Chương 10: Bảo mật và An toàn thông tin

Tìm hiểu một số cơ chế bảo mật & an toàn thông tin trong Hệ điều hành

Nội dung

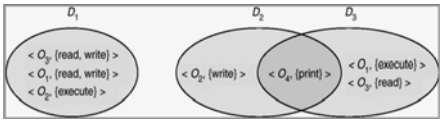
- Protection Problem
  - Cấu trúc Protection Domain
  - Ma trận truy nhập - Access Matrix
- Security Problem
  - Thẩm định quyền - Authentication
  - Các hiểm họa chương trình - Program Threats
  - Các hiểm họa hệ thống - System Threats
  - Giám sát hiểm họa - Threat Monitoring
  - Tường lửa - Firewall
  - Mã hóa - Encryption

1. The Protection Problem

- Hệ thống máy tính gồm một tập hợp các tiến trình và các đối tượng (hardware và software).
- Mỗi đối tượng có một tên duy nhất và có thể được truy nhập qua một tập các thao tác xác định.
- Protection problem – đảm bảo rằng mỗi đối tượng được truy nhập đúng và chỉ bởi những tiến trình được phép.
- Chỉ quan tâm đến môi trường bên trong hệ thống (internalenvironment)

1.1. Cấu trúc Protection Domain

- Access-right = <*object-name*, *rights-set*>
  - Trong đó *rights-set* là một tập con của tất cả các thao tác hợp lệ có thể được thực hiện trên đối tượng.
- Domain = tập các access-right



- Một Domain có thể chua: user, process, procedure

1.2. Ma trận truy nhập - Access Matrix

- Coi protection là một ma trận (*access matrix*)
- Các hàng biểu diễn các domain
- Các cột biểu diễn các đối tượng (objects)
- *Access(i, j)* là tập hợp các thao tác mà một tiến trình thực hiện trong Domaini có thể tác động trên Objectj

domain \ object	F_1	F_2	F_3	printer
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read write		read write	

1.3. Cách sử dụng Access Matrix

- Nếu một tiến trình trong Domain *Di* cố gắng thực hiện thao tác "op" trên đối tượng *Oj*, thì "op" phải có trong access matrix, trên giao điểm hàng *Di* và cột *Oj*
- Có thể được mở rộng thành bảo vệ động (dynamic protection).
  - Các thao tác để thêm, xóa các access right.
  - Các access right đặc biệt:
    - *chủ của Oi (owner of Oi)*
    - *copy thao tác từ Oi đến Oj*
    - *control – Di có thể thay đổi các access right của Dj*
    - *transfer – chuyển từ domain Di đến Dj*

1.4. Sự thực hiện của Access Matrix

- Mỗi cột = Danh sách quyền truy nhập (access-control list) đối với một object.
  Xác định domain nào có thể thực hiện thao tác gì.
  - Domain 1 = Read, Write
  - Domain 2 = Read
- Mỗi hàng = Danh sách khả năng (capability list)
  Đối với mỗi domain, những thao tác gì được phép trên những object nào.
  - Object 1 – Read
  - Object 5 – Read, Write, Delete, Copy

2. Security Problem

- Security phải quan tâm đến môi trường bên ngoài hệ thống (external environment), và bảo vệ hệ thống khỏi:
  - truy nhập trái phép - unauthorized access
  - cố tình/vô tình thay đổi hoặc phá hoại
- Bảo vệ để chống lại sự sử dụng sai (misuse) vô tình dễ hơn cố tình

2.1. Sự thẩm định quyền - Authentication

- Xác nhận người dùng (User identity)
  - Thường được thiết lập thông qua mật khẩu (*password)*
  - Có thể được coi là một trường hợp đặc biệt của chìa khóa hoặc khả năng.
  - Authorization

2.2. Tìm Password

- Nếu bạn biết user, hãy thử với tên hoặc ngày sinh của chồng/vợ người đó.
- *Brute force*: thử tất cả các sự kết hợp của chữ và số.
- *Dictionary attack*: thử tất cả các từ trong từ điển, cả từ đơn và từ ghép.
- *Shoulder surfing*: nhìn bàn phím khi user gõ mật khẩu.
- *Keystroke recorder*: Các máy tính Internet cafe ghi tất cả lần bấm phím.
- Ăn cắp password file khi sử dụng hệ thống.

2.3. Bảo vệ Password

- Thường xuyên thay đổi password
- Sử dụng password khó đoán: dài, không phải từ trong từ điển, các ký tự đầu tiên trong câu, hệ thống các dấu.
- Bắt đợi sau mỗi lần thử gõ password sai.
- Lưu password ở dạng mã hóa (Unix crypt()).
- Chỉ administrator có thể truy nhập file password và bằng một chương trình đặc biệt.
- Sử dụng password 1 lần: máy đưa ra một bài toán *c*, user tính rồi trả lời *f(c)*, máy cũng tính *f(c)* rồi so sánh. Chỉ user và computer biết hàm *f*.

2.4. Các hiểm họa chương trình-Program Threats(1)

- Trojan Horse – Chú ngựa thành Troa
  - Là đoạn mã mà dùng sai môi trường của nó.
  - Khai thác kỹ thuật cho phép chương trình viết bởi người này có thể được thực hiện bởi người khác.
- VD1
  - Bob soạn một plugin mới hấp dẫn cho một chương trình soạn thảo văn bản.
  - Sue, nhân viên của Bob, sử dụng plugin đó, và nó làm việc tốt...
  - ... ngoại trừ một điều là nó copy mọi file Sue soạn thảo vào một thư mục của Bob.
  - Khi Sue soạn một bức thư mật cho Tổng giám đốc về sự quản lý yếu kém của Bob, Bob đọc nó trước khi Sue gửi

2.4. Các hiểm họa chương trình-Program Threats(2)

- VD2
  - Bọb viết một chương trình hiển thị một hộp thoại full-screen trông giống hệt màn hình đăng nhập Windows.
  - Bob chạy chương trình rồi rời Internet cafe mà không log out.
  - Sue gõ username và password trong chương trình của Bob.
  - Bob cất thông tin đó, rồi chương trình của anh ta thực hiện việc log out, vì vậy Sue sẽ thấy màn hình đăng nhập thật của Windows.
  - Sue nghĩ rằng mình gõ đã sai mật khẩu, thử lại và vào được…
- Internet Trojan horse:
  - Bob mua một domain tên là www.citibanc.com, và lập một trang web giống trang chủ của Citibank.
  - Sue gõ nhầm URL, vào trang web của Bob.
  - Bob ăn cắp được password của Sue, rồi gửi (redirect) Sue tới đúng trang web của Citibank.

2.4. Các hiểm họa chương trình-Program Threats(3)

- *Trap door*
  - User-id hoặc password riêng làm hỏng thủ tục bảo mật thông thường.
  - Có thể được gắn trong một trình biên dịch (compiler).
- Ví dụ:
  - Bob được Ngân hàng Vietnam thuê viết 1 phần mềm quản lý tài khoản.
  - Bob viết CT, và nó làm việc hoàn hảo, ngoại trừ nó có 2 trap door:
  - 1. Mã của Bob làm tròn xuống, vd $1.995 trở thành $1.99. $0.005 được gửi vào tài khoản cá nhân của Bob.
  - 2. Mã của Bob bao gồm một đoạn mà tại đó anh ta kiểm tra một username và password cố định riêng thay vì kiểm tra trong password file. Bob đăng nhập vào sử dụng tài khoản đó để kích hoạt đoạn mã trên chỉ vào ngày Ngân hàng tính tiền lãi phải trả.
  - Hãy tưởng tượng rằng Bob viết 1 compiler mà thêm một trap door vào mọi chượng trình!

2.4. Các hiểm họa chương trình-Program Threats(4)

- Stack and Buffer Overflow
  - Là cách tấn công phổ biến nhất từ một kẻ ngoài hệ thống trên một mạng hoặc kết nối dial-up để đạt được sự truy nhập trái phép vào hệ thống đích
  - Kiểu tấn công này lợi dụng một lỗi trong một chương trình (tràn stack hoặc bộ nhớ đệm buffer.)

2.5. Các hiểm họa hệ thống - System Threats(1)

- Worms – là 1 chương trình sử dụng cơ chế đẻ trứng để tấn công liên tục hệ thống; tự động copy chính nó, dùng hết tài nguyên hệ thống và có thể khóa tất cả các tiến trình khác sử dụng hệ thống.
- Internet worm? Morris Internet worm – 1988?
- Denial of Service (DOS)
- Làm quá tải máy tính đích để ngăn nó làm việc có ích.
- SCO (1 công ty Mỹ) được tài trợ bởi Microsoft để sắp xếp việc kiện cáo chống lại các công ty sử dụng Linux.
- SCO làm một số fan của Linux tức giận, họ thực hiện cuộc tấn công DOS vào web site của công ty.
- Họ viết những đoạn script đơn giản giả là trình duyệt muốn kết nối tới web site của SCO...
- nhưng dừng kết nối ngay sau khi họ gửi yêu cầu, và...
- lập tức gửi 1 yêu cầu khác, rồi 1 nữa và cứ tiếp tục như vậy…
- web site của SCO đã không thể truy cập trong vài tháng.

2.5. System Threats(2): Viruses

- Giống như trap door, virus là 1 đoạn mã được nhúng trong 1 chương trình có ích. Nhưng 1 virus đơn lẻ có thể tự nó tấn công nhiều chương trình khác nhau.
- Đơn giản là nó tự chèn vào giữa đoạn chương trình bình thường.
- Khi được thực hiện, nó copy chính nó đến các chương trình khác, và/hoặc gây ra sự hư hại (lựa chọn thường phụ thuộc vào thời gian đã thực hiện, hoặc vào ngày nhất định, vd virus Michelangelo).
- Các chương trình và dữ liệu không độc lập là cửa ngõ tốt cho virus tấn công:
  - Các macro của Word là chương trình VB được thực hiện khi tài liệu được nạp.
  - Các file đính kèm email (vd virus *love bug*).
  - Web pages (vd mã javascript thay *hosts* file, chuyển www.yahoo.com tới một web site quảng cáo)

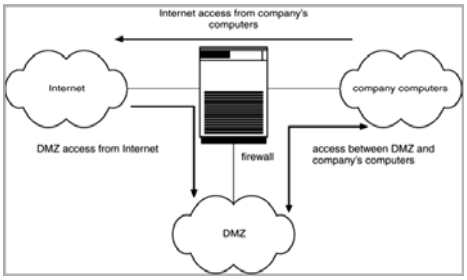
2.6. Giám sát hiểm họa (Threat Monitoring)

- Kiểm tra các hoạt động đáng nghi – vd một số lần thử password sai có thể báo hiệu đang thử password.
- Audit log (kiểm định truy nhập) – ghi thời gian, user, và kiểu của tất cả sự truy nhập một đối tượng; hữu dụng cho sự phục hồi từ một sự xâm phạm và cho việc phát triển những biện pháp bảo mật tốt hơn.
- Định kỳ quét (scan) hệ thống tìm các lỗi bảo mật rồi tự động sửa hoặc thông báo cho người quản trị hệ thống.
  - Password ngắn hoặc dễ đoán
  - Các chương trình có quyền trái phép
  - Các tiến trình chạy lâu không mong đợi
  - Trojan horse, …

2.7. FireWall

- Firewall tương tự như một màn ngăn lửa giữa động cơ ô tô với ghế ngồi của hành khách.
- LAN firewall: router kiểm tra kỹ và có thể loại bỏ các gói tin:
  - Một firewall được đặt giữa các host đáng tin T và không đáng tin U.
  - Nó cho phép các message đi từ T tới U không giới hạn.
  - Các message từ U tới T chỉ đi qua được nếu chúng là các hồi âm (reply) của các message trước đó được gửi từ T tới U.
- DMZ (Demilitarized Zone – Vùng phi quân sự):
  - Tất cả message từ U tới T mà không phải hồi âm thì đi đến các máy tính DMZ.
  - DMZ chứa web server, VPN server (truy nhập máy T an toàn với tư cách của các host U được phép),

2.8.1. Dùng Firewall thực hiện an ninh mạng qua các Domain



2.9. Mã hóa – Encryption(1)

- Mã hóa văn bản rõ ràng thành mật mã.
- Những đặc tính của kỹ thuật mã hóa tốt:
  - Tương đối đơn giản để người sử dụng có phép (authorized user) có thể mã hóa và giải mã.
  - Cách mã hóa không chỉ phụ thuộc vào sự bí mật của giải thuật mà còn vào một tham số của giải thuật được gọi là khóa mã hóa (encryption key).
  - Thực sự khó đối với kẻ xâm phạm có thể xác định được khóa mã hóa.
- *Data Encryption Standard* thay thế các ký tự và sắp xếp lại thứ tự của chúng trên nền tảng của khóa mã hóa được cung cấp bởi người sử dụng có phép thông qua một kỹ thuật mã hóa.

2.9. Mã hóa – Encryption(2): Ví dụ

- SSL – Secure Socket Layer
- Giao thức bằng mật mã giới hạn 2 máy tính chỉ trao đổi dữ liệu với nhau.
- Được sử dụng giữa các web server và các browser nhằm giao tiếp an toàn (credit card numbers)
- Server được xác nhận bởi một **certificate** (≈ giấy chứng nhận).
- Giao tiếp giữa mỗi máy tính sử dụng mật mã khóa đối xứng.

Q & A

- List câu hỏi