COMP6015 – Secure OS

Coursework 1

19141283

https://github.com/patet001/COMP-6015-Secure-OS-CW1

* 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. This has been a feature of Windows since its inception in 1985.
* 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.
* Auditing – The file system should be able to log access to all files and directories and provide an auditing trail of who accessed the data and when. This helps security as it allows for administrators to know what has been changed and when, in case of incident. It can also establish who is at fault for the issues and allow for an investigation to be performed to determine whether the fault was malicious.
* File Permissions – The file system should be able to set separate read, write, execute permissions for files, these will specify which users and groups can complete the above processes in order to protect the system.

1. Windows 11

* User Authentication – Windows, like most other operating systems, uses user passwords / credentials to authenticate users to prevent them from accessing someone else's data on that machine. In their documentation, Microsoft call this a Graphical Identification and Authentication (GINA), GINA was used from 2000 in windows server 2000 until Windows Server 2008 and Vista and was later replaced with a different architecture called the credential provider model. Both of these models require user credentials such as usernames and passwords to authenticate users, but they function differently under the hood. (Microsoft, 2021)
* Access Control / Authorisation - Access Control in windows is 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 - 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. (Microsoft, 2022)
* Auditing – Audit File System – Audit File System determines whether the OS generates audit events when users attempt to access file system objects. If success auditing is enabled, an audit entry is created whenever a user successfully accesses a file system object that is in a purpose-created ACL (access control list). (Microsoft, 2022) Windows Auditing was released in Windows 2000 initially.
* File Permissions – Windows 11 allows files to have RWX permissions set on a per file basis. This will determine whether each group or user on a system is able to read, write to, or execute the file. This process is performed by a user in a GUI in windows, opposed to Linux where it is often done in a CLI. File permissions were added to windows NT in 1993 and has been refined in subsequent versions.

1. MacOS X /Linux

* User Authentication – MacOS – Mac OS also uses its own auth system. This allows for conventional credential logins like in Windows as well as the option to log in with Apple ID (wind+ows also allows Microsoft login). This has been a feature since OS X was created in 2001.
* Access Control / Authorisation – Linux – Linux also has separate user spaces in which users can store their data, this data cannot be accessed by other users excluding administrators and root. Access Control is handled similarly to file permissions on Linux, using rwx values between 0 and 7. These can be set for groups and users and determine whether areas can be accessed by the user. Access control was in the initial release of Linux 0.12 in 1991.
* Drive Encryption – FileVault – FileVault is apples own full-disk encryption service that protects data stored on a Mac’s hard drive. To access the encrypted data the user must provide login credentials or a recovery key. (Apple, 2023) Apple introduced file vault to OS X 10.3 in 2003.
* Auditing – Linux (CentOS) – On CentOS you can install auditd, this includes a kernel component and a daemon component. The kernel component intercepts system calls from user apps, records events and sends these audit messages to the daemon, which creates log entries in a file. (auditd(8) — Linux manual page, 2021) Auditd was released in 2003.
* File Permissions – Linux (Red Hat) – Linux uses rwx between 0 and 7 to determine whether a user or group can read, write to, or execute a file these values can be set for users and groups. This will mostly be set in a CLI. (Red Hat, 2023) File permissions were added in 1991 in the initial release of Linux 0.12.

1. User Authentication Will have very little effect on application developers as it takes place before applications are run. However, a developer could, if the OS supported it, create an application with integration that allowed for the user to login with their user account for the computer. Windows and apple both offer this service for their in-house applications.

Access Control / Authorisation – Some applications will need access to areas that aren’t available to the user, installers in particular require access to space on the file system that is restricted to administrators (on Windows). This means that only certain users can perform these administrative tasks on a machine. Developers will need to consider who will be running their application and determine whether use the methods requiring admin privilege or perform the task a different way.

Drive Encryption will have very little effect on an application developer as before applications are run, the device must be encrypted. It would only affect the developer if the application was designed for working on external drives and the drive in use happened to be encrypted. In which case it is unlikely to be able to access any data as this is the purpose of drive encryption.

Auditing is also unlikely to have an effect on an application developer as all it would do is log if the application made system calls or other changes to the system and files. It would not interfere with the application. Logs could however be used theoretically in the development process for checking if the correct system changes are being made.

An application developer would have to consider file permissions as the user must be able to run the application, however the developer may want to prevent users from modifying or executing other files associated with the application. To do this they could set different file permissions on different files to tailor it to their purpose.

1. In conclusion, these File System features are essential to security in operating systems, and all provide their own security benefit. Authentication, authorisation, file permissions, access control and drive encryption all focus on prevention and auditing on identifying when a problem has occurred and remediation. To improve OS file systems, I would recommend hardening the system defaults, this would include making drive encryption the default so that it does not need to be activated by a user manually. I would do the same with auditing, as the operating systems I researched did not log by default. To improve authentication, I would also include restrictions on the chosen passwords for the user accounts, including length of password and inclusion of special characters and numbers as well as checking for commonly used passwords and blacklisting them.

# References

Apple. (2023). *Intro to FileVault*. Retrieved from https://support.apple.com/: https://support.apple.com/en-gb/guide/deployment/dep82064ec40/web

*auditd(8) — Linux manual page*. (2021, September). Retrieved from man7.org: https://man7.org/linux/man-pages/man8/auditd.8.html

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

Microsoft. (2021, July 29). *Credentials Processes in Windows Authentication*. Retrieved from https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication

Microsoft. (2022, December 16). *Audit File System*. Retrieved from https://learn.microsoft.com/: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-file-system

Microsoft. (2022, December 9). *BitLocker*. Retrieved from learn.microsoft.com: https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

Red Hat. (2023). *Chapter 25. Managing file permissions*. Retrieved from Access.redhat.com: https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/8/html/configuring\_basic\_system\_settings/assembly\_managing-file-permissions\_configuring-basic-system-settings