COMP 7024

1. Introduction:
2. File System Security in Windows:
3. Recent changes with respect to security :
4. Compatibility of the listed features with the OS:
5. Impact on Application developers:
6. Comparison of security features between Windows and MacOS:
7. Conclusion:
8. References:

Windows and macOS are the two most popular commercial operating systems (OSes) in use today. OS security has become more crucial as computer technology has advanced in order to safeguard user data from unauthorised parties. In this article, we'll examine the security capabilities of the Windows and macOS file systems with a particular emphasis on recent updates that have improved security for each of these operating systems.

File sys:

Access control enables an administrator or file user to monitor who can access and alter files upon a system files. User accounts, password protection, and file permissions are used to achieve this.

Encryption: Using encryption methods, data is transformed into an unintelligible format. Confidential material on the file system can be protected by encryption, which can be applied to certain files, directories, or the complete file system.

Auditing and logging: This function keeps track of all file system activities, such as requests, changes, and alterations. This aids in identifying and looking into security lapses.

Integrity protection: This makes sure the information on the file system is unaltered and undamaged. File checksums, file system journaling, and other methods are employed to achieve this.

A crucial component that aids in shielding the file system from viruses, worms, Trojan horses, and other forms of harmful software is anti-virus and anti-malware protection.

These are only a few of the security measures that an operating system file system may contain. With respect to the operating system and file system version being utilised, certain security mechanisms and how they are implemented might change.

Windows file system security is provided by the NTFS (New Technology File System). Access control lists (ACLs), discretionary access control (DAC), and obligatory access control are among the security features offered by the NTFS (MAC). Based on user or group permissions, administrators can grant or prohibit access to files and directories using ACLs.

Users have the option to grant or prohibit access to files and directories using DAC at their own will. Based on labels, MAC is used to restrict access to items (e.g. top-secret, confidential, etc.). Moreover, Windows offers the Encrypting File System for file and folder encryption (EFS).

In contrast to these security mechanisms, Microsoft has recently added a number of additional capabilities to the Windows 10 OS to adequately secure the file system. They consist of Credential Guard, Device Guard, and Secure Boot. Malicious programmes cannot load during the startup process thanks to a technology called Safe Boot. Administrators have the option to limit which programmes can be run on a device thanks to Device Guard. Credential Guard, which isolates user credentials from hostile attackers, offers a last degree of safety. It secures and isolates the sensitive data it keeps, making it impossible for hackers to access them.

To further improve the security of their file systems, new security measures have been added to subsequent versions of Windows 10. On Windows, these features consist of Secure Boot, Device Guard, and Credential Guard.

By ensuring that only authorised kernels are booted during the boot process for Windows, Secure Boot prevents malicious malware from loading. Administrators can limit which applications can run on a device with Device Guard. By separating user credentials from hostile actors, Credential Guard adds an extra degree of security. Device Guard, a feature supported by Windows 10, protects your device from harmful programmes by stopping it from running on the device. Credential Guard is an additional feature that aids in preventing device theft of sensitive credentials.

A number of security improvements have been made to the most recent version of Windows 10 to help safeguard your device from harmful software. A more thorough threat protection system, including real-time protection, automated updates, enhanced security software, and a secure processor, has been added to Windows Security. User account control, BitLocker, firewall and network security, secure boot and Exploit Guard are some additional we get in Windows 10.

References:

<https://learn.microsoft.com/en-GB/troubleshoot/windows-client/backup-and-storage/fat-hpfs-and-ntfs-file-systems>

<https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage>

<https://techcommunity.microsoft.com/t5/windows-hardware-certification/driver-compatibility-with-device-guard-in-windows-10/ba-p/364865>