Mục tiêu của việc bảo vệ

Mục Tiêu Của Việc Bảo Vệ

- Một hệ thống máy tính bao gồm một tập các tài nguyên.
- Mỗi tài nguyên có một định danh và có thể được truy xuất thông qua một tập các thao tác được định nghĩa sẵn bởi hệ điều hành.
- Một trong những chức năng chính của hệ điều hành là quản lý việc truy xuất đến các nguồn tài nguyên hệ thống của người dùng (chương trình) sao cho việc sử dụng tài nguyên đạt hiệu năng cao nhất.

Nội Dung

Nguyên Tắc Bảo Vệ

- Nguyên tắc đặc quyền tối thiểu:
  - Các tiến trình, người dùng chỉ nên được cấp các quyền tối thiểu đủ để thực hiện tác vụ của họ.
  - Giới hạn việc ảnh hưởng nếu một thành phần bị lỗi
  - Đặc quyền dành cho một tiến trình, người dùng có thể là tĩnh (static, không thay đổi trong suốt vòng đời của tiến trình) hay động (dynamic, có thể thay đổi như leo thang đặc quyền,...)
- Nên xem xét việc sử dụng "hạt" (grain):
  - Hạt thô (Rough-grained): dễ quản lý, đơn giản nhưng không mềm dẻo.
  - Hạt mịn (fine-grained): phức tạp hơn, mất chi phí hơn nhưng tính bảo vệ cao hơn.

Miền bảo vệ

Mục Tiêu Của Việc Bảo Vệ

- Mục tiêu của việc bảo vệ:
  - **Chống lỗi của hệ thống**: đảm bảo việc truy xuất các tài nguyên là đúng đắn. Trong môi trường đa nhiệm, việc bảo vệ hệ thống ngăn chặn việc lan truyền các lỗi làm ảnh hưởng đến các tiến trình khác
    $\Rightarrow$ tăng cường độ tin cậy của hệ thống.
  - **Chống sự truy xuất bất hợp pháp**: đảm bảo tài nguyên của hệ thống chỉ được truy xuất bởi các tiến trình được phép truy xuất.

Cơ Chế và Chính Sách

- Vai trò của bộ phận bảo vệ là cung cấp một cơ chế (mechanism) để áp dụng các chính sách (policy) quản trị tài nguyên:
  - Cơ chế: xác định là thế nào để thực hiện bảo vệ, bao gồm cơ chế phần mềm và cơ chế phần cứng.
  - Chính sách: quyết định việc bảo vệ được áp dụng cho những đối tượng nào, các thao tác hợp lệ trên các đối tượng này.
- Cần tách rời cơ chế và chính sách để đảm bảo cho hệ thống có tính khả chuyển cao (cơ chế mang tính tĩnh, chính sách mang tính động, dễ thay đổi).

Liên Kết Giữa Miền Bảo Vệ và Tiến Trình

- **Liên kết tĩnh**: một tiến trình chỉ hoạt động trong 1 miền bảo vệ
  - tiến trình cần xin tất cả các quyền ngay từ đầu
  - vi phạm nguyên tắc need-to-know
    $\Rightarrow$ phải có cơ chế cập nhật miền bảo vệ
- **Liên kết động**: tiến trình có thể chuyển miền bảo vệ
  - có thể tạo miền bảo vệ mới với nội dung thay đổi qua từng giai đoạn của tiến trình
  - tuân theo nguyên lý need-to-know
- Miền bảo vệ có thể được tạo cho: người dùng, tiến trình, hay thủ tục (procedure, hay biến cục bộ bên trong các thủ tục).

Khái Niệm Miền Bảo Vệ (Protection Domain)

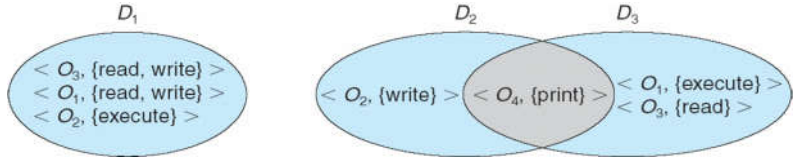
- Một hệ thống máy tính bao gồm một tập các tài nguyên: phần cứng (CPU, bộ nhớ, đĩa từ, ...), phần mềm (tập tin, chương trình, semaphore, ...).
- Mỗi tài nguyên có một định danh duy nhất, chỉ được truy xuất thông qua một tập các thao tác được định nghĩa chặt chẽ, rõ ràng.
- Các tiến trình chỉ được phép truy xuất đến các tài nguyên mà nó có quyền, trong thời điểm cho phép để nó có thể hoàn thành tác vụ (nguyên lý need-to-know) nhằm hạn chế lỗi.
- Miền bảo vệ: là một miền xác định, định nghĩa:
  - các tài nguyên mà các t/trình hoạt động trong miền đó có thể sử dụng
  - các thao tác hợp lệ trên các nguồn tài nguyên

Ma trận quyền truy xuất

Cấu Trúc Miền Bảo Vệ

- Miền bảo vệ = {quyền truy xuất (access right)}
- Quyền truy xuất là một bộ: <đối tượng, {quyền thao tác (rights)}>

  Trong đó, quyền thao tác là các thao tác (operations) được phép thực hiện trên đối tượng.



- Các miền bảo vệ có thể giao nhau (D_2, D_3)

Sử Dụng Ma Trận Quyền Truy Xuất

- Nếu một tiến trình trong domain D_i muốn thực hiện thao tác t trên đối tượng O_j, t phải hiện diện trong ma trận truy xuất tại vị trí (i, j)
- Người chủ sở hữu của một đối tượng có thể chỉ định các thao tác truy xuất trong cột tương ứng.
- Một số mở rộng để cài đặt việc bảo vệ động:
  - các thao tác thêm, xóa các quyền
  - một số quyền truy xuất đặc biệt:
    - chủ sở hữu (owner): của một đối tượng
    - sao chép (copy): các thao tác từ O_i sang O_j
    - điều khiển (control): D_i có thể thay đổi quyền truy xuất của D_j
    - chuyển đổi (transfer/switch): chuyển từ miền này sang miền khác

Ma Trận Quyền Truy Xuất

- Mô hình miền bảo vệ có thể được biểu diễn như một ma trận quyền truy xuất (access matrix):
  - **hàng** (row): thể hiện cho các miền (domain)
  - **cột** (column): thể hiện cho các đối tượng (tài nguyên)
  - *access*(i, j) là một tập các thao tác (operations) mà một tiến trình trong miền i có thể thực hiện trên đối tượng j

Sử Dụng Ma Trận Quyền Truy Xuất – VD

Ma trận quyền truy xuất với domain:

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

Ma Trận Quyền Truy Xuất – Ví Dụ

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	

Cài đặt Ma trận quyền truy xuất

Cài Đặt Ma Trận Quyền Truy Xuất

- Một số phương pháp cài đặt ma trận quyền tury xuất:
  - Bảng toàn cục (global table)
  - Danh sách quyền truy xuất (Access Control List – ACL)
  - Danh sách tiềm năng miền bảo vệ (Capability Lists for Domains)
  - Cơ chế khóa và chìa (Lock-Key Mechanism)

Sử Dụng Ma Trận Quyền Truy Xuất – VD

Ma trận quyền truy xuất với quyền chủ sở hữu:

domain \ object	F_1	F_2	F_3
D_1	owner execute		write
D_2		read* owner	read* owner write
D_3	execute		

(a)

domain \ object	F_1	F_2	F_3
D_1	owner execute		write
D_2		owner read* write*	read* owner write
D_3		write	write

(b)

Sử Dụng Ma Trận Quyền Truy Xuất – VD

Thay đổi ma trận quyền truy xuất:

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

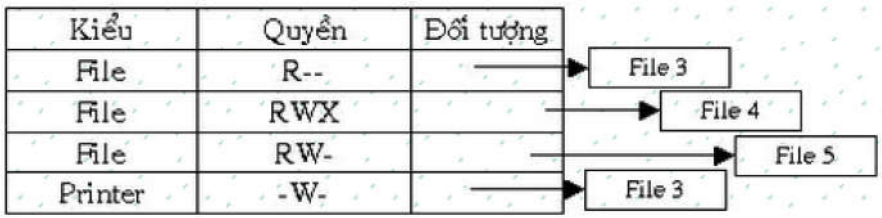
Danh Sách Tiềm Năng Của Miền Bảo Vệ

- Mỗi dòng (row) trong ma trận quyền truy xuất được tổ chức thành 1 danh sách tiềm năng (capability list)
- Một danh sách tiềm năng (C_List) là một danh sách các đối tượng và các thao tác mà tiến trình được quyền thực hiện trên đối tượng khi hoạt động trong miền bảo vệ
- Mỗi phần tử của C_List được gọi là một tiềm năng (capability) hay quyền truy xuất đến đối tượng.
- Một tiến trình chỉ có thể thực hiện thao tác M trên đối tượng O_j trong miền D_i nếu trong C_List của D_i có chứa tiềm năng tương ứng của O_j.

Bảng Toàn Cục (Global Table)

- Lưu trữ các bộ ba $< D_i, O_j, R_k >$ (domain, object, rights) trong một table
- Một yêu cầu thực hiện thao tác M trên đối tượng O_j trong domain D_i chỉ được cho phép nếu tồn tại một bộ ba $< D_i, O_j, R_k >$ sao cho $M \in R_k$
- Ưu điểm: đơn giản, dễ cài đặt
- Hạn chế:
  - Bảng toàn cục có thể rất lớn
    $\Rightarrow$ có thể không chứa đủ trong bộ nhớ chính
  - Không thể gom nhóm (group) các đối tượng có cùng đặc điểm

Danh Sách Tiềm Năng Của Miền Bảo Vệ



Danh Sách Quyền Truy Xuất (ACL)

- Cài đặt mỗi cột trong ma trận quyền truy xuất như là một danh sách các quyền truy xuất đối với 1 đối tượng.
- Mỗi đối tượng trong hệ thống sẽ có một danh sách bao gồm các bộ <miền bản vệ D_i, {các quyền truy xuất R_k}>
- Khi một yêu cầu thực hiện thao tác M trên đối tượng O_j trong miền D_i chỉ được cho phép nếu trong ACL của O_j tồn tại một bộ $<D_i, R_k>$ sao cho $M \in R_k$
- Ví dụ: cho A, B, C là các người dùng và root, users là các nhóm, ta có:
  - file1: (A, *, rwx)
  - file2: (B, users, rx), (C, root, rwx)

An Toàn Hệ Thống (Security)

- Bảo vệ hệ thống (protection): kiểm soát việc sử dụng tài nguyên, có tính chất nội bộ
- An toàn hệ thống: mức độ tin cậy của một hệ thống đối với các vấn đề phát sinh từ nội bộ lẫn bên ngoài
- Một hệ thống là an toàn nếu các tài nguyên được sử dụng đúng qui ước trong mọi trường hợp $\Rightarrow$ khó đạt được:
  - Phá hoại từ các hackers
  - Cạnh tranh giữa các luồng (thread)
  - Các cuộc tấn công từ bên ngoài, cả vô ý lẫn cố ý.
  - ...

Cơ Chế Khóa và Chìa

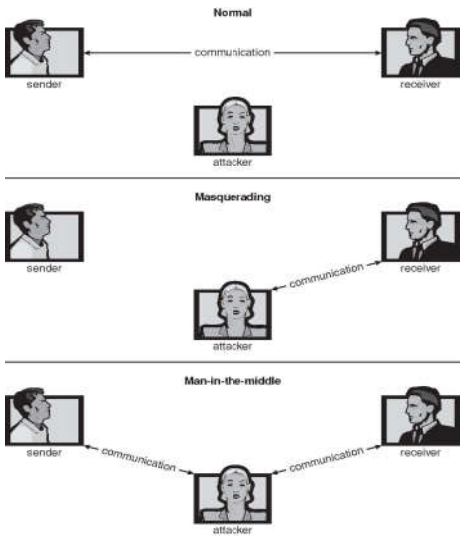
- Là sự kết hợp giữa danh sách quyền truy xuất và danh sách tiềm năng:
  - Mỗi đối tượng sở hữu một danh sách các mã nhị phân, được gọi là khóa (lock).
  - Mỗi miền bảo vệ sẽ sở hữu một danh sách mã nhị phân gọi là chìa (key)
- Mỗi tiến trình hoạt động trong miền bảo vệ chỉ có thể truy xuất đến một đối tượng nếu miền bảo vệ sở hữu một chìa tương ứng với một khóa trong danh sách khóa của đối tượng.

Đảm Bảo An Toàn Hệ Thống

- Nếu như bảo vệ hệ thống có thể đạt độ tin cậy tuyệt đối thì các cơ chế an toàn chỉ nhằm hạn chế thấp nhất các vấn đề về an ninh.
- Việc bảo vệ hệ thống phải được thực hiện ở nhiều mức:
  - Mức vật lý: trang thiết bị an toàn cho hệ thống (data center, servers)
  - Con người: chọn lọc nhân sự cẩn thận
  - Hệ điều hành: cơ chế bảo vệ, gỡ rối, ...

An toàn hệ thống (Security)

Các Phương Pháp Tấn Công Hệ Thống



Các Loại Vi Phạm An Toàn Hệ Thống

- Vi phạm về bảo mật (Breach of confidentiality):
  - đọc dữ liệu trái phép
- Vi phạm tính toàn vẹn (Breach of integrity):
  - sửa đổi trái phép dữ liệu
- Đánh cắp dịch vụ (Theft of service):
  - sử dụng trái phép tài nguyên.
- Tấn công từ chối dịch vụ (Denial of service):
  - cản trở việc sử dụng hay truy cập hợp pháp.

Kiểm Định Danh Tính (Authentication)

- Là một trong những cơ chế cơ bản nhất trong việc bảo đảm an toàn cho hệ thống
- Hoạt động của hệ thống bảo vệ phụ thuộc vào khả năng xác định các tiến trình đang thực thi.
- Khả năng này lại phụ thuộc vào việc xác định người dùng đang sử dụng hệ thống để kiểm tra tính hợp lệ của các thao tác.
- Cách tiếp cận phổ biến nhất là sử dụng mật khẩu (password) để kiểm định danh tính người dùng.
- Mật khẩu có thể được sử dụng để bảo vệ từng đối tượng trong hệ thống. Trong một số trường hợp đặc biệt, một đối tượng có nhiều mật khẩu khác nhau tương ứng với những quyền truy xuất khác nhau.

Các Phương Pháp Tấn Công Hệ Thống

- Giả mạo (vi phạm chứng thực): giả vờ là một người dùng được ủy quyền để leo thang đặc quyền
- Tấn công man-in-the-middle: kẻ phá hoại can thiệp vào luồng dữ liệu của người gửi và người nhận để giả mạo hay đánh cắp thông tin.
- Cướp quyền: đánh chặn một phiên đã thành lập để vượt qua xác thực.
- ...

Tổng Kết

Mục tiêu của việc bảo vệ

Miền bảo vệ

Ma trận quyền truy xuất

Cài đặt Ma trận quyền truy xuất

An toàn hệ thống

Mối Đe Dọa Từ Các Chương Trình

- Ngựa thành Troy:
  - Là một chương trình thu thập dữ liệu của *nạn nhân* để gửi cho *chủ nhân* của nó.
  - Khi người dùng A thực thi một chương trình X do một người B viết trong miền bảo vệ của mình (A), X có thể thao tác trên tài nguyên dưới danh nghĩa của A để truy xuất các tài nguyên của A.
  - Nếu X là một đoạn mã có mục đích xấu thì nó có thể thu thập dữ liệu của A để gửi cho B.

Mối Đe Dọa Từ Các Chương Trình

- Cửa hậu (backdoor):
  - Là một lổ hổng vô ý hay cố ý trong phần mềm do người lập trình tạo ra.
  - Đây là một mối đe dọa đặc biệt nguy hiểm và khó phòng tránh.
  - Cửa hậu cho phép chủ nhân của nó sử dụng để thâm nhập trái phép hệ thống, qua đó thực hiện phá hoại hệ thống.