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

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

1. MỞ ĐẦU

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

An toàn an ninh thông tin là gì?

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

- Tài nguyên hệ thống:
  - Phần cứng
  - Phần mềm
  - Dữ liệu
  - Người dùng

  An toàn an ninh mạng: Đặt các yêu cầu an toàn an ninh thông tin vào ngữ cảnh môi trường mạng máy tính
- 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

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

5

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
- …

6

Thông tin chung về môn học

- Mã HP: IT4263
- Tên học phần: An ninh mạng (Network Security)
- Khối lượng: 3(2-0-2-4)
  - Lý thuyết: 30 tiết
  - Thực hành: 30 tiết (5 bài)
- Đánh giá:
  - Quá trình (40%): điểm thực hành
  - Cuối kỳ (60%): thi viết
- Website: https://users.soict.hust.edu.vn/tungbt/it4263

Quy định điểm quá trình

- Điểm QT = Trung bình các bài thực hành + Chuyên cần
- 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

Nội dung môn học

- An toàn bảo mật trong mạng TCP/IP
  - Tấn công các giao thức và dịch vụ trong mạng
  - Tấn công từ chối dịch vụ
- An toàn bảo mật Web
- An toàn quá trình truyền tin:
  - Mật mã học và ứng dụng
  - Các giao thức bảo mật trong mạng TCP/IP

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.

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

Thông tin giảng viên

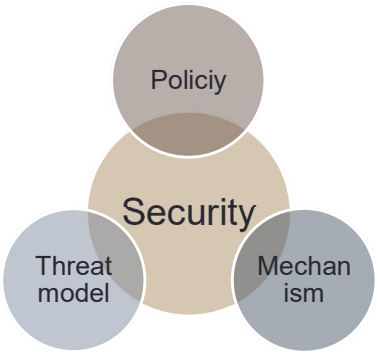
Bùi Trọng Tùng,
Khoa Kỹ thuật máy tính
Email: tungbt@soict.hust.edu.vn
Địa chỉ: phòng 405, nhà B1
FB: https://www.facebook.com/tungbui.hust
Group: https://www.facebook.com/groups/FAQ.TungBT

2. CÁC KHÁI NIỆM CƠ BẢN

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

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

13

Mục tiêu - 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

14

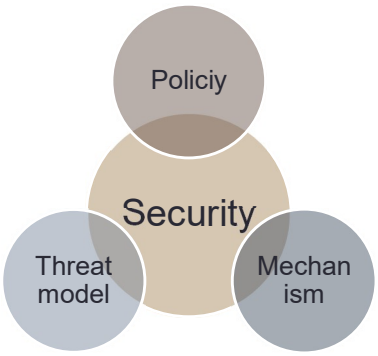
Mục tiêu – AAA

- 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

15

AT-ANTT là gì?

- Bao gồm các khía cạnh:
  - Chính sách
  - Mô hình đe dọa
  - Cơ chế AT-ANTT



- Threat Model: mô tả những tiềm ẩn về mất an toàn an ninh 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?

16

Lỗ hổng và tấn công AT-ANTT

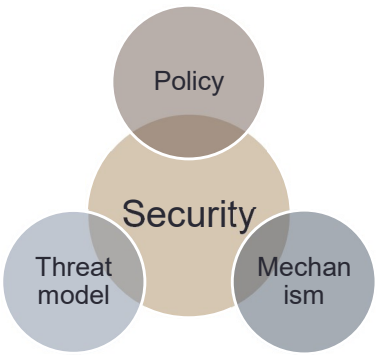
- Lỗ hổng (Vulnerability): là những điểm yếu trong hệ thống có thể bị khai thác, lợi dụng để gây tổn hại cho hệ thống
  - https://www.cvedetails.com/
  - Tầm soát lỗ hổng định kỳ là một trong những giải pháp phòng chống tấn công
- Tấn công (Attack): thực thi các hành vi gây hại
  - Thường lợi dụng, khai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

Risk = Threat * Impact

17

AT-ANTT là gì?

- Bao gồm các khía cạnh:
  - Chính sách
  - Mô hình đe dọa
  - Cơ chế AT-ANTT



- Cơ chế AT-ANTT: Là các kỹ thuật, thủ tục để thi hành và đảm bảo chính sách AT-ANTT được thi hành
  - Ngăn chặn (Prevention): ngăn chặn chính sách bị xâm phạm
  - Phát hiện (Detection) và Ứng phó(Response): phát hiện chính sách bị xâm phạm

18

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)

19

Những thách thức ATAN mạng

- Hệ thống mở
- Tài nguyên phân tán
- Người dùng ẩn danh
- TCP/IP được không được thiết kế để đối mặt với các nguy cơ ATBM
  - Không xác thực các bên
  - Không xác thực, giữ bí mật dữ liệu trong gói tin

"On the Internet, nobody knows you're a dog."

20

3. TẤN CÔNG MẠNG

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

Những giả định về tấn công

- Những giả định này là bi quan nhưng là sự cận trọng cần thiết
- Kẻ tấn công có thể tương tác với hệ thống mà không gây ra sự khác biệt rõ rang
- 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

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

23

Các dạng tấn công

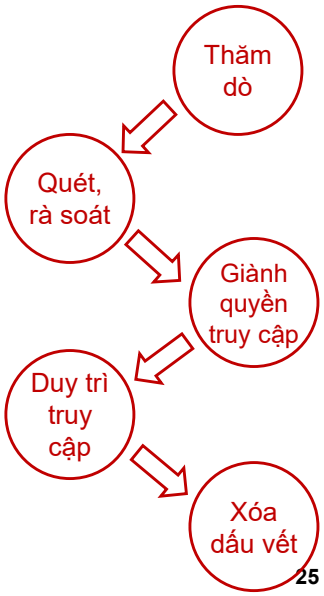
- Tấn công vào tính bí mật
- Tấn công vào tính toàn vẹn
  - Sửa đổi nội dung
  - Giả mạo
  - Phát lại
- Tấn công vào tính sẵn sàng:
  - Tấn công từ chối dịch vụ
- Tấn công thăm dò
  - Quét mạng
  - Quét cổng dịch vụ
- Tấn công truy cập
- Tấn công vào tính sẵn sàng:
  - Tấn công từ chối dịch vụ

24

Kịch bản tấn công

Các giai đoạn thực hiện tấn công:

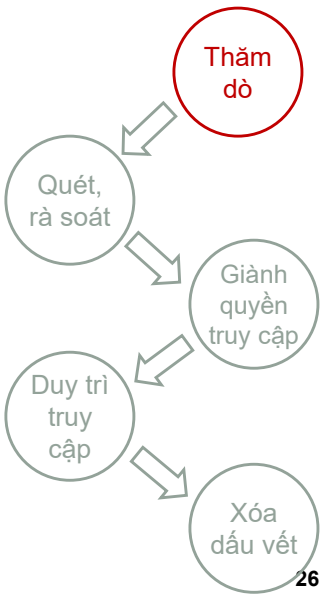
- Chuẩn bị tấn công
  - Thăm dò thông tin
  - Quét, rà soát hệ thống
- Thực thi tấn công
  - Giành quyền truy cập
  - Duy trì truy cập
- Xóa dấu vết



25

Thăm dò

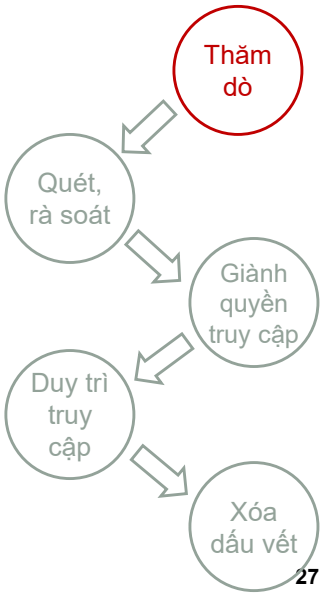
- Là các hành vi mà kẻ tấn công thực hiện nhằm thu thập thông tin về hệ thống: người dùng, khách hàng, các hoạt động nghiệp vụ, thông tin về tổ chức…
- Có thể lặp đi lặp lại một cách định kỳ đến khi có cơ hội tấn công dễ dàng hơn
- Thăm dò chủ động: có tương tác với mục tiêu
- Thăm dò bị động: không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



26

Thăm dò(tiếp)

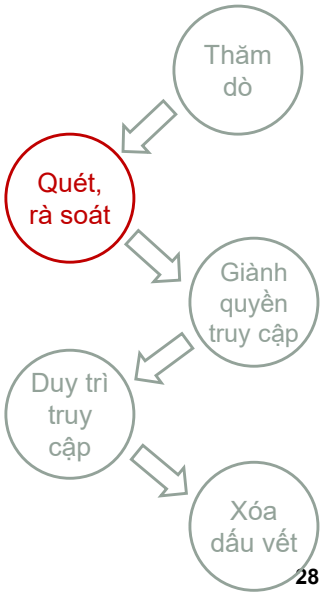
- Sử dụng các công cụ tìm kiếm: Google, Shodan, Censys
- Thông tin từ mạng xã hội: FB, Tweetter, Linkedin
- Thông tin từ website của đối tượng: Burp Suite, ZAP, Web Spider, Web Mirroring
- Thăm dò hệ thống email
- WHOIS, DNS
- Thăm dò kết nối mạng: trace route
- Social Engineering



27

Quét rà soát

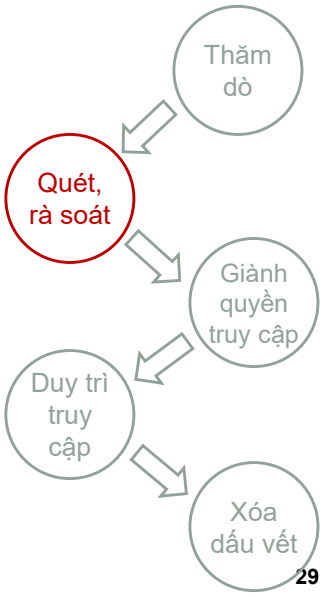
- Quét rà soát để xác định các thông tin về hệ thống dựa trên các thông tin thu thập được từ quá trình thăm dò
- Kẻ tấn công có cái nhìn chi tiết hơn và sâu hơn về hệ thống: các dịch vụ cung cấp, các cổng dịch vụ đang mở, địa chỉ IP, hệ điều hành và phần mềm…
- Trích xuất thông tin từ giai đoạn này cho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



28

Quét rà soát(tiếp)

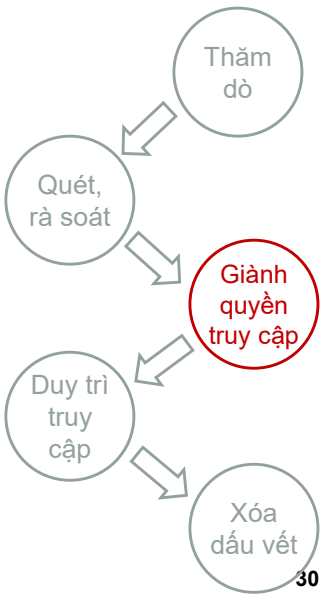
- Xác định các nút mạng kết nối: Ping Sweep
- Kiểm tra các cổng dịch vụ đang mở: TCP Scanning, UDP Scanning
- Xác định thông tin hệ điều hành trên hệ thống mục tiêu: ID Serve, Netcraft
- Quét lỗ hổng: Nessus, GFI LanGuard
- Xác định topology của mạng mục tiêu: Network Topology Mapper
- Tương tác và thống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



29

Giành quyền truy cập

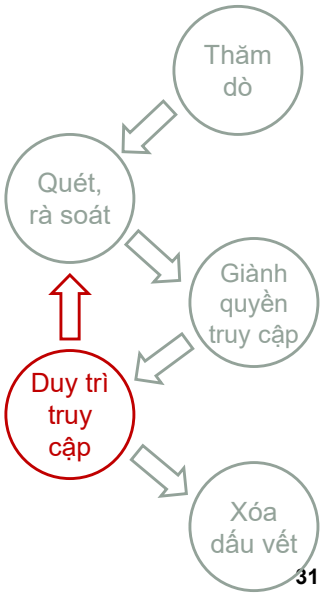
- Kẻ tấn công giành được quyền truy cập vào hệ thống ở các mức độ khác nhau: mức mạng, mức hệ điều hành, mức ứng dụng
- Có thể dựa trên các quyền truy cập đã có để leo thang truy cập



30

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

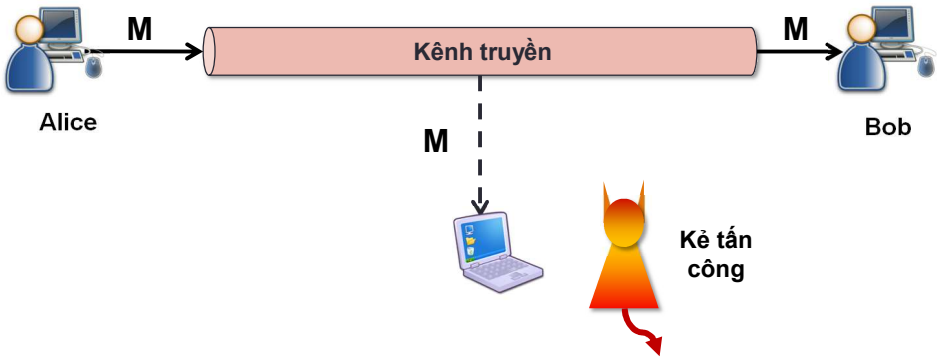


31

Nghe lén

- Thu nhận trái phép các thông tin trong quá trình truyền

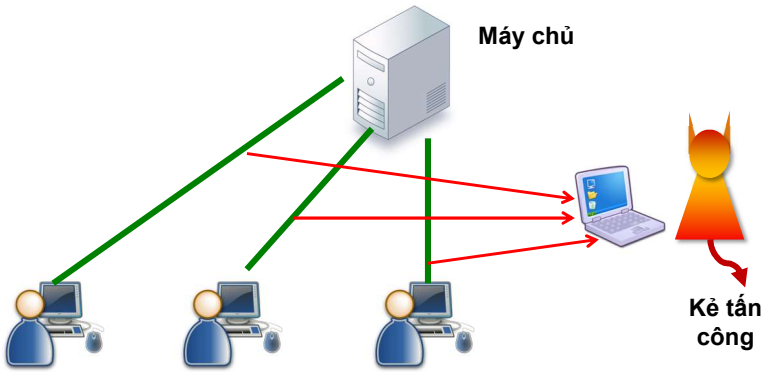
→ tấn công vào tính bí mật của thông tin



32

Phân tích tải

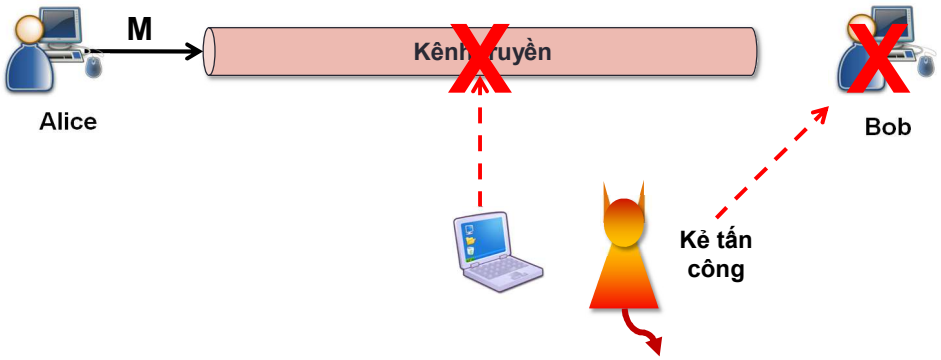
- Quan sát quá trình truyền tin giữa các máy tính trên mạng
- Sau quá trình quan sát, kẻ tấn công có thể phát hiện ra vị trí các tài nguyên-tài sản của hệ thống (máy chủ dịch vụ, máy chủ cơ sở dữ liệu...)



33

Chặn giữ thông điệp

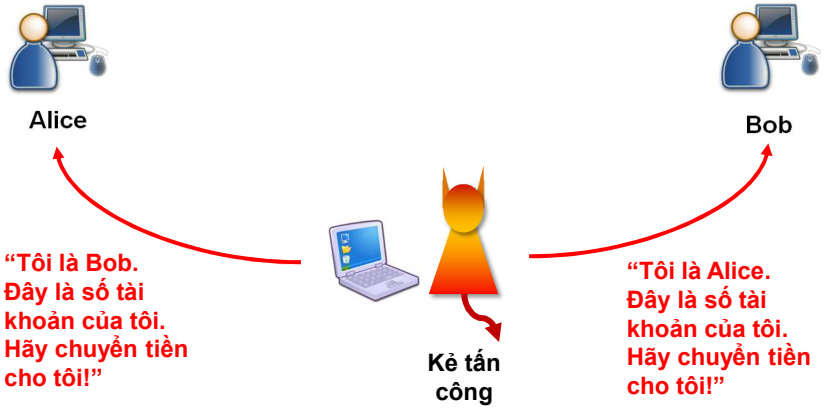
- Chặn giữ thông điệp, ngăn cản việc truyền tin tới các bên



34

Mạo danh

- Kẻ tấn công mạo danh một bên và chuyển các thông điệp cho bên kia.

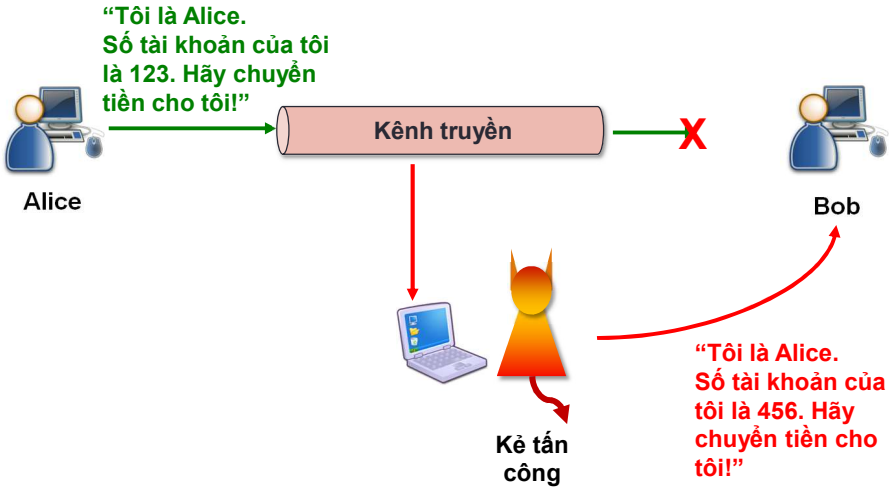


35

35

Thay đổi nội dung thông điệp

- Chặn thông điệp, thay đổi nội dung và chuyển tiếp cho bên kia

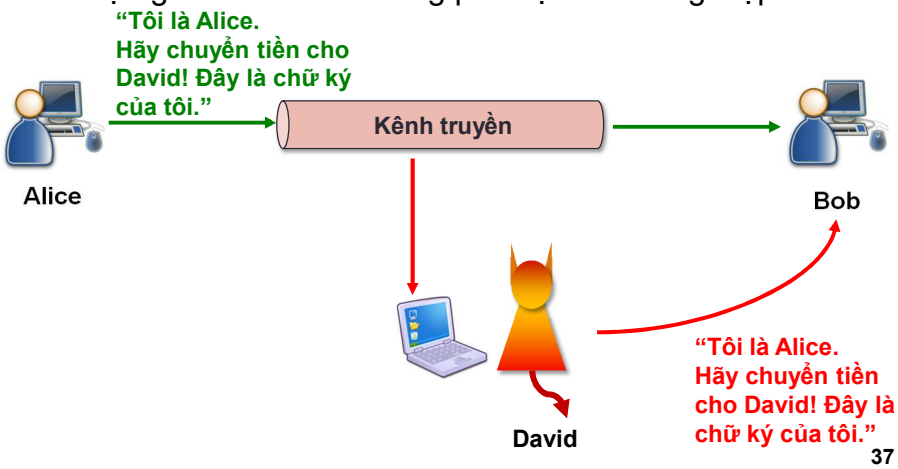


36

36

Phát lại thông điệp

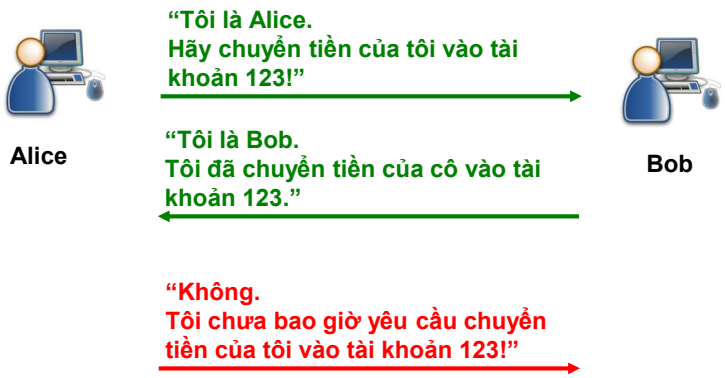
- Lỗ hổng: trên các thông điệp có dấu hiệu xác thực tính tin cậy, nhưng không có giá trị xác định thời điểm thông điệp được gửi đi → kẻ tấn công phát lại các thông điệp cũ



37

Tấn công phủ nhận gửi

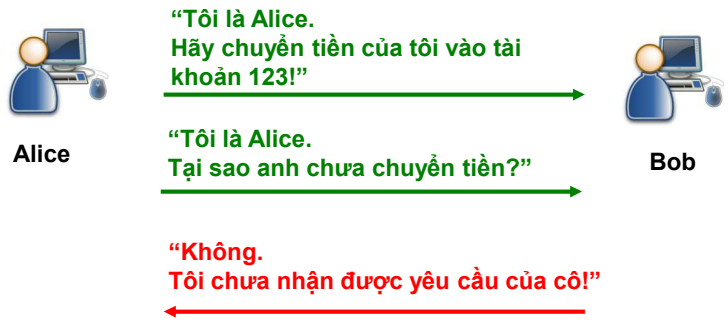
- Bên gửi phủ nhận việc đã gửi đi một thông tin



38

Tấn công phủ nhận nhận

- Bên nhận phủ nhận đã nhận được thông tin



39

4. Xây dựng hệ thống an toàn bảo mật

40

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

Quy trình xây dựng

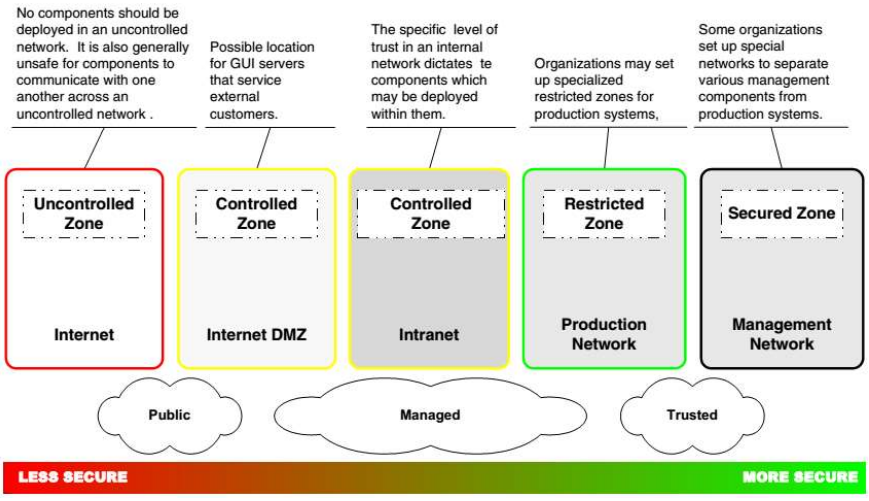
- Xây dựng chính sách: có thể mô tả ban đầu bằng ngôn ngữ tự nhiên:
  - Hành vi phải thực hiện/được phép/ không được phép
  - Chủ thể của hành vi
  - Đối tượng hành vi tác động tới
  - Điều kiện

  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

Quy trình xây dựng

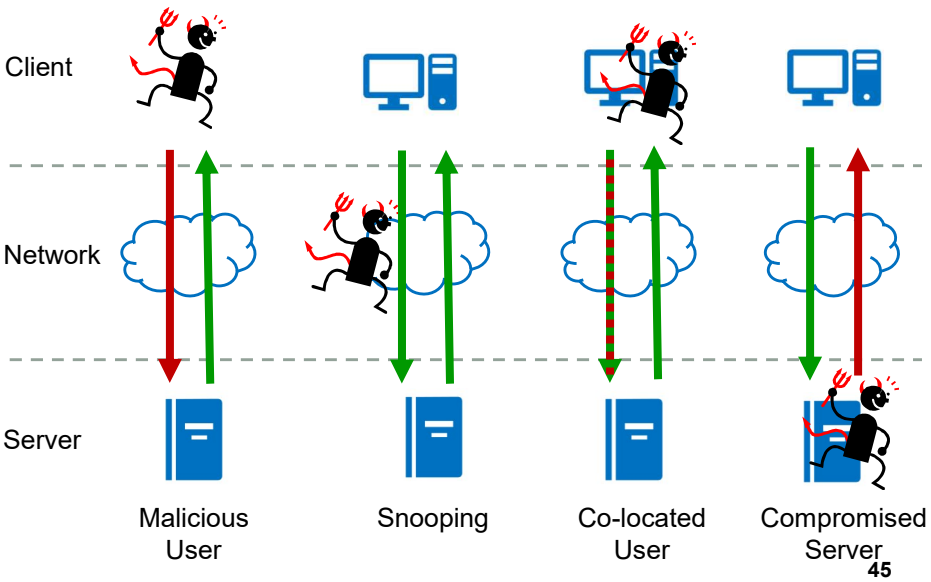
- Xây dựng mô hình nguy cơ:
  1. Xác định, phân vùng tài nguyên cần bảo vệ
  2. Xác định các thành phần, luồng dữ liệu, hành vi tương tác trên tài nguyên
  3. Phân tích các hoạt động diễn ra trên tài nguyên
  4. Xác định các nguy cơ có thể có, phân loại và đánh giá
  5. Xác định các lỗ hổng liên quan

Ví dụ: phân vùng mạng



IBM Security Solutions Architecture for Network, Server and Endpoint

Xây dựng mô hình nguy cơ



45

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

46

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

47

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!

48

AT-ANTT là bài toán kinh tế

TL-15

TL-30

TRTL-30

TXTL-60

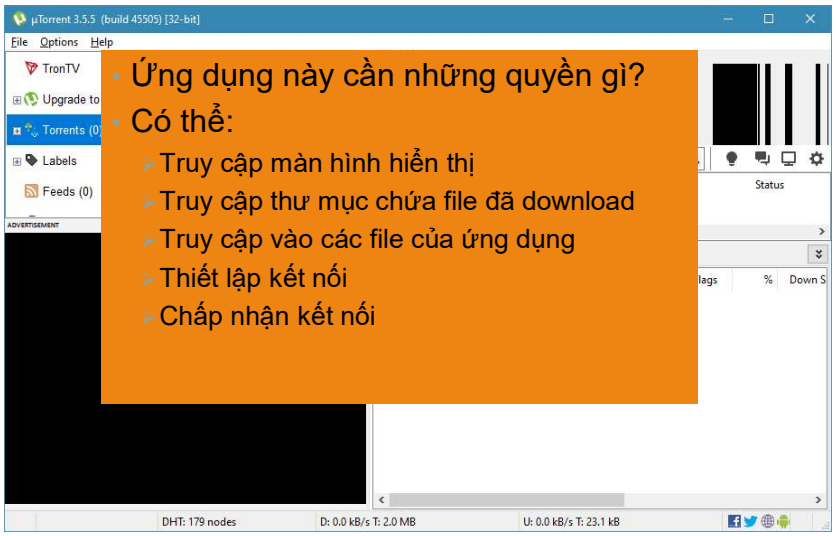
49

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.

50

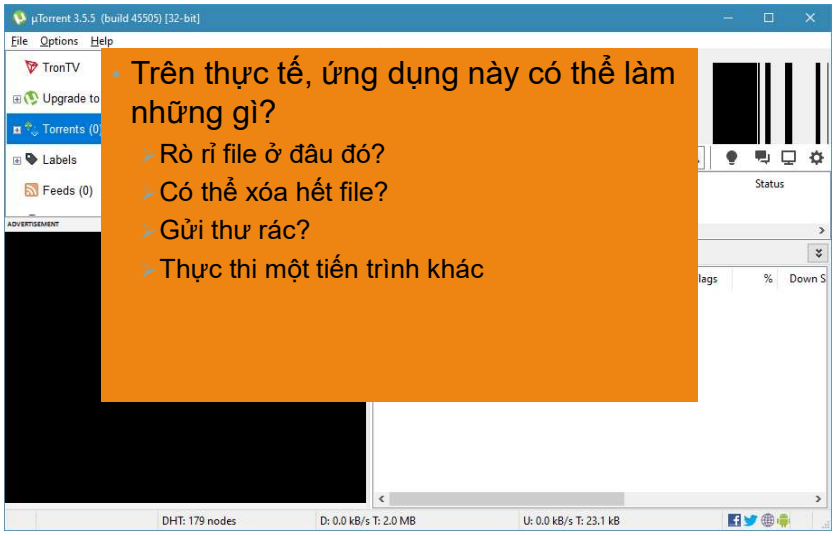
Tối thiểu hóa quyền



- 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

51

Tối thiểu hóa quyền

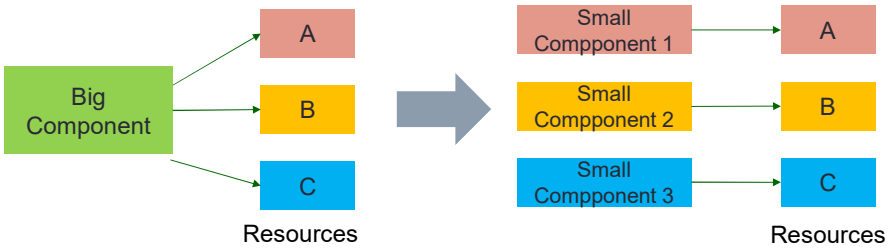


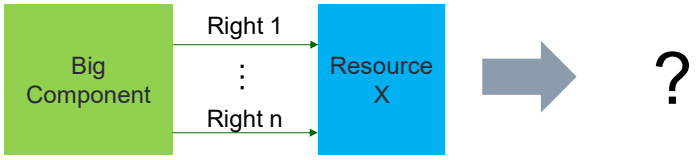
- Trên thực tế, ứng dụng này có thể làm những gì?
  - Rò rỉ file ở đâu đó?
  - Có thể xóa hết file?
  - Gửi thư rác?
  - Thực thi một tiến trình khác

52

Phân chia quyền (Privilege separation)

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





53

Chia sẻ trách nhiệm(Separation of responsibility)

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

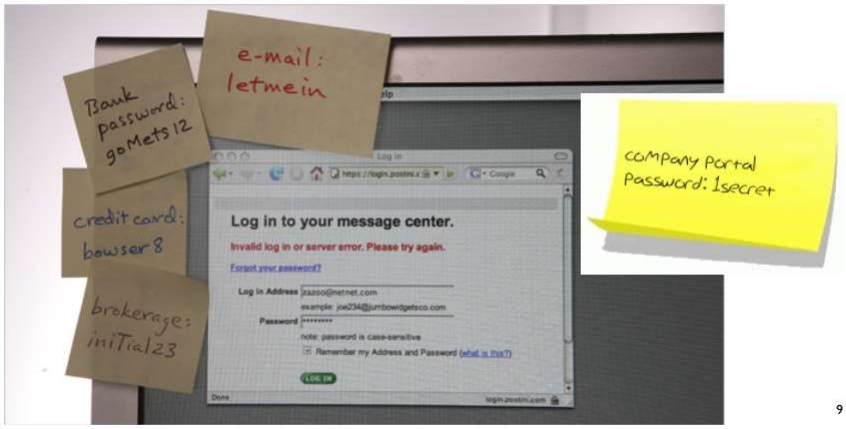
54

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.

55

Dễ hiểu, dễ sử dụng cho người dùng



9

56

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)
  - …

57

Một số nguyên tắc(tiếp)

- Kiểm tra tất cả truy cập

58

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

59

Bảo vệ theo chiều sâu

60

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 obsecurity”)
  - Shannon's Maxim: "The Enemy Knows the System"
- Phát hiện những kỹ thuật tấn công không thể ngăn chặn

61

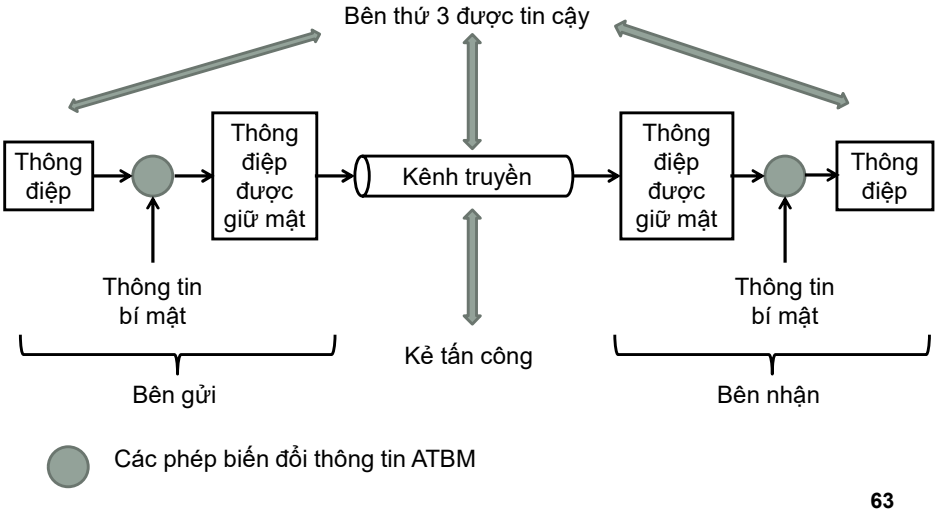
Một số nguyên tắc (tiếp)

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

62

Một số mô hình

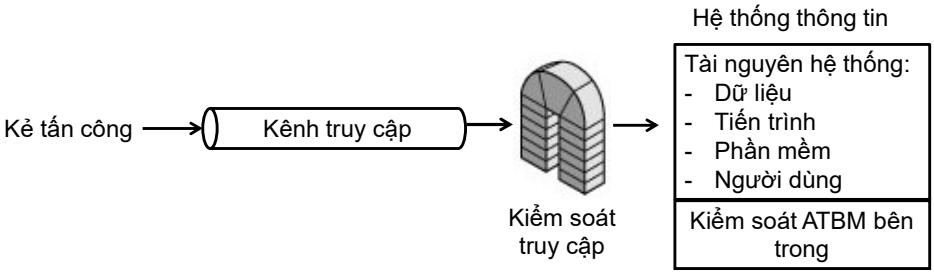
- Mô hình ATBM truyền tin



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

Mô hình ATBM truy cập hệ thống



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

65

65

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

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

66

66