Bài 1.

Tổng quan về an toàn an ninh thông tin

ONE LOVE. ONE FUTURE.

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

1. Mở đầu

ONE LOVE. ONE FUTURE.

3

1. Mở đầu

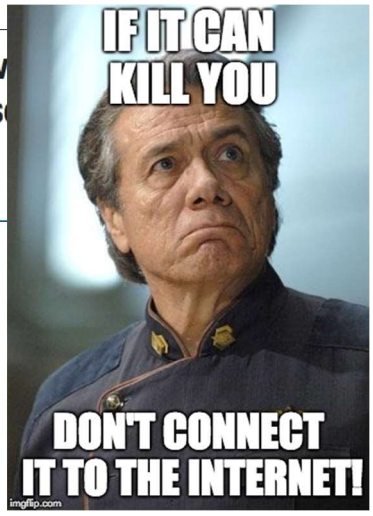
- Báo cáo về an toàn an ninh thông tin:
  - IBM X-Force Threat Intelligence Index 2022
  - Verizon 2022 Data Breach Investigations Report
  - Sophos 2022 Threat Report
  - Viettel Security - Báo cáo tình hình nguy cơ ATTT
  - http://www.networkworld.com/category/security0/

Tấn công AT-ANTT là phổ biến

- Thứ gì có thể hack được?

TOP DEVICE TYPES PERFORMING IOT ATTACKS (YEAR)

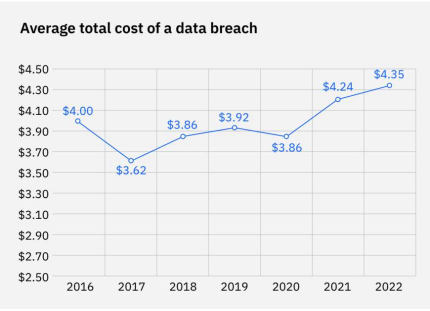
DEVICE TYPE	PERCENT
Router	75.2
Connected Camera	15.2
Multi Media Device	5.4
Firewall	2.1
PBX Phone System	0.6
NAS (Network Attached Storage)	0.6
VoIP phone	0.2
Printer	0.2
Alarm System	0.2
VoIP Adapter	0.1



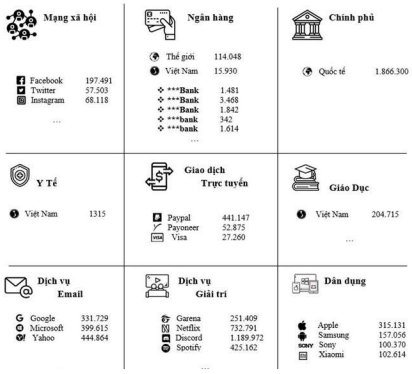
Symatec Internet Security Threat Report 2019

Tấn công AT-ANTT là phổ biến

- Đánh cắp thông tin cá nhân

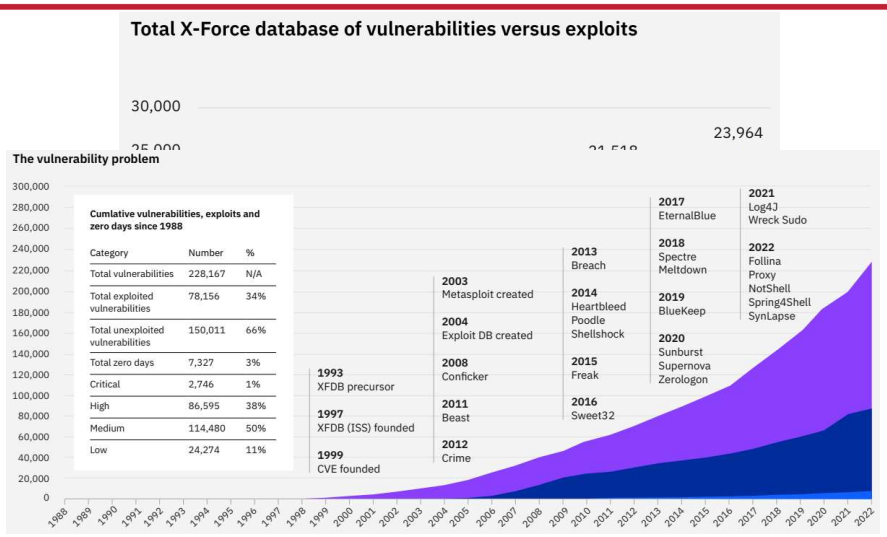


Data breach report – IBM 2023



Vitetel Threat Intelligence Report Q2,3/2022

Tấn công AT-ANTT là phổ biến



IBM X-Force Threat Intelligence Index 2023

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

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

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
- …

Nguy cơ với an toàn thân thể

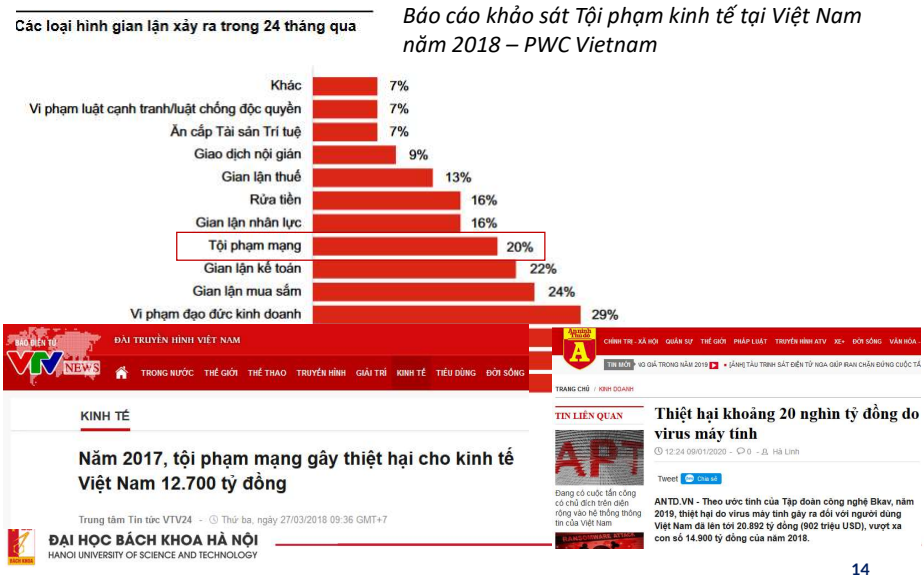
Đánh cắp thông tin cá nhân

Đánh cắp tài sản

13

13

Tác động tới nền kinh tế



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

14

14

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.

Xâm phạm chủ quyền quốc gia

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

Published time: 4 Jul, 2015 16:22 Get short URL

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

▲ Cables released by WikiLeaks allege communications from German chancellor Angela Merkel were intercepted. Photograph: Arben Çeli/Reuters

Người lao động

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

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

Về môn học này

- Mã học phần: IT4015/IT4010Q
- 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

Quy định điểm quá trình

- Điểm QT = 0.75*Điểm thi GK + 0.25*Điểm bài tập trắc nghiệm + Chuyên cần
- Điểm bài tập trắc nghiệm = Tỉ 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 MOOC

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

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

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

Chúng ta học gì?

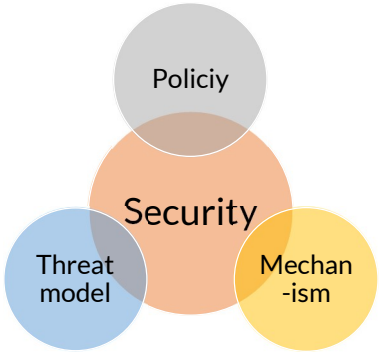
- Suy nghĩ về hệ thống thông tin như một kẻ tấn công
  - Xác định mối đe dọa và điểm yếu của hệ thống
- Làm cách nào để thực hiện một số kỹ thuật tấn công
  - Khai thác lỗ hổng phần mềm
- Suy nghĩ về hệ thống như người thiết kế giải pháp AT-ANTT
  - Cách thức ngăn chặn và giảm thiểu tấn công
  - Hiểu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

2. Khái niệm cơ bản trong AT-ANTT

ONE LOVE. ONE FUTURE.

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
  - 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 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

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: 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(Auditting)
- 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

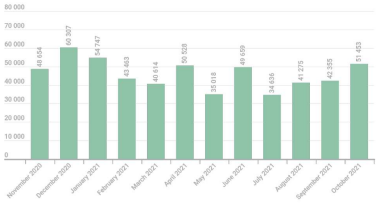
- Threat Model: mô tả những mối đe dọa kẻ tấn công có thể gây ra cho hệ thống và hậu quả
  - Cái gì cần bảo vệ?
  - Ai có thể tấn công vào hệ thống? Chúng có gì?
  - Hệ thống có thể bị tấn công như thế nào?
- Độ rủi ro (Risk): khả năng xảy ra các sự cố làm mất an toàn an ninh thông tin và thiệt hại của chúng cho hệ thống
- 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

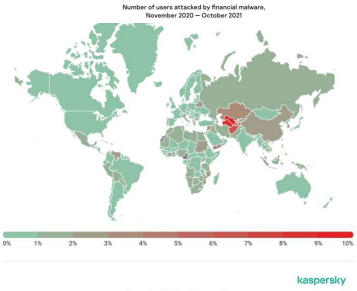
Ai có thể tấn công bạn?

- 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





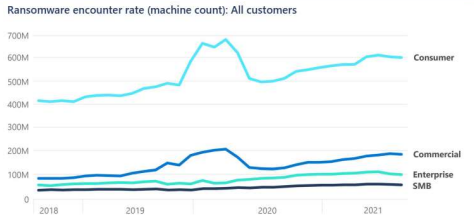
Kaspersky Security Bulletin 2021

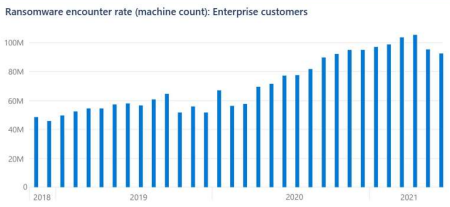
Top 10 financial malware

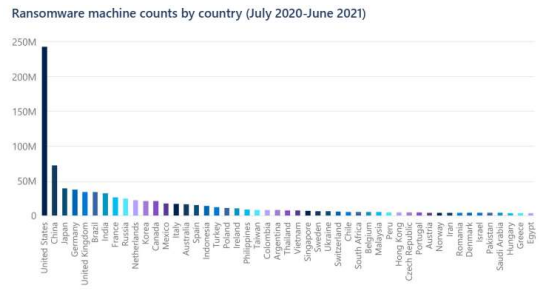
	Name
1	Zbot
2	CliptoShuffler
3	SpyEye
4	Trickster
5	RTM
6	Nimnul
7	Danabot
8	Cridex
9	Nymaim
10	Neurevt

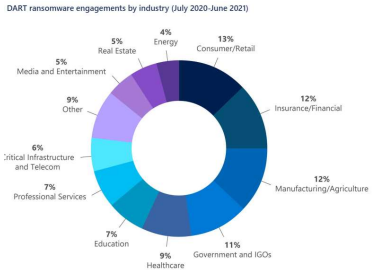
	Country*	%**
1	Turkmenistan	8.4
2	Afghanistan	6.7
3	Tajikistan	6.6
4	Uzbekistan	5.7
5	Yemen	3.1
6	Paraguay	2.9
7	Costa Rica	2.7
8	Sudan	2.4
9	Kazakhstan	2.2
10	Syria	2.2

Ransomware(2021)



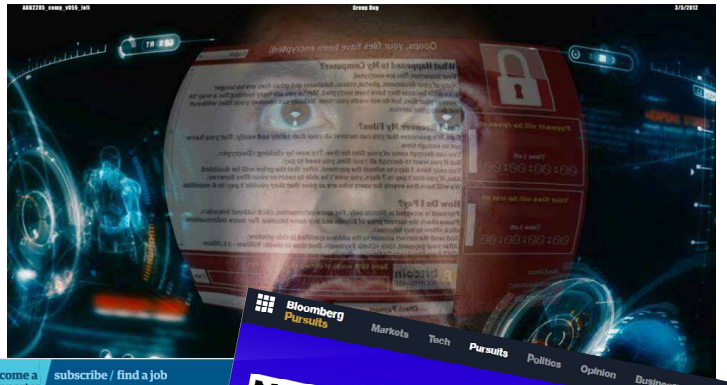






Microsoft Digital Defense Report 2021

WannaCry (05/2017)



become a supporter | subscribe / find a job

news / opinion / sport / arts /

tech / world / UK / science / cities / globa

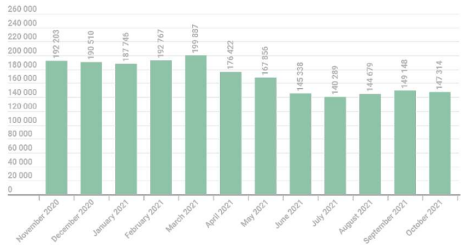
Malware

WannaCry: hackers withdraw £108,000 or bitcoin ransom

Bloomberg Pursuits | Markets | Tech | Pursuits | Politics | Opinion | Businessweek | Subscribe to Businessweek | Sign In

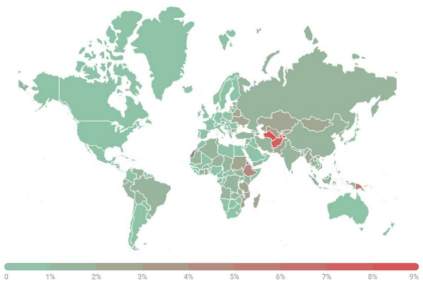
Next WannaCry Cyber Attack Could Cost Insurers $2.5 Billion

Coinminer(2021)



Number of users attacked by miners, November 2020 – October 2021

	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



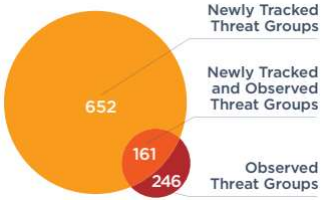
Geography of miner-related attacks, November 2020 – October 2021

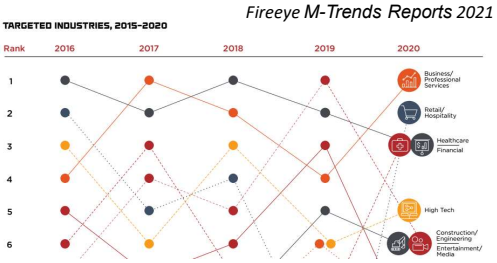
Kaspersky Security Bulletin 2020

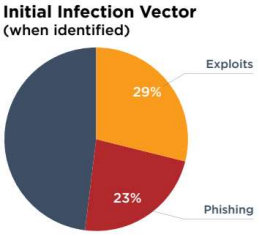
Động cơ tấn công

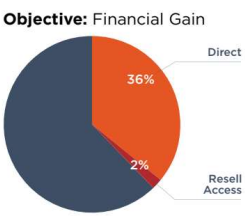
- Gián điệp, tình báo: Tấn công có chủ đích

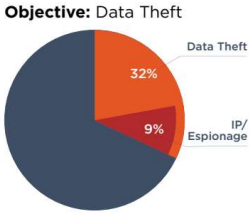
Fireeye M-Trends Reports 2021











Động cơ tấn công

- Mục đích chính trị

Động cơ tấn công

- Đùa cợt

- Thú vui phá hoại

Những giả định về tấn công

- Những giả định này là bi quan nhưng là sự cận trọng 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,…)

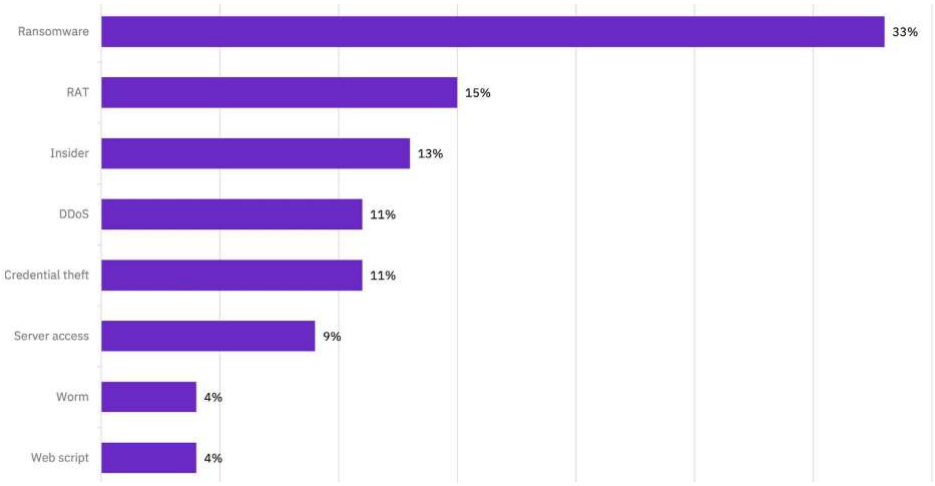
Những giả định về tấn công(tiếp)

- 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



IBM X-Force Threat Intelligence Index 2021

41

3. Xây dựng hệ thống AT-ANTT

ONE LOVE. ONE FUTURE.

42

Quy trình xây dựng

4 giai đoạn:

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

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

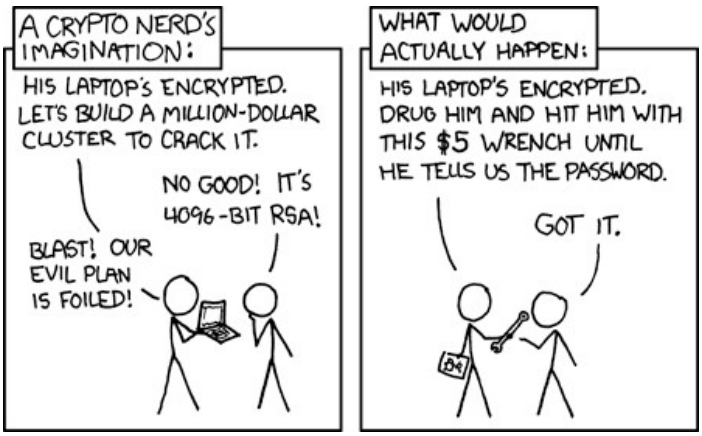
Quy trình xây dựng

- 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$)

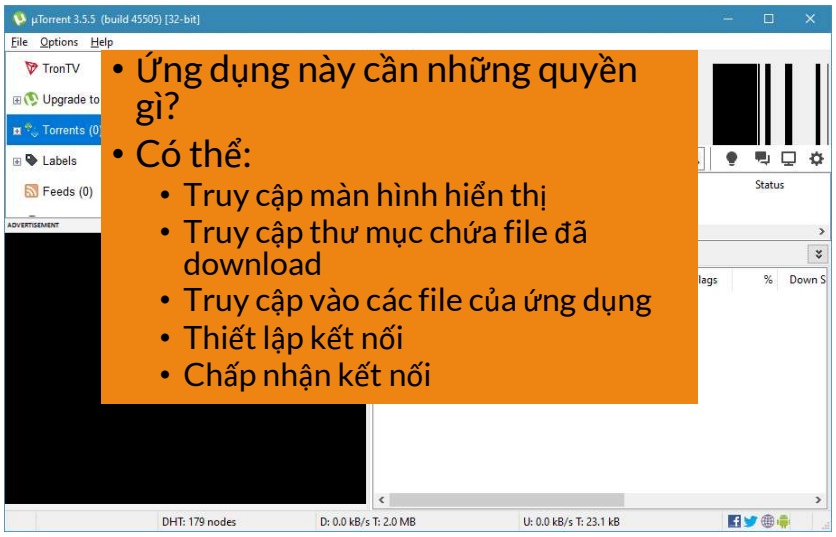
TRTL-30
(10.000$)

TXTL-60
(>50.000$)

Một số nguyên tắc(tiếp)

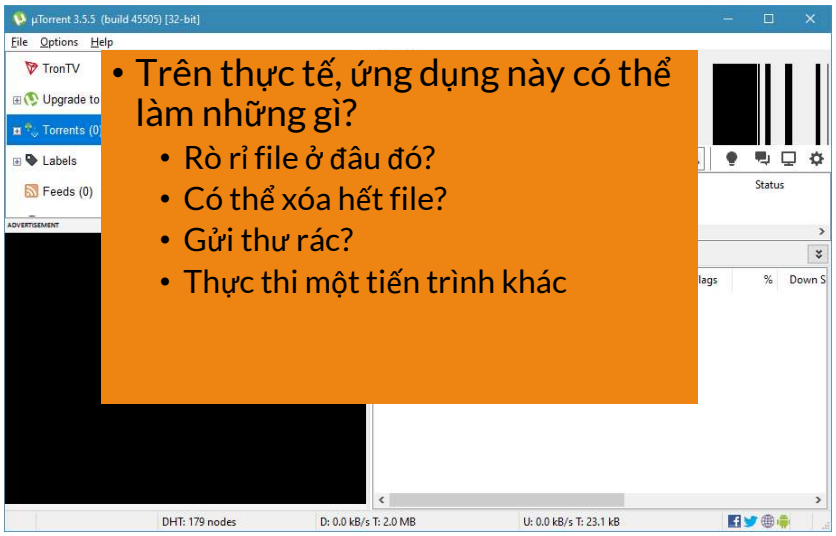
- Tối thiểu hóa quyền (Least privilege): không cấp quyền nhiều hơn những gì mà đối tượng cần để hoàn thành nhiệm vụ.

Tối thiểu hóa quyền – Ví dụ



- Ứng dụng này cần những quyền gì?
- Có thể:
  - Truy cập màn hình hiển thị
  - Truy cập thư mục chứa file đã download
  - Truy cập vào các file của ứng dụng
  - Thiết lập kết nối
  - Chấp nhận kết nối

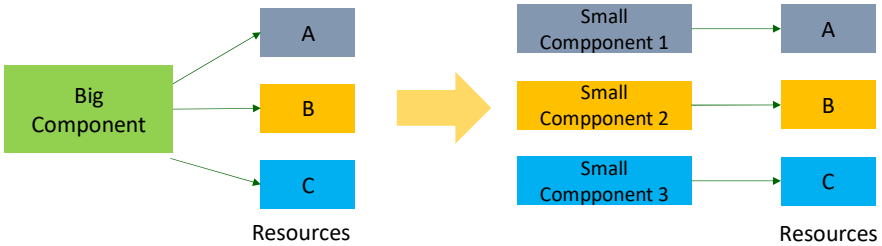
Tối thiểu hóa quyền

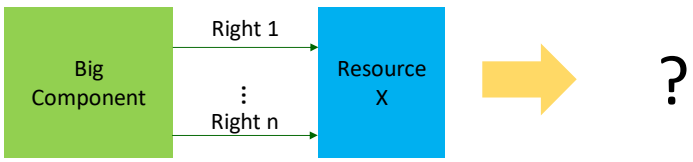


- Trên thực tế, ứng dụng này có thể làm những gì?
  - Rò rỉ file ở đâu đó?
  - Có thể xóa hết file?
  - Gửi thư rác?
  - Thực thi một tiến trình khác

Phân chia quyền (Privilege separation)

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





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.

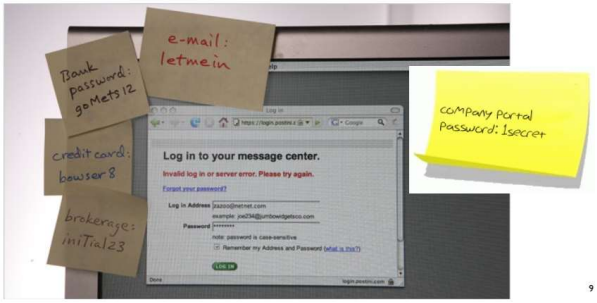
→KISS: Keep It Simple, Sir!

→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

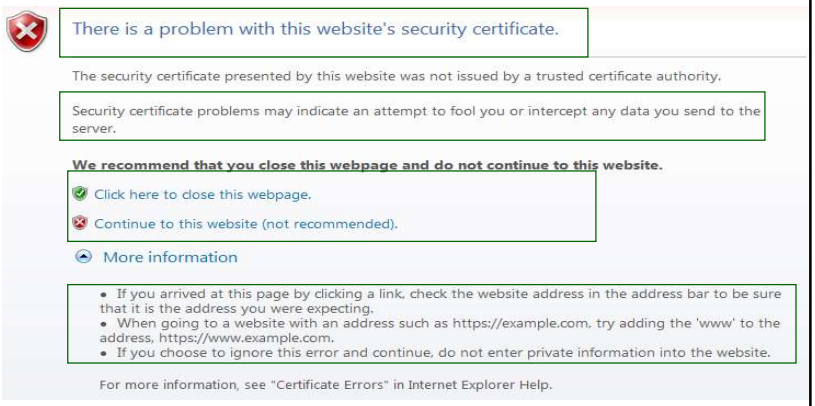
- Trên IE8

Source

Risk

Choices

Process



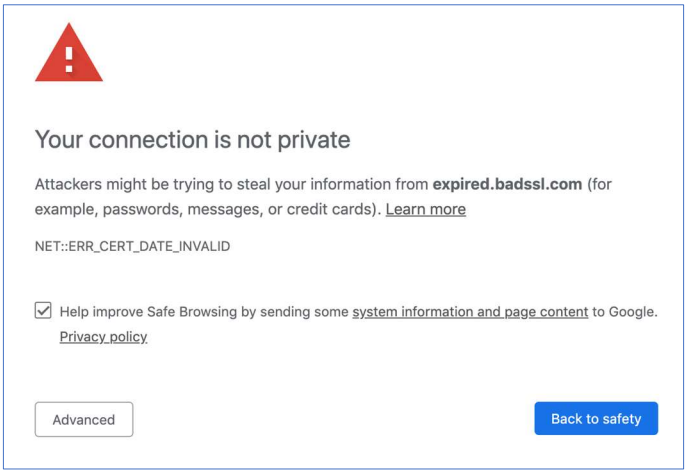
Dễ hiểu cho người dùng – Ví dụ

- Google Chrome

Risk

Explanation

Choices

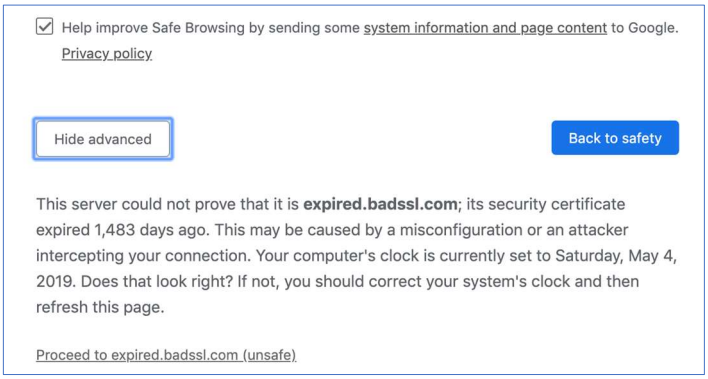


Dễ hiểu cho người dùng – Ví dụ

- Google Chrome

Process

Choices

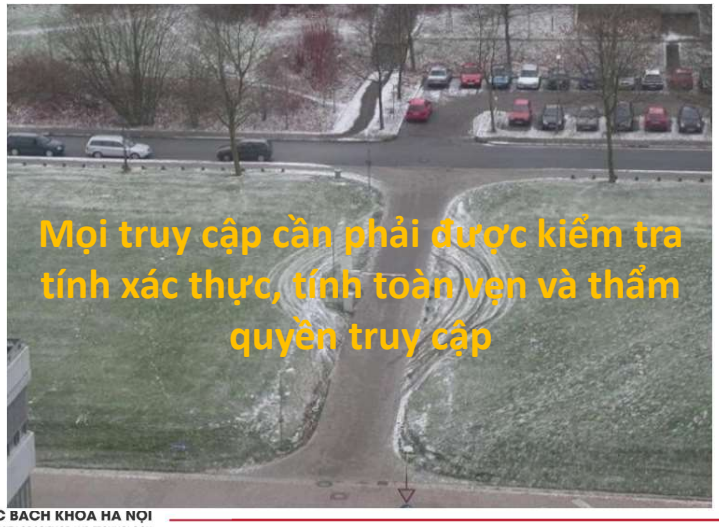


Một số nguyên tắc(tiếp)

- 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)
  - …

Một số nguyên tắc(tiếp)

- Kiểm soát tất cả truy cập(Complete mediation)



Kiểm tra tất cả truy cập

- Time Of Check To Time Of Use: TOCTTOU
  - Lỗ 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?

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 obsecurity”)
  - 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)

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

- 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?

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...

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