JTE
HCMUTE
ISSN: 1859-1272

TẠP CHÍ KHOA HỌC GIÁO DỤC KỸ THUẬT
Trường Đại học Sư phạm Kỹ thuật Thành phố Hồ Chí Minh
Website: https://jte.edu.vn
Email: jte@hcmute.edu.vn

Internet of Things Security: Firmware Approach

Cong Doan Dinh
Ho Chi Minh City University of Technology and Education, Vietnam.

Corresponding author. *Email: doandc@hcmute.edu.vn*

ARTICLE INFO

Received: 14/03/2024
Revised: 22/04/2024
Accepted: 23/04/2024
Published: 28/04/2024

KEYWORDS

Internet of Things (IoT);
Embedded Systems;
Firmware;
Hardware;
Security.

ABSTRACT

Internet of Things (IoT) is increasingly widely used, creating many opportunities to bring people smart applications (smart city, smart home, smart health, etc.), making our life more convenient, higher production efficiency (smart industry, smart agriculture). Besides the advantages, many security challenges also arise such as privacy issues, authentication, management issues, information storage, etc. The different factors make the issue of security in the IoT environments more challenging than that of the regular information technology (IT) devices. The IoT environment gives rise to problems and vulnerabilities, the IoT applications create various cyber threats. There have been various security and privacy attacks on devices that have been deployed: the Mirai attack in 2016 was estimated to have infected about 2.5 million Internet-connected devices and launched the Distributed denial of service (DDOS) attack. The IoT devices are also implanted into the human body to monitor the vital status of various organs. These devices are targets for attacks to falsify data. Such attacks, if any, will very dangerous. This article focuses on presenting the challenges of securing the IoT systems, then diving into a security aspect of the IoT systems coming from inside the hardware device - the firmware of the device.

Bảo Mật Vạn Vật Kết Nối Internet: Tiếp Cận Từ Firmware

Đinh Công Đoan
Trường Đại Học Sư Phạm Kỹ Thuật Thành Phố Hồ Chí Minh, Việt Nam

Tác giả liên hệ. *Email: doandcc@.hcmute.edu.vn*

THÔNG TIN BÀI BÁO

Ngày nhận bài: 14/03/2024
Ngày hoàn thiện: 22/04/2024
Ngày chấp nhận đăng: 23/04/2024
Ngày đăng: 28/04/2024

TỪ KHÓA

Vạn vật kết nối Internet (IoT);
Hệ thống nhúng;
Phần sụn;
Phần cứng;
Bảo mật.

TÓM TẮT

IoT được dùng ngày càng nhiều, tạo ra nhiều ứng dụng thông minh (thành phố thông minh, ngôi nhà thông minh, y khoa thông minh...), giúp cuộc sống con người tiện nghi hơn. Hiệu quả của việc sản xuất cũng tăng cao (Công nghiệp, nông nghiệp thông minh). Bên cạnh những ưu điểm, cũng nảy sinh nhiều thách thức về: tính riêng tư, tính xác thực, quản lý, lưu trữ thông tin...Các yếu tố khác làm phát sinh nhiều thách thức trong bảo mật môi trường IoT hơn so với các thiết bị công nghệ thông tin (IT) bình thường. Môi trường IoT tồn tại nhiều lỗ hổng, các ứng dụng IoT tạo ra các nguy cơ bảo mật khác nhau. Đã có nhiều cuộc tấn công vào thiết bị được triển khai: Cuộc tấn công Mirai năm 2016 làm lây nhiễm khoảng 2.5 triệu thiết bị kết nối Internet và khởi động cuộc tấn công từ chối dịch vụ phân tán (DDoS). Các thiết bị IoT cũng được cấy nghép vào cơ thể người để theo dõi tình trạng sống của các cơ quan khác nhau, trở thành mục tiêu của những cuộc tấn công nhằm làm sai lệch dữ liệu. Tấn công như vậy sẽ rất nguy hiểm. Bài báo này tập trung trình bày các thách thức của việc bảo mật hệ thống IoT, sau đó đi sâu vào một khía cạnh an toàn của các hệ thống IoT xuất phát từ bên trong thiết bị phần cứng – đó chính là firmware của thiết bị.

Doi: https://doi.org/10.54644/jte.2024.1546

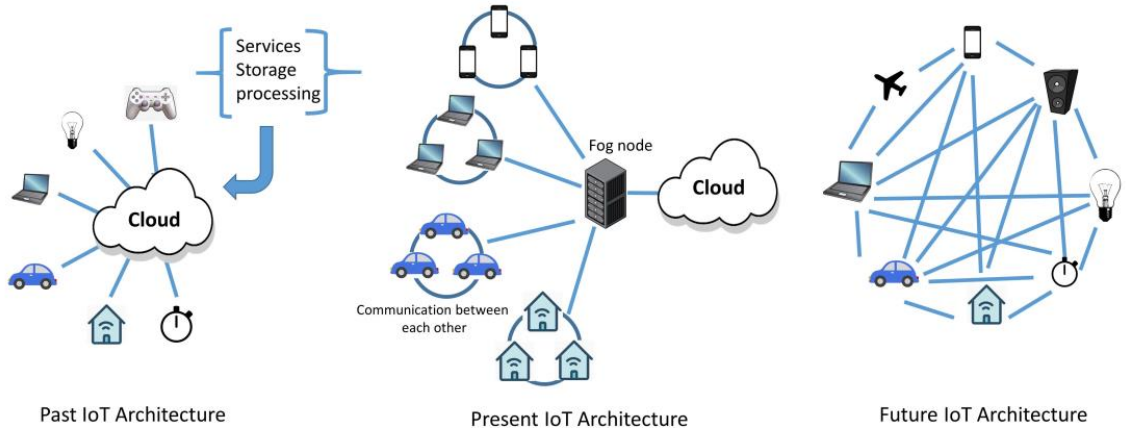
Copyright © JTE. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial 4.0 International License which permits unrestricted use, distribution, and reproduction in any medium for non-commercial purpose, provided the original work is properly cited.

JTE
HCMUTE
ISSN: 1859-1272

TẠP CHÍ KHOA HỌC GIÁO DỤC KỸ THUẬT
Trường Đại học Sư phạm Kỹ thuật Thành phố Hồ Chí Minh
Website: https://jte.edu.vn
Email: jte@hcmute.edu.vn

1. Giới thiệu

Tốc độ kết nối thiết bị Internet xung quan chúng ta đã tăng lên nhanh chóng. Báo cáo của Gartner [1]: Có khoảng 8,4 tỷ kết nối mọi thứ trên toàn thế giới năm 2020, dự kiến tăng lên 20,4 tỷ vào năm 2022. Việc sử dụng các ứng dụng IoT đang gia tăng ở mọi nơi trên thế giới. Dẫn đầu xu hướng này là các nước trong khu vực Tây Âu, Bắc Mỹ, Trung Quốc. Số lượng các thiết bị IoT theo chuẩn máy đến máy (M2M) dự kiến sẽ tăng từ 5,6 tỷ năm 2016 lên 27 tỷ vào năm 2024. Điều này chứng tỏ IoT sẽ là một trong những thị trường lớn có thể hình thành nên nền tảng của nền kinh tế kỹ thuật số đang mở rộng. IoT ngành dự kiến sẽ tăng trưởng về mặt doanh thu từ 892 tỷ USD năm 2018 lên 4 nghìn tỷ USD vào năm 2025. Kết nối M2M bao gồm một loạt các ứng dụng như thành phố thông minh, môi trường thông minh, lưới điện thông minh, bán lẻ thông minh, nông nghiệp thông minh, Hình 1 cho thấy kiến trúc quá khứ, hiện tại và tương lai của IoT



Hình 1. *Kiến trúc hiện tại và tương lai của IoT [1]*

Khi chúng ta ngày càng dựa vào các hệ thống kết nối này, việc bảo mật IoT trở nên tối quan trọng [2]. Bảo mật IoT gồm các biện pháp bảo vệ các thiết bị được kết nối cũng như hệ thống mạng chứa chúng. Khi các thiết bị IoT thâm nhập vào mọi khía cạnh của cuộc sống, chúng sẽ gây ra các vấn đề bảo mật đặc biệt. Lỗ hổng của các thiết bị IoT này có thể dẫn đến rủi ro đáng kể, bao gồm khả năng vi phạm dữ liệu cá nhân, gián đoạn hoạt động kinh doanh và thậm chí là các mối đe dọa đối với an toàn vật lý. Số liệu từ hãng công nghệ Palo Alto: 98% dữ liệu IoT không được mã hóa. Thông qua hình thức nghe lén, hacker có thể dễ dàng thu thập và đọc được các dữ liệu mật được trao đổi giữa các thiết bị với nhau trên hệ thống hoặc giữa chúng với hệ thống quản lý, giám sát; 57% các thiết bị IoT trong hệ thống được xem là các rủi ro an toàn thông tin và khởi nguồn cho các cuộc tấn công mạng quy mô vừa và lớn; 83% các thiết bị y khoa phục vụ công tác chẩn đoán bằng hình ảnh đang sử dụng các hệ điều hành đã ngừng hỗ trợ từ các hãng. Số liệu có sự tăng vọt so với năm 2018, với 56% [3].

1.1. Tình hình nghiên cứu trong nước

Theo [4] Tại Việt Nam, có khoảng 10 thành phố chính thức ký kết các hợp đồng với đối tác trong và ngoài nước để xây dựng thành phố thông minh (Smart City), trong đó sẽ triển khai thí điểm ở một số lĩnh vực như y tế, giáo dục. Căn cứ tình hình thực tế hiện nay, để phát triển Smart City thành công và đảm bảo an toàn thông tin phải sử dụng nền tảng (platform) của Việt Nam. VNPT là một trong các đơn vị đẩy mạnh phát triển hạ tầng công nghệ thông tin, mà trọng tâm là IoT. Đơn vị này đã nghiên cứu và phát triển IoT Smart Connected Platform có 6 đặc điểm cốt lõi: kết nối, thu thập, quản lý, kiểm soát, xây dựng và phân phối. Tuy là một nền tảng mở, cho phép tất cả các nhà phát triển có thể tham gia xây dựng ứng dụng của riêng mình, sản phẩm vẫn đảm bảo các yêu cầu về an toàn thông tin nghiêm ngặt. Bên cạnh VNPT, Viettel cũng đang đẩy nhanh triển khai nền tảng để thiết kế hệ sinh thái cho các ứng dụng về NB-IoT của Viettel tới khách hàng như đỗ xe thông minh, giám sát chất lượng không khí, giám sát vị trí, thiết bị đo lường. Nghị quyết số 52-NQ/TW ngày 27/9/2019 đề ra những chủ trương chính sách tham gia vào cuộc cách mạng số hay đề án xây dựng chuyển đổi số. Nghị quyết đã đề cập đến việc

đầu tư nâng cấp hạ tầng kỹ thuật đảm bảo an toàn an ninh mạng, xây dựng và triển khai có hiệu quả Nghị quyết số 30-NQ/TW, ngày 25/7/2018 của Bộ Chính trị về Chiến lược an ninh mạng quốc gia

1.2. Tình hình nghiên cứu nước ngoài

Chính phủ các nước trên thế giới nhận thức rất rõ các rủi ro tiềm ẩn trong các thiết bị IoT, nên đã có nhiều chính sách, quy định liên quan nhằm hạn chế rủi ro. Theo [4]: Tại Mỹ, điều luật SB-327 - California có hiệu lực từ ngày 01/01/2020 đã quy định về việc ngăn cấm sử dụng mật khẩu mặc định với thiết bị IoT có kết nối Internet. Chính phủ Anh cũng đã đưa ra dự thảo liên quan đến vấn đề an toàn an ninh lĩnh vực IoT vào ngày 27/01/2020. Liên minh châu Âu cũng đã ban hành "Danh mục hướng dẫn bảo mật thiết bị IoT" vào ngày 19/11/2019. Trong khu vực châu Á, Nhật Bản đã thực hiện các chính sách về an toàn không gian mạng, trong đó chú trọng vào hạ tầng thiết bị IoT.

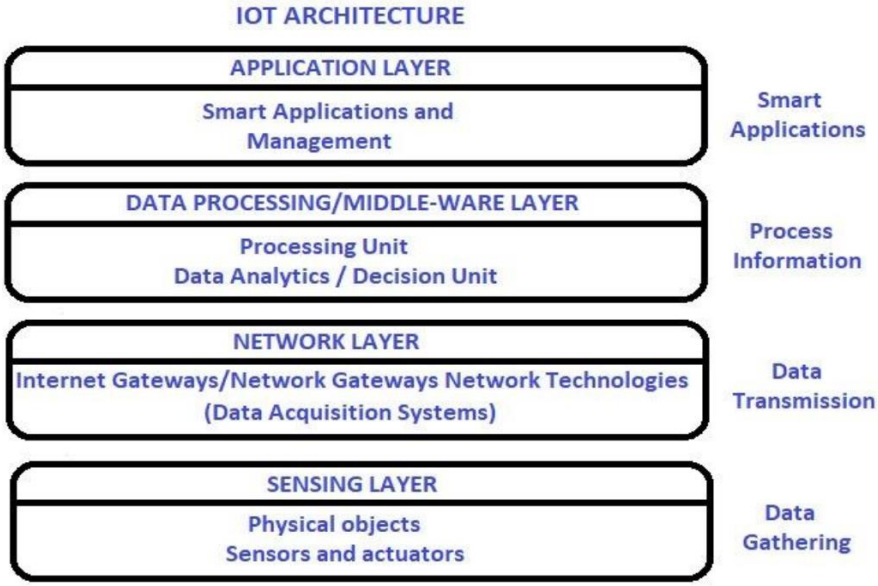
2. Một số vấn đề liên quan tới bảo mật IoT (IoT security)

2.1. Bảo mật IoT (IoT Security)

Bảo mật IoT là tập hợp các kỹ thuật, chiến lược và công cụ được dùng để bảo vệ các thiết bị này khỏi bị xâm phạm, chính khả năng kết nối vốn có của IoT lại khiến các thiết bị này ngày càng dễ bị tấn công mạng. Vì IoT rất rộng nên bảo mật IoT còn rộng hơn. Điều này đã dẫn đến một loạt các phương pháp bảo mật IoT: Bảo mật giao diện chương trình ứng dụng (API), xác thực cơ sở hạ tầng khóa công khai (PKI)... và bảo mật mạng chỉ là một số phương pháp mà các nhà lãnh đạo CNTT có thể sử dụng để chống lại mối đe dọa ngày càng tăng của tội phạm mạng và khủng bố mạng bắt nguồn từ các thiết bị IoT dễ bị tấn công [5].

2.2. Kiến trúc IoT và Những Phát Sinh Bảo Mật Liên Quan Tại Mỗi Lớp

Kiến trúc IoT: Có một số kiến trúc IoT được đề xuất, có thể chứa từ 3 tới 7 lớp. Hình 2 là kiến trúc cơ bản gồm 4 lớp [6]



Hình 2. *Kiến trúc IoT 4 lớp [6]*

- Lớp cảm nhận (Sensing layer): chứa các cảm biến và cơ cấu chấp hành, dùng để thu thập dữ liệu từ môi trường xung quanh và truyền tới lớp mạng
- Lớp mạng (Network layer): chứa các thiết bị được kết nối với nhau, có thể theo phương thức có dây hoặc không dây. Có một số lớp bên trong kiến trúc mạng, lớp Network đóng vai trò quan trọng nhất trong việc thiết lập hạ tầng truyền thông và lưu trữ dữ liệu. Nhiều loại mạng khác nhau được sử dụng như: LANs, WANs, PANs.

- Middleware layer: đóng vai trò cầu nối giữa lớp cảm nhận và lớp ứng dụng, nhiệm vụ là tích hợp các thiết bị và mạng, cung cấp nền tảng để phát triển các ứng dụng IoT và cho phép tích hợp nhiều thiết bị và mạng
- Lớp ứng dụng (Application layer): cung cấp cho người dùng giao diện đầu cuối để tương tác với hệ thống IoT

Các Phát sinh bảo mật

Có một số thách thức liên quan đến kiến trúc IoT bốn lớp, trong đó thách thức quan trọng là đảm bảo tính bảo mật và quyền riêng tư của dữ liệu được thu thập bởi Internet. Để các hệ thống IoT không trở thành mục tiêu của các cuộc tấn công mạng, cần có các biện pháp an ninh thích hợp được thực hiện ở mỗi lớp. Bên cạnh đó cũng cần phải đảm bảo khả năng tương tác giữa các thiết bị và mạng khác nhau sử dụng các giao thức truyền thông khác nhau.

Thách thức bảo mật tại các lớp

Các phát sinh bảo mật liên quan tới các lớp theo [7], [8] như sau:

- Lớp ứng dụng: tùy vào từng loại ứng dụng, cụ thể như: xác thực (Authentication), truy cập dữ liệu (data access), bảo vệ và khôi phục dữ liệu, tính tin cậy.
- Middleware layer: gồm một số công nghệ lưu trữ dữ liệu, nên phải đối mặt với những rủi ro tấn công mạng lớn như: DoS, jamming, truy cập trái phép, đầu độc bên trong, bad output, node modification, malicious-code, …
- Network layer: Có nhiều lỗ hổng trong lớp mạng bất chấp các biện pháp bảo vệ nó bao gồm: Spoofing, denial of service (DoS), eavesdropping, man-in-themiddle, sybil attack, cluster security problems, sinkhole attack, sleep deprivation attack.
- Lớp cảm nhận: lớp này gồm các cảm biến có khả năng tính toán và lưu trữ hạn chế. Dữ liệu thu thập được truyền qua mạng không dây làm phơi bày chúng với những nguy cơ an toàn và tấn công, chủ yếu vì các thiết bị vật lý có một số điểm yếu như: Node capture, unauthorized access, tag cloning, mass node authentication, fake node and malicious data, DoS, eavesdropping, spoofing, routing attack, RF jamming, replay, side channel attack…

3. Firmware (Phần sụn)

3.1. Khái niệm

Thuật ngữ firmware được dùng để chỉ phần mềm dạng mã máy được lưu trong EEPROM hoặc FLASH [9], [10], [11]. Có 2 dạng firmware phổ biến: firmware mức thấp và firmware mức cao. Firmware mức thấp thường được lưu trong EEPROM nên khó thay đổi và cập nhật, firmware mức cao được lưu trong bộ nhớ flash. Firmware nằm giữa phần cứng và chương trình ứng dụng, đóng vai trò giao diện lập trình cho phần mềm bằng cách thực hiện hóa các lệnh phần cứng. Firmware là kết hợp các thành phần khác nhau của các file nhị phân: bootloader, kernel hệ điều hành, hệ thống tập tin. Vì các thiết bị IoT có năng lực tính toán và lưu trữ hạn chế, nên firmware thường được burnt dưới dạng nén. Chức năng chủ yếu của firmware là điều khiển phần cứng thiết bị. Firmware là thành phần thiết yếu trong các thiết bị phổ biến như [12]: Wife router, camera, television, laptop computer, mobile phone, printer.

3.2. Ảnh firmware (firmware image)

Ảnh firmware [10] là tập tin chứa mã firmware cho thiết bị hoặc hệ thống cụ thể. Nó thường chứa tất cả các mã cần thiết cho thiết bị cùng với các thiết lập cấu hình, các cấu trúc dữ liệu và các thông tin được yêu cầu khác cho thiết bị. Ảnh firmware được phân phối bởi nhà sản xuất thiết bị và được cập nhật theo thời gian để sửa lỗi cũng như thêm vào các đặc điểm mới hoặc cải thiện hiệu suất.

Ảnh firmware khác với mã ứng dụng truyền thống, vì chúng chứa tất cả các phần mềm hệ thống cần thiết để làm cho phần cứng làm việc, có thể chứa hoặc không chứa hệ điều hành. Điều này làm cho chúng trở nên cực kỳ quan trọng về mặt bảo mật IoT: Firmware điều khiển toàn bộ hoạt động của thiết bị IoT, còn được gọi là linh hồn của thiết bị. Nên chỉ một lỗi duy nhất ẩn dấu trong firmware có thể gây bất lợi về tính toàn vẹn của phần mềm dẫn tới những tác động bảo mật rất lớn. Việc phát triển firmware

yêu cầu hiểu biết sâu về kiến trúc phần cứng của thiết bị cũng như yêu cầu cụ thể của ứng dụng mà thiết bị được dùng. Các kỹ sư sử dụng các ngôn ngữ lập trình như C và hợp ngữ để viết code tương tác trực tiếp với phần cứng thiết bị

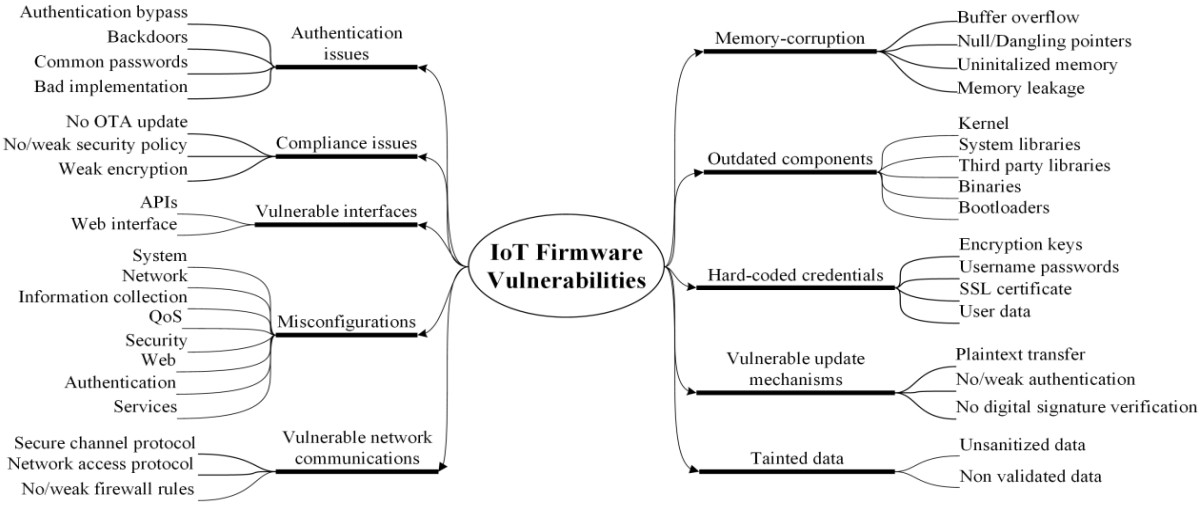
3.3. Định dạng file ảnh firmware (firmware image formats)

Có nhiều định dạng ảnh firmware khác nhau đang được dùng ([11], [12]) điều này cho thấy hệ sinh thái firmware rất đa dạng, có các định dạng sau:

- **squashfs:** đây là dạng file chỉ đọc, được dùng để chứa các file nén, chủ yếu để tối thiểu hóa dữ liệu của phần đầu (header)
- **cramfs:** loại file này thường dùng trong các hệ thống nhúng
- **jffs2:** đây là loại hệ thống tập tin có cấu trúc dài, để xử lý các thiết bị nhớ flash
- **yaffs2:** đây là loại hệ thống tập tin có cấu trúc dài, chỉ được ghi một lần theo khối với đầy đủ thông tin và tổ chức lại thứ tự các khối tùy vào việc sử dụng gần đây.
- **ext2:** đây là hệ thống tập tin được mở rộng, chủ yếu dùng làm cho việc xử lý nhanh hơn.

3.4. Các lỗ hổng firmware

Có nhiều lỗ hổng bảo mật firmware được phát hiện bởi các tổ chức như OWASP (The Open Web Application Security Project), các nhóm nghiên cứu. Theo [11], [12], [13] các lỗ hổng firmware được phân loại như trong hình 3



Hình 3. *Phân loại lỗ hổng firmware IoT [13]*

3.5. An toàn firmware (Bảo mật firmware)

Không có định nghĩa nào được chấp nhận rộng rãi về bảo mật firmware, nhưng nó thường chỉ tới việc bảo vệ firmware khỏi bị khai thác, sửa đổi và truy cập trái phép. Như đã nói, firmware là thành phần quan trọng của nhiều thiết bị điện tử và nếu bị xâm hại, có thể dẫn đến các lỗ hổng bảo mật nghiêm trọng khó phát hiện và giảm thiểu [9]. Các nhà phát triển firmware phải tuân thủ các phương pháp mã hóa an toàn và thiết kế chương trình firmware có lưu ý đến tính bảo mật ngay từ đầu, gồm: sử dụng các cơ chế mã hóa, xác thực, điều khiển truy cập để bảo vệ firmware khỏi truy cập trái phép hoặc giả mạo. Để sản xuất một thiết bị thực sự an toàn, cần nhiều thứ hơn là chỉ mã hóa an toàn. Để đạt được điều này, phải kích hoạt một bộ tính năng bảo mật tối thiểu. Lý tưởng nhất là tất cả các biện pháp bảo mật do nền tảng phần cứng và chuỗi công cụ phần mềm cung cấp phải được sử dụng. Một số tính năng bảo mật phổ biến cần được xem xét:

- Secure boot: là quá trình đảm bảo chỉ firmware và phần mềm đáng tin cậy mới được thực thi trên thiết bị, bao gồm việc xác minh tính toàn vẹn của firmware trước khi nó được thực thi và ngăn thiết bị khởi động nếu firmware bị giả mạo.

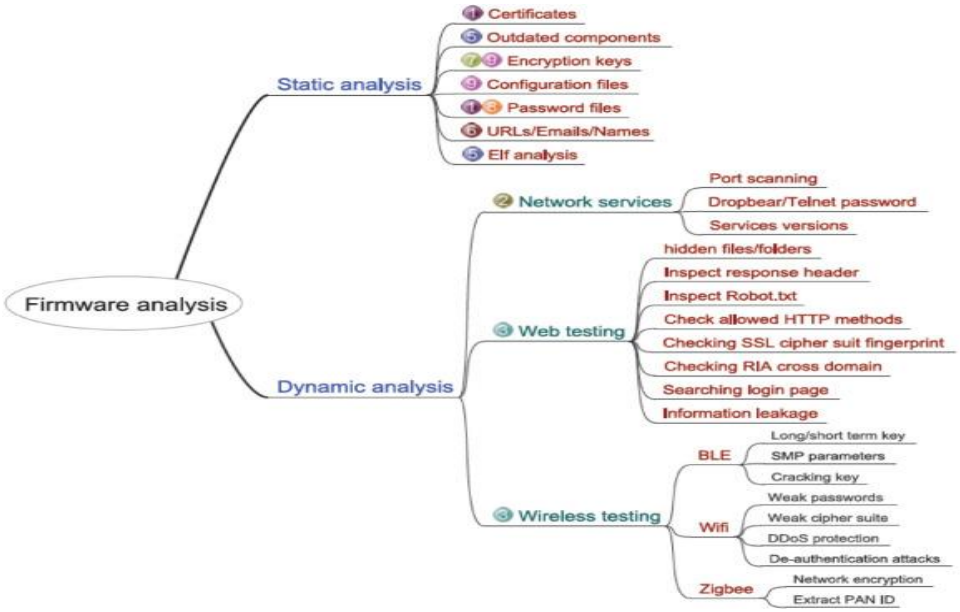
- Firmware updates: Cập nhật firmware rất quan trọng để giải quyết các lỗ hổng bảo mật và sửa lỗi. Tuy nhiên, bản thân quá trình cập nhật cũng có thể gây ra rủi ro bảo mật nếu nó không được thực hiện đúng cách. Tính toàn vẹn của các bản cập nhật firmware phải được bảo vệ để ngăn chặn kẻ tấn công tiêm mã độc vào thiết bị.
- Cryptography: là triển khai đúng cách mật mã trong các thiết bị IoT để đảm bảo tính bảo mật, tính toàn vẹn, tính xác thực của dữ liệu được truyền qua internet. Nếu không có mật mã thích hợp, thông tin nhạy cảm như dữ liệu cá nhân, thông tin tài chính và thậm chí cả cơ sở hạ tầng quan trọng có thể bị xâm phạm.
- Access control (điều khiển truy cập): firmware cần triển khai các cơ chế kiểm soát truy cập để hạn chế khả năng người dùng truy cập trái phép hoặc sửa đổi hoặc tác động đến tính toàn vẹn của phần mềm.
- Monitoring and auditing: Cần giám sát thiết bị để kịp thời phát hiện các thay đổi, và ghi lại để phát hiện các thay đổi trái phép.
- Physical security: bảo vệ chống lại các giả mạo vật lý như: dùng con dấu chống giả mạo, lưu trữ an toàn.
- Vulnerability assessments: thường xuyên đánh giá lỗ hổng để phát hiện và giải quyết mọi lỗ hổng tiềm ẩn trong firmware.
- Education and training: tất cả các bên liên quan gồm: nhà phát triển, quản trị, người dùng đầu cuối phải được huấn luyện các biện pháp thực hành tốt nhất về bảo mật firmware.

3.6. Phân tích firmware

Các thiết bị IoT có thể bị tấn công, và chặng cuối là firmware, vì các thành phần riêng biệt được nhúng trong firmware, kernel có thể bị xử lý nếu truy cập được vào bootloader. Đó là lý do tại sao việc bảo mật firmware bắt đầu bằng việc phân tích nó để tìm ra sơ hở [10]. Hơn nữa nếu có thể điều khiển firmware, người ta có thể điều khiển thiết bị, và cũng tìm thấy nhiều lỗ hổng trong thiết bị. Một thiết bị IoT cũng là một điểm nhập dễ dàng cho kẻ tấn công vào hệ thống mạng.

Có 2 phương pháp phân tích: phân tích tĩnh và phân tích động [13], [14].

- Phân tích tĩnh (static analysis): là việc phân tích phần mềm mà không cần thực thi nó
- Phân tích động (dynamic analysis): được thực hiện bằng cách thực thi firmware hoặc thông qua platform vật lý hoặc môi trường giả lập
- Mục đích của phân tích tĩnh và động [15] như tóm tắt trong hình 4



Hình 4. *Phân tích tĩnh và phân tích động firmware [15]*

- Khi phân tích firmware người ta có thể tìm thấy [13], [16]:
  - Các thành phần được mã cứng (hardcoded) như: Credentials, Keys, Network values
  - Các thông tin nhạy cảm không được mã hóa (Encryption not used for sensitive information) như các tập tin chứa thông tin mật khẩu, tài khoản, tập tin cấu hình, các file kịch bản…
  - Các bản cập nhật không được mã hóa (Updates not encrypted)
  - Bản cập nhật chưa được xác minh trước khi tải lên/cài đặt (Update not verified before upload/install)
  - Các lỗ hổng CVE (Common Vulnerabilities and Exposures): các lỗ hổng bảo mật được công khai.
  - Các lỗ hổng CWE (Common Weakness Enumeration): Danh sách các lỗi phần mềm nguy hiểm nhất.

3.7. Những thách thức và cơ hội đối mặt với việc phát hiện lỗ hổng firmware

Theo [17] việc phát hiện các lỗ hổng firmware có những thách thức sau:

- **Các loại thiết bị IoT rất phức tạp và có các tiêu chuẩn khác nhau:** Có nhiều nhà sản xuất IoT nhưng không có đặc tả thống nhất, mỗi nhà sản xuất áp dụng các định dạng file, kiến trúc CPU, và các phương pháp mã hóa khác nhau. Điều này làm cho việc phân tích firmware đối mặt với những thách thức lớn, vì thế rất khó để tạo ra một hệ thống phân tích lỗ hổng hoàn chỉnh. Hơn nữa kiến trúc CPU của thiết bị IoT khác với kiến trúc của các nền tảng thông thường dẫn đến sự khác biệt trong tập lệnh. Phần cứng các ngoại vi của thiết bị IoT rất đa dạng, làm gia tăng khó khăn trong việc ứng dụng công nghệ phân tích động
- **Firmware khó lấy và giải nén:** công nghệ phân tích động nói chung cần thực hiện giám sát và phân tích ở ngoại vi của chương trình đang chạy. Do hạn chế về tài nguyên lưu trữ của các thiết bị IoT nên các modul phân tích liên quan không thể triển khai được, dẫn đến không thể áp dụng công nghệ phân tích động. Đồng thời năng lực tính toán của phần cứng CPU hạn chế làm giảm hiệu suất phân tích động. Trong thực tế thiết bị IoT thường không cung cấp mã nguồn firmware và thậm chí hầu hết firmware không được cung cấp công khai. Vì vậy việc lấy được firmware cũng là công việc khó khăn.
- **Tỷ lệ thành công trong việc mô phỏng firmware động rất thấp:** hiện tại việc phát hiện lỗ hổng dựa trên giao diện web firmware là phương pháp hiệu quả hơn để phát hiện lỗ hổng firmware, nhưng phương pháp này yêu cầu thiết bị thực hoặc mô phỏng firmware động. Vì một số thiết bị đắt tiền và mô phỏng firmware phổ biến hơn nên hầu hết các nghiên cứu hiện tại đều áp dụng mô phỏng firmware động dựa trên QEMU. Theo thống kê, chỉ 13% - 20% firmware có thể được mô phỏng hoàn toàn.
- **Cơ hội khai thác lỗ hổng trong các thiết bị IoT:** đặc điểm của thiết bị IoT không chỉ mang lại những thách thức trong việc khai thác lỗ hổng mà còn mang đến những cơ hội mới:
  - (1) Sự phong phú của tương tác hệ thống: Mặc dù phục vụ cho việc khai thác lỗ hổng của các thiết bị IoT, nhưng các thiết bị IoT thường tương tác với thiết bị đầu cuối, đám mây và các hệ thống khác nên bản thân thiết bị có nhiều bề mặt tấn công hơn.
  - (2) Tái sử dụng ồ ạt mã thành phần: Trong quá trình phát triển các chương trình thiết bị IoT, để tiết kiệm chi phí phát triển, một số lượng lớn thư viện nguồn mở của bên thứ ba được sử dụng, dẫn đến một số lượng lớn lỗ hổng của các thành phần bên thứ ba
  - (3) Sự hội tụ của các loại lỗ hổng: Các loại lỗ hổng phần mềm chung bao gồm các lớp hỏng bộ nhớ (tràn ngăn xếp, tràn heap, ứng dụng con trỏ null, bản phát hành thứ cấp, v.v.), các lớp xác minh đầu vào (chèn lệnh, v.v.), các lớp lỗi cấu hình, v.v.

4. Phân tích một số firmware và kết quả

4.1. Giới thiệu công cụ phân tích firmware EMBA

Hiện nay có nhiều công cụ phân tích firmware, như: Binwalk, OFRAK, FAT, Firmwalker, Firmadyne, QEMU, Frida, EMBA. Trong phạm vi của nghiên cứu này, tác giả chọn dùng công cụ

EMBA, vì: là công cụ mã nguồn mở, nó tích hợp nhiều công cụ thành phần bên trong giúp tự động hoá quá trình phân tích (cả phân tích tĩnh và phân tích động), đồng thời cho kết quả dưới dạng giao diện web, dễ theo dõi.

EMBA (Embedded Analysis Toolkit) được thiết kế làm công cụ phân tích firmware trung tâm dành cho cá nhân và các đội kiểm tra an toàn các sản phẩm. Nó hỗ trợ quy trình phân tích bảo mật hoàn chỉnh bắt đầu bằng việc trích xuất firmware, thực hiện phân tích tĩnh và phân tích động thông qua mô phỏng và cuối cùng là tạo báo cáo dạng web. EMBA tự động phát hiện các điểm yếu và lỗ hổng có thể có trong firmware. Ví dụ: các tập tin nhị phân không an toàn, các thành phần phần mềm cũ và lỗi thời, mật khẩu được mã hóa cứng. EMBA là công cụ dòng lệnh có khả năng tạo ra báo cáo web. Việc cài đặt, cách phân tích, đọc kết quả theo hướng dẫn trong [18], [19], [20], [21], [22], [23].

4.2. Cấu hình máy tính để chạy công cụ phân tích EMBA

Công cụ phân tích EMBA được chạy trên máy ảo Virtual box 7.0. Máy ảo chạy hệ điều hành Ubuntu 20.04, bộ nhớ 20GB, đĩa cứng 100GB, CPU 8 nhân.

4.3. Các firmware được phân tích

Thông tin về các firmware được phân tích được liệt kê tóm tắt trong bảng 2

Bảng 1. *Thông tin các firmware được phân tích*

Thiết bị	Nhà cung cấp	Ảnh Firmware	Dung lượng
Wifi Router	D-Link	dir300_rev_b_v2.05_abnj.rar	3.2MB
Camera	D-Link	DCS5020L_REVA_FIRMWARE_v1.15.12.zip	7.4MB
Router	Linksys	DVRF_v03.bin	7.8MB
Webcam	Foscam	c1_firmware_2.x.2.5_1.zip	13.5MB

4.4. Kết quả phân tích

4.4.1. Router wifi D-Link

Kết quả phân tích được trình bày tóm tắt trong bảng 2

4.4.2. D-Link DCS-5020L Camera

Kết quả phân tích được trình bày tóm tắt trong bảng 2

Bảng 2. *Kết quả phân tích firmware trong mục 4.4.1 và 4.4.2*

	Phân tích firmware trong 4.4.1	Phân tích firmware trong 4.4.2
Iterm	**Explaination**	**Explaination**
Architecture	Detected architecture and endianness (verified): MIPS / EL	Detected architecture and endianness (verified): MIPS / EL
OS	Operating system detected (verified): Linux / v2.6.21	Operating system detected (verified): Linux / v2.6.21
File System	1041 files and 75 directories detected.	692 files and 103 directories detected.
Shell scripts		Found 230 issues in 42 shell scripts
Configuration issues		Found 10 password related details via STACS. Found 2 outdated certificates and 1 expiring certificates in 3 certificate files and in a total of 6 certificates. Found 14 kernel modules with 0 licensing issues.

		Found 0 interesting files and 1 files that could be useful for post-exploitation.
SBOM		Dentified a SBOM including 7 software components with version details
CVE analysis	Identified 2116 CVE entries. Identified 569 High rated CVE entries / Exploits: 63 Identified 1254 Medium rated CVE entries / Exploits: 95 Identified 293 Low rated CVE entries /Exploits: 21 179 possible exploits available (16 Metasploit modules). Remote exploits: 3 / Local exploits: 32 / DoS exploits: 13 / Github PoCs: 0 / Known exploited vulnerabilities: 0 / Verified Exploits: 0	Identified 2108 CVE entries. Identified 577 High rated CVE entries / Exploits: 66 Identified 1246 Medium rated CVE entries / Exploits: 97 Identified 285 Low rated CVE entries /Exploits: 20 183 possible exploits available (14 Metasploit modules). Remote exploits: 3 / Local exploits: 32 / DoS exploits: 11 / Github PoCs: 0 / Known exploited vulnerabilities: 0 / Verified Exploits: 0
Password information		Found 2 password related files: chpasswd.sh; wifipass.sh
CWE		cwe-checker found a total of 5200 of the following security issues in 20 tested binaries
Certification		Found 3 possible certification files
Configuration files		Found 3 possible configuration files: fstab; upnpd.conf; lld2d.conf

4.4.3. Router wifi Linksys

Kết quả phân tích được trình bày tóm tắt trong bảng 3

4.4.4. Webcam Foscam

Kết quả phân tích được trình bày tóm tắt trong bảng 3

Bảng 3. *Kết quả phân tích firmware trong mục 4.4.3 và 4.4.4*

	Phân tích firmware trong 4.4.3	Phân tích firmware trong 4.4.4
Iterm	**Explaination**	**Explaination**
Architecture	(verified): MIPS / EL	(verified): ARM / EL
OS	(verified): Linux / v2.6.22	(verified): Linux / v3.0.8
File System	244 files and 62 directories detected.	523 files and 198 directories detected.
Shell scripts	Found 3 issues in 4 shell scripts	Found 170 issues in 48 shell scripts
Configuration issues	Found the following configuration issues:Found 6 areas with weak permissions. Found 22 kernel modules with 5 licensing issues. Found 0 interesting files and 2 files that could be useful for post-exploitation	Found 411 areas with weak permissions. Found 16 password related details. Found 35 password related details via STACS (2 passwords cracked.) Found 41 kernel modules with 21 licensing issues.
SBOM	Identified a SBOM including 13 software components with version details	Identified a SBOM including 10 software components with version details

CVE analysis	Identified 2060 CVE entries.	Identified more than 100 CVE entries
Password information		
CWE	cwe-checker found a total of 3443 security issues in 14 tested binaries	we-checker found a total of 6010 security issues in 18 tested binaries
Kernel	Verified 161 kernel vulnerabilities (kernel symbols)	Verified 106 kernel vulnerabilities (kernel symbols)

Nhận xét: Các thiết bị nhúng và IoT hiện nay đa phần sử dụng các bộ xử lý MIPS hoặc ARM, trong đó tích hợp firmware với hệ điều hành thông dụng là Linux, chứa kernel, hệ thống tập tin với các file cấu hình, các file chứa thông tin được mã cứng (như user name và password) thường ẩn chứa bên trong nhiều phát sinh về bảo mật, các lỗ hổng này thường là các lỗ hổng đã được công bố, hoặc lỗ hổng mới phát sinh, tuy nhiên hay bị bỏ qua trong quá trình phát triển và triển khai. Đây có lẽ là khó khăn với các nhà bảo mật hệ thống sau này.

5. Kết luận

Trong hệ thống IoT, hầu như các thiết bị đều có firmware, trong firmware luôn tiềm ẩn những nguy cơ rủi ro cao về các lỗ hổng mà nhà sản xuất không lường trước được. Việc phân tích firmware có thể giúp phát hiện những lỗ hổng trong thiết bị, qua đó có thể giúp những người triển khai IoT có thể đưa ra các biện pháp phòng tránh. Bài báo này đã trình bày một số khía cạnh khác nhau của firmware, các lỗ hổng, các mối đe dọa mà thiết bị IoT có thể gặp phải khi firmware được phân tích. Một số firmware của một số thiết bị đã được phân tích dùng công cụ mã nguồn mở EMBA để tìm ra các lỗ hổng khác nhau mà đối phương có thể tận dụng để tấn công vào hệ thống IoT.

- **Ưu điểm:** Đã phân tích được một số firmware phổ biến, cả những firmware đã được update gần đây, không lấy từ các dự án có sẵn như: OWASP, Github, Webbylab…Có thể dựa vào kết quả để đưa ra các cảnh báo cho nhà sản xuất và triển khai
- **Nhược điểm:** Firmware có dung lượng lớn thì thời gian phân tích tương đối lâu, chỉ sử dụng công cụ mã nguồn mở EMBA, chưa so sánh, đánh giá công cụ này với các công cụ phân tích khác. Chưa sử dụng đầy đủ framework phân tích linh hoạt. Chưa trình bày đầy đủ, chi tiết các công đoạn của việc phân tích.
- **Hướng phát triển:** Sử dụng các framework để phân tích firmware theo các giai đoạn, qua đó có cái nhìn đầy đủ hơn, đưa ra những nhận xét, kết luận mang tính hệ thống hơn. Hơn nữa thông qua việc phân tích có thể đưa ra những cảnh báo, những khuyến nghị cho những nhà cung cấp thiết bị, những nhà triển khai để phòng tránh.

Xung đột lợi ích

Tác giả tuyên bố không có xung đột lợi ích trong bài báo này.

TÀI LIỆU THAM KHẢO

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," Department of CSE and IT, Jaypee Institute of Information Technology, Noida, 201309 India, IEEE, 2019.
[2] M. Toback. "An Introduction to IoT Security: Protecting Your Devices." https://smallbizepp.com/introduction-to-iot-security (accessed Sep. 16, 2023).
[3] Ministry of Information and Communications, Vietnam. "IoT Devices - Information Security Risks and Remediation Solutions," (in Vietnamese). https://mic.gov.vn/atantt/Pages/TinTuc/143262/Thiet-bi-IoT---Cac-rui-ro-an-toan-thong-tin-va-giai-phap-khac-phuc.html (accessed Sep. 24, 2020).
[4] Ministry of Information and Communications, Vietnam. "Information Security in IoT Worldwide and in Vietnam," (in Vietnamese). https://mic.gov.vn/atantt/Pages/TinTuc/143264/An-toan-thong-tin-trong-IoT-tren-the-gioi-va-Viet-Nam.html (accessed Sep. 24, 2020).
[5] K. Yasar. "IoT security (internet of things security)." https://www.techtarget.com/iotagenda/definition (accessed Aug. 2023)
[6] P. Ramesh and M. S. V. R. Reddy, "Architecture, Protocols, Layers and Elements of IoT," *IJCRT*, ISSN: 2320-2882, vol. 9, no. 9, Sep. 2021.
[7] A. El bekkali and M. Essaaidi. "Systematic Literature Review of Internet of Things (IoT) Security." https://www.ripublication.com/adsa.htm (accessed Nov., 2022).
[8] M. R. Ahmed and A. Al Shihimi, *Internet of things network architecture and security challenges*, AIRCC Publishing Corporation, 2023.
[9] S. U. Haq and Y. Singh, *A survey on IoT & embedded device firmware security: architecture, extraction techniques, and vulnerability analysis frameworks*, Springer, October 2023.
[10] A. Szász. "Firmware and Firmware Security." https://bugprove.com/knowledge-hub/7-questions-and-answers-about-firmware-and-firmware-security (accessed Apr. 4, 2023).

[11] M. Toback. "OWASP Top 10 IoT Vulnerabilities: How to Avoid Them." https://smallbizepp.com/owasp-iot-top-10-vulnerabilities (accessed Sep. 2023).
[12] S. Chougule. "IoT Device Penetration Testing." https://owasp.org/www-chapter-pune/meetups/2019/August (accessed Aug. 2019).
[13] Intuz. "A Guide On IoT Firmware Development And Integration." https://www.intuz.com/guide-iot-firmware-development-and-integration (accessed Feb. 2023).
[14] F. Bolandi, "Automated Security Analysis of Firmware," KTH Royal Institute of Technology, 2022.
[15] M. K. Kagita, "A framework for intelligent IoT firmware compliance testing," KeAi, September 2021.
[16] K. P. Siri. "The Various Facets of IoT Firmware Analysis." https://www.cigniti.com/blog/iot-firmware-analysis (accessed Jul. 11, 2023).
[17] W. Wang, T. Zhao, and X. Li, "Research on Known Vulnerability Detection Method Based on Firmware Analysis." https://www.techscience.com/JCS/v4n1/47669/html (accessed Apr. 2022).
[18] P. Bourmeau, "A brief introduction to firmware extraction," 2020.
[19] S. Vasile, D. Oswald, and T. Chothia, "Breaking all the things - a systematic survey of firmware extraction techniques for iot devices," University of Birmingham, 2018.
[20] J. M. Smith, "Case Analysis of Firmware Vulnerabilities and Exploitation," 2016.
[21] R. Sharma. "Unveiling Vulnerabilities: A Deep Dive into Firmware Penetration Testing- Part1." https://ravi73079.medium.com/unveiling-vulnerabilities-a-deep-dive-into-firmware-penetration-testing-part-1-904599cd79be (accessed Sep. 19, 2023).
[22] D. D. Ruck, V. Goeman, and J. Lapon, "Hands-on workshop: Hacking and Protecting Embedded Devices," June 2022.
[23] I. Nadir, H. Mahmood, and G. Asadullah, "A Taxonomy of IoT Firmware Security and Principal Analysis Techniques," March 2023.

TÓM TẮT TIỂU SỬ TÁC GIẢ BẰNG TIẾNG ANH

Dinh Cong Doan graduated from university in Electronics and Telecommunication in 1999 at the HCM City University of Technology, received a master's degree in computer science in 2002 at Ho Chi Minh City University of Technology. He is currently working at the Faculty of Information Technology, HCMC University of Technology and Education. His research interests include Network security, Data communications, Logic Design, IoT, Embedded Systems related technologies.
Email: doandc@hcmute.edu.vn. ORCID: https://orcid.org/0009-0004-2138-5939