HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC

An toàn hệ điều hành

Cơ chế bảo vệ phần cứng

Giảng viên: TS. Phạm Hoàng Duy

Điện thoại/E-mail: phamhduy@gmail.com

Bộ môn: An toàn thông tin - Khoa CNTT1

Nội dung

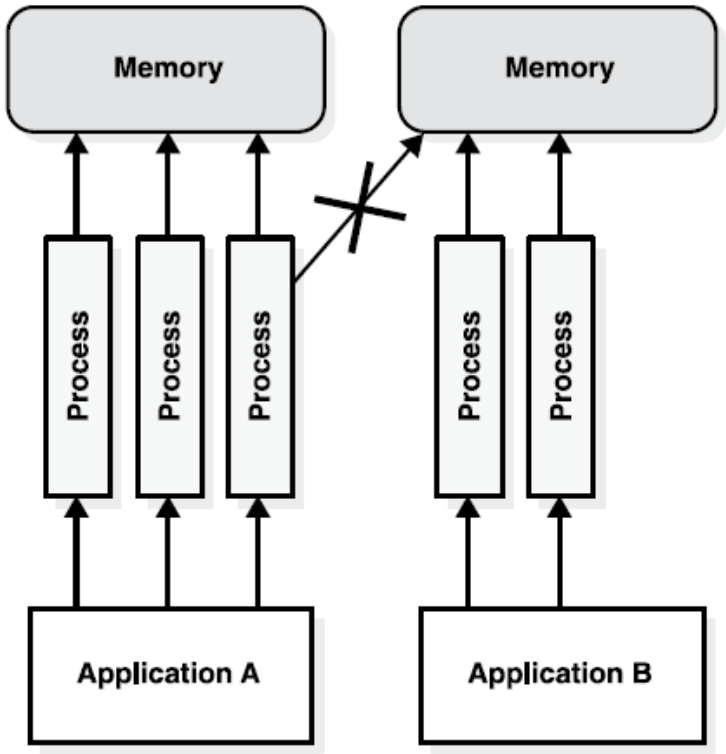
- Phân đoạn bộ nhớ
- Lớp bảo vệ (protection rings)

Chế độ bảo vệ CPU

- Để hệ điều hành hoạt động ổn định, hệ điều hành cần phân biệt được các hoạt động của riêng bản thân và các hoạt động của người dùng (chương trình)
  - Việc này phức tạp do bản thân hệ điều hành cũng là môt chương trình nên hệ điều hành phải theo dõi toàn bộ các hoạt động và đảm bảo các hoạt động này không vi phạm chính sách an toàn.
  - Hệ điều hành sử dụng một số cơ chế bảo vệ với sự hỗ trợ từ phần cứng để thực thi các cơ chế bảo vệ này

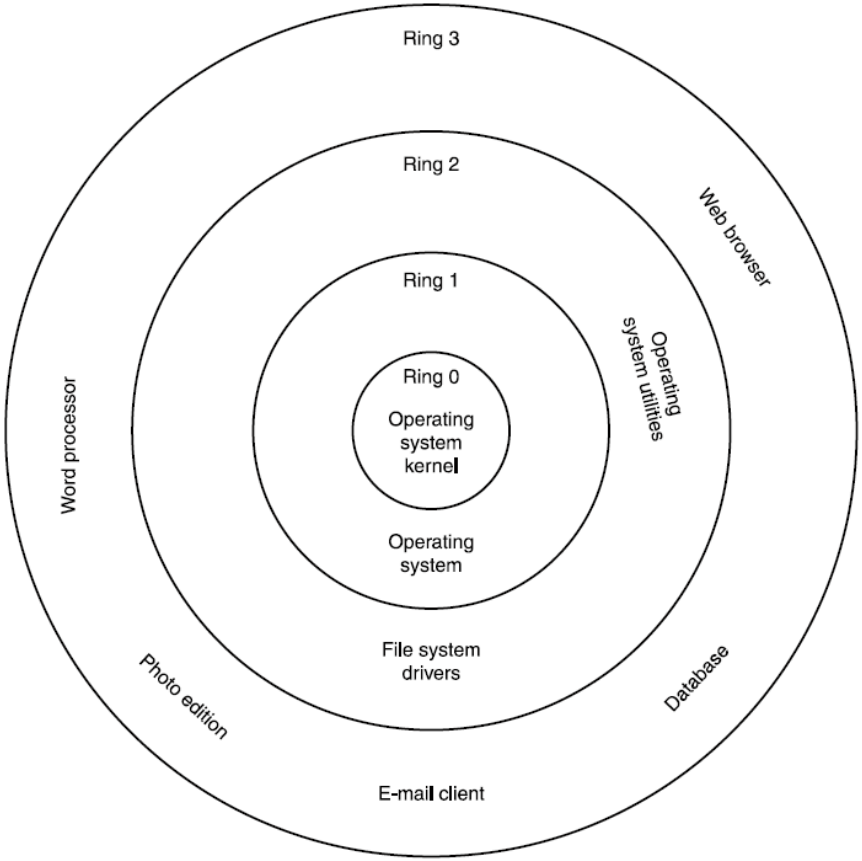
Phân đoạn bộ nhớ

- Phân đoạn bộ nhớ là một trong những cơ chế đảm bảo việc cách ly giữa các chương trình người dùng với nhau và với hệ điều hành
  - Các chương trình thay vì truy nhập trực tiếp bộ nhớ mà thông qua các bảng chỉ số và con trỏ mô tả phần không gian nhớ lô-gíc của chương trình.
  - Chỉ có hệ điều hành mới truy nhập trực tiếp bộ nhớ nhờ các lệnh sử dụng đặc quyền



Lớp bảo vệ (Protection rings)

- Các lớp đặt ra các ranh giới chặt chẽ và các mô tả những việc mã các chương trình (tiến trình) hoạt động trong từng lớp những thứ được truy nhập và những thao tác được phép thực hiện
  - Các chương trình nằm ở các lớp bên trong có nhiều đặc quyền hơn là nằm ở lớp ngoài



Lớp bảo vệ

- Các thành phần của hệ điều hành hoạt động tại lớp cung cấp các truy nhập tới vị trí bộ nhớ, thiết bị ngoại vi, trình điều khiển hệ thống và các tham số cấu hình nhạy cảm
  - Chính vì sử dụng các tài nguyên quan trọng nên đây là lớp được bảo vệ chặt chẽ nhất
- Các chương trình người dùng chịu hạn chế đến bộ nhớ và các thiết bị phần cứng và chịu giám sát của hệ điều hành thông qua các chức năng của hệ điều hành hay lời gọi hệ thống.
  - Nếu người dùng cố yêu cầu CPU thực hiện các lệnh vượt quá quyền hạn thì CPU xử lý những yêu cầu này như là lỗi hay cố gắng khóa chương trình lại.

Lớp bảo vệ

- Các lớp tiêu biểu
  - Lớp 0: Nhân hệ điều hành
  - Lớp 1: Phần còn lại của hệ điều hành
  - Lớp 2: Các trình điều khiển vào/ra và tiện ích
  - Lớp 3: chương trình ứng dụng
- Thực tế, các lớp bảo vệ được triển khai bằng cách kế hợp giữa phần cứng và hệ điều hành.
  - Phần cứng (CPU) được cấu hình để hoạt động với một số lớp nhất định
  - Hệ điều hành được xây dựng sao cho cùng hoạt động ở các lớp này

Lớp bảo vệ

- Các lớp bảo vệ hình thành nên các rào cản giữa chủ thể và đối tượng và thực thi việc giám sát truy nhập khi các chủ thể thực hiện việc truy nhập tới các đối tượng
  - Mỗi đối tượng và chủ thể được gán một số thể hiện cấp độ của lớp bảo vệ
  - Chủ thể có cấp độ thấp thì không thể truy nhập trực tiếp đối tượng có cấp độ cao hơn. Trong trường hợp cần thiết thì chủ thể có thể yêu cầu thông qua lời gọi hệ thống. Hệ điều hành sẽ thực hiện việc kiểm soát và hoàn tất truy nhập.

Lớp bảo vệ x86

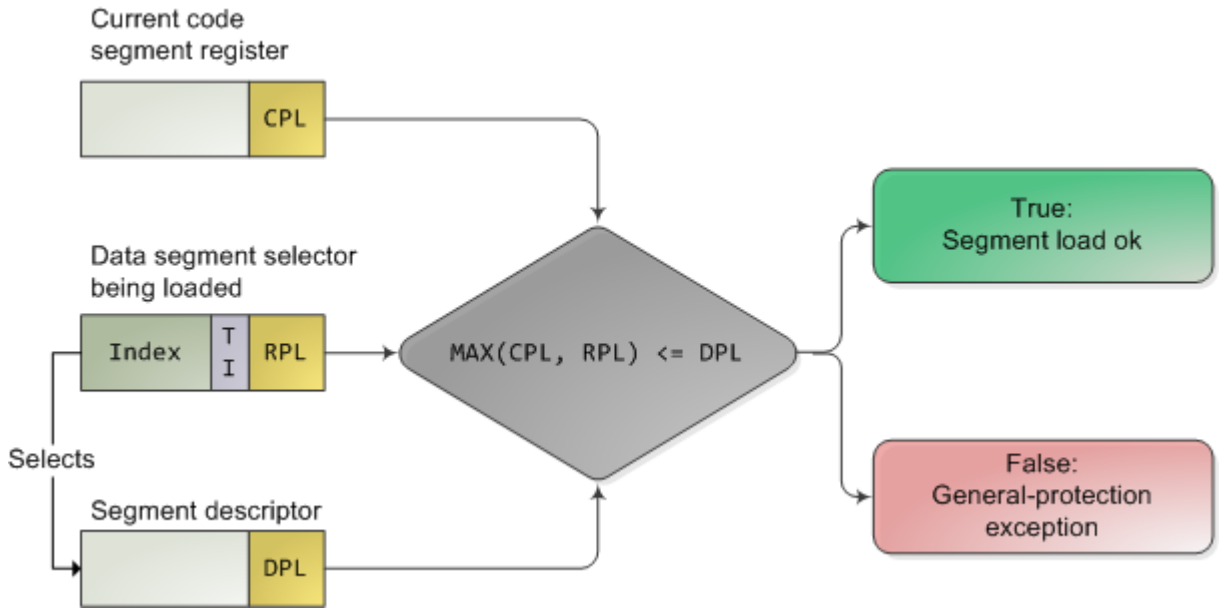
- CPU theo dõi mức đặc quyề (lớp bảo vệ) thông qua các trường:
  - ***RPL: Requested Privilege Level*** trên thanh ghi đoạn dữ liệu. Giá trị của trường này không thể được gán trực tiếp bởi các câu lệnh nạp dữ liệu mà chỉ bởi các câu lệnh thay đổi luồng thực hiện chương trình như câu lệnh *call*

Lớp bảo vệ x86

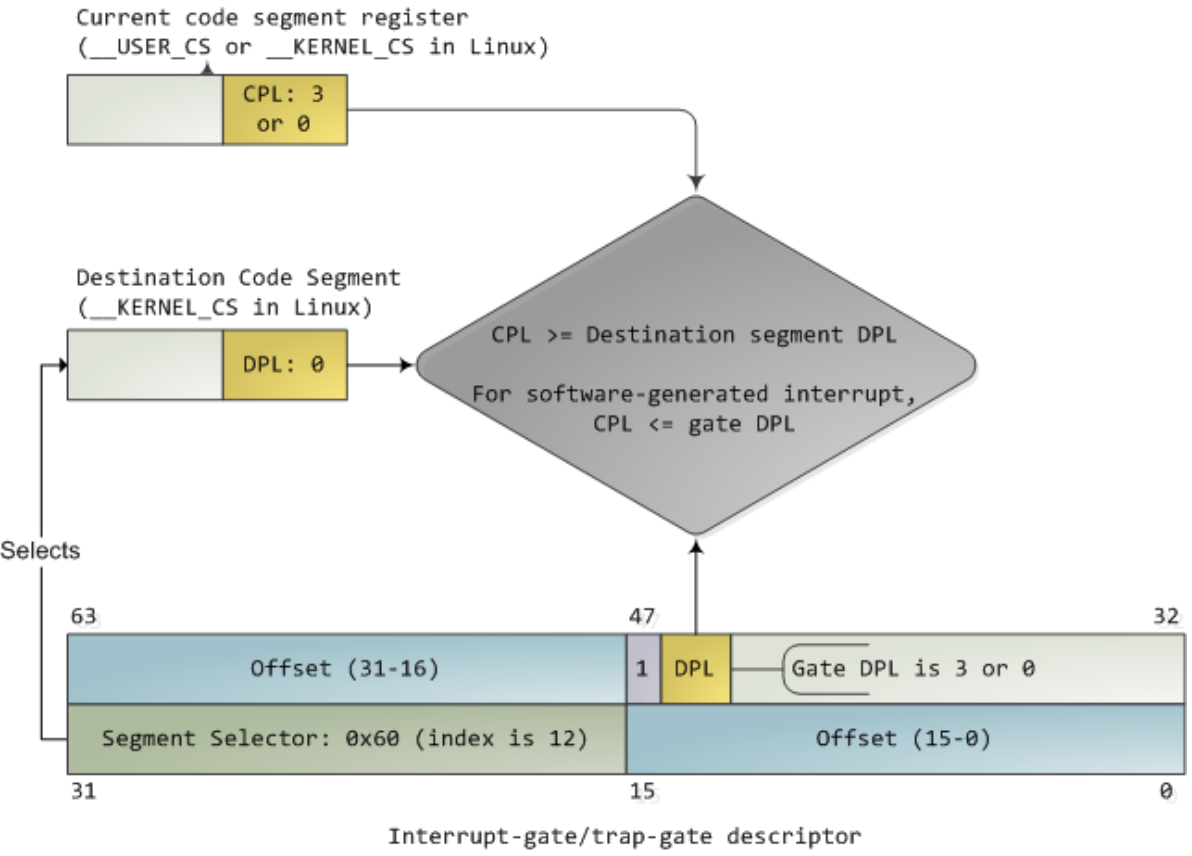
- ***CPL: Current Privilege Level*** trên thanh ghi đoạn lệnh. Giá trị này được duy trì bởi chính CPU và nó luôn bằng với mức bảo vệ hiện thời của CPU. Nói cách khác, giá trị CPL cho biết mức độ bảo vệ của đoạn mã được thực hiện.

Bảo vệ đoạn bộ nhớ x86

- Khi đoạn dữ liệu được nạp việc kiểm tra được diễn ra như trong hình dưới đây:
  - Mức độ bảo vệ của đoạn bộ nhớ DPL được so sánh với CPL và RPL. Giá trị DPL mà nhỏ hơn thì việc truy nhập là hợp lệ



Bảo vệ khi gọi ngắt



- Ngắt không chuyển quyền điều khiển từ lớp có cấp độ cao (0) sang lớp có cấp độ thấp hơn (3)
- Cấp độ bảo vệ cần giữ nguyên hoặc nâng cấp khi ngắt xảy ra với người dùng. Việc nâng cấp kèm theo với việc chuyển ngăn xếp (bộ nhớ) sang không gian nhớ phù hợp