Chapter 5. Protection and Security

Protection

Security

Bảo vệ hệ thống

- Mục tiêu của việc bảo vệ hệ thống là:
  - Bảo vệ chống lỗi của chương trình
  - Chống sự truy xuất bất hợp lệ
- Vai trò của bộ phận bảo vệ trong hệ thống là cung cấp một cơ chế để áp dụng các chiến lược quản trị việc sử dụng tài nguyên:
  - Cơ chế: Xác định làm thế nào để thực hiện việc bảo vệ, có thể có các cơ chế phần mềm hoặc cơ chế phần cứng.
  - Chiến lược: Quyết định việc bảo vệ được áp dụng như thế nào ? Những đối tượng nào trong hệ thống cần được bảo vệ và các thao tác thích hợp trên các đối tượng này.

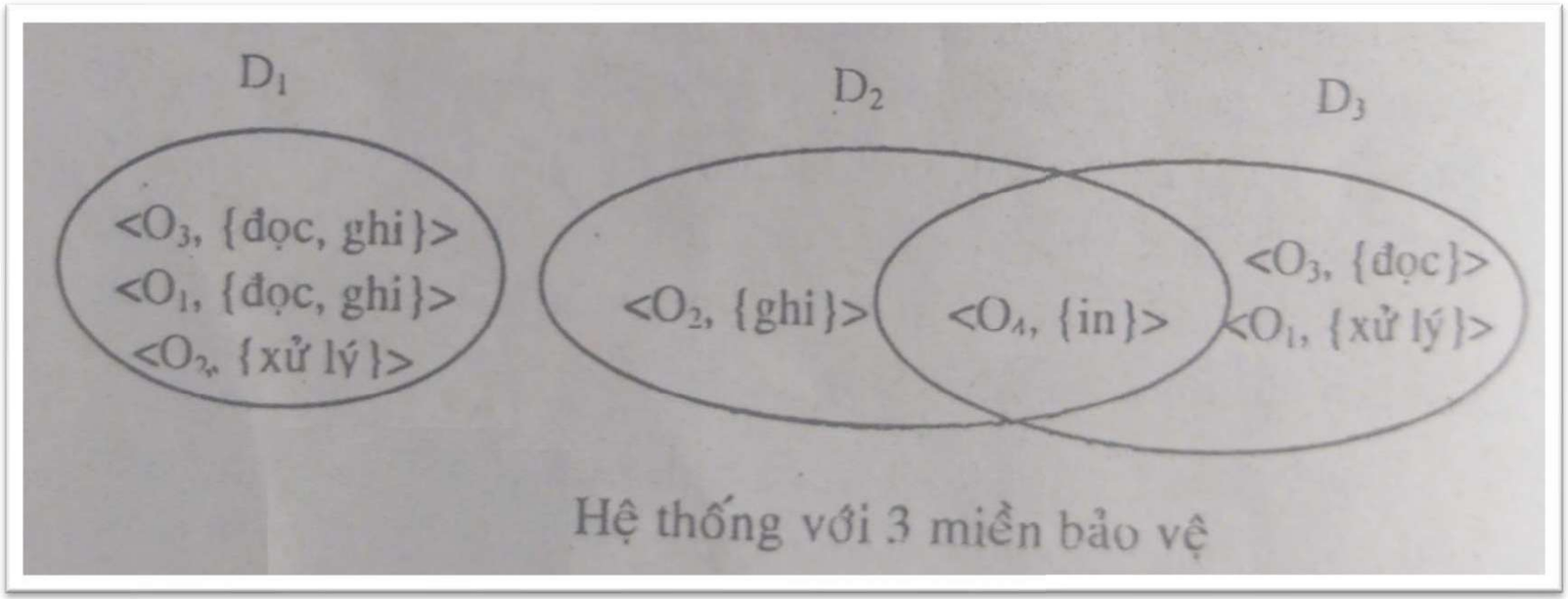
Miền bảo vệ

- Khái niệm
  - Một hệ thống máy tính được xem như một tập các đối tượng. Một đối tượng có thể là một bộ phận phần cứng hay một thực thế phần mềm.
  - Mỗi đối tượng có một định danh duy nhất để phân biệt với các đối tượng khác trong hệ thống, và chỉ được truy xuất đến thông qua các thao tác được định nghĩa chặt chẽ và được quy định ngữ nghĩa rõ ràng. Các thao tác có thể thực hiện được trên một đối tượng được xác định cụ thể tùy vào đối tượng.

- Để có thể kiểm soát được tình hình sử dụng tài nguyên trong hệ thống, hệ điều hành chỉ cho phép các tiến trình được truy xuất đến các tài nguyên mà nó có quyền sử dụng, hơn nữa tiến trình chỉ được truy xuất đến các tài nguyên cần thiết trong thời điểm hiện tại để nó hoàn thành tác vụ (nguyên lý need to know) nhằm hạn chế các lỗi truy xuất mà tiến trình có thể gây ra trong hệ thống.
- Mỗi tiến trình trong hệ thống đều hoạt động trong một miền bảo vệ (protection domain) nào đó. Một miền bảo vệ sẽ xác định các tài nguyên (đối tượng) mà những tiến trình hoạt động trong miền bảo vệ này có thể sử dụng, và các thao tác hợp lệ các tiến trình này có thể thực hiện trên những tài nguyên đó.

Cấu trúc của miền bảo vệ

- Các khả năng thao tác trên một đối tượng được gọi là quyền truy xuất (access right). Một miền bảo vệ là một tập hợp các quyền truy xuất, mỗi quyền truy xuất được định nghĩa bởi một bộ hai thứ tự <đối tượng, {quyền thao tác}>. Các miền bảo vệ khác nhau có thể giao nhau một số quyền truy xuất:



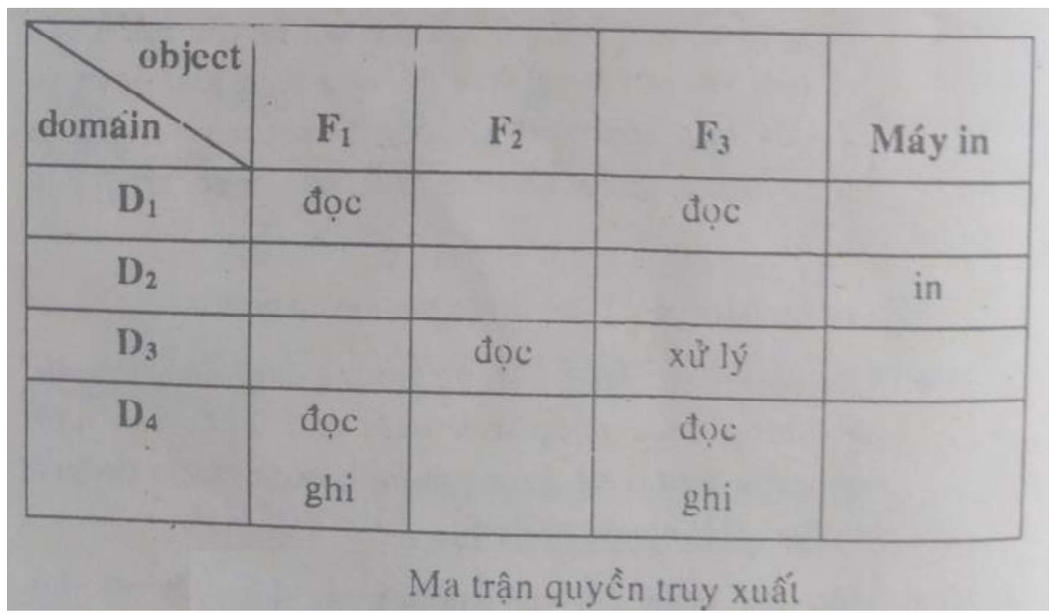
Hệ thống với 3 miền bảo vệ

- Mối liên kết giữa một tiến trình và một miền bảo vệ có thể tĩnh hay động.
- Một miền bảo vệ có thể được xây dựng cho:
  - Một người sử dụng
  - Một tiến trình
  - Một thủ tục

Ma trận quyền truy xuất

Ma trận quyền truy xuất được định nghĩa như sau:

- Các dòng của ma trận biểu diễn các miền bảo vệ và các cột tương ứng với các đối tượng của hệ thống.
- Phần tử access[i,j] của ma trận xác định các quyền truy xuất mà một tiến trình hoạt động trong miền bảo vệ D_i có thể thao tác trên đối tượng O_j.



object / domain	F_1	F_2	F_3	Máy in
D_1	đọc		đọc	
D_2				in
D_3		đọc	xử lý	
D_4	đọc ghi		đọc ghi	

Ma trận quyền truy xuất

- Cơ chế bảo vệ được cung cấp khi ma trận quyền truy xuất được cài đặt, lúc này người sử dụng có thể áp dụng các chiến lược bảo vệ bằng cách đặc tả nội dung các phần tử tương ứng trong ma trận – xác định các quyền truy xuất ứng với từng miền bảo vệ, và cuối cùng, hệ điều hành sẽ quyết định cho phép tiến trình hoạt động trong miền bảo vệ thích hợp.
- Ma trận quyền truy xuấ cũng cung cấp một cơ chế thích hợp để định nghĩa và thực hiện một sự kiểm soát nghiêm ngặt cho cả phương thức liên kết tĩnh và động các tiến trình với các miền bảo vệ. Cụ thể:
  - Có thể kiểm soát việc chuyển đổi giữa các miền bảo vệ nếu quan niệm miền bảo vệ cũng là một đối tượng trong hệ thống, và bổ sung các cột mô tả cho nó trong ma trận quyền truy xuất.

- Khi đó tiến trình được phép chuyển từ miền bảo vệ D_i sang miền bảo vệ D_j nếu phần tử access(i,j) chứa đựng quyền "chuyển" (switch).

object / domain	F_1	F_2	F_3	Máy in	D_1	D_2	D_3	D_4
D_1	đọc		đọc			chuyển		
D_2				in			chuyển	chuyển
D_3		đọc	xử lý					
D_4	đọc ghi		đọc ghi		ch ryển			

Ma trận quyền truy xuất với domain là một đối tượng

- Có thể kiểm soát việc sửa nội dung ma trận (thay đổi các quyền truy xuất trong một miền bảo vệ) nếu quan niệm bản thân ma trận cũng là một đối tượng. Các thao tác sửa đổi nội dung ma trận được phép thực hiện bao gồm: sao chép quyền (copy), chuyển quyền (transfer), quyền sở hữu (owner), quyền kiểm soát (control)
- Vấn đề cài đặt ma trận quyền truy xuất (SV xem trong tài liệu tham khảo)

An toàn hệ thống

- Các vấn đề an toàn hệ thống
- Kiểm định danh tính
- Mối đe dọa từ các chương trình
- Mối đe dọa từ hệ thống
- Giám sát các mối đe dọa

Các vấn đề an toàn hệ thống

- Bảo vệ hệ thống (protection) là một cơ chế kiểm soát việc sử dụng tài nguyên của các tiến trình hay người sử dụng để đối phó với các tình huống lỗi có thể phát sinh từ trong hệ thống.
- Khái niệm an toàn hệ thống (security) muốn đề cập đến mức độ tin cậy mà hệ thống duy trì khi phải đối phó không những với vấn đề nội bộ, mà còn cả với những tác hại đến từ môi trường ngoài.
- Hệ thống được gọi là an toàn nếu các tài nguyên được sử dụng đúng như quy ước trong mọi hoàn cảnh.
- Bảo vệ hệ thống có thể đạt độ tin cậy tuyệt đối; trong khi cơ chế an toàn hệ thống được cung cấp chỉ với hy vọng ngăn chặn bớt các tình huống bất an hơn là đạt đến độ an toàn tuyệt đối.

Kiểm định danh tính

- Để đảm bảo an toàn, hệ điều hành cần giải quyết tốt vấn đề chủ yếu là kiểm định danh tính (authentication). Hoạt động của hệ thống bảo vệ phụ thuộc vào khả năng xác định các tiến trình đang xử lý; khả năng này, đến lượt nó, lại phụ thuộc vào việc xác định được người dùng đang sử dụng hệ thống để có thể kiểm tra người dùng này được cho phép thao tác trên những tài nguyên nào.
- Cách tiếp cận phổ biến nhất để giải quyết vấn đề là sử dụng password để kiểm định đúng danh tính của người dùng. Mỗi khi người dùng muốn sử dụng tài nguyên, hệ thống sẽ kiểm tra password của người dùng đăng nhập vào với password được lưu trữ, nếu đúng, người dùng mới được cho phép sử dụng tài nguyên.

- Password có thể được bảo vệ từng đối tượng trong hệ thống, thậm chí cùng một đối tượng sẽ có các password khác nhau ứng với những quyền truy xuất khác nhau.
- Cơ chế password dễ sử dụng, tuy nhiên yếu điểm nghiêm trọng của phương pháp này là khả năng bảo mật password rất khó đạt được sự hoàn hảo, những tác nhân tiêu cực có thể đoán ra password của người khác nhờ nhiều cách thức khác nhau.

Mối đe dọa từ các chương trình

Trong môi trường mà một chương trình được tạo lập bởi người này lại có thể được người khác sử dụng, có thể xảy ra các tình huống sử dụng không đúng, từ đó dẫn đến những hậu quả khó lường. Hai trường hợp điển hình là:

- Ngựa thành Troy: Khi một người dùng A sử dụng chương trình do B viết hoạt động dưới danh nghĩa của người dùng A (trong miền bảo vệ được gán tương ứng cho người dùng A). Chương trình này có thể trở thành một "con ngựa thành Troy" vì khi đó các đoạn lệnh trong chương trình có thể thao tác trên các tài nguyên với những quyền tương ứng của người dùng A (mà có thể người dùng B bị cấm); nhiều chương trình như thế đã lợi dụng để gây ra các tác hại đáng tiếc.

- Cánh cửa nhỏ (Trap - door): Một mối đe dọa đặc biệt nguy hiểm và khó chống đỡ đến từ sự vô tình hay ý nghĩa bất chính của các lập trình viên. Khi xây dựng chương trình, các lập trình có thể để lại một "cánh cửa nhỏ" trong phần mềm mà chỉ có họ là có khả năng sử dụng, qua đó thâm nhập và phá hoại hệ thống (ví dụ làm tròn số lẻ trong những tài khoản và thu lợi riêng từ phần dư này,...). Vấn đề này rất khó đối phó vì cần phải tiến hành phân tích chương trình nguồn để tìm ra chỗ sơ hở.

Mối đe dọa từ hệ thống

- Hầu hết các hệ điều hành đều cung cấp phương tiện cho phép các tiến trình khi hoạt động có thể tạo ra những tiến trình khác. Trong các môi trường như thế, tài nguyên hệ thống và các tập tin của người dùng có thể bị sử dụng sai lệch để gây tác hại.
- Hai phương pháp phổ biến để phá hoại hệ thống theo phương thức này là:
  - Các chương trình sâu bọ (worm)
  - Các chương trình virus

Các chương trình sâu bọ (worm)

- Một chương trình "sâu bọ" là chương trình lợi dụng cơ chế phát sinh tiến trình của hệ thống để đánh bại chính hệ thống. Tiến trình sâu bọ có khả năng phát sinh các phiên bản ngay cả trên môi trường mạng; sau đó chiếm dụng các tài nguyên hệ thống và làm ngưng trệ hoàn toàn hoạt động của các tiến trình khác trên hệ thống mạng.

Các chương trình virus

- Virus máy tính là một dạng phá hoại nguy hiểm khác đối với các hệ thống thông tin. Khác với sâu bọ là những chương trình hoàn chỉnh, virus chỉ là những đoạn code có khả năng lây truyền vào các chương trình chính thống khác và từ đó tàn phá hệ thống.

Giám sát các mối đe dọa

- Việc bảo đảm an toàn hệ thống là rất khó do có các yếu tố con người. Hệ điều hành chỉ có thể áp dụng một số kỹ thuật để giảm bớt khả năng bị phá hoại như việc ghi nhận các sự kiện sau:
  - Cố gắng nhập nhiều lần password sai
  - Sử dụng các password dễ đoán
  - Các tiến trình với định danh nghi ngờ không được ủy quyền
  - Các tiến trình không được ủy quyền trong những thư mục hệ thống
  - Các chương trình kéo dài thời gian xử lý một cách đáng ngờ
  - Bảo vệ tập tin và thư mục không hợp lý
  - Thay đổi kích thước của các chương trình hệ thống
- Việc kiểm tra thường kỳ và ghi nhận các thông tin này giúp hệ thống phát hiện kịp thời các nguy cơ, và cho phép phân tích, dự đoán các cách đối phó về sau.

Hết