COMP6015 – Secure OS

Coursework 1

19141283

* User Authentication – The operating system must identify users that request access and verify whether the user is who they pertain to be. This is usually performed through password verification.
* User AC / Authorisation – Access Control is usually implemented on a per user basis or by group. This prevents unauthorized users from accessing files that they shouldn’t be able to and keeps users personal workspaces separate. It also restricts what non-administrator users can do and access in the file system, e.g. only administrators can modify certain files or perform administrative functions (e.g. installing programs, changing system settings). (Microsoft, 2021)
* Drive Encryption - Prevents the data from being accessed from the drive without being first decrypted by the operating system. This stops data being stolen if a storage device is stolen or accessed by a bad actor.
* Auditing – The file system should be able to log access to all files and directories and provide an auditing trail of who accessed the data and when. This helps security as it allows for administrators to know what has been changed and when, in case of incident. It can also establish who is at fault for the issues and allow for an investigation to be performed to determine whether the fault was malicious.
* File Permissions – The file system should be able to set separate read, write, execute permissions for files, these will specify which users and groups can complete the above processes in order to protect the system.

1. Windows 11

* User Authentication – Windows, like most other operating systems, uses user passwords / credentials to authenticate users to prevent them from accessing someone else's data on that machine. In their documentation, Microsoft call this a Graphical Identification and Authentication (GINA), GINA was used from 2000 in windows server 2000 until Windows Server 2008 and Vista and was later replaced with a different architecture called the credential provider model. Both of these models require user credentials such as usernames and passwords to authenticate users, but they function differently under the hood. (Microsoft, 2021)
* Access Control / Authorisation - Access Control in windows is implemented on a per user basis or by group. This prevents unauthorized users from accessing files that they shouldn’t be able to and keeps users personal workspaces separate. It also restricts what non-administrator users can do and access in the file system, e.g. only administrators can modify certain files or perform administrative functions (e.g. installing programs, changing system settings). (Microsoft, 2021)
* Drive Encryption - Bitlocker – Bitlocker is a Windows service that encrypts the file system. Preventing the data from being accessed from the drive without being first decrypted by the operating system. This was introduced in Windows vista in 2007 and later updated with new encryption algorithms for Windows 10. (Microsoft, 2022)
* Auditing – Audit File System – Audit File System determines whether the OS generates audit events when users attempt to access file system objects. If success auditing is enabled, an audit entry is created whenever a user successfully accesses a file system object that is in a purpose-created ACL (access control list). (Microsoft, 2022)
* File Permissions – Windows 11 allows

# References

Microsoft. (2021, January 7). *Access Control (Authorization)*. Retrieved from learn.microsoft.com: https://learn.microsoft.com/en-us/windows/win32/secauthz/access-control

Microsoft. (2021, July 29). *Credentials Processes in Windows Authentication*. Retrieved from https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication

Microsoft. (2022, December 16). *Audit File System*. Retrieved from https://learn.microsoft.com/: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-file-system

Microsoft. (2022, December 9). *BitLocker*. Retrieved from learn.microsoft.com: https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview