HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI TẬP LỚN
HỌC PHẦN: AN TOÀN HỆ ĐIỀU HÀNH
MÃ HỌC PHẦN: INT1484

ĐỀ TÀI: TÌM HIỂU HỆ ĐIỀU HÀNH CHO CÁC THIẾT BỊ DI ĐỘNG APPLE IOS

Các sinh viên thực hiện (trưởng nhóm xếp số 1):

B22DCAT063	Lê Tiến Dương
B22DCAT027	Đồng Gia Bảo
B22DCAT028	Lê Đình Bảo
B22DCAT064	Nguyễn Đăng Dương
B22DCAT052	Nguyễn Khắc Dũng
B22DCAT038	Đỗ Huy Cường

Tên nhóm: 02

Tên lớp: 02

Giảng viên hướng dẫn: PGS. TS. Hoàng Xuân Dậu

HÀ NỘI 3-2025

PHÂN CÔNG NHIỆM VỤ NHÓM THỰC HIỆN

TT	Công việc / Nhiệm vụ	SV thực hiện	Thời hạn hoàn thành
1	Thuyết trình, tìm hiểu phần tổng quan về iOS.	Đồng Gia Bảo	22/02/2025
2	Tìm hiểu phần cài đặt iOS.	Lê Đình Bảo	16/02/2025
3	Tìm hiểu phần tính năng nổi bật của iOS.	Đỗ Huy Cường	16/02/2025
4	Tìm hiểu kiến trúc, thành phần của iOS, demo.	Nguyễn Khắc Dũng	16/02/2025
5	Tìm hiểu các vấn đề an ninh, an toàn. Tổng hợp lại lý thuyết, chỉnh sửa báo cáo, làm demo, làm slide thuyết trình.	Lê Tiến Dương	05/03/2025
6	Tìm hiểu các vấn đề an ninh, an toàn, demo.	Nguyễn Đăng Dương	18/02/2025

NHÓM THỰC HIỆN TỰ ĐÁNH GIÁ

TT	SV thực hiện	Thái độ tham gia	Mức hoàn thành CV	Kỹ năng giao tiếp	Kỹ năng hợp tác	Kỹ năng lãnh đạo
1	Đồng Gia Bảo	4	3	3	3	1
2	Lê Đình Bảo	5	5	3	3	1
3	Đỗ Huy Cường	5	5	3	3	1
4	Nguyễn Khắc Dũng	5	5	5	5	2
5	Lê Tiến Dương	5	5	5	5	5
6	Nguyễn Đăng Dương	5	4	5	5	3

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
OTA	Over The Air	Cập nhật phần mềm qua mạng không dây
DFU	Device Firmware Upgrade	Chế độ khôi phục phần mềm thiết bị
XNU	X is Not Unix	Nhân hệ điều hành của iOS
BSD	Berkeley Software Distribution	Hệ thống UNIX được sử dụng trong iOS
VPN	Virtual Private Network	Mạng riêng ảo
2FA	Two-Factor Authentication	Xác thực hai yếu tố
SEP	Secure Enclave Processor	Bộ xử lý bảo mật trong các thiết bị Apple
JIT	Just-In-Time Compilation	Kỹ thuật biên dịch tức thời giúp tối ưu hiệu suất
KPP	Kernel Patch Protection	Cơ chế bảo vệ nhân hệ điều hành
KTRR	Kernel Text Read-Only Region	Vùng bảo vệ chống ghi trong nhân iOS

MỞ ĐẦU

Trong bối cảnh các mối đe dọa an ninh mạng ngày càng gia tăng, an toàn hệ điều hành trở thành yếu tố sống còn đối với các thiết bị di động, nơi lưu trữ hàng loạt dữ liệu nhạy cảm của người dùng. iOS, hệ điều hành dành riêng cho các thiết bị Apple như iPhone, iPad và iPod Touch, nổi bật với kiến trúc bảo mật tiên tiến và các cơ chế bảo vệ chặt chẽ, trở thành một trong những nền tảng an toàn nhất hiện nay.

Tuy nhiên, không hệ điều hành nào hoàn toàn miễn nhiễm trước các lỗ hổng và tấn công. Với môn học "An toàn hệ điều hành" làm nền tảng, bài báo cáo này khám phá iOS qua các góc độ quan trọng: tổng quan giới thiệu, kiến trúc hệ thống, thành phần cốt lõi, phương pháp cài đặt, tính năng nổi bật, đặc biệt tập trung vào các vấn đề an ninh và an toàn mà iOS đối mặt. Qua đó, nghiên cứu không chỉ làm sáng tỏ những điểm mạnh trong thiết kế bảo mật của iOS mà còn phân tích các thách thức tiềm ẩn, cung cấp cái nhìn sâu sắc về cách bảo vệ hệ điều hành trước các mối đe dọa trong môi trường số hiện đại.

Báo cáo bài tập lớn gồm 4 chương với nội dung chính như sau:

- Chương 1 nghiên cứu tổng quan về hệ điều hành iOS, bao gồm các nội dung về giới thiệu chung, lịch sử phát triển của hệ điều hành iOS.
- Chương 2 thực hiện việc phân tích kiến trúc và các thành phần của hệ điều hành iOS, bao gồm nhiều lớp và nhiều thành phần khác nhau.
- Chương 3 đưa ra các phương pháp cài đặt hệ điều hành iOS tùy vào nhu cầu của người dùng và giới thiệu các tính năng nổi bật mà hệ điều hành này mang lại.
- Chương 4 đề cập đến những vấn đề an ninh, an toàn mà hệ điều hành iOS gặp phải và thực nghiệm chế độ phong tỏa trên thiết bị sử dụng hệ điều hành iOS.

CHƯƠNG 1. TỔNG QUAN VỀ HỆ ĐIỀU HÀNH IOS

1.1 Giới thiệu chung

iOS (iPhone Operating System) là hệ điều hành do hãng Apple phát triển cho các thiết bị điện thoại thông minh iPhone, máy tính bảng iPad và máy nghe nhạc iPod của hãng này. Phiên bản thương mại đầu tiên của iOS được giới thiệu vào năm 2007 và hiện nay đây là một trong những hệ điều hành thông dụng nhất cho thiết bị di động bên cạnh Android. Apple giữ độc quyền về hệ điều hành này và không cung cấp bản quyền để chạy iOS trên thiết bị của nhà sản xuất khác.

Như các sản phẩm khác của Apple, tiêu chí đặt ra khi thiết kế iOS là giúp cho việc sử dụng thiết bị di động được thuận tiện, dễ dàng, thậm chí đối với người không biết nhiều về kỹ thuật. Đây là yếu tố quan trọng đảm bảo sự thành công cho hệ điều hành này.

1.2 Lịch sử phát triển

iOS, hệ điều hành di động của Apple, đã trải qua hành trình phát triển từ năm 2007, định hình công nghệ di động với bảo mật và hiệu suất vượt trội. Sau đây là các giai đoạn phát triển chính của iOS, từ khởi nguồn đến hiện tại (tháng 2/2025), làm rõ sự đổi mới và tầm ảnh hưởng của hệ điều hành này.

Hình 1 – Lịch sử phát triển của iOS từ 2007 đến 2022

- **Khởi nguồn và mở rộng (2007-2012):** iOS ra mắt ngày 29/6/2007 với tên iPhone OS 1.0, cùng iPhone đầu tiên, sử dụng XNU kernel từ macOS, giới thiệu giao diện cảm ứng đa điểm. iPhone OS 2 (2008) mang đến App Store, mở hệ sinh thái ứng dụng. iPhone OS 3 (2009) thêm MMS và Push Notifications. Đổi tên thành iOS từ iOS 4 (2010), hỗ trợ đa nhiệm và FaceTime. iOS 5 (2011) giới thiệu Siri và iCloud, iOS 6 (2012) ra Apple Maps.

- **Bảo mật và thiết kế mới (2013-2016)**: iOS 7 (2013) áp dụng thiết kế phẳng, thêm Touch ID. iOS 8 (2014) tích hợp Apple Pay, Handoff. iOS 9 (2015) cải thiện hiệu suất, iOS 10 (2016) nâng cấp iMessage và Siri.
- **Hiện đại hóa (2017-2021)**: iOS 11 (2017) ra Face ID, iOS 12 (2018) tối ưu thiết bị cũ với Screen Time. iOS 13 (2019) có Dark Mode, iOS 14 (2020) thêm Widget, iOS 15 (2021) cải thiện quyền riêng tư.
- **Trí tuệ nhân tạo (2022-2025)**: iOS 16 (2022) tùy chỉnh màn hình khóa, iOS 17 (2023) bổ sung StandBy Mode. iOS 18 (2024) ra Apple Intelligence, nâng cấp AI và Siri. Đến tháng 2/2025, iOS 18.x tiếp tục hoàn thiện bảo mật và AI.

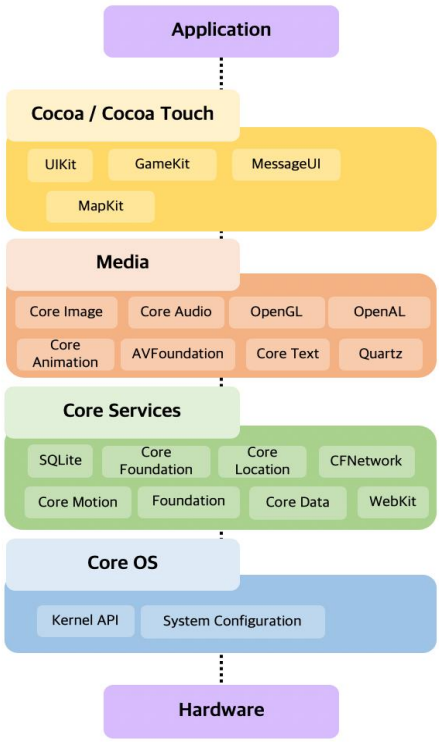
Hình 2 – iOS 17 ra mắt năm 2023 và iOS 18 ra mắt năm 2024

Hành trình phát triển của iOS từ iPhone OS 1.0 (2007) đến iOS 18 (2025) phản ánh sự chuyển mình từ một hệ điều hành đơn giản thành nền tảng dẫn đầu về bảo mật và hiệu suất. Các cột mốc như App Store (2008), Touch ID (2013), Face ID (2017), và Apple Intelligence (2024) không chỉ nâng cao trải nghiệm người dùng mà còn củng cố an toàn hệ thống qua hành trình cập nhật liên tục. Sự tích hợp chặt chẽ với hệ sinh thái Apple đã định hình iOS thành chuẩn mực trong công nghệ di động, đồng thời đặt nền tảng cho các phân tích sâu hơn về cơ chế bảo mật và thách thức an ninh trong các phần tiếp theo.

CHƯƠNG 2. KIẾN TRÚC VÀ CÁC THÀNH PHẦN CỦA HỆ ĐIỀU HÀNH IOS

2.1 Kiến trúc

Kiến trúc của iOS là kiến trúc phân lớp. Với cấu trúc phân lớp, các ứng dụng không giao tiếp trực tiếp với phần cứng mà giao tiếp với phần cứng thông qua các giao diện được hệ thống xác định. Kiến trúc iOS được phân ra thành 4 lớp theo hình:



Hình 3 – Kiến trúc hệ điều hành iOS

2.1.1 Lớp Core OS

Lớp Core OS là lớp nằm cuối cùng trong ngăn xếp iOS, ngay đầu phần cứng của thiết bị. Nó chứa các tính năng cấp thấp mà hầu hết các công nghệ khác được xây dựng trên đó. Các công nghệ lớp Core OS bao gồm:

- *Accelerate Framework*: Framework này thực hiện các tính toán toán học quy mô lớn và tính toán hình ảnh, được tối ưu hóa cho hiệu suất cao và tiêu thụ năng lượng thấp.
- *Security Services Framework*: Framework này kiểm soát quyền truy cập vào ứng dụng và dữ liệu mà ứng dụng duy trì.
- *Local Authorization Framework*: Framework này xác thực người dùng bằng sinh trắc học hoặc mật khẩu.
- *External Accessories Framework*: Framework này giao tiếp với các phụ kiện của thiết bị được kết nối qua Bluetooth hoặc đầu nối Apple Lightning.

Lớp Core OS hỗ trợ 64-Bit từ IOS7 hỗ trợ phát triển ứng dụng 64-bit và cho phép ứng dụng chạy nhanh hơn.

2.1.2 Lớp Core Services

Lớp Core Services thường được xây dựng dựa trên chức năng được cung cấp bởi Core OS để cung cấp các tính năng phức tạp hơn và dành riêng cho ứng dụng. Dịch vụ cốt lõi cung cấp các dịch vụ thiết yếu cho ứng dụng nhưng không ảnh hưởng trực tiếp đến giao diện người dùng của ứng dụng. Lớp này cung cấp một tập hợp Framework bao gồm:

- *Address Book framework*: Cấp quyền truy cập theo chương trình vào cơ sở dữ liệu liên hệ của người dùng.
- *Cloud Kit framework*: Cung cấp phương tiện để di chuyển dữ liệu giữa ứng dụng của người dùng và iCloud.
- *Core Foudation framework*: Cung cấp các tính năng quản lý dữ liệu và dịch vụ cơ bản cho các ứng dụng iOS.
- *Core Lotion Framework*: Cung cấp thông tin vị trí và tiêu đề cho các ứng dụng.
- *Core Motion Framework*: Truy cập tất cả dữ liệu dựa trên chuyển động có sẵn trên thiết bị. Sử dụng khung chuyển động cốt lõi này, thông tin dựa trên gia tốc kế có thể được truy cập.
- *Foundation Framework*: Cung cấp một lớp chức năng cơ bản cho các ứng dụng và framework, bao gồm lưu trữ và duy trì dữ liệu, xử lý văn bản, tính toán ngày và giờ, sắp xếp, lọc, cũng như kết nối mạng. Các lớp, giao thức và kiểu dữ liệu được xác định bởi Foundation được sử dụng trong các SDK macOS, iOS, watchOS và tvOS..
- *Social framework*: Truy cập các tài khoản mạng xã hội của người dùng.
- *StoreKit framework*: Hỗ trợ mua hàng trong ứng dụng và tương tác với App Store.

2.1.3 Lớp Media

Lớp Media xử lý tất cả các dịch vụ âm thanh, video, đồ họa và hoạt họa theo yêu cầu của các ứng dụng.

- *Khung đồ họa:*
    - *UIKit Graphics*: Mô tả hỗ trợ cấp cao để thiết kế hình ảnh và được sử dụng để tạo hoạt ảnh cho nội dung chế độ xem của người dùng.
    - *Core Graphics framework*: Vẽ gốc cho các ứng dụng iOS và hỗ trợ kết xuất dựa trên hình ảnh và vector 2D tùy chỉnh.
    - *Core Animation*: Giúp tối ưu hóa trải nghiệm hoạt họa cho các ứng dụng của người dùng.
    - *Core Images*: Hỗ trợ nâng cao để điều khiển video và hình ảnh bất động theo cách hoàn chỉnh, không bị phá hoại.
    - *Metal*: Cho phép hiệu suất rất cao cho các công việc tính toán và kết xuất đồ họa phức tạp của người dùng
- *Khung âm thanh:*

- *Media Player Framework*: Giúp sử dụng thư viện iTunes của người dùng đơn giản và hỗ trợ phát danh sách phát.
- *AV Foundation*: Giao diện Objective C để xử lý việc ghi và phát lại âm thanh và video.
- *OpenAL*: Công nghệ tiêu chuẩn công nghiệp để cung cấp âm thanh.

- *Khung video:*
  - *AV Kit*: Cung cấp một bộ sưu tập các giao diện dễ sử dụng để trình bày video.
  - *AV Foundation*: Cung cấp khả năng phát lại và ghi video nâng cao.
  - *Core Media*: Mô tả các giao diện cấp thấp và kiểu dữ liệu để vận hành phương tiện.

2.1.4 Lớp CoCoa Touch

Lớp CoCoa Touch cung cấp một lớp trừu tượng giúp các thư viện khác nhau cho iPhone và các thiết bị iOS khác có thể truy cập được. Lớp này hỗ trợ thông báo, đa nhiệm, đầu vào dành riêng cho cảm ứng, tất cả các dịch vụ hệ thống cấp cao và các công nghệ quan trọng khác. Nó cũng cung cấp hỗ trợ cơ sở hạ tầng cơ bản cho một ứng dụng. Lớp CoCoa Touch chứa một số Framework như:

- *Event Kit UI framework*: Mô tả một giao diện hệ thống chung sử dụng bộ điều khiển chế độ xem để hiển thị và thay đổi các sự kiện.
- *Game Kit framework*: Cho phép người dùng chia sẻ dữ liệu liên quan đến trò chơi của họ trực tuyến thông qua Game Center.
- *Map Kit framework*: Cung cấp một bản đồ có thể cuộn và được đưa vào giao diện người dùng của ứng dụng.
- *Message UI framework*: Xây dựng giao diện soạn email và tin nhắn văn bản để người dùng có thể cập nhật và gửi tin nhắn mà không cần rời khỏi ứng dụng của họ.
- *UI Kit framework*: Cung cấp nền tảng quan trọng để phát triển các ứng dụng đồ họa, theo hướng sự kiện cho iOS. Một số tính năng quan trọng nhất của UI Kit framework là:
  - Hỗ trợ đa nhiệm.
  - Cơ sở hạ tầng và quản lý ứng dụng cơ bản.
  - Quản trị giao diện người dùng.
  - Hỗ trợ các thao tác cảm ứng và chuyển động.

2.2 Các thành phần

2.2.1 Quản lý bộ nhớ

iOS sử dụng phương pháp quản lý bộ nhớ phức tạp để đảm bảo sử dụng hiệu quả tài nguyên bộ nhớ của nó. Các khái niệm quản lý bộ nhớ trong iOS bao gồm :

- *Không gian địa chỉ lớn*: iOS đạt được điều này thông qua việc sử dụng bộ nhớ ảo. Bộ nhớ ảo trong iOS có thể được điều chỉnh cho phù hợp với yêu cầu của người dùng.
- *Sự che chở*: Các không gian địa chỉ ảo theo các tiến trình khác nhau và cơ chế phần cứng không cho phép ghi đè các không gian địa chỉ ảo được bảo vệ.
- *Lập bản đồ bộ nhớ*: Về cơ bản được sử dụng để ghi dữ liệu vào vị trí địa chỉ vật lý của các tiến trình.
- *Phân bổ bộ nhớ địa chỉ vật lý công bằng*: Mục tiêu của quản lý bộ nhớ là đảm bảo mỗi tiến trình nhận được một lượng bộ nhớ hợp lý theo yêu cầu của nó và bộ nhớ có sẵn.

Hình 4 – Giao diện quản lý bộ nhớ của thiết bị iOS

2.2.2 Giao diện người dùng (User Interface)

Giao diện người dùng (UI) của iOS nổi bật với thiết kế trực quan, tối giản và dễ sử dụng, được tối ưu hóa cho màn hình cảm ứng. Giao diện này được Apple liên tục cập nhật và cải tiến qua các phiên bản, với một trong những thay đổi lớn nhất diễn ra ở iOS 7 khi Apple chuyển sang phong cách thiết kế phẳng (flat design) với màu sắc tươi sáng và các hiệu ứng chuyển động mượt mà.

Hình 5 – Giao diện người dùng phát triển theo từng giai đoạn

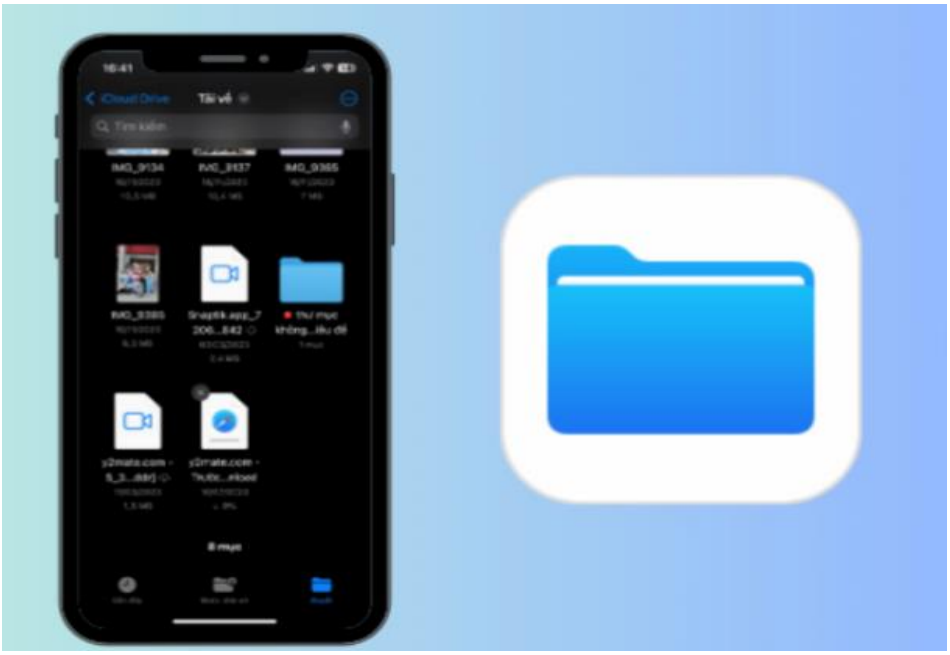
2.2.3 Quản lý mạng

Một khả năng thiết yếu mà điện thoại thông minh phải có là có thể truy cập mạng và tài nguyên mạng trong bất kỳ cài đặt nhất định nào. Do đó, iOS phải kết hợp khả năng truy cập mạng vào hệ điều hành. Để đạt được những điều này, iOS có các dịch vụ quản lý mạng sẵn có chạy dưới dạng các tiến trình nền.

Ngoài các dịch vụ quản lý mạng có sẵn được tích hợp vào iOS, Apple Inc. đã phát triển các ứng dụng quản lý mạng như Brooklyn cho Nagios, có khả năng giám sát hệ thống Nagios cho phép quản trị viên mạng điều khiển mạng từ xa thông qua điện thoại thông minh.

iOS cũng kết hợp các khả năng của iPhone để có quyền truy cập vào mạng WLAN thông qua việc sử dụng hệ thống Wi-Fi tích hợp trong iPhone. iPhone được tích hợp các cảm biến mạng không dây có thể phát hiện bất kỳ môi trường nào đang phát tín hiệu không dây phù hợp với tần số của iPhone. Các phương pháp truy cập mạng khác được phát triển bởi iOS bao gồm 3G, 4G và Bluetooth.

2.2.4 Quản lý file và thư mục



Hình 6 – Quản lý file và thư mục trong iOS

Hệ điều hành iOS có thể lưu trữ và quản lý các file, văn bản, bảng tính, hình ảnh,... nhờ vào ứng dụng Tệp. Sau đây là một số thông tin về cách quản lý file và thư mục trên hệ điều hành iOS:

- *Lưu file và thư mục về máy*:
  - Truy cập trang web muốn tải file -> Mở file muốn tải -> Chọn icon “Chia sẻ”.
  - Chọn “Lưu vào tệp” tự động màn hình chuyển qua ứng dụng Tệp -> Chọn “Lưu” để tải về.
- *Mở file và thư mục*: Bật ứng dụng “Tệp” -> Nhìn lên phía trên màn hình sẽ thấy ô tìm kiếm -> Gõ tên file cần tìm -> File người dùng cần tìm sẽ xuất hiện ngay lập tức.

- *Xóa file và thư mục*: Để xóa một file hoặc thư mục, chạm và giữ một file hoặc thư mục, sau đó chọn "Xóa".
- *Sắp xếp, quản lý file và thư mục*: Mở ứng dụng "Tệp" -> Nhấn vào biểu tượng 4 ô vuông nhỏ và chọn cách sắp xếp phù hợp mới nhu cầu của người dùng.
- *Khôi phục file và thư mục đã xóa*: Truy cập vào mục "Duyệt" -> Chọn "Đã xóa gần đây". Tìm tệp cần khôi phục và nhấn giữ -> Chọn "Khôi phục" và tệp sẽ được phục hồi.

2.2.5 Quản lý vào/ra

Trên hệ điều hành iOS, quản lý vào ra (input/output) là quá trình điều khiển và quản lý các hoạt động liên quan đến việc nhập và xuất dữ liệu trên thiết bị. Dưới đây là một số thông tin về quản lý vào ra trong hệ điều hành iOS:

- *Bàn phím để nhập liệu*: iOS cung cấp bàn phím ảo cho việc nhập liệu trên màn hình cảm ứng của thiết bị. Người dùng có thể sử dụng bàn phím ảo để nhập văn bản, số liệu và các lệnh khác trên các ứng dụng và trình duyệt.
- *Cảm biến và đầu vào từ các thiết bị ngoại vi*: Thiết bị iOS có tích hợp nhiều cảm biến như cảm biến gia tốc, con quay hồi chuyển, cảm biến ánh sáng, cảm biến vân tay, cảm biến khuôn mặt và cảm biến vị trí GPS. Các cảm biến này cho phép người dùng tương tác và cung cấp đầu vào cho các ứng dụng và trò chơi trên thiết bị.
- *Âm thanh và đầu ra âm thanh*: Thiết bị iOS có khả năng phát âm thanh thông qua loa tích hợp và tai nghe. Người dùng có thể nghe nhạc, xem video, thực hiện các cuộc gọi và nghe thông báo âm thanh từ các ứng dụng trên thiết bị.
- *Camera nhận hình ảnh từ bên ngoài*: Thiết bị iOS có khả năng chụp lại hình ảnh từ thực tế và lưu vào kho dữ liệu của thiết bị đó thông qua camera được gắn trên thiết bị.
- *Màn hình cảm ứng*: Màn hình cảm ứng trên thiết bị iOS cho phép người dùng tương tác trực tiếp với các ứng dụng và nội dung trên màn hình. Người dùng có thể chạm, vuốt, kéo và nhấn vào các phần tử trên màn hình để thực hiện các tác vụ và điều khiển ứng dụng.

CHƯƠNG 3. CÀI ĐẶT VÀ CÁC TÍNH NĂNG NỔI BẬT CỦA IOS

3.1 Cài đặt hệ điều hành iOS

3.1.1 Phương pháp và chuẩn bị trước cài đặt

3.1.1.1 Các phương pháp cài đặt

Hệ điều hành iOS được thiết kế để tích hợp chặt chẽ phần cứng, đảm bảo tính bảo mật và hiệu suất tối ưu. Việc cài đặt hoặc cập nhật iOS có thể được thực hiện thông qua nhiều phương pháp khác nhau, tùy thuộc vào nhu cầu của người dùng, từ cập nhật đơn giản trên thiết bị đến khôi phục hoàn toàn qua máy tính. Dưới đây là các phương pháp chính để cài đặt iOS:

- *Cập nhật iOS qua OTA (Over The Air)*: Cập nhật trực tiếp trên thiết bị mà không cần máy tính.
- *Cài dặt iOS qua iTunes/Finder*: Cài đặt bằng máy tính thông qua iTunes (Windows/macOS cũ) hoặc Finder (macOS mới).
- *Cài đặt iOS bằng DFU Mode*: Khôi phục thiết bị khi gặp sự cố nghiêm trọng.
- *Cài đặt thông qua Apple Configurator*: Hỗ trợ cấu hình, triển khai và quản lý hàng loạt thiết bị trong môi trường như trường học, doanh nghiệp hoặc tổ chức.

3.1.1.2 Chuẩn bị trước cài đặt

Trước khi tiến hành cài đặt iOS, người dùng cần chuẩn bị các yếu tố sau:

- *Thiết bị hỗ trợ*: Đảm bảo các thiết bị tương thích với phiên bản iOS mới nhất.
- *Sao lưu dữ liệu*: Sử dụng iCloud hoặc iTunes/Finder để sao lưu những dữ liệu quan trọng. Trước khi sao lưu cần kiểm tra dung lượng iCloud (nếu dùng iCloud) hoặc kết nối thiết bị với máy tính.
- *Kết nối mạng ổn định*: Đảm bảo kết nối mạng ổn định để tải bản cập nhật. Đảm bảo pin của thiết bị trên 50% hoặc được kết nối với nguồn sạc.
- *Máy tính*: Cài đặt iTunes (Windows) hoặc sử dụng Finder (macOS Catalina trở lên). Chuẩn bị cáp USB chính hãng để kết nối thiết bị với máy tính.

3.1.2 Tiến hành cài đặt

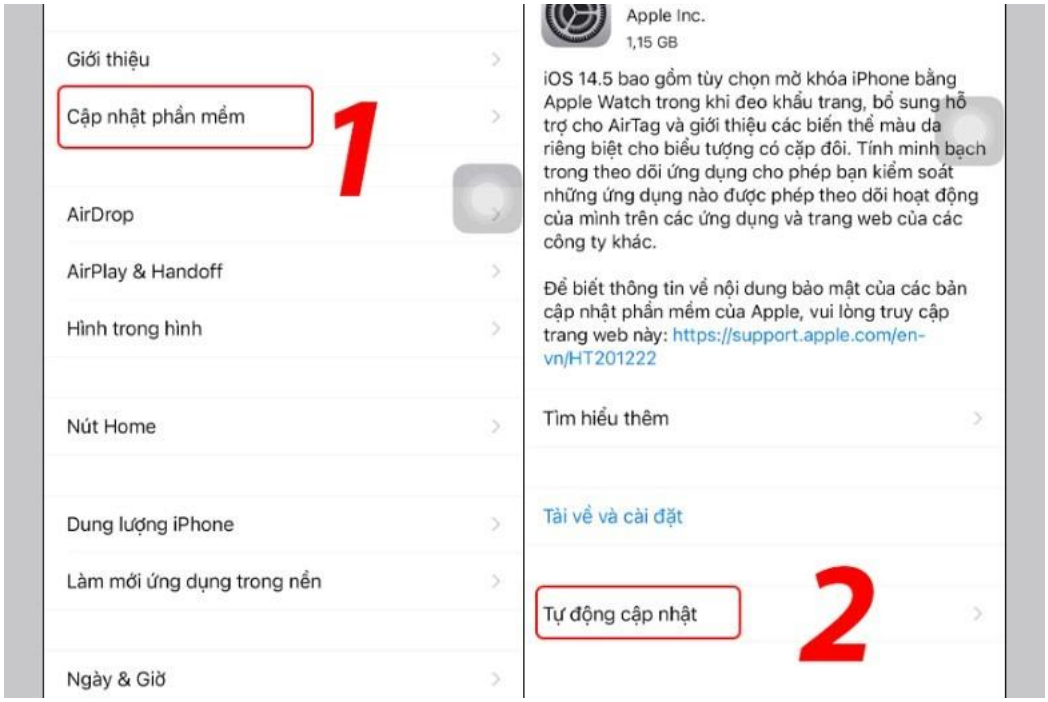
Hệ điều hành iOS có thể được cài đặt theo nhiều phương pháp khác nhau phụ thuộc vào nhu cầu của người dùng. Dưới đây là cách cài đặt hệ điều hành iOS thông qua một số phương pháp phổ biến.

3.1.2.1 Cài đặt iOS qua OTA

- Vào Cài đặt (Settings) -> Cài đặt chung (General) -> Cập nhật phần mềm (Software Update).

Hình 7 – Vào Cài đặt của thiết bị

- Nếu có bản cập nhật, chọn Tải về và cài đặt (Download and Install).



Hình 8 – Tiến hành tải về và cài đặt.

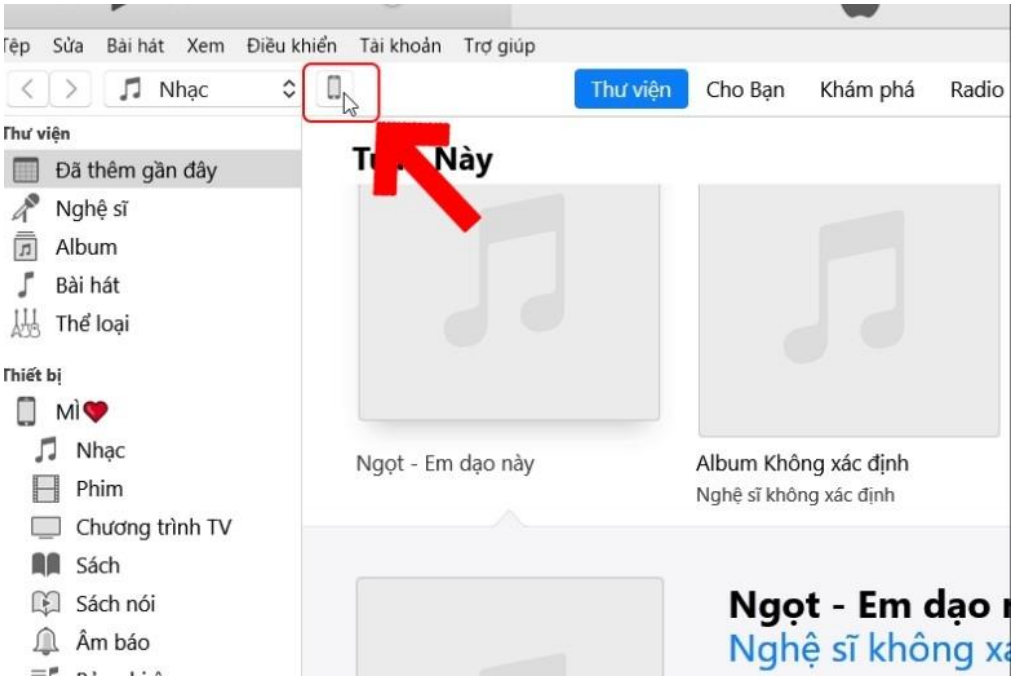
- Nhập mã Passcode (nếu có). Nhấn Đồng ý (Agree) để chấp nhận điều khoản.
- Đợi quá trình tải xuống hoàn tất và nhấn Cài đặt ngay (Install now). Thiết bị sẽ tự động khởi động lại và hoàn tất cập nhật.

3.1.2.2 Cài đặt iOS qua iTunes/Finder

- *Chuẩn bị*

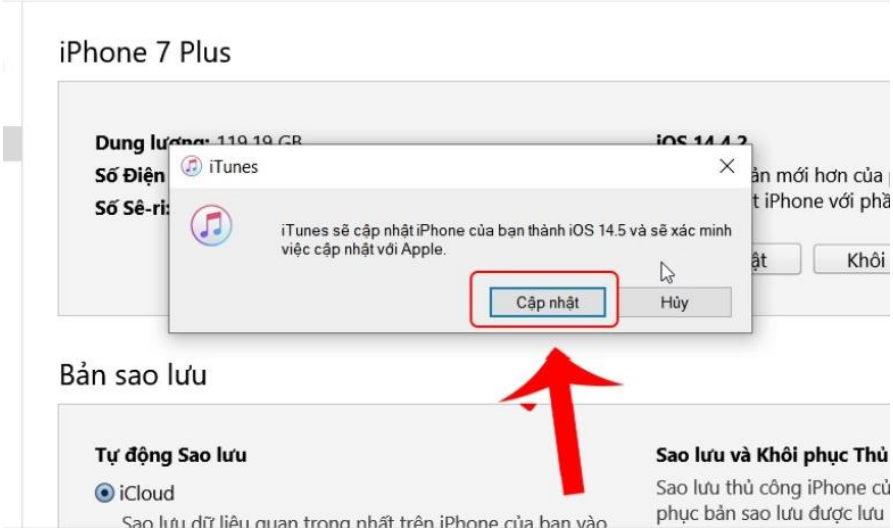
- Máy tính có cài đặt iTunes (Windows/macOS cũ) hoặc Finder (macOS Catalina trở lên).
- Cáp kết nối Lightning hoặc USB-C.
- Tải xuống file IPSW phù hợp với thiết bị (tùy chọn).

- *Các bước thực hiện*
  - Kết nối iPhone với máy tính qua cáp.
  - Mở iTunes (hoặc Finder trên macOS mới).
  - Chọn thiết bị của bạn trong iTunes/Finder.



Hình 9 – Mở iTunes và chọn thiết bị

- Nhấn kiểm tra cập nhật (Check for Update) nếu muốn cập nhật hoặc Khôi phục iPhone (Restore iPhone) để cài mới.



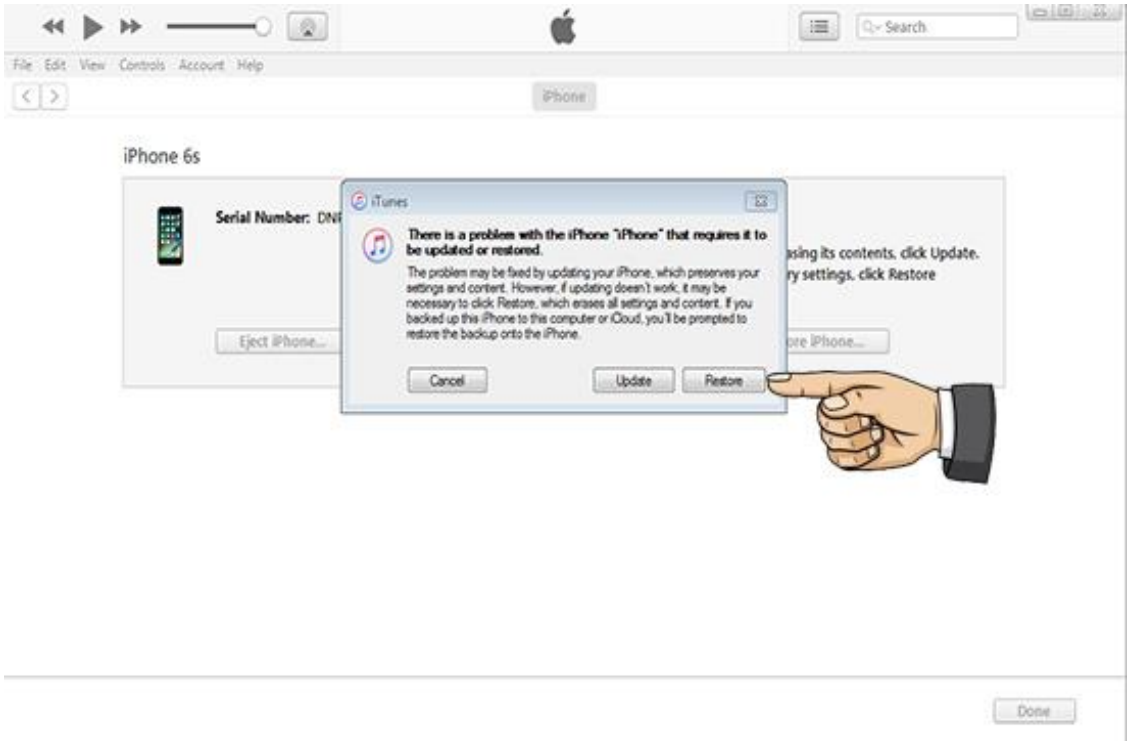
Hình 10 – Giao diện cập nhật

- Nếu khôi phục, chọn Tải về và cài đặt (Download and Install) hoặc chọn tệp IPSW đã tải về.
- Xác nhận cài đặt và chờ quá trình hoàn tất. Sau khi hoàn tất, thiết bị sẽ tự động khởi động lại.

3.1.2.3 Cài đặt iOS qua DFU Mode (Khôi phục)

DFU Mode (Device Firmware Update) Mode dùng để khôi phục thiết bị khi gặp sự cố nghiêm trọng. Dưới đây là các bước tiến hành khôi phục hệ thống sử dụng DFU:

- Kết nối thiết bị với máy tính sử dụng cáp USB và mở iTunes/Finder.
- Vào DFU Mode:
  - Tắt nguồn thiết bị.
  - Nhấn và giữ Nút Nguồn + Nút Home (iPhone 6s trở xuống) hoặc Nút Nguồn + Nút Giảm Âm Lượng (iPhone 7 trở lên).
  - Sau 10 giây, thả nút nguồn nhưng tiếp tục giữ nút Home/Nút Giảm Âm Lượng.
  - Khi iTunes/Finder nhận diện thiết bị trong chế độ khôi phục, thả nút.
- Khôi phục và cài đặt iOS:
  - Trong giao diện iTunes/Finder, nhấn Restore.



Hình 11 – Giao diện khôi phục

- iTunes/Finder sẽ tải bản iOS phù hợp và cài đặt lên thiết bị.
- Thiết bị sẽ khởi động lại và hiển thị màn hình thiết lập ban đầu.

3.1.3 Các lưu ý quan trọng

- *Kiểm tra tính tương thích của thiết bị*: Trước khi cập nhật, hãy đảm bảo rằng iPhone tương thích với phiên bản iOS mới. Kiểm tra danh sách các thiết bị được hỗ trợ trên trang web chính thức của Apple.
- *Xóa các ứng dụng không sử dụng*: Trước khi cập nhật, hãy xem xét xóa bỏ những ứng dụng không cần thiết hoặc không sử dụng để giải phóng dung lượng lưu trữ trên iPhone.
- *Giải phóng dung lượng*: Đảm bảo rằng có đủ dung lượng trống trên iPhone để tiến hành cài đặt bản cập nhật. Xóa bớt các tập tin không cần thiết, hình ảnh, video hoặc sao lưu chúng trên máy tính hoặc dịch vụ lưu trữ đám mây trước khi cập nhật.
- *Cài đặt bản cập nhật ứng dụng mới nhất*: Trước khi cập nhật iOS, đảm bảo rằng đã cài đặt các bản cập nhật mới nhất cho các ứng dụng trên iPhone. Điều này giúp đảm bảo sự tương thích và ổn định với phiên bản iOS mới.
- *Cập nhật iTunes lên phiên bản mới nhất*: Nếu bạn sử dụng iTunes để quản lý iPhone của mình, hãy đảm bảo rằng đã cập nhật iTunes lên phiên bản mới nhất. Điều này giúp đảm bảo tương thích và hỗ trợ tốt nhất cho cập nhật iOS.
- *Sao lưu iPhone*: Trước khi tiến hành cập nhật, cần sao lưu dữ liệu quan trọng trên iPhone. Có thể sử dụng iCloud hoặc iTunes để sao lưu dữ liệu để đảm bảo rằng không bị mất dữ liệu quan trọng trong quá trình cập nhật.

3.2 Các tính năng nổi bật

Hệ điều hành iOS không chỉ nổi bật nhờ hiệu suất tối ưu và bảo mật vượt trội, mà còn bởi những tính năng độc đáo giúp nâng cao trải nghiệm người dùng và tạo nên sự khác biệt trong thị trường di động. Được thiết kế tích hợp chặt chẽ với phần cứng Apple, iOS mang đến giao diện thân thiện, hệ sinh thái liền mạch cùng các công cụ hiện đại như Apple Pay và Siri. Phần này sẽ điểm qua những tính năng nổi bật nhất của iOS, thể hiện sức mạng và sự sáng tạo của Apple trong việc định hình công nghệ di động.

3.2.1 Tính năng bảo mật vượt trội

Bảo mật luôn là một trong những trụ cột quan trọng nhất của iOS, giúp hệ điều hành này nổi bật trong việc bảo vệ dữ liệu và quyền riêng tư của người dùng. Sau đây là một số tính năng bảo mật vượt trội, khẳng định cam kết của Apple trong việc đặt an toàn lên hàng đầu:

- *Apple Store*: Tất cả ứng dụng trước khi được phát hành đều phải trải qua quá trình kiểm tra kỹ lưỡng về mã độc, vi phạm bản quyền và tuân thủ các quy định của Apple. Điều này giúp giảm thiểu nguy cơ người dùng tải về các ứng dụng độc hại hoặc không an toàn. Tuy nghiêm ngặt nhưng nó cũng cung cấp rất nhiều ứng dụng đa dạng phù hợp với người dùng.
- *Mã hóa dữ liệu*: iOS tự động mã hóa dữ liệu trên thiết bị, bao gồm tin nhắn, email, ảnh, video, danh bạ và các thông tin cá nhân khác bằng AES 256-bit. Ngay cả khi

thiết bị bị mất hoặc đánh cắp, dữ liệu của người dùng vẫn được bảo vệ an toàn nhờ Secure Enclave và Data Protection API.

- *Face ID và Touch ID*: Đây là hai tính năng xác thực sinh trắc học tiên tiến, cho phép người dùng mở khóa thiết bị, xác thực các giao dịch mua hàng trực tuyến và truy cập các ứng dụng bảo mật chỉ bằng khuôn mặt (Face ID) hoặc dấu vân tay (Touch ID).
- *Cập nhật bảo mật thường xuyên*: Apple thường xuyên phát hành các bản cập nhật iOS để vá các lỗ hổng bảo mật và tăng cường khả năng bảo vệ thiết bị của người dùng.

3.2.2 Hiệu suất mượt mà ổn định

- *Tối ưu hóa phần cứng và phần mềm*: iOS được thiết kế để hoạt động tối ưu trên các thiết bị Apple. Sự tương thích hoàn hảo giữa phần cứng và phần mềm giúp các ứng dụng chạy nhanh chóng, mượt mà và ít gặp sự cố.
- *Cập nhật hệ điều hành thường xuyên*: Apple liên tục cải tiến hệ điều hành iOS thông qua các bản cập nhật. Các bản cập nhật này không chỉ mang đến các tính năng mới mà còn tối ưu hóa hiệu suất, giúp thiết bị hoạt động ổn định hơn.

3.2.3 Hệ sinh thái và đồng bộ hóa

Một trong những điểm mạnh nổi bật của iOS nằm ở hệ sinh thái được xây dựng chặt chẽ và khả năng đồng bộ hóa mượt mà giữa các thiết bị Apple. IOS tạo ra một môi trường kết nối hoàn hảo, giúp người dùng truy cập dữ liệu và tiếp tục công việc mọi lúc, mọi nơi. Phần này sẽ làm rõ hệ sinh thái của Apple nâng cao hiệu quả và trải nghiệm của người dùng thông qua sự đồng bộ hóa thông minh.

- *iCloud*: dịch vụ lưu trữ đám mây của Apple, đóng vai trò trung tâm trong việc đồng bộ và liên kết dữ liệu giữa các thiết bị iOS, iPadOS và macOS. Nó cho phép người dùng lưu trữ dữ liệu trực tuyến và truy cập từ bất kỳ thiết bị nào. iCloud cũng giúp người dùng dễ dàng sao lưu và khôi phục dữ liệu khi cần thiết.
- *AirDrop*: Tính năng này cho phép người dùng chia sẻ dữ liệu nhanh chóng giữa các thiết bị Apple ở gần, chẳng hạn như chia sẻ ảnh, video, tài liệu...
- *Handoff*: Tính năng Handoff cho phép người dùng tiếp tục công việc trên một thiết bị khác một cách dễ dàng. Ví dụ, bạn có thể bắt đầu soạn email trên iPhone và tiếp tục hoàn thành nó trên iPad.

3.2.4 Một số tính năng nổi bật khác

Bên cạnh bảo mật và hệ sinh thái vượt trội, iOS còn mang đến loạt tính năng độc đáo, từ trí tuệ nhân tạo đến các công cụ hỗ trợ cuộc sống hàng ngày. Dưới đây là môt số tính năng ấn tượng khác, khẳng định vị thế dẫn đầu của iOS trong công nghệ di động.

- *Apple Intelligence*: hệ thống trí tuệ nhân tạo (AI) do Apple phát triển, được tích hợp sâu vào các thiết bị như iPhone, iPad và Mac. Ra mắt vào tháng 10 năm 2024, Apple Intelligence mang đến nhiều tính năng tiên tiến, giúp nâng cao trải nghiệm người dùng và tối ưu hóa hiệu suất công việc.

- *Siri*: Một trợ lý ảo thông minh được tích hợp sẵn trên các thiết bị của Apple, cho phép người dùng tương tác với thiết bị bằng giọng nói. Siri có thể thực hiện nhiều tác vụ khác nhau, từ tìm kiếm thông tin, điều khiển thiết bị, đến thực hiện các tác vụ phức tạp hơn như đặt lịch hẹn, gửi tin nhắn, hay dịch ngôn ngữ.
- *Find My*: Tính năng của iOS giúp người dùng tìm kiếm thiết bị Apple bị mất, chia sẻ vị trí với bạn bè, định vị AirTag, và bảo vệ dữ liệu trong trường hợp thiết bị bị đánh cắp. Định vị thiết bị cho dù bị tắt nguồn nhiều giờ, chia sẻ vị trí theo thời gian thực với người thân hoặc bạn bè.
- *VoiceOver*: Tính năng trợ năng trên iOS giúp người khiếm thị và người gặp khó khăn trong việc đọc màn hình có thể điều khiển thiết bị thông qua giọng nói và cử chỉ chạm.
- *Apple Pay*: dịch vụ thanh toán di động của Apple, cho phép người dùng thanh toán không tiếp xúc bằng iPhone, Apple Watch, iPad và Mac. Người dùng có thể sử dụng Face ID, Touch ID hoặc mật mã để xác thực giao dịch một cách an toàn.

CHƯƠNG 4. CÁC VẤN ĐỀ AN NINH, AN TOÀN VÀ THỰC NGHIỆM CHẾ ĐỘ PHONG TỎA TRÊN IOS

4.1 Các vấn đề an ninh, an toàn và các lỗ hổng tiêu biểu

4.1.1 WebKit (Động cơ trình duyệt Safari)

WebKit là động cơ trình duyệt mã nguồn mở được sử dụng trong Safari và tất cả các trình duyệt khác trên iOS (do chính sách của Apple yêu cầu mọi ứng dụng trình duyệt phải sử dụng WebKit). Đây là một trong những thành phần dễ bị tấn công nhất trên iOS vì:

- ***Điểm yếu**:*
  - *Bề mặt tấn công lớn*: WebKit xử lý nội dung web phức tạp (HTML, JavaScript, CSS), vốn là mục tiêu phổ biến của các cuộc tấn công dựa trên trình duyệt như XSS (Cross-Site Scripting) hoặc khai thác bộ nhớ.
  - *Tính phức tạp của mã*: WebKit có hàng triệu dòng mã, điều này làm tăng khả năng xuất hiện lỗi lập trình (memory corruption, use-after-free, buffer overflow), những lỗi thường bị khai thác trong các zero-day.
  - *Tần suất cập nhật:* Mặc dù Apple vá lỗi nhanh chóng, các nhà nghiên cứu bảo mật thường xuyên tìm thấy lỗ hổng mới trong WebKit vì nó là mục tiêu chính của các cuộc tấn công từ xa (remote code execution).
  - *Sự phụ thuộc duy nhất:* Việc buộc tất cả trình duyệt trên iOS dùng WebKit khiến toàn bộ hệ sinh thái phụ thuộc vào tính bảo mật của một động cơ duy nhất. Nếu WebKit bị khai thác, không có lựa chọn thay thế nào khác.
- ***Ví dụ thực tế**:*
  - Các vụ khai thác zero-day như trong chuỗi tấn công FORCEDENTRY của NSO Group (2021) đã lợi dụng lỗ hổng trong WebKit để triển khai spyware Pegasus mà không cần người dùng tương tác.
  - CVE-2024-44308 và CVE-2024-44309 (Tháng 11/2024): Lỗ hổng trong JavaScriptCore và WebKit, cho phép thực thi mã tùy ý hoặc tấn công XSS khi người dùng truy cập trang web độc hại. Ảnh hưởng chủ yếu đến hệ thống Mac dựa trên Intel, nhưng cũng áp dụng cho iOS 18.1.1 và các phiên bản khác.
- ***Hệ quả**:* WebKit là cửa ngõ phổ biến cho các cuộc tấn công từ xa, đặc biệt khi kết hợp với các kỹ thuật sandbox escape để vượt qua lớp bảo vệ của iOS.

4.1.2 Nhân XNU

Nhân XNU là một nhân lai (hybrid kernel) kết hợp giữa microkernel Mach, driver BSD, và một số thành phần độc quyền của Apple. Đây là nền tảng cốt lõi của iOS, và các lỗ hổng trong XNU có thể dẫn đến việc leo thang đặc quyền hoặc kiểm soát hoàn toàn thiết bị.

- ***Điểm yếu**:*

- *Thiết kế lai phức tạp*: Sự kết hợp giữa microkernel và monolithic kernel làm tăng độ phức tạp, dẫn đến khả năng xảy ra lỗi trong quản lý bộ nhớ hoặc xử lý quyền truy cập (privilege escalation).
- *Mã cũ từ BSD*: Một số thành phần của XNU kế thừa từ BSD đã cũ và không được tối ưu hóa cho các mối đe dọa hiện đại, tạo cơ hội cho các kỹ thuật khai thác như kernel buffer overflow.
- *Tấn công từ sandbox escape*: Các lỗ hổng zero-day thường được sử dụng để thoát khỏi sandbox của iOS và sau đó nhắm vào nhân XNU để giành quyền kiểm soát cấp kernel.
- *Thiếu minh bạch*: Vì XNU không hoàn toàn mã nguồn mở (chỉ một phần được công khai), việc cộng đồng phát hiện và vá lỗi bị hạn chế so với các nhân như Linux

- ***Ví dụ thực tế***:
  - Lỗ hổng trong XNU đã được khai thác trong jailbreak như unc0ver hay checkra1n, cho thấy nhân này không miễn nhiễm với các cuộc tấn công tinh vi. Một số zero-day đã nhắm vào các lỗi trong IPC (Inter-Process Communication) của Mach để leo thang đặc quyền.
  - CVE-2023-32434 (Operation Triangulation - 2023): Lỗ hổng trong nhân XNU, bị khai thác trong chiến dịch gián điệp nhắm vào Nga. Gần đây (tháng 3/2025), một khai thác mới mang tên "Trigon" đã được công bố liên quan đến lỗ hổng này, cho phép đọc/ghi bộ nhớ kernel tùy ý, ảnh hưởng đến nhiều phiên bản iOS.
- ***Hệ quả:*** Nếu nhân XNU bị xâm phạm, toàn bộ hệ thống bảo mật của iOS (bao gồm Secure Enclave) có thể bị đe dọa, dù Apple đã bổ sung nhiều lớp bảo vệ như KPP (Kernel Patch Protection) hay KTRR (Kernel Text Read-Only Region).

4.1.3 Core Media và các Framework quan trọng khác

Core Media là framework xử lý đa phương tiện (âm thanh, video, hình ảnh) trên iOS. Các framework khác như Core Graphics, Core Animation, hay Metal cũng đóng vai trò quan trọng trong trải nghiệm người dùng và là mục tiêu tiềm năng của các lỗ hổng zero-day.

- ***Điểm yếu:***
  - *Xử lý dữ liệu không tin cậy:* Core Media thường xuyên xử lý nội dung từ nguồn bên ngoài (ví dụ: video, hình ảnh được tải xuống), dễ bị tấn công qua các tệp độc hại (malformed media files) gây ra lỗi tràn bộ nhớ hoặc thực thi mã tùy ý.
  - *Tính phức tạp của định dạng:* Các định dạng đa phương tiện hiện đại (H.264, HEVC, MP4) rất phức tạp, và lỗi trong quá trình phân tích cú pháp (parsing) thường bị khai thác. Ví dụ, một tệp MP4 được chế tạo đặc biệt có thể kích hoạt lỗ hổng zero-day.

- *Tích hợp sâu với phần cứng:* Các framework này giao tiếp trực tiếp với phần cứng (GPU, T2 chip), và lỗi trong driver hoặc giao tiếp phần cứng-cơ chế phần mềm có thể bị khai thác để vượt qua sandbox hoặc gây ra lỗi kernel.
- *Tần suất vá chậm hơn:* So với WebKit, các lỗ hổng trong Core Media đôi khi không được vá nhanh chóng vì chúng ít được chú ý hơn, tạo cửa sổ khai thác dài hơn cho tin tặc.

- ***Ví dụ thực tế:***
  - Lỗ hổng trong Core Media đã từng được phát hiện liên quan đến xử lý hình ảnh TIFF hoặc video HEVC, cho phép thực thi mã từ xa khi người dùng mở tệp độc hại.
  - CVE-2025-24085 (Core Media - Tháng 1/2025): Đây là lỗ hổng use-after-free trong Core Media, framework xử lý âm thanh và video trên iOS. Tin tặc có thể khai thác để nâng quyền truy cập hệ thống. Có thể cho phép thực thi mã tùy ý hoặc chiếm quyền điều khiển thiết bị. Ảnh hưởng đến iPhone (từ XS trở lên), iPad, Mac (macOS Sequoia), và các thiết bị khác. Apple xác nhận lỗ hổng này đã bị khai thác trong thực tế.
- ***Hệ quả:*** Các framework này thường là bước thứ hai trong chuỗi khai thác zero-day, sau khi kẻ tấn công đã vượt qua WebKit hoặc một điểm vào khác, để leo thang đặc quyền hoặc duy trì quyền truy cập.

4.1.4 Kết luận và giải pháp tiềm năng

- *WebKit:* Apple cần tiếp tục đầu tư vào fuzzing (kiểm tra lỗi tự động) và giảm sự phụ thuộc duy nhất vào WebKit bằng cách cho phép các động cơ trình duyệt khác (dù điều này khó xảy ra vì triết lý của Apple).
- *Nhân XNU:* Hiện đại hóa mã nguồn cũ từ BSD, tăng cường minh bạch, và bổ sung thêm các cơ chế bảo vệ như PAC (Pointer Authentication Code) để giảm thiểu khai thác bộ nhớ.
- *Core Media:* Cải thiện kiểm tra đầu vào (input validation) và sandboxing cho các framework đa phương tiện, đồng thời vá lỗi nhanh hơn khi phát hiện.

4.2 Thực nghiệm chế độ phong tỏa (Lockdown Mode)

4.2.1 Giới thiệu về Lockdown Mode

Chế độ Lockdown là một tùy chọn bảo vệ cực đoan, được thiết kế dành cho một số ít cá nhân, những người mà bản thân hay công việc của họ có thể trở thành mục tiêu cá nhân của những mối đe dọa kỹ thuật số tinh vi nhất.

Khi bật chế độ phong tỏa, thiết bị của người dùng sẽ không hoạt động như bình thường. Để giảm thiểu bề mặt tấn công có thể bị khai thác bởi các phần mềm gián điệp chuyên nghiệp có mục tiêu cao, một số ứng dụng, trang web và tính năng sẽ bị hạn chế nghiêm ngặt về mặt bảo mật và một số trải nghiệm có thể không khả dụng.

Lockdown Mode được phát triển từ phiên bản iOS 16 về sau. Vì vậy, để được bảo vệ hoàn toàn, người dùng cần cập nhật thiết bị của mình lên phiên bản mới nhất trước khi bật chế độ này.

Chế độ phong tỏa bảo vệ thiết bị người dùng được biểu hiện dựa trên những khía cạnh sau:

- ***Tin nhắn***: Hầu hết các loại tệp đính kèm tin nhắn đều bị chặn, ngoại trừ một số hình ảnh, video và âm thanh. Một số tính năng như liên kết và xem trước liên kết đều không khả dụng.
- ***Duyệt web***: Một số công nghệ web phức tạp bị chặn, có thể khiến một số trang web tải chậm hơn hoặc không hoạt động đúng cách. Ngoài ra, phông chữ trên web có thể không được hiển thị và hình ảnh có thể bị thay thế bằng biểu tượng hình ảnh bị thiếu.
- ***FaceTime***: Các cuộc gọi FaceTime đến sẽ bị chặn trừ khi người dùng đã gọi cho người đó hoặc liên hệ đó trước đó. Các tính năng như SharePlay và Live Photos không khả dụng.
- ***Dịch vụ Apple***: Lời mời cho các dịch vụ Apple, chẳng hạn như lời mời quản lý nhà trong ứng dụng Home, sẽ bị chặn trừ khi bạn đã mời người đó trước đó. Game Center cũng bị vô hiệu hóa.
- ***Ảnh***: Khi người dùng chia sẻ ảnh, thông tin vị trí sẽ bị loại trừ. Album được chia sẻ sẽ bị xóa khỏi ứng dụng Ảnh và lời mời Album được chia sẻ mới sẽ bị chặn. Người dùng vẫn có thể xem các album được chia sẻ này trên các thiết bị khác không bật chế độ phong tỏa.
- ***Kết nối với thiết bị khác***: Để kết nối iPhone hoặc iPad của người dùng với các phụ kiện hoặc máy tính khác, thiết bị cần được mở khóa. Để kết nối với Mac, máy Mac của người dùng phải được mở khóa và cần sự chấp thuận của người dùng.
- ***Kết nối không dây***: Thiết bị của người dùng sẽ không tự động kết nối với mạng Wi-Fi không an toàn và sẽ ngắt kết nối khỏi mạng Wi-Fi không an toàn khi người dùng bật chế độ phong tỏa. Hỗ trợ mạng di động 2G sẽ bị tắt.

Như vậy, chế độ phong tỏa cung cấp một lớp bảo vệ bổ sung chống lại các mối đe dọa mạng phức tạp bằng cách vô hiệu hóa hoặc hạn chế các tính năng có thể bị khai thác, giúp bảo vệ dữ liệu cá nhân và thông tin nhạy cảm bằng cách hạn chế các vectơ tấn công tiềm ẩn. Tuy nhiên, khi bật chế độ này, một số tính năng và ứng dụng có thể không hoạt động như mong đợi hoặc bị vô hiệu hóa hoàn toàn. Chế độ này được thiết kế dành cho người dùng có nguy cơ cao như nhà báo, nhà hoạt động hoặc quan chức chính phủ.

4.2.2 Thực hiện demo trên thiết bị iOS

4.2.2.1 Kịch bản

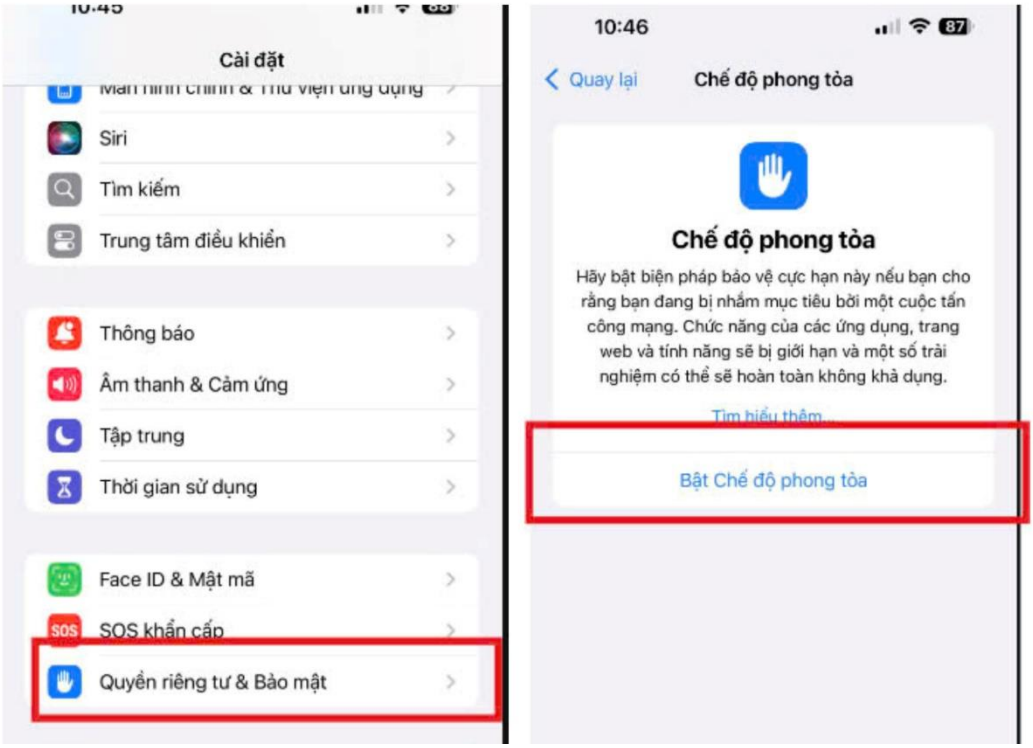
- ***Mục tiêu:***
    - Hướng dẫn cách bật và tắt Lockdown Mode trên iOS.

- Trình bày các tính năng bị giới hạn khi chế độ này được bật.
- So sánh trạng thái hoạt động khi bật và tắt Lockdown Mode.

- ***Chuẩn bị***:
  - Đảm bảo iPhone chạy iOS 16 hoặc phiên bản mới hơn.
  - Sao lưu dữ liệu quan trọng trước khi tiến hành demo.
  - Chuẩn bị sẵn các thiết bị phụ trợ (Một thiết bị khác để gửi lời mời FaceTime,…).

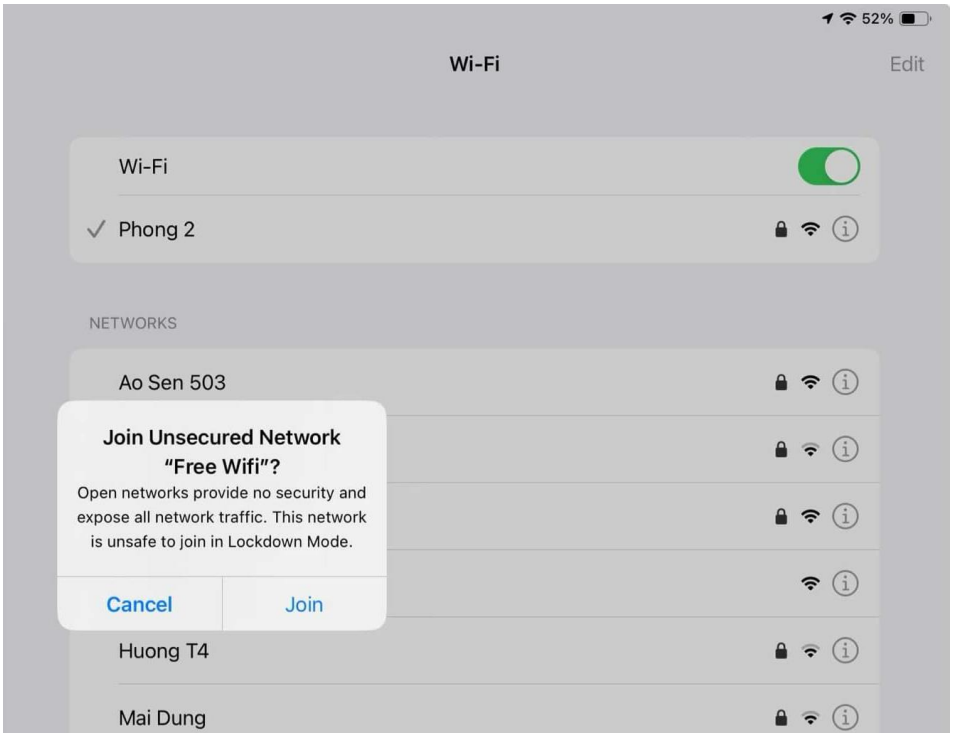
4.2.2.2 Thực hành

- Bật chế độ phong tỏa:
  - Mở cài đặt trên iPhone.
  - Cuộn xuống chọn **Bảo mật và Quyền riêng tư**.
  - Chọn **Chế độ phong tỏa** và nhấn **Bật chế độ phong tỏa**.



Hình 12 – Chế độ phong tỏa có thể được bật trong cài đặt

- Thử nghiệm một số tính năng bị giới hạn khi bật chế độ phong tỏa:
  - ***Giới hạn kết nối Wifi***: Thiết bị sẽ không tự động kết nối với Wifi không an toàn khi người dùng không cho phép. Trên thiết bị đang bật chế độ phong tỏa thử kết nối với một mạng không mật khẩu, kết quả hiển thị như hình bên dưới.

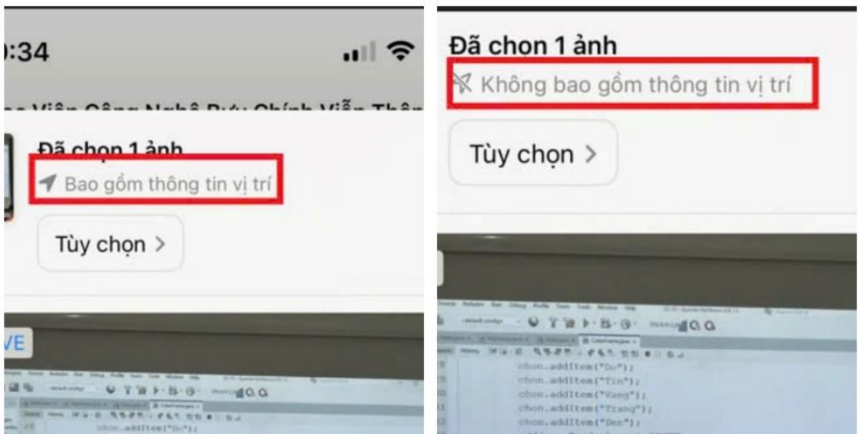


Hình 13 – Giới hạn kết nối wifi

- ***FaceTime***: Sử dụng một thiết bị iOS khác gửi lời mời FaceTime đến thiết bị đang bật chế độ này, đảm bảo thông tin người dùng chưa được lưu trong danh bạ. Quan sát trên thiết bị demo, thấy lời mời FaceTime không xuất hiện hoặc bị chặn.

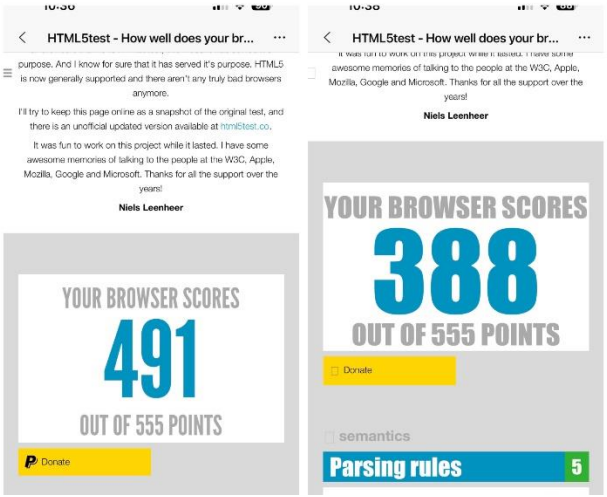
Hình 14 – Người dùng chưa được lưu trong danh bạ sẽ bị chặn

- ***Hạn chế trong tính năng chia sẻ ảnh***: Ảnh được chia sẻ sẽ mặc định không chia sẻ vị trí trừ khi người dùng chỉnh sửa.



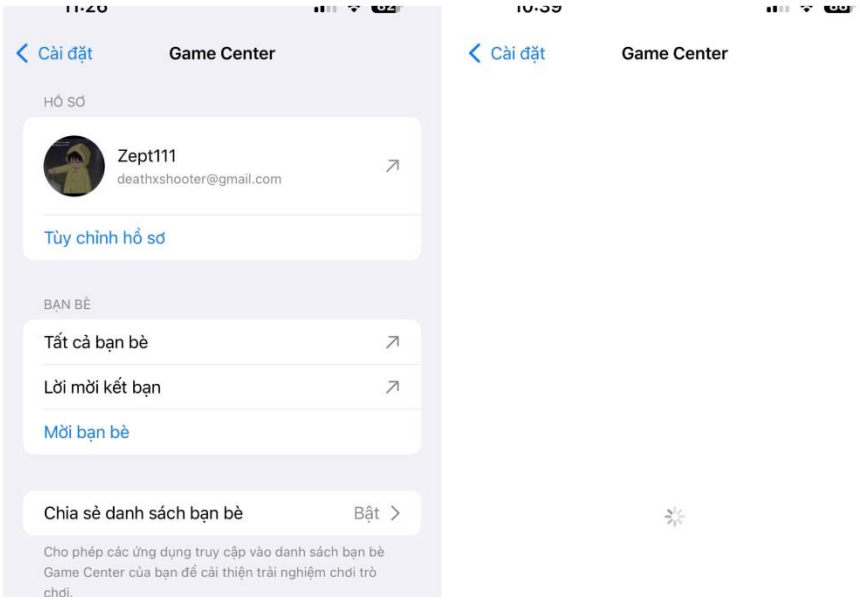
Hình 15 – Tùy chọn chia sẻ ảnh trước và sau khi bật chế độ

- ***Hạn chế trong duyệt Web***: Một số công nghệ Web phức tạp có thể bị chặn. Khiến trang Web tải chậm hơn hoặc không hiển thị đúng như yêu cầu. Sử dụng trang Web HTML5Test để kiểm tra mức độ hỗ trợ của trình duyệt với các tiêu chuẩn HTML5 để xem sự khác biệt.



Hình 16 – Điểm hỗ trợ HTML5 trước và sau khi bật Lockdown Mode

- ***Hạn chế trong dịch vụ Apple***: Một số dịch vụ như GameCenter,… có thể không khả dụng trong chế độ này.



Hình 17 – Giao diện GameCenter trước và sau khi bật chế độ phong tỏa

4.2.2.3 Kết luận

Mục tiêu của phần demo giúp người dùng hiểu rõ hơn về sự đánh đổi giữa mức độ bảo mật và tính tiện ích khi sử dụng chế độ phong tỏa. Đây là công cụ rất hữu ích để bảo vệ thông tin cá nhân khỏi những mối đe dọa tinh vi. Tùy thuộc vào nhu cầu bảo vệ thông tin cá nhân mà người dùng có thể sử dụng chế độ này.

KẾT LUẬN

Các kết quả đạt được

Nhóm thực hiện đề tài "Tìm hiểu hệ điều hành cho các thiết bị di động Apple iOS" đã hoàn thành việc nghiên cứu, phân tích và đánh giá toàn diện về iOS theo các nội dung đã đăng ký trong đề cương. Các kết quả đạt được bao gồm:

- Nghiên cứu tổng quan về iOS, bao gồm lịch sử phát triển, đặc điểm nổi bật và vai trò trong hệ sinh thái Apple, đặt nền tảng cho việc hiểu sâu về hệ điều hành này.
- Phân tích kiến trúc iOS, từ XNU kernel đến các lớp bảo mật như Secure Enclave, cùng các thành phần cốt lõi như sandboxing và mã hóa phần cứng.
- Làm rõ các phương pháp cài đặt iOS, bao gồm OTA, iTunes/Finder, DFU Mode và Apple Configurator, với các bước thực hiện cụ thể.
- Đánh giá các tính năng nổi bật của iOS, từ bảo mật (Face ID, mã hóa AES-256), hiệu suất tối ưu, đến hệ sinh thái (iCloud, Handoff) và các công cụ như Apple Intelligence, Siri.
- Phân tích các vấn đề an ninh và an toàn của iOS, bao gồm điểm yếu trong WebKit, nhân XNU và các Framework.

Báo cáo được thực hiện dựa trên tài liệu chính thức từ Apple (iOS Security Guide) và các nguồn uy tín khác, đảm bảo tính chính xác và phù hợp với môn "An toàn hệ điều hành" tại Học viện Công nghệ bưu chính viễn thông.

Hướng phát triển

Đề tài này có tiềm năng mở rộng theo các hướng sau:

- Nghiên cứu sâu hơn về các lỗ hổng zero-day mới nhất trên iOS (nếu có sau 2025) và cách Apple vá chúng, nhằm cập nhật các mối đe dọa an ninh hiện đại.
- Phân tích chi tiết các kỹ thuật tấn công phần cứng nâng cao (như side-channel attacks) và đề xuất biện pháp phòng chống trong bối cảnh bảo mật hệ điều hành.
- Khám phá việc tích hợp trí tuệ nhân tạo (Apple Intelligence) vào bảo mật iOS, đánh giá tác động đến hiệu suất và an toàn dữ liệu.
- Phát triển các phương pháp kiểm tra bảo mật iOS cục bộ, chẳng hạn như mô phỏng tấn công sandbox hoặc khai thác kernel, để thử nghiệm tính bền vững của hệ thống.

Những hướng phát triển này không chỉ mở rộng phạm vi nghiên cứu mà còn góp phần nâng cao hiểu biết về an toàn hệ điều hành trong môi trường thực tế.

TÀI LIỆU THAM KHẢO

[1] Cách sử dụng File trên iPhone và iPad, https://viendidong.com/tep-tren-iphone/#2-Cach-su-dung-tep-tren-iPhoneiPad, truy cập tháng 02.2025.

[2] iPhone Operating Systems Analysis Research Paper, https://ivypanda.com/essays/iphone-operating-systems-analysis/, truy cập tháng 02.2025.

[3] Dịch vụ Apple Services là gì? Khám phá tất cả những gì bạn cần biết, https://memart.vn/tin-tuc/blog/cac-dich-vu-thuoc-dich-vu-apple-services-la-gi-va-nhung-tinh-nang-noi-bat-vi-cb.html, truy cập tháng 02.2025.

[4] iOS Feature Availability, https://www.apple.com/ios/feature-availability/ , truy cập tháng 02.2025.

[5] Hướng dẫn cập nhật iOS, https://didongviet.vn/dchannel/cach-cap-nhat-ios/, truy cập tháng 02.2025.

[6] Restore iPhone thông qua chế độ DFU, https://www.thegioididong.com/hoi-dap/restore-iphone-thong-qua-che-do-dfu-973726, truy cập tháng 02.2025.

[7] Weaknesses in Webkit Becoming Problematic, Weaknesses in Webkit Becoming Problematic | Threatpost, truy cập tháng 02.2025.

[8] Hướng dẫn sử dụng iPhone,

https://support.apple.com/vi-vn/guide/iphone/iph73b8c43/ios, truy cập tháng 02.2025.

[9] Search Vulnerability Database, https://nvd.nist.gov/vuln/search, truy cập tháng 02.2025.

[10] Introduction to Kernel Exploits on iOS, https://hoploninfosec.com/trigon-a-deep-dive-into-the-latest-ios-exploit/, truy cập tháng 02.2025.

[11] iOS Security Guide, https://www.apple.com/vn/privacy/docs/iOS_Security_Guide.pdf, truy cập tháng 02.2025.