ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN TRONG KỶ NGUYÊN INTERNET VẠN VẬT

Nguyễn Linh Giang
Trường Đại học Bách khoa Hà Nội

Internet of things (IoT) hay Internet vạn vật đang mở ra một cuộc cách mạng trong việc giao tiếp giữa con người với đồ vật và giữa các đồ vật với nhau. Tuy nhiên, khi cuộc sống kết nối ngày càng phát triển và trở nên phong phú hơn thì nhu cầu về một mô hình an toàn, an ninh thông tin mạnh mẽ cũng trở nên cấp thiết hơn bao giờ hết. Để có thể khai thác được những tiềm năng, lợi ích to lớn mà IoT mang lại, còn nhiều vấn đề cần phải giải quyết, trong đó có bài toán về an toàn thông tin cho các thiết bị và hệ thống IoT.

Tổng quan về IoT

IoT là một kịch bản của thế giới, khi mà mỗi đồ vật, con người được cung cấp một định danh của riêng mình, và tất cả có khả năng truyền tải, trao đổi thông tin, dữ liệu qua một mạng duy nhất mà không cần đến sự tương tác trực tiếp giữa người với người, hay người với máy tính. IoT đã phát triển từ sự hội tụ của công nghệ không dây, công nghệ vi mạch và Internet. Hiểu một cách đơn giản, IoT là một tập hợp các thiết bị có khả năng kết nối với nhau, với Internet và với thế giới bên ngoài để thực hiện một công việc nào đó.

Trước xu thế bùng nổ như hiện nay, có rất nhiều hướng triển khai ứng dụng IoT. Từ việc kết nối các thiết bị gần gũi với cuộc sống thường ngày như: ổ điện bảo vệ trẻ em được trang bị các cảm biến để phân biệt phích cắm với các vật khác, chỉ phát điện khi nhận phích cắm, bất cứ thứ gì khác đưa vào cũng vô tác dụng; thiết bị theo dõi sức khỏe dạng đeo như các vòng tay giúp theo dõi việc tập luyện, theo dõi giấc ngủ và đặt giờ báo thức trên smartphone vào thời điểm mà nó cho là phù hợp nhất dựa trên chu kỳ ngủ tự nhiên của cơ thể; đồ gia dụng thông minh giúp bạn kiểm soát đồ gia dụng trong nhà, chẳng hạn người dùng lò vi sóng CombiSteam của Electrolux có thể bật lò, điều chỉnh nhiệt độ, thời gian và quan sát thức ăn được nấu chín thông qua một camera ngoại vi, các món đồ nhỏ hơn như máy pha café Wi-Fi của Smarter lại cho phép bạn pha cafe khi đang ở trên giường... Đến các ứng dụng ở tầm cao hơn như: xe hơi thông minh, tòa nhà thông minh, giao thông thông minh, thành phố thông minh... Dự báo, IoT sẽ kéo theo sự ra đời của thị trường thiết bị lớn nhất trên thế giới. Ước tính đến năm 2020, thị trường này sẽ gấp đôi quy mô thị trường smartphone, PC, tablet, xe hơi kết nối và thị trường các thiết bị đeo bên người cộng lại, với khoảng 50 tỷ thiết bị sẽ được kết nối. IoT sẽ mang lại 4 nghìn tỷ USD giá trị gia tăng cho nền kinh tế toàn cầu vào năm 2020, bao gồm phần cứng, phần mềm, chi phí lắp đặt, dịch vụ quản lý.

Tuy nhiên, IoT đang thiếu một bộ tiêu chuẩn và nền tảng công nghệ chung, vì thế đang hạn chế sự tương thích và tiện dụng. Hiện có rất ít tiêu chuẩn (hay nguyên tắc) cần thiết khi sử dụng một thiết bị IoT. Các nhóm liên quan trên toàn cầu như các ngành công nghiệp, công nghệ và các công ty điện tử, viễn thông đang nỗ lực tiêu chuẩn hóa IoT và giải quyết những quan ngại trong vấn đề an ninh, bảo mật. IoT có sự khác biệt lớn so với Internet truyền thống trong cách triển khai. Rất nhiều mạng trong IoT là mạng tiêu thụ năng lượng và hao tổn thấp (Low-power Lossy Networks - LLN), một số khác được triển khai theo mô hình mạng động ở mức cao, tùy thuộc vào từng ứng dụng (mạng những thiết bị giao thông, mạng những thiết bị y tế...). Mạng LLN có sự hạn chế về năng lượng, bộ nhớ và khả năng tính toán, thường có xác suất mất gói dữ liệu ở mức cao và được triển khai dưới dạng mạng lưới bao gồm nhiều nút (với mỗi nút là một thiết bị). Hầu hết thiết bị trong LLN là di động hoặc có gắn cảm biến, vì vậy vấn đề đảm bảo tài nguyên và tự động hóa cần được xem xét một cách nghiêm túc do trước đây những vấn đề này chưa được đề cập đến trong các chuẩn của hạ tầng mạng Internet truyền thống.

Một số hình thức tấn công trong IoT

Để có thể kiểm thử và nhận biết được những mối đe dọa về an toàn và các cuộc tấn công vào IoT, dưới đây xin đưa ra các hình thức tấn công vào hệ thống này:

- Tấn công lớp vật lý: trên đường truyền giữa 2 nút trong IoT, dễ dàng xảy ra những tấn công chặn bắt luồng dữ liệu. Những cuộc tấn công này có thể khai thác được những dữ liệu mật,

khóa... từ thiết bị. Dựa vào đó, kẻ tấn công có thể khởi động lại thiết bị khi cần. Nếu kẻ tấn công chặn bắt được khóa riêng thì chỉ làm tổn thương một nút mạng, nhưng nếu là khóa chung thì tấn công này có thể ảnh hưởng tới toàn bộ hệ thống. IoT cũng có thể phải đối mặt với các cuộc tấn công từ chối dịch vụ từ lớp vật lý làm tắc nghẽn mạng, cản trở thiết bị gây ra mất kết nối.

- Tấn công lỗi xác thực: là tấn công mạo danh có thể dẫn tới một loạt các tấn công khác như: cung cấp các thông tin điều khiển sai, kiểm soát nút mạng hoặc ảnh hưởng tới truyền thông trên toàn mạng. Một nút mạng giả mạo hình thành khi tấn công giả mạo vào một nút hợp pháp thành công. Khi có nhiều nút giả mạo có thể thực hiện cuộc tấn công trên toàn mạng bằng những nút này.

- Tấn công tiêu hao tài nguyên nút: xảy ra khi kẻ tấn công liên tục xâm nhập vào mạng, làm tràn bộ nhớ lưu trữ của nút mạng và còn có thể ảnh hưởng xuống nút phía dưới của mạng, gây tiêu hao tài nguyên mạng.

- Tấn công tính bí mật: diễn ra tại tầng mạng nhằm mục đích dò tìm những thông tin định tuyến hoặc dữ liệu trao đổi định tuyến. Cuộc tấn công này xảy ra khi thực thể định tuyến để lộ thông tin trong khi kết nối với một thực thể định tuyến ngoài mạng do lỗi cấu hình hoặc một cuộc tấn công vào điểm yếu của thực thể định tuyến. Việc truyền thông giữa các nút nên theo phương thức ngang hàng (peer-to-peer) để đảm bảo không có nút nào gửi thông tin tới bên nhận chưa được biết. Những biện pháp trên không thể ngăn chặn được hết các cuộc tấn công dò tìm thông tin định tuyến sơ hở, nhưng có thể hạn chế được chúng. Để thành công thì các cuộc tấn công này phải làm cho các nút tổn thương hoạt động nhiều hơn, nhằm làm lộ, lọt các thông tin định tuyến.

- Tấn công nghe lén thụ động: nghe lén dữ liệu được truyền đi giữa các nút bằng cách phân tích lưu lượng truyền thông. Qua đó, kẻ tấn công có thể tìm hiểu được về hệ thống mạng. Trong IoT, với nền tảng là mạng LLN, có mức năng lượng và tiêu hao thấp, thì thuật toán mật mã thường được dùng là AES ở chế độ CCM (Counter with CBC-MAC) [RFC6550]. CCM kết hợp bản mã ở chế độ đếm (Counter mode) và mã xác thực thông báo xích mã khối (CBC-MAC) để xác thực. Ví dụ, ZigBee chỉ rõ việc sử dụng CCM, PANA và EAP-TLS trong việc quản lý khóa. Việc sử dụng AES-CCM sẽ an toàn đối với hầu hết các cuộc tấn công vét cạn. Mạng IoT sử dụng mã hóa an toàn với tấn công nghe lén nhưng lại tồn tại nhiều điểm yếu từ những tấn công khai thác nút bị tổn thương.

- Tấn công tính toàn vẹn: sửa đổi bất hợp pháp thông điệp trên đường truyền hoặc dữ liệu lưu trữ. Những tấn công này có thể dễ dàng được ngăn chặn bằng cách tăng thêm quyền kiểm soát truy cập với dữ liệu lưu trữ và cài đặt các dịch vụ toàn vẹn dữ liệu trên đường truyền cho thông điệp.

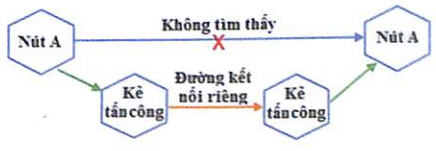
- Tấn công Overclaiming và Misclaiming: nhằm mục đích thay đổi mô hình logic của mạng và các thông tin định tuyến bằng cách tạo ra các tuyến đường sai. Tấn công này có thể chống được bằng cách xác định các tuyến đường xấu thông qua các gói tin cũ và thiết kế mô hình mạng phân vùng hạn chế quyền truy cập.

- Tấn công dùng lại các thông tin định tuyến: xảy ra khi kẻ tấn công ghi lại những thông điệp đã được gửi đi trên mạng và gửi chúng quay trở lại nhằm làm gián đoạn hoạt động của mạng. Giao thức định tuyến cho mạng LLN là RPL (RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks) trên nền IPv6 được IETF thiết kế để chống lại loại tấn công này. Trong RPL, thông điệp sẽ có nhiều phiên bản và những thông điệp phiên bản cũ sẽ bị loại bỏ mà không ảnh hưởng tới hoạt động định tuyến bình thường.

- Tấn công tính sẵn sàng: là những cuộc tấn công chuyển tiếp lựa chọn mục tiêu gây ảnh hưởng tới các tuyến đường định tuyến, nhằm mục đích làm gián đoạn truyền thông trong mạng. Trong hình 1, có thể thấy một nút bị tổn thương có thể tạo bộ lọc chọn ngẫu nhiên các gói tin đi qua gây rối loạn trong mạng. Nếu như nút mạng loại bỏ tất cả các gói tin nhận được thì được gọi là cuộc tấn công hố đen. Có 2 biện pháp ngăn chặn tấn công này là định tuyến đa điểm trên các tuyến đường tách biệt không giao nhau hoặc mỗi nút phải có cơ chế lựa chọn ngẫu nhiên điểm đến tiếp theo trong tập hợp những điểm đến. Phương pháp định tuyến đa đường tốn nhiều năng lượng nên không được sử dụng trong IoT.

Hình 1: tấn công chuyển tiếp lựa chọn

- Tấn công Wormhole: là khi hai nút bị tổn thương hoặc nhiễm mã độc, nên ngộ nhận rằng có một tuyến đường ngắn và tốt hơn cho chúng. Một cuộc tấn công Wormhole thuần túy rất khó phát hiện, vì nó không ảnh hưởng tới dữ liệu cũng như lưu lượng truyền thông. Trong trường hợp xấu, tấn công Wormhole sẽ khiến thiết bị mạng tính toán lại các tuyến đường. Khi kết hợp Wormhole với tấn công khác như tấn công chuyển tiếp lựa chọn mục tiêu có thể làm gián đoạn truyền thông mạng (hình 2).



Hình 2: tấn công Wormhole

- Tấn công Sinkhole: sử dụng một nút tổn thương để đánh lừa về tuyến đường tốt, nhằm thu hút lưu lượng

mạng truy cập đến. Tấn công này chỉ có thể thực hiện bởi một nút bên trong mạng. Nếu Sinkhole kết hợp với tấn công chuyển tiếp có lựa chọn, thì một phần mạng có thể bị vô hiệu hóa. Biện pháp để ngăn chặn tấn công này là, cần phải có một ngưỡng nhất định tiếp nhận lưu lượng mạng trong mỗi nút, hoặc cơ chế lựa chọn điểm đến kế tiếp cho thông điệp trong một tập hợp các điểm đến có thể.

- Tấn công giả mạo gói ACK và HELLO Flood của giao thức TCP trong IoT có thể được thực hiện bởi những cách thức khác nhau nhằm mục đích khiến cho các nút tin rằng tồn tại những tuyến đường mà thực tế không có. Cách tối ưu để chống lại những cuộc tấn công này là thông qua kết nối hai hướng trong đó có sự điều khiển xác nhận kết nối hợp lệ ở lớp liên kết dữ liệu.

Đề xuất một số giải pháp an toàn thông tin trong IoT

Từ những phân tích nêu trên, xin đưa ra một số giải pháp đảm bảo an toàn trong triển khai IoT:

Thứ nhất, thiết lập kiến trúc an toàn trong IoT trên cả 4 lớp: để thiết lập kiến trúc an ninh trong IoT thì yêu cầu an ninh của mỗi lớp phải đảm bảo như sau: lớp cảm quan (Perceptual Layer) phải chứng thực tại nút đầu tiên thông qua các ký tự được mã hóa, điều này rất cần thiết để ngăn chặn truy cập bất hợp pháp vào mode, giúp bảo mật khi truyền tải thông tin; lớp mạng (Network Layer) phải có cơ chế chứng thực nhận dạng nhằm ngăn chặn các nút bất hợp pháp, là tiền đề cho các cơ chế an toàn, bảo mật (ví dụ, để chống lại tấn công từ chối dịch vụ DDoS cần có Anti-DDoS nhằm ngăn chặn các nút bất hợp pháp); lớp hỗ trợ (Support Layer) cần nhiều hệ thống bảo mật như an ninh điện toán đám mây, điện toán đa nhóm... gần như tất cả các thuật toán mã hóa mạnh và giao thức mã hóa, kỹ thuật bảo mật, diệt virus đều tập trung ở Layer này; lớp ứng dụng (Application Layer) cần có chứng thực và key agreement qua mạng không đồng nhất giúp bảo vệ quyền riêng tư cho người dùng, đồng thời phải nâng cao yêu cầu đảm bảo an toàn thông tin, đặc biệt là đối với password.

Thứ hai, sử dụng tốt một số kỹ thuật an ninh chủ yếu: 1) Các thuật toán mã hóa như: mã hóa đối xứng (symmetric encryption algorithm) và mã hóa bất đối xứng (asymmetric algorithm); 2) Cơ chế mã hóa, tầng mạng và tầng ứng dụng gần với nhau, nên nếu yêu cầu bảo mật cao ta sử dụng mã hóa end to end, nếu yêu cầu bảo mật thấp hơn ta sử dụng cơ chế By-hop, bởi mỗi cơ chế có những ưu nhược điểm riêng. Trong cơ chế By-hop sử dụng ở tầng mạng, mỗi thiết bị nhận được tin sẽ giải mã, xử lý và mã hóa rồi mới gửi cho thiết bị kế tiếp, còn cơ chế end to end cho tầng ứng dụng thì bên gửi sẽ mã hóa tin, truyền qua các thiết bị kế tiếp, tin được mã hóa chỉ được giải mã khi nó đến được bên nhận.

Thứ ba, đảm bảo thông tin liên lạc: trong giao thức truyền thông có một số giải pháp được thiết lập, các giải pháp này có thể cung cấp tính toàn vẹn, tính xác thực, bảo mật cho thông tin liên lạc. Ví dụ: TLS/SSL hoặc IPSec: 1) TLS/SSL được thiết kế để mã hóa các liên kết trong quá trình truyền tải, giao thức Secure Socket Layer (SSL) cung cấp khả năng bảo mật thông tin, xác thực và toàn vẹn dữ liệu đến người dùng. Tổ chức IETF (Internet Engineering Task Force) đã chuẩn hóa SSL và đặt lại tên là TLS (Transport Layer Security), TLS được coi như một phiên bản mới của SSL; 2) IPSec (IP Security) được thiết kế để bảo vệ an ninh của các lớp mạng, nó có thể cung cấp tính toàn vẹn, tính xác thực và bảo mật trong lớp. IPSec bao gồm một hệ thống các giao thức để bảo mật quá trình truyền thông tin trên nền tảng Internet Protocol (IP), người dùng có thể sử dụng để mã hóa dữ liệu trước khi truyền chúng qua mạng, do đó không ai có thể nghe trộm trên đường truyền.

Thứ tư, bảo vệ dữ liệu cảm biến: vấn đề chính của cảm biến là sự riêng tư. Phần lớn thời gian con người không ý thức được hết các cảm biến xung quanh họ, nên cần thiết lập một số điều chỉnh để đảm bảo sự riêng tư. Cụ thể, một kẻ tấn công có thể đặt bộ cảm biến riêng của hắn tác động qua lại với chúng ta, nhờ đó chúng đánh cắp được những thông tin, dữ liệu mà chúng muốn.

Thứ năm, nâng cao ý thức cho người sử dụng về an toàn thông tin, an toàn dữ liệu: sẵn sàng, chủ động trong việc đảm bảo an toàn thông tin cá nhân của mình thông qua một số nguyên tắc chung nhất như: dùng mật khẩu siêu mạnh và tránh lặp lại; xác thực 2 bước trong mọi trường hợp cụ thể, dùng thẻ RSA Token (tạo mã code và mã pin); cập nhật bản nâng cấp phần mềm thường xuyên để vá các lỗ hổng bảo mật; an toàn thông tin cũng như quyền riêng tư trên mạng xã hội; dùng phần mềm bảo vệ các thiết bị di động; sử dụng hệ thống lưu trữ đám mây để lưu dữ liệu cá nhân cần độ bảo mật cao...

Để đảm bảo triển khai hiệu quả IoT thì các thách thức về công nghệ là không đáng kể so với vấn đề an toàn, an ninh thông tin. Một sự kiểm soát chặt chẽ ngay từ những thiết lập, triển khai ban đầu sẽ đảm bảo sự tồn tại an toàn của thế giới vạn vật kết nối. Do vậy, ngay từ lúc này cần xây dựng các chính sách, quy trình về an toàn thông tin để đảm bảo sự phát triển khi đưa vào vận hành kiến trúc mới, kiến trúc IoT, giúp tất cả các tổ chức, cá nhân sẽ mạnh dạn tham gia với tư cách những doanh nghiệp khởi nghiệp hoặc những người chơi trong không gian được bảo mật an toàn