An ninh trong IoT

>ThS. ĐÀO MẠNH TÚ, TS. NGUYỄN CHIẾN TRINH, ThS. TRỊNH HỒNG HẢI

Mạng vạn vật (Internet of Things - IoT) là một công nghệ tiên tiến mang lại nhiều lợi ích cho người dùng. Trong tương lai, mô hình IoT sẽ liên quan đến hàng tỷ thiết bị thông minh với khả năng xử lý, cảm biến và kết nối Internet. Tuy nhiên, vấn đề bảo mật và riêng tư là một thách thức lớn đối với IoT. Một hệ thống IoT nói chung được chia làm 3 lớp chính là: nhận thức, vận chuyển và ứng dụng; mỗi lớp có những thách thức an ninh riêng. Bài báo phân tích những mối đe dọa an ninh chính của IoT trên cả 3 lớp, các hình thức tấn công phổ biến trên các lớp, mô hình bảo mật CIA và những yêu cầu đối với các giải pháp an ninh trên IoT.

Vấn đề an ninh trong IoT đang tồn tại nhiều thách thức, bởi việc thiếu các tiêu chuẩn chuyên biệt, các thiết bị có nguồn năng lượng hạn chế và công nghệ không đồng nhất, ngoài ra, các thiết bị IoT tồn tại nhiều lỗ hổng. Trên thực tế, vào cuối năm 2016, đã có các cuộc tấn công DDoS vào các nhà cung cấp DNS Dyn (hỗ trợ các nền tảng và dịch vụ Internet quan trọng như PayPal, Twitter, VISA...) thông qua mạng botnet khiến cho một số lượng lớn các thiết bị IoT dễ bị tổn thương (như máy in, camera IP, ...) đã bị nhiễm phần mềm độc hại Mirai. Cũng trong thời gian này, các nhà nghiên cứu đã phát hiện một lỗ hổng trong giao thức Zigbee, và thử nghiệm việc sử dụng máy bay không người lái tấn công một bộ bóng đèn thông minh Philip trong một tháp văn phòng, lây nhiễm các bóng đèn bằng 1 loại virus cho phép kẻ tấn công bật tắt đèn thành tin nhắn SOS bằng mã Morse, hơn thế nữa, phần mềm độc hại này còn có thể lây lan như một mầm bệnh giữa các thiết bị lân cận.

CÁC MỐI ĐE DỌA ĐỐI VỚI HỆ THỐNG IoT

Một hệ thống IoT nói chung có thể được mô tả đầy đủ bằng 3 lớp chính: Nhận thức, vận chuyển và ứng dụng. Mỗi lớp hệ thống có những công nghệ cụ thể cùng với những vấn đề an ninh riêng, như được thể hiện trong Bảng 1. Trên thực tế, các vấn đề an ninh của mỗi lớp được phân tích riêng để tìm kiếm các giải pháp mới và khả thi.

Lớp nhận thức

Lớp đầu tiên liên quan đến cảm biến vật lý IoT làm nhiệm vụ thu thập và xử lý dữ liệu, sử dụng các công nghệ khác nhau như: nhận dạng tần số vô tuyến RFID (Radio Frequency Identification), WSN (mạng cảm biến không dây), mạng cảm biến nhận dạng tần số vô tuyến RSN (RFID Sensor Network) và GPS. Lớp này gồm các cảm biến và cơ cấu kích động (actuators) thực hiện các phép đo khác nhau (nhiệt độ, gia tốc, độ ẩm...) và các chức năng như truy vấn vị trí, điều khiển từ xa. Do sự hạn chế của nguồn năng lượng thiết bị, cấu trúc tổ chức phân phối, các mối đe dọa an ninh chính đến từ những vấn đề sau:

- Các tấn công vật lý: Kiểu tấn công này tập trung vào phần cứng thiết bị của hệ thống IoT và kẻ tấn công phải có kết nối vật lý hoặc nằm trong hệ thống IoT để thực hiện tấn công. Một số ví dụ về kiểu tấn công này:

+ Giả mạo nút: Kẻ tấn công có thể gây thiệt hại cho nút cảm biến bằng cách thay thế toàn bộ hoặc một phần của nút, hoặc thậm chí truy cập và thay đổi các thông tin nhạy cảm như mật mã dùng chung hay bảng định tuyến.

+ Chèn mã độc hại: Kẻ tấn công chèn trực tiếp mã độc hại vào nút để giúp xâm nhập vào hệ thống IoT.

+ Mạo danh: Xác thực trong một môi trường phân tán là rất khó, điều đó cho phép các nút độc hại sử dụng giả mạo nhận dạng cho các cuộc tấn công.

- Tấn công từ chối dịch vụ DoS: Kẻ tấn công khai thác khả năng xử lý hữu hạn của các nút, làm cho chúng trở thành không khả dụng.

- Tấn công định tuyến: Các nút độc hại trung gian có thể sửa đổi đường dẫn định tuyến trong quá trình thu thập và chuyển tiếp dữ liệu.

- Các tấn công chuyển dữ liệu: Các cuộc tấn công khác nhau về tính bảo mật và tính toàn vẹn trong quá trình truyền dữ liệu (ví dụ: Sniffing, Man In The Middle).

Lớp vận chuyển

Lớp vận chuyển chủ yếu cung cấp môi trường tiếp cận cho lớp nhận thức. Mục đích của lớp này là truyền tải thông tin thu thập được từ lớp nhận thức tới các hệ thống xử lý thông tin cụ thể thông qua các mạng truyền thông hiện có, bao gồm cả mạng truy nhập (3G, Wifi, Ad Hoc) hoặc mạng lõi (Internet). Ở lớp này, các mối đe dọa an ninh chính là:

- Tấn công định tuyến: Các nút độc hại trung gian có thể sửa đổi đường dẫn định tuyến trong quá trình thu thập và chuyển tiếp dữ liệu.

- Tấn công từ chối dịch vụ DoS: Kẻ tấn công khai thác khả năng xử lý hữu hạn của các nút, làm cho chúng trở thành không khả dụng.

- Các tấn công chuyển dữ liệu: Các cuộc tấn công khác nhau về tính bảo mật và tính toàn vẹn trong quá trình truyền dữ liệu (ví dụ: Sniffing, Man In The Middle).

Lớp ứng dụng

Lớp ứng dụng cung cấp các dịch vụ thông minh chất lượng cao theo yêu cầu của khách hàng. Nhiều môi trường IoT khác nhau (như nhà máy thông minh, thành phố thông minh, chăm sóc sức khỏe thông minh) có thể được thực hiện ở lớp này. Các mối đe dọa an ninh chính của lớp này bao gồm:

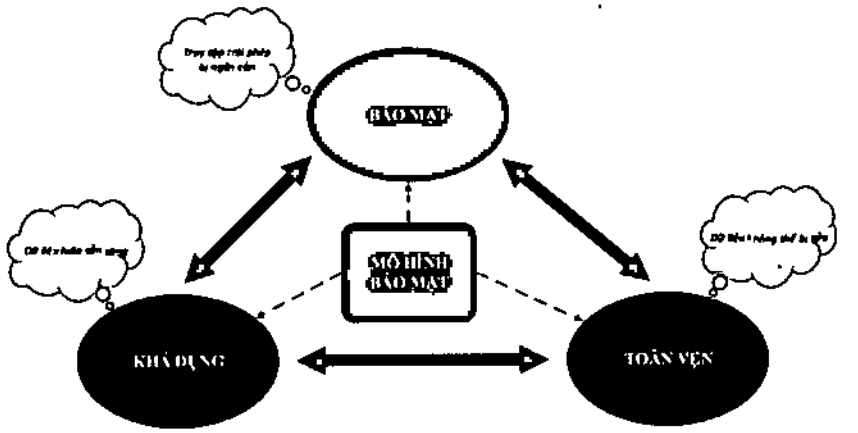
- Rò rỉ dữ liệu: Kẻ tấn công có thể dễ dàng ăn cắp dữ liệu (kể cả dữ liệu người dùng như mật khẩu cá nhân) bằng cách phát hiện các lỗ hổng của dịch vụ hoặc ứng dụng.

- Tấn công DoS: Kẻ tấn công có thể phá hủy sự khả dụng của ứng dụng hay dịch vụ.

- Chèn mã độc: Kẻ tấn công có thể tải mã độc lên phần mềm ứng dụng, khai thác các lỗ hổng được biết đến.

Bảng 1. Các đe dọa an ninh trong IoT

Lớp	Đe dọa an ninh chính
Lớp ứng dụng	Rò rỉ dữ liệu
	Tấn công DoS
	Chèn mã độc
Lớp vận chuyển	Tấn công định tuyến
	Tấn công DoS
	Tấn công chuyển dữ liệu
Lớp nhận thức	Tấn công vật lý
	Mạo danh
	Tấn công DoS
	Tấn công định tuyến
	Tấn công chuyển dữ liệu



Hình 1. Mô hình CIA

AN NINH TRONG IoT: MÔ HÌNH BẢO MẬT CIA

An ninh trong IoT thường bị bỏ quên hoặc không được quan tâm bởi các nhà sản xuất IoT. Một vài thiết bị hỗ trợ bảo mật thường sử dụng các giải pháp phần mềm như firmware signing. Tuy nhiên, sự tập trung chú ý vào các chương trình bảo vệ phần mềm thường bỏ quên phần cứng, cho phép các kiểu tấn công mới.

Trong phần này, chúng ta sẽ thảo luận về mô hình bảo mật CIA và các chính sách an ninh cho IoT.

CIA là một mô hình đặc biệt cho sự phát triển của các cơ chế an ninh, thực hiện bảo mật trên 3 lĩnh vực chính là: bảo mật dữ liệu, tính toàn vẹn và tính khả dụng.

Bảo mật dữ liệu là khả năng cung cấp sự tin tưởng cho người dùng về sự riêng tư của các thông tin nhạy cảm bằng cách sử dụng các cơ chế khác nhau khiến cho việc rò rỉ bị ngăn chặn và chỉ có thể được truy cập bởi người dùng. Tính bảo mật dữ liệu thường được hỗ trợ qua các cơ chế khác nhau như mã hóa dữ liệu hoặc điều khiển truy nhập.

Tính toàn vẹn dữ liệu đề cập đến việc bảo vệ thông tin trước tội phạm mạng hoặc sự can thiệp từ bên ngoài trong quá trình truyền dữ liệu thông qua một số phương pháp phổ biến, như thuật toán toàn vẹn dữ liệu hay ngăn ngừa sự thay đổi dữ liệu.

Tính khả dụng của dữ liệu đảm bảo việc truy cập thông tin không chỉ trong các điều kiện bình thường mà còn trong những điều kiện đặc biệt như khi xảy ra các cuộc tấn công từ chối dịch vụ DoS. Các cơ chế phổ biến bảo vệ tính khả dụng là: tường lửa, hệ thống phát hiện xâm nhập (IDS).

YÊU CẦU ĐỐI VỚI GIẢI PHÁP BẢO MẬT TRONG IoT

Theo mô hình an ninh CIA, giải pháp bảo mật phải được phát triển ở các lớp khác nhau. Chính sách bảo mật trong mỗi lớp của IoT phải xem xét các vấn đề cơ bản sau:

Bảo mật phần cứng: Sử dụng bộ xử lý mã hóa hoặc công nghệ chống giả mạo (như bảo vệ chip hoặc bộ nhớ, tự hủy v.v...).

Hệ thống điều khiển truy cập và xác thực: Ngăn chặn truy cập các nút cảm biến hoặc ứng dụng từ những người dùng trái phép.

Cơ chế mã hóa dữ liệu: Được đảm bảo bởi các thuật toán mã hóa đối xứng và bất đối xứng, được sử dụng trong suốt quá trình truyền nhận và lưu trữ dữ liệu.

Định tuyến an toàn: Để đảm bảo phát hiện đường đi chính xác, cũng như xây dựng và duy trì đích đến, ngay cả khi các mối đe dọa và các cuộc tấn công mạng xảy ra.

Đánh giá rủi ro: Để khám phá những mối đe dọa hệ thống mới, ngăn ngừa các vi phạm an ninh và xác định chiến lược an ninh.

Hệ thống phát hiện xâm nhập IDS: Phát hiện các xâm nhập trái phép vào hệ thống. Nó cũng hữu ích trong việc phát hiện và ngăn ngừa các cuộc tấn công DDoS.

Giải pháp chống phần mềm độc hại: Phát hiện và ngăn chặn cập nhật mã độc hại vào firmware hoặc vào dịch vụ và ứng dụng của thiết bị.

Tường lửa: Ngăn chặn các máy chủ trái phép.

Hệ thống quản lý độ tin cậy: Đảm bảo các mục tiêu an ninh được thực hiện và các giải pháp bảo mật được triển khai thành công. Cần đảm bảo sự tin cậy trong mối quan hệ giữa các thiết bị IoT hoặc giữa các thiết bị này với người dùng.

KẾT LUẬN

Mạng vạn vật IoT là một công nghệ tiên tiến mang lại nhiều tiện ích cho con người. Nhờ có IoT, chúng ta có thể điều khiển và giám sát các đồ gia dụng từ xa (Công nghệ nhà thông minh), được chăm sóc sức khỏe thông minh (Smart Healthcare) và nhiều lợi ích khác nữa. Bên cạnh những điều tuyệt vời mà IoT đem lại, mạng vạn vật cũng đặt ra những thách thức an ninh mới do cấu trúc linh động, dễ bị tấn công, thiếu nguồn năng lượng và thiếu khả năng tính toán tại các thiết bị trong mạng... Đây sẽ là vấn đề trọng tâm cần giải quyết của các nhà sản xuất cũng như các nhà nghiên cứu IoT trong những năm tới.❖

Tài liệu tham khảo

[1] MARIO FRUSTACI, PASQUALE PACE, GIANLUCA ALOI, GIANCARLO FORTINO DIMES (2017), "Evaluating critical security issues of the IoT world: Present and Future challenges", IEEE Internet of Things Journal

[2] G. FORTINO, AND P. TRUNFIO (2014), "Internet of Things Based on Smart Objects, Technology, Middleware and Applications", Springer.

[3] VALERIY G. SEMIN, ARTEM S. KABANOV, ALEXEI B.LOS, "Problems of Information Security Technology the Internet of Things"

[4] ADITYA PARASHAR, SACHIN RISHISHWAR, "Security Challenges In IoT", 3rd International Conference an Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB 17)