



1

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%
- MOOC: <https://soict.daotao.ai/courses/course-v1:SoICT+IT4015+TungBT/course/>



ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

2

2

1

Quy định điểm quá trình

- Điểm QT = 0.75*Điểm thi GK + 0.25*Điểm bài tập về nhà + Chuyên cần
- Bài tập về nhà:
 - Trắc nghiệm trên hệ thống MOOC
 - Được làm lại nhiều lần
 - Điểm bài tập về nhà = $10 \times$ Tỉ lệ số câu đúng

Điểm chuyên cần

- Điểm chuyên cần gồm 2 thành phần:
 $\text{Điểm chuyên cần} = \text{Điểm kỳ A} + \text{Điểm kỳ B}$
 - Nếu Điểm chuyên cần > 1: Điểm chuyên cần = +1
 - Nếu Điểm chuyên cần < -2: Điểm chuyên cần = -2
 - Tổng số buổi không đạt = 4: Điểm chuyên cần = -1
- Điểm bài trắc nghiệm > 50% được coi là đạt
- Điểm thành phần:
 - Đạt tất cả các bài trắc nghiệm: +1
 - Không đạt 1-2 bài: 0
 - Không đạt 3-4 bài: -1
 - Không đạt ≥5 bài: -2

Thông tin giảng viên

Bùi Trọng Tùng,
Khoa Kỹ thuật máy tính, trường CNTT-TT, BKHN
Email: tungbt@soict.hust.edu.vn
Địa chỉ: phòng 405, nhà B1
FB: <https://www.facebook.com/tungbui.hust>



5

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: Một số vấn đề an toàn - an ninh hệ thống
- Mở rộng: blockchain, ẩn danh, quyền riêng tư



6

6

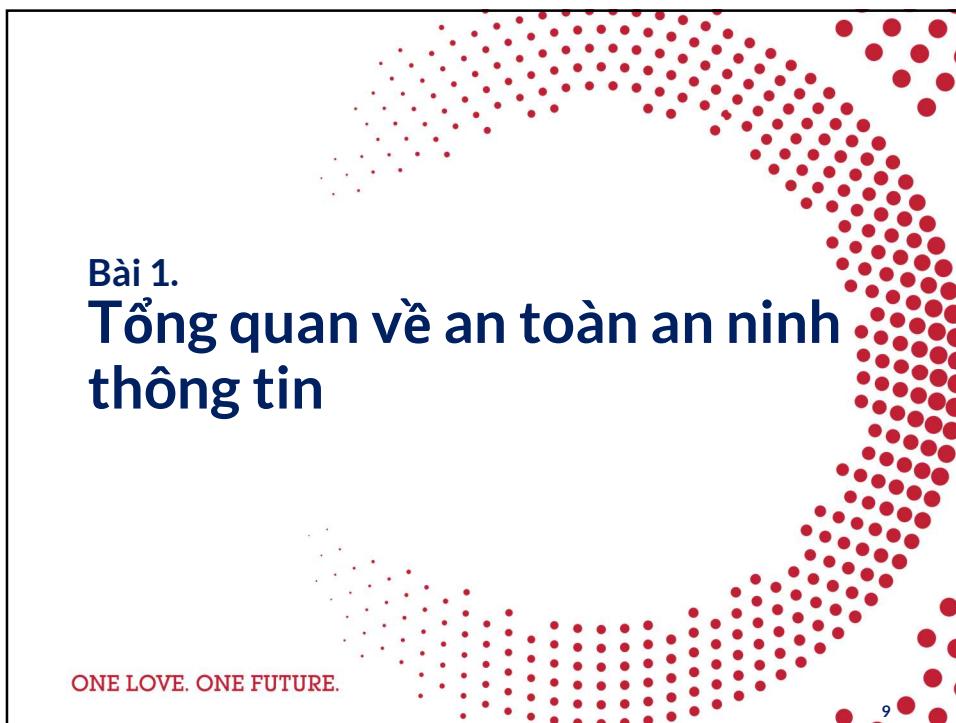
3

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

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



9

Nội dung

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





11

1. Mở đầu

- Báo cáo về an toàn an ninh thông tin:
 - IBM X-Force Threat Intelligence Index 2024
 - Verizon 2024 Data Breach Investigations Report
 - Microsoft Digital Defense Report 2024
 - Viettel Threat Intelligence 2024



ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

12

12

Tấn công AT-ANTT là phổ biến

- Thứ gì có thể hack được?

For The First Time, Hackers Have Used A Refrigerator To Attack Businesses

JULIE BORT | Jan. 16, 2014, 1:36 PM | 195,469 | 39

46%
Of the 78% of IoT devices with known vulnerabilities on customer networks, 46% cannot be patched.

32%

57%
of devices on legacy firmware are exploitable to a high number of CVEs (

Find out more on page 81

IF IT CAN KILL YOU
DON'T CONNECT IT TO THE INTERNET!

imgflip.com

ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

13

13

Tấn công AT-ANTT là phổ biến

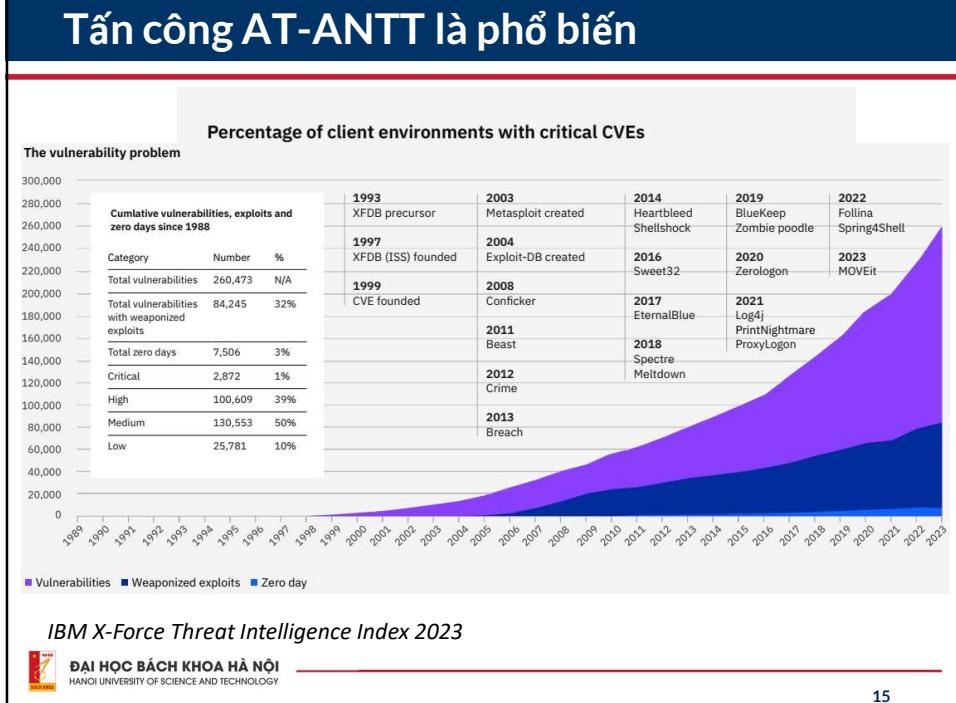
- Đánh cắp thông tin cá nhân



14

14

Tấn công AT-ANTT là phổ biến



15

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



ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

16

16

An toàn an ninh thông tin là gì?

- Yêu cầu tính đúng đắn: hệ thống xử lý đầy đủ và chính xác với mọi giá trị đầu vào
- AT-ANTT: là một dạng của tính đúng đắn, nhưng “chặt” hơn
 - Hệ thống có khả năng phát hiện và ngăn chặn các giá trị đầu vào độc hại và đầu ra không mong muốn
 - Rất dễ để xử lý một yêu cầu bất kỳ nhưng rất khó để xác định các yêu cầu có dữ liệu độc hại
 - Đạt được tính đúng đắn ngay trong ngữ cảnh có sự hiện diện của kẻ tấn công
 - Rất dễ để xử lý yêu cầu mà không quan tâm đến ngữ cảnh nhưng rất khó để xác định yêu cầu đến từ nguồn trái phép

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
- An ninh quốc gia
- ...

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 Travel

UK news World news Royals Health Defence Science Education Investors

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 / 6:05 PM / 3 YEARS AGO

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

Jim Finkle 2 MIN READ

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

2805

ĐẠI HỌC BÁCH KHOA HÀ NỘI HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

19

19

Đánh cắp thông tin cá nhân

British Airways faces record \$230 million fine over data theft

Paul Sandle 2 MIN READ

CONG NHIEU

Vụ rò rỉ hơn 163 triệu tài khoản Zing ID: Chủ các tài khoản nên thay đổi mật khẩu

DuoLingo (2.6 Million Entries) Scrape by House - Tuesday January 24, 2023 at 02:18 AM

House Email, joinedDate, shakeToReport, hasRecentActivity

Post: 46 Threads: 7 Joined: Jul 2022 Reputation: 637

Jon Fingas Reporter Sun, Apr 4, 2021 • 1 min read

Personal data for 533 million Facebook users leaks on the web

It had been circulating privately since January.

2 triệu dữ liệu ngân hàng nghi bị hacker đánh cắp

Anh Vũ Mai Hà

ngendt@gmail.com maha01@gmail.com

10:47 - 22/11/2019 - 0 | THANH NIEN ONLINE

Một Ngân hàng TMCP vừa bị các hacker "điểm danh" khi tuyên bố đang nắm trong tay 2 triệu dữ liệu khách hàng.

g: Cảnh báo bảo mật camera

ĐẠI HỌC BÁCH KHOA HÀ NỘI HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

20

20

10

Đánh cắp tài sản

tuoitre 2020

Người phụ nữ ở TP HCM mất 1,2 tỉ đồng chỉ vì nhấp vào đường link trên Zalo

09-03-2021 - 03:47 PM | Pháp luật

TUYỂN SINH

VNEXPRESS | Thứ tư, 17/3/2021

Mới nhất | International |

Góc nhìn | Thế giới | Video | Kinh doanh | Giải trí | Thể thao | Pháp luật | Giáo dục | Sức khỏe | Đời sống | Du lịch |

Kính doanh | Ebank | Ngân hàng

Thứ ba, 12/5/2020, 18:07 (GMT+7)

Tài khoản 'bốc hơi' gần 850 triệu vì vào đường link lạ

Sau khi đăng nhập vào đường link lạ do kẻ gian gửi, tài khoản ngân hàng của bà Hoa tại Vietinbank đã bị chiếm đoạt 848 triệu đồng.

Bà Hoàng Thị Hoa (nguồn 7) cho biết, rạng sáng 21/3 cô nhận được tin nhắn để nghỉ thuê nhà 6 tháng từ một tài khoản trên mạng xã hội. Người này xưng tên Phạm Hồng Mis, đang ở Mỹ và đề nghị bà Hoa đưa số tài khoản để chuyển tiền cọc giữ chỗ 240 USD.

11/22 - 12/05/2016

THÀNH NIÊN

TÀI CHÍNH - KINH DOANH

KINH TẾ XANH | CHÍNH SÁCH - PHÁT TRIỂN | NGÂN HÀNG | CHỨNG KHOẢN | DOANH NGHIỆP | DOANH NHÂN | TIỀU DÙNG

54 triệu đồng trong tài khoản Eximbank "bốc hơi"

Đăng nhập vào đường link lạ, tài khoản của bà Trang lập tức bị "bốc hơi" 54 triệu đồng trong chốc lát.

12/04 - 06/02/2020 - C

ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

21

21

Tác động tới các tổ chức

Share of attacks by industry 2019–2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

IBM X-Force Threat Intelligence Index 2024

ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

22

22

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

Loại hình gian lận	Tỷ lệ (%)
Khác	7%
Vi phạm luật cạnh tranh/luật chống độc quyền	7%
Ăn cắp Tài sản Trí tuệ	7%
Giao dịch nội gián	9%
Gian lận thuế	13%
Rửa tiền	16%
Gian lận nhân lực	16%
Tội phạm mạng	20%
Gian lận kế toán	22%
Gian lận mua sắm	24%
Vi phạm đạo đức kinh doanh	29%

VÀO ĐIỆN TỬ **ĐÀI TRUYỀN HÌNH VIỆT NAM** **VTVCENTER** **NEWS**

TRANG CHỦ | KHO DOANH | CHÍNH TRỊ | XÃ HỘI | QUẦN SỰ | THẾ GIỚI | PHÁP LUẬT | TRUYỀN HÌNH ATV | XE | ĐỜI SỐNG | VĂN HÓA

TRANG CHỦ | KHO DOANH | CHÍNH TRỊ | XÃ HỘI | QUẦN SỰ | THẾ GIỚI | PHÁP LUẬT | TRUYỀN HÌNH ATV | XE | ĐỜI SỐNG | VĂN HÓA

KINH TẾ

Năm 2017, tội phạm mạng gây thiệt hại cho kinh tế Việt Nam 12.700 tỷ đồng

Trung tâm Tin tức VTV24 | Thứ ba, ngày 27/03/2018 09:36 GMT+7

ĐẠI HỌC BÁCH KHOA HÀ NỘI

HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

Thiết hại khoảng 20 nghìn tỷ đồng do virus máy tính

ANTD.VN - Theo ước tính của Tập đoàn công nghệ Bkav, năm 2019, thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên tới 20.892 tỷ đồng (902 triệu USD), vượt xa con số 14.900 tỷ đồng của năm 2018.

23

Tác động tới nền kinh tế

McAfee
Together is power.

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.

ĐẠI HỌC BÁCH KHOA HÀ NỘI

HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

24



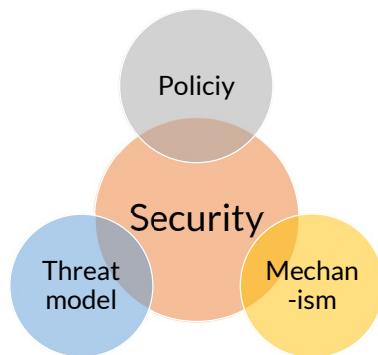
25



26

AT-ANTT là gì?

- Bao gồm các khía cạnh:
 - Chính sách
 - Mô hình đe dọa
 - 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 thực hiện
 - Hành vi phải thực hiện/được phép/không được phép
 - Tài nguyên



Mục tiêu: Mô hình CIA

- Confidentiality (Bí mật): tài nguyên chỉ được tiếp cận bởi các bên được cấp quyền
- Integrity (Toàn vẹn): tài nguyên chỉ được sửa đổi bởi các bên được cấp quyền
- Availability (Sẵn sàng): tài nguyên sẵn có để đáp ứng 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

Mục tiêu: Mô hình 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,. VD: 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

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: Tỉ lệ cảnh báo sai
 - False negative rate: Tỉ lệ bỏ sót tấn công
- Cần phát hiện những dạng xâm phạm không thể ngăn chặn

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(Auditing)
- Sao lưu và khôi phục (Backup and Recovery)
- Dự phòng (Redundancy)
- Giả lập, ngụy trang (Deception)
- Gây nhiễu, ngẫu nhiên(randomness)

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?
- 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

$$\text{Risk} = \text{Threat} \times \text{Impact}$$

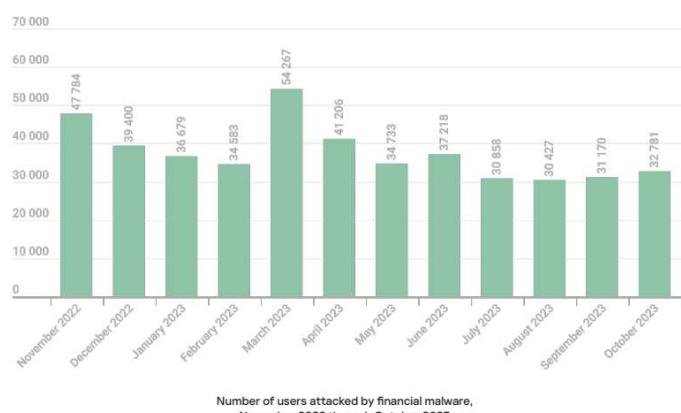
- Lỗ hổng (Vulnerability): là những điểm yếu trong hệ thống có thể bị khai thác, lợi dụng để gây tổn hại cho hệ thống
 - <https://www.cvedetails.com/>
 - Tầm soát lỗ hổng định kỳ là một trong những giải pháp phòng chống tấn công

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

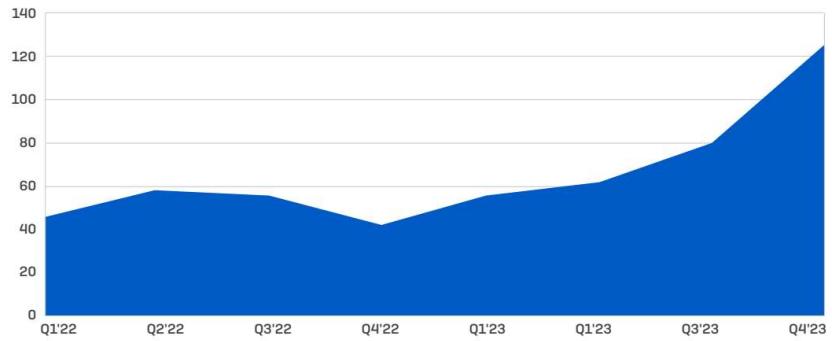
Động cơ tấn công

- Tiền bạc

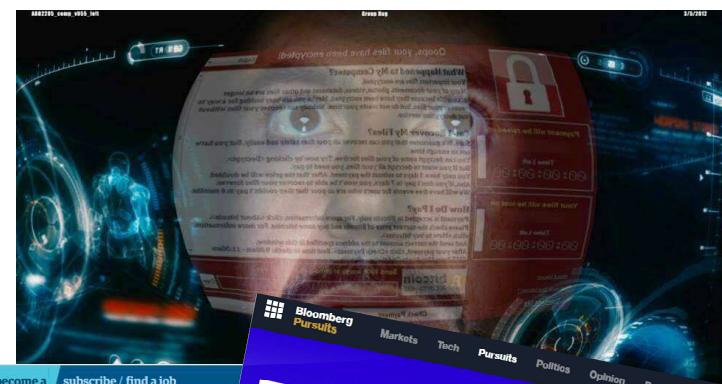


Ransomware(2024)

Remote ransomware incidents, 2022-2023



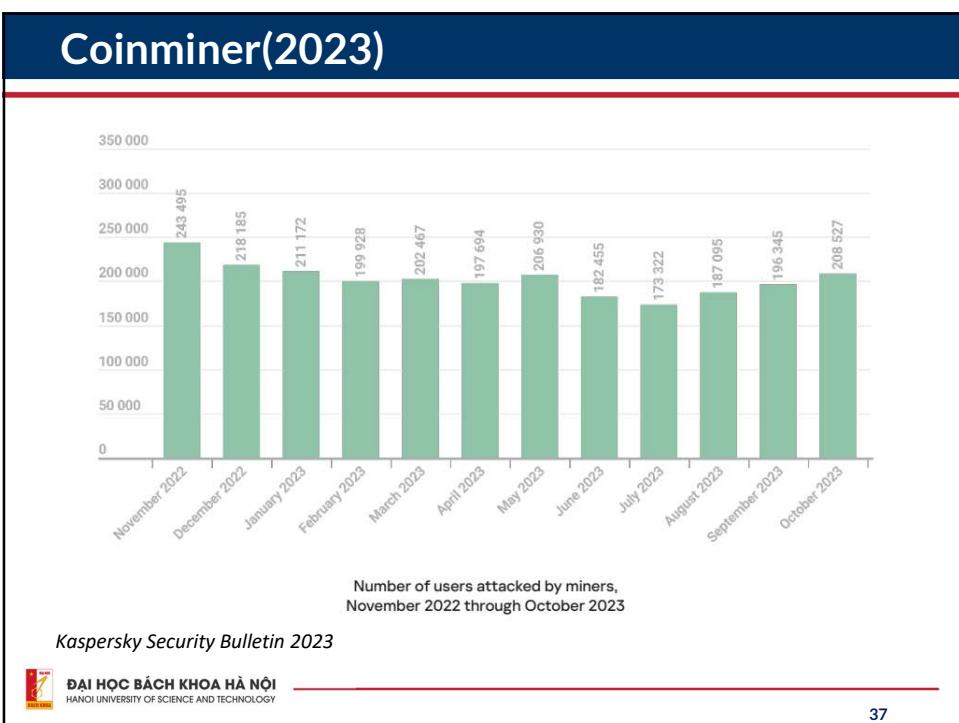
WannaCry (05/2017)



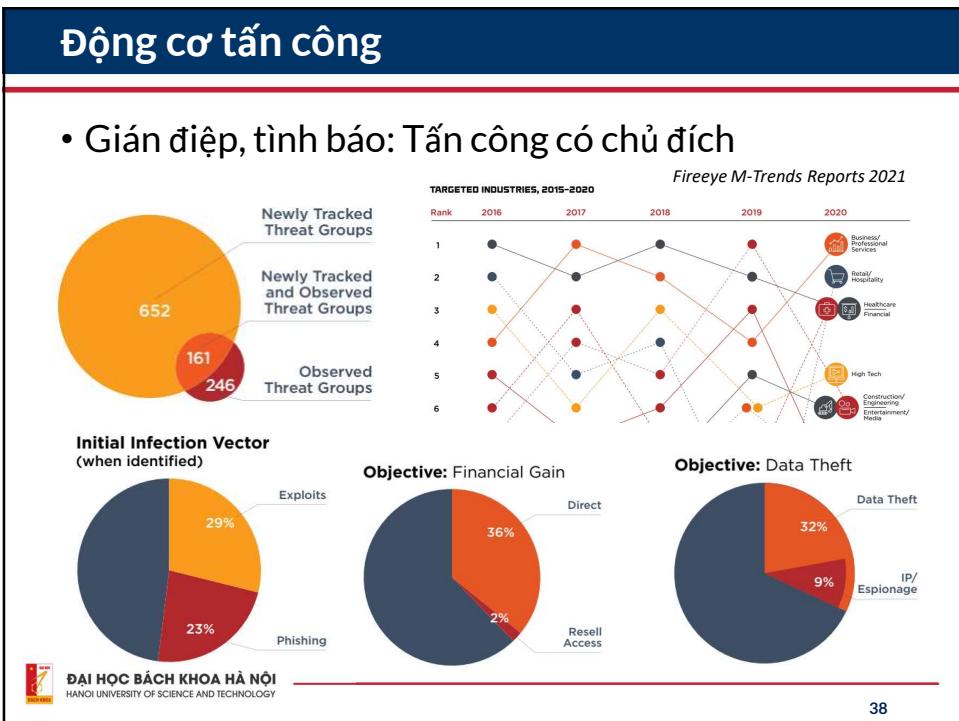
become a supporter / subscribe / find a job
news / opinion / sport / arts /
tech / world / UK / science / cities / global
Malware

WannaCry: hackers withdraw £108,000 or
bitcoin ransom

**Next WannaCry Cyber Attack Could
Cost Insurers \$2.5 Billion**



37

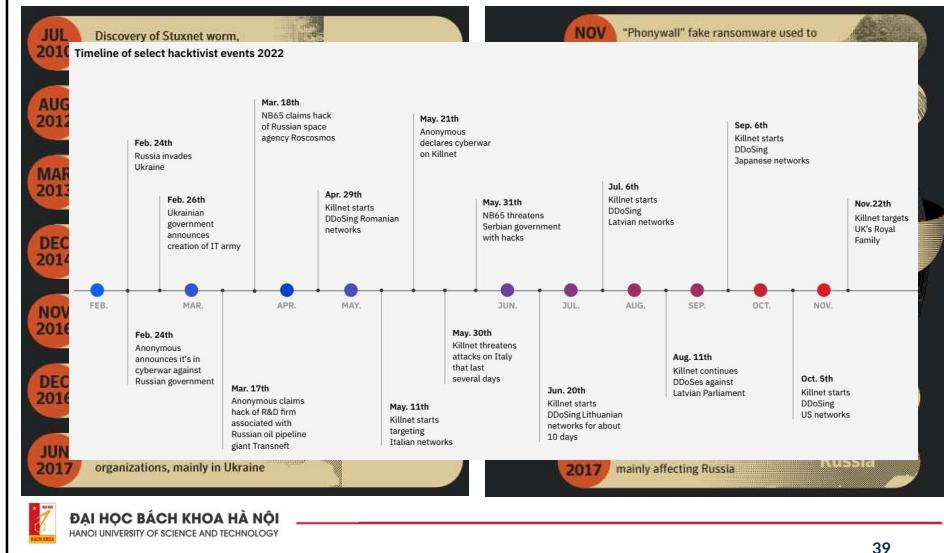


38

19

Động cơ tấn công

- Mục đích chính trị



39

Động cơ tấn công

- Đùa cợt



- Thú vui phá hoại



40

Những giả định về tấn công

- Những giả định này là bi quan nhưng là sự cần thiết
- Kẻ tấn công luôn có cơ hội thành công và kiên trì tới khi đạt được mục đích
- 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,...)

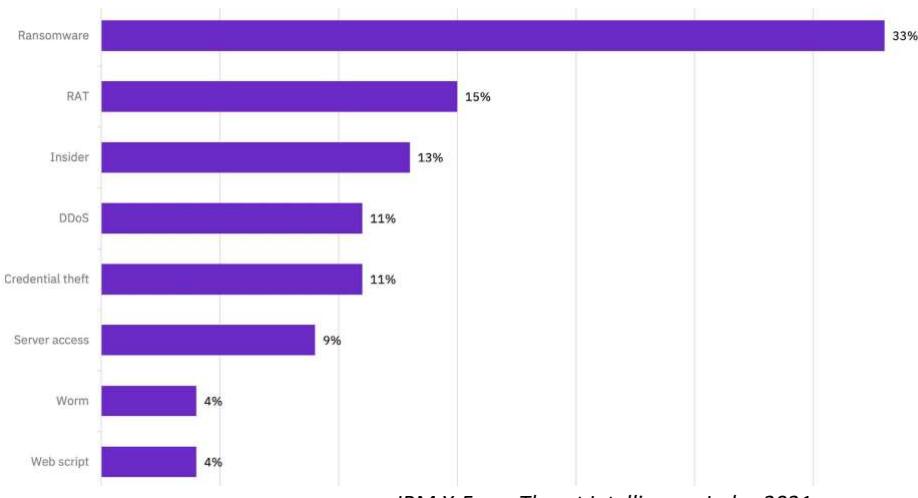
Những giả định về tấn công(tiếp)

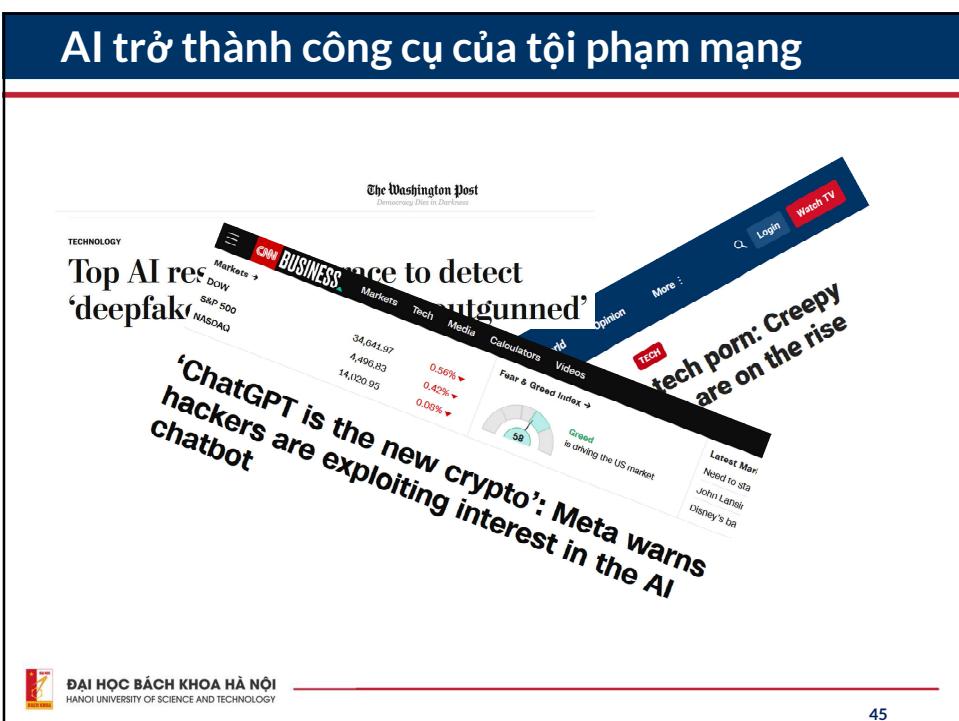
- Kẻ tấn công có thể truy cập vào hệ thống tương tự để xác định được cách thức hệ thống hoạt động như thế nào
- Kẻ tấn công có thể có một số quyền truy cập nhất định nào đó trên hệ thống mục tiêu
- Kẻ tấn công có khả năng tự động hóa các hành vi tấn công
- Kẻ tấn công có khả năng phối hợp, điều phối các hệ thống/thành phần khác nhau
- Kẻ tấn công có nguồn tài nguyên tính toán rất lớn

Phân loại tấn công

- Tấn công thụ động(passive attack) và tấn công chủ động(active attack)
 - Tấn công thụ động: không can thiệp, làm thay đổi hoạt động của hệ thống
 - Tấn công chủ động: can thiệp, làm thay đổi hoạt động của hệ thống
- Tấn công có chủ đích(targeted attack/APT attack) và tấn công không có chủ đích(non-targeted attack)
 - Tấn công có chủ đích: mục tiêu đã xác định
 - Tấn công không có chủ đích: mục tiêu bất kỳ
- Tấn công bên trong và tấn công bên ngoài

Một số dạng tấn công phổ biến





45



46

Quy trình xây dựng

4 giai đoạn:

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

Quy trình xây dựng

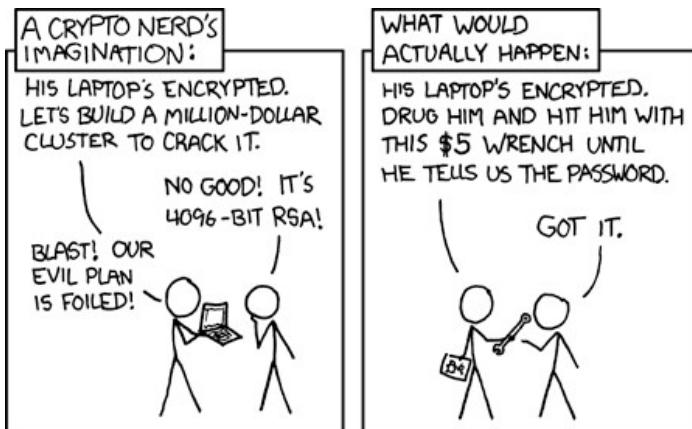
- Xây dựng chính sách: có thể mô tả ban đầu bằng ngôn ngữ tự nhiên:
 - Hành vi phải thực hiện/được phép/ không được phép
 - Chủ thể của hành vi
 - Đối tượng hành vi tác động tới
 - Điều kiện
- Xây dựng các tình huống lạm quyền minh họa cho sự xâm phạm chính sách
- Chính sách AT-ANTT phải phù hợp với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

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)

Xây dựng mô hình đe dọa

- AT-ANTT trên thực tế khác với lý thuyết



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°C trong thời gian tối thiểu 30 phút khi nhiệt độ bên ngoài > 1000°C
 - Bảo vệ tài sản ở nhiệt độ bên trong < 55°C trong thời gian tối thiểu 30 phút khi nhiệt độ bên ngoài > 1000°C

→ Chọn mua két sắt loại nào?



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



Một số nguyên tắc

- AT-ANTT là bài toán kinh tế(Security is Economics): 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

AT-ANTT là bài toán kinh tế - Ví dụ

TL-15
(3.000\$)



TL-30
(4.500\$)



TRTL-30
(10.000\$)



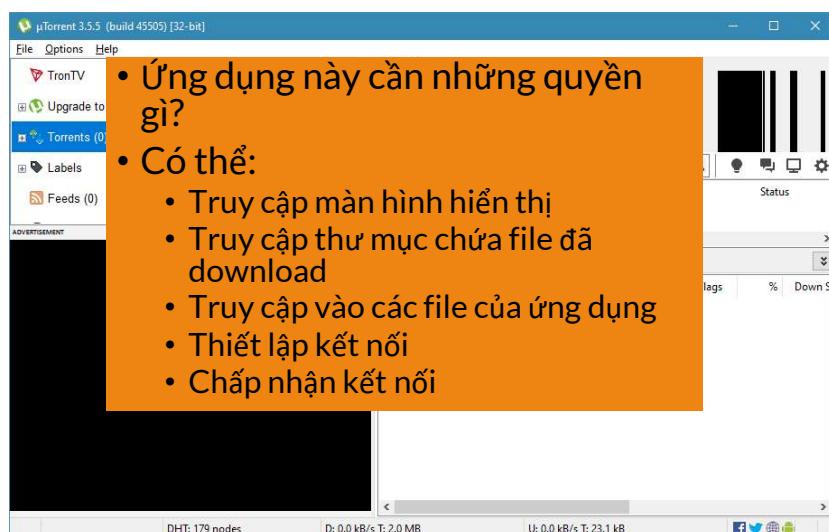
TXTL-60
(>50.000\$)



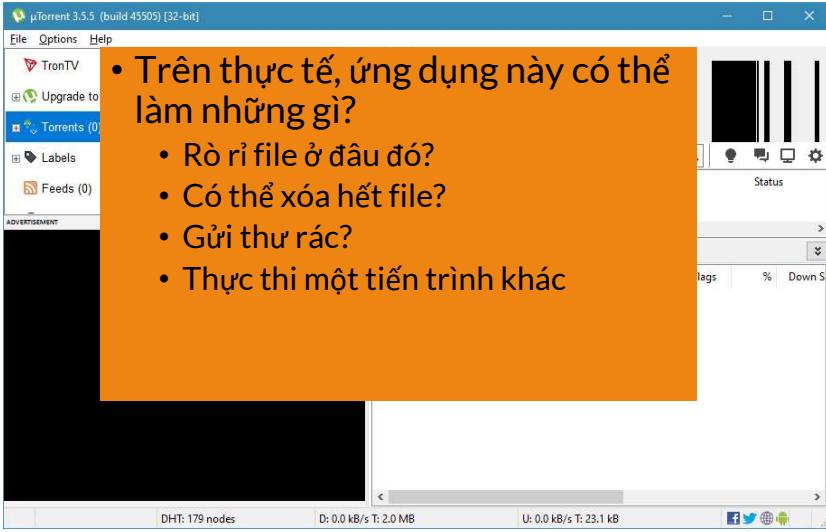
Một số nguyên tắc(tiếp)

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

Tối thiểu hóa quyền – Ví dụ



Tối thiểu hóa quyền



- Trên thực tế, ứng dụng này có thể làm những gì?
 - Rò rỉ file ở đâu đó?
 - Có thể xóa hết file?
 - Gửi thư rác?
 - Thực thi một tiến trình khác

DHT: 179 nodes D: 0.0 kB/s T: 2.0 MB U: 0.0 kB/s T: 23.1 kB

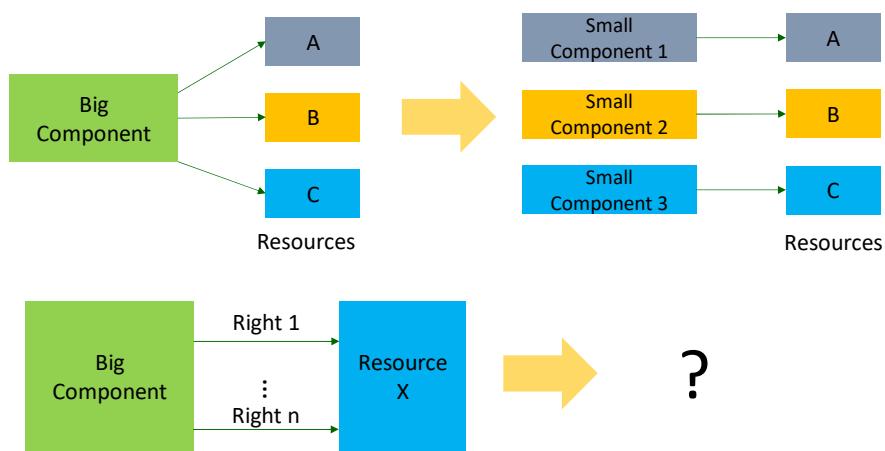
ĐẠI HỌC BÁCH KHOA HÀ NỘI HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

57

57

Phân chia quyền (Privilege separation)

- Phân chia hệ thống sao cho các thành phần được cấp quyền nhỏ nhất có thể.



58

58

Chia sẻ trách nhiệm(Separation of responsibility)

- Quyền chỉ được thực thi khi có yêu cầu đồng thời từ nhiều bên



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(Usable):
 - 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!

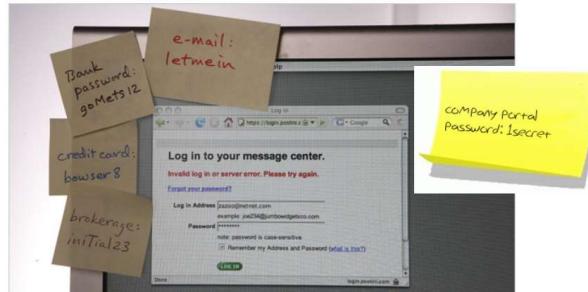
→Complexity is the enemy

Dễ hiểu, dễ sử dụng cho người dùng – Ví dụ

Thứ mà admin nhìn thấy



Thứ mà user nhìn thấy



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

Dễ hiểu cho người dùng – Ví dụ

• Trên IE8

Source



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Risk

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

- 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.

For more information, see "Certificate Errors" in Internet Explorer Help.



ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

63

63

Dễ hiểu cho người dùng – Ví dụ

• Google Chrome

Risk



Your connection is not private

Explanation

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

Choices

Help improve Safe Browsing by sending some [system information and page content](#) to Google.
[Privacy policy](#)

[Advanced](#)

[Back to safety](#)



ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

64

64

Dễ hiểu cho người dùng – Ví dụ

- Google Chrome

Process

Choices

Help improve Safe Browsing by sending some [system information and page content](#) to Google.
[Privacy policy](#)

[Hide advanced](#)

[Back to safety](#)

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.

[Proceed to expired.badssl.com \(unsafe\)](#)



ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

65

65

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)
 - ...



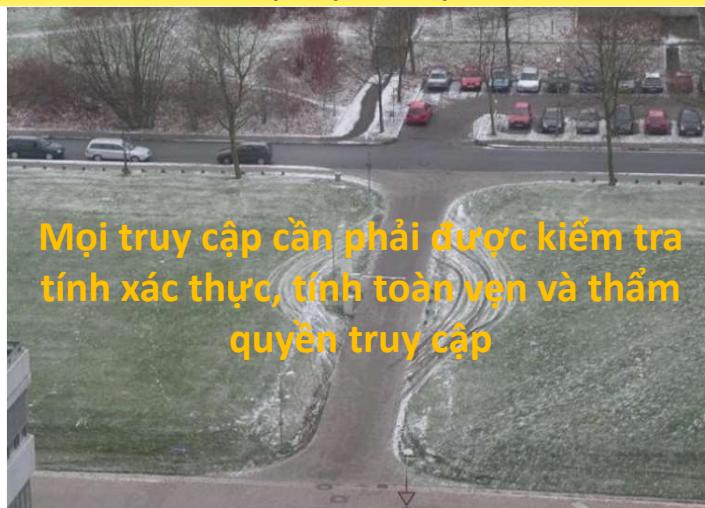
ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

66

66

Một số nguyên tắc(tiếp)

- Kiểm soát tất cả truy cập(Complete mediation)



ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

67

67

Kiểm tra tất cả truy cập

- Time Of Check To Time Of Use: TOCTTOU
 - Lỗi hổng 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?



ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

68

68

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



Một số nguyên tắc (tiếp)

- An toàn của hệ thống đặt tại mắt xích yếu nhất (weakest link)
- Thiết kế mở(Open Design): Không phụ thuộc vào các giải pháp an toàn bảo mật dựa trên việc che giấu mọi thứ ("security through obsecrity")
 - Shannon's Maxim: "The Enemy Knows the System"



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

4. Cơ sở tính toán được tin cậy (Trusted Computing Base)

ONE LOVE. ONE FUTURE.

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



TCB – Ví dụ

- Người dùng sử dụng dịch tin nhắn Zalo
- TCB có thể gồm những gì?



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 được gửi trái phép tới đâu không?
 - Nếu không tin tưởng
 - Kiểm tra mã nguồn hoặc tự viết lại mã nguồn
 - Vấn đề đã được giải quyết chưa?
- Chúng ta tin cậy vào cái gì?
- Có thể lấy rất nhiều ví dụ khác...



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

TCB – Ví dụ

- TPM (Trusted Platform Module)
- Apple Secure Enclave Processor
- Qualcomm Trusted Execution Environment
- Samsung TEEGRIS
- Huawei TrustedCore

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

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