**NT212 – AN TOÀN DỮ LIỆU VÀ KHÔI PHỤC THÔNG TIN SAU SỰ CỐ**

**BÁO CÁO BÀI TẬP 2.2**

***Data Integrity trong hệ điều hành Mac OS***

**\*\*\***

# THÔNG TIN CHUNG

## 1. Thông tin nhóm

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Dương Phạm Huy Thông | 22521431 | 22521431@gm.uit.edu.vn |
| 2 | Cao Quí | 22521208 | 22521208@gm.uit.edu.vn |

## 2. Nội dung thực hiện

**Yêu cầu:** Nghiên cứu và trình bày về các cơ chế để đảm bảo Data Integrity đã được thiết lập sẵn trong hệ điều hành Mac OS. Đánh giá mức độ hiệu quả tương ứng.

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Nội dung** | **Tự đánh giá** | **Phụ trách** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |

***Bên dưới đây là toàn bộ bài báo cáo chi tiết đã được nhóm thực hiện.***

# BÀI LÀM

## 1. Tổng quan về các cơ chế đảm bảo Data Integrity trên hệ điều hành Mac OS.

**Data Integrity** hay **Tính toàn vẹn của dữ liệu** được định nghĩa là khả năng đảm bảo dữ liệu chính xác, hoàn chỉnh và không bị thay đổi hoặc hỏng hóc trong suốt vòng đời của nó[[1]](#footnote-1). Trong môi trường hệ điều hành Mac OS, việc bảo vệ tính toàn vẹn dữ liệu là cực kỳ quan trọng, đặc biệt khi mọi chức năng như lưu trữ và xử lý thông tin cá nhân, công việc cũng như dữ liệu nhạy cảm của người dùng đều phải phụ thuộc vào hệ thống. Sự mất mát hoặc thay đổi không hợp pháp liên quan đến dữ liệu có thể dẫn đến hậu quả nghiêm trọng, trong đó có thể kể đến là việc mất mát thông tin cá nhân cho đến ảnh hưởng đến hoạt động kinh doanh, như mất dữ liệu quan trọng trong các tổ chức tài chính hoặc y tế.

Các khái niệm cơ bản liên quan đến Data Integrity bao gồm:

***Checksum (mã kiểm tra lỗi)***, được sử dụng để xác minh tính toàn vẹn của dữ liệu bằng cách tạo ra một giá trị duy nhất dựa trên nội dung dữ liệu, giúp phát hiện lỗi nếu dữ liệu bị thay đổi.

***Mã băm (Hash) như SHA-256***, giúp xác định xem tệp có bị thay đổi hay không cũng thường được sử dụng trong việc xác minh tệp tải xuống.

***Bản sao lưu dữ liệu (Backup)***, cho phép khôi phục dữ liệu trong trường hợp xảy ra lỗi, như khi hệ thống bị crash hoặc bị tấn công ransomware.

Những khái niệm này rất quan trọng đối với người dùng Mac OS vì chúng đảm bảo rằng dữ liệu hệ thống và người dùng không bị hỏng do lỗi phần cứng, phần mềm, hoặc các cuộc tấn công mạng, chẳng hạn như malware lợi dụng quyền root để thay đổi tệp hệ thống.

Mac OS tích hợp sẵn nhiều cơ chế để đảm bảo Data Integrity[[2]](#footnote-2), bao gồm các tính năng an ninh hệ thống như System Integrity Protection (SIP), bảo vệ file system thông qua Apple File System (APFS) với các tính năng như snapshots, clones, và checksums, cũng như quản lý phân quyền và mã hóa dữ liệu với FileVault. Những cơ chế này phối hợp để tạo ra một môi trường an toàn, giảm thiểu rủi ro mất mát hoặc thay đổi dữ liệu không mong muốn, đặc biệt trong bối cảnh ngày càng nhiều mối đe dọa an ninh mạng.

## 2. Các chức năng bảo toàn dữ liệu trên Mac OS

### a. System Integrity Protection (SIP):

**System Integrity Protection (SIP)** được giới thiệu từ OS X El Capitan vào năm 2015[[3]](#footnote-3), là một cơ chế an ninh dữ liệu cốt lõi giúp bảo vệ các tệp và hệ thống thư mục khỏi các thay đổi trái phép, đặc biệt là ngay cả khi được thực hiện bởi người dùng root hoặc với quyền quản trị viên.

SIP hoạt động bằng cách sử dụng các quyền hạn bắt buộc *(****mandatory access controls****)* để hạn chế quyền ghi vào các khu vực hệ thống quan trọng, như ***/System, /bin, và /sbin***. Chúng chỉ cho phép các quy trình được ký bởi Apple và có quyền đặc biệt ***(entitlements)*** mới có thể thực hiện quyền thay đổi, ví dụ tiêu biểu là bản cập nhật hệ thống chính thức. Chính điều này giúp ngăn chặn phần mềm độc hại lợi dụng quyền root để chỉnh sửa hệ thống, từ đó bảo vệ tính toàn vẹn của dữ liệu hệ thống, đặc biệt trong các môi trường đơn người dùng, nơi người dùng cũng là quản trị viên, dễ bị tấn công[[4]](#footnote-4).

Trong thực tế, SIP thường được người dùng nhận thấy khi cố gắng cài đặt phần mềm từ nguồn không rõ ràng hoặc chạy các lệnh cần quyền root, chẳng hạn như khi sử dụng Terminal. Ví dụ, nếu một ứng dụng cố gắng ghi vào thư mục hệ thống mà không có quyền, hệ thống sẽ hiển thị thông báo lỗi, yêu cầu người dùng tắt SIP thông qua chế độ ***Recovery Mode*** bằng cách khởi động lại máy, giữ phím Cmd + R, mở Terminal và nhập lệnh *"csrutil disable"*. Tuy nhiên, Apple khuyến cáo không nên vô hiệu hóa SIP trừ khi cần thiết, vì điều này có thể làm tăng nguy cơ bảo mật, đặc biệt trong các hệ thống không được quản lý chặt chẽ. Một trường hợp cụ thể là khi cập nhật hệ thống, SIP đảm bảo rằng chỉ các bản cập nhật được ký bởi Apple, như bản cập nhật macOS Sonoma, mới có thể thay đổi các tệp hệ thống, giảm thiểu rủi ro từ phần mềm độc hại giả mạo bản cập nhật.

### b. File System Integrity and APFS Features:

**Apple File System (APFS)** được giới thiệu từ macOS High Sierra vào năm 2017, là một hệ thống tệp được thiết kế tối ưu cho ổ SSD, với nhiều tính năng hỗ trợ bảo vệ tính toàn vẹn dữ liệu[[5]](#footnote-5).

APFS sử dụng thuật toán checksum mà cụ thể là **Fletcher’s checksum**[[6]](#footnote-6)nhằm đảm bảo tính toàn vẹn của metadata. Qua đó giúp phát hiện lỗi nếu metadata bị hỏng do lỗi **phần cứng** *(ví dụ như ổ SSD bị bad sector)* hoặc **phần mềm** *(ví dụ như lỗi trong quá trình cập nhật hệ thống)*. Ngoài ra, APFS áp dụng **cơ chế copy-on-write**, tránh ghi đè trực tiếp lên dữ liệu hiện có, từ đó bảo vệ dữ liệu khỏi bị mất mát trong trường hợp hệ thống gặp sự cố như mất điện hoặc crash. Chính điều này giúp APFS cải tiến hơn so với HFS+, bởi vì hệ thống tệp cũ HFS+ cần ghi hai lần (journaling). Hơn thế nữa, **tính năng snapshots** cho phép tạo bản sao read-only tại một thời điểm nhất định, hỗ trợ khôi phục dữ liệu nhanh chóng khi cần thiết. Ví dụ như khi người dùng vô tình xóa tệp quan trọng, hệ thống có thể hỗ trợ khôi phục dữ liệu ngay từ nguồn bản sao read-only. **Tính năng clones** là một tính năng khác giúp tối ưu hóa không gian lưu trữ bằng cách tạo bản sao nhanh của tệp mà không sao chép toàn bộ dữ liệu, giảm nguy cơ lỗi trong quá trình sao chép.

Người dùng có thể nhận thấy các tính năng này thông qua các thông báo hệ thống khi xảy ra lỗi. Ví dụ:

- Khi APFS phát hiện metadata bị hỏng và tự động sử dụng bản sao dự phòng để sửa lỗi

- Khi sử dụng Time Machine để khôi phục dữ liệu, snapshots của APFS giúp giảm thời gian khôi phục bằng cách cung cấp phiên bản trước đó của tệp.

Một ví dụ thực tế là trong môi trường doanh nghiệp, các quản trị viên hệ thống sử dụng snapshots để tạo bản sao định kỳ, đảm bảo có thể khôi phục dữ liệu trong trường hợp ransomware tấn công. Các báo cáo từ chuyên gia an ninh mạng cũng như từ các bài phân tích trên [Intego](https://www.intego.com/mac-security-blog/the-ins-and-outs-of-apples-new-file-system-apfs/) cũng chỉ ra rằng APFS cải thiện đáng kể khả năng chống lại lỗi phần cứng nhờ tích hợp **ECC (Error Correcting Code)** trong ổ SSD của Apple, đảm bảo dữ liệu không bị thay đổi trong quá trình truyền tải[[7]](#footnote-7). Dù vậy, APFS vẫn gặp một số hạn chế là không cung cấp checksum cho dữ liệu người dùng, phụ thuộc vào ECC, có thể không đủ trong một số trường hợp lỗi nghiêm trọng(ví dụ như ổ SSD bị hỏng hoàn toàn).

### c. Encryption with FileVault:

**FileVault** là một cơ chế mã hóa toàn bộ đĩa được tích hợp sẵn trong Mac OS, chúng sử dụng chuẩn mã hóa **AES-XTS 128-bit** để bảo vệ dữ liệu ở trạng thái nghỉ (data at rest)[[8]](#footnote-8). Bằng cách mã hóa toàn bộ ổ đĩa, FileVault đảm bảo rằng ngay cả khi thiết bị xảy ra kịch bản đánh cắp hoặc truy cập trái phép về mặt vật lý thì dữ liệu vẫn không thể bị đọc khi không có mật khẩu hoặc khóa giải mã. Chí vì lý do đó mà cơ chế này có thể ngăn chặn việc thay đổi hoặc truy cập không được phép vào dữ liệu, đặc biệt trong môi trường doanh nghiệp hoặc cá nhân sử dụng dữ liệu nhạy cảm (như thông tin tài chính hoặc y tế).

FileVault hoạt động bằng cách yêu cầu người dùng nhập mật khẩu khi khởi động máy và dữ liệu chỉ được giải mã khi có khóa hợp lệ, điều này góp phần vào Data Integrity bằng cách đảm bảo dữ liệu không bị tampered (thay đổi trái phép) ngay cả khi thiết bị bị xâm nhập vật lý.

Trong thực tế, người dùng có thể bật FileVault thông qua ***System Preferences > Security & Privacy > FileVault*** và hệ thống sẽ yêu cầu nhập mật khẩu để giải mã khi khởi động. Quản trị viên hệ thống thường sử dụng FileVault để bảo vệ dữ liệu trong trường hợp mất máy, với ví dụ cụ thể là các tổ chức tài chính yêu cầu nhân viên kích hoạt FileVault để tuân thủ quy định bảo mật, như GDPR hoặc HIPAA. Khi xảy ra sự cố như quên mật khẩu, FileVault cho phép khôi phục thông qua khóa khôi phục được lưu trữ an toàn, chẳng hạn trong iCloud, đảm bảo tính toàn vẹn của dữ liệu không bị ảnh hưởng, và người dùng có thể truy cập lại dữ liệu mà không cần định dạng lại ổ đĩa.

## 3. Tổng kết

Tóm lại, Mac OS tích hợp nhiều cơ chế quan trọng để đảm bảo Data Integrity, bao gồm System Integrity Protection (SIP) để bảo vệ tệp hệ thống khỏi thay đổi trái phép, Apple File System (APFS) với checksums và copy-on-write để bảo vệ tính toàn vẹn tệp, và FileVault để mã hóa dữ liệu ở trạng thái nghỉ. Mỗi cơ chế đều có điểm mạnh:

- **SIP** tăng cường an ninh hệ thống bằng cách hạn chế quyền root

- **APFS** cải thiện khả năng chống lỗi phần cứng với snapshots và copy-on-write

- **FileVault** bảo vệ dữ liệu nhạy cảm khỏi truy cập trái phép.

Tuy nhiên, một hạn chế là APFS không cung cấp checksum cho dữ liệu người dùng, phụ thuộc vào ECC của phần cứng, có thể không đủ trong một số trường hợp lỗi nghiêm trọng, như ổ SSD bị hỏng hoàn toàn, còn với SIP lại có thể gây khó khăn cho người dùng khi cần chỉnh sửa hệ thống, đòi hỏi quy trình phức tạp để vô hiệu hóa.

Các cơ chế này phối hợp chặt chẽ để tạo ra một môi trường an toàn cho người dùng Mac OS, đặc biệt trong bối cảnh ngày càng nhiều mối đe dọa an ninh mạng, như ransomware hoặc tấn công phần mềm độc hại.

Nhìn về tương lai, Apple có thể cân nhắc bổ sung tính năng checksum cho dữ liệu người dùng trong APFS hoặc tích hợp thêm các công nghệ như ZFS, vốn hỗ trợ checksum cho cả dữ liệu và metadata, để tăng cường khả năng phát hiện lỗi. Những cải tiến này có thể giúp Mac OS duy trì vị thế dẫn đầu trong bảo mật và tính toàn vẹn dữ liệu, đáp ứng nhu cầu ngày càng cao của người dùng doanh nghiệp và cá nhân.

1. [What is Data Integrity | Issues & Types Explained | Imperva](https://www.imperva.com/learn/data-security/data-integrity/) [↑](#footnote-ref-1)
2. [Operating system integrity - Bộ phận hỗ trợ của Apple (VN)](https://support.apple.com/vi-vn/guide/security/sec8b776536b/web) [↑](#footnote-ref-2)
3. [System Integrity Protection - Wikipedia](https://en.wikipedia.org/wiki/System_Integrity_Protection) [↑](#footnote-ref-3)
4. [About System Integrity Protection on your Mac - Apple Support](https://support.apple.com/en-us/102149) [↑](#footnote-ref-4)
5. [Apple File System - Wikipedia](https://en.wikipedia.org/wiki/Apple_File_System) [↑](#footnote-ref-5)
6. [Frequently Asked Questions](https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/APFS_Guide/FAQ/FAQ.html) [↑](#footnote-ref-6)
7. [The Ins and Outs of Apple's New File System, APFS - The Mac Security Blog](https://www.intego.com/mac-security-blog/the-ins-and-outs-of-apples-new-file-system-apfs/) [↑](#footnote-ref-7)
8. [How to Encrypt and Password Protect Files on Your Mac - The Mac Security Blog](https://www.intego.com/mac-security-blog/how-to-encrypt-and-password-protect-files-on-your-mac/) [↑](#footnote-ref-8)