An toàn Hệ điều hành

Trần Đức Khánh
Bộ môn HTTT – Viện CNTT&TT
ĐH BKHN

Hệ điều hành

- Vai trò
  - Giao diện giữa phần cứng và phần mềm
  - Quản lý tài nguyên
  - Cung cấp các phương tiện bảo vệ phần cứng và ứng dụng

An toàn Hệ điều hành

- Các vấn đề bảo vệ trong Hệ điều hành
  - Bảo vệ bộ nhớ và địa chỉ
  - Bảo vệ tệp
  - Xác thực người dùng
- Kiểm soát truy nhập
  - Các mô hình KSTN
  - KSTN trong Unix, Windows NT/2000
- Nguyên tắc thiết kế Hệ điều hành
  - Giám sát thẩm quyền (Reference Monitor)
  - Phân hoạch (Separation)/Cách ly (Isolation)
  - Thiết kế phân tầng (Layered Design)

An toàn Hệ điều hành

- Các vấn đề bảo vệ trong Hệ điều hành
  - Bảo vệ bộ nhớ và địa chỉ
  - Bảo vệ tệp
  - Xác thực người dùng
- Kiểm soát truy nhập
- Nguyên tắc thiết kế Hệ điều hành
  - Giám sát thẩm quyền (Reference Monitor)
  - Phân hoạch (Separation)/Cách ly (Isolation)
  - Thiết kế phân tầng (Layered Design)

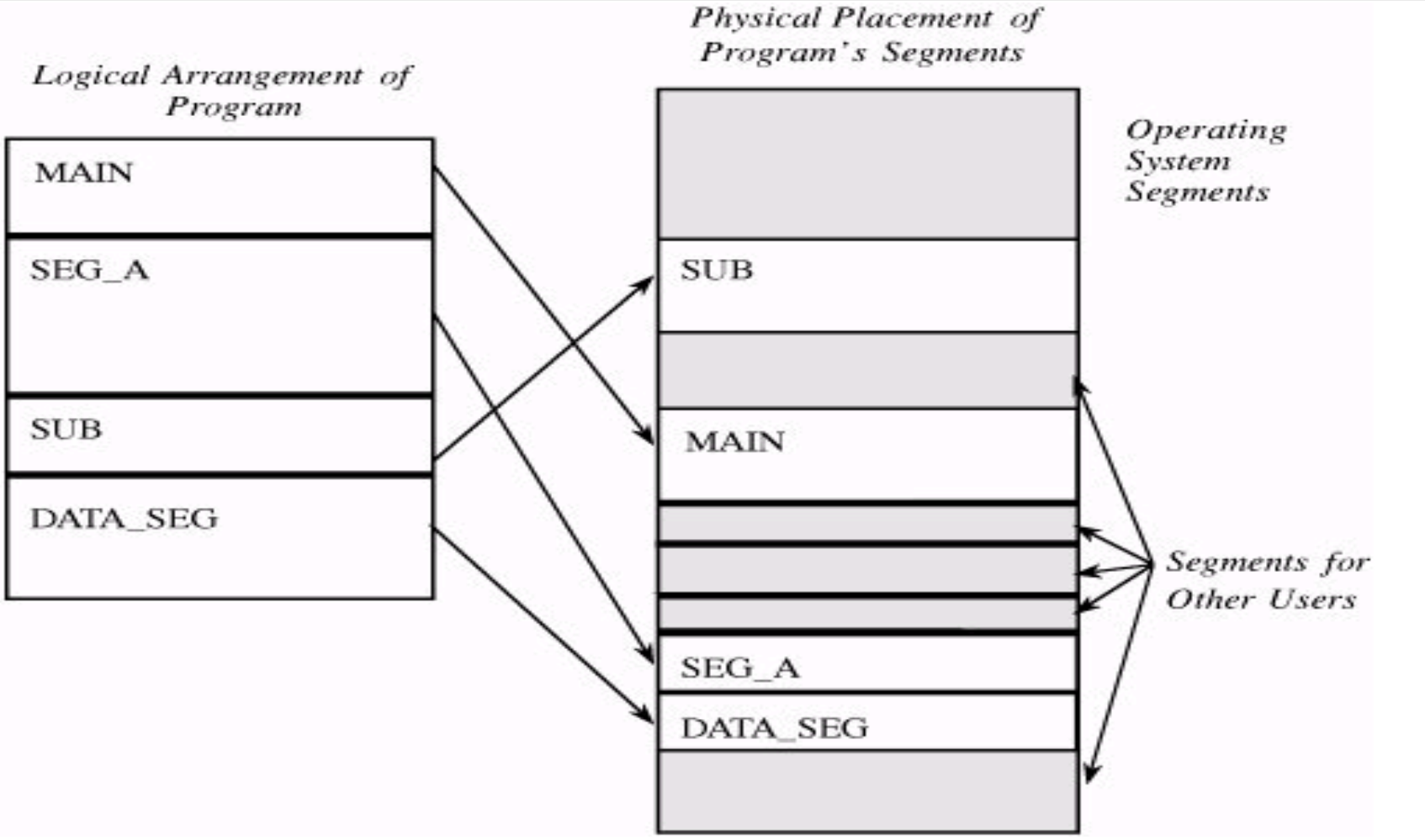
Bảo vệ bộ nhớ và địa chỉ

- Làm thế nào ngăn chặn một chương trình/người dùng can thiệp vào không gian bộ nhớ của chương trình/người dùng khác?
  - Phân đoạn (Segmentation)
  - Phân trang (Paging)

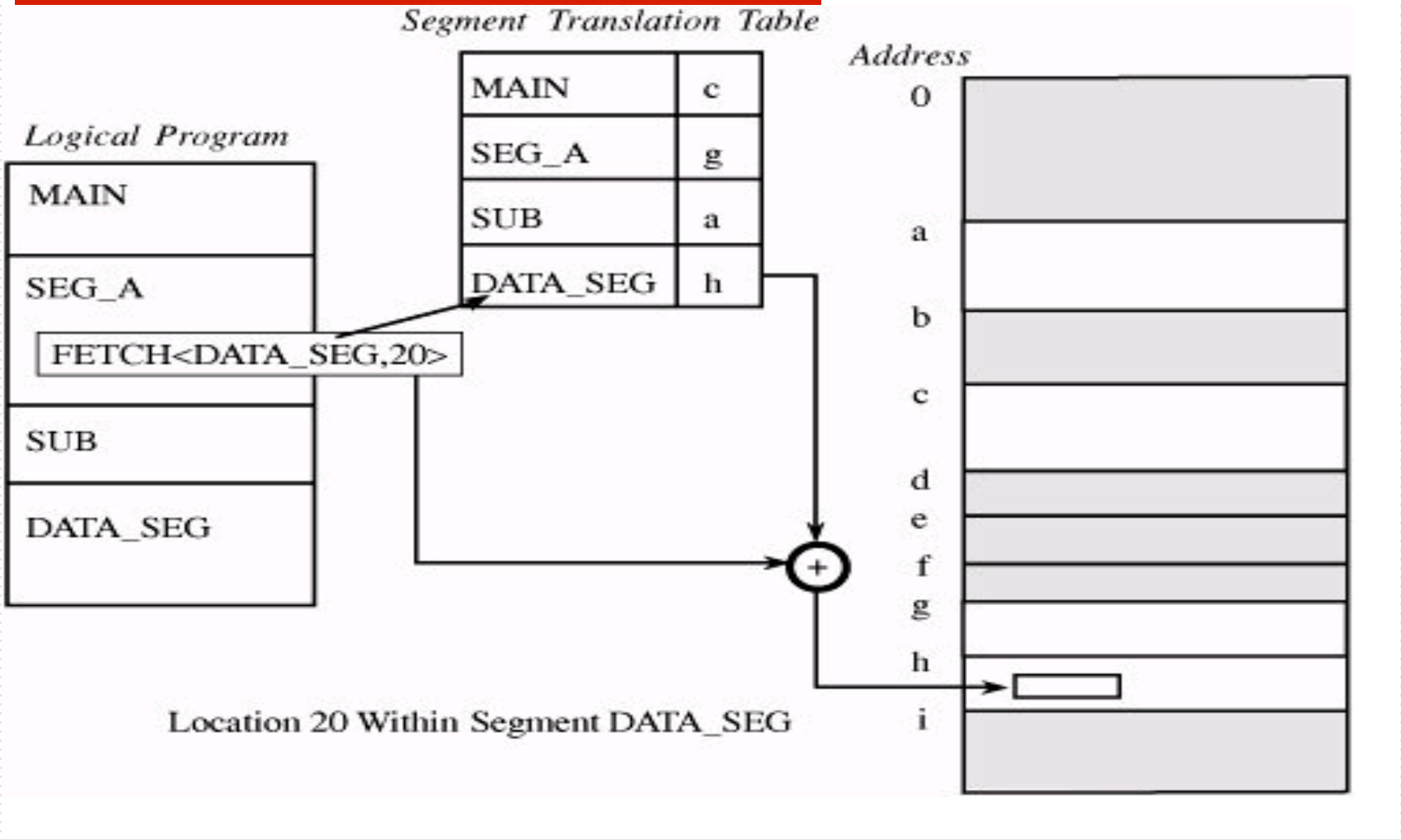
Phân đoạn (Segmentation)

- Phân chia chương trình thành các đoạn
  - Tương ứng với các đoạn dữ liệu, các chương trình con
  - Mỗi đoạn có quyền khác nhau (R,W,E)
- Phân chia bộ nhớ vật lý thành các đoạn
  - Tương ứng với, các mảng dữ liệu người dùng hoặc các đoạn mã chương trình
- Mỗi đoạn có một tên duy nhất
  - <Name,Offset>
- Hệ điều hành phải duy trì một bảng các đoạn

Đoạn logic và đoạn vật lý



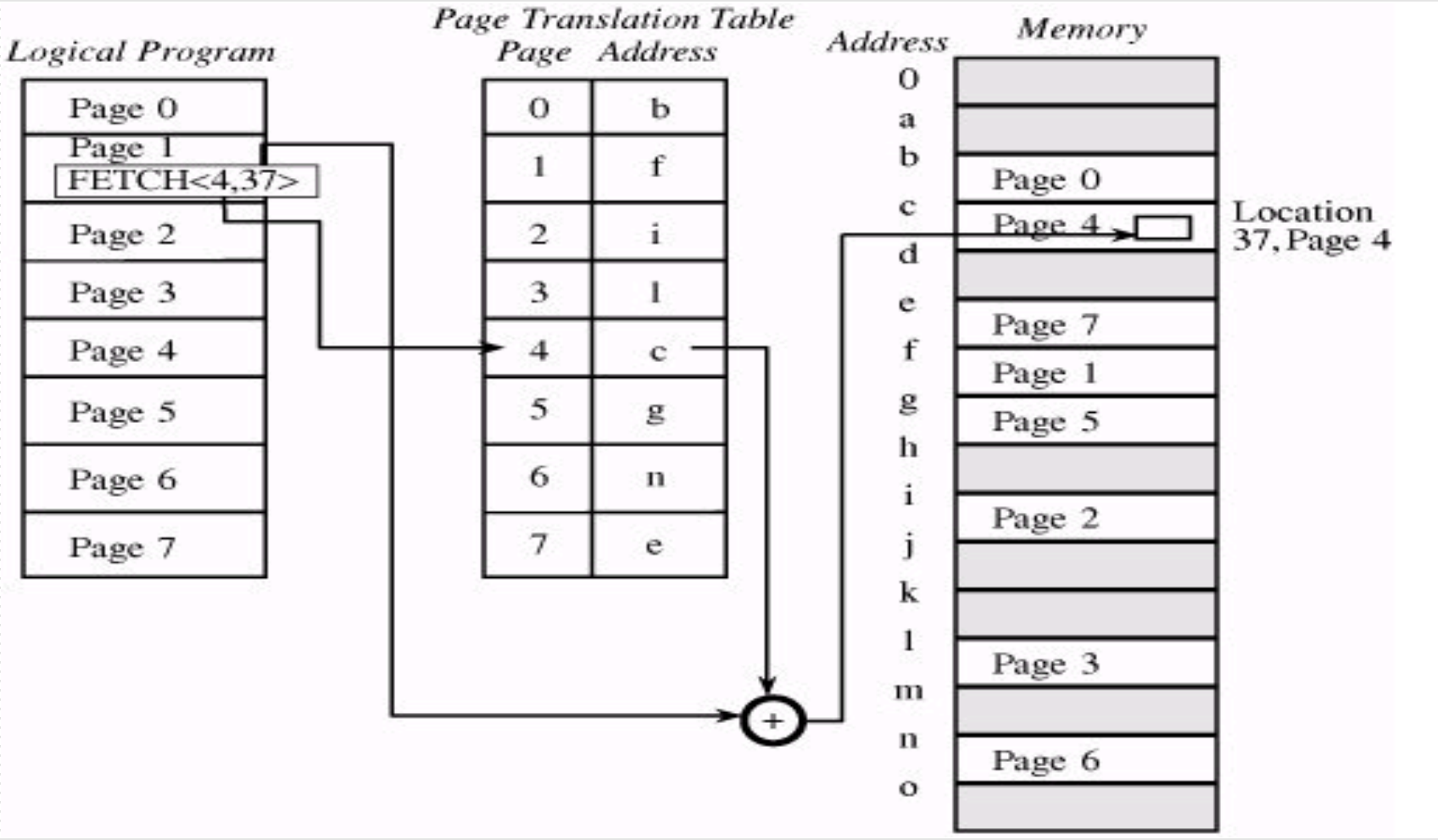
Tính địa chỉ đoạn



Phân trang (Paging)

- Phân chia chương trình thành các trang (page) cùng kích thước
- Phân chia bộ nhớ vật lý thành các khung trang (page frame) cùng kích thước
  - 512 đến 4096 byte
- Mỗi trang có một tên duy nhất
  - <Page,Offset>
- Hệ điều hành phải duy trì một bảng các trang

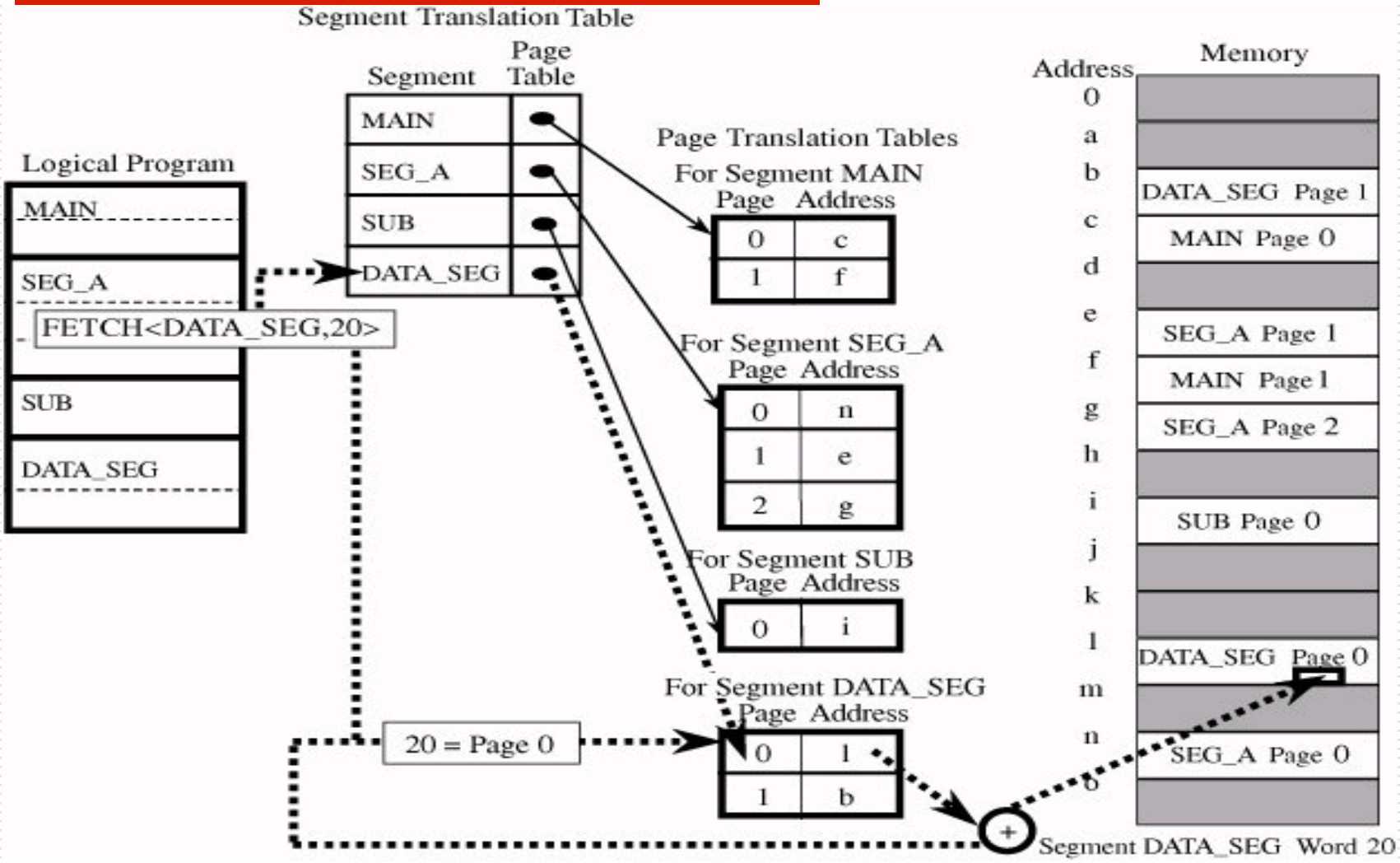
Tính địa chỉ trang



Kết hợp Phân đoạn và Phân trang

- Ưu điểm của phân đoạn
  - Bảo vệ bộ nhớ bằng cách phân quyền theo chương trình/người dùng
  - Hệ điều hành kiểm soát việc quyền đọc/ ghi/thực hiện trên bộ nhớ
- Ưu điểm của phân trang
  - Tốc độ
- Trong các hệ điều hành hiện đại
  - Kết hợp Phân đoạn+Phân trang

Kết hợp Phân đoạn và Phân trang



Bảo vệ tệp

- Bảo vệ nhóm
  - Tất cả người dùng được phân thành nhóm
  - Quyền sử dụng được một người dùng thiết lập cho mình và cả nhóm
- Bảo vệ cá thể
  - Mỗi người dùng có một số quyền
    - Quyền sử dụng lâu dài
    - Quyền sử dụng tạm thời

Bảo vệ tệp

- Hệ thống tệp UNIX/LINUX
  - Mỗi tệp có chủ sở hữu và nhóm sở hữu
  - Quyền được thiết lập bởi chủ sở hữu
    - R,W,E
    - setid, owner, group, other
  - Chỉ có chủ sở hữu và root mới được phép thay đổi quyền

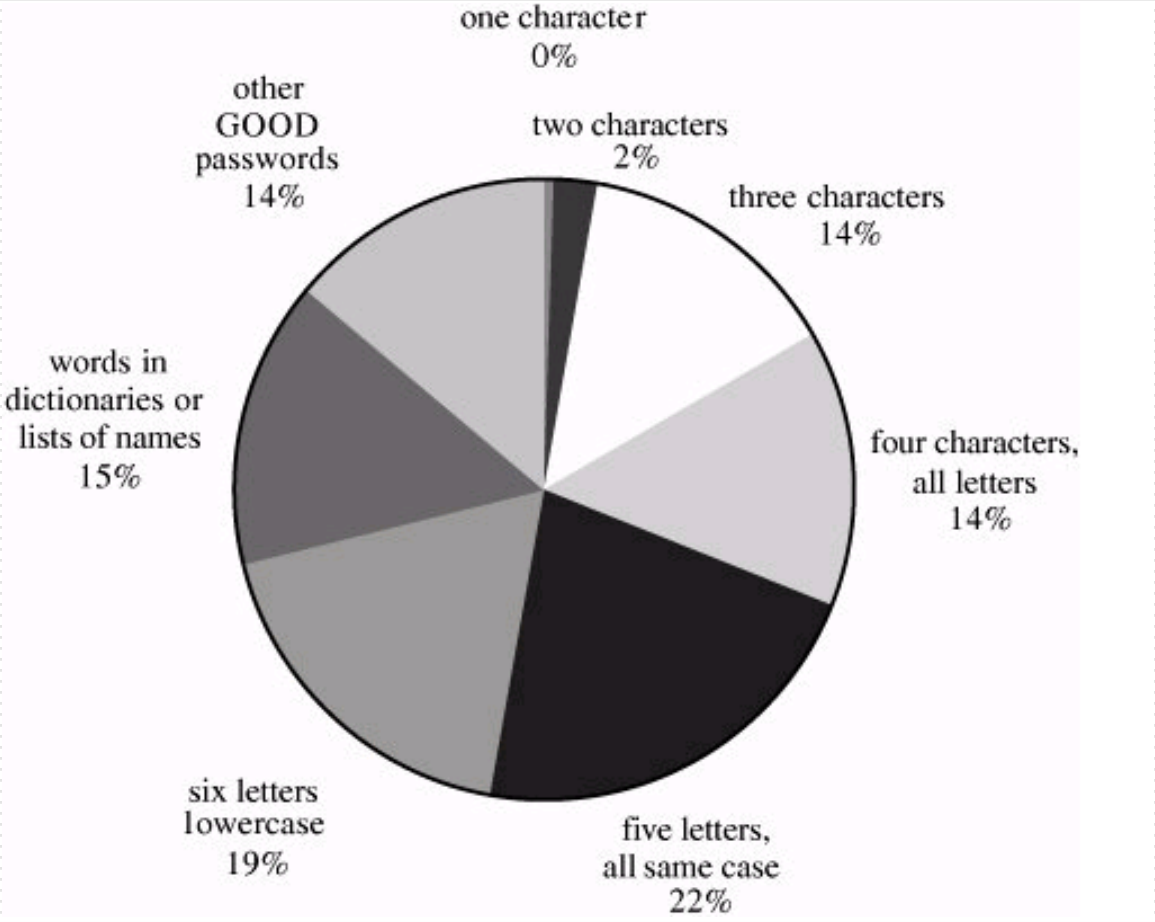
Xác thực người dùng

- Hệ điều hành quản lý nhiều người dùng
  - Ai là ai?
- Giải pháp xác thực người dùng
  - Mật khẩu
  - Một số đặc điểm sinh trắc học

Xác thực bằng mật khẩu

- Hệ điều hành lưu trữ một tệp người dùng/mật khẩu
  - Tệp thông thường
    - Thông tin lưu dạng văn bản
    - Độ an toàn thấp
  - Tệp mã hóa
    - Mã hóa cả tệp hoặc chỉ mã hóa mật khẩu
    - Độ an toàn phụ thuộc vào hệ mật mã
- Để tăng cường độ an toàn
  - Mật khẩu đủ dài, tránh chứa các thông tin đặc biệt
  - Thay đổi mật khẩu đều đặn
  - Đề phòng tấn công dạng “đăng nhập giả”

Thống kê lựa chọn mật khẩu



Xác thực bằng sinh trắc học

- Các đặc điểm sinh trắc học
  - Vân tay, mắt, khuôn mặt, chữ viết…
- Xác thực bằng sinh trắc học tương đối mới
  - Phát triển nhanh trong những năm
- Một số nhược điểm
  - Giá thành
  - Tốc độ/Độ chính xác
  - Giả mạo

An toàn Hệ điều hành

- Các vấn đề bảo vệ trong Hệ điều hành
  - Bảo vệ bộ nhớ và địa chỉ
  - Bảo vệ tệp
  - Xác thực người dùng
- Kiểm soát truy nhập
  - Các mô hình KSTN
  - KSTN trong Unix, Windows NT/2000
- Nguyên tắc thiết kế Hệ điều hành
  - Giám sát thẩm quyền (Reference Monitor)
  - Phân hoạch (Separation)/Cách ly (Isolation)
  - Thiết kế phân tầng (Layered Design)

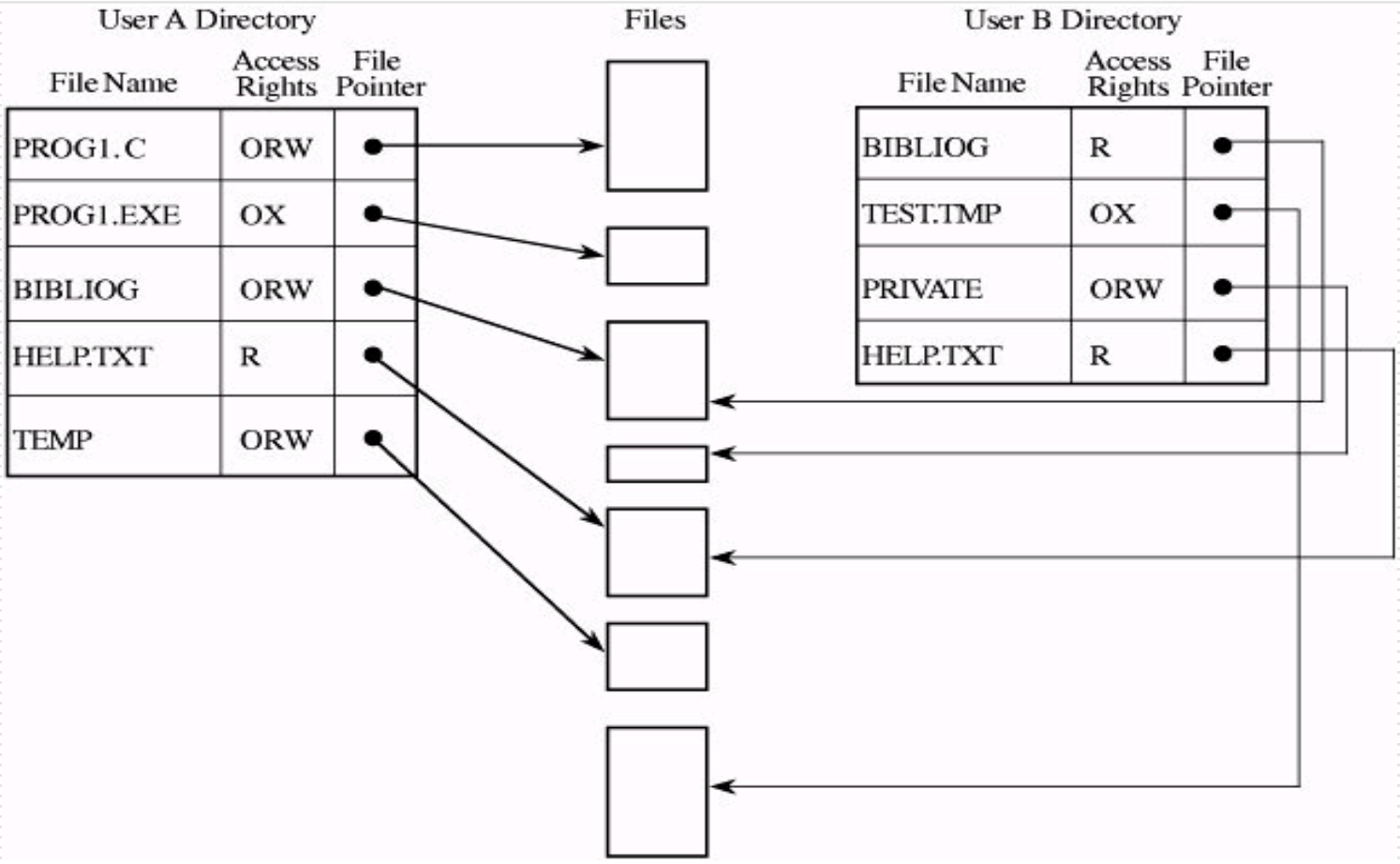
Kiểm soát truy nhập

- Rất nhiều đối tượng được truy nhập
  - Bộ nhớ
  - Phần cứng
  - Tệp
  - Thông tin hệ thống: bảng, cơ chế bảo vệ, lệnh đặc quyền
  - …
- Vấn đề an toàn đặt ra
  - Ai được truy nhập gì với đặc quyền nào?

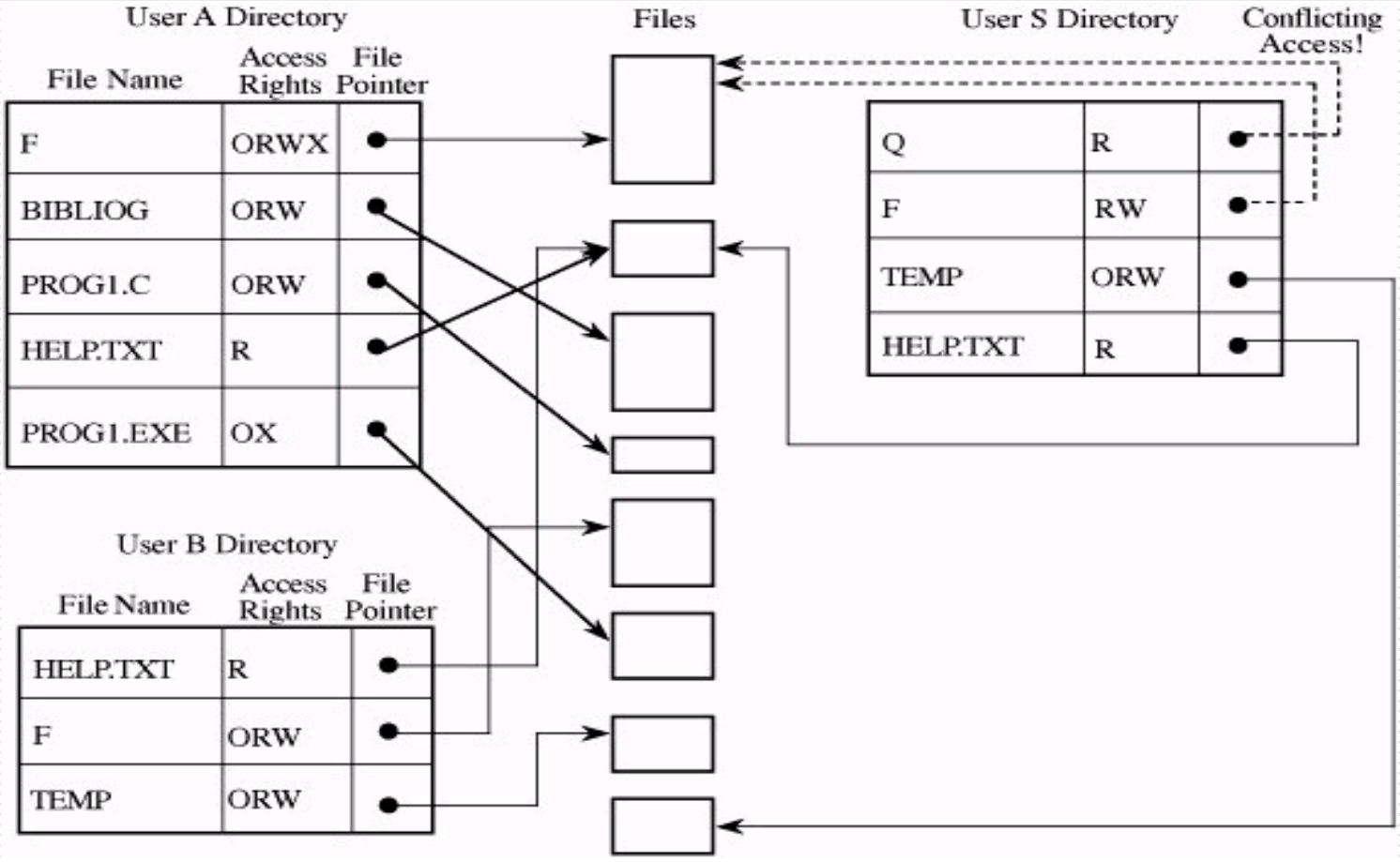
Cơ chế kiểm soát truy nhập

- Truy nhập thư mục
  - Mỗi đối tượng cần bảo vệ giống như một tệp
  - Mỗi người dùng có một số quyền nhất định trên một số tệp
- Danh sách kiểm soát truy nhập
  - Danh sách các đối tượng truy nhập
  - Mỗi đối tượng có một danh sách các chủ thể
- Ma trận kiểm soát truy nhập
  - Một chiều là danh sách các chủ thể
  - Một chiều là danh sách các đối tượng truy nhập tương ứng với các chủ thể

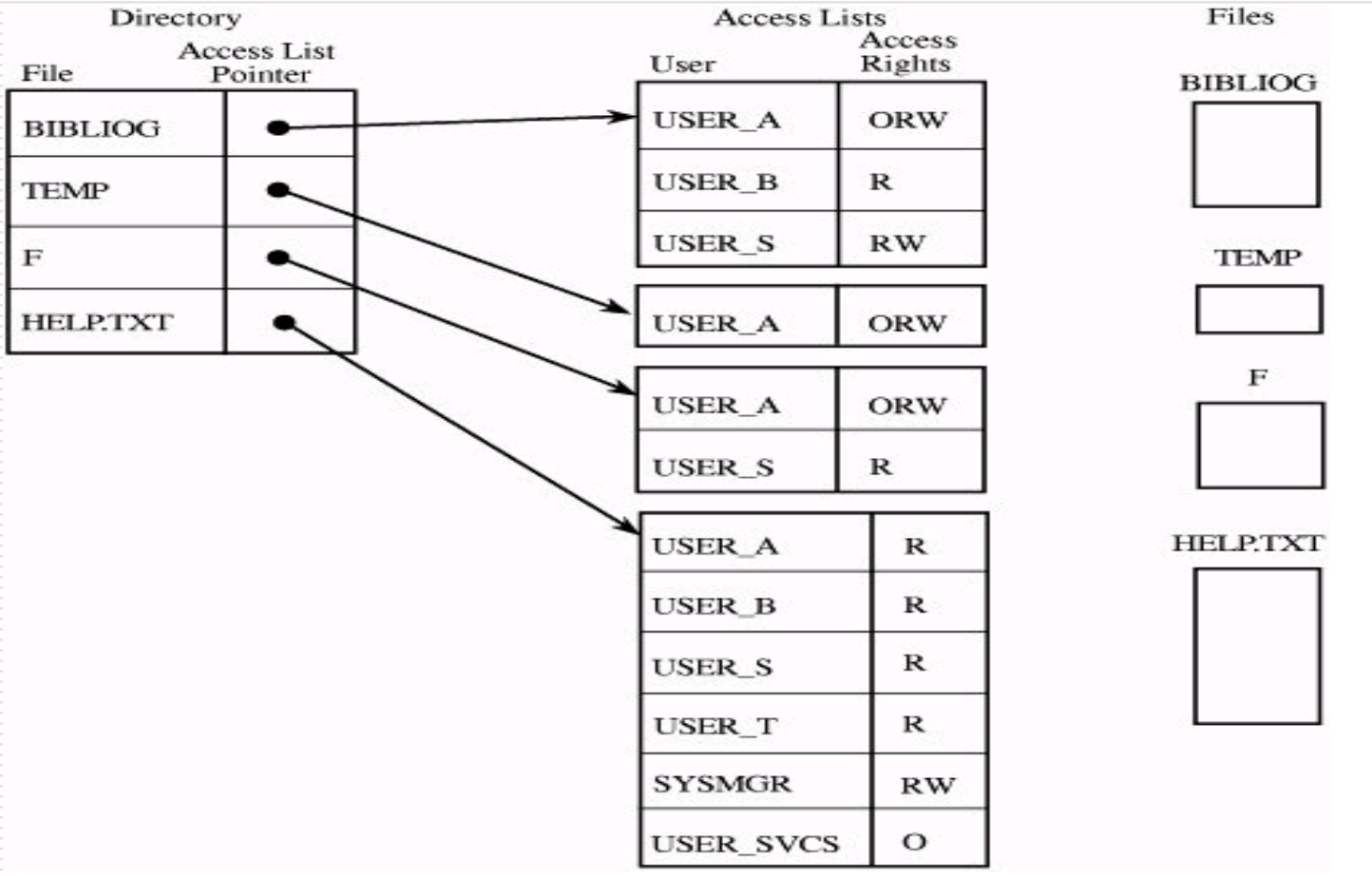
Truy nhập thư mục
Directory Access



Đường dẫn truy nhập thư mục



Danh sách kiểm soát truy nhập Access Control List



Ma trận kiểm soát truy nhập Access Control Matrix

	BIBLIOG	TEMP	F	HELP.TXT	C_COMP	LINKER	SYS_CLOCK	PRINTER
USER A	ORW	ORW	ORW	R	X	X	R	W
USER B	R			R	X	X	R	W
USER S	RW		R	R	X	X	R	W
USER T				R	X	X	R	W
SYS_MGR				RW	OX	OX	ORW	O
USER_SVCS				O	X	X	R	W

KSTN trong UNIX/LINUX

- Dùng ACL
- Đối với các tệp, thuộc tính *rwx* cho
  - Chủ sở hữu
  - Nhóm
  - Tất cả
  - Ví dụ

    drwxrwxrwx Alice Accounts

    -rw-r------ Bob Accounts
- Các chương trình chạy trong lúc hệ thống khởi động có đặc quyền quản trị (root)
- Các chương trình khác chạy với quyền người dùng (user)

KSTN trong UNIX/LINUX

- Làm thế nào để duy trì bộ 3 (người dùng, chương trình, tệp)
  - UNIX/LINUX dùng suid và sgid
- Vấn đề an toàn
  - suid root
- Vấn đề theo dõi thực thi chương trình
  - Thu hồi đặc quyền
- Vấn đề quản lý tiến trình
  - Tiến trình có một group id

KSTN trong WINDOWS NT/2000

- Quản lý (nhóm) người dùng sử dụng Active Directory
- Xác thực sử dụng Kerberos
- Các thuộc tính của tệp mịn hơn UNIX/ LINUX
  - read, write, execute, accessdenied, accessallowed, systemaudit,…
- Vấn đề quản trị có toàn quyền
  - Dùng Registry, một hình thức của ACL

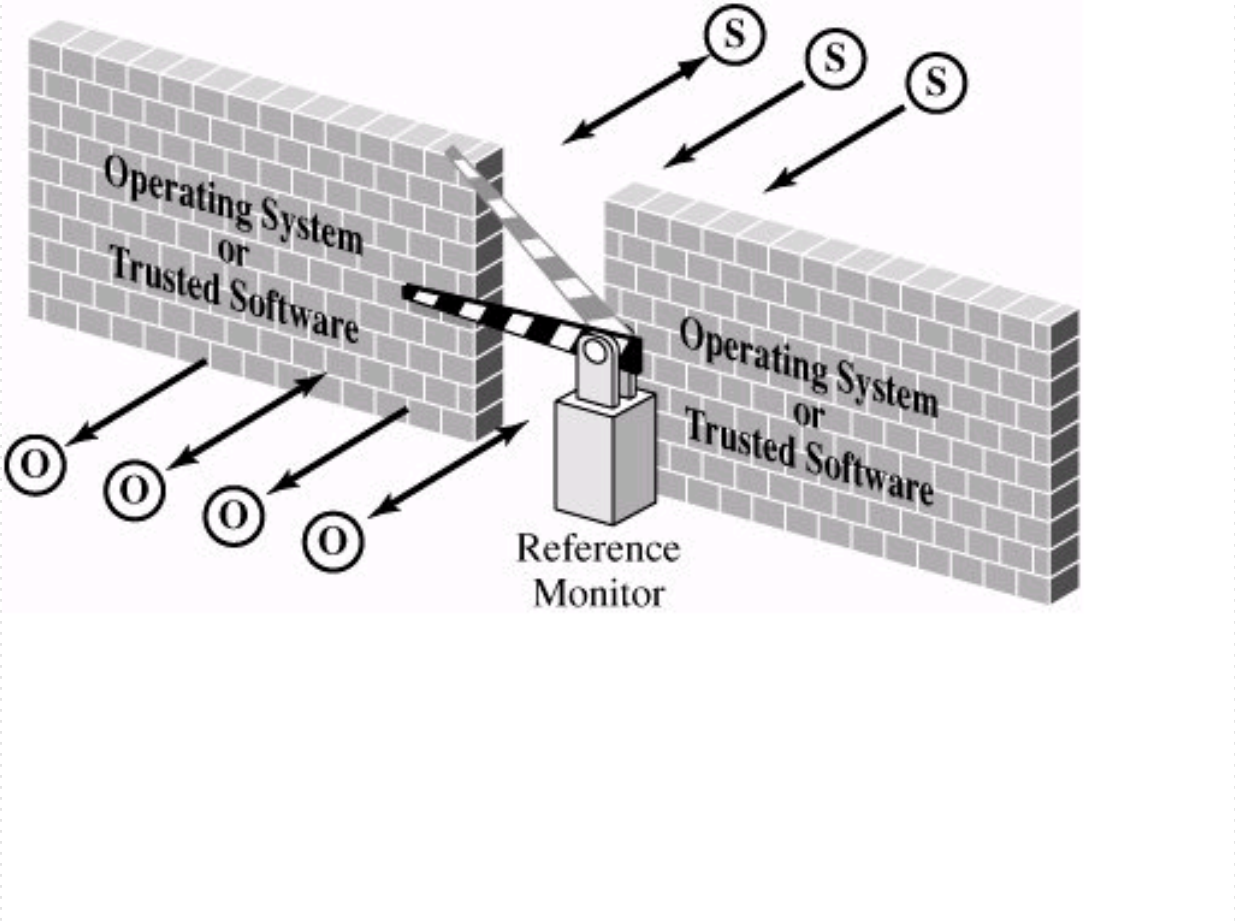
An toàn Hệ điều hành

- Các vấn đề bảo vệ trong Hệ điều hành
  - Bảo vệ bộ nhớ và địa chỉ
  - Bảo vệ tệp
  - Xác thực người dùng
- Kiểm soát truy nhập
  - Các mô hình KSTN
  - KSTN trong Unix, Windows NT/2000
- Nguyên tắc thiết kế Hệ điều hành
  - Giám sát thẩm quyền (Reference Monitor)
  - Phân hoạch (Separation)/Cách ly (Isolation)
  - Thiết kế phân tầng (Layered Design)

Giám sát thẩm quyền

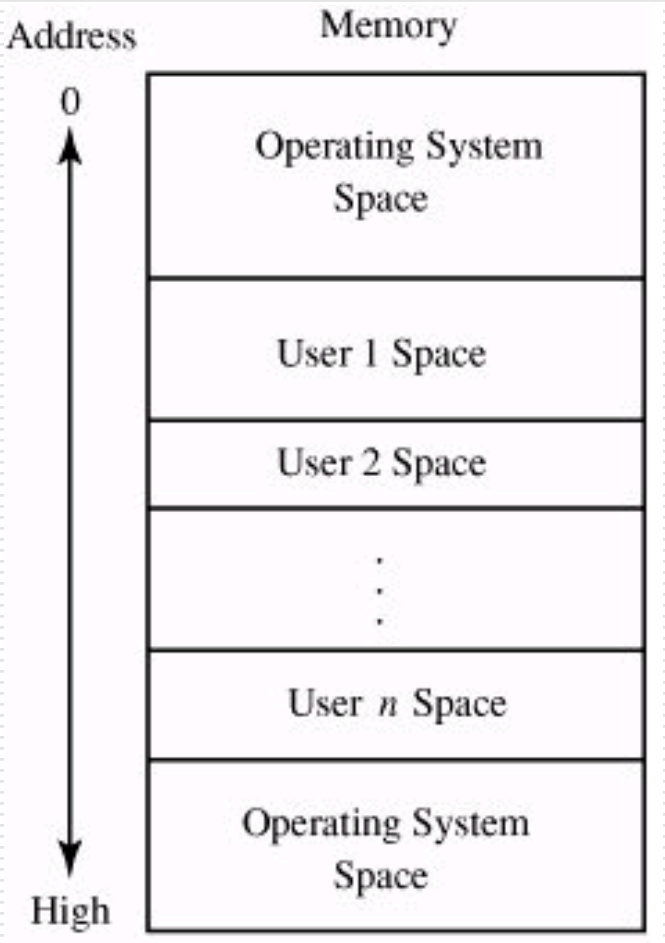
- Phần quan trọng nhất của hệ điều hành
- Là một tập các kiểm soát truy nhập các đối tượng
  - Bộ nhớ, thiết bị, tệp, thông tin các tiến trình, …
- Đặc điểm
  - Không bao giờ bị suy yếu, tê liệt
  - Luôn được gọi đến khi một đối tượng được yêu cầu sử dụng
  - Nhỏ gọn, để có thể dễ dàng phân tích và kiểm thử và đảm bảo tính đầy đủ

Giám sát thẩm quyền



Phân hoạch/Cách ly

- Phân hoạch vật lý
  - Các tiến trình khác nhau sử dụng các thiết bị khác nhau
- Phân hoạch thời gian
  - Các tiến trình với yêu cầu khác nhau thực hiện tại các thời gian khác nhau
- Phân hoạch logic (Cách ly)
  - Người dùng/tiến trình thực hiện nhiệm vụ của mình trong không gian của mình
- Phân hoạch mật mã
  - Người dùng/tiến trình giấu thông tinh của mình



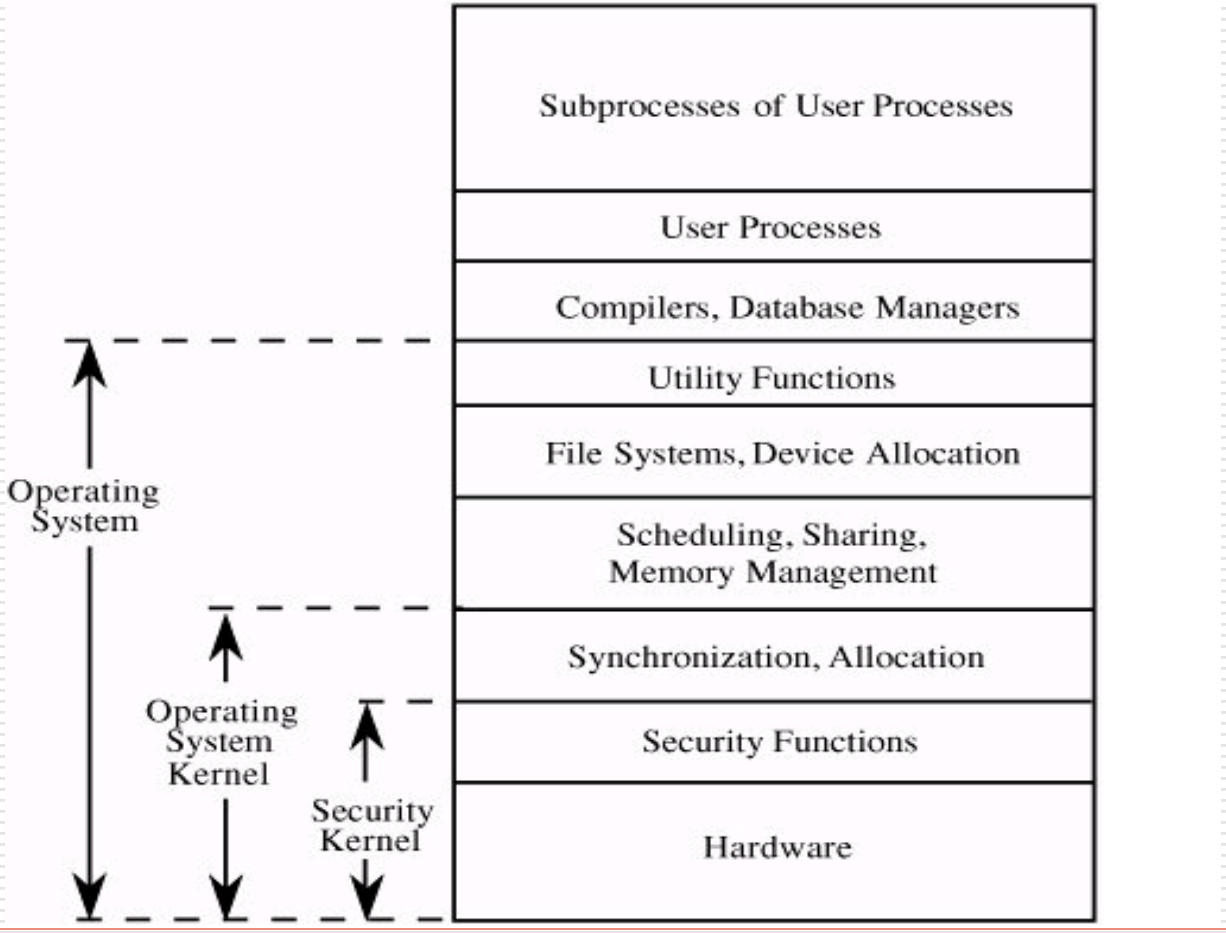
Thiết kế phân tầng

1. Lõi an toàn (Security Kernel)
    1. Phần cứng
    2. An toàn
2. Lõi hệ điều hành
    1. Đồng bộ
    2. Cấp phát
3. Hệ điều hành
    1. Sắp đặt, Chia xẻ, Quản lý bộ nhớ
    2. Hệ thống tệp, Cấp phát thiết bị
    3. Tính năng khác
4. Ứng dụng

Thiết kế phân tầng

- Một mô đun = nhiều mô đun hợp phần
  - Mỗi mô đun hợp phần thuộc một tầng khác nhau của kiến trúc đa tầng
- Ví dụ: Mô đun xác thực người dùng
  1. Cập nhật thông tin người dùng
  2. So sánh thông tin người dùng
  3. Tìm kiếm người dùng
  4. Giao diện xác thực người dùng

Thiết kế phân tầng



Môđun xác thực trong thiết kế phân tầng