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.
* File and I/O device access control – The OS must protect user and system files from access by unauthorized users. Similarly I/O device use should be protected. Data protecting is usually achieved by table lookup as with an access control matrix.
* 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.

1. Windows 11

* User Authentication -
* File and I/O Device Access Control –
* User Access Control / Authorisation -
* 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.

# References

Microsoft. (2021, 7 1). *Access Control (Authorization)*. Retrieved from learn.microsoft.com: https://learn.microsoft.com/en-us/windows/win32/secauthz/access-control