COMP6015 - File System Security

Repo Link: <https://github.com/TBlackmoreUni/COMP6015Report>

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 on motherboards to even run the OS as listed on Microsoft’s system requirements [1].

Also stated on Microsoft’s documentation is what a TPM is and how it is utilised [2]. It describes the “TPM’s as microchips designed to provide basic security-related functions, primarily involving encryption keys.” This device enables systems to create and encrypt keys in a way that can only be decoded by a TPM. This wrapping and binding of a key helps provide another layer of security by preventing the key from being read.

Windows uses this as part of its Cryptographic API: Next Generation (CNG) to provide additional layers of security beyond what software-only CNG providers are able. The two primary features, as shown in the documentation [3], the TPM’s enable is the previously mentioned key protection as well as protection from dictionary attacks. These attacks involve a programme attempting to guess a PIN through a brute force method. The TPM can prevent this by returning an error upon reaching a specified number of attempts.

These 2 features provide the core function of the Platform Crypto Provider first introduced in Windows 8, and as such, are able to provide a much higher level of security.

## BitLocker

BitLocker Drive Encryption is another example use of the TPM chip and is used to address threats regarding data theft or exposure from lost, stolen, or disposed computers [3]. The chip is not required for BitLocker to be effective, but it makes the process much more streamlined. Without a TPM, a user would be required to use a USB or, from windows 8 onwards, a password however this does not prevent all potential attacks.

In a more normal setting, BitLocker splits the hard drive into several volumes with the OS and user data on one holding confidential information. Whereas on the other volumes, the public information is stored. This public information typically comprises of boot components, system information and recovery tools. In combining its protection with the keys provided by the TPM, it allows for a secure system in the event of theft.

Since, BitLocker has received constant updates with a notable one being the introduction of Direct Memory Access (DMA) Port protection. This involved blocking the DMA ports on startup as well as disabling any ports that are not currently being used and even enabling devices using those ports to still function even if the port itself is disabled. This feature was released in the Widows 10 version 1507 update [4].

## Resilient File System

The Resilient File System or ReFS is the newest file system developed by Microsoft initially for the Windows Server. However, it is slowly being implemented into windows 11 to replace the New Technology File System (NTFS) in some areas. While it cannot perform all functions of NTFS, the ReFS does provide some key features that guard against file corruption and data loss. One, big downside of ReFS is that it cannot be utilised as a boot file system as there is no way to convert a storage partition from one system to another [5]. The biggest benefit though by far is being able to repair corrupted files as showcased in Integrity-Streams.

### Integrity-Streams

Integrity-Streams enable the File System to detect corrupt files by utilising checksums for metadata. This feature can be enabled to extend to file data as well allowing ReFS to determine if the data is valid or corrupt. It does this by adding a checksum to the files metadata, allowing the check to take place before the file is accessed. Once the checksum is calculated, it is compared to the one in the meta data and if valid, the data is returned to the user, otherwise an attempt is made to repair the file [6]. If this is not possible, an error is thrown.

A downside to this however is that the processing time to check through each file can cause latency issues with IO devices. Especially if data because fragmented across a drive and therefore take much longer.

On top of this, ReFS has a background scrubber allowing for the validation of data that is not commonly accessed.

# 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]. |
| [2] | Microsoft Corporation, “Trusted Platform Module (TPM) fundamentals,” 09 March 2023. [Online]. Available: https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-fundamentals. [Accessed 15 March 2023]. |
| [3] | Microsoft Corporation, “How Windows uses the TPM,” 27 Feburary 2023. [Online]. Available: https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/how-windows-uses-the-tpm?source=recommendations. [Accessed 15 March 2023]. |
| [4] | Microsoft Corporation, “What's new in Windows 10, versions 1507 and 1511 (Windows 10) - What's new in Windows,” 27 Feburary 2023. [Online]. Available: https://learn.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1507-and-1511#bitlocker. [Accessed 16 March 2023]. |
| [5] | Cartsen, “Overview: Resilient File System (ReFS),” Folder Security Viewer, 3 August 2018. [Online]. Available: https://blog.foldersecurityviewer.com/overview-resilient-file-system-refs/#:~:text=An%20outstanding%20feature%20of%20ReFS,without%20compromising%20the%20volume%20availability.. [Accessed 12 March 2023]. |
| [6] | Microsoft Corporation, “ReFS integrity streams,” 29 March 2022. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/storage/refs/integrity-streams. [Accessed 14 March 2023]. |