

BÀI 1. TỔNG QUAN VỀ AN TOÀN AN NINH THÔNG TIN

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

1

1

Nội dung

- An toàn an ninh thông tin (security) là gì?
- Chính sách và các cơ chế an toàn an ninh
- Lỗ hổng an toàn bảo mật, nguy cơ an toàn an ninh
- Nguyên lý xây dựng hệ thống an toàn an ninh

2

2

1. MỞ ĐẦU

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

3

3

1. Mở đầu

- Báo cáo về an toàn an ninh thông tin:
 - IBM X-Force Threat Intelligence Index 2019
 - Symantec Internet Security Threat Report 2019
 - Verizon 2018 Data Breach Investigations Report
 - Cisco 2019 Annual Security Report
- <http://www.networkworld.com/category/security0/>

4

4

An toàn an ninh thông tin là gì?

Bảo vệ tài nguyên hệ thống thông tin trước các hành vi gây tổn hại

- Tài nguyên hệ thống:
 - Phần cứng: máy tính, đường truyền, thiết bị mạng...
 - Phần mềm
 - Dữ liệu
 - Người dùng
- Các hành vi gây tổn hại: phần lớn là các hành vi tấn công cố ý
 - Tấn công vật lý: tấn công vào phần cứng
 - Tấn công logic: sử dụng các chương trình phá hoại để can thiệp vào quá trình xử lý và truyền dữ liệu

5

5

An toàn an ninh thông tin là gì?

- Hoạt động của hệ thống: yêu cầu tính đúng đắn là thực hiện đầy đủ và chính xác với mọi giá trị đầu vào
 - Có thể không phát hiện được tình huống đáp ứng một giá trị đầu vào độc hại sẽ dẫn đến một kết quả đầu ra nằm ngoài mong đợi
- AT-ANTT: là một dạng của tính đúng đắn
 - Hệ thống có khả năng phát hiện và ngăn chặn các giá trị đầu vào không mong muốn
 - Đạt được tính đúng đắn ngay cả khi có sự hiện diện của kẻ tấn công

6

6

Tại sao AT-ANTT là quan trọng?

Các hành vi tấn công AT-ANTT tác động tiêu cực tới:

- An toàn thân thể của mỗi cá nhân
- Sự bí mật của thông tin cá nhân và tổ chức
- Tài sản của cá nhân và tổ chức
- Sự phát triển của một tổ chức
- Nền kinh tế của một quốc gia
- Tính an toàn của một quốc gia
- ...

7

7

Nguy cơ với an toàn thân thể

Former CIA director: 'We kill people based on metadata'

12 May, 2014 18:27 / Updated 5 years ago

The Telegraph News Politics Sport Business Money Opinion Tech Life Style Tr

News - SCIENCE
Hackers could kill patients by attacking their pacemakers, warns Royal Academy of Engineering

REUTERS

Business Markets World Politics TV More

TECHNOLOGY NEWS | OCTOBER 4, 2016 | 4:08 PM | 3 YEARS AGO

J&J warns diabetic patients: Insulin pump vulnerable to hacking

Jon Pridle

6 MIN READ



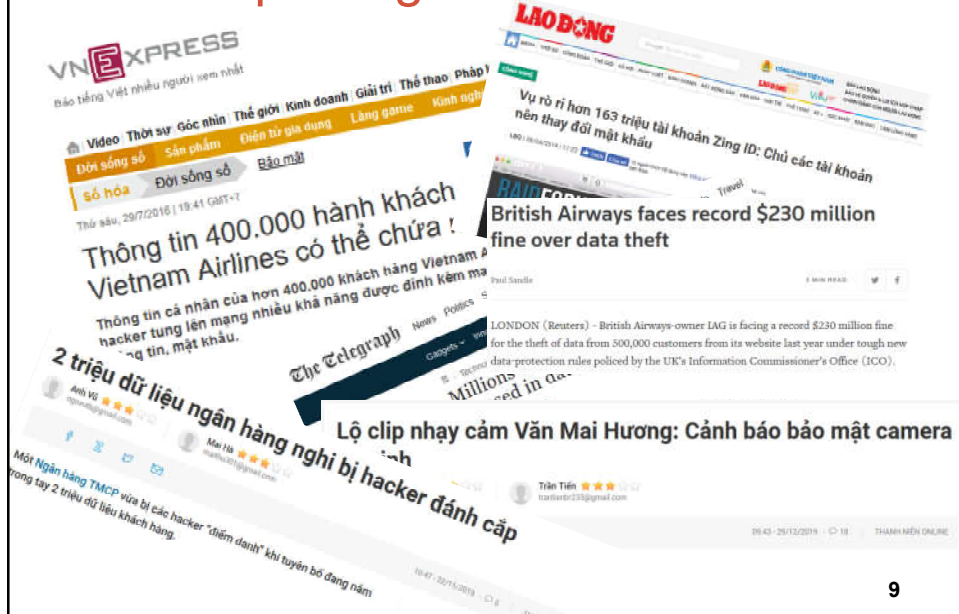
Former National Security Agency (NSA) and Central Intelligence Agency (CIA) Director Michael Hayden (Reuters/Larry Downing) © Reuters

2805

8

8

Đánh cắp thông tin cá nhân



9

9

Đánh cắp tài sản



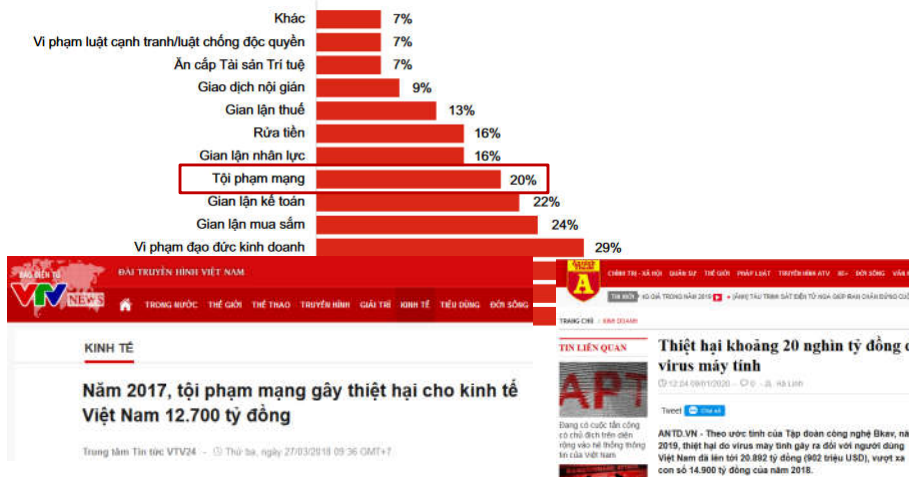
10

10

Tác động tới nền kinh tế

Các loại hình gian lận xảy ra trong 24 tháng qua

Báo cáo khảo sát Tội phạm kinh tế tại Việt Nam năm 2018 – PWC Vietnam



11

11

Tác động tới nền kinh tế



There's Nowhere to Hide from the Economics of Cybercrime

Cybercrime cost the global economy as much as \$600 billion in 2017. New technologies and connections mean new threats to some countries and new opportunities to others. Cybercrime impacts nearly every location on the globe. The first step to fighting it is understanding its scope and reach. McAfee, an industry leader in device-to-cloud security, teamed up with the Center for Strategic and International Studies (CSIS) to study the global economic impact of cybercrime. The costs vary by location, income levels, cybersecurity maturity, and other variables.

12

12

Xâm phạm chủ quyền quốc gia

NSA spied on Brazil's President Rousseff, dozens of top officials - WikiLeaks



U.S. President Barack Obama (R) and Brazil's President Dilma Rousseff (Reuters / Kevin Lamarque) © Reuters

NSA tapped German Chancellery for decades, WikiLeaks claims

New documents released suggest communications between top officials including Angela Merkel were intercepted by the US spy agency



▲ Cable released by WikiLeaks allege communications from German Chancellor Angela Merkel were intercepted (Photograph: AP/WideWorld)

Người lao động

TRONG NƯỚC QUỐC TẾ BẠN ĐỌC CÔNG ĐOÀN KINH TẾ SỨC KHỎE GIÁO DỤC PHÁP LUẬT VĂN NGHỆ THỂ THAO

Thời sự trong nước Chính trị Xã hội Câu chuyện hôm nay Phóng sự - Bút ký

Trang chủ Thời sự trong nước

Hacker Trung Quốc gây sự cố tại sân bay Nội Bài, Tân Sơn Nhất



13

Về môn học này

- Mã học phần: IT4015
- Tên học phần: Nhập môn An toàn thông tin
- Khối lượng: 3(3-1-0-6)
- Đánh giá:
 - Quá trình: 40%
 - Cuối kỳ: 60%
- Website:
<https://users.soict.hust.edu.vn/tungbt/it4015>

14

14

Quy định điểm quá trình

- Điểm QT = $0.75 \times \text{Điểm thi GK} + 0.25 \times \text{Điểm bài tập trắc nghiệm} + \text{Chuyên cần}$
- Điểm bài tập trắc nghiệm = Tỷ lệ số câu đúng
- Điểm chuyên cần:
 - Hoàn thành đúng 100% tất cả bài tập trắc nghiệm: +1
 - Không hoàn thành 1-2 bài: +0
 - Không hoàn thành 3-4 bài: -1
 - Không hoàn thành ≥ 5 bài: -2
- Bài tập trắc nghiệm có trên Google Classroom

15

15

Thông tin giảng viên

Bùi Trọng Tùng,

Bộ môn Truyền thông và Mạng máy tính

Email: tungbt@soict.hust.edu.vn

Địa chỉ: phòng 405, nhà B1

FB: <https://www.facebook.com/tungbui.hust>

Group: <https://www.facebook.com/groups/FAQ.TungBT>

16

Nội dung học phần

- Mở đầu: Các khái niệm và nguyên lý cơ bản
- Phần 1: Các hệ mật mã và ứng dụng
 - Hệ mật mã khóa đối xứng
 - Hệ mật mã khóa công khai
 - Xác thực thông điệp
- Phần 2: Kiểm soát truy cập
 - Xác thực danh tính
 - Ủy quyền
- Phần 3: An toàn-an ninh phần mềm

17

17

Tài liệu tham khảo

- [1] TS. Nguyễn Khanh Văn (2015). *Giáo trình Cơ Sở An Toàn Thông Tin*. Nhà xuất bản Bách Khoa Hà nội.
- [2] Matt Bishop (2004). *Introduction to Computer Security*. Addison-Wesley
- [3] Tài liệu đọc thêm theo từng bài

18

18

Chúng ta học gì?

- Suy nghĩ về hệ thống thông tin như một kẻ tấn công
 - Xác định mối đe dọa và điểm yếu của hệ thống
- Làm cách nào để thực hiện một số kỹ thuật tấn công
 - Khai thác lỗ hổng phần mềm
- Suy nghĩ về hệ thống như người thiết kế giải pháp AT-ANTT
 - Cách thức ngăn chặn và giảm thiểu tấn công
 - Hiểu và ứng dụng các nguyên lý AT-ANTT
 - Hiểu và ứng dụng các cơ chế, công cụ AT-ANTT

19

19

2. KHÁI NIỆM CƠ BẢN VỀ AT-ANTT

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

20

20

AT-ANTT là gì? - CIA

- Confidentiality (Bí mật): tài nguyên chỉ được tiếp cận bởi các bên được ủy quyền
- Integrity (Toàn vẹn): tài nguyên chỉ được sửa đổi bởi các bên được ủy quyền
- Availability (Sẵn sàng): tài nguyên sẵn sàng khi có yêu cầu
 - Thời gian đáp ứng chấp nhận được
 - Tài nguyên được định vị trí rõ ràng
 - Khả năng chịu lỗi
 - Dễ dàng sử dụng
 - Đồng bộ khi đáp ứng yêu cầu

21

21

AT-ANTT là gì? – AAA

- Assurance (Đảm bảo): hệ thống cung cấp sự tin cậy và quản trị được sự tin cậy
 - Ví dụ: tính tin cậy trong hệ thống thanh toán trực tuyến
 - Bao gồm khía cạnh kỹ thuật phần mềm: Làm thế nào chắc chắn rằng mã nguồn phần mềm được viết theo đúng thiết kế?
- Authenticity (Xác thực): khẳng định được danh tính của chủ thể trong hệ thống
- Anonymity (Ẩn danh): che giấu được thông tin cá nhân của chủ thể

22

22

Chính sách và cơ chế AT-ANTT

- Chính sách AT-ANTT(security policy): tuyên bố về các mục tiêu/yêu cầu AT-ANTT của hệ thống
 - Chủ thể
 - Hành vi phải thực hiện/được phép/không được phép
 - Tài nguyên
- Là cơ sở để xây dựng hạ tầng AT-ANTT
- Phục vụ cho quản trị AT-ANTT

23

23

Cơ chế AT-ANTT

- Là các kỹ thuật, thủ tục để thi hành và đảm bảo chính sách AT-ANTT được thi hành
- Phân loại:
 - Ngăn chặn (Prevention): ngăn chặn chính sách bị xâm phạm
 - Phát hiện (Detection) và Ứng phó(Response): phát hiện chính sách bị xâm phạm
 - ✓ False positive rate: Tỷ lệ cảnh báo sai
 - ✓ False negative rate: Tỷ lệ bỏ sót tấn công

24

24

Một số cơ chế AT-ANTT(tiếp)

- Bảo vệ vật lý (Physical protection)
- Mật mã học (Cryptography)
- Định danh (Identification)
- Xác thực (Authentication)
- Ủy quyền (Authorization)
- Nhật ký (Logging)
- Kiểm toán(Auditting)
- Sao lưu và khôi phục (Backup and Recovery)
- Dự phòng (Redundancy)
- Giả lập, ngụy trang (Deception)
- Gây nhiễu, ngẫu nhiên(randomness)

25

25

3. Lỗ hổng và tấn công AT-ANTT

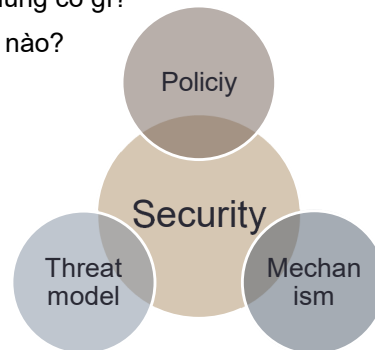
- Mối đe dọa (Threat): các hành vi tiềm ẩn khả năng gây hại cho hệ thống
- Tấn công (Attack): thực thi nguy cơ
 - Thường lợi dụng, khai thác lỗ hổng
 - Kẻ tấn công là ai? Kẻ tấn công có gì?
- Độ rủi ro (Risk): khả năng xảy ra các sự cố làm mất an toàn an ninh thông tin và thiệt hại của chúng cho hệ thống
- Lỗ hổng (Vulnerability): là những điểm yếu trong hệ thống có thể bị khai thác, lợi dụng để gây tổn hại cho hệ thống
 - <https://www.cvedetails.com/>
 - Tầm soát lỗ hổng định kỳ là một trong những giải pháp phòng chống tấn công

26

26

Mô hình đe dọa

- Threat Model: mô tả những mối đe dọa kẻ tấn công có thể gây ra cho hệ thống và hậu quả
 - Cái gì cần bảo vệ?
 - Ai có thể tấn công vào hệ thống? Chúng có gì?
 - Hệ thống có thể bị tấn công như thế nào?



27

27

Ai có thể tấn công bạn?

- Tội phạm vì động cơ tiền bạc
- Tội phạm vì động cơ phá hoại
- Chính phủ các nước
 - Nếu bạn đủ quan trọng và đáng giá :D
- Người thân quen:
 - Kẻ tấn công nguy hiểm nhất

28

28

Những giả định về tấn công

- Những giả định này là bi quan nhưng là sự cần trọng cần thiết
- Kẻ tấn công có thể tương tác với hệ thống mà không gây ra sự khác biệt rõ ràng
- Kẻ tấn công có thể dễ dàng thu thập các thông tin thông thường của hệ thống(Ví dụ: hệ điều hành, phần mềm, dịch vụ,...)
- Kẻ tấn công có thể truy cập vào hệ thống tương tự để xác định được cách thức hệ thống hoạt động như thế nào

29

29

Những giả định về tấn công(tiếp)

- Kẻ tấn công có khả năng tự động hóa các hành vi tấn công
- Kẻ tấn công có khả năng phối hợp, điều phối các hệ thống/thành phần khác nhau
- Kẻ tấn công có nguồn tài nguyên tính toán rất lớn
- Kẻ tấn công có thể có một số quyền truy cập nhất định nào đó

30

30

Tại sao tấn công AT-ANTT là phổ biến?

- Thứ gì có thể hack được?

**For The First Time, Hackers Have
Refrigerator To Attack Business**



JULIE BORT

Jan. 16, 2014, 1:36 PM

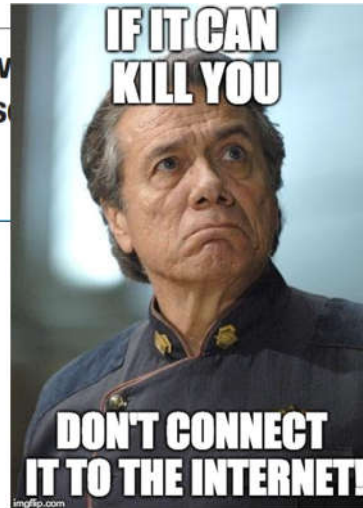
195,469

39

TOP DEVICE TYPES PERFORMING IOT ATTACKS (YEAR)

DEVICE TYPE	PERCENT
Router	75.2
Connected Camera	15.2
Multi Media Device	5.4
Firewall	2.1
PBX Phone System	0.6
NAS (Network Attached Storage)	0.6
VoIP phone	0.2
Printer	0.2
Alarm System	0.2
VoIP Adapter	0.1

Symantec Internet Security Threat Report 2019

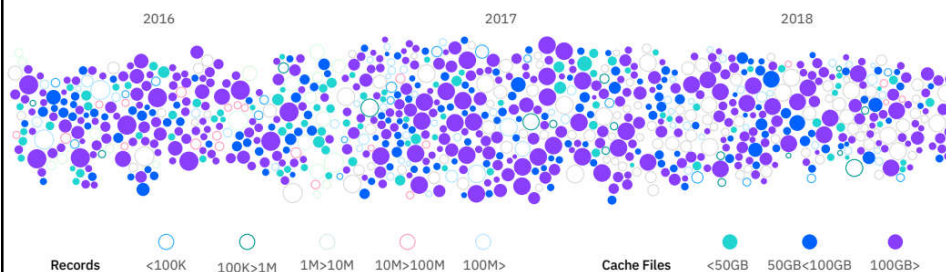


31

31

Tại sao tấn công AT-ANTT là phổ biến?

- Đánh cắp thông tin cá nhân

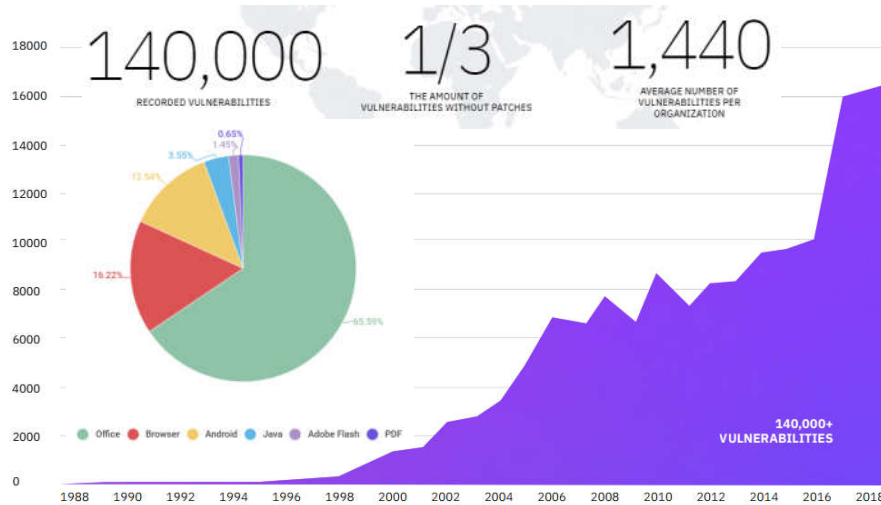


IBM X-Force Threat Intelligence Index 2019

32

32

Tại sao tấn công AT-ANTT là phổ biến?



IBM X-Force Threat Intelligence Index 2019

33

Tại sao tấn công AT-ANTT là phổ biến?

• Công cụ có sẵn

Rank	Exploit Kit	2015 (%)	2016 (%)	Percentage Point Difference
1	Unclassified	38.9	37.9	-1.0
2	Angler	13.3	22.2	8.9
3	Spartan	7.3	11.9	4.6
4	RIG	2.0	7.9	5.9
5	Magnitude	1.1	5.8	4.7
6	Neutrino	1.3	5.8	4.5
7	VIP	24.8	3.2	-21.6
8	Nuclear	4.0	1.6	-2.4
9	Fiesta	2.5	1.0	-1.5
10	G01 Pack	2.2	0.8	-1.4

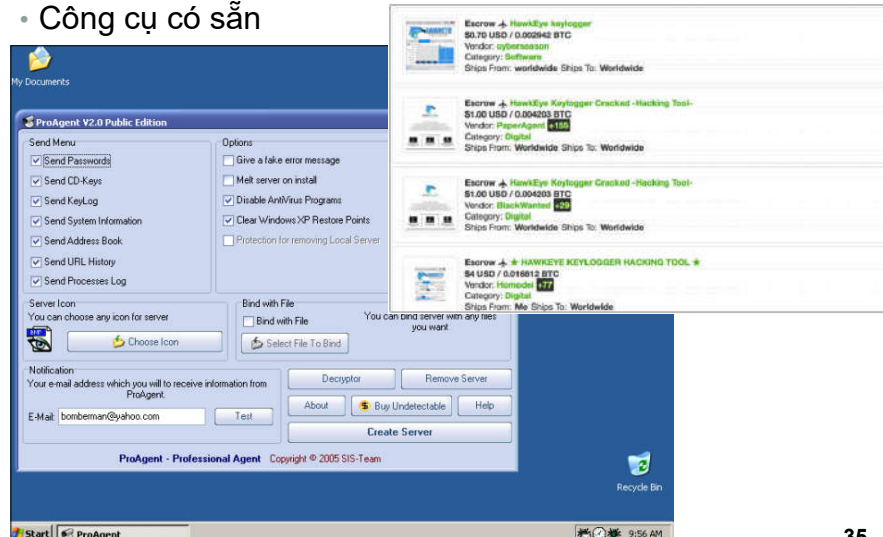
Top 10 Web attack toolkits

Symantec Internet Security Threat Report 2017

34

Tại sao tấn công AT-ANTT là phổ biến?

- Công cụ có sẵn

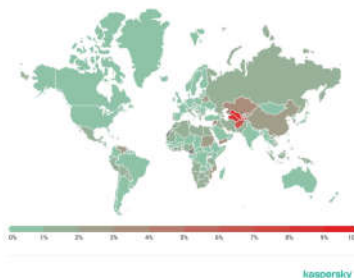
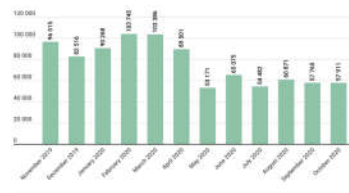


35

35

Động cơ tấn công

- Tiền bạc



Kaspersky Security Bulletin 2020

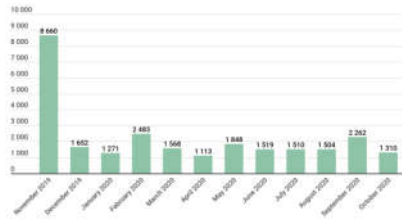
Name	%*
1 Zbot	21.6
2 Emotet	15.1
3 ClptoShuffler	15
4 RTM	11.1
5 Trickster	5.3
6 Nimnul	4.2
7 Neurevt	3.3
8 Danabot	3.2
9 SpyEye	3.2
10 Nymaim	2.1

Country*	%**
1 Uzbekistan	10.4
2 Turkmenistan	8.6
3 Tajikistan	7.5
4 Afghanistan	6.6
5 Costa Rica	4.0
6 Yemen	3.9
7 Kazakhstan	3.5
8 Syria	3.3
9 Guatemala	2.8
10 South Korea	2.7

36

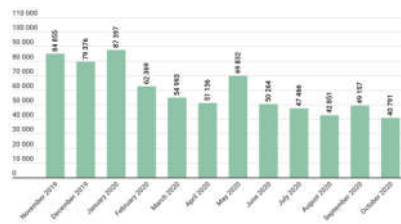
36

Ransomware(2019)



Number of new ransomware modifications detected, November 2019 – October 2020

Country*	%**
1 Bangladesh	8.12
2 Mozambique	3.13
3 Turkmenistan	2.65
4 Haiti	2.47
5 Uzbekistan	2.39
6 Ethiopia	2.10
7 Afghanistan	2.06
8 Nepal	1.97
9 Sudan	1.92
10 Kyrgyzstan	1.77



Number of users attacked by ransomware Trojans, November 2019 – October 2020

Top 10 most common families of ransomware Trojans

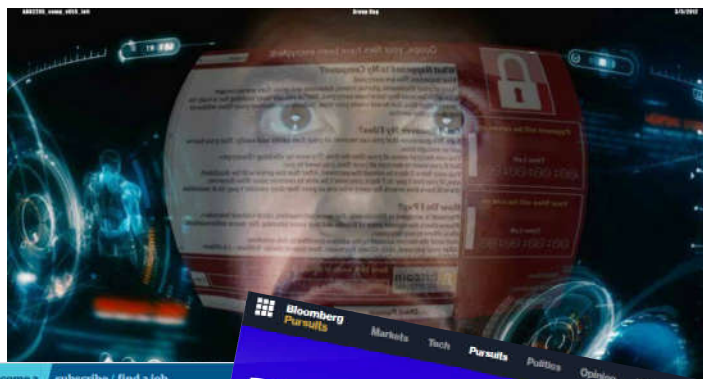
Name	Verdict	%*
1 WannaCry	Trojan-Ransom.Win32.Wanna	18.56
2 (generic verdict)	Trojan-Ransom.Win32.Phy	15.56
3 (generic verdict)	Trojan-Ransom.Win32.Gen	11.37
4 Stop	Trojan-Ransom.Win32.Stop	7.76
5 (generic verdict)	Trojan-Ransom.Win32.Encoder	6.48
6 (generic verdict)	Trojan-Ransom.Win32.Generic	4.77
7 (generic verdict)	Trojan-Ransom.Win32.Cryptor	4.07
8 PolyRansom/VX.lock	Virus.Win32.PolyRansom	2.54
9 Cryptor/Thema	Trojan-Ransom.Win32.Cryptor	2.21
10 (generic verdict)	Trojan-Ransom.Win32.Cryptor	1.85

Kaspersky Security Bulletin 2020

37

37

WannaCry (05/2017)



become a supporter | subscribe / find a job

news / opinion / sport / arts / tech / world / UK / science / cities / global

Malware

WannaCry: hackers withdraw £108,000 or bitcoin ransom

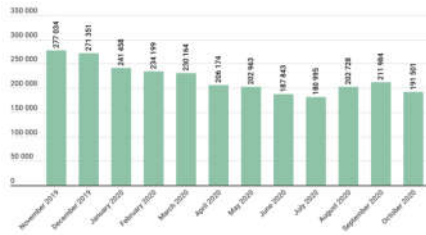
Next WannaCry Cyber Attack Could Cost Insurers \$2.5 Billion

Bloomberg Pursuits | Markets | Tech | Pursuits | Politics | Opinion | Businessweek | Subscribe to Bloomberg | Digital

38

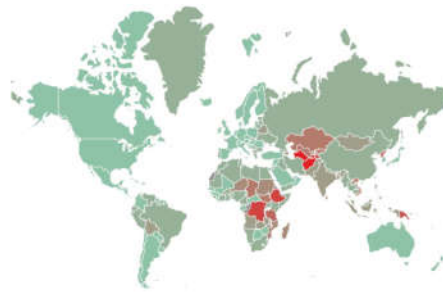
38

Coinminer(2018)



Number of users attacked by miners, November 2019 – October 2020

	Name	%
1	Trojan.Win32.Miner.bbb	17.53
2	Trojan.Win32.Miner.ays	10.86
3	Trojan.JS.Miner.m	10.28
4	Trojan.Win32.Miner.gen	8.00



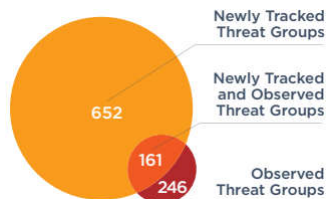
Kaspersky Security Bulletin 2020

39

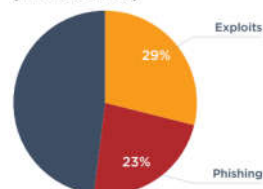
39

Động cơ tấn công

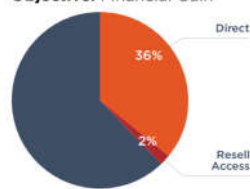
- Gián điệp, tình báo: Tấn công có chủ đích



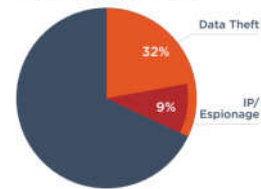
Initial Infection Vector (when identified)



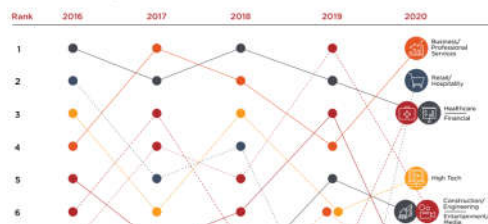
Objective: Financial Gain



Objective: Data Theft



TARGETED INDUSTRIES, 2015-2020



Fireeye M-Trends Reports 2021

40

40

Động cơ tấn công

- Mục đích chính trị



41

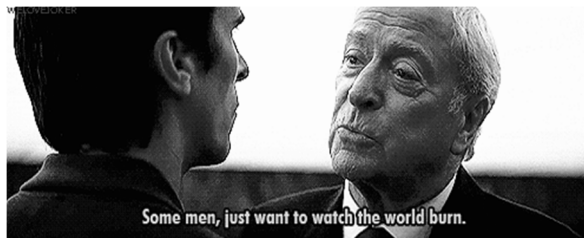
41

Động cơ tấn công

- Đùa cợt



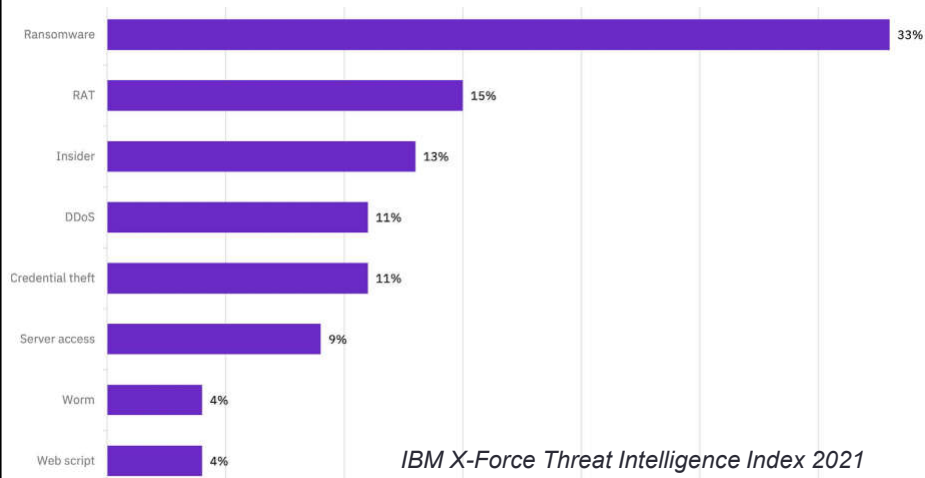
- Thú vui phá hoại



42

42

Một số dạng tấn công phổ biến



43

43

4. Xây dựng hệ thống AT-ANTT

44

44

Quy trình xây dựng

4 giai đoạn:

- Phân tích yêu cầu
 - Thiết kế
 - Triển khai
 - Kiểm thử và bảo trì
- Xây dựng chính sách AT-ANTT
 - Xác định các tình huống lạm quyền
 - Xây dựng mô hình nguy cơ
 - Thiết kế hướng bảo mật
 - Duyệt mã nguồn (Code review)
 - Kiểm thử theo nguy cơ ATBM
 - Kiểm thử xâm nhập

- Các giai đoạn được thực hiện tuần tự
- Luôn có sự phản hồi của giai đoạn sau tới giai đoạn trước
- Chia để trị

45

45

Quy trình xây dựng

- Xây dựng chính sách: có thể mô tả ban đầu bằng ngôn ngữ tự nhiên:
 - Hành vi phải thực hiện/được phép/ không được phép
 - Chủ thể của hành vi
 - Đối tượng hành vi tác động tới
 - Điều kiện
- Xây dựng các tình huống lạm quyền minh họa cho sự xâm phạm chính sách
- Chính sách AT-ANTT phải phù hợp với quy định luật pháp

46

46

Quy trình xây dựng

- Xây dựng mô hình đe dọa(Threat model):

1. Xác định, phân vùng tài nguyên cần bảo vệ
2. Xác định các luồng dữ liệu, hành vi tương tác tới tài nguyên
3. Phân tích các hoạt động diễn ra trên tài nguyên
4. Xác định các mối đe dọa có thể có, phân loại và đánh giá
5. Xác định các lỗ hổng liên quan

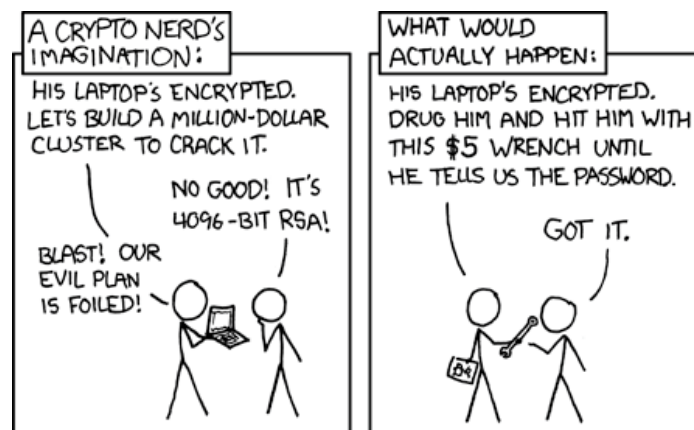
Mô hình đe dọa tồi(bad model) → Giải pháp AT-ANTT tồi
(bad security)

47

47

Xây dựng mô hình đe dọa

- AT-ANTT trên thực tế khác với lý thuyết



48

48

Hiểu biết về mô hình đe dọa với hệ thống

- Ví dụ: Phần lớn két sắt chỉ có khả năng chống cháy
 - Bảo vệ tài sản ở nhiệt độ bên trong $< 177^{\circ}\text{C}$ trong thời gian tối thiểu 30 phút khi nhiệt độ bên ngoài $> 1000^{\circ}\text{C}$
 - Bảo vệ tài sản ở nhiệt độ bên trong $< 55^{\circ}\text{C}$ trong thời gian tối thiểu 30 phút khi nhiệt độ bên ngoài $> 1000^{\circ}\text{C}$
- Chọn mua két sắt loại nào?



49

49

Quy trình xây dựng

- Thiết kế các thành phần theo mô hình nguy cơ: lựa chọn cơ chế AT-ANTT
 - Ngăn chặn: Loại bỏ hoàn toàn nguy cơ
 - Giảm thiểu
 - Chấp nhận nguy cơ
 - Chuyển nhượng rủi ro
- Triển khai
 - Chú ý: đào tạo người dùng
- Vận hành và bảo trì:
 - Chú ý: cần liên tục giám sát hệ thống

50

50

Một số nguyên tắc

- AT-ANTT là bài toán kinh tế: để tăng mức độ an toàn phải tăng chi phí
 - Giá trị tài nguyên cần bảo vệ/ Chi phí để bảo vệ
 - Mức tổn thương mà tấn công gây ra / Chi phí để chống lại các kỹ thuật tấn công
 - Chi phí thực thi tấn công / Giá trị thu lại
- Xây dựng hệ thống là an toàn nhất trong các điều kiện ràng buộc
- KISS: Keep It Simple, Sir!
- Complexity is the enemy

51

51

AT-ANTT là bài toán kinh tế

TL-15



TL-30



TRTL-30



TXTL-60



52

52

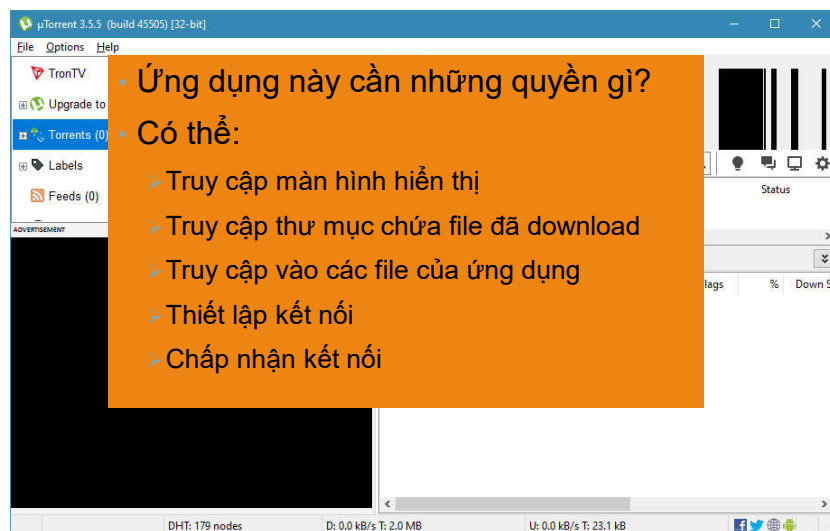
Một số nguyên tắc(tiếp)

- Tối thiểu hóa quyền (Least privilege): không cấp quyền nhiều hơn những gì mà đối tượng cần để hoàn thành nhiệm vụ.

53

53

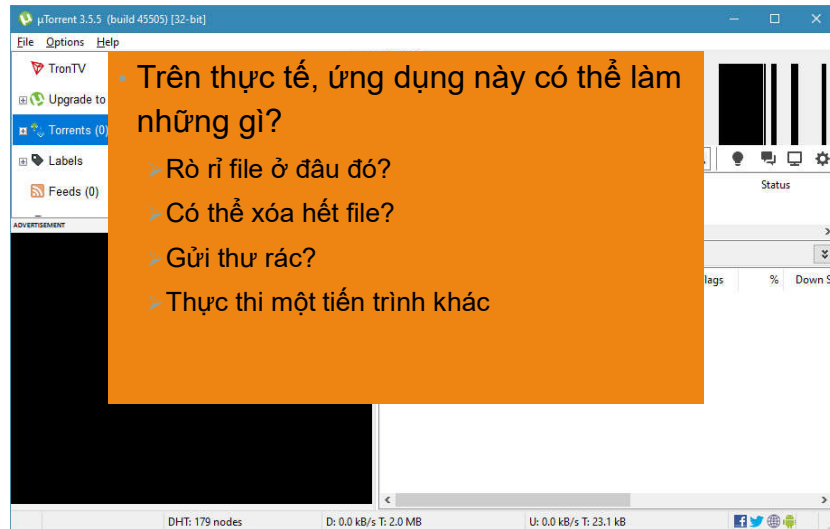
Tối thiểu hóa quyền



54

54

Tối thiểu hóa quyền

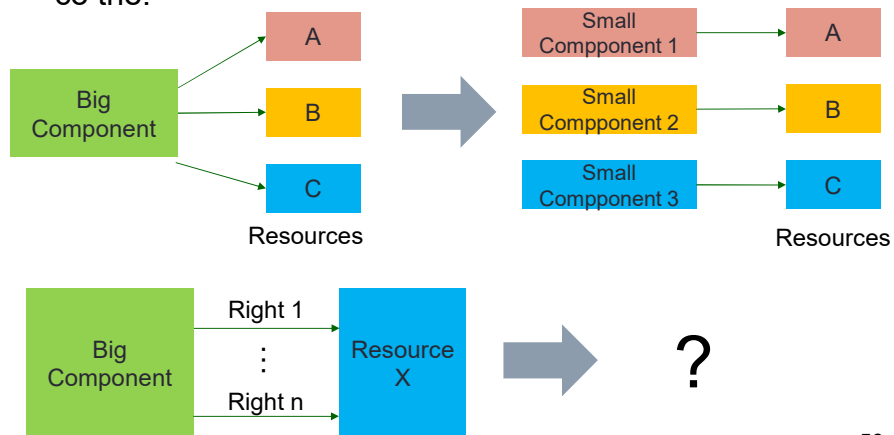


55

55

Tối thiểu hóa quyền

- Phân chia quyền (Privilege separation): Phân chia hệ thống sao cho các thành phần được cấp quyền nhỏ nhất có thể.



56

56

Tối thiểu hóa quyền

- Chia sẻ trách nhiệm (Separation of responsibility): quyền chỉ được thực thi khi có sự phối hợp của nhiều thành phần



57

57

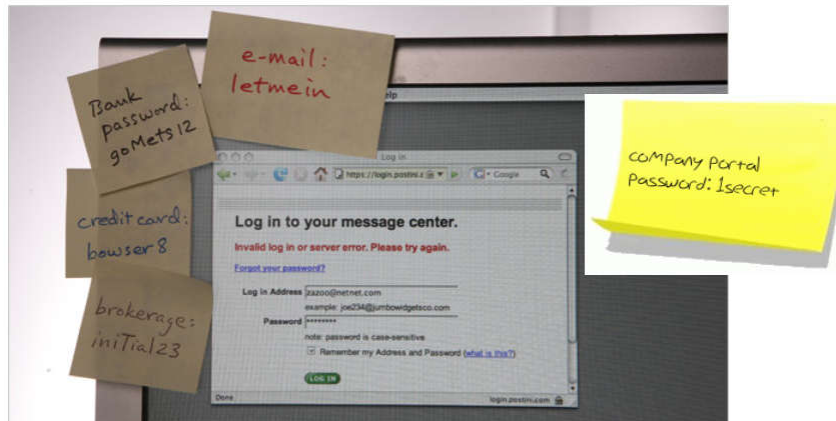
Một số nguyên tắc(tiếp)

- Chia sẻ tối thiểu (Least common mechanism): Tài nguyên cần được chia sẻ tới ít bên nhất có thể
- Dễ hiểu, dễ sử dụng cho người dùng:
 - Người dùng sẽ tuân thủ cơ chế an toàn bảo mật hay quyết định phá vỡ nó?
 - Nếu bạn không làm hệ thống dễ sử dụng và an toàn thì người dùng sẽ làm cho nó dễ sử dụng và không an toàn.
- KISS: Keep It Simple, Sir!
- Complexity is the enemy

58

58

Dễ hiểu, dễ sử dụng cho người dùng



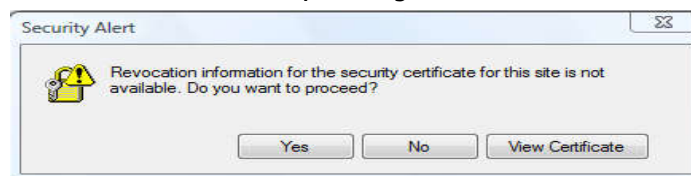
9

59

59

Dễ hiểu cho người dùng – Ví dụ

Báo lỗi xác thực chứng thư số HTTPS trên IE6




- Phần lớn người dùng không hiểu “revocation information”
- Lựa chọn không rõ ràng, người dùng không biết điều gì sẽ xảy ra khi chọn Yes/No

60

60

Dễ hiểu cho người dùng – Ví dụ

- Trên IE8


Source	 There is a problem with this website's security certificate.
Risk	The security certificate presented by this website was not issued by a trusted certificate authority. Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
Choices	We recommend that you close this webpage and do not continue to this website. Click here to close this webpage. Continue to this website (not recommended). More information
Process	<ul style="list-style-type: none">• If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.• When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.• If you choose to ignore this error and continue, do not enter private information into the website. <p>For more information, see "Certificate Errors" in Internet Explorer Help.</p>

61

61

Dễ hiểu cho người dùng – Ví dụ

- Google Chrome

Risk	
Explanation	Your connection is not private Attackers might be trying to steal your information from expired.badssl.com (for example, passwords, messages, or credit cards). Learn more NET::ERR_CERT_DATE_INVALID <input checked="" type="checkbox"/> Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy
Choices	Advanced Back to safety

62

62

Dễ hiểu cho người dùng – Ví dụ

- Google Chrome

Process

Choices

The screenshot shows a Chrome security warning dialog. At the top, there is a checkbox labeled 'Help improve Safe Browsing by sending some system information and page content to Google.' with a link to 'Privacy policy'. Below this is a 'Hide advanced' button. To the right is a 'Back to safety' button. The main text of the warning states: 'This server could not prove that it is expired.badssl.com; its security certificate expired 1,483 days ago. This may be caused by a misconfiguration or an attacker intercepting your connection. Your computer's clock is currently set to Saturday, May 4, 2019. Does that look right? If not, you should correct your system's clock and then refresh this page.' At the bottom, there is a link that says 'Proceed to expired.badssl.com (unsafe)'.

63

63

Một số nguyên tắc(tiếp)

- Mặc định an toàn (Fail-safe default): nếu có ngoại lệ xảy ra, hệ thống cần xử lý mặc định sao cho đầu ra là an toàn
 - Sử dụng danh sách trắng(white list) thay vì danh sách đen (black list)
 - Sử dụng cơ chế mặc định từ chối (default-deny policies)
 - Khi một đối tượng được khởi tạo, mặc định quyền truy cập của nó là rỗng
 - Sao lưu (backup)
 - ...

64

64

Một số nguyên tắc(tiếp)

- Kiểm soát tất cả truy cập



65

65

Kiểm tra tất cả truy cập

- Time Of Check To Time Of Use: TOCTTOU
 - Lỗi hỏng tranh đua điều kiện (Race Condition)

```
procedure withdrawal(w)
// contact central server to get balance
1. let b := balance
2. if b < w, abort
// balance could have decreased at this point
// contact server to set balance
3. set balance := b - w
4. dispense $w to user
```

Điều gì xảy ra nếu thủ tục trên được gọi trên các luồng thực thi song song?

66

66

Một số nguyên tắc (tiếp)

- Bảo vệ theo chiều sâu (Defense in depth): tạo ra nhiều lớp bảo vệ khác nhau cho tài nguyên
- Kẻ tấn công cần phải phá vỡ tất cả các lớp bảo vệ
- Tuy nhiên, sẽ làm gia tăng chi phí và ảnh hưởng tới hiệu năng của hệ thống

67

67

Bảo vệ theo chiều sâu



68

68

Bảo vệ theo chiều sâu



69

69

Một số nguyên tắc (tiếp)

- Mức độ an toàn của hệ thống tương đương mức độ an toàn ở thành phần yếu nhất
- Thiết kế mở: Không phụ thuộc vào các giải pháp an toàn bảo mật dựa trên việc che giấu mọi thứ ("security through obscurity")
 - Shannon's Maxim: "The Enemy Knows the System"

70

70

Một số nguyên tắc (tiếp)

- Security is process, not service
- AT-ANTT là quá trình, không phải dịch vụ
 - Thiết kế AT-ANTT ngay từ đầu

71

71

5. CƠ SỞ TÍNH TOÁN ĐƯỢC TIN CẬY (TRUSTED COMPUTING BASE)

72

72

Trusted Computing Base(TCB)

- TCB: Là một tập con của hệ thống, bao gồm phần cứng, phần mềm, mà hệ thống dựa vào nó để đạt được các mục tiêu AT-ANTT
 - Các thành phần của TCB luôn tuân thủ chính sách AT-ANTT của hệ thống
- TCB được xây dựng để đảm bảo chính sách AT-ANTT được giữ vững ngay cả khi các thành phần ngoài TCB xâm phạm chính sách
- TCB phải đủ lớn để không có thành phần nào ngoài nó có thể xâm phạm AT-ANTT của hệ thống
- Trusted Path: là một kênh truyền thông mà các thành phần trên kênh đó có thể tin cậy lẫn nhau

73

73

TCB – Ví dụ

- Giả sử mục tiêu AT-ANTT là những người dùng được cấp quyền có thể sử dụng Teamviewer để điều khiển máy tính từ xa.
- TCB có thể gồm những gì?

74

74

Trusting trust?

- “Reflections on Trusting Trust” – Ken. Thompson
 - Nếu tin tưởng vào các chương trình thực thi?
 - ✓ Ví dụ: #login
 - ✓ RedHat có đáng tin không?
 - ✓ Mật khẩu của người dùng có gửi đi đâu không?
 - Nếu không tin tưởng
 - ✓ Kiểm tra mã nguồn hoặc tự viết lại mã nguồn
 - ✓ Vấn đề đã được giải quyết?
- Chúng ta tin cậy vào cái gì?
- Có thể lấy rất nhiều ví dụ khác...



75

75

TCB

- Thiết kế AT-ANTT cho hệ thống luôn phải chỉ ra được các thành phần trong TCB
- Yêu cầu với TCB:
 - Không thể vòng tránh(unbypassable)
 - Chống sửa đổi (Tamper-resistant)
 - Có thể thẩm tra (Verifiable)
- Thiết kế TCB sao cho đơn giản là rất quan trọng
 - Simple = Small

76

76

Thiết kế theo TCB – Ví dụ

- Bài toán: Xây dựng một hệ thống lưu trữ bản sao của thư điện tử (email) được gửi đi từ các nhân viên
- Yêu cầu: Các bản lưu trữ không thể bị xóa (append-only)

77

77

Bài giảng có sử dụng hình ảnh từ các khóa học:

- Computer and Network Security, Stanford University
- Computer Security, Berkeley University

78

78