BÀI 11 : An toàn và bảo vệ hệ thống

- An toàn hệ thống (security):
  - Bảo vệ cái gì ?
  - Chiến lược ?
- Bảo vệ hệ thống (protection)
  - Cơ chế kỹ thuật hỗ trợ thiết lập an toàn hệ thống

Các mối nguy hiểm

- Truy xuất bất hợp lệ
  - thâm nhập
  - thao tác lạm quyền
- "Núp bóng" truy xuất hợp lệ để phá hoại
  - "trojan horse
- "Kẻ xấu thật sự"
  - virus
  - worm

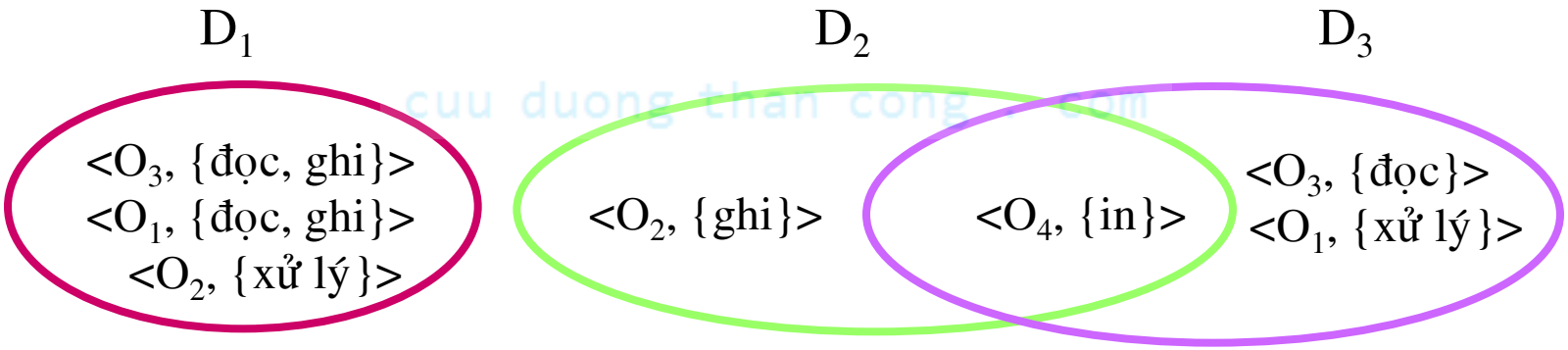
Thiết lập an toàn cho hệ thống

- Kiểm định danh tính (Authentication)
  - Xác định quyền hạn của *người dùng(authorized)*
  - password ?
- Sử dụng cơ chế nào để thực hiện các chiến lược kiểm tra an toàn?

Thuật ngữ

- *objects*: đối tượng cần được kiểm soát truy xuất
- *rights*: **Các khả năng thao tác trên một đối tượng**
- *domains*: **tập các quyền truy xuất,**

quyền truy xuất = <*đối tượng, {quyền thao tác}* >.



Ma trận quyền truy xuất

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	

Các cơ chế bảo vệ

- Cài đặt ma trận quyền truy xuất :
  - Access Control List:
    - Mỗi Object cómột ACL <domains,rights>
  - Capabilities
    - Mỗi Domain có một capabilities <objects,rights>