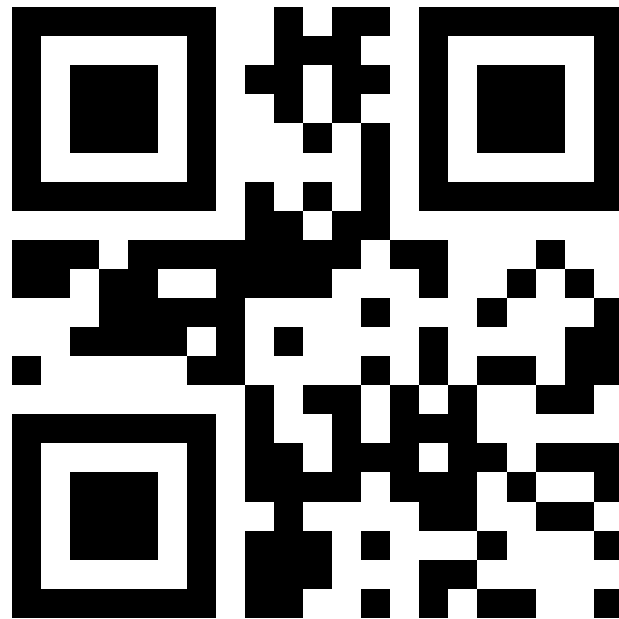


Thông tin về giảng viên

- **Họ và tên:** ThS Nguyễn Ngọc Toàn
- **Đơn vị công tác:** Khoa ANTT– Học viện ANND
- **Email:** ngoctoan.hvan@gmail.com



PHONE NUMBER



CƠ SỞ AN TOÀN THÔNG TIN

Bài 01. Tổng quan về an toàn thông tin

1

Giới thiệu học phần

2

Tình hình an toàn thông tin gần đây

3

Đối tượng an toàn thông tin

4

Khái niệm an toàn thông tin

1

Giới thiệu học phần

2

Tình hình an toàn thông tin gần đây

3

Đối tượng an toàn thông tin

4

Khái niệm an toàn thông tin

Mục tiêu học phần

❑ Học phần: Cơ sở an toàn thông tin

❑ Mục tiêu:

- Khái niệm an toàn thông tin
- Hiểm họa an toàn thông tin
- Phương pháp đảm bảo an toàn thông tin
- Phương tiện đảm bảo an toàn thông tin

Cấu trúc học phần

- Tổng thời lượng: 45 tiết
- Số buổi: 15 buổi
- Hình thức thi: viết (90' – không sử dụng tài liệu).

Kế hoạch học phần

TT	Nội dung	Phân bổ theo tiết				
		Lên lớp			TH	Cộng
		LT	BT	TL		
1.	Chương 1. Tổng quan về an toàn thông tin	6				6
	Chương 2. Các hiểm họa gây mất an toàn thông tin	9				9
3.	Chương 3. Các phương pháp đảm bảo an toàn thông tin	15				15
	Chương 4. Chính sách và mô hình an toàn thông tin	9				9
5.	Chương 5. Các tiêu chí đánh giá và chuẩn an toàn thông tin	6				6
	Tổng	45				45

❖ Thực hiện theo kế hoạch các buổi học

❖ Bài tập lớn

1

Giới thiệu học phần

2

Tình hình an toàn thông tin gần đây

3

Đối tượng an toàn thông tin

4

Khái niệm an toàn thông tin

Sự kiện an ninh mạng gần đây

❑ 2010: Sâu Stuxnet

Siêu vũ khí chiến tranh mạng: Stuxnet, sâu máy tính bí ẩn

Cập nhật lúc 13h22' ngày 04/01/2011

Hàng ngàn máy ly tâm làm giàu uranium của Iran đột nhiên “chết đứng”. Một cuộc chiến không bom đạn và thương vong đã bắt đầu và dường như đã đẩy lùi chương trình hạt nhân của Iran đến 2 năm.

Đây là một cuộc chiến không có tiếng động, không có xác chết mà các chuyên gia về máy tính đã báo động từ lâu nhưng mới được đề cập một cách nghiêm túc hồi tháng 6-2010.

Vũ khí tối mật trong cuộc chiến này là một con sâu máy tính cực kỳ bí ẩn không rõ của ai, có sức tàn phá vật chất khủng khiếp. Nó không chỉ hủy diệt những vật thể mà nó len lỏi vào mà còn có thể hủy diệt cả những ý tưởng.

Siêu vũ khí có nguồn gốc mơ hồ

Tên "*cúng com*" của nó là sâu **Stuxnet**, một "*siêu vũ khí*" chiến tranh mạng - theo nhận định của các chuyên gia an ninh máy tính - thực sự gây lo ngại cho mọi quốc gia.

Sự kiện an ninh mạng gần đây

❑ 2/2013: Mandiant về Đơn vị 61398

'Trung Quốc có hàng ngàn hacker chuyên tấn công mạng'

20/02/2013 | 08:42

Đó là kết luận điều tra của công ty an ninh mạng hàng đầu của Mỹ, Mandiant, đưa ra hôm qua (19/2).

Công ty Mandiant tiết lộ, hàng trăm cuộc điều tra của công ty đã cho thấy:

Các nhóm hacker đột nhập vào các tờ báo Mỹ, cơ quan Chính phủ và nhiều công ty 'nằm ở Trung Quốc và chính quyền Trung Quốc biết về họ'.

Bản báo cáo dài 74 trang tập trung vào một nhóm hacker mang tên 'APT1' - viết tắt của cụm từ Đe dọa Liên tục Cấp cao.

'Chúng tôi tin APT1 có thể tiến hành các chiến dịch phá hoại qua mạng kéo dài, với quy mô rộng bởi nhóm này được sự ủng hộ từ chính quyền' - Mandiant nói.

Sự kiện an ninh mạng gần đây

□ 5/2017: WannaCry



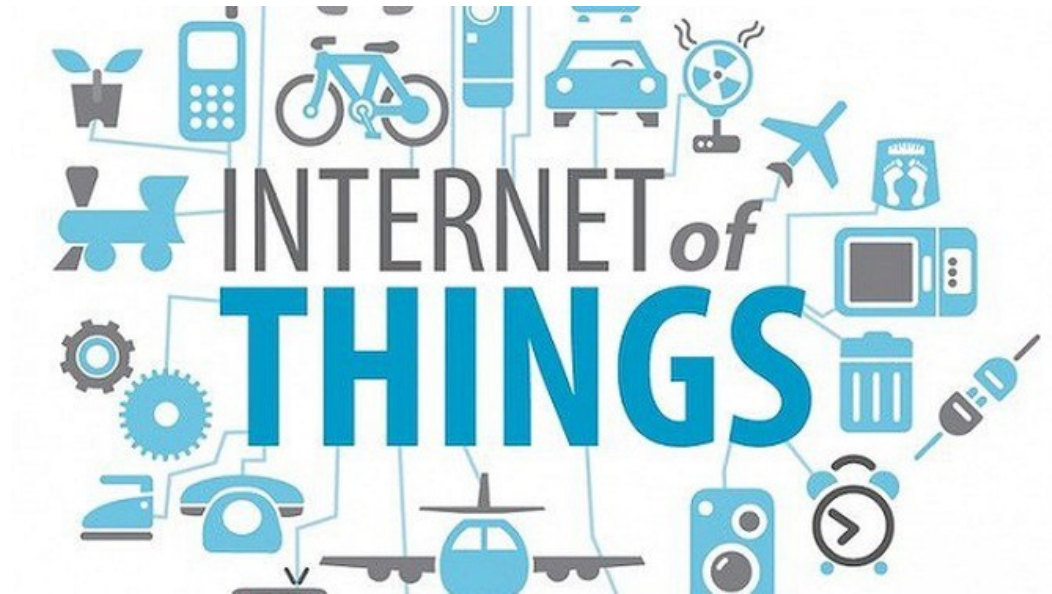
Sự kiện an ninh mạng gần đây

- ❑ 2020: Giám điệp mạng của Trung Quốc nhằm mục tiêu vào các công ty viễn thông ở Mỹ, châu Á, châu Âu



Sự kiện an ninh mạng gần đây

- ❑ Theo báo cáo dự báo của Statista sẽ có 30,9 tỉ thiết bị kết nối Internet được sử dụng trên khắp thế giới vào năm 2025.
- ❑ Số lượng biến thể mã độc trên thiết bị di động tăng 54% trong năm 2017
- ❑ Tấn công nhằm vào các thiết bị IoT cũng tăng hơn 600% (mã độc Mirai lây nhiễm hơn 1,2 triệu thiết bị IoT với lưu lượng tấn công DDoS được ghi nhận là lớn nhất từ trước đến nay ở ngưỡng 1,2 Tbps)



Sự kiện an ninh mạng gần đây

❑ Các hệ thống nổi tiếng để lộ tài khoản người dùng ở quy mô lớn

- 2012: 130 triệu tài khoản LinkedIn
- 2013: 340 triệu tài khoản MySpace
- 5/2014: 233 triệu tài khoản eBay
- 9/2014: 5 triệu tài khoản Gmail
- 6/2016: 100 triệu tài khoản VK (Facebook Nga)

Sự kiện an ninh mạng gần đây

❑ 6/2015: Lộ thông tin cá nhân ở Mỹ

Hơn 4 triệu nhân viên liên bang Mỹ bị tin tặc tấn công

Thứ sáu, 05/06/2015, 12:10 (GMT+7)

*** Mỹ đang mở rộng chương trình do thám Internet”**

Chính phủ Mỹ ngày 4-6 thừa nhận tin tặc có thể đã tiếp cận được thông tin cá nhân của khoảng 4 triệu nhân viên liên bang Mỹ, kể cả những người đã nghỉ hưu. Đây là vụ tấn công mạng lớn nhất từ trước tới nay nhằm vào các cơ quan liên bang của Mỹ.

Sự kiện an ninh mạng gần đây

❑ 6/2015: Kaspersky bị tấn công

PC World VN » Công nghệ » An ninh mạng

Thứ Năm, 11/06/2015 15:17 (GMT+7)

Kaspersky bị tấn công mạng trong thời gian dài

T.H.A



(PCWorldVN) Hãng an ninh mạng Nga Kaspersky hôm 10/6 bất ngờ tuyên bố các hệ thống máy tính của họ từng bị thâm nhập hồi đầu năm 2015, đồng thời ám chỉ có quốc gia hậu thuẫn các hoạt động này.

Tuyên bố chính thức được **Kaspersky** phát đi được đánh giá là "gây sốc" bởi một hãng bảo mật hàng đầu thế giới vẫn có thể là nạn nhân của một vụ tấn công không gian mạng tức điều đó có nghĩa là trình độ của nhóm **hacker** thực hiện không phải dạng vừa.

Tuy nhiên, Kaspersky khẳng định mọi dữ liệu khách hàng của hãng vẫn an toàn tuyệt đối bởi vụ tấn công đầy phức tạp này "tránh xa" thôn tin người dùng, thay vào đó hacker chỉ tập trung thâm nhập vào

Sự kiện an ninh mạng gần đây

❑ 7/2015: Hacking Team bị hack

[Trang chủ](#) » [Hacker/Virus](#) » [Hacker](#)

Lượt xem: 2291 | Gửi lúc: 10/07/2015 17:10:36

 SHARE    ...

“Hacking Team” bị hack – Không gì là an toàn tuyệt đối!

Ngày 5/7/2015, Một nhóm hacker đã thực hiện tấn công vào Công ty chuyên cung cấp phần mềm gián điệp Hacking Team và sau đó sử dụng tài khoản Twitter của chính công ty này để công khai các dữ liệu khai thác được. Có khoảng 500GB dữ liệu đã được phát tán trên Internet nhằm mục đích tiết lộ danh sách các khách hàng và những mã nguồn được bảo vệ.

Sự kiện an ninh mạng gần đây

❑ 6/2016: Hàn Quốc tố hacker Triều Tiên đánh cắp bí mật quân sự

- Sử dụng 16 máy chủ từ Bình Nhưỡng
- Đánh cắp 42.000 tài liệu

Sự kiện an ninh mạng gần đây

□ **8/2016: Nhóm Hacker NSA bị hack**

- Equation Group: nhóm hacker thuộc NSA
- Equation Group: đã hoạt động ~20 năm
- Equation Group: liên quan Stuxnet
- The Shadow Brokers: đã hack EQ
- The Shadow Brokers: được cho là của Nga

Sự kiện an ninh mạng gần đây

□ 8/2021: Vụ việc BKAV bị tấn công

August 22, 2021 at 02:38 AM This post was last modified: August 22, 2021 at 03:05 AM by chunxong. Edited 5 times in total.

Hi there,
I'm still here for selling.

\$20k for BKAV Pro source + \$30k for server side code
\$10k for BKAV Mobile AV source + \$10k for server side code.
\$20 for BKAV Endpoint Security. + \$10k for server side code
\$50k for GD5 source code.
\$100k for AI source code.

So far, 3 copies of Bkav Pro source code has been sold. So, no one could buy this product exclusively anymore.

If you want to buy anything above, please, send the number of XMR appropriate to their price to the address:
47SonhEFSikNjwcmGAnKG6frXzkCkA2aZ7yBe8ourjnnNPDgQnjhwCa89NUyew62AxP7b8Uqqmh8dS2RCzg2E

Then, I will send the source code for the sender.


Because too much of people just ask the price for their curiousness, I will not make a trade for anyone if there

Note: if u want to buy anything exclusively, the price will be double

Important:
If you have a facebook account, please report this facebook account (belongs to Nguyen Tu Quang) as he co

posts a link to the source code (but blocking/deleting comments).


chunx



Tay to

GOD

Posts 42
Threads 1
Joined Aug 2021
Reputation 89



Sự kiện an ninh mạng gần đây

- ❑ Xu hướng tấn công chuỗi cung ứng (Supply Chain Attack): Thay vì nhắm vào từng nạn nhân riêng lẻ, tin tặc tấn công vào các nhà sản xuất phần mềm. Mã độc được cài ngay từ khi phần mềm này xuất xưởng.



Sự kiện an ninh mạng gần đây

Tình hình trong nước?

Sự kiện an ninh mạng gần đây tại Việt Nam

- ❑ Từ 2001 đến 2019, các cơ quan chức năng đã phát hiện hơn 1.100 vụ lộ, mất bí mật nhà nước, trong đó lộ, mất bí mật nhà nước qua hệ thống thông tin chiếm tỷ lệ lớn với trên 80% số vụ.
- ❑ Từ 2010 đến 2019 đã có 53.744 lượt cổng thông tin, trang tin điện tử có tên miền .vn bị tấn công, trong đó có 2.393 lượt cổng thông tin, trang tin điện tử của các cơ quan Đảng, Nhà nước “.gov.vn”, xuất hiện nhiều cuộc tấn công mang màu sắc chính trị, gây ra những hậu quả nghiêm trọng

Sự kiện an ninh mạng gần đây

❑ 10/2014: VCCorp bị tấn công

Bài học rút ra sau vụ việc VCCorp bị tấn công.

07/11/2014 09:14:00

Trung tuần tháng 10 vừa qua hệ thống Data center của VCCorp bị tấn công khiến toàn bộ các sản phẩm của VCCorp và các trang báo điện tử của VCCorp như: Dân Trí, Người Lao Động, Gia đình & Xã hội, VnEconomy....không thể truy cập trong nhiều ngày. Theo thông tin mới nhất điều tra được, phần mềm độc hại cài cắm vào hệ thống của VCCorp không phải phần mềm viết tay của một nhóm nghiệp dư hoặc một cá nhân mà là của một nhóm chuyên nghiệp. Phần mềm kiểu này trên thế giới được định giá khoảng 200.000 - 1 triệu USD. Bên cạnh khoản đầu tư phần mềm độc hại này, nhóm tấn công còn dành khoảng 3 - 5 người theo dõi hệ thống của VCCorp trong vòng 6 tháng. Ước tính chi phí đầu tư cho "chiến dịch" tấn công vào VCCorp trung tuần tháng 10/2014 lên tới 500.000 USD và thiệt hại gây ra khoảng 20 - 30 tỷ đồng. Cơ quan an ninh vẫn đang tiếp tục điều tra.

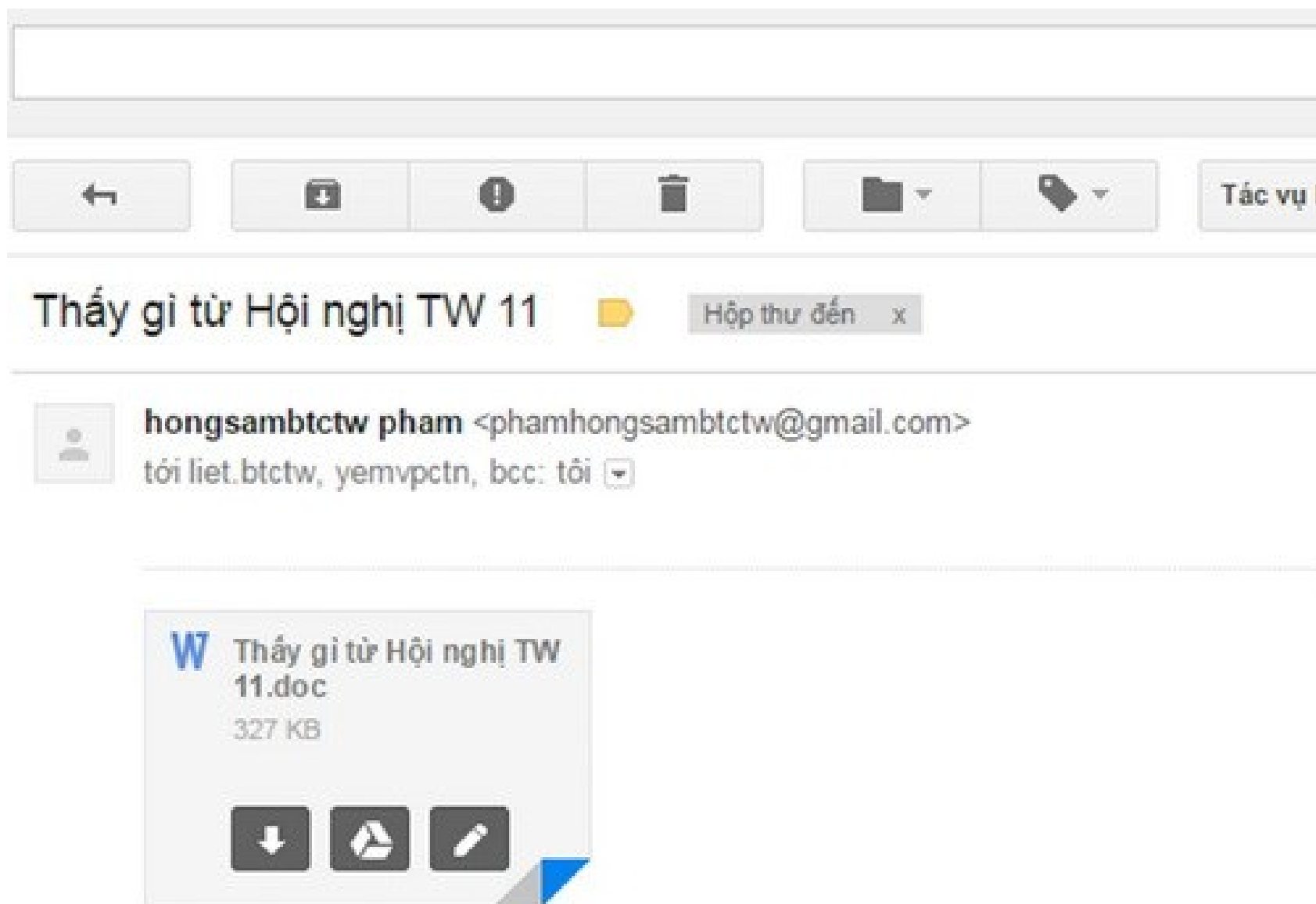
Sự kiện an ninh mạng gần đây

❑ 5/2015: Nhà báo Việt bị theo dõi

Nhóm tin tặc theo dõi nhiều nhà báo Việt Nam suốt 10 năm

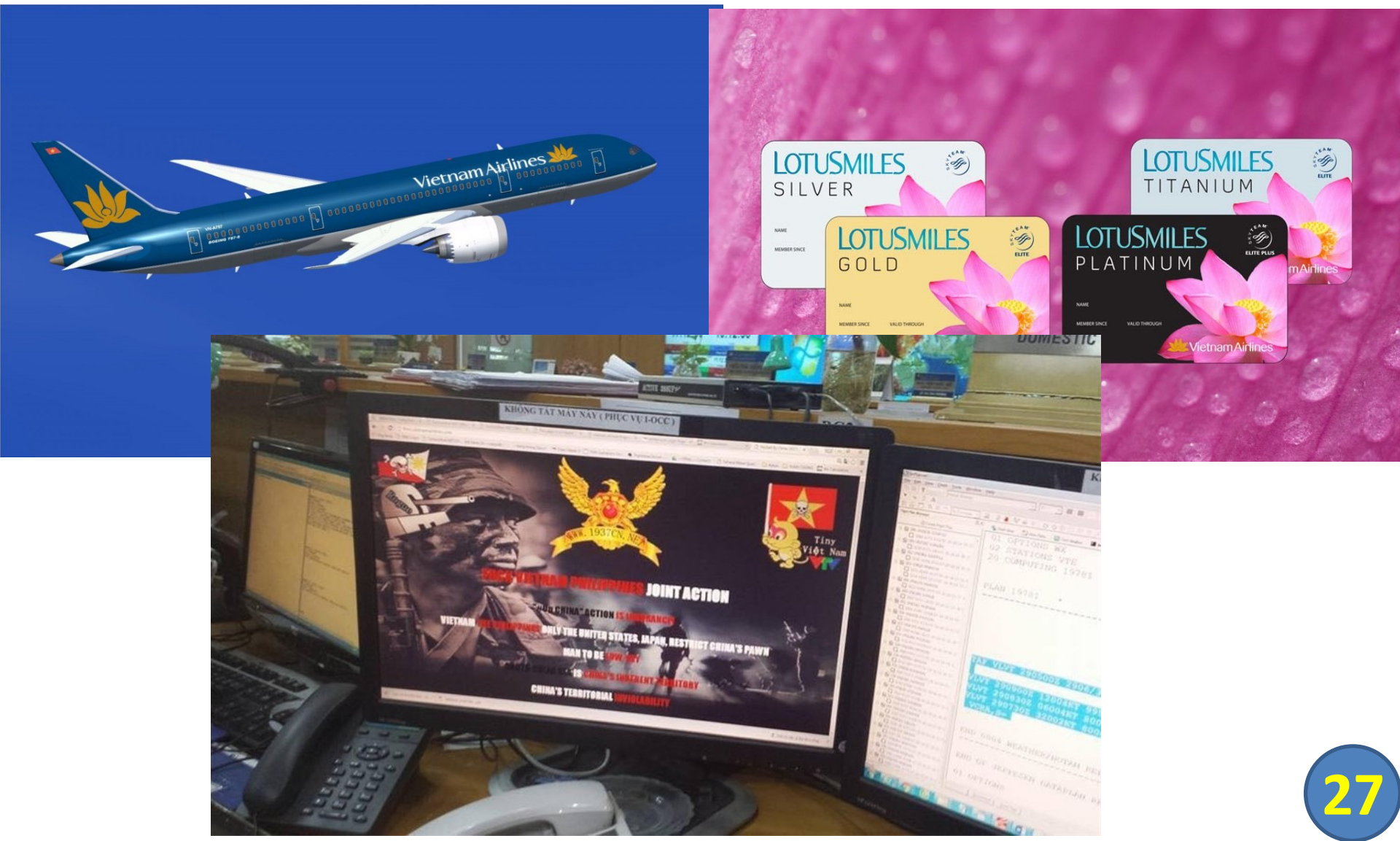
Công ty bảo mật FireEye cho biết họ nhận thấy một số dấu hiệu chứng tỏ nhóm tin tặc này được đặt tại Trung Quốc và do một chính phủ hậu thuẫn.

Sự kiện an ninh mạng gần đây



Sự kiện an ninh mạng gần đây

□ 7/2016: Vietnam Airlines



Điểm yếu bảo mật ở Việt Nam

147K trên 316K camera ở VN có lỗ hổng bảo mật



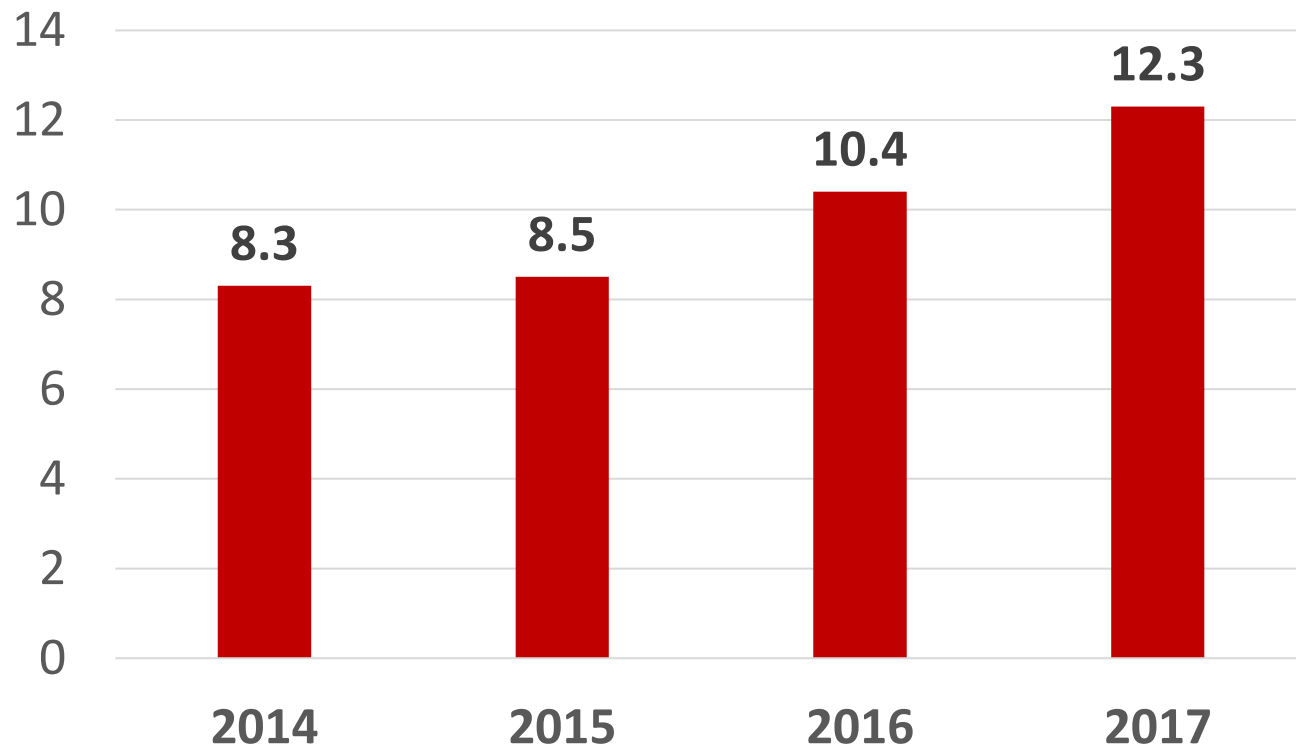
300K trên 5.6M Router tại VN có lỗ hổng bảo mật



Việt Nam có số lượng thiết bị nhiễm mã độc này cao nhất trên thế giới

Thiệt hại do các tấn công mạng tại Việt Nam

Thống kê thiệt hại (đơn vị: nghìn tỷ đồng)



Sự kiện an ninh mạng gần đây

- 2010: Padding Oracle Attack
- 2011: BEAST (Browser Exploit Against SSL/TLS)
- 2012: CRIME (Compression Ratio Info-leak Made Easy)
- 2014: HeartBleed
- 2015: FREAK (Factoring Attack on RSA-EXPORT Keys)

1

Giới thiệu học phần

2

Tình hình an toàn thông tin gần đây

3

Đối tượng an toàn thông tin

4

Khái niệm an toàn thông tin

Thông tin và dữ liệu

- Bảo mật **dữ liệu** \leftrightarrow Bảo mật **thông tin**
- Toàn vẹn **dữ liệu** \leftrightarrow Toàn vẹn **thông tin**

• **Dữ liệu là gì?**

Thông tin là gì?

Dữ liệu là tập hợp các kí hiệu được sắp xếp theo những trật tự và nhất định để nhằm đạt được sự hiểu biết, tạo ra bất định và đưa ra thể hiện trên một phương tiện lưu trữ nhất định.

**Ví dụ về dữ liệu
và thông tin?**

Thông tin và dữ liệu

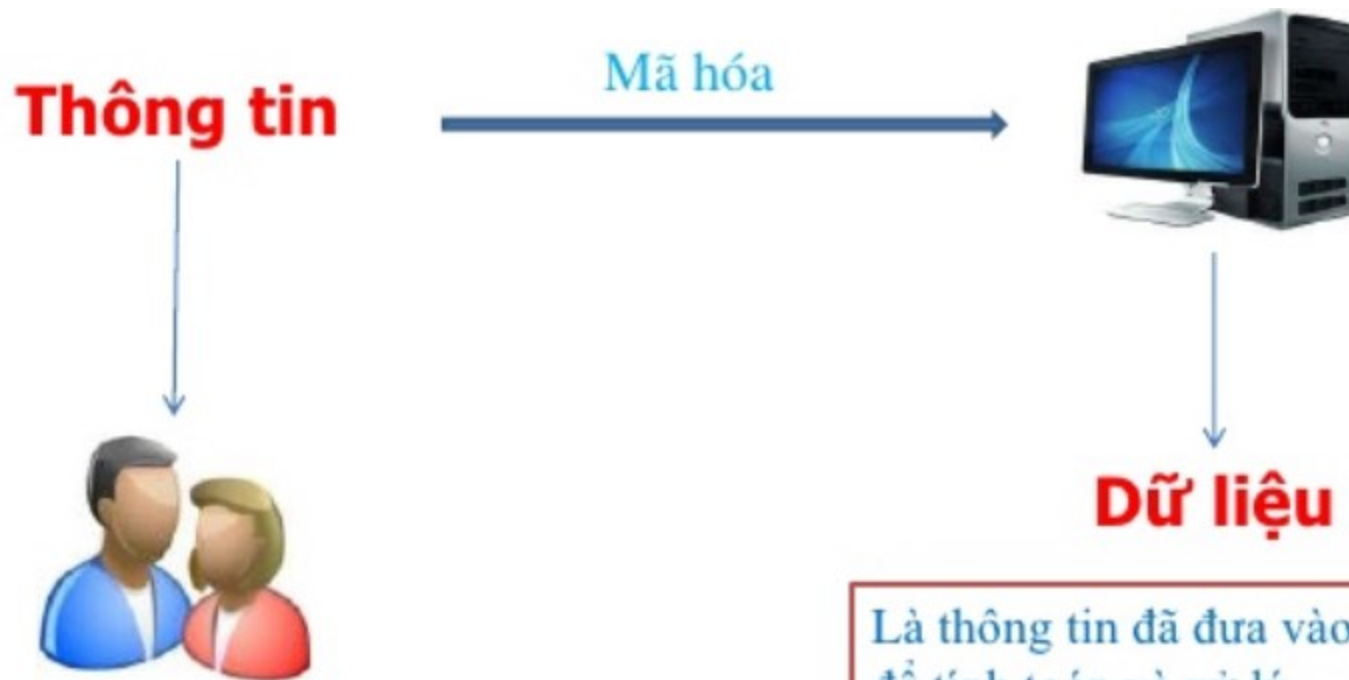
- 明天将有雨
- Míngtiān jiāng yǒu yǔ
- Завтра будет дождь
- There will be rain tomorrow
- Ngày mai trời mưa



Thông tin và dữ liệu

- Thông tin chứa đựng ý nghĩa, còn dữ liệu là các dữ kiện không có ý nghĩa rõ ràng nếu nó không được xử lý.
- Cùng một thông tin có thể được biểu diễn bằng những dữ liệu khác nhau.
- Cùng một dữ liệu có thể biểu diễn những thông tin khác nhau.

Thông tin và dữ liệu



Là những hiểu biết có được về một sự vật, sự kiện nào đó.

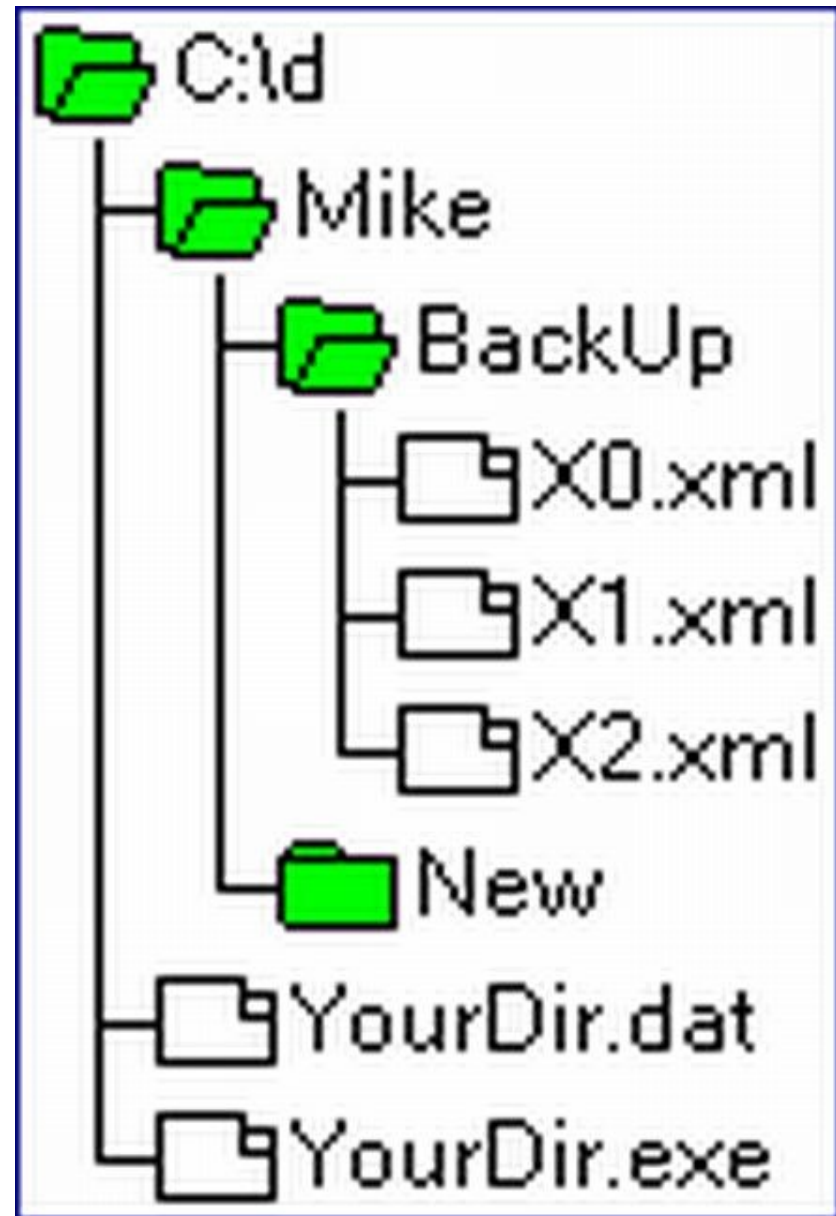
Là thông tin đã đưa vào máy tính để tính toán và xử lý.

Trong ATTT, ta có thể đồng nhất thông tin và dữ liệu

Hệ thống thông tin

□ **Hệ thống TT – VT** là tập hợp các thiết bị phần cứng và phần mềm, liên hệ với nhau bằng các kênh truyền và nhận thông tin thành một thể thống nhất để xử lý thông tin (tìm kiếm, lưu trữ, bảo vệ, xử lý,...) và cung cấp kết quả cho người dùng.

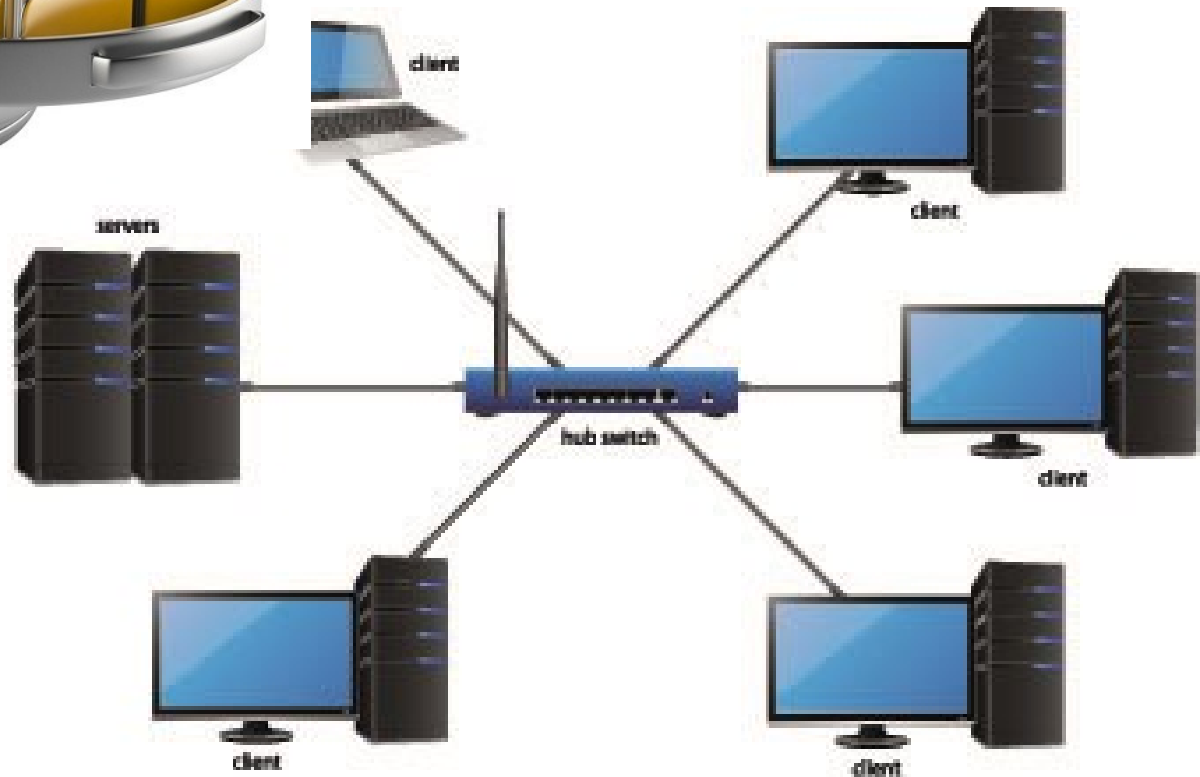
Hệ thống thông tin



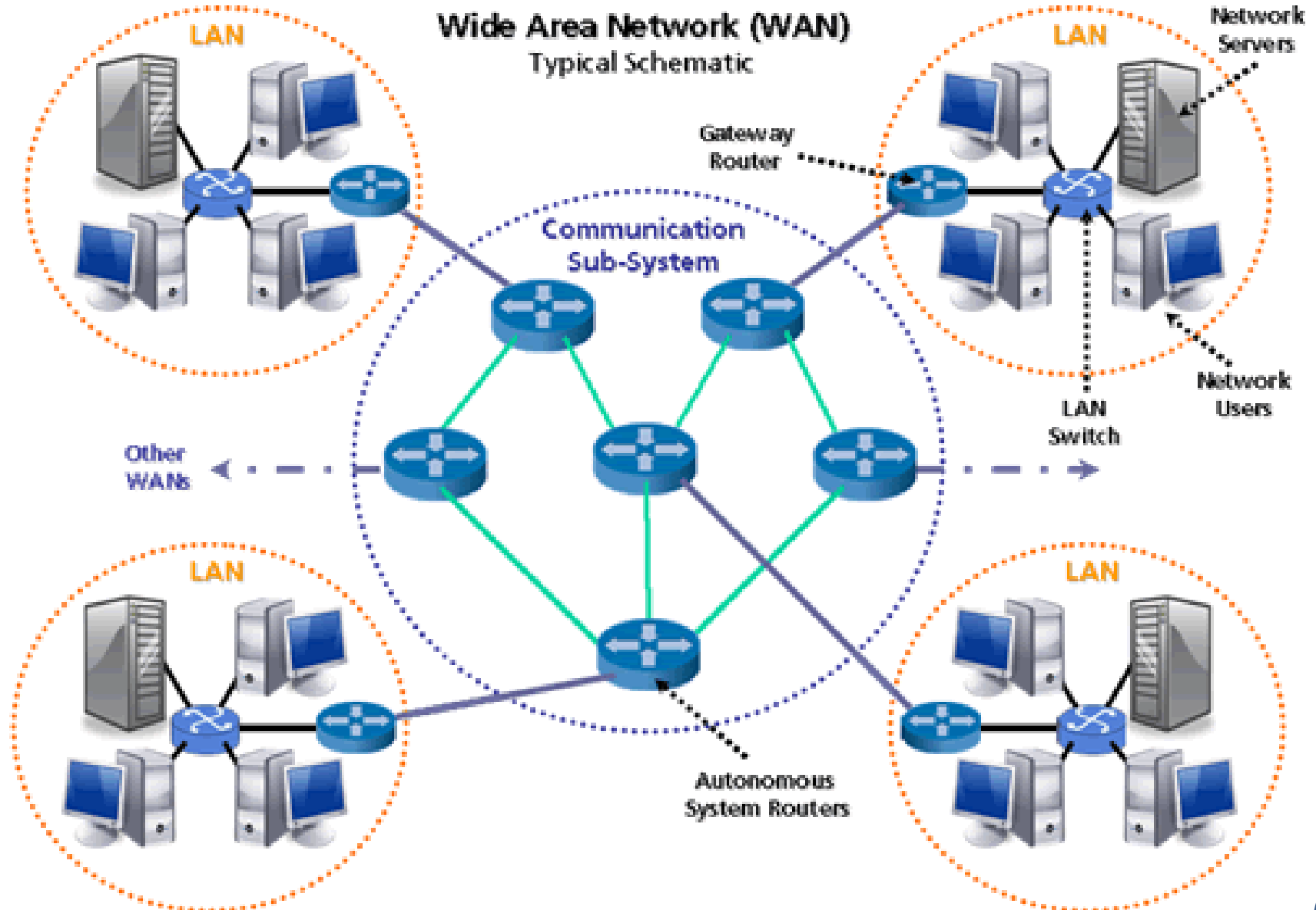
Hệ thống thông tin



Hệ thống thông tin



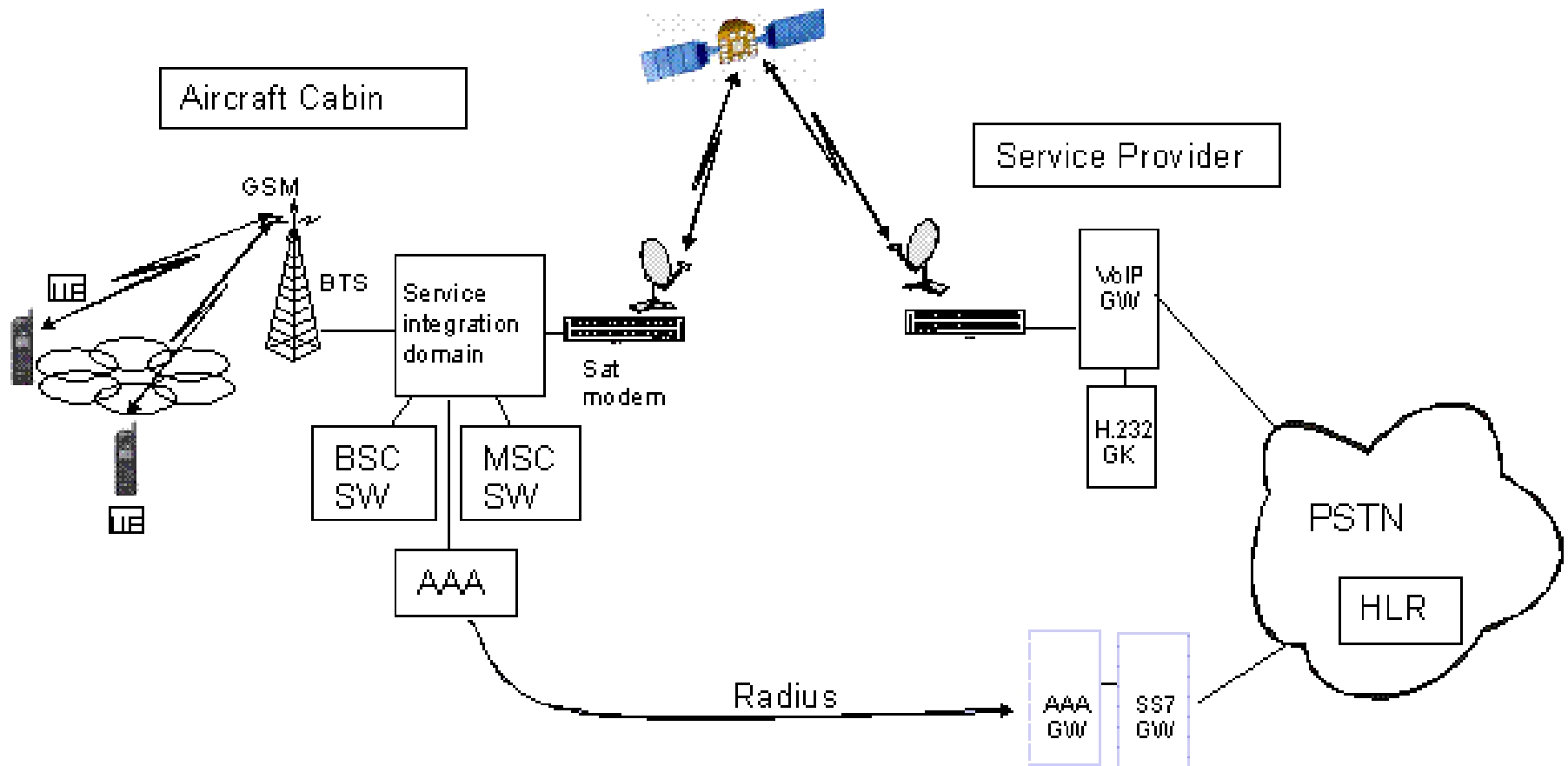
Hệ thống thông tin



Hệ thống thông tin



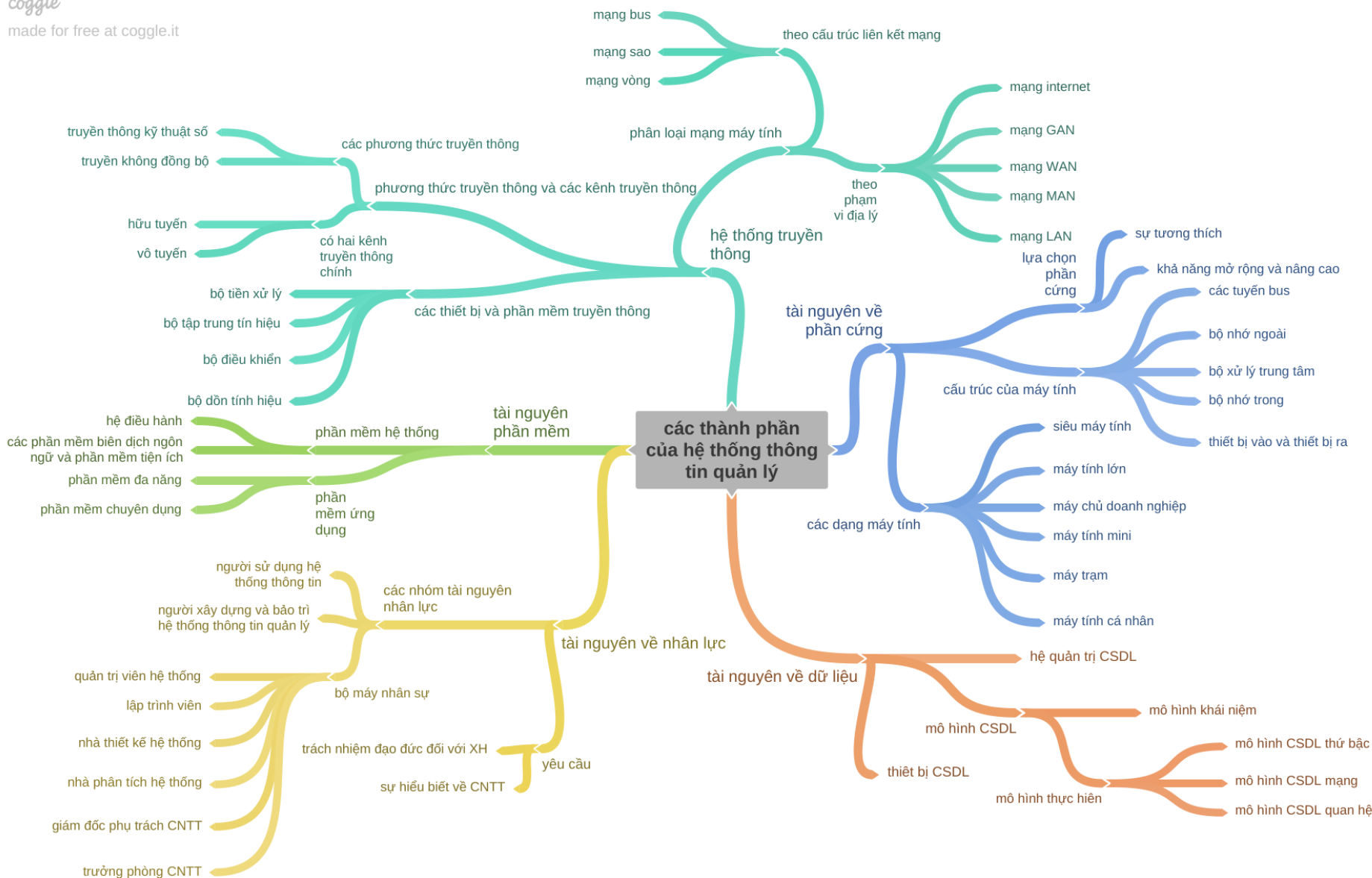
Hệ thống thông tin



Các thành phần của hệ thống thông tin quản lý

coggle

made for free at coggle.it



1

Giới thiệu học phần

2

Tình hình an toàn thông tin gần đây

3

Đối tượng an toàn thông tin

4

Khái niệm an toàn thông tin

Khái niệm An toàn thông tin

❑ **An toàn thông tin** là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin [72/2013/NĐ-CP].

Khái niệm An toàn thông tin

Ba tính chất an toàn của thông tin

1. Tính bí mật (Confidentiality)
2. Tính toàn vẹn (Integrity)
3. Tính khả dụng (Availability)



→ **Bộ ba CIA**

Khái niệm An toàn thông tin

1. Tính bí mật

- Khái niệm: thông tin chỉ cung cấp cho những người có thẩm quyền
- Nguyên nhân phá vỡ tính bí mật:
 - Nghe lén, xem lén, đọc lén
 - Đánh cắp vật mang
 - Xâm nhập trái phép
 - Sự bất cẩn (nhầm lẫn, mất cảnh giác) của người có bí mật
 - Gián điệp



Khái niệm An toàn thông tin

2. Tính toàn vẹn

- Khái niệm: đảm bảo thông tin không bị thay đổi một cách trái phép hoặc thay đổi không như ý muốn
- Nguyên nhân phá vỡ tính toàn vẹn:
 - Lỗi đường truyền
 - Lỗi phát sinh khi lưu trữ
 - Tấn công sửa đổi, phá hủy



Khái niệm An toàn thông tin



Khái niệm An toàn thông tin

3. Tính khả dụng (sẵn sàng)

- Khái niệm: đảm bảo khả năng truy cập thông tin, tính năng của hệ thống thông tin mỗi khi người dùng hợp lệ có nhu cầu.
- Nguyên nhân phá vỡ tính khả dụng:
 - Tấn công DoS, DDoS
 - Cấu hình sai
 - Tính toàn vẹn bị phá vỡ
 - Hỏng hóc,
 - Mất điện, thiên tai, hỏa hoạn



Khái niệm An toàn thông tin

«Information Security» là bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức, xã hội và quốc gia trong lĩnh vực thông tin

hợp pháp của tổ chức, cá nhân

[72/2013/NĐ-CP].

Các lĩnh vực trong an toàn thông tin



Các biện pháp đảm bảo an toàn thông tin

- ❑ Xây dựng hệ thống thông tin an toàn
- ❑ Định hướng: Xác định cấp độ, hiện trạng ATTT, tìm hiểu giải pháp, khả năng về kinh phí, con người, ...
- ❑ Giải quyết các điểm nóng: Xác định nơi trọng yếu, ưu tiên trong hệ thống
- ❑ Xây dựng chủ trương, chính sách: Thống nhất về chủ trương, xây dựng qui chế đảm bảo ATTT
- ❑ Đào tạo và tuyên truyền: Đào tạo hạt nhân, tuyên truyền chính sách ATTT
- ❑ Triển khai nhân rộng: Triển khai theo kinh phí được cấp, làm đến đâu bảo đảm an toàn đến đó



Các biện pháp đảm bảo an toàn thông tin



Bản đồ Ứng Dụng Bảo Mật

CYBERSECURITY MARKET MAP

IOT/ IIOT SECURITY



MOBILE SECURITY



CLOUD SECURITY



THREAT INTELLIGENCE



BEHAVIORAL DETECTION



DECEPTION SECURITY



RISK REMEDIATION



NETWORK & ENDPOINT SECURITY



CONTINUOUS NETWORK VISIBILITY



QUANTUM ENCRYPTION



WEBSITE SECURITY



 CBINSIGHTS

Các công ty Bảo Mật tại Việt Nam



Các nguyên tắc trong đảm bảo ATTT

- ☐ Nguyên tắc đặc quyền tối thiểu
- ☐ Nguyên tắc phân quyền
- ☐ Nguyên tắc hợp lý đầy đủ
- ☐ Nguyên tắc mặc định an toàn
- ☐ Nguyên tắc toàn diện
- ☐ Nguyên tắc phổ biến tối thiểu
- ☐ Nguyên tắc đơn giản trong sử dụng
- ☐ Nguyên tắc cách ly trong đảm bảo an toàn thông tin
- ☐ Nguyên tắc đóng gói trong đảm bảo an toàn thông tin
- ☐ Nguyên tắc mềm dẻo hệ thống
- ☐ Nguyên tắc phòng thủ chiều sâu
- ☐ Nguyên tắc tường minh trong đảm bảo an toàn thông tin
- ☐ Nguyên tắc mở trong đảm bảo an toàn thông tin



