**COMP6015 Coursework**

**03/03/2023 17:00**

Due date and time**:**

**Coursework**

Assessment title :

|  |  |  |  |
| --- | --- | --- | --- |
| Module No: | **COMP6015** | Module title: | **Principals of Secure Operating Systems** |

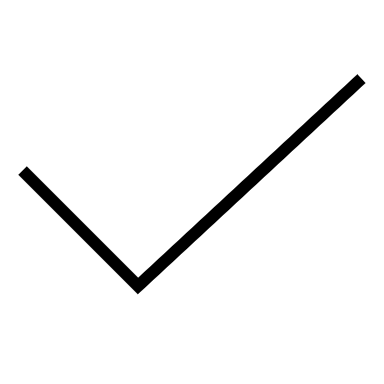
35 hours per student

Estimated total time to be spent on assignment:

**LEARNING OUTCOMES**

|  |
| --- |
| **On successful completion of this module, students will be able to achieve the module following learning outcomes (LOs):** *LO numbers and text copied and pasted from the module descriptor* |
| LO 1: Demonstrate a thorough understanding of the fundamentals of OS design, including process/thread, file, IO, and memory management. |
| LO 3: Critically evaluate the security, reliability, and protection in a given OS configuration. Use the results of the  evaluation to produce recommendations for hardening the system. |

|  |  |
| --- | --- |
| **Engineering Council AHEP4 LOs assessed (from S1 2022-23)**  *LOs copied and pasted from the AHEP4 matrix* | |
|  |  |
|  |  |
|  |  |
|  |  |

I declare that the work submitted is my own and that the work I submit is fully in accordance with the University regulations regarding assessments *(*[*www.brookes.ac.uk/uniregulations/current*](http://www.brookes.ac.uk/uniregulations/current)*)*

**COMP6015 – Principals of Secure Operating Systems - Coursework**

**Security of the Windows OS- File System Security**

1. ***A high-level description of the security features of an OS file system***

OS security is majorly important in keeping the rigidity and anonymity of the operating system’s data and user files. The security features of an established OS are in place to protect the system’s resources such as the CPU, Memory, Storage, and any important user data stored software/hardware-side.

If these systems are not in place or poorly developed , then the severity of an attack could be dire. Any user’s data is vulnerable if any unauthorized or malicious access is granted.

The windows OS currently has many features providing top-level security for users across all systems. Windows provides extensive measures to improve the encryption and protection of data, the robustness of its system/network security and the overall intelligence of its procedures, allowing the OS to evolve and learn to counter and battle ever-developing threats.

1. ***A detailed description of how Windows OS supports and provides the listed security features.***

Windows has had many iterations of file systems over the years. From the inception of MS-DOS, the FAT file system was introduced. Since then, FAT has gone through many revisions; FAT8, FAT16 and FAT32. FAT, or File Allocation Table, was revolutionary at the time. However nowadays it is considered reasonably simplistic. FAT32 is still in use today for most trivial, low-capacity flash drives. A drive formatted in FAT32 or lower is divided into clusters. The cluster’s size is determined by the capacity of the volume. When a file is added, it is given the next available location on the drive. This is because there is no organisation implemented into the FAT directory structure.[2]

After recognising that the FAT file system wasn’t going to last for ever, windows introduced the New Technology File System, also known as NTFS, during the release of windows NT 3.1 in 1993. This replaced FAT32 as windows main file system. NTFS is more proficient in its performance and extendibility, but most importantly in its security capabilities, compared to FAT32.

Two of the main security features in the NTFS system are ACL and BitLocker support:

**ACL**

Access Control List or ACL based security allows one to set specific permissions on any file or folder. It allows the OS to control the security behaviour associated with said files/folders, while also restricting the amount of access specific users have to the data (writing/reading permission).[1] An ACL list consists of individual classification rules, each with their own specific action, called an ACE (Access Control Element). To determine the classification rules, each ACE consists of filters which are used to grant/block access to users trying to gain access to a file/folder.[3]

There are two main types of ACLs: Discretionary ACLs and System ACLs. A discretionary ACL is a list of ACEs that each define the rights to access for the said object. The access allowed is at the discretion of the user(s) with given administrative rights, hence the name “Discretionary”. A System ACL is similar to the discretionary ACL, but each ACE describes the auditing and alarm policies for each object protected. Discretionary ACL systems are common practice in a more relaxed environment like windows, where as in a more tight-nit environment, where systems are programmed to prevent access to information within its own domain, a mandatory control approach may be present. This would mean even the owner of a given file or folder may be unable to grant access to the object to other users within the same system.[4]

The implementation of ACLs is a major step forward in improving not only local security between clients/users, but also network security. Having an ACL in place stops malicious traffic gaining access to files or folders with strict access permissions.

**BitLocker Drive Encryption**

In 2012, the support for BitLocker Drive Encryption was implemented into windows 8.1 and windows server 20212. Even with the windows EFS (encryption file system) in place, which was introduced in version 3.0 of NTFS, the support for BitLocker brought about another low-level interagtion of protection, directly associated with the OS.[5] A main focus of BitLocker is the protection from offline tampering or theft of data. Most modern computers are now installed with what is known as a TPM (Trusted Platform Module). The TPM is a hardware component which BitLocker works side-by-side with to ensure safety of data when the computer is in any state (online, offline, powered on/off, etc). BitLocker supports x86 and x64- based systems, helping protect user data from malware and unauthorised users from accessing the OS files. This is because the OS boot files are used by malware to access user’s passwords. It can also protect individual physical drives from being removed from its computer and being accessed from an external system.[6]

NTFS can support volume sizes of up to 8 petabytes, however this depends on the cluster size allocated when the drive is formatted as NTFS.

On the 1st August 2012, a new file system was introduced with the release of windows server 2012. Codenamed “Protogon” the Resilient File System or ReFS was introduced as windows latest file system. It is claiming to increase the data availability, efficiency to scaling to larger data sets across multiple workloads and providing state-of-the-art corruption resiliency.

1. ***A Comparison of the listed features from the Windows OS with MacOS.***

There are many comparisons to be made between NTFS and Apple’s file system APFS.

**Encryption**

As stated before, NTFS has multiple systems in place creating a solid base for safe encryption of user data; the EFS and BitLocker just to name a few. However APFS takes great pride in their data encryption services, and some may say theirs is stronger than what NTFS offers. Apple’s answer to BitLocker is their FileVault capability. The internal APFS volumes stay encrypted and are secured from unauthorised access even if the physical storage device is removed and connected to another computer. This will be the case until proper login details or a “cryptographic recovery key” is given[7].

**Data Protection**

Where NTFS creates ACLs from ACEs to filter accessibility, the APFS system constructs and manages keys, each created for each file on the system, and all managed in a hierarchical fashion. For every file, there is a “class key” appended to that file, determining the level of access that is approved. When the class key is unlocked, the access is granted if the user has the correct level of access. A useful feature of this approach is that each file can be broken down into sub-class keys, allowing different areas of a file can have different levels of access.[8]

1. ***The effects that the listed security features have on application developers.***

Since the introduction of BitLocker Drive Encryption, it has been important for developers of applications that perform offline restorations and backups to understand the process on how to restore data onto an encrypted drive. When in the process of this, it is important for the developer to perform any restoration or backup after the deactivation of BitLocker. After the action is done, the restored OS is re-booted, and BitLocker is reactivated.[9]

Developers may also need access to the ACLs on a system. There are many functions available to developers, providing the ability to determine access rights that an ACL grants to a specific user or group. There are also functions allowing developers to gain information from specific ACEs within an ACL. The flexibility of these functions allow for a wide range of data retrieval and manipulation. An example of this is the function “GetExplicitEntriesFromAcl” which retrieves an array of data describing the ACEs within a specified ACL. This can be used to create equivalent ACEs in a newer ACL, by also using the “SetEntriesInAcl” function.[10]

1. ***Conclusion***

In conclusion, the security of OS file systems in general is a critical aspect of protecting data and preventing malicious and/or unauthorized access. There will always be ways to improve the security of an OS system, some of the following suggestions may be considered important aspects of this:

* Implementing strong, multi-layered authenticity mechanisms.
* Increasing the strength and rigidity of encryption used in data protection.
* Using more third-party tools to further improve encryption.
* Regular OS and application security updates to remove the chance of out of date software which would reduce the strength of security on a system.
* Improving Access controls to increase the difficulty of unauthorised access to user data.

1. ***Bibliography***

GitHub Repository: <https://github.com/FreddieHulbert22/COMP6015-Coursework>

[1] JasonGerend (n.d.). *NTFS overview*. [online] learn.microsoft.com. Available at: <https://learn.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview#increased-security> [Accessed 27 February. 2023].

[2] Deland-Han (2021). *Overview of FAT, HPFS, and NTFS File Systems - Windows Client*. [online] learn.microsoft.com. Available at: <https://learn.microsoft.com/en-us/troubleshoot/windows-client/backup-and-storage/fat-hpfs-and-ntfs-file-systems> [Accessed 28 February. 2023].

‌[3] www.cisco.com. (n.d.). *Access Control*. [online] Available at: <https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_2_015/help/nk_configuring_quality_service03.html#:~:text=An%20ACL%20is%20a%20ordered> [Accessed 2 Mar. 2023].

[4] lorihollasch (n.d.). *Access Control List - Windows drivers*. [online] learn.microsoft.com. Available at: <https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/access-control-list>. [Accessed 2 Mar. 2023]

[5] alvinashcraft (n.d.). *File Encryption - Win32 apps*. [online] learn.microsoft.com. Available at: <https://learn.microsoft.com/en-us/windows/win32/fileio/file-encryption> [Accessed 3 Mar. 2023].

‌[6] Dansimp (2022). *BitLocker - Windows security*. [online] learn.microsoft.com. Available at: <https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview> [Accessed 3 Mar. 2023].

[7] Apple Support. (n.d.). *Volume encryption with FileVault in macOS*. [online] Available at: <https://support.apple.com/en-gb/guide/security/sec4c6dc1b6e/web#:~:text=All%20APFS%20volumes%20are%20created>

[Accessed 3 Mar. 2023].

‌[8] Apple Support. (n.d.). *Data Protection overview*. [online] Available at: <https://support.apple.com/en-gb/guide/security/secf6276da8a/web> [Accessed 3 Mar. 2023].

‌[9] GrantMeStrength (n.d.). *Working with File System and Security Features - Win32 apps*. [online] learn.microsoft.com. Available at: <https://learn.microsoft.com/en-us/windows/win32/vss/working-with-file-system-and-security-features> [Accessed 3 Mar. 2023].

‌[10] alvinashcraft (n.d.). *Getting Information from an ACL - Win32 apps*. [online] learn.microsoft.com. Available at: <https://learn.microsoft.com/en-us/windows/win32/secauthz/getting-information-from-an-acl?source=recommendations> [Accessed 3 Mar. 2023].

‌

‌

‌

‌