COMP6015 - File System Security

In this report I shall be explaining some of the core security features of the Windows 11 OS, as well as describe some of the core features of the newer Resilient File System (ReFS) that is being used as a substitute for the older New Technology File System (NTFS). I will also briefly cover some of the fundamental evolutionary changes between Windows 10 and 11 and the reasoning behind them.

# What does an Operating System do?

An operating system is the core of a computer. It enables the user to interact with the hardware of the machine. Allows said hardware to perform the functions required of them, manages the general running of processes such as disk and memory access as well as provide a base layer of security to the whole.

At the lowest level of the OS is the Kernal which itself is responsible for all the base line interactions the OS takes. Interacting with the hardware and the memory when called upon by various programs and routines whether it be a command line requesting the contents of a directory, or a performing a set of boot instructions. Since the Kernal has access to the entire machine, it is also very vulnerable to attack, and that is where the rest of the OS comes into play.

# OS Security

## The Trusted Platform Module

One of the core security features utilised by Windows is the Trusted Platform Module (TPM). This is especially the case in Windows 11 as TPM 2.0 chips are required to even run the OS as listed on Microsoft’s system requirements [1].

## ReFS

### Integrity

### Block Cloning

### ReFS vs NTFS

# How does MacOS compare?

# Developer Interactions

# Conclusion

# References

|  |  |
| --- | --- |
| [1] | Microsoft Corporation, “Windows 11 Specs and System Requirements | Microsoft,” 2023. [Online]. Available: https://www.microsoft.com/en-us/windows/windows-11-specifications. [Accessed 10 March 2023]. |