Bài 8: Một số vấn đề an ninh hệ thống

Thời lượng 2 tiết

Lương Thái Lê

Nội dung

- Kẻ xâm nhập: các kỹ thuật xâm nhập, xác định kẻ xâm nhập
- Quản trị mật khẩu
- Các phần mềm có hại: cửa sập, virus, sâu
  - Hệ thống máy tính an toàn
  - Mô hình kiểm soát truy cập

Kẻ xâm nhập

- Một số tình huống xâm nhập:
  - Đoán và lấy mật khẩu, sao chép dữ liệu
- Vấn đề quan trọng đối với hệ thống mạng là chống lại việc truy cập không mong muốn
- Có thể phân loại kẻ xâm nhập:
  - Kẻ giả danh
  - Kẻ lạm quyền
  - Người sử dụng giấu mặt
- Có nhiều kỹ thuật xâm nhập: duyệt toàn bộ, dùng mã độc Trojan horse…

  =>Lấy pass

Đoán mật khẩu

- Là một trong các hướng tấn công chung nhất
- Kẻ tấn công đã biết tên người sử dụng login (từ trang email/web)
- Tìm cách đoán mật khẩu
  - Mặc định, mật khẩu ngắn, tìm kiếm các từ chung
  - Thông tin của người dùng (thay đổi tên, ngày sinh, số phone, các mối quan tâm và từ chung)
  - Tìm kiếm tổng thể mọi khả năng của mật khẩu
- Kiểm tra login với file mật khẩu đánh cắp được
- Thành công phụ thuộc vào mật khẩu được chọn bởi người dùng
- Tổng quan chỉ ra rằng nhiều người sử dụng chọn mật khẩu không cẩn thận

Lấy mật khẩu

- Theo dõi qua vai khi nhập password
- Sử dụng chương trình ngựa thành Toroa để thu thập
- Theo dõi login mạng không an toàn
  - Chẳng hạn Telnet, FTP, Web, email
- Chắt lọc thông tin ghi lại được sau lần vào mạng thành công (đệm/lịch sử web, số quay cuối,…)
- Sử dụng login/password đúng để nhại lại người sử dụng

=>Người sử dụng cần được học để dùng các biện pháp đề phòng và ngăn ngừa thích hợp

Phát hiện kẻ xâm nhập

- Giả thiết rằng kẻ xâm nhập sẽ hành động khác so với người dùng hợp pháp
  - giờ, địa điểm login
  - thử nhiều password
  - đọc, viết, sửa quá nhiều…
- Có 2 hướng tiếp cận:
  - Phát hiệ bất thường thống kê: phát hiện những hành vi thông thường (audit record, profile-based)
  - Phát hiện dựa vào luật (rule-based detection): phát hiện hành vi riêng biệt
    - Tự sinh luật dựa vào dữ liệu
    - Dựa vào ý kiến chuyên gia

Quản trị mật khẩu

- Là bảo vệ tuyến đầu chống kẻ xâm nhập
- Người sử dụng được cung cấp cả hai:
  - Login – xác định đặc quyền của người sử dụng
  - Password – xác định danh tính của họ
- Passwords thường được lưu trữ mã hoá
  - Unix sử dụng DES lặp
  - Các hệ thống gần đây sử dụng hàm hash
- Cần phải bảo vệ file passwords trong hệ thống

Tìm hiểu về mật khẩu

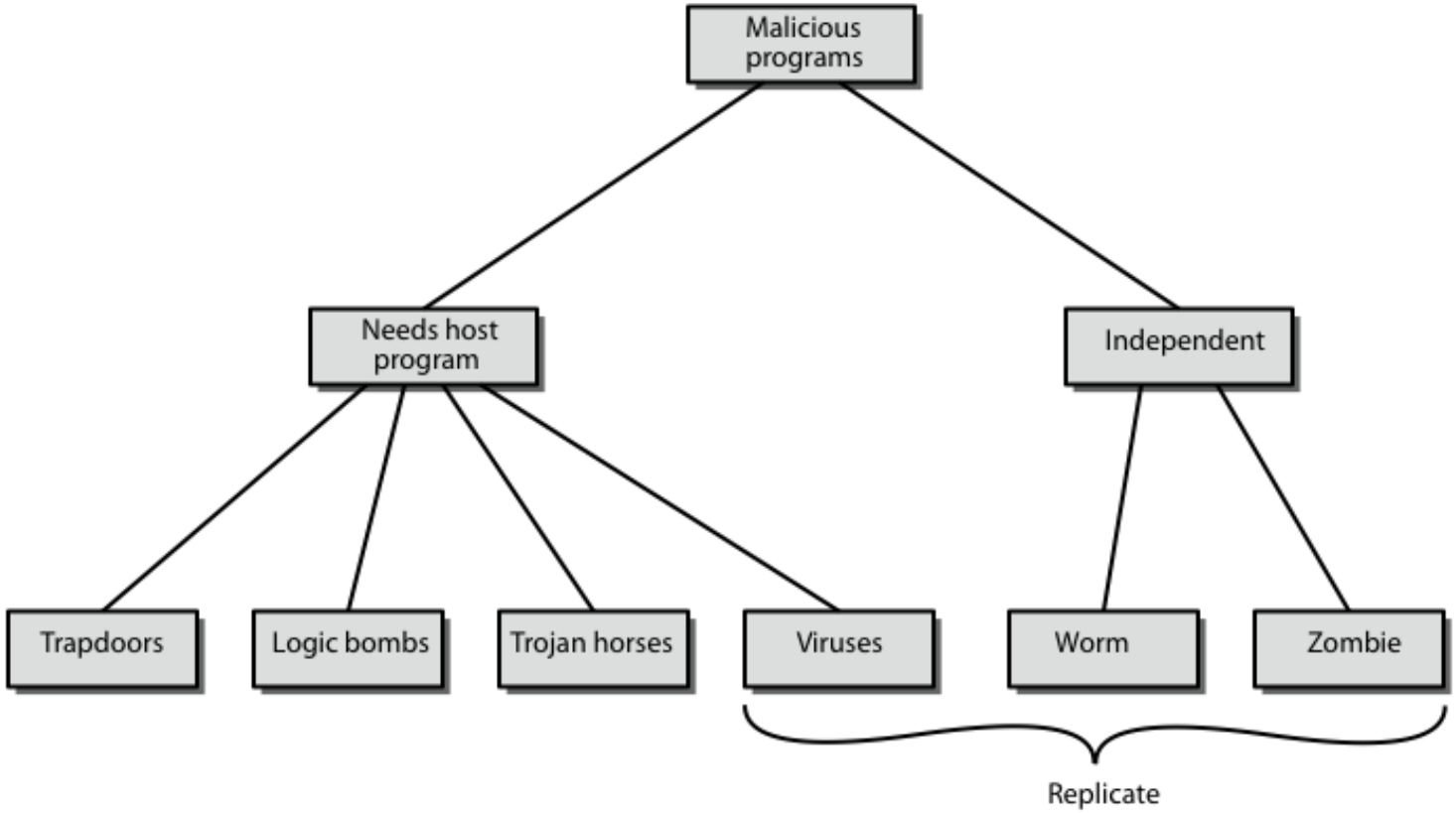
- Purdue 1992 – có nhiều mật khẩu ngắn
- Klein 1990 – có nhiều mật khẩu đoán được

=>người sử dụng thường chọn các mật khẩu không tốt

- Cần một cách tiếp cận để chống lại điều đó:
  - Cách tạo MK đủ khó
  - Dùng phần mềm gợi ý MK khó (FIPS PUB 181)

Phần mềm độc hại (malware)

- Là phương pháp tấn công an ninh tinh vi nhất
- Có 2 loại chính:



Một số loại mã độc hại

- **Cửa sau hay cửa sập** (Back door or Trapdoors): lối vào bí mật của 1 phần mềm mà ko cần qua xác thực
  - Dùng để bảo trì, sửa chữa phần mềm nhưng bị kẻ tấn công sử dụng

  $\Rightarrow$phải nâng cấp phần mềm
- **Bom logic** (Logic bom): là đoạn mã được nén trong 1 phần mềm hợp pháp, bị kích "nổ" khi gặp điều kiện hợp lý.
  - vd: sự có mặt hoặc thiếu 1 file nào đó, 1 ngày giờ đặc biệt nào đó…
  - có thể xóa hoặc thay thế dữ liệu…
- **Ngựa thành Tơ roa** (Trojan horse): là một chương trình hoặc đoạn lệnh thủ tục hữu ích (vd:calculator) chứa một đoạn mã ẩn mà khi được gọi sẽ thực hiện một vài chức năng không mong muốn hoặc có hại
  - cho phép truy cập từ xa, xóa dữ liệu, sao chép hoạt động của bàn phím để lấy mật khẩu, …

Một số loại mã độc hại (tiếp)

- Virus: là một đoạn mã chương trình có khả năng tự nhân bản và lây nhiễm sang các chương trình khác để thực hiện các hành vi được lập trình trước.
  - thường được cấy vào 1 tập tin thực thi (microsoft)
  - xóa dữ liệu, làm hỏng ổ cứng… lấy cắp thông tin
  - WannaCry (2017): tống tiền bằng cách mã hóa dữ liệu (Window)
- Các hình thức lây nhiễm virus:
  - cổ điển: usb, đĩa cứng di động…
  - qua email: qua file đính kèm, qua đường link, hoặc ngay khi mở thư
  - qua internet: tải phần mềm,

Một số loại mã độc hại (tiếp)

- Sâu (Worm): là một chương trình có khả năng tự nhân bản trên chính nó mà không cần cấy vào một chương trình thực thi khác
  - thường lây lan qua Internet => để phòng ngừa thì cần luôn cập nhật những bản an ninh mới nhất cho hệ điều hành.
- Zombie: Chương trình được kích hoạt trên một máy bị nhiễm được kích hoạt để khởi động các cuộc tấn công gián tiếp vào các máy khác
  - thường để khởi động tấn công từ chối dịch vụ phân tán

Các biện pháp chống malware

- Biện pháp tốt nhất là ngăn ngừa
- Nhưng nói chung là không thể
- Suy ra cần phải có một trong nhiều biện pháp sau:
  - Phát hiện virus nhiễm trong hệ thống
  - Định danh loại virus nhiễm
  - Loại bỏ, khôi phục hệ thống về trạng thái sạch

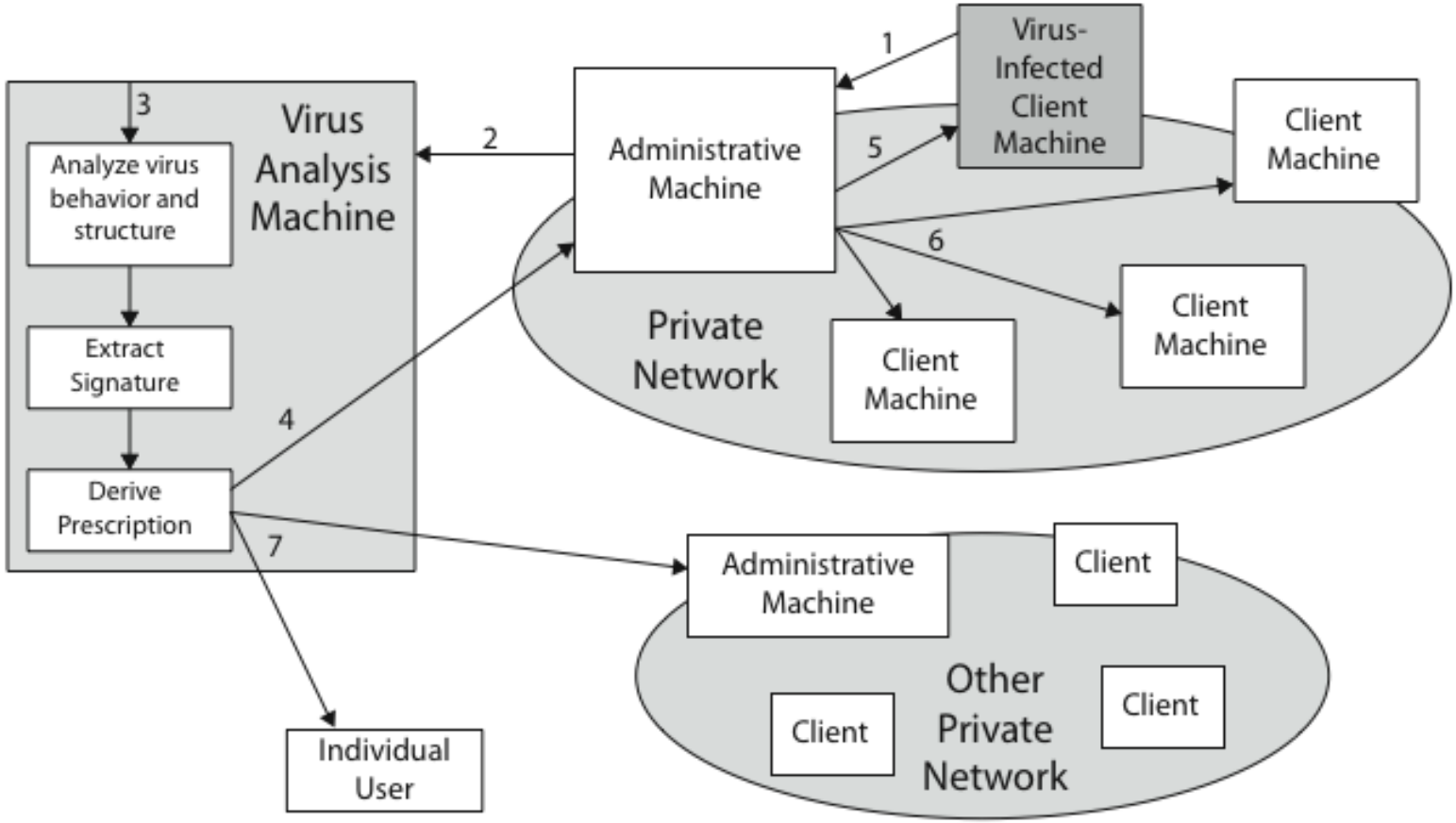
Các thế hệ Phần mềm chống Virus

- Thế hệ đầu tiên
  - Quét sử dụng chữ ký của virus để định danh
  - Hoặc phát hiện sự thay đổi độ dài của chương trình
- Thế hệ thứ hai
  - Sử dụng các qui tắc trực quan để phát hiện nhiễm virus
  - Sử dụng mã hash của chương trình để phát hiện sự thay đổi
- Thế hệ thứ ba
  - Chương trình thường trú trong bộ nhớ định danh virus theo hành động
- Thê hệ thứ tư
  - Đóng gói với rất nhiều kiểu kỹ thuật chống virus
  - Quét và lần vết tích cực, kiểm soát truy cập
- Diệt bằng tay vẫn được dùng

Kỹ thuật chống Virus nâng cao

- Giải mã mẫu
  - Sử dụng mô phỏng CPU kiểm tra chương trình, chữ ký và hành vi trước khi chạy chúng
- Hệ thống miễn dịch số (IBM)
  - Hành động đa muc tiêu và chống Virus
  - Mọi virus nhập vào tổ chức được nắm bắt, phân tích, phát hiện/tấm chắn tạo ra chống nó và loại bỏ

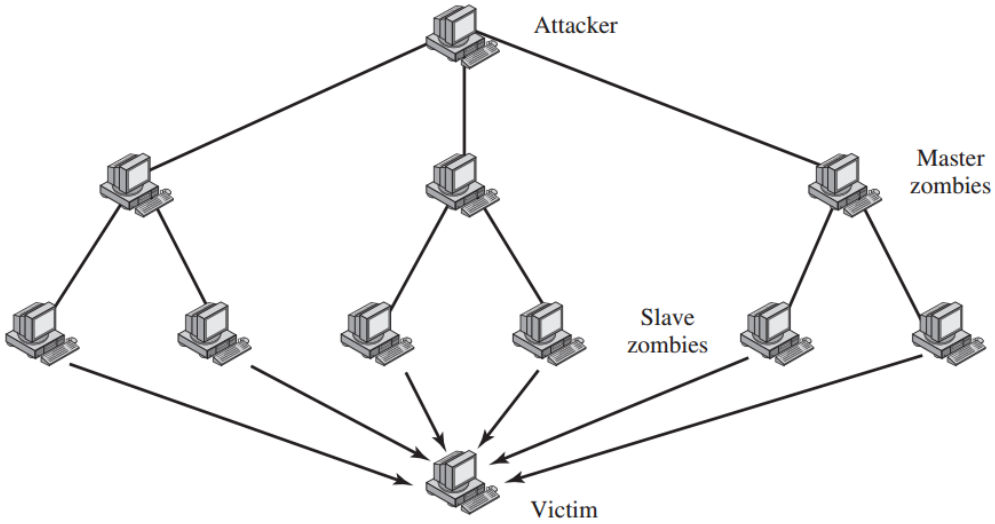
Hệ miễn dịch số - Digital Immune System



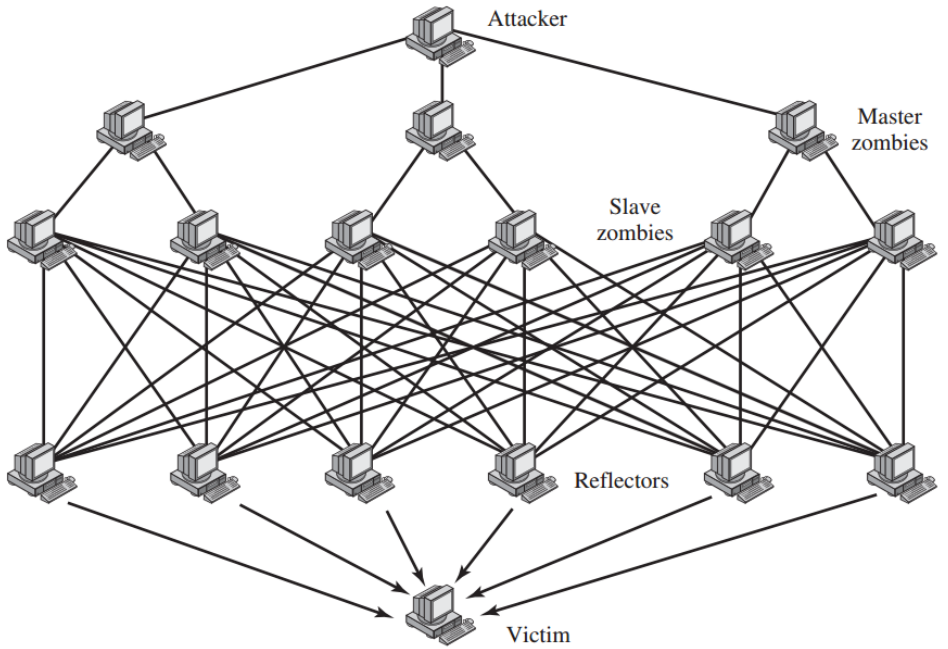
Tấn công từ chối dịch vụ từ xa (Distributed Denial of Service Attacks-DDoS)

- **Mục đích**: Làm cho hệ thống không sẵn sàng bằng cách làm tràn bởi sự vận chuyển vô ích
- Trong một cuộc tấn công DDoS, kẻ tấn công có thể tuyển dụng một số máy chủ lưu trữ trên Internet (host) để phối hợp phát động một cuộc tấn công vào mục tiêu
- Sử dụng một số lớn các “zombies”
- Chia thành 2 kiểu: trực tiếp & gián tiếp

DDoS: trực tiếp và gián tiếp



(a) Direct DDoS Attack



(b) Reflector DDoS Attack

=> cần lây nhiễm
Zombie cho nhiều máy

Chống tấn công từ chối dịch vụ từ xa

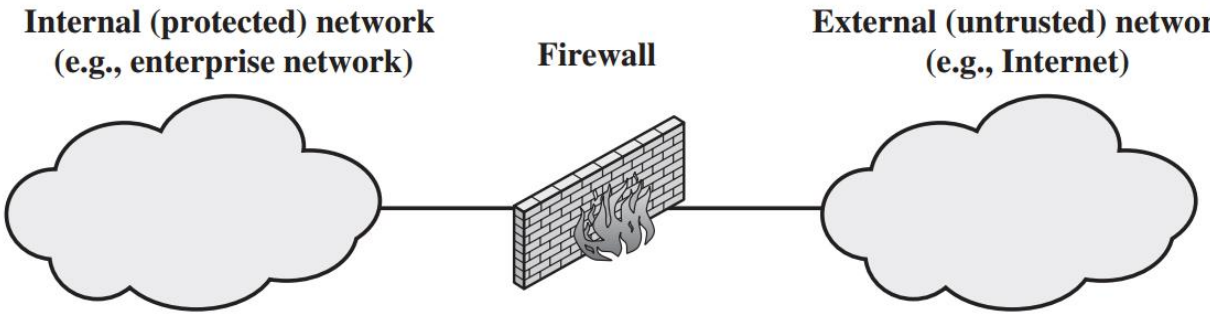
- Ba cách bảo vệ được dùng rộng rãi
  1. Ngăn ngừa tấn công và chiếm lĩnh trước khi bị tấn công
     - Kỹ thuật bao gồm thực thi chính sách tiêu thụ tài nguyên và cung cấp tài nguyên dự phòng có sẵn theo yêu cầu
  2. Phát hiện tấn công và lọc trong quá trình bị tấn công
     - tìm kiếm các mô hình hành vi đáng ngờ
  3. Lần vết nguồn tấn công và định danh sau khi bị tấn công
     - thường dùng để chống các tấn công tiếp theo

Tường lửa – Firewall

- Là một thiết bị phần cứng và/hoặc một phần mềm (router) để kiểm soát và theo dõi thông tin vào ra mạng cục bộ. Nó quyết định sự vận chuyển nào được đi qua và đi theo hướng nào.

  =>bảo vệ các nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống

- Thường thực thi như bộ lọc ở tầng đóng gói IP hoặc có thể ở 1 tầng giao thức cao hơn
- Tường lửa miễn nhiễm với các xâm nhập trái phép
- Được công bố năm 1988 bởi Jeff Mogul



(a) General model

Phân loại và vai trò của tường lửa

- Phân loại theo phạm vi truyền thông được lọc: 2 loại
  - **Tường lửa cá nhân**: một ứng dụng phần mềm với chức năng thông thường là lọc dữ liệu ra vào một máy tính đơn
  - **Tường lửa mạng**: thường chạy trên một thiết bị mạng hay máy tính chuyên dụng đặt tại ranh giới của hai hay nhiều mạng
- Vai trò:
  - Vai trò chính là bảo mật thông tin, ngăn chặn sự truy cập không mong muốn từ bên ngoài (Internet) và cấm truy nhập từ bên trong (Intranet) ra bên ngoài (Internet).
  - Điều tiết lưu lượng mạng giữa các phân đoạn mạng (bên trong lẫn bên ngoài).
  - Là nơi áp đặt các chính sách điều khiển truy cập

Hạn chế của tường lửa

- Làm chậm tốc độ kết nối mạng
- những người sử dụng có hiểu biết có thể dễ dàng vượt qua tường lửa bằng cách sử dụng các proxy không bị ngăn chặn
- Không bảo vệ chống các mối đe dọa từ bên trong
- Không thể bảo vệ chống việc truyền các chương trình hoặc file nhiễm virus

=>Kỹ thuật vượt tường lửa:

- thay đổi địa chỉ proxy, DNS
- sử dụng phần mềm: Tor, Freegate

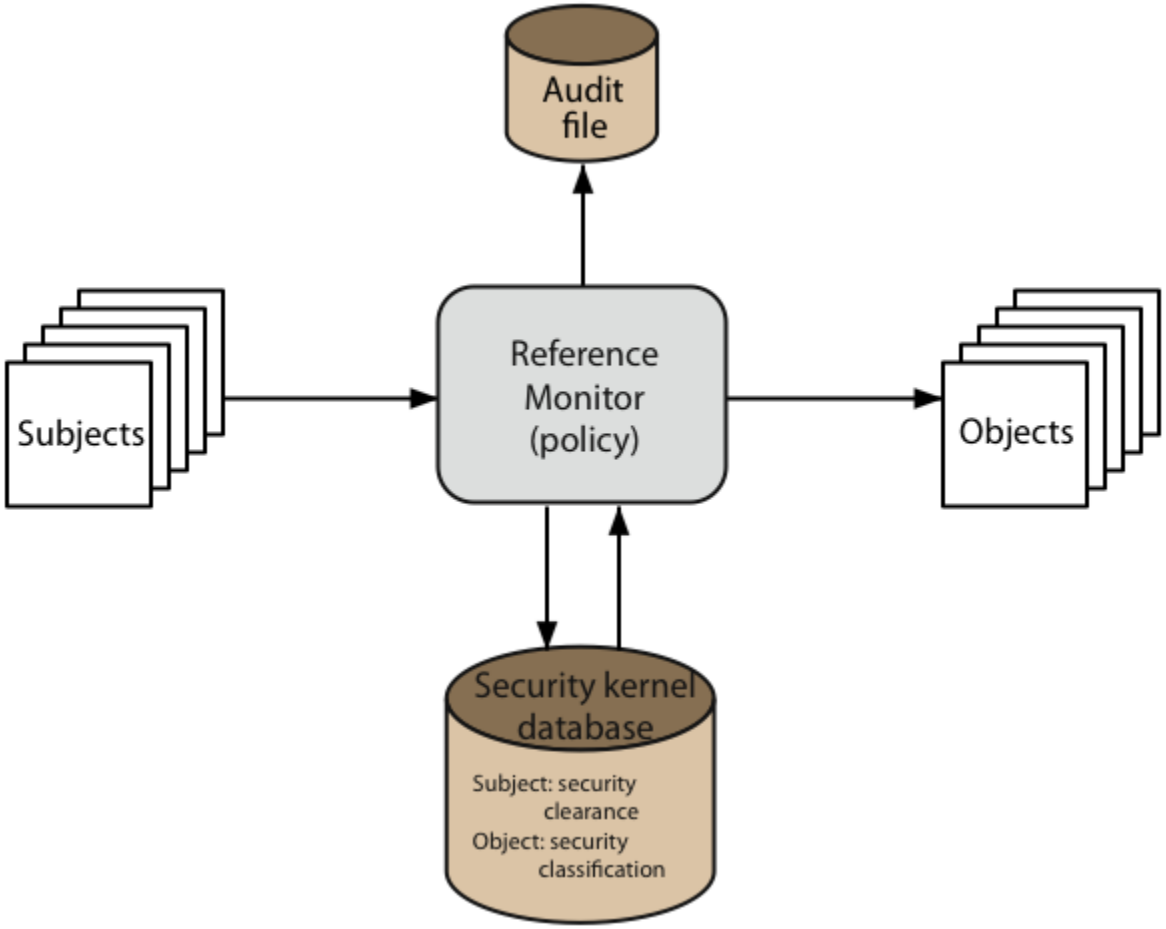
8.4 Các hệ thống máy tính tin cậy

- An toàn thông tin ngày càng quan trọng
- Có các mức độ khác nhau về sự nhạy cảm của thông tin
  - Phân loại thông tin quân sự: bảo mật, bí mật
- Chủ thể (người hoặc chương trình) có nhiều quyền khác nhau truy cập đến các đối tượng thông tin
- Được biết như an toàn nhiều tầng
  - Chủ thể có mức độ an toàn tối đa và hiện tại
  - Đối tượng có phân loại mức độ tin cậy cố định
- Muốn xem xét các cách tăng độ tin tưởng trong hệ thống để củng cố các quyền đó

Mô hình Bell LaPadula

- Một trong những mô hình an toàn nổi tiếng nhất
- Được cài đặt như các chính sách bắt buộc trong hệ thống
- Có hai chính sách chính
  - Không đọc lên (tính chất an toàn đơn giản)
    - Chủ thể chỉ có thể đọc các đối tượng nếu mức độ an toàn hiện tại của chủ thể trội hơn (>=) phân loại của đối tượng
  - Không viết xuống (tính chất *)
    - Chủ thể chỉ có thể bổ sung/viết lên đối tượng nếu mức độ an toàn hiện tại của chủ thể được trội (<=) bởi phân loại của đối tượng

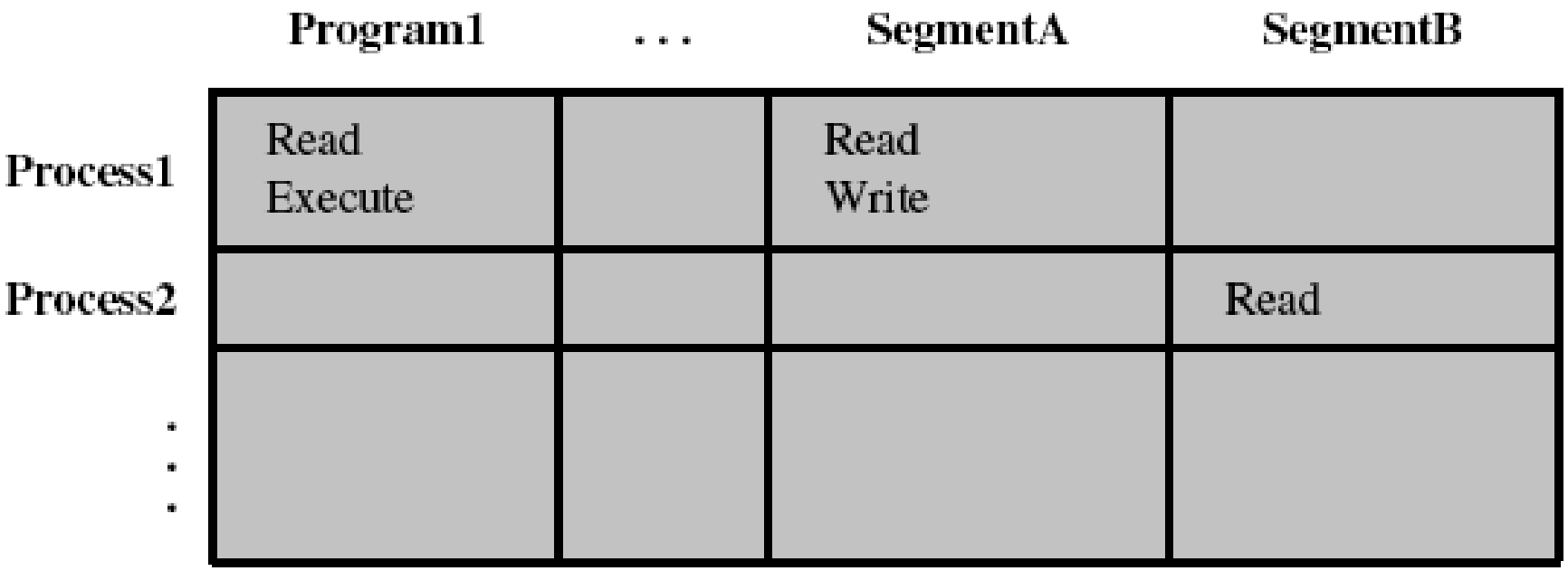
Giám sát tham chiếu



Kiểm soát truy cập

- Hệ thống đã cho được định danh như người sử dụng
- Xác định các nguồn gốc nào nó có thể truy cập
- Mô hình tổng quát là ma trận truy cập với
  - Chủ thể - thực thể chủ động (người sử dụng, quá trình)
  - Đối tượng - thực thể bị động (file hoặc nguồn)
  - Quyền truy cập – cách mà đối tượng được truy cập
- Có thể được phân tách bởi
  - Các cột như danh sách kiểm soát truy cập đến đối tượng đầu cột
  - Các hàng như các thẻ về khả năng truy cập của chủ thể đầu hàng

Ma trận kiểm soát truy cập



(a) Access matrix

Tóm lại

- Đã xem xét:
  - Kẻ xâm nhập
  - Quản trị mật khẩu
  - Virus và các phần mềm có hại
  - Các hệ thống tin cậy
  - Kiểm soát truy cập

Câu hỏi trắc nghiệm

1. Mục nào không thuộc phân loại của Kẻ xâm nhập:
   A. Kẻ giả danh
   B. @Kẻ xem lén
   C. Kẻ lạm quyền
   D. Người sử dụng giấu mặt
2. Đâu không phải là mục tiêu của kẻ xâm nhập
   A. Nắm bắt mật khẩu người sử dụng hợp pháp
   B. Đăng nhập vào hệ thống để khai thác và phá hoại thông tin
   C. Leo thang tăng quyền truy cập thông tin
   D. @Đăng ký thành viên hợp pháp
3. Không dựa vào giả thiết nào để đoán mật khẩu
   A. Mật khẩu ngắn, dễ nhớ
   B. Thông tin cá nhân người sở hữu tài khoản
   C. @Mật khẩu dài, ngẫu nhiên, không có ngữ nghĩa
   D. File mật khẩu đánh cắp được hoặc dò tìm mò

Câu hỏi trắc nghiệm

4. Mục nào không thuộc việc cần làm để phát hiện kẻ xâm nhập:
   A. Chia khối để phát hiện nhanh
   B. @Bảo mật dữ liệu
   C. Hành động ngăn chặn
   D. Thu thập thông tin để tăng cường an ninh

5. Điều nào không đúng trong cách tiếp cận phát hiện hành động bất thường theo ngưỡng:
   A. Đếm sự xuất hiện của sự kiện đặc biệt theo thời gian
   B. Nếu vượt quá giá trị nào đó thì cho là đã có xâm nhập
   C. Nếu chỉ dùng nó thì đây là phát hiện thô không hiệu quả
   D. @Theo dõi lý lịch hành vi của người sử dụng đó

6. Điều gì không đúng với việc phát hiện xâm nhập dựa trên mô tả
   A. @ Đếm sự xuất hiện của sự kiện đặc biệt theo thời gian
   B. Đặc trưng hành vi quá khứ của người sử dụng
   C. Phát hiện hệ quả quan trọng từ đó
   D. Mô tả bằng nhiều tham số

Câu hỏi trắc nghiệm

7. Điều gì không đúng với Bản ghi kiểm tra đơn giản:
   A. Một phần của hệ điều hành đa người sử dụng
   B. Sẵn sàng để sử dụng
   C. Có thể không có thông tin trong định dạng mong muốn
   D. @Được tạo chuyên dùng để thu thập một số thông tin mong muốn
8. Điều nào không đúng đối với phát hiện dựa trên qui tắc:
   A. Phân tích bản ghi để xác định mẫu sử dụng và qui tắc tự sinh
   B. Quan sát hành vi hiện tại và sánh với các qui tắc
   C. @Xác định các tham số ngưỡng tần suất xuất hiện sự kiện
   D. Không đòi hỏi kiến thức biết trước về sai lầm an ninh
9. Điều nào không đúng trong việc định danh kẻ xâm nhập theo qui tắc
   A.@ Phân tích bản ghi kiểm tra
   B. Sử dụng công nghệ hệ chuyên gia
   C. Dùng các mẫu điểm yếu, hoặc các hành vi nghi ngờ
   D. So sánh các bản ghi kiểm tra hoặc các trạng thái theo qui tắc

Câu hỏi trắc nghiệm

10. Điều nào không đúng trong việc thu hút kẻ tấn công
    A. Tách khỏi sự truy cập đến các hệ thống then chốt
    B. Để thu thập các thông tin về hoạt động của chúng
    C. Kích thích kẻ tấn công ở lại trong hệ thống để có thể phán đoán
    D. @Giăng bẫy tại các phần quan trọng
11. Điều nào không phải là định hướng mật khẩu tốt
    A. Độ dài tối thiểu > 6
    B. @Dựa trên các thông tin cá nhân
    C. Đòi hỏi trộn chữ hoa và chữ thường, số và dấu chấm
    D. Không chọn từ trong từ điển
12. Điều nào không đúng trong việc kiểm tra trước mật khẩu:
    A. Được chọn trước mật khẩu để kiểm tra
    B. Bắt buộc theo qui tắc đơn giản như không dựa vào thông tin cá nhân
    C. So sánh với từ điển các mật khẩu tồi
    D. @Thường dùng Từ điển lớn hỗ trợ

Câu hỏi trắc nghiệm

13. Điều nào không đúng với phần mềm cửa sập
    A. Điểm vào chương trình bí mật
    B. Cho phép những người biết truy cập mà bỏ qua các thủ tục an toàn
    C. @Có thể lây lan sang các hệ thống khác
    D. Là mối đe doạ khi chương trình được khai thác bởi kẻ tấn công
14. Điều nào không đúng đối với Ngựa thành Tơ roa
    A. Chương trình có tác động phụ được giấu kín
    B. @Được kích hoạt bởi ngày tháng cụ thể
    C. Thường hấp dẫn như trò chơi, phần mềm miễn phí
    D. Thực hiện nhiệm vụ bổ sung như lan truyền virus, sâu, phá hoại dữ liệu
15. Điều nào không đúng đối với Zombie:
    A. @Được kích hoạt bởi chương trình khác
    B. Chương trình bí mật điều khiển máy tính của mạng khác
    C. Dùng để khởi động tấn công từ chối dịch vụ phân tán
    D. Khai thác các lỗ hổng trong hệ thống

Câu hỏi trắc nghiệm

16. Điều nào không đúng đối với Virus
    A. Là đoạn code tự sinh lặp đính kèm code khác
    B. Tự nó lan truyền mà mang theo code để tạo bản sao của nó
    C. Thực hiện các hành động ngầm phá hoại
    D. @Có thể hoạt động độc lập không cần chương trình khác của máy
17. Điều nào không đúng đối với sâu:
    A. Sinh lặp chủ yếu, có thể có các hành động phụ
    B. Lan truyền trên mạng cực nhanh tấn công từ chối dịch vụ
    C. @Cần có chương trình khác của máy để đính kèm
    D. Khai thác các lỗ hổng của hệ thống
18. Đâu không phải là biện pháp hiệu quả phòng chống virus:
    A. @Không sao chép chương trình không biết nguồn gốc
    B. Phân tích, ngăn ngừa các phần mềm nghi ngờ, ngăn chặn hành vi
    C. Sử dụng mã hash của chương trình để phát hiện bị nhiễm
    D. Định danh virus, loại bỏ, khôi phục trạng thái sạch

Câu hỏi trắc nghiệm

19. Mục nào không phải là cách bảo vệ chống tấn công từ chối dịch vụ:
    A. Ngăn ngừa tấn công và chiếm lĩnh trước
    B. Phát hiện tấn công và lọc trong quá trình
    C. Lần vết nguồn tấn công và định danh tấn công
    D. @Xây dựng hệ thống máy tính mạnh đáp ứng mọi yêu cầu
20. Đâu không phải là chính sách của mô hình máy tính an toàn Bell LaPadula
    A. Không đọc lên: chủ thể được đọc các đối tượng có mức an ninh <=
    B. @Có nhiều mức độ an ninh cho đối tượng và chủ thể
    C. Không viết xuống: chủ thể được viết lên đối tượng có mức an ninh >=
    D. @Chủ thể có mức độ an ninh tối đa vfa hiện tại, đối tượng có mức an ninh cố định
21. Điều nào không đúng đối với ma trận kiểm soát truy cập
    A. Cột đầu là các chủ thể, hàng đầu là các đối tượng
    B. Các cột như danh sách kiểm soát truy cập đến đối tượng đầu cột
    C. Các hàng như các thẻ về khả năng truy cập của chủ thể đầu hàng
    D. @Cột đầu là các đối tượng, hàng đầu là các chủ thể

Glossary - Từ điển thuật ngữ

- **Kẻ xâm nhập:** là con người hoặc phần mềm mà truy cập không hợp pháp vào hệ thống máy tính của một tổ chức hoặc cá nhân nào đó
- **Bình mật ong**: nơi chăng lưới thu hút các kẻ tấn công và tách nơi đó khỏi sự truy cập đến các hệ thống then chốt với mục đích thu thập các thông tin về hoạt động của kẻ tấn công
- **Cửa sau hoặc cửa sập**

  điểm vào chương trình bí mật, cho phép những người biết truy cập mà bỏ qua các thủ tục an toàn thông thường. Kỹ thuật này có thể được sử dụng chung bởi những người phát triển và là mối đe doạ khi có trong chương trình sản phẩm
- **Bom logic**

  đây là một trong những phần mềm có hại kiểu cổ, code được nhúng trong chương trình hợp pháp.

Glossary - Từ điển thuật ngữ

- **Ngựa thành Tơ roa**

  Chương trình với các tác động phụ được dấu kín, mà thông thường rất hấp dẫn như trò chơi hoặc phần mềm nâng cấp. Khi chạy thực hiện những nhiệm vụ bổ sung, cho phép kẻ tấn công gián tiếp dành quyền truy cập mà họ không thể trực tiếp. Thông thường sử dụng lan truyền virus/sâu (worm) hoặc cài đặt cửa sau hoặc đơn giản phá hoại dữ liệu.

- **Zombie**

  đây là chương trình bí mật điều khiển máy tính của mạng khác và sử dụng nó để gián tiếp tiến hành các tấn công. Thông thường sử dụng để khởi động tấn công từ chối các dịch vụ phân tán (DdoS). Nó khai thác các lỗ hổng trong các hệ thống.

- **Virus**

- là đoạn code tự sinh lặp đính kèm với code khác như virus sinh học. Nó tự lan truyền mang theo code để tạo các bản sao của chính nó. Và nó cũng thực hiện nhiệm vụ ngầm nào đó như phá hoại các files hệ thống..

Glossary - Từ điển thuật ngữ

- **Sâu**

  là chương trình tự sinh lặp và gửi các bản sao lan truyền trên mạng từ hệ thống này sang hệ thống khác. Khi đến nơi mới nó có thể tự kích hoạt sinh tiếp và lan truyền. Nó thực hiện các hành động phá hoại.

- **Tấn công lặp**

  là tấn công mà ở đó dịch vụ có chủ quyền đã được thực hiện xong, nhưng bị giả mạo bởi yêu cầu lặp khác để tìm cách sử dụng lại những lệnh có chủ quyền.

- **Tấn công từ chối dịch vụ**

  là tấn công làm cho hệ thống trở nên không sẵn sàng, làm tràn bởi sự vận chuyển và thực hiện những việc vô ích. Kẻ tấn công thường sử dụng một số lớn các “zombies” để tăng độ khó của các tấn công.

FAQ – Câu hỏi thường gặp

- **Câu 1.** Liệt kê và mô tả ba loại kẻ xâm nhập?
- **Câu 2.** Kỹ thuật chung để bảo vệ file mật khẩu là gì?
- **Câu 3.** Các lợi ích nào đem lại nếu được trang bị hệ thống phát hiện kẻ xâm nhập?
- **Câu 4.** Nêu sự khác biệt giữa phát hiện dựa trên thống kê hành vi bất thường và phát hiện dựa trên qui tắc?
- **Câu 5.** Những đại lượng nào hữu ích cho phát hiện kẻ xâm nhập dựa trên hồ sơ?
- **Câu 6.** Bình mật ong là gì?
- **Câu 7.** Muối là gì trong bối cảnh quản trị khóa Unix?
- **Câu 8**. Liệt kê và mô tả vắn tắt các kỹ thuật chống đoán mật khẩu?

FAQ – Câu hỏi thường gặp

- **Câu 9.** Mô tả một số loại phần mềm có hại?
- **Câu 10.** Mô tả hoạt động của virus đơn giản?
- **Câu 11.** Nêu các pha của thao tác virus và sâu?
- **Câu 12.** Mô tả một số kiểu virus?
- **Câu 13.** Nêu khái quát sâu được lan truyền như thế nào?
- **Câu 14.** Nêu các biện pháp chống virus?
- **Câu 15.** Hệ miễn dịch số là gì?
- **Câu 16**. Giải thích ý nghĩa của ma trận kiểm soát quyền truy cập?

Hướng dẫn trả lời câu hỏi thường gặp FAQ

1. Ba loại kẻ xâm nhập
   - Kẻ giả danh: thâm nhập tài khoản hợp pháp
   - Kẻ lạm quyền: tìm cách truy cập trái phép
   - Người sử dụng giấu mặt: tiếm quyền quản trị, giả danh người khác
2. Kỹ thuật chung bảo vệ file mật khẩu:
   - Bổ sung mật khẩu đủ dài và mã hóa
   - Lưu giữ bản băm mật khẩu hoặc khóa sinh từ mật khẩu
3. Lợi ích dùng hệ thống phát hiện kẻ xâm nhập:
   - Kịp thời ngăn chặn
4. Sự khác biệt giữa phát hiện dựa thống kê và qui tắc:
   - Thống kê: không phụ thuộc các lỗ hổng và đặc trưng của hệ thống
   - Qui tắc: dựa vào các đặc trưng của hệ thống, các lỗ hổng
5. Đại lượng hữu ích cho phát hiện dựa hồ sơ: Bản ghi kiểm tra

Hướng dẫn trả lời câu hỏi thường gặp FAQ

6. Bình mật ong
   - Lôi kéo kẻ thám mã đến và hoạt động lâu ở đó
   - Tung thông tin giả, ở những nơi không quan trọng
   - Thu thập thông tin về kẻ thám mã, nhận diện
7. Muối trong quản lý mật khẩu của Unix:
   - Độ dài 12 bit bổ sung vào khóa và mã hóa
   - Cho đủ dài và thêm yếu tố ngẫu nhiên không phụ thuộc NSD
8. Các kỹ thuật chống đoán mật khẩu:
   - Tìm mật khẩu tồi, kiểm tra mật khẩu khi đăng ký, so sánh với từ điển mật khẩu tồi
9. Mô tả phần mềm có hại:
   - Cần chương trình máy chủ: cửa sập, bom logic, ngựa thành Tơ roa, virus
   - Độc lập lan truyền: Sâu, Zombie

Hướng dẫn trả lời câu hỏi thường gặp FAQ

10. Hoạt động virus đơn giản
    - Đính kèm – nhiễm sang các file
    - Đủ điều kiện thì kich hoạt phá hoại
11. Các pha thao tác của virus và sâu:
    - Nằm in, lan truyền, kích hoạt, thực hiện bộ tải
12. Một số kiểu virus:
    - Ăn bám, cư trú ở bộ nhớ, ở sector khởi động
    - Lén lút, nhiều hình thái, biến hoá
13. Xem bài giảng
14. Xem bài giảng
15. Hệ miễn dịch: sử dụng máy quản trị và máy phân tích phòng chống
16. Ma trận kiểm soát truy cập:
    - Cột gắn với đối tượng được truy cập bởi các chủ thể
    - Hàng gắn với chủ thể: quyền truy cập đến các đối tượng của nó