissions on folders/files. However, Windows uses ACLs to provide permissions whereas Apple uses traditional Unix permissions.
* Auditing –
* Access control lists – Both Windows and Apple support access control lists that comprise of access control entries, which provide the capabilities to allow users to   
  read, write, execute, and append permissions to a file.
* BitLocker Drive Encryption – Apple also supports full-disk encryption with the feature FileVault. For the encryption Apple uses XTS-AES-128 encryption with a 256-bit key and Windows uses AES-128 with the option of a 128 bit or 256 bit key.
* Controlled Folder Access –
* User Account Control –

The effects that the listed security features have on application developers (20%). (WORDS: 300) 7 security features 42 words each

If you were to write a program, how will the security features affect you as a developer

The developer would need to set to executable to run, and make sure its read only so its not accidentally overwritten by the user

Privileges are only set to that user

Creates any files, must be his group and privilege and if it is shared.

* Security Descriptors - When developers are dependent on objects in applications, the object’s security descriptors must grant appropriate access to users. The developer must construct the data structure of the security descriptor to apply fitting access to users.
* File System Permissions – Applications that involve accessing files, must have appropriate permissions for the user on the file. With such permissions as letting the user execute the file, so that the application can run as intended, as well as making it read only so it cannot be edited by the user to prevent any accidental overwrites.
* Auditing – Users can select window events to be logged, for example, applications accessing file systems. The developer should be aware of this as strict polices are put in place to protect users of the file system. If the application doesn’t conform, then appropriate consequences would be delivered.
* Access Control Lists – ACLs are prevalent in security descriptors for files. When applications handle files, the developer needs to create an Access-allowed Access Control Entry containing either the user's SID or their group SID in the security descriptor or make sure that the user is a part of the same group of the object, granting access to a user.
* BitLocker Drive Encryption - The building and compilation processes are transparent to full drive encryption. When switching to complete drive encryption using BitLocker, there are no changes made to the building, compiling, or debugging processes.
* Controlled Folder Access – Developers creating applications that depend on access to folders in file systems, need to be aware of controlled folder access only permitting applications that are known to be trusted.
* User Account Control – When creating applications that need administrator privileges to execute, developers must be aware that users must have access to administrator permissions to authorise the increase in privilege.

A conclusion section that includes recommendations for improving the security of OS File Systems and personal reflection (15%). (WORDS: 225) Improving: 125 Reflection: 100

Improvements:

* System Compatibility for Android Phone - When enabling android devices to read and write to the file system, third party applications must be used as they do not support NTFS. Leading to users authorising third party applications with administrative access over file systems, trusting that the application behaves accordingly with no malicious intent.
* System Compatibility for Mac OS Computers – Windows file systems that are formatted with NTFS cannot be written to from MAC OS computers. Again, this leads to third party applications being used and trusted with access over the users file system to enable the application to write to the file system.

Overall due to the severity that comes with protecting vital and sensitive information on a file system, Windows provides an extensive range of security features that live up to the expectations needed. With features focus on mitigating unwanted users, applications, and malware from accessing files that are not intended for them, to provide safeguarding and trust for the user.

When using windows file systems, the user’s needs should be taken into consideration when choosing the format of their drive. Whether it be NTFS which is advantageous in exclusive use of Windows. Or whether it be FAT32 which is more practical and better suited for removable storage.

# References

Ashcraft, A., 2020. *NT-Security-Descriptor attribute.* [Online]   
Available at: https://learn.microsoft.com/en-us/windows/win32/adschema/a-ntsecuritydescriptor  
[Accessed 11 February 2023].

Ashcraft, A., 2023. *Access control lists.* [Online]   
Available at: https://learn.microsoft.com/en-us/windows/win32/secauthz/access-control-lists  
[Accessed 11 February 2023].

Gerend, J., 2021. *NTFS overview.* [Online]   
Available at: https://learn.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview#increased-security   
[Accessed 11 February 2023].

Hollasch, L. W., 2021. *Auditing.* [Online]   
Available at: https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/auditing  
[Accessed 11 February 2023].

Matarazzo, P., 2022. *How User Account Control works.* [Online]   
Available at: https://learn.microsoft.com/en-gb/windows/security/identity-protection/user-account-control/how-user-account-control-works  
[Accessed 11 February 2023].

Oliver, W., 2022. *Share and NTFS Permissions.* [Online]   
Available at: https://learn.microsoft.com/en-us/iis/web-hosting/configuring-servers-in-the-windows-web-platform/configuring-share-and-ntfs-permissions  
[Accessed 11 February 2023].

Vangel-MSFT, D., 2023. *Protect important folders with controlled folder access.* [Online]   
Available at: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide  
[Accessed 11 February 2023].