HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC

An toàn hệ điều hành

Các vấn đề kiến trúc an toàn

Giảng viên: TS. Phạm Hoàng Duy

Điện thoại/E-mail: phamhduy@gmail.com

Bộ môn: An toàn thông tin - Khoa CNTT1

Nội dung

- Cơ chế bảo vệ
- Nhân an toàn và giám sát tham chiếu

Giới thiệu

- Hệ điều hành cung cấp cơ chế thực thi truy nhập tới các tài nguyên chung của hệ thống
- Cơ chế thực thi truy nhập cho phép các yêu cầu (lời gọi hệ thống) từ các chủ thể khác nhau (subject) như người dùng, tiến trình để thực hiện các thao tác (đọc ghi,...) lên các đối tượng (tài nguyên của hệ thống)
- Đây là các khái niệm căn bản của hệ thống bảo vệ nhằm đảm bảo an toàn cho hệ điều hành

Hệ thống bảo vệ

- Hệ thống bảo vệ gồm có
  - Trạng thái bảo vệ mô tả các thao tác mà các chủ thể của hệ thống có thể thực hiện lên các đối tượng hệ thống
  - Tập các thao tác trạng thái bảo vệ làm thay đổi các trạng thái này
- Hệ thống bảo vệ xác định các yêu cầu an ninh của hệ điều hành và thực hiện việc quản lý các yêu cầu này.
  - Ma trận truy nhập
  - Hệ thống bảo vệ bắt buộc

Ma trận truy nhập

- Các trạng thái bảo vệ của hệ thống được biểu diễn bằng ma trận truy nhập được định nghĩa bằng
  - Tập các chủ thể
  - Tập các đối tượng
  - Các thao tác được phép của chủ thể lên đối tượng
- Ma trận cũng mô tả các thao tác mà chủ thể có thể thực hiện lên trên ô của ma trận như *sở hữu*

	File 1	File 2	File 3	Process 1	Process 2
Process 1	Read	Read, Write	Read, Write	Read	-
Process 2	-	Read	Read, Write	-	Read

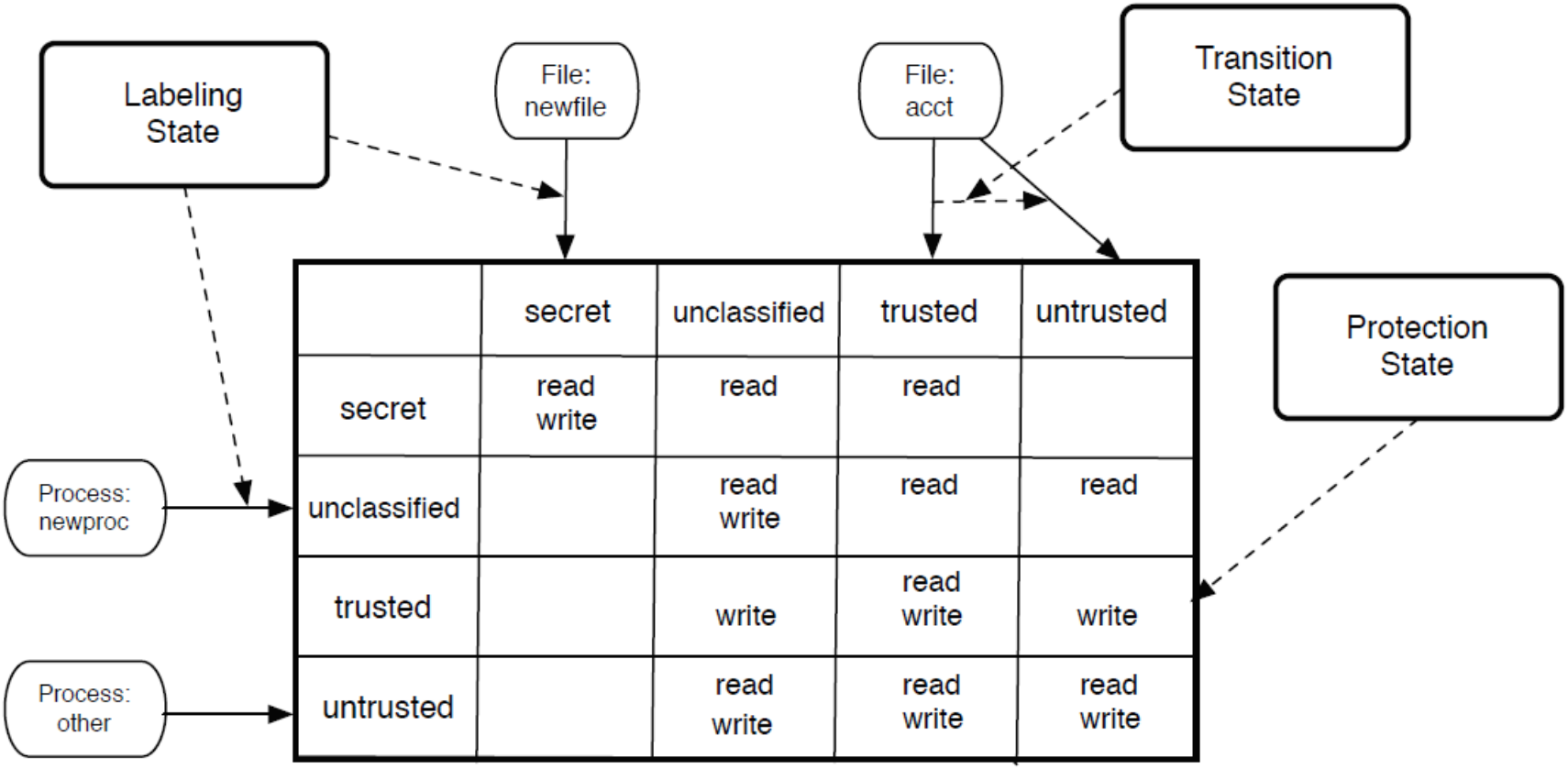
Ma trận truy nhập

- Ma trận truy nhập cũng được sử dụng để mô tả miền bảo vệ (*protection domain*)
- *Miền bảo vệ* là tập các đối tượng (tài nguyên) mà tiến trình có thể truy nhập và các thao tác mà tiến trình có thể dùng để truy nhập tới các đối tượng như vậy.
  - Hàng trong ma trận truy nhập cho biết thông tin về miền hoạt động của tiến trình
  - Với hệ điều hành an toàn, cần đảm bảo miền an toàn của mỗi tiến trình thỏa mãn các mục tiêu an toàn như tính bí mật hay toàn vẹn

Hệ thống bảo vệ bắt buộc

- Hệ thống bảo vệ bắt buộc là hệ thống mà chỉ có thể được sửa đổi bởi người quản trị tin cậy thông qua phần mềm tin cậy gồm các biểu diễn trạng thái như sau:
  - *Trạng thái bảo vệ bắt buộc* là trạng thái mà các chủ thể và các đối tượng được biểu diễn bằng các *nhãn.* Các trạng thái mô tả các thao tác mà các nhãn chủ thể có thể thực hiện lên các nhãn đối tượng.
  - *Trạng thái dán nhãn* để ánh xạ các tiến trình và các đối tượng tài nguyên hệ thống tới các nhãn
  - *Trạng thái dịch chuyển* mô tả cách thức hợp lệ mà các tiến trình và các đối tượng có thể được dán nhãn lại

An toàn hệ điều hành



	secret	unclassified	trusted	untrusted
secret	read write	read	read	
unclassified		read write	read	read
trusted		write	read write	write
untrusted		read write	read write	read write

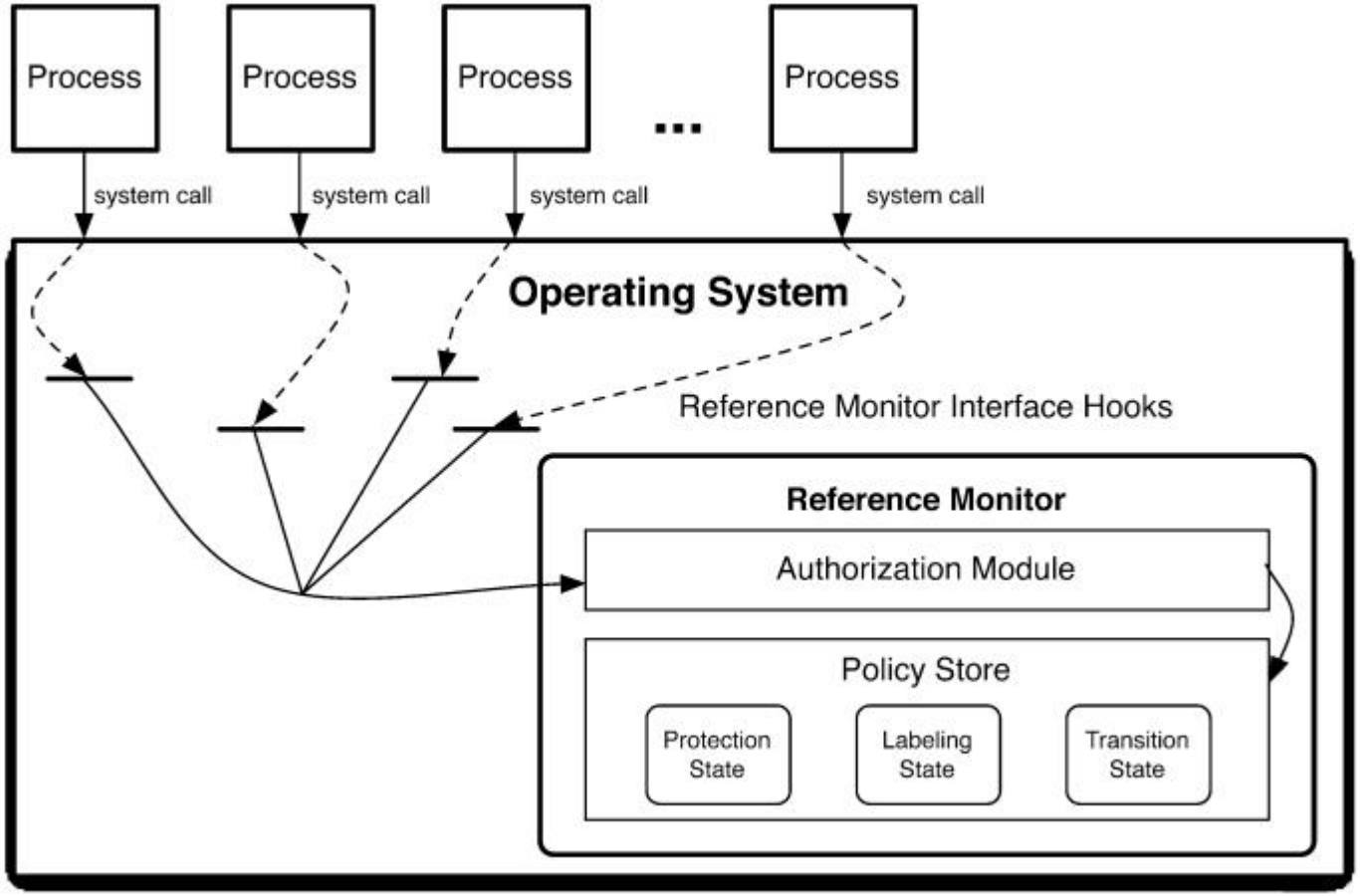
Hệ thống bảo vệ bắt buộc

- Trong hệ điều hành an toàn, nhãn chính là các định danh khái quát. Các nhãn này chống lại việc xâm nhập (temper-proof) nhờ
  - Tập các nhãn này được xây dựng bởi người quản trị tin cậy bằng phần mềm tin cậy
  - Tập các nhãn không thay đổi được (bởi các tiến trình không tin cậy của người dùng)

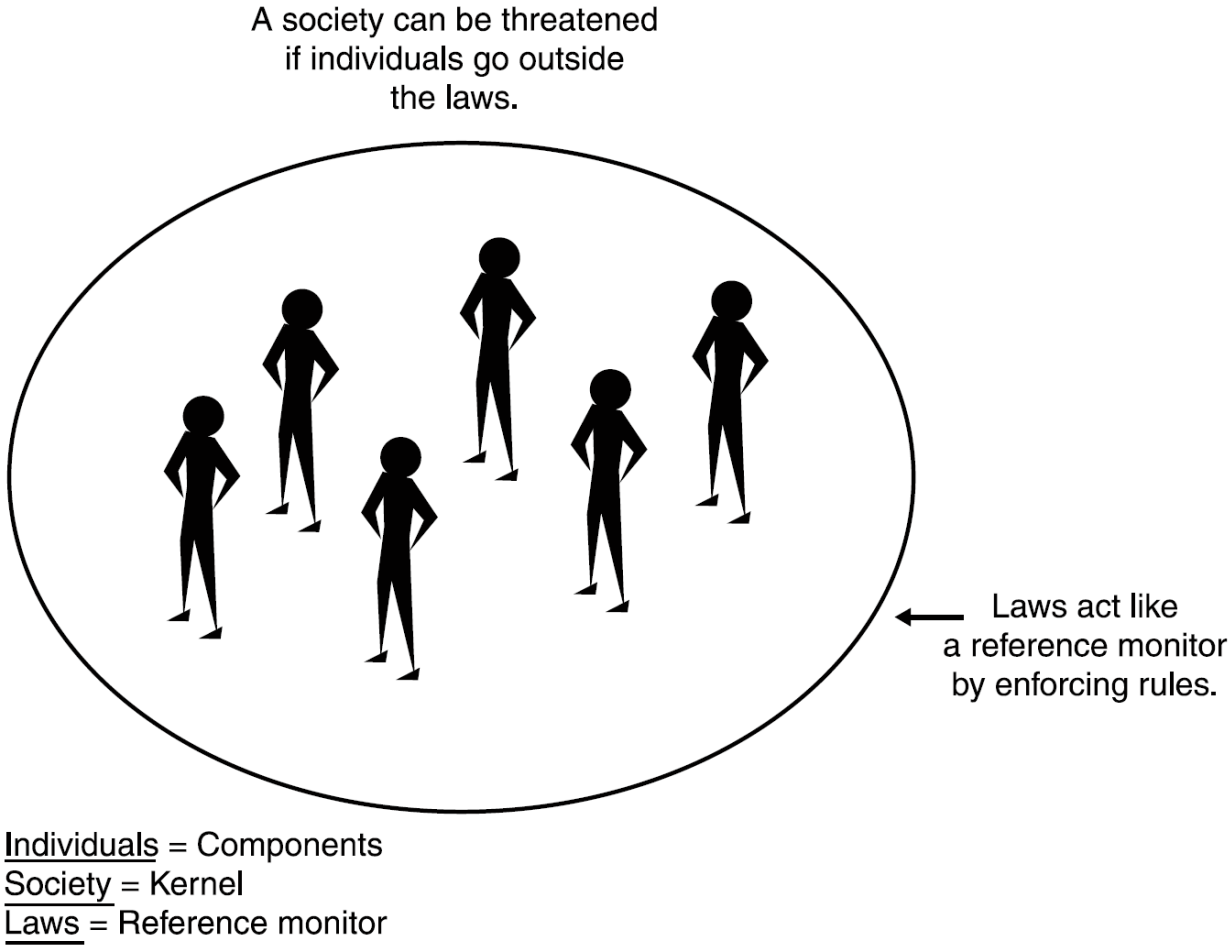
Nhân an toàn và giám sát tham chiếu

- Giám sát tham chiếu (Reference Monitor) là cơ chế thực thi truy nhập cổ điển. Khi có yêu cầu truy nhập, bộ phận giám sát trả lời chấp nhận hay từ chối truy nhập. Giám sát tham chiếu bao gồm 3 phần
  - Giao tiếp
  - Mô-đun xác thực
  - Kho chính sách

Giám sát tham chiếu



Giám sát tham chiếu



Giao tiếp giám sát tham chiếu

- Giao tiếp xác định vị trí các truy vấn/yêu cầu hệ thống bảo vệ được thực hiện tới bộ giám sát
  - Về cơ bản tất cả các thao tác nhạy cảm về an ninh được xác thực bởi cơ chế thực thi truy nhập
  - Các thao tác nhạy cảm là các thao tác thực hiện trên một đối tượng cụ thể (file, socket...) mà các thao tác này có thể xâm phạm các yêu cầu an ninh của hệ thống.

Mô-đun xác thực

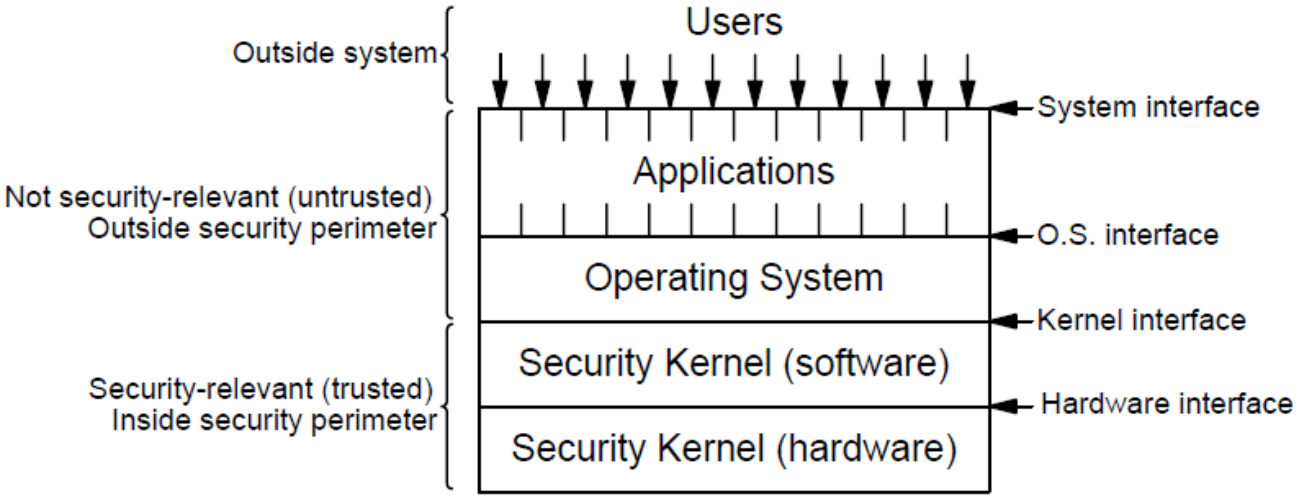
- Là bộ phận cốt lõi của bộ phận giám sát tham chiếu
- Nhận các tham số đầu vào từ giao tiếp như định danh tiến trình, tham chiếu đối tượng, tên lời gọi hệ thống ... và thực hiện truy vấn kho chính sách để trả lời về tính hợp lệ của truy vấn từ giao tiếp.

Kho chính sách

- Chính là cơ sở dữ liệu về trạng thái bảo vệ, các nhãn trạng thái và trạng thái dịch chuyển
  - Các câu truy vấn có cấu trúc {nhãn chủ thể, nhãn đối tượng, tập thao tác} và trả về kết quả nhị phân (hợp lệ/không hợp lệ)
  - Các truy vấn về việc dịch chuyển có dạng {nhãn chủ thể, nhãn đối tượng, tập thao tác, tài nguyên}

Nhân an toàn

- Nhân an toàn là cách tiếp cận dựa trên giám sát tham chiếu có kết hợp phần cứng và phần mềm để đảm bảo thực thi các chính sách an toàn của hệ thống
  - Giám sát tham chiếu đảm bảo việc giám sát mỗi truy nhập từ các chủ thể khác nhau của hệ thống tới từng tài nguyên/đối tượng



Nhân an toàn

- Cơ cở chính của nhân dựa trên việc chỉ có phần nhỏ của hệ thống phần mềm chịu trách nhiệm về an toàn ngay cả trong hệ thống lớn.
- Các chức năng an toàn được bố trí trong phần lõi (nhân) tin cậy. Kích cỡ nhỏ của nhân giúp cho việc kiểm chứng tính đúng đắn của nó được thuận tiện và dễ dàng.
- Phần lõi này phải được bảo vệ chống giả mạo và việc kiểm soát truy nhập của phần lõi này không thể bị bỏ qua