Table of Contents

[Introduction 2](#_Toc128302566)

[Security Features 2](#_Toc128302567)

[Access Control Lists (ACLs) 2](#_Toc128302568)

[File Permissions 2](#_Toc128302569)

[File Encryption 3](#_Toc128302570)

[Secure Boot 3](#_Toc128302571)

[Sandboxing 3](#_Toc128302572)

[Conclusion 3](#_Toc128302573)

[References 4](#_Toc128302574)

# make into page and not table

# Introduction

macOS is a UNIX-based operating system with its file system design and security as one of its primary goals. It provides various security features, including access control lists (ACLs), file permissions, file encryption, secure boot, and sandboxing, to prevent unauthorized access, ensure system integrity, and protect user data (Apple Inc., 2021). In this report, we will discuss the security features of the macOS file system and their implementation. (continue to list more features, -more marks more features)

# Security Features

Following are the security features that macOS offers:

FileVault

FileVault is a built-in encryption feature in macOS that encrypts the entire hard drive. When FileVault is enabled, all data on the hard drive is encrypted, including the operating system, applications, and user data. This provides protection against unauthorized access to data, even if the computer is lost or stolen.

Gatekeeper

Gatekeeper is a security feature in macOS that helps to protect the computer against malicious software. Gatekeeper ensures that only software from trusted developers can be installed on the computer. It does this by verifying the digital signature of the software before allowing it to be installed.

SIP (System Integrity Protection)

SIP is a security feature in macOS that protects system files and directories from being modified by unauthorized users or software. When SIP is enabled, certain critical system files and directories are protected from modification, even by the root user.

Time Machine

Time Machine is a backup feature in macOS that automatically backs up the entire system, including user data and applications. Time Machine provides a simple and easy-to-use backup solution that can be used to recover data in case of data loss due to hardware failure or other issues.

## Access Control Lists (ACLs)

macOS uses Access Control Lists (ACLs) to control access to files and directories. ACLs define permissions for specific users and groups, allowing or denying access to files and directories. This feature is useful in environments where multiple users can access the system, allowing for fine-grained control over file access.

## File Permissions

File permissions are an essential part of macOS file system security. Each file and directory have permissions defining who can read, write, and execute them (Apple Inc., 2021). Permissions are assigned to the owner of the file or directory, members of the group that owns the file, and all other users. The permissions can be set using the chmod command and viewed using the ls command with the -l option.

## File Encryption

macOS provides built-in encryption capabilities through its FileVault feature. FileVault encrypts the entire hard drive, protecting all user data from unauthorized access. The encryption key is securely stored in the system, and the user must enter a password to unlock the encrypted drive. This feature protects against data theft, even if the drive is physically removed from the system.

## Secure Boot

macOS uses secure boot to ensure that the operating system has not been tampered with during startup. The boot process verifies the integrity of the system's firmware, kernel, and other critical components, preventing malicious code from running. This feature protects against rootkits and other malware that attempt to modify the system's boot process.

## Sandboxing

macOS uses sandboxing to isolate applications and prevent them from accessing system resources without permission. Sandboxing limits the access that an application has to the system, reducing the risk of exploitation by malicious code. This feature also prevents applications from interfering with each other, improving the stability and security of the system.

How macOS Provides Security Features

macOS provides the above security features through various mechanisms. For example, FileVault is enabled through the System Preferences panel, where users can turn on encryption for their hard drive. Gatekeeper is enabled by default and can be configured in the Security & Privacy preferences panel. SIP is a system-level protection feature that is always enabled, and users cannot disable it. Time Machine can be configured through the Time Machine preferences panel, and it automatically backs up the system at regular intervals. – try find out how the other security features are provided. – create a graphic for the timeline, check if any missed features in timeline. – lower words : more space for comparison.

The timeline for these features is as follows:

* FileVault was introduced in Mac OS X 10.3 (Panther) in 2003, and it has been available in all subsequent versions of macOS.
* Gatekeeper was introduced in OS X 10.7 (Lion) in 2011, and it has been available in all subsequent versions of macOS.
* SIP was introduced in OS X 10.11 (El Capitan) in 2015, and it has been available in all subsequent versions of macOS.
* Time Machine was introduced in OS X 10.5 (Leopard) in 2007, and it has been available in all subsequent versions of macOS.

# Conclusion

The macOS file system is designed with security as one of its primary goals. It provides various security features, including access control lists (ACLs), file permissions, file encryption, secure boot, and sandboxing. These features work together to prevent unauthorized access, ensure the system's integrity, and protect user data. By using these security features, macOS provides a secure platform for users to work on.- finish last

# References

* Apple Inc. (2021). macOS Security Architecture. Retrieved from <https://developer.apple.com/library/archive/documentation/Security/Conceptual/Security_Overview/Introduction/Introduction.html>
* Apple Inc. (2021). macOS User Guide. Retrieved from <https://support.apple.com/guide/mac-help/welcome/mac>
* Apple Inc. (2022). macOS Catalina. https://www.apple.com/macos/catalina/
* Apple Inc. (2022). macOS Developer Documentation. https://developer.apple.com/documentation/macos-release-notes
* Apple Inc. (2022). macOS High Sierra. <https://www.apple.com/macos/high-sierra/>

make into Harvard style and cite at end (5% marks so spend time on it)