Chương I. Tổng quan về An toàn thông tin và An ninh mạng

1. Bối cảnh thực tế

Lịch sử:

Gậy mật mã của người Hy lạp cổ:

C T B T C G	Ứ Ô I Ấ Ô	U I N N

Bản mã trên băng giấy da: CTBTCGỨÔỊẤÔUI NN

Bản rõ đọc được sau khi quấn vào gậy: CỨUTÔIBỊ TẤNCÔNG

Máy Enigma

Ngày nay: chiến tranh thông tin, chiến tranh mạng chi phí rất thấp, hiệu quả cao và tức thời, dễ dàng che giấu nguồn gốc, đã trở thành một phần của chiến tranh hiện đại.

Quốc tế

Năm 2009, Mỹ thành lập Bộ tư lệnh tác chiến mạng

Năm 2014, Australia lập ra Trung tâm An ninh mạng quốc gia

Tháng 6/2016, Tổng thư ký NATO – Jens Stoltenberg phát biểu coi không gian mạng là mặt trận tác chiến mới.

Năm 2017, bộ trưởng Quốc phòng Singapore thông báo thành lập Bộ chỉ huy an ninh mạng

Năm 2018, NATO đã thành lập Trung tâm tác chiến không gian mạng (Cyberspace Operation Centre), một phần của cấu trúc chỉ huy NATO.

Tháng 8/2018, Tổng thống Hoa Kỳ Donald John Trump đã ký sắc lệnh cho phép quân đội Hoa Kỳ triển khai vũ khí mạng tiên tiến mà không bị Bộ Ngoại giao và Cộng đồng tình báo nước này ngăn cản.

Các nước APEC (Diễn đàn hợp tác kinh tế châu Á-Thái Bình Dương) đã ký Công ước về tội phạm mạng và thống nhất phòng chống tội phạm mạng.

Nước ta

Ngày 28 tháng 8 năm 2014, Bộ Công an công bố Quyết định thành lập Cục An ninh mạng (nay là Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao).

8/1/2018, Bộ Quốc phòng tổ chức Lễ công bố Quyết định của Thủ tướng về việc thành lập Bộ tư lệnh Tác chiến không gian mạng.

Dân sự: rất nhiều hình thức lừa đảo, tấn công mạng khiến cho người dùng phải có hiểu biết để áp dụng những hình thức bảo mật để tự bảo vệ an toàn thông tin của mình, người quản trị mạng phải được đào tạo để bảo vệ được hệ thống thông tin và những giao dịch của cơ quan.

==========

An ninh thông tin từ lâu đã đóng vai trò không nhỏ trong quân sự và trong những lĩnh vực hoạt động xã hội. Việc giải mã các mật mã và đảm bảo an toàn trong truyền thông đã được coi là các cuộc chiến phức tạp và kéo dài.

Có 3 nguyên nhân làm cho các vấn đề an ninh truyền thông ngày càng trở nên nghiêm trọng:

- Liên kết giữa các máy tính và các mạng gia tăng không ngừng → dễ dàng bị truy cập trái phép.
- Các thông tin truyền trên mạng ngày càng nhiều.
- Kỹ thuật tấn công mạng máy tính ngày càng trở nên dễ dàng, bất kỳ người hiếu kỳ nào cũng có thể sở hữu các công nghệ tinh vi và trở thành kẻ tấn công mạng.

Các vụ đột nhập mạng thường có phạm vi tác động rất rộng và gây hậu quả nghiêm trọng, mất nhiều công sức và tiền bạc để khắc phục

- Sâu mạng (Internet Worm) được thả lên mạng Internet vào tháng 11 năm 1988 bởi sinh viên Robert Morris Jr của trường đại học Cornell. Con sâu mạng này là một chương trình đột nhập tự nhân bản. Nó tiến hành quét toàn mạng Internet để lây lan và khống chế tối thiểu 1200 (có thể lên tới 6000) máy tính chạy hệ điều hành Unix.

Câu hỏi:

Hành động dùng email cá nhân của bà Clinton là sai luật lưu trữ liên bang, đó là kết luận ngày 25/5/2016 của Tổng thanh tra Bộ Ngoại giao Mỹ về trường hợp bà Clinton sử dụng email cá nhân cho công việc trong thời gian làm Ngoại trưởng Mỹ.

Vì sao quy định không được dùng?

Và vì sao người ta vẫn muốn dùng?

Nước ta có quy định tương tự hay không?

2. Khái niệm an ninh mạng

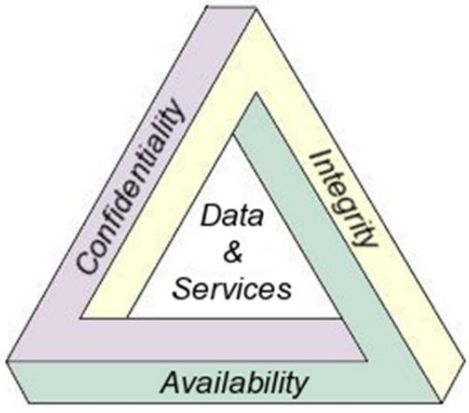
Theo Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ NIST (National Institute of Standards and Technology):

- **An toàn thông tin/ An ninh thông tin** (Information Security) là các biện pháp nhằm bảo đảm an toàn mạng và an toàn thông tin trong quá trình khởi tạo, truyền và lưu trữ dữ liệu trên máy tính cá nhân/server và trên mạng.
- **An ninh máy tính** (Computer Security) là sự bảo vệ đối với hệ thống thông tin nhằm đảm bảo tính toàn vẹn, tính sẵn sàng và tính bí mật của hệ thống thông tin bao gồm phần cứng, phần mềm, firmware, thông tin, dữ liệu và viễn thông.
- **An ninh mạng** (Network Security, Cyber Security) là tổng thể các giải pháp về mặt tổ chức và kỹ thuật nhằm ngăn cản mọi nguy cơ tổn hại đến mạng, bảo vệ dữ liệu truyền trên một tập hợp các mạng có kết nối với nhau.

3. Các yếu tố đảm bảo an toàn thông tin

Bộ ba CIA: **Confidentiality** (tính Bí mật), **Integrity** (tính Toàn vẹn), **Availability** (tính Sẵn sàng).

Bộ ba CIA cung cấp một công cụ đo (tiêu chuẩn để đánh giá) đối với mức độ an ninh của máy tính và mạng..



➢ **Tính bí mật (Confidentially):** Đảm bảo dữ liệu không bị lộ, không bị xem bởi những những người không được cấp phép.

Ví dụ về công cụ để đảm bảo tính bí mật là User ID + Password, kiểm tra sinh học ...

Tính bí mật rất cần thiết, nhưng chưa đủ.

- **Tính toàn vẹn (Integrity)**: đảm bảo thông tin không bị thay đổi so với bản gốc khi được tạo ra; chỉ được chỉnh sửa bởi người có thẩm quyền; Tính toàn vẹn đảm bảo sự nhất quán, chính xác và đáng tin cậy của dữ liệu trong suốt thời gian tồn tại của nó; đảm bảo dữ liệu không bị sửa đổi trái phép hoặc bởi sự cố trong quá trình truyền thông.

  Tính toàn vẹn bao gồm 2 phần:

  - **Tính toàn vẹn dữ liệu** (Data Integrity): Dữ liệu không bị biến đổi, mất mát trong khi lưu trữ hay truyền tải.
  - **Tính toàn vẹn của hệ thống** (System Integrity): đảm bảo rằng một hệ thống thực hiện các chức năng một cách đúng đắn, không thực hiện các thao tác tự do, trái phép.

  Việc đảm bảo tính toàn vẹn dữ liệu nhằm ba mục đích chính:

  - Ngăn cản việc làm biến đổi nội dung thông tin bởi những người sử dụng không được phép hoặc bởi các sự cố như nhiễu điện từ trên đường truyền.
  - Ngăn cản việc làm biến đổi nội dung thông tin một cách không chủ tâm của những người sử dụng hợp lệ.
  - Duy trì sự toàn vẹn dữ liệu cả trong nội bộ và bên ngoài.

- **Tính sẵn sàng (Availability):** đảm bảo người sử dụng có thể truy cập và sử dụng bất cứ lúc nào và không bị ngắt quãng tới các thông tin của hệ thống; đảm bảo thông tin luôn sẵn sàng khi cần đến. Tính sẵn sàng phản ánh đến độ tin cậy của hệ thống.

Có nhiều tranh luận về việc mở rộng tam giác này và bổ sung thêm các yếu tố khác, như:

- **Tính chống chối bỏ** (Non-repudiation): bảo đảm người gửi và người nhận không thể chối bỏ hành động đã thực hiện. Một bên giao dịch không thể phủ nhận việc họ đã thực hiện giao dịch với các bên khác.
- **Tính xác thực (Authenticity)**: bảo đảm xác minh được định danh của người sử dụng là hợp lệ (ví dụ thông qua sử dụng một mật khẩu password) hay không; đảm bảo rằng dữ liệu, giao dịch, kết nối hoặc các văn kiện (tài liệu điện tử hoặc tài liệu in trên giấy) đều là thật; xác nhận các bên liên quan để biết họ là ai trong hệ thống; giúp chống mạo danh (spoofing).
- Sự định danh (Identification): hành động của người sử dụng khi xác nhận một sự định danh tới hệ thống, ví dụ như định danh thông qua tên (username) của cá nhân.

- Sự kiểm toán (Accountability): sự xác định các hành động hoặc hành vi của một cá nhân bên trong hệ thống và nắm chắc được trách nhiệm cá nhân hoặc các hành động của họ.
- Sự uỷ quyền (Authorization): các quyền được cấp cho một cá nhân (hoặc tiến trình) mà chúng cho phép truy cập và tài nguyên trên mạng hoặc máy tính.

4. Các nguy cơ và mối đe dọa đối với an toàn thông tin và an ninh mạng

Sự cố khách quan, thảm họa thiên nhiên

Sự cố về điện đột ngột, linh kiện điện tử bị hỏng do quá thời hạn sử dụng, động đất, cháy nổ, sét đánh, bão, lụt lội ...

Hacker (Tin tặc).

Hacker (tin tặc): kẻ thâm nhập vào mạng máy tính của người khác một cách trái phép để lấy thông tin, phá hoại dữ liệu, phá hủy chương trình.

BigData

- Là những dữ liệu lớn, thay đổi nhanh, phức tạp, không chắc chắn mà các công cụ truyền thống không xử lý được
- Là một lĩnh vực hot, thiếu nhân lực IT

Ví dụ: Hãy giải thích nhận xét: "*mỗi sản phẩm trên các website thương mại điện tử như Tiki, Lazada, Sendo… đều là Big Data*"

Những ứng dụng của Big Data trong thương mại điện tử

- Phân tích dự đoán: dự đoán khuynh hướng thị hiếu người tiêu dùng.
- Liên tục thay đổi giá để cạnh tranh bằng cách phân tích thời gian thực.

BigData khiến khối lượng dữ liệu cần bảo vệ trở nên khổng lồ với nhiều định dạng phức tạp. Mặt khác giới nghiên cứu và ứng dụng BigData đang tập trung chú ý vào việc thu thập và phân tích dữ liệu, khâu giám sát truy cập ít được quan tâm.

Những đặc trưng của Big Data: IBM định nghĩa Big Data là 4V, nay đã thành 6V:

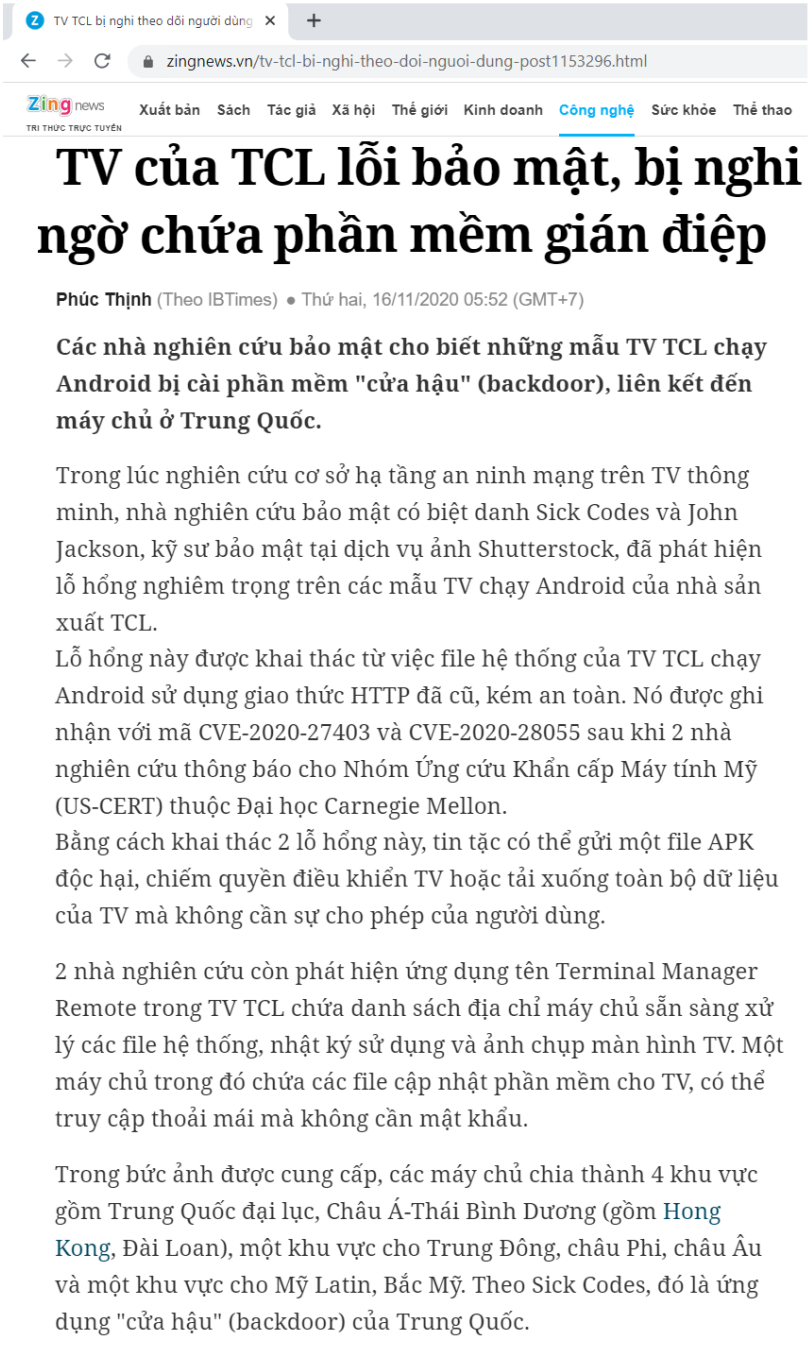
- **Volume (**Khối lượng dữ liệu lớn)**:** ít nhất hàng trăm Terabyte, thường là Petabyte, Exabyte, thậm chí lên tới Zettabyte.
- **Velocity (**Tốc độ dữ liệu được tạo ra nhanh)**:** mỗi ngày 90 triệu bức ảnh được upload lên Facebook, 500 triệu tweets cho Twitter , 0.4 triệu

giờ video được upload lên Youtube, 3.5 tỷ lượt tìm kiếm trên Google

- **Variety** (dữ liệu rất đa dạng): dữ liệu có cấu trúc (structure) như các bảng trong cơ sở dữ liệu quan hệ; dữ liệu phi cấu trúc (unstructured) như văn bản (text), dữ liệu ảnh (pictures), video, audio, …; dữ liệu bán cấu trúc (semi-structure) như file xml
    - **Variability** (tính biến thiên của dữ liệu): ví dụ: trong xử lý ngôn ngữ tự nhiên, câu "ông già đi nhanh quá" có bao nhiêu cách hiểu?
- **Veracity** (độ tin cậy của dữ liệu thấp): sự đa dạng càng lớn, tốc độ càng cao, tính biến thiên càng nhiều thì độ tin cậy càng thấp
- **Value** (có giá trị lớn). Ví dụ: Hãy tìm hiểu những vụ rò rỉ / mất trộm thông tin người dùng của Facebook, Yahoo, Google

IoT khiến cho sự riêng tư trở nên dễ bị xâm phạm. Các thiết bị IoT có thể bị khai thác, lợi dụng, những thiết bị đó thường không được bảo mật kỹ càng như máy tính.

Ví dụ 1: TCL hiện đang là tập đoàn điện tử đứng trong TOP 20 trên thế giới.



TV TCL bị nghi theo dõi người dùng

zingnews.vn/tv-tcl-bi-nghi-theo-doi-nguoi-dung-post1153296.html

Zing news TRI THỨC TRỰC TUYẾN | Xuất bản | Sách | Tác giả | Xã hội | Thế giới | Kinh doanh | Công nghệ | Sức khỏe | Thể thao

TV của TCL lỗi bảo mật, bị nghi ngờ chứa phần mềm gián điệp

Phúc Thịnh (Theo IBTimes) ● Thứ hai, 16/11/2020 05:52 (GMT+7)

Các nhà nghiên cứu bảo mật cho biết những mẫu TV TCL chạy Android bị cài phần mềm "cửa hậu" (backdoor), liên kết đến máy chủ ở Trung Quốc.

Trong lúc nghiên cứu cơ sở hạ tầng an ninh mạng trên TV thông minh, nhà nghiên cứu bảo mật có biệt danh Sick Codes và John Jackson, kỹ sư bảo mật tại dịch vụ ảnh Shutterstock, đã phát hiện lỗ hổng nghiêm trọng trên các mẫu TV chạy Android của nhà sản xuất TCL.
Lỗ hổng này được khai thác từ việc file hệ thống của TV TCL chạy Android sử dụng giao thức HTTP đã cũ, kém an toàn. Nó được ghi nhận với mã CVE-2020-27403 và CVE-2020-28055 sau khi 2 nhà nghiên cứu thông báo cho Nhóm Ứng cứu Khẩn cấp Máy tính Mỹ (US-CERT) thuộc Đại học Carnegie Mellon.
Bằng cách khai thác 2 lỗ hổng này, tin tặc có thể gửi một file APK độc hại, chiếm quyền điều khiển TV hoặc tải xuống toàn bộ dữ liệu của TV mà không cần sự cho phép của người dùng.

2 nhà nghiên cứu còn phát hiện ứng dụng tên Terminal Manager Remote trong TV TCL chứa danh sách địa chỉ máy chủ sẵn sàng xử lý các file hệ thống, nhật ký sử dụng và ảnh chụp màn hình TV. Một máy chủ trong đó chứa các file cập nhật phần mềm cho TV, có thể truy cập thoải mái mà không cần mật khẩu.

Trong bức ảnh được cung cấp, các máy chủ chia thành 4 khu vực gồm Trung Quốc đại lục, Châu Á-Thái Bình Dương (gồm Hong Kong, Đài Loan), một khu vực cho Trung Đông, châu Phi, châu Âu và một khu vực cho Mỹ Latin, Bắc Mỹ. Theo Sick Codes, đó là ứng dụng "cửa hậu" (backdoor) của Trung Quốc.

Ví dụ 2: khai thác thông tin qua ảnh vệ tinh

vnexpress.net/covid-19-co-the-xuat-hien-o-vu-han-tu-thang-8-2019-4112689.html

Covid-19 có thể xuất hiện ở Vũ Hán từ tháng 8/2019

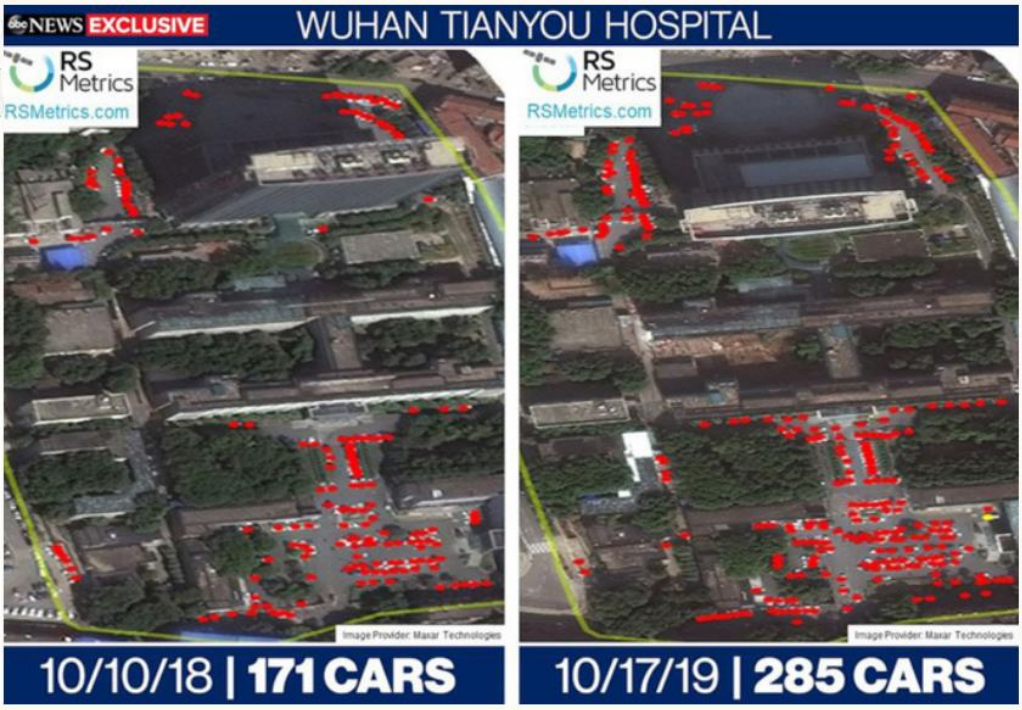
VNEXPRESS

Nghiên cứu của Trường Y, Đại học Harvard, sử dụng ảnh vệ tinh và xu hướng tìm kiếm trên mạng cho thấy Covid-19 có thể đã lây lan ở Trung Quốc từ tháng 8/2019.

Nghiên cứu mới chỉ ra số lượng ôtô trong bãi đậu xe 5 bệnh viện ở Vũ Hán từ đầu tháng 8/2019 cao đáng kể so với mùa hè và mùa thu năm trước. "Lượng xe tăng mạnh từ tháng 8/2019 và đạt đỉnh vào tháng 12/2019", nhóm nghiên cứu do giám đốc sáng tạo Bệnh viện Nhi Boston John Brownstein dẫn đầu, viết trong một bản tin được đăng trên cổng thông tin DASH của Đại học Harvard, Mỹ, hôm 8/6.

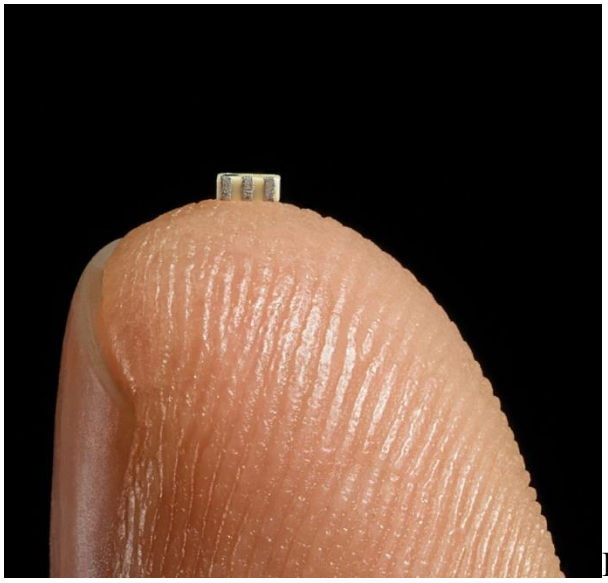
Trong ảnh vệ tinh tháng 10/2018, các nhà nghiên cứu đếm được 171 ôtô trong các bãi đậu ở Thiên Hựu, bệnh viện lớn nhất Vũ Hán. Ảnh vệ tinh một năm sau cho thấy 285 ôtô trong cùng các bãi đậu, tăng khoảng 67%, cũng như lưu lượng giao thông tăng 90% cùng thời điểm tại các bệnh viện khác ở Vũ Hán.

"Các bệnh viện riêng lẻ ghi nhận số ngày có lượng xe tương đối cao trong cả mùa thu và mùa đông 2019. Tuy nhiên, từ tháng 9 đến tháng 10/2019, 5 trong số 6 bệnh viện cho thấy lượng xe đậu trong bãi hàng ngày cao nhất trong loạt phân tích, trùng thời điểm mức độ tìm kiếm trên Baidu tăng cao đối với các từ khóa 'tiêu chảy' và 'ho'", nhóm nghiên cứu viết.



Số lượng xe trong các bãi đậu tại bệnh viện Thiên Hựu tại hai thời điểm tháng 10/2018 và tháng 10/2019. Ảnh: *ABC News*.

Ví dụ 3: cài chip nghe lén vào thiết bị tin học

 Hình.

Nguồn: https://news.zing.vn/chip-gian-diep-trung-quoc-de-doa-an-ninh-lau-nam-goc-post882306.html

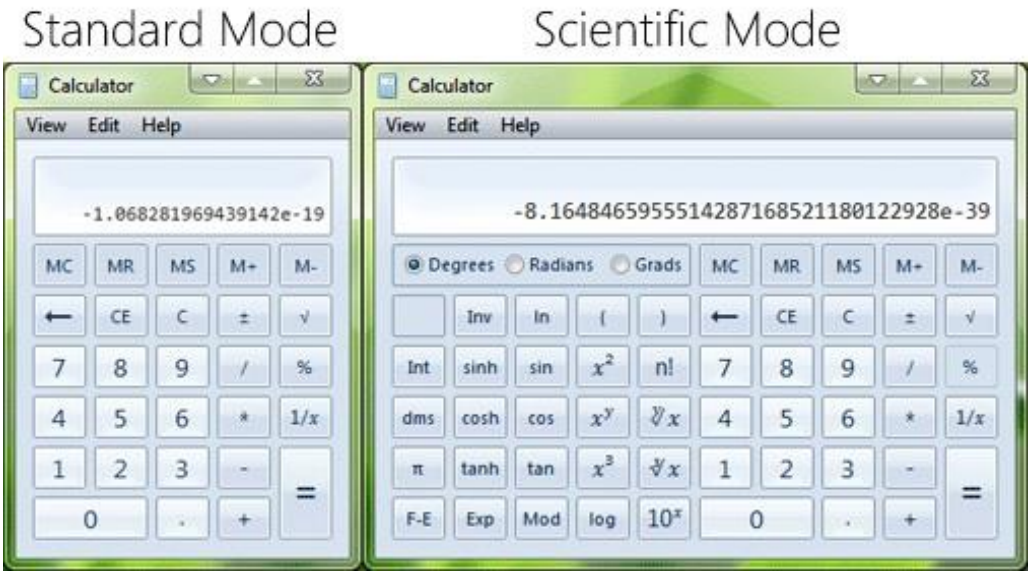
Bloomberg phát hiện Trung Quốc cài "chip hạt gạo" có backdoor lên bo mạch chủ của công ty SuperMicro để điều hướng luồng dữ liệu về server lạ.

Lỗi phần mềm. Do bị tin tặc (virus) phá hoại, hoặc do lập trình viên và người thiết kế chương trình sai lầm.

Ví dụ:

- Y2K: Year 2000 và được gọi là “lỗi thiên niên kỷ”.
- Ngày 4/6/1996 tên lửa Ariane 5 (châu Âu) trị giá 500 triệu đô la phát nổ sau khi phóng do lỗi phần mềm Integer Overflow (chuyển dữ liệu số thực 64-bit sang số nguyên có dấu 16-bit)
- YouTube phải nâng cấp bộ đếm vì Gangnam Style:
- Ngày 14/8/2003, 256 nhà máy điện không hoạt động khiến 8 tiểu bang Hoa Kỳ và Canada mất điện, ảnh hưởng tới 50 triệu người. Cơ quan PC Authority công bố nguyên nhân là lỗi phần mềm “race condition” xảy ra khi 2 thread riêng biệt của cùng một chương trình sử dụng cùng tài nguyên mà không đồng bộ đúng cách dẫn đến sụp đổ hệ thống.

Ví dụ: phần mềm Calculator của Windows: sqrt(4) -2 cho kết quả khác 0.



Lừa đảo và lấy cắp thông tin. Nhiều công ty bị lộ thông tin từ bên trong.

Cách tốt nhất để phòng tránh nguy cơ này là: phải có những chính sách bảo mật được thiết kế tốt.

Virus máy tính, mã độc.

Thường gọi tắt là virus (mã độc, malware): là phần mềm được lập trình để có khả năng:

- Tự nhân bản, lây nhiễm vào những tệp tin trong máy, thiết bị lưu trữ (đĩa cứng, đĩa mềm, USB) cắm vào máy, lây lan qua mạng
- Phá hoại hoạt động bình thường của hệ thống, lấy cắp thông tin

Có rất nhiều loại mã độc: virus, sâu máy tính, Trojan horse,… Khi đã xâm nhập vào máy nạn nhân, mã độc có thể mở cổng hậu (back door) để kẻ tấn công có thể truy cập và làm mọi việc trên máy nạn nhân; ghi lại thông tin sử dụng máy tính (thao tác bàn phím, sử dụng mạng, thông tin đăng nhập…).

Mã độc vào máy tính qua nhiều con đường: lỗ hổng phần mềm (điển hình như adobe Flash rất nhiều lỗ hổng 0-days được phát hiện, hay Java Runtime Environment thời gian gần đây cũng liên tục đưa ra bản vá bảo mật); hệ thống bị hacker điều khiển; do sử dụng phần mềm crack, phần mềm lậu (không có giấy phép sử dụng);

Cách tốt nhất để tránh nguy cơ này là luôn cập nhật phần mềm xử lý dữ liệu, hệ điều hành và phần mềm an ninh mạng, diệt virus.

Tấn công mạng

Một trong những hình thức tấn công mạng là từ chối dịch vụ: làm hệ thống không thể phục vụ người dùng bằng cách truy cập liên tục với số lượng lớn

- DoS (Denny of Service – tấn công từ chối dịch vụ): tấn công này có thể xảy ra với cả ứng dụng trực tuyến và ứng dụng offline. Với ứng dụng trực tuyến, hacker sử dụng các công cụ tấn công (tấn công Syn floods, Fin floods, Smurfs, Fraggles) trên một máy tính để tấn công vào hệ thống, khiến nó không thể xử lý được yêu cầu, hoặc làm nghẽn băng thông. Với ứng dụng offline, hacker tạo ra những dữ liệu cực lớn, hoặc các dữ liệu xấu (làm cho quá trình xử lý của ứng dụng bị ngưng trệ, treo)
- DDoS (Distributed Denny of Service – tấn công từ chối dịch vụ phân tán): các nguồn tấn công được điều khiển bởi một (một vài) server của hacker (gọi là server điều khiển), cùng tấn công vào hệ thống.

Lỗ hổng nằm trong hạn chế của con người: người quản trị mạng, người dùng mạng

(Xem Social engineering ở chương sau)

Lỗ hổng hệ thống (Vulnerable)

Lỗ hổng hệ thống là những điểm yếu trong hệ thống có thể bị khai thác, lợi dụng để xâm phạm chính sách an toàn bảo mật, đối tượng tấn công có thể khai thác để thực hiện các hành vi tấn công hệ thống. Lỗ hổng hệ thống có thể tồn tại trong hệ thống mạng hoặc trong thủ tục quản trị mạng.

- Lỗ hổng lập trình (back-door)
- Lỗ hổng hệ điều hành
- Lỗ hổng ứng dụng
- Lỗ hổng vật lý
- Lỗ hổng trong thủ tục quản lý (mật khẩu, chia sẻ)