AN NINH MẠNG VÀ THÁCH THỨC ĐỐI VỚI HỆ THỐNG INTERNET VẠN VẬT

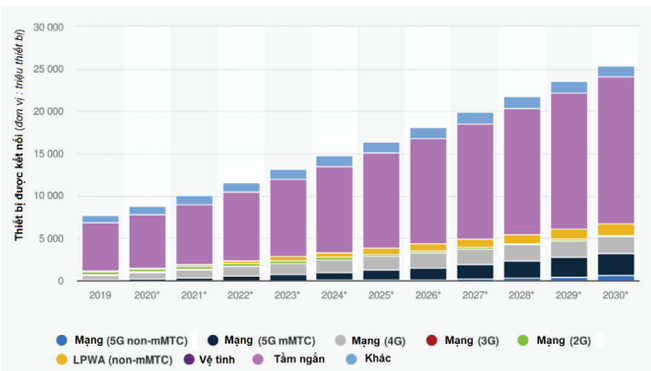
TS Phạm Ngọc Minh, ThS Hà Thị Hồng Vân

Viện Công nghệ Thông tin, Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Việc ứng dụng công nghệ Internet vạn vật (IoT) trong nhiều lĩnh vực như lưới điện thông minh, giám sát môi trường, y tế, sản xuất, logistics… khiến nguy cơ an ninh mạng gia tăng. Đặc biệt, đặc điểm động và đa dạng của các kết nối IoT cùng với hạn chế về tài nguyên đặt ra thách thức lớn về bảo mật. Bài viết cung cấp cái nhìn tổng quan về sự phát triển của IoT và nguy cơ an ninh mạng liên quan, từ đó đưa ra khuyến nghị về việc bảo vệ các hệ thống IoT trong tương lai.

Xu hướng phát triển của công nghệ Internet vạn vật

Theo một cuộc khảo sát vào tháng 12/2020, số lượng thiết bị kết nối IoT trên toàn thế giới vào năm 2019 là 7,74 tỷ và dự kiến vượt quá 25 tỷ vào năm 2030. Đến cuối năm 2022, số lượng thiết bị IoT trực tuyến đã đạt 13,1 tỷ, vượt qua các dự báo được đưa ra trước đó. Tổng số thiết bị IoT, cảm biến và cơ cấu chấp hành, kể cả những thiết bị không kết nối trực tiếp với Internet, ước tính đạt gần 43 tỷ (hình 1) [1].



Hình 1. Dự kiến sự tăng trưởng toàn cầu của các thiết bị kết nối Internet vạn vật giai đoạn 2019-2030 được phân loại theo giải pháp truyền thông [1].

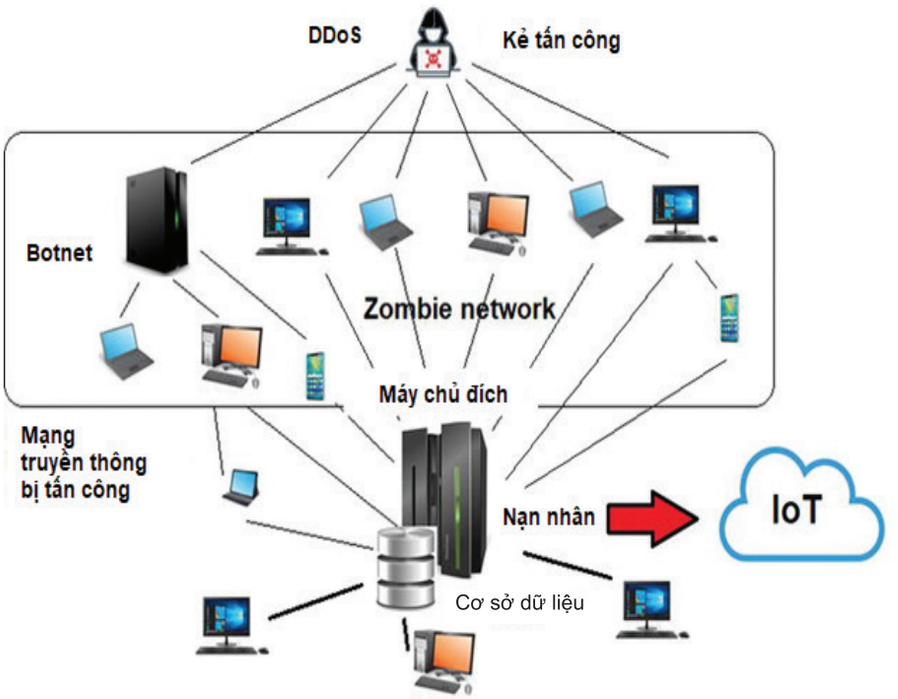
Công nghệ mạng 5G với băng thông rộng, độ trễ thấp và khả năng kết nối nhiều thiết bị hơn đang thúc đẩy mạnh mẽ sự phát triển của IoT. Các giao thức như Zigbee, LoRa và NB-IoT đóng vai trò quan trọng: Zigbee cho IoT tiêu thụ ít năng lượng và truyền dữ liệu tầm ngắn; LoRa cho IoT công nghiệp và nông nghiệp với truyền thông tầm xa và tiêu thụ ít năng lượng; NB-IoT cho kết nối thiết bị IoT với tiêu thụ năng lượng thấp và vùng phủ sóng rộng. Xu hướng hiện nay của IoT bao gồm quản lý từ xa hàng nghìn thiết bị, dựa trên phân tích dữ liệu và trí tuệ nhân tạo (AI) để tối ưu hóa quy trình và ra quyết định thông minh. Công nghệ điện toán đám mây hỗ trợ lưu trữ và xử lý dữ liệu mạnh mẽ, giúp mở rộng quy mô dịch vụ IoT linh hoạt. Những xu hướng này cho thấy, IoT đang ngày càng phát triển và trở thành một phần không thể thiếu trong các lĩnh vực đời sống và công nghiệp.

Nhận diện và đánh giá các nguy cơ đe dọa an ninh mạng đối với Internet vạn vật

Một số cuộc tấn công vào các hệ thống IoT công nghiệp

Hệ thống IoT công nghiệp đang đối mặt với nhiều mối đe dọa bảo mật nghiêm trọng. Các tấn công từ chối dịch vụ (Distributed denial of service - DDoS) làm quá tải các thiết bị IoT, gây ra tình trạng tê liệt hoặc giảm hiệu suất. Tấn công Man-in-the-Middle (MitM) cho phép kẻ tấn công chặn và thay đổi dữ liệu truyền giữa các thiết bị, dẫn đến mất thông tin và giảm độ tin cậy. Phần mềm độc hại như virus và ransomware có thể lây nhiễm, phá hủy hoặc chiếm quyền kiểm soát thiết bị, gây mất dữ liệu và gián đoạn hoạt động.

Đầu tháng 4/2022, nhóm tin tặc Voodoo Bear tấn công hệ thống trạm biến áp cao áp, máy tính và thiết bị mạng



Hình 2. Sơ đồ tấn công từ chối dịch vụ trên hệ thống Internet vạn vật, sử dụng botnet để tấn công máy chủ quản lý thông tin của thiết bị Internet vạn vật, từ đó tiếp cận và kiểm soát cơ sở dữ liệu và mạng kết nối [5].

ở Ukraine bằng biến thể mới của phần mềm độc hại Industryer gây gián đoạn cung cấp điện và thiệt hại lớn cho mạng và máy tính. Cuộc tấn công là một phần của chiến dịch mạng có tổ chức nhằm vào các cơ sở hạ tầng quan trọng của Ukraine, cho thấy mức độ nguy hiểm và tinh vi của các mối đe dọa an ninh mạng hiện nay [2]

Ngày 19/3/2019, Nhà máy nhôm Norsk Hydro tại Mỹ bị tấn công mạng bằng phần mềm tống tiền, gây đình trệ nhiều hoạt động sản xuất. Các hệ thống máy tính và điều khiển tự động bị vô hiệu hóa, buộc công ty phải chuyển sang sản xuất thủ công, làm giảm năng suất và tăng nguy cơ lỗi. Tình trạng này kéo dài nhiều ngày, gây gián đoạn chuỗi cung ứng và giảm sản lượng nhôm. Norsk Hydro phải đầu tư lớn để khôi phục hệ thống, với tổng thiệt hại tài chính ước tính 52 triệu USD. Sự cố này cảnh báo về mức độ dễ bị tổn thương của cơ sở hạ tầng công nghiệp trước các cuộc tấn công mạng [3].

Năm 2018, Nhà máy sản xuất chip TSMC ở Đài Loan (Trung Quốc) bị tấn công mạng nghiêm trọng, virus WannaCry ransomware lan nhanh trong hệ thống máy tính. Sự cố này làm đình trệ hầu hết các dây chuyền sản xuất trong ba ngày, gây gián đoạn nghiêm trọng và ảnh hưởng đến sản xuất, giao hàng của các khách hàng lớn là các công ty công nghệ hàng đầu. Thiệt hại tài chính ước tính khoảng 170 triệu USD, bao gồm chi phí khôi phục hệ thống, tổn thất sản xuất và ảnh hưởng doanh thu. Sự cố này làm nổi bật rủi ro bảo mật mà các nhà sản xuất công nghệ cao phải đối mặt và nhấn mạnh tầm quan trọng của an ninh mạng trong sản xuất công nghiệp [4].

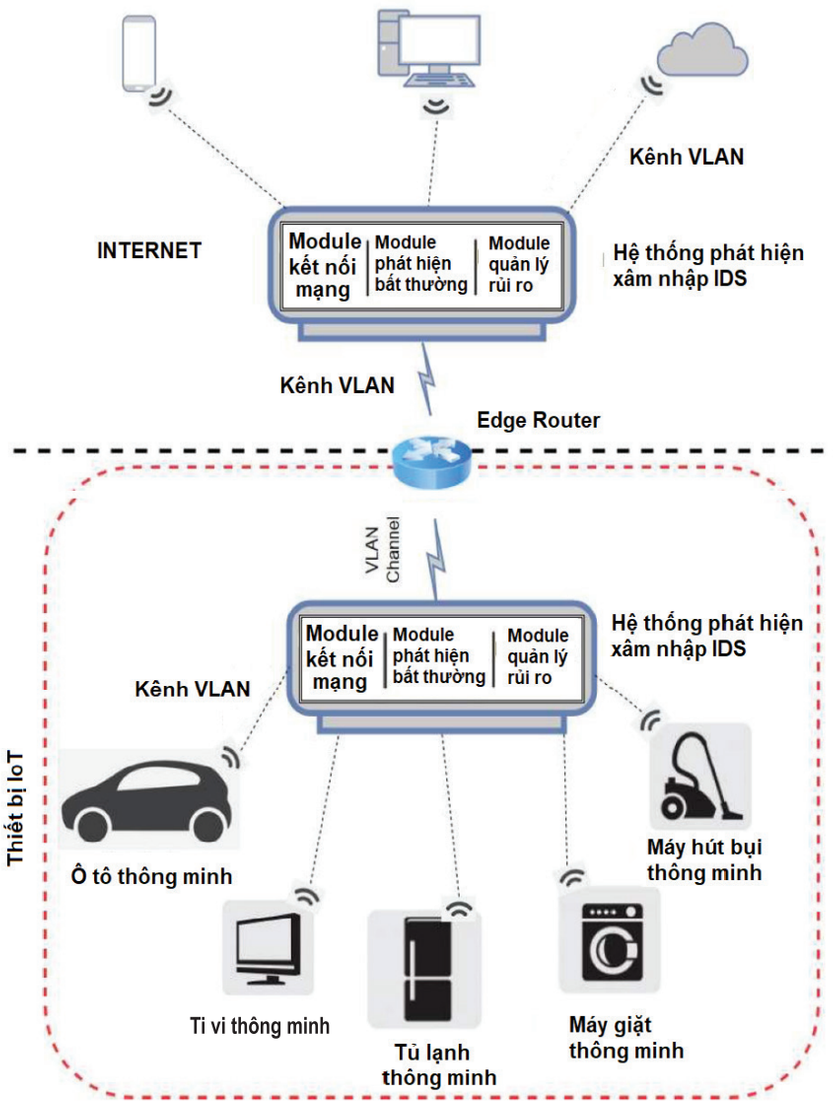
Các nguy cơ đe dọa an ninh mạng trong hệ thống Internet vạn vật

Các hình thức tấn công vào hệ thống IoT đặt ra thách thức lớn về bảo mật, đòi hỏi biện pháp bảo vệ mạnh mẽ. Đặc biệt là các hình thức tấn công chủ yếu như: i) Tấn công DDoS làm ngập lụt hệ thống bằng lượng lớn yêu cầu từ nhiều nguồn, khiến hệ thống quá tải và ngừng hoạt động, gây gián đoạn dịch vụ (hình 2); ii) Tấn công MitM can thiệp vào giao tiếp giữa hai thiết bị IoT, nghe trộm và sửa đổi thông tin trao đổi, dẫn đến đánh cắp thông tin nhạy cảm hoặc hành động giả mạo; iii) Tấn công vào thiết bị đầu cuối khai thác lỗ hổng trong phần cứng hoặc phần mềm của thiết bị IoT để chiếm quyền điều khiển, thực hiện hành động độc hại như kiểm soát từ xa và thu thập thông tin người dùng; iv) Tấn công bằng phần mềm độc hại: kẻ tấn công cài đặt phần mềm độc hại vào thiết bị IoT để lấy cắp thông tin nhạy cảm, hoặc biến thiết bị thành một phần của mạng botnet.

Một số lỗ hổng an ninh trong hệ thống Internet vạn vật

Lỗ hổng phần cứng và phần mềm trong Internet vạn vật

Các thiết bị IoT đang đối mặt với nhiều lỗ hổng bảo mật, đe dọa tính bảo mật và sự riêng tư của người dùng như: (i) Phần cứng: mã hóa yếu khiến dữ liệu dễ bị đánh cắp. Thiết bị thường thiếu khả năng chống lại các cuộc tấn công phần cứng và các cơ chế như phân mảnh dữ liệu hay kiểm tra tính toàn vẹn; (ii) Phần mềm: thiếu cập



Hình 3. Phát hiện xâm nhập và giám sát an ninh [6].

nhật định kỳ làm lộ ra các lỗ hổng bảo mật. Quản lý dữ liệu không an toàn dẫn đến lộ thông tin cá nhân và nhạy cảm, dễ bị sử dụng sai mục đích. Các nhà sản xuất và phát triển phần mềm cần tập trung vào giải pháp bảo mật hiệu quả để bảo vệ người dùng và hạn chế mối đe dọa.

Lỗ hổng giao thức truyền thông trong Internet vạn vật

Những lỗ hổng này có thể bị kẻ tấn công lợi dụng để nghe lén, giả mạo, hoặc chiếm đoạt thông tin. Một số giao thức truyền thông IoT không mã hóa dữ liệu đầy đủ hoặc sử dụng các thuật toán mã hóa yếu, làm cho thông tin gửi và nhận dễ bị phá vỡ. Điều này dẫn đến rủi ro lộ thông tin nhạy cảm như thông tin cá nhân, y tế, hay tài chính.

Ngoài ra, giao thức IoT thường thiếu tính năng xác thực mạnh mẽ, giúp kẻ tấn công dễ dàng giả mạo thiết bị hoặc lừa đảo hệ thống để truy cập dữ liệu, chiếm quyền điều khiển thiết bị. Nguy cơ này đặc biệt cao trong các lĩnh vực như y tế, hạ tầng đô thị thông minh và công nghiệp.

Để giảm thiểu các mối đe dọa này, các nhà phát triển và quản lý hệ thống IoT cần áp dụng các giao thức truyền thông mạnh mẽ, đảm bảo tính an toàn cho dữ liệu trong quá trình truyền tải và lưu trữ. Sử dụng các giao thức mã hóa mạnh, xác thực hai yếu tố và cập nhật thường xuyên là những biện pháp cần thiết để củng cố hệ thống IoT.

Một số giải pháp bảo mật cho hệ thống Internet vạn vật

Các giải pháp bảo mật cho hệ thống IoT bao gồm nhiều phương pháp và công nghệ nhằm bảo vệ thiết bị và dữ liệu. Một số giải pháp quan trọng gồm: i) Mã hóa dữ liệu: sử dụng các thuật toán mã hóa mạnh như AES (Advanced Encryption Standard) và RSA (Rivest-Shamir-Adleman) để bảo vệ dữ liệu trong quá trình lưu trữ và truyền tải; ii) Phát hiện xâm nhập và giám sát an ninh: sử dụng IDS (Intrusion Detection System-IDS) và SIEM (Security Information and Event Management) để phát hiện và xử lý sớm các mối đe dọa an ninh (hình 3); iii) Quản lý danh tính và phân quyền: cơ chế quản lý danh tính để xác thực và ủy quyền người dùng, ngăn chặn các cuộc tấn công giả mạo; iv) Bảo mật mạng và tường lửa: triển khai tường lửa để ngăn chặn tấn công từ bên ngoài và kiểm soát lưu lượng mạng; v) Cập nhật phần mềm định kỳ: đảm bảo thiết bị IoT luôn cập nhật phần mềm, firmware và ứng dụng mới nhất để chống lỗ hổng bảo mật; vi) Giải pháp mã hóa trong phần cứng: sử dụng HSM (Hardware

Security Module) hoặc chip TPM (Trusted Platform Module) để bảo vệ khóa mã hóa và thông tin nhạy cảm; vii) Giám sát và bảo vệ chống DDoS: triển khai giải pháp phòng ngừa và đáp ứng các cuộc tấn công DDoS, giảm thiểu ảnh hưởng đến mạng IoT. Các giải pháp này cùng nhau xây dựng hệ thống IoT an toàn, đảm bảo tính toàn vẹn và bảo mật của dữ liệu, và chống lại các mối đe dọa an ninh phức tạp.

Tương lai của an ninh mạng Internet vạn vật

Trong tương lai gần, các thiết bị IoT sẽ gia tăng và mở rộng sang nhiều lĩnh vực quan trọng như giám sát và phát hiện các nguy cơ biến đổi khí hậu, giảm phát thải khí nhà kính, ô nhiễm môi trường, an ninh quốc phòng. Mặc dù thách thức không nhỏ song những tiến bộ của công nghệ mã hóa lượng tử, internet lượng tử, AI hứa hẹn sẽ hỗ trợ các thiết bị IoT giảm thiểu nguy cơ bị tấn công. Cụ thể: i)Tăng cường giám sát thiết bị: sử dụng IDS và SIEM để phát hiện và phản ứng nhanh chóng với mối đe dọa. Chia sẻ thông tin về mối đe dọa an ninh mạng CTI (Cyber Threat Intelligence) giúp xây dựng hồ sơ kẻ tấn công và cải thiện kiểm soát an ninh cho IoT và Hệ thống điều khiển công nghiệp (ICS); ii) Thêm tính năng bảo mật: mã hóa toàn bộ dữ liệu lưu trữ và truyền tải để bảo vệ thông tin. Sử dụng xác thực mạnh mẽ và phân vùng lưu lượng IoT để quản lý hiệu quả các mối đe dọa an ninh; iii) Tuân thủ các tiêu chuẩn an ninh: tuân thủ khuyến nghị của Viện Tiêu chuẩn và Công nghệ quốc gia Mỹ (NIST) và các tiêu chuẩn khác để đảm bảo thiết bị IoT an toàn và bảo mật.

*

* *

Công nghệ IoT mang đến nhiều lợi ích trong các lĩnh vực như đô thị thông minh, y tế, nông nghiệp, sản xuất… Tuy nhiên, sự phát triển nhanh chóng này đi kèm với nguy cơ an ninh mạng ngày càng cao. Các cuộc tấn công DDoS, botnet và lỗ hổng bảo mật trong thiết bị IoT đe dọa đến tính bảo mật của dữ liệu và hệ thống. Để giải quyết vấn đề này, việc đầu tư vào các giải pháp bảo mật tiên tiến và tuân thủ các tiêu chuẩn quốc tế là cực kỳ cần thiết. Điều này sẽ giúp tăng cường sự tin tưởng và đảm bảo an toàn cho hệ thống IoT trong tương lai ✍

TÀI LIỆU THAM KHẢO

[1] A.A. Kamaris (2023), *Cyber Security in Internet of Things*, Master of Science in Law & Informatics, University of Macedonia, Democritus University of Thrace, https://dspace.lib.uom.gr/bitstream/2159/28688/1/KamarisAthanasiosMsc2023.pdf, truy cập ngày 19/06/2024.

[2] M. Willett (2022), "The cyber dimension of the Russia-Ukraine war", *Survival*, **64(5)**, pp.7-26, DOI: 10.1080/00396338.2022.2126193.

[3] B. Briggs (2019), "Hackers hit Norsk Hydro with ransomware. The company responded with transparency", *Microsoft*, https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency, truy cập ngày 19/06/2024.

[4] S. Peng (2018), "The real reason behind the TSMC cyber attack", *CommonWealth Magazine*, https://english.cw.com.tw/article/article.action?id=2194, truy cập ngày 19/06/ 2024.

[5] J.E.M. Díaz (2020), "Internet of things and distributed denial of service as risk factors in information security", *Bioethics in Medicine and Society*, IntechOpen, DOI: 10.5772/intechopen.94516.

[6] G. Thamilarasu, S. Chawla (2019), "Towards deep-learning-driven intrusion detection for the internet of things", *Sensors*, **19(9)**, DOI: 10.3390/s19091977.