**Assessment cover**

**STUDENTS, PLEASE COPY THIS PAGE AND USE AS THE COVER PAGE FOR YOUR SUBMISSION**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Module No: | **COMP6015** | Module title: | | **Principals of Secure Operating Systems** | |
| Assessment title : | **Coursework** | | | | |
| Due date and time**:** | | | | **03/03/2023 17:00** | | | |
| Estimated total time to be spent on assignment: | | | | | 35 hours per student | | |

**LEARNING OUTCOMES**

|  |  |
| --- | --- |
| **On successful completion of this module, students will be able to achieve the module following learning outcomes (LOs):** *LO numbers and text copied and pasted from the module descriptor* | |
| LO 1: Demonstrate a thorough understanding of the fundamentals of OS design, including process/thread, file, IO, and memory management. | |
| LO 3: Critically evaluate the security, reliability, and protection in a given OS configuration. Use the results of the evaluation to produce recommendations for hardening the system. | |
| **Engineering Council AHEP4 LOs assessed (from S1 2022-23)** *LOs copied and pasted from the AHEP4 matrix* | |
|  |  |
|  |  |
|  |  |
|  |  |

**STUDENT NAMES (ONLY IF GROUP ASSIGNMENT, OTHERWISE ANONYMOUS)**

|  |  |  |
| --- | --- | --- |
| **Student No:** | **Student Name:** | **Group Name and Number:** |
| **1.** |  |  |

**Statement of Compliance *(please tick to sign)***

I declare that the work submitted is my own and that the work I submit is fully in accordance with the University regulations regarding assessments [*(www.brookes.ac.uk/uniregulations/current*](http://www.brookes.ac.uk/uniregulations/current)*)*

✓

Description of Security Features for Windows

* **Security Descriptor** - Holds metadata about all the access rights to users or groups for a windows object in a data structure (Ashcraft, 2020).
* **File System Permissions** - Limit how users and groups interact with folders and files. This is done by allocating rights, making interactions managed (Oliver, 2022).
* **Auditing** - 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 for a post-mortem analysis of a potentially compromised file/system (Hollasch, 2021).
* **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 (Ashcraft, 2023).
* **BitLocker Drive Encryption** – This provides whole-disk or volume encryption and authentication features to conceal and protect a hard drive’s contents from unauthorized access. This is typically useful for portable electronic devices that may be stolen/lost (Gerend, 2021).

* **Controlled folder access** - When an app wants to access the file system, the app must be on the database of well-known, trustworthy apps. Thus, it mitigates malicious apps from accessing the file system (Vangel-MSFT, 2023).

* **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).

How Windows OS **supports** and **provides** the listed security features.

* 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 controls over who has access to an object in the file system (Ashcraft, 2020).
* File System Permissions – File System Permissions – Windows allows users to 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 in the file system (Oliver, 2022).
* Auditing – Windows provides a log of the specific events and behaviours the users have performed on files/folders. This supports the user when a file system becomes compromised; the log details how the system has become compromised. This can then be used to fix the vulnerability that the file system acquires (Hollasch, 2021).  
  (By default, auditing is not enabled)
* Access Control List – Windows provides a list 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 of users/groups, which include allowed, denied, or audited for a selected trustee (Ashcraft, 2023).
* BitLocker Drive Encryption – Windows allows the user to encrypt the most sensitive information on their hard drive strongly. This protects the user from any malicious intent from other users, such as trying to access their system files (Gerend, 2021).
* Controlled folder access – Windows provides regulations on only allowing trusted apps to access protected folders/files. Windows supports the user with a list of apps deemed trusted by their prevalence and reputation, with the ability of the user to add and remove apps. They secure file systems from unauthorised apps (Vangel-MSFT, 2023).
* User Account Control – Windows provides a measurement of trust for applications marked by integrity levels, including low, medium, high and system. Applications with a low integrity level cannot change data in applications with a high integrity level. This supports the user by limiting applications to a standard privilege until an administrator provides a password to authorise an increase in access. They are, overall, managing applications receiving administrator access to prevent malware from compromising the file system (Matarazzo, 2022).

Timeline

A **comparison** of the **listed features** in your selected OS with an **alternative OS** (15%).

* **Security Descriptors** – Windows has security descriptors that detail the access rights for users on files or folders, which can be modified in windows security settings (Ashcraft, 2020). Mac OS’s equivalent of security descriptors are Access Control Lists and can be modified through the Get Info Window or the terminal (Anon., n.d.).
* **File System Permissions** – Both systems provide the feature of permissions on folders/files. However, Windows uses ACLs to provide permissions (Oliver, 2022).

Whereas Apple uses traditional Unix permissions (Anon., n.d.).

* **Auditing** – Again, both systems provide auditing. However, Windows provides two types of auditing: process tracking auditing and object access auditing (Hollasch, 2021). Mac is more straightforward, with only one type of auditing called file access auditing (Anon., n.d.).
* **Access control lists** – Both Windows and Apple support access control lists that comprise access control entries, which provide the capabilities to allow users to   
  read, write, execute, and append permissions to a file (Ashcraft, 2023) (Anon., n.d.).
* **BitLocker Drive Encryption** – Apple also supports full-disk encryption with the feature FileVault (Anon., 2022). 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 (Gerend, 2021).
* **Controlled Folder Access** – There is no equivalent feature in Mac OS.
* **User Account Control** – There is no equivalent feature in Mac OS.

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

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

* **Security Descriptors** - When developers depend on objects in applications, the object’s security descriptors must grant appropriate access to their 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 the user cannot edit it to prevent accidental overwrites.

* **Auditing** – Users can select window events to be logged, for example, applications accessing file systems. The developer should be aware of these as strict policies are put in place to protect file system users. If the application does not conform, then appropriate consequences will 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 ensure 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, no changes are 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%).

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 formatted with NTFS cannot be written from MAC OS computers. Again, this leads to third-party applications being used and trusted with access to the user’s file system to enable the application to write to the file system.

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

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

The comparison of features between Windows and Mac showed that both provide and equip the user with robust security features that can ultimately protect users’ data.   
However, choosing a favourable file system depends on personal preference and requirements.

Lastly, having these extensive ranges of security features is all good, but if the user does not use them or does not know how to set them up, they are not helpful. Educating the system user on how the features work and how they are configured to adapt to their needs is essential, as human error is one of the most prominent attack vectors hackers exploit.

# References

Anon., 2022. *Use FileVault to encrypt your Mac startup disk.* [Online]   
Available at: https://support.apple.com/en-gb/HT204837  
[Accessed 24 February 2023].

Anon., n.d. *Access Control Lists.* [Online]   
Available at: https://developer.apple.com/documentation/security/keychain\_services/access\_control\_lists  
[Accessed 24 February 2023].

Anon., n.d. *Change permissions for files, folders or disks on Mac.* [Online]   
Available at: https://support.apple.com/en-gb/guide/mac-help/mchlp1203/mac  
[Accessed 24 February 2023].

Anon., n.d. *iOS Manual Pages.* [Online]   
Available at: https://developer.apple.com/library/archive/documentation/System/Conceptual/ManPages\_iPhoneOS/man2/audit.2.html  
[Accessed 24 February 2023].

Anon., n.d. *iOS Manual Pages.* [Online]   
Available at: https://developer.apple.com/library/archive/documentation/System/Conceptual/ManPages\_iPhoneOS/man3/acl.3.html  
[Accessed 24 February 2023].

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., 2021. *Alternatives to using Transactional NTFS.* [Online]   
Available at: https://learn.microsoft.com/en-us/windows/win32/fileio/deprecation-of-txf  
[Accessed 24 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].