GIỚI THIỆU CHUNG VỀ HỌC PHẦN AN NINH MẠNG

Bùi Trọng Tùng, SoICT, HUST

1

Thông tin chung

- Mã HP: IT4260
- Tên học phần: An ninh mạng (Network Security)
- Khối lượng: 2(2-1-0-4)
  - Lý thuyết: 30 tiết
  - Bảo vệ bài tập lớn: 15 tiết
- Đánh giá:
  - Quá trình (30%): điểm bài tập lớn
  - Cuối kỳ (70%): thi viết
- Website: https://users.soict.hust.edu.vn/tungbt/it4260

2

Nội dung môn học

- An toàn quá trình truyền tin:
  - Các hệ mật mã
  - Xác thực thông điệp: MAC, hàm băm
  - Giao thức mật mã
  - Xác thực người dùng
- An toàn bảo mật trong mạng TCP/IP
- An toàn bảo mật Web

Tấn công và Phòng thủ

- Nhiều kiến thức trình bày về các kỹ thuật tấn công. Sinh viên chịu hoàn toàn trách nhiệm nếu thực hiện các kỹ thuật này ngoài phạm vi môn học mà không có sự đồng ý của các bên liên quan.

3

Tài liệu tham khảo

1. **Security in Computing, 4th edition,** *Charles P. Pfleeger - Pfleeger Consulting Group, Shari Lawrence Pfleeger*, Prentice Hall 2006
2. **Cryptography and Network Security Principles and Practices, 4th edition,** *William Stallings,* Prentice Hall 2005
3. **Security Engineering, 2nd edition,** *Ross J. Anderson,* Wiley 2008
4. Tài liệu đọc thêm theo từng bài

4

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

5

BÀI 1.
TỔNG QUAN VỀ AN TOÀN AN NINH MẠNG

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

6

6

Nội dung

- An toàn bảo mật (security) là gì?
- Chính sách và các cơ chế an toàn bảo mật
- Lỗ hổng an toàn bảo mật, nguy cơ an toàn bảo mật
- Nguyên tắc chung của hệ thống an toàn bảo mật

7

7

1. Đặt vấn đề

- Báo cáo về an toàn bảo mật:
  - IBM X-Force Threat Intelligence Index 2019
  - Symatec Internet Security Threat Report 2019
  - Verizon 2018 Data Breach Investigations Report
  - Cisco 2019 Annual Security Report
- http://www.networkworld.com/category/security0/

8

8

“Security” là gì?

Ngăn chặn, bảo vệ tài nguyên hệ thống trước các hành vi làm tổn hại

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

9

9

“Security” là gì?(tiếp)

Hoạt động của hệ thống	An toàn bảo mật hệ thống
Đầu vào (dữ liệu, hành vi...) → Kết quả đáp ứng “good input” → “good output” “bad input” → “bad output”	Đầu vào không hợp lệ → hệ thống vẫn hoạt động bình thường “bad input” ↛ “bad output”
Nâng cấp, thêm các thành phần mới: hệ thống hoạt động tốt hơn	Các nguy cơ mất an toàn bảo mật tăng lên

10

10

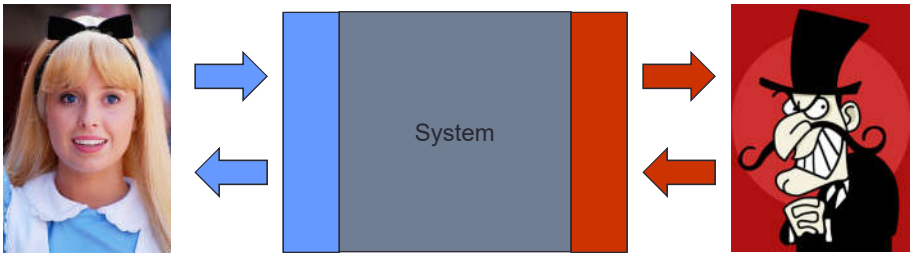
“Security” là gì? - CIA

- Confidentiality (Bí mật): tài nguyên không được tiếp cận bởi các bên không được ủy quyền
- Integrity (Toàn vẹn, tin cậy): tài nguyên không được sửa đổi bởi các bên không 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

11

11

Một ví dụ

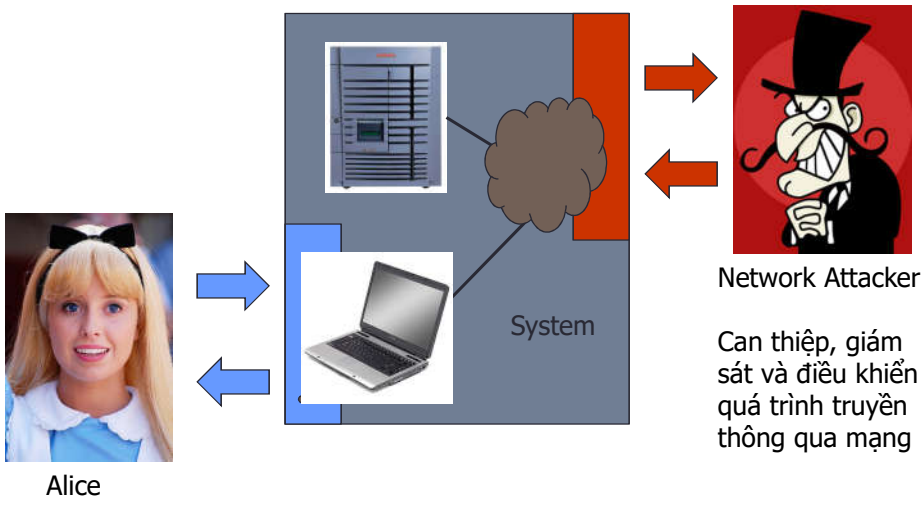


- Alice: người sử dụng hợp lệ
- Attacker:
  - ✓Ngăn cản Alice sử dụng hệ thống (Integrity, Availability)
  - ✓Do thám những thông tin mà chỉ Alice được biết (Confidentiality)

12

12

Một ví dụ (tiếp) – Network Security



Alice

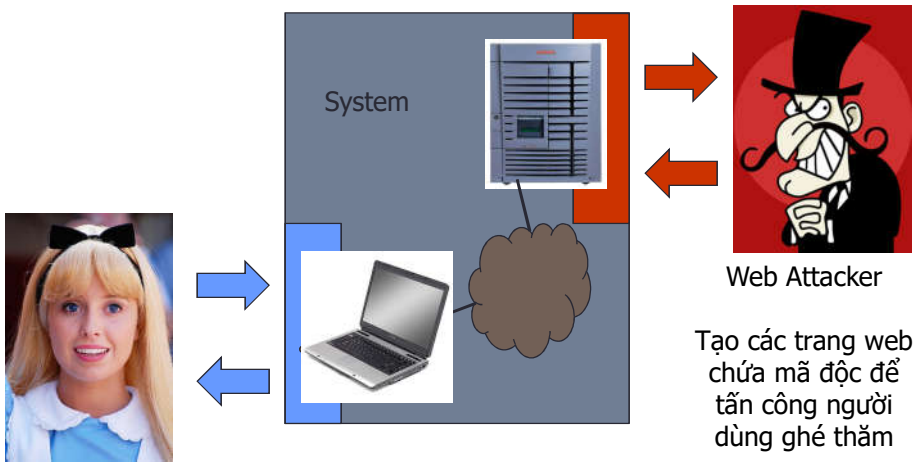
Network Attacker

Can thiệp, giám sát và điều khiển quá trình truyền thông qua mạng

13

13

Một ví dụ (tiếp) – Web Security



Alice

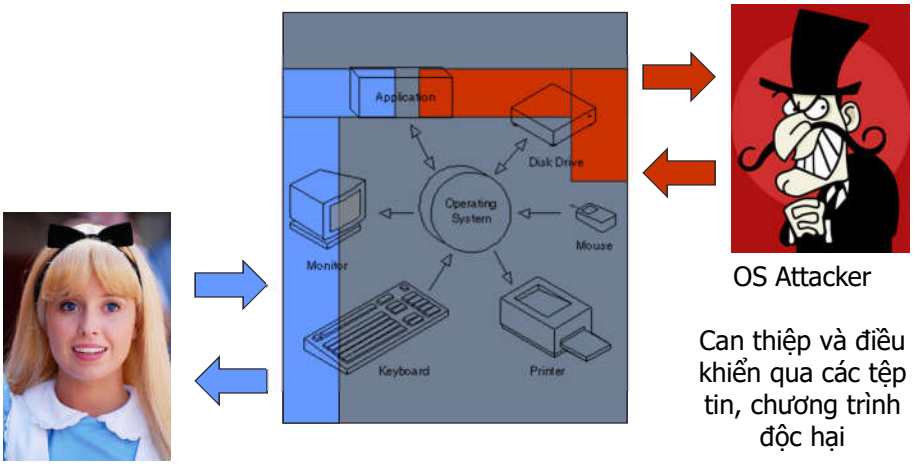
Web Attacker

Tạo các trang web chứa mã độc để tấn công người dùng ghé thăm

14

14

Một ví dụ (tiếp) – Operating System Security



Alice

OS Attacker

Can thiệp và điều khiển qua các tệp tin, chương trình độc hại

15

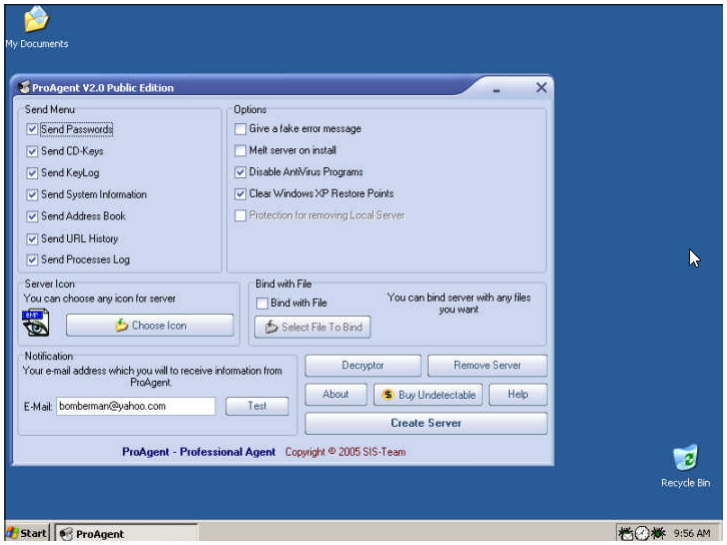
15

Khó khăn

- Các phương thức tấn công gây tổn hại
  - Không dễ dàng để phát hiện
  - Phát triển nhanh
  - Rẻ, dễ dàng thực hiện
  - Phân tán
  - Ẩn danh (Tor, VPN, proxy...)
  - Có thể xuất phát từ bên trong hệ thống
- Rất nhiều hệ thống ban đầu không được thiết kế để đối mặt với các hành vi xâm phạm
- Yêu cầu an toàn bảo mật xung đột với các yêu cầu khác của hệ thống.
- Tài nguyên phân tán
- Người sử dụng không được đào tạo đầy đủ

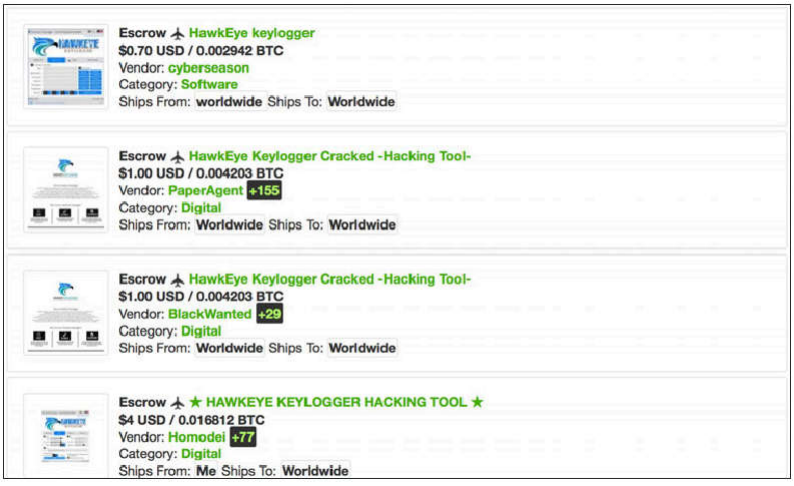
16

16



17

17



"North American Underground The Glass Tank" – Trend Micro

18

18

Nguy cơ trên thiết bị IoT

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

The notorious Mirai distributed denial of service (DDoS) worm remained an active threat and, with 16 percent of the attacks, was the third most common IoT threat in 2018.

TOP IOT THREATS (YEAR)

THREAT NAME	PERCENT
Linux.Lightaidra	31.3
Linux.Kaiten	31.0
Linux.Mirai	15.9

ATTACKS AGAINST IOT DEVICES (YEAR)

YEAR	TOTAL ATTACKS	PERCENT CHANGE
2017	57,691	
2018	57,553	-0.2

AVERAGE ATTACKS AGAINST IOT DEVICES (MONTH)

PER MONTH
5,233

Symatec Internet Security Threat Report 2019

19

19

Trusting trust?

- Chúng ta tin cậy vào cái gì?
- "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?
- Có thể lấy rất nhiều ví dụ khác...

→ Cần phải giám sát tất cả các thành phần

→ Phối hợp nhiều giải pháp khác nhau

20

20

2. Chính sách và cơ chế ATBM

- Chính sách an toàn bảo mật(security policy): tuyên bố về
  - Chủ thể
  - Hành vi phải thực hiện/được phép/không được phép
  - Tài nguyên

  Ví dụ: Nhà quản trị được phép sửa nội dung tệp tin chứa mật khẩu
- "Security" thể hiện qua chính sách ATBM

→tập chính sách phải thỏa mãn yêu cầu CIA

- Là cơ sở để xây dựng hạ tầng ATBM
- Phục vụ cho quản trị ATBM

21

21

Một số loại chính sách

- Access Control Policy
- Remote-Access Policy
- Network Connection Policy
- Passwords Policy
- User-Account Policy
- Data Protection Policy
- Email Policy
- Application Policy
- Tham khảo thêm:

http://www.lse.ac.uk/intranet/LSEServices/IMT/about/policies/home.aspx

22

22

Cơ chế an toàn bảo mật

- Là các kỹ thuật, phương pháp, thành phần để thi hành và đảm bảo chính sách ATBM được thi hành
  - Ngăn chặn (Preventation): ngăn chặn chính sách bị xâm phạm
  - Phát hiện (Detection): phát hiện chính sách bị xâm phạm
    - Thường kết hợp với các cơ chế phục hồi (recovery)
    - Có thể bao hàm giảm thiểu (deterrence)

Ví dụ:?

23

23

Cơ chế an toàn bảo mật (tiếp)

- Bảo vệ vật lý (Physical protection)
- Định danh (Identification)
- Xác thực (Authentication)
- Ủy quyền (Authorization)
- Nhật ký (Logging)
- Kiểm toán(Auditting)
- Mật mã học (Cryptography)
- Giả lập, ngụy trang (Deception)
- Gây nhiễu, ngẫu nhiên(randomness)

Mô hình AAA

24

24

3. Lỗ hổng và nguy cơ ATBM

- Nguy cơ (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): xác suất hệ thống bị tổn hại bởi nguy cơ
- 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://cve.mitre.org/
  - Tầm soát lỗ hổng định kỳ

25

25

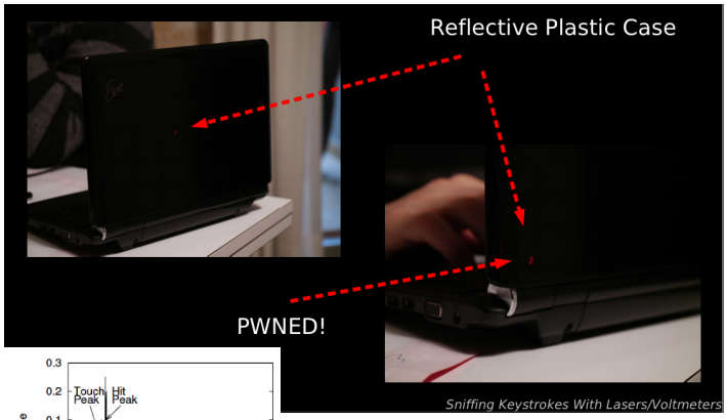
Lỗ hổng và nguy cơ ATBM (tiếp)

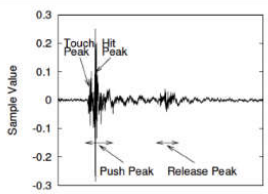
- Tấn công vào tính bảo mật:
  - Nghe lén
  - Phân tích tải
- Tấn công vào tính toàn vẹn:
  - Sửa đổi nội dung
  - Giả mạo
  - Từ chối
  - Phát lại
- Tấn công vào tính sẵn sàng:
  - Tấn công từ chối dịch vụ

26

26

Nghe lén bằng kỹ thuật tấn công kênh bên (side-channel attack)





27

27

Nghe lén

Figure 6. Reflections in two other tea pots, taken from a distance of 5m. The 18pt font is readable from the reflection in the left picture, and almost readable in the right picture.

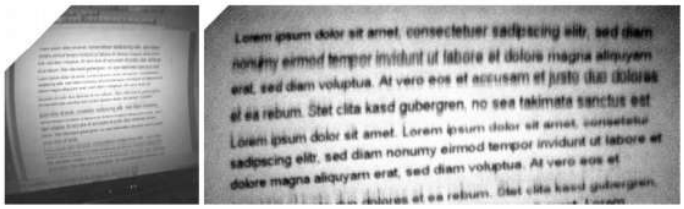


Figure 7. Reflection of a Word document with small 12pt font size in a tea pot, taken from a distance of 5m. The 12pt font is readable from the reflection.

28

28

Nghe lén

Figure 9. Image taken with a macro lens from very short distance, with realistic distance between the monitor and the eye. Readability is limited by the resolution of the camera.

Figure 10. Reflections in two different pairs of glasses, taken from a distance of 5m. Both the inner side and the outer side of glasses produce reflections. The 18pt font is readable from the reflection.

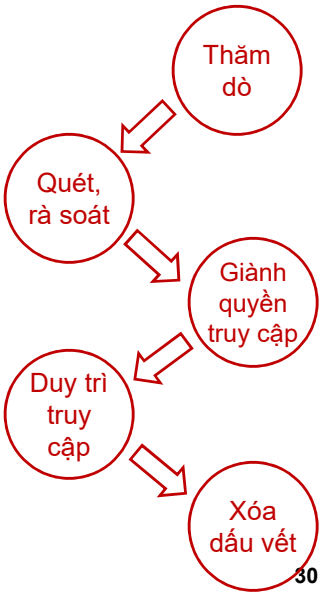
29

29

Kịch bản tấn công

Các giai đoạn thực hiện tấn công:

- Chuẩn bị tấn công
  - Thăm dò thông tin
  - Quét, rà soát hệ thống
- Thực thi tấn công
  - Giành quyền truy cập
  - Duy trì truy cập
- Xóa dấu vết

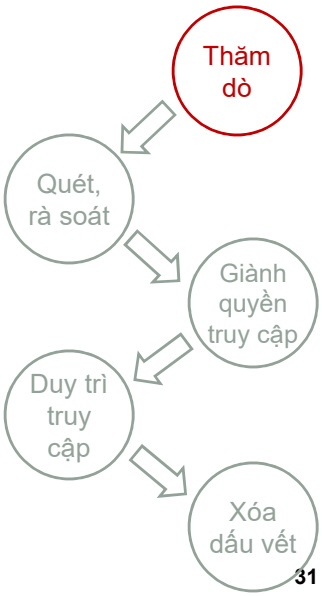


30

30

Thăm dò

- Là các hành vi mà kẻ tấn công thực hiện nhằm thu thập thông tin về hệ thống: người dùng, khách hàng, các hoạt động nghiệp vụ, thông tin về tổ chức…
- Có thể lặp đi lặp lại một cách định kỳ đến khi có cơ hội tấn công dễ dàng hơn
- Thăm dò chủ động: có tương tác với mục tiêu
- Thăm dò bị động: không có tương tác với mục tiêu

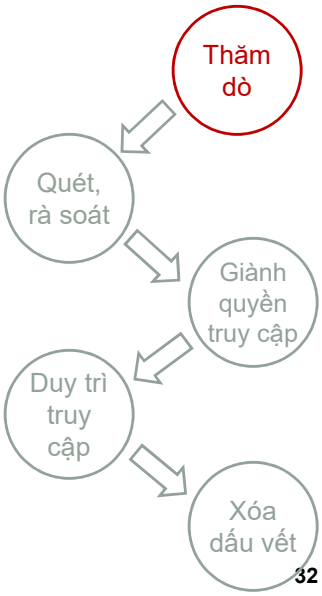


31

31

Thăm dò(tiếp)

- Sử dụng các công cụ tìm kiếm: Google, Shodan, Censys
- Thông tin từ mạng xã hội: FB, Tweetter, Linkedin
- Thông tin từ website của đối tượng: Burp Suite, ZAP, Web Spider, Web Mirroring
- Thăm dò hệ thống email
- WHOIS, DNS
- Thăm dò kết nối mạng: trace route
- Social Engineering

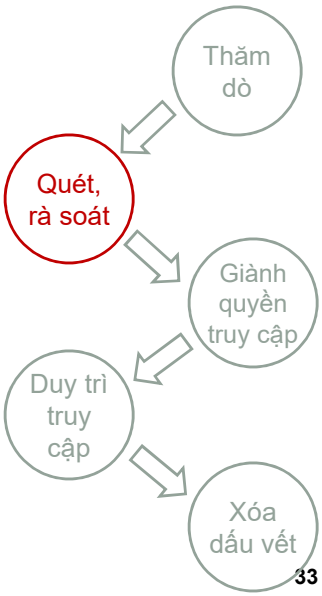


32

32

Quét rà soát

- Quét rà soát để xác định các thông tin về hệ thống dựa trên các thông tin thu thập được từ quá trình thăm dò
- Kẻ tấn công có cái nhìn chi tiết hơn và sâu hơn về hệ thống: các dịch vụ cung cấp, các cổng dịch vụ đang mở, địa chỉ IP, hệ điều hành và phần mềm…
- Trích xuất thông tin từ giai đoạn này cho phép kẻ tấn công lên kế hoạch chi tiết để thực hiện tấn công

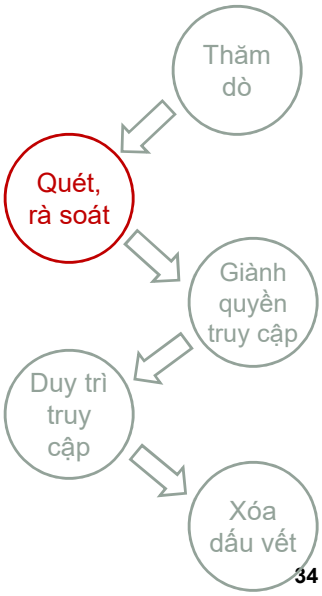


33

33

Quét rà soát(tiếp)

- Xác định các nút mạng kết nối: Ping Sweep
- Kiểm tra các cổng dịch vụ đang mở: TCP Scanning, UDP Scanning
- Xác định thông tin hệ điều hành trên hệ thống mục tiêu: ID Serve, Netcraft
- Quét lỗ hổng: Nessus, GFI LanGuard
- Xác định topology của mạng mục tiêu: Network Topology Mapper
- Tương tác và thống kê(enumeration)

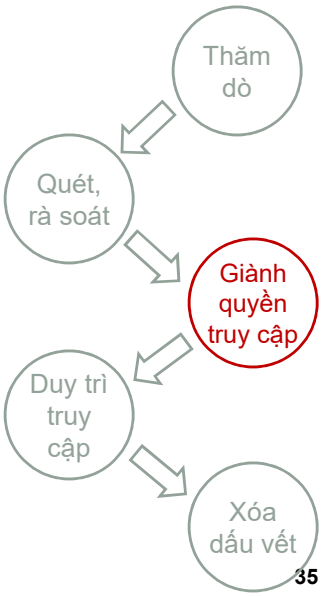


34

34

Giành quyền truy cập

- Kẻ tấn công giành được quyền truy cập vào hệ thống ở các mức độ khác nhau: mức mạng, mức hệ điều hành, mức ứng dụng
- Có thể dựa trên các quyền truy cập đã có để leo thang truy cập

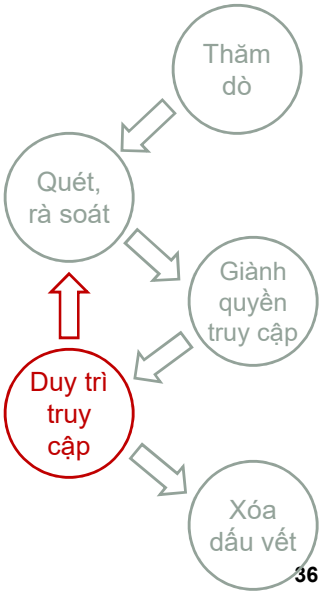


35

35

Duy trì truy cập

- Thay đổi, can thiệp và hoạt động của hệ thống
- Cài đặt các phần mềm gián điệp
- Che giấu các hành vi trên hệ thống
- Quét rà soát sâu vào hệ thống
- Mở rộng phạm vi tấn công
- Leo thang tấn công
- Nếu cần thiết, kẻ tấn công có thể nằm vùng, chờ thời điểm thích hợp để phát động tấn công



36

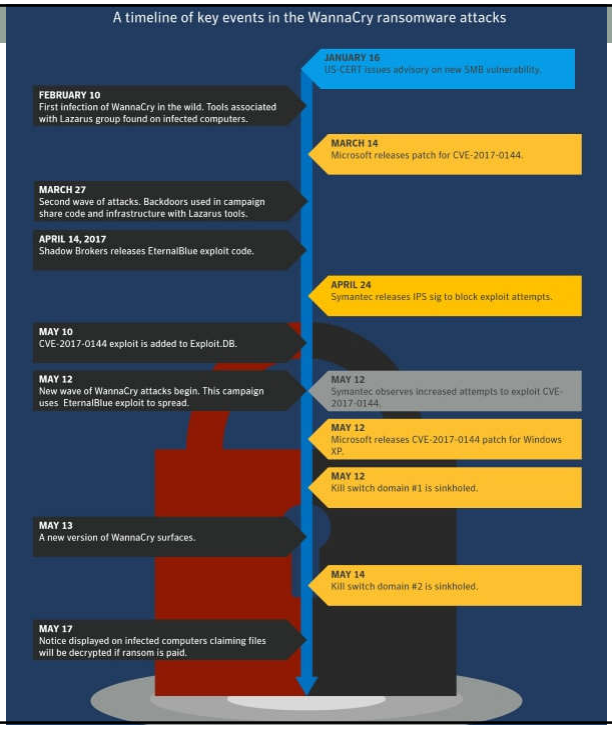
36

Xu hướng các hành vi tấn công ATBM

- Cuộc đua giữa tin tặc và các nhà nghiên cứu, nhà sản xuất
- Công cụ tự động hóa tấn công
- Hình thành thị trường ngầm
  - http://www.darkreading.com/cloud/cybercrime-a-black-market-price-list-from-the-dark-web/d/d-id/1324895?image_number=1
- Mở rộng các hành vi đánh cắp thông tin cá nhân
- Tình báo
- Trở thành vấn đề an ninh quốc gia:
  - Kiểm duyệt
  - Tình báo
  - Chiến tranh mạng

37

37



38

38

Xu hướng các hành vi tấn công ATBM

- Cuộc đua giữa tin tặc và các nhà nghiên cứu, nhà sản xuất
- Công cụ tự động hóa tấn công
- Hình thành thị trường ngầm
  - http://www.darkreading.com/cloud/cybercrime-a-black-market-price-list-from-the-dark-web/d/d-id/1324895?image_number=1
- Mở rộng các hành vi đánh cắp thông tin cá nhân
- Tình báo
- Trở thành vấn đề an ninh quốc gia:
  - Kiểm duyệt
  - Tình báo
  - Chiến tranh mạng

39

39

Top10 Web Attack Toolkits

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

Symatec Internet Security Threat Report 2017 40

40

Xu hướng các hành vi tấn công ATBM

- Cuộc đua giữa tin tặc và các nhà nghiên cứu, nhà sản xuất
- Công cụ tự động hóa tấn công
- Hình thành thị trường ngầm
  - http://www.darkreading.com/cloud/cybercrime-a-black-market-price-list-from-the-dark-web/d/d-id/1324895?image_number=1
- Mở rộng các hành vi đánh cắp thông tin cá nhân
- Tình báo
- Trở thành vấn đề an ninh quốc gia:
  - Kiểm duyệt
  - Tình báo
  - Chiến tranh mạng

41

41

3/30/2016
10:10 AM

Ericka Chickowski
Slideshows

Connect Directly

0 COMMENTS
COMMENT NOW

Cybercrime: A Black Market Price List From The Dark Web

What does it cost for malware, stolen identities and other tools of the cybercriminal trade? Probably less than you think.

1 of 10

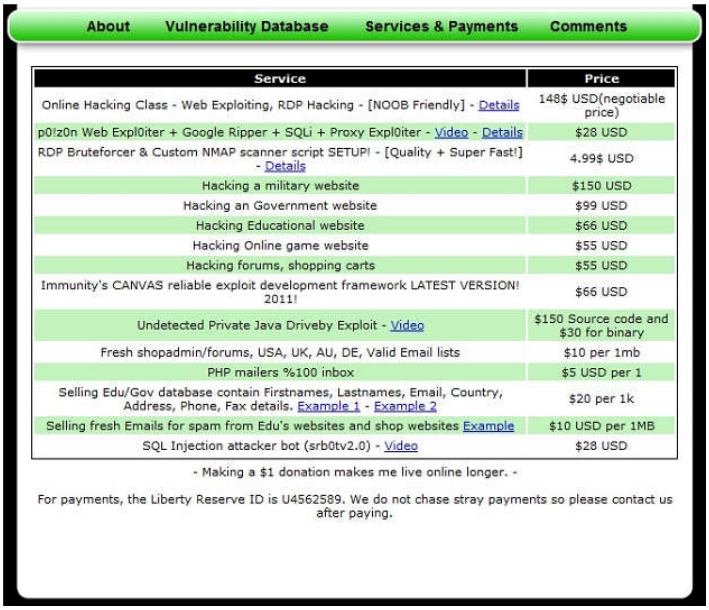
Image Source: Adobe Stock

1 of 10

http://www.darkreading.com

42

42



About | Vulnerability Database | Services & Payments | Comments

Service	Price
Online Hacking Class - Web Exploiting, RDP Hacking - [NOOB Friendly] - Details	148$ USD(negotiable price)
p0!z0n Web Expl0iter + Google Ripper + SQLi + Proxy Expl0iter - Video - Details	$28 USD
RDP Bruteforcer & Custom NMAP scanner script SETUP! - [Quality + Super Fast!] - Details	4.99$ USD
Hacking a military website	$150 USD
Hacking an Government website	$99 USD
Hacking Educational website	$66 USD
Hacking Online game website	$55 USD
Hacking forums, shopping carts	$55 USD
Immunity's CANVAS reliable exploit development framework LATEST VERSION! 2011!	$66 USD
Undetected Private Java Driveby Exploit - Video	$150 Source code and $30 for binary
Fresh shopadmin/forums, USA, UK, AU, DE, Valid Email lists	$10 per 1mb
PHP mailers %100 inbox	$5 USD per 1
Selling Edu/Gov database contain Firstnames, Lastnames, Email, Country, Address, Phone, Fax details. Example 1 - Example 2	$20 per 1k
Selling fresh Emails for spam from Edu's websites and shop websites Example	$10 USD per 1MB
SQL Injection attacker bot (srb0tv2.0) - Video	$28 USD

- Making a $1 donation makes me live online longer. -

For payments, the Liberty Reserve ID is U4562589. We do not chase stray payments so please contact us after paying.

43

43

Offering	Price
40GBps for 300 seconds	US$5
70GBps for 300 seconds	US$9
40GBps for 2,700 seconds	US$25
125GBps for 300 seconds	US$25
70GBps for 7,200 seconds	US$30
125GBps for 2,000 seconds	US$60

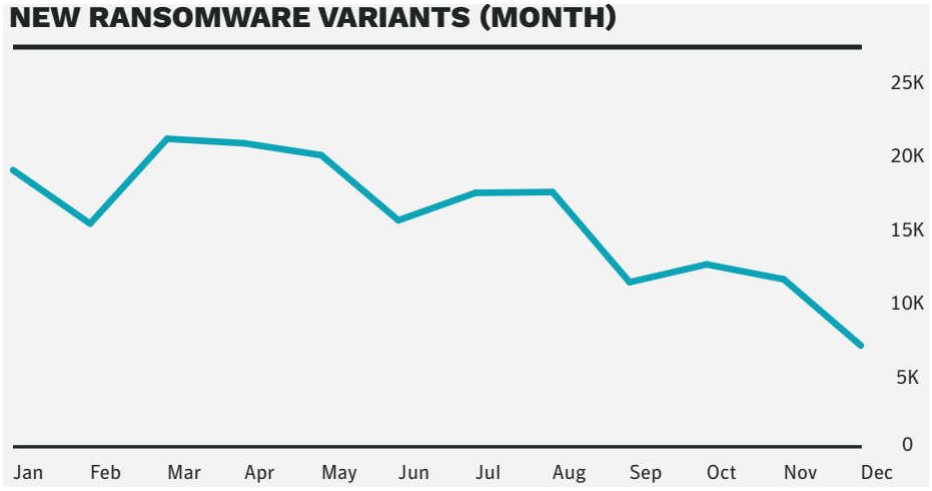
Offering	Price
Classic US-issued credit card credentials	US$19–22 (100 sets)
Gold, Platinum, or Business US-issued credit card credentials	US$36–42 (50 sets)
Classic Canada-issued credit card credentials	US$47–50 (40 sets)
Gold, Platinum, or Business Canada-issued credit card credentials	US$50–65 (35 sets)
Fake US-issued credit card (physical)	US$210–874

"North American Underground The Glass Tank" – Trend Micro

44

44

Sự phát triển của Ransomware(2018)

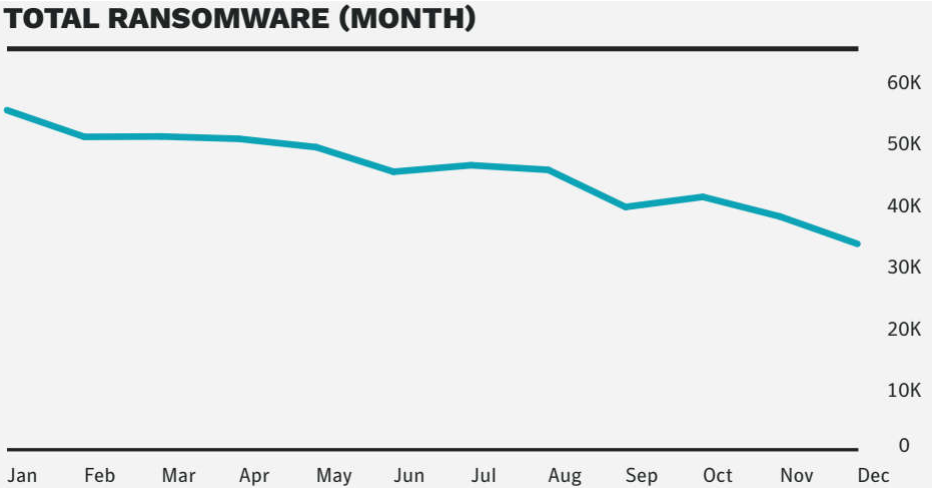


Symatec Internet Security Threat Report 2019

45

45

Sự phát triển của Ransomware(2018)

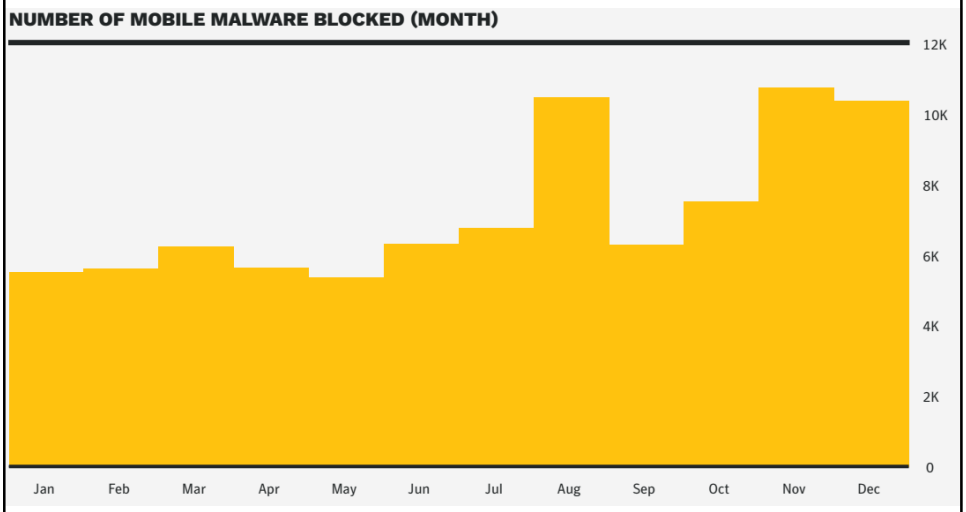


Symatec Internet Security Threat Report 2019

46

46

Sự phát triển của Ransomware(2018)



Symatec Internet Security Threat Report 2019

47

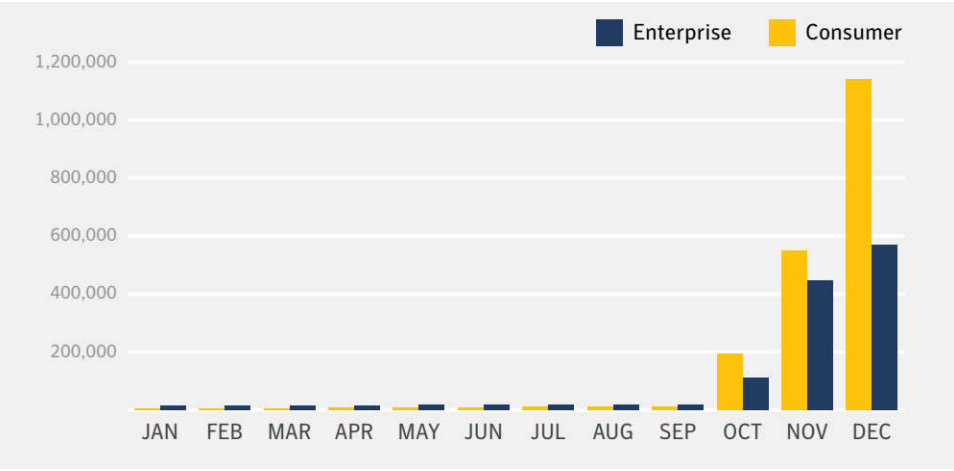
47

WannaCry (05/2017)

48

48

Lan tràn mã độc "coinminer"



Symatec Internet Security Threat Report 2018

49

49

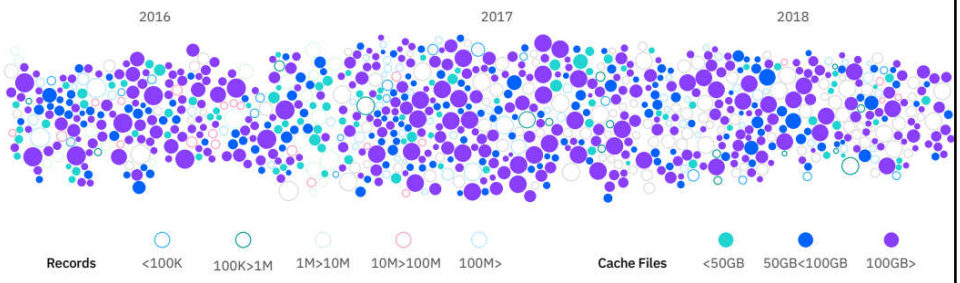
Xu hướng các hành vi tấn công ATBM

- Cuộc đua giữa tin tặc và các nhà nghiên cứu, nhà sản xuất
- Công cụ tự động hóa tấn công
- Hình thành thị trường ngầm
  - http://www.darkreading.com/cloud/cybercrime-a-black-market-price-list-from-the-dark-web/d/d-id/1324895?image_number=1
- Mở rộng các hành vi đánh cắp thông tin cá nhân
- Tình báo
- Trở thành vấn đề an ninh quốc gia:
  - Kiểm duyệt
  - Tình báo
  - Chiến tranh mạng

50

50

Đánh cắp thông tin cá nhân

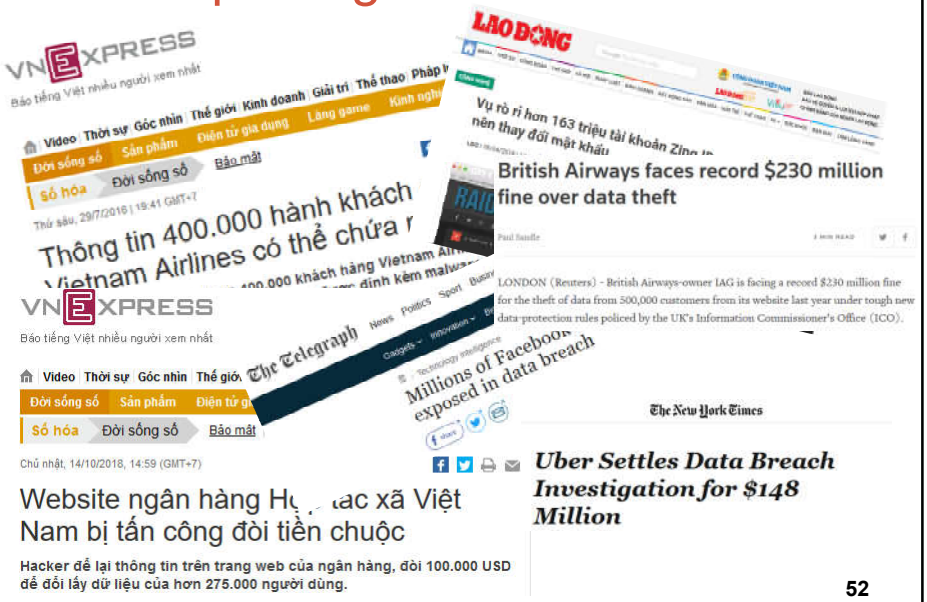


IBM X-Force Threat Intelligence Index 2019

51

51

Đánh cắp thông tin cá nhân



52

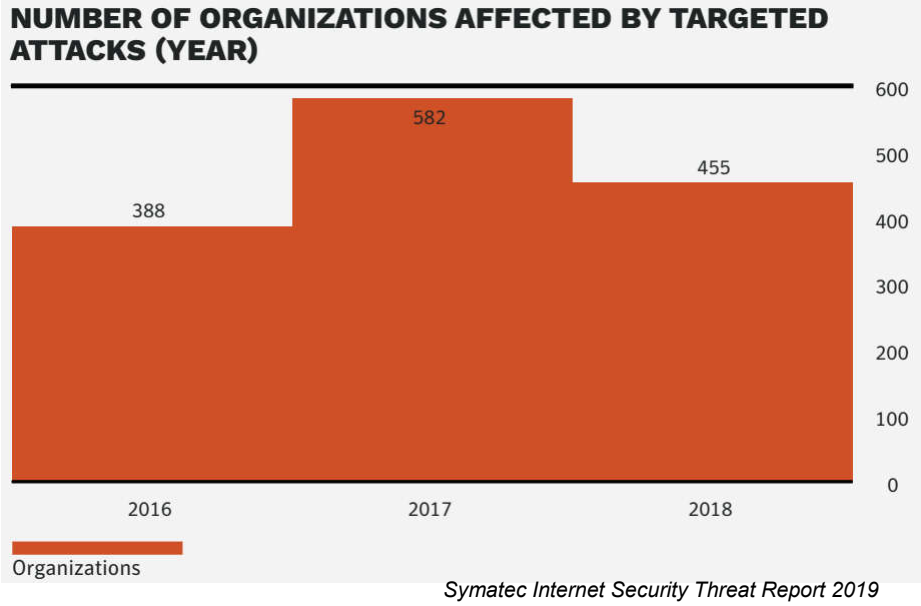
52

Xu hướng các hành vi tấn công ATBM

- Cuộc đua giữa tin tặc và các nhà nghiên cứu, nhà sản xuất
- Công cụ tự động hóa tấn công
- Hình thành thị trường ngầm
  - http://www.darkreading.com/cloud/cybercrime-a-black-market-price-list-from-the-dark-web/d/d-id/1324895?image_number=1
- Mở rộng các hành vi đánh cắp thông tin cá nhân
- Tình báo
- Trở thành vấn đề an ninh quốc gia:
  - Kiểm duyệt
  - Tình báo
  - Chiến tranh mạng

53

53



Symatec Internet Security Threat Report 2019

54

54

55

55

Symatec Internet Security Threat Report 2018

56

56

4. Xây dựng hệ thống an toàn bảo mật

57

57

Quy trình xây dựng

4 giai đoạn:

- Phân tích yêu cầu
  - Xây dựng chính sách ATBM(yêu cầu)
  - 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

58

58

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

  Chú ý: cần xác định ngay các cơ chế ATBM để đảm bảo việc thực thi các chính sách
- Xây dựng các tình huống lạm quyền minh họa cho chính sách
- Chính sách ATBM phải phù hợp với quy định luật pháp

59

59

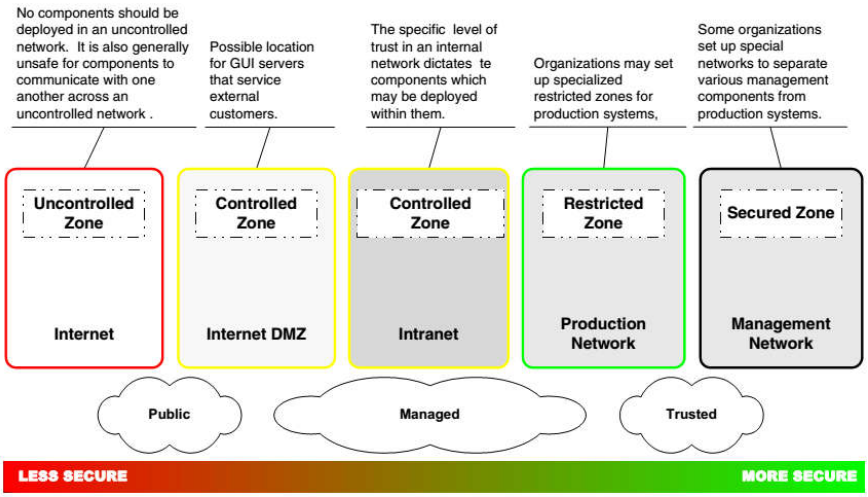
Quy trình xây dựng

- Xây dựng mô hình nguy cơ:
  1. Xác định, phân vùng tài nguyên cần bảo vệ
  2. Xác định các thành phần, luồng dữ liệu, hành vi tương tác trên tài nguyên
  3. Phân tích các hoạt động diễn ra trên tài nguyên
  4. Xác định các nguy cơ có thể có, phân loại và đánh giá
  5. Xác định các lỗ hổng liên quan

60

60

Ví dụ: phân vùng mạng

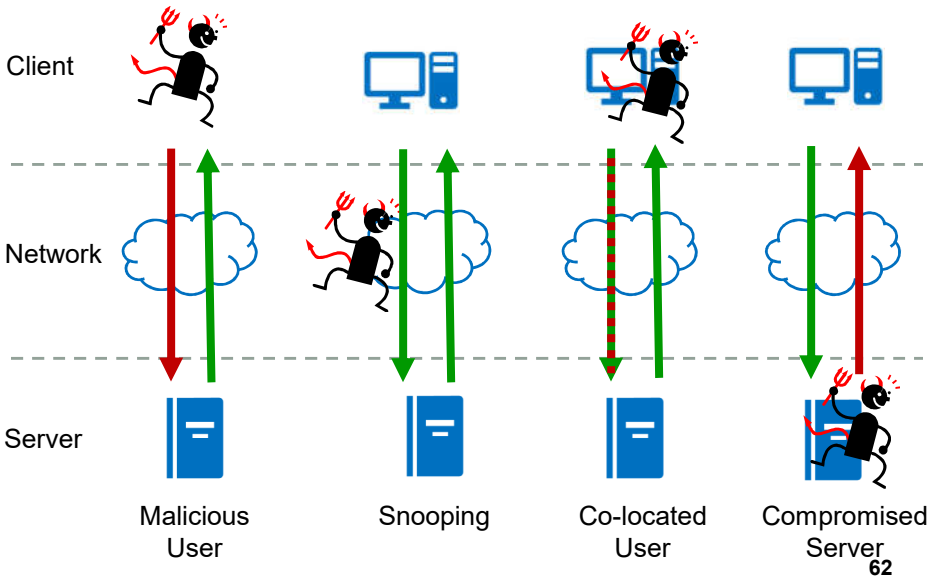


IBM Security Solutions Architecture for Network, Server and Endpoint

61

61

Xây dựng mô hình nguy cơ



62

62

Quy trình xây dựng

- Thiết kế các thành phần theo mô hình nguy cơ:
  - 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

63

63

Một số nguyên tắc thiết kế

- Không thể đạt an toàn hoàn hảo
  - Xây dựng hệ thống là an toàn nhất trong các điều kiện ràng buộc
  - Đôi khi giải pháp tốt nhất là giải pháp làm cho hệ thống không phải mục tiêu dễ dàng nhất.
- An toàn bảo mật là bài toán kinh tế:
  - Giá trị tài nguyên cần bảo vệ/ Chi phí để bảo vệ
  - Mức tổn thương mà một nguy cơ gây ra / Chi phí để chống lại các kỹ thuật tấn công thực hiện nguy cơ
  - Chi phí thực thi 1 nguy cơ / Giá trị thu lại
  - Xác suất nguy cơ được thực thi → quản trị độ rủi ro (risk management)

  → để giảm ½ độ rủi ro cần tăng gấp đôi chi phí (Adi Shamir)

64

64

An toàn bảo mật là bài toán kinh tế

TL-15

TL-15

TXTL-60

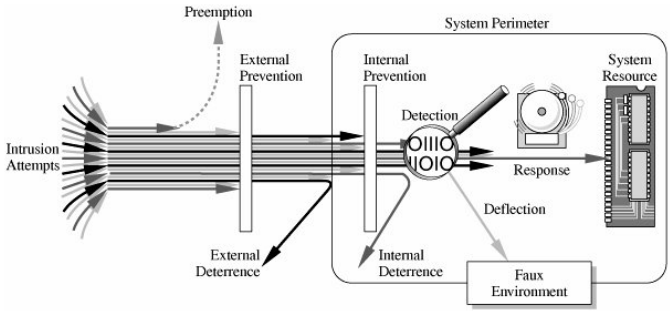
65

65

Một số nguyên tắc thiết kế(tiếp)

- Giám soát hoàn toàn các truy cập
- Bảo vệ theo nhiều tầng (Defense in Depth)

Ví dụ:



66

66

Một số nguyên tắc thiết kế(tiếp)

- Sử dụng chính sách “mặc định cấm” (default-deny): từ chối tất cả các yêu cầu thực thi quyền không được liệt kê
- Tối thiểu hóa quyền(Least privilege): không cấp quyền nhiều hơn những gì mà đối tượng cần để hoàn thành nhiệm vụ.
  - Không làm giảm độ rủi ro nhưng làm giảm thiệt hại
- Chia sẻ trách nhiệm: quyền chỉ được thực thi khi có sự phối hợp của >= 2 thành phần

67

67

Một số nguyên tắc thiết kế(tiếp)

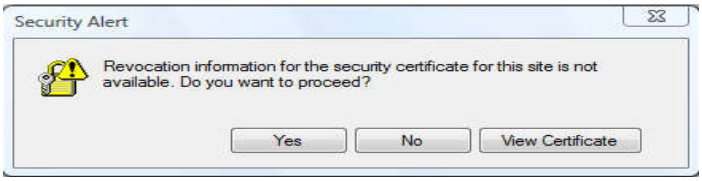
- Mức độ an toàn của hệ thống ~ Mức độ an toàn ở thành phần yếu nhất
- KISS: Keep It Simple
- Dễ hiểu để sử dụng
- Không phụ thuộc vào các giải pháp an toàn bảo mật dựa trên việc che giấu mọi thứ (“security through obsecurity”)
  - Ví dụ: giữ mật thiết kế, thuật toán, mã nguồn...
- Phát hiện những kỹ thuật tấn công không thể ngăn chặn
- Dự phòng và khôi phục

68

68

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

69

69

Dễ hiểu cho người dùng – Ví dụ

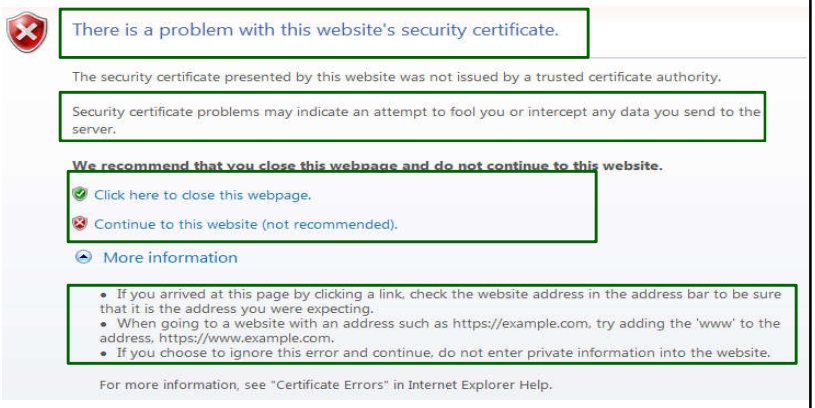
- Trên IE8

Source

Risk

Choices

Process



70

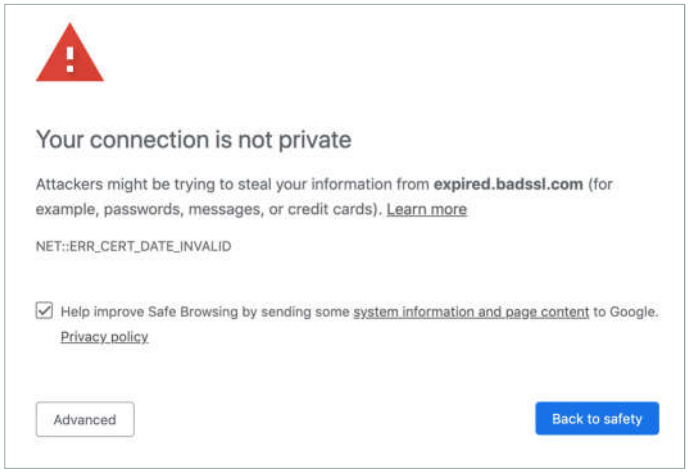
70

Dễ hiểu cho người dùng – Ví dụ

- Google Chrome

Risk

Explanation



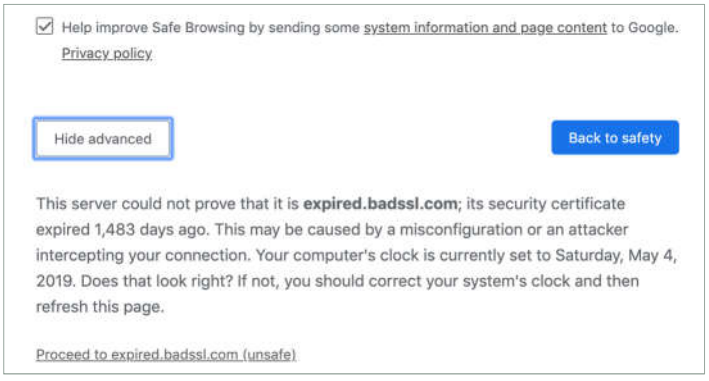
Choices

71

71

Dễ hiểu cho người dùng – Ví dụ

- Google Chrome



Process

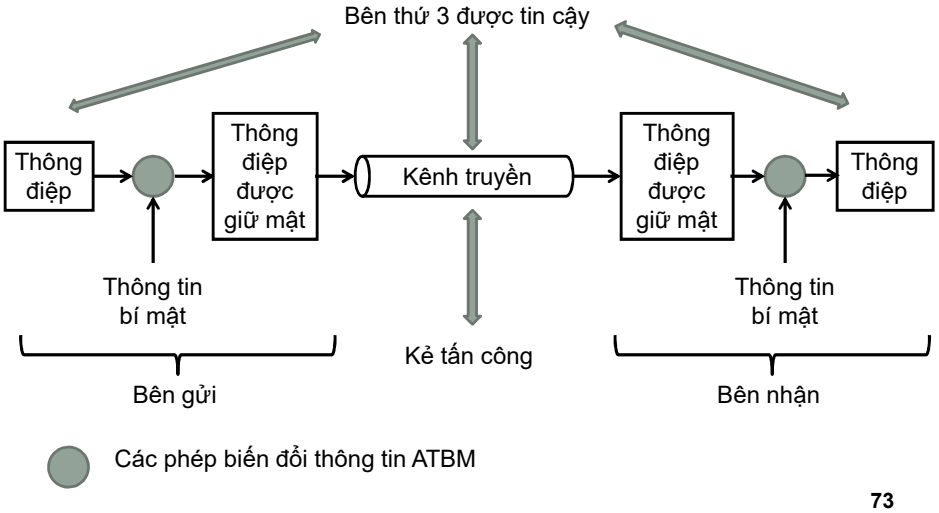
Choices

72

72

Một số mô hình

- Mô hình ATBM truyền tin



73

73

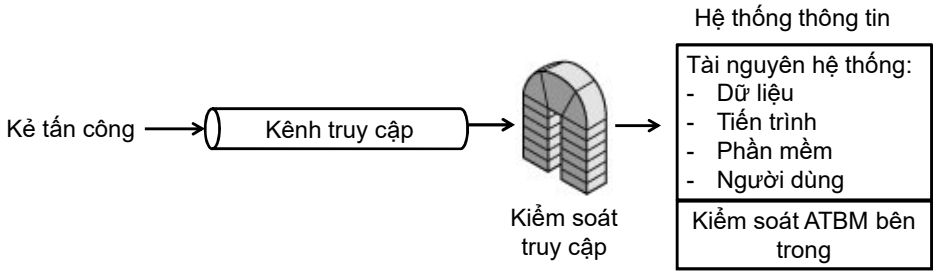
Mô hình ATBM truyền tin

- Các kỹ thuật sử dụng trong mô hình ATBM truyền tin có 2 thành phần chính:
  - Các phép biến đổi thông tin ATBM
  - Thông tin mật chia sẻ giữa 2 bên truyền tin
- Các bên truyền tin: người dùng, chương trình (trình duyệt Web, mail client...)
- Bên thứ 3 được tin cậy:trọng tài, người phân xử...
- Kẻ tấn công: người dùng, chương trình(chặn bắt và phân tích gói tin, phân tích tải...)
- Các nhiệm vụ chính:
  - Xây dựng thuật toán để biến đổi thông tin
  - Sinh thông tin bí mật
  - Phát triển các phương pháp phân phối thông tin bí mật
  - Xây dựng giao thức chia sẻ thông tin

74

74

Mô hình ATBM truy cập hệ thống



- Kiểm soát truy cập: firewall, IDS, quét và phát hiện mã độc...
- Bảo vệ đa tầng

75

75

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

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

76

76