

AN TOÀN HỆ ĐIỀU HÀNH (Operating System Security)

Nguyễn Hồng Sơn
PTIT HCM

MỤC TIÊU CỦA MÔN HỌC

Kiến thức:

- Giải thích được các yếu tố cần đảm bảo để một hệ điều hành là an toàn
- Phân tích được các nguy cơ và lỗ hổng tiềm tàng đối với an toàn hệ điều hành
- Nắm vững các giải pháp an toàn cho hệ điều hành

Kỹ năng:

- Thực hiện được các tấn công khai thác lỗ hổng hệ điều hành
- Thực hiện được các giải pháp an toàn cho hệ điều hành

KẾ HOẠCH

- Số tín chỉ : 2 (30 tiết)
- Lý thuyết: 20 tiết (5 buổi)
- Thực hành: 10 tiết (3 buổi)
- Kiểm tra đánh giá:
 - Chuyên cần: 10%
 - Thực hành: 40%
 - Lý thuyết (cuối kỳ): tự luận, 50%

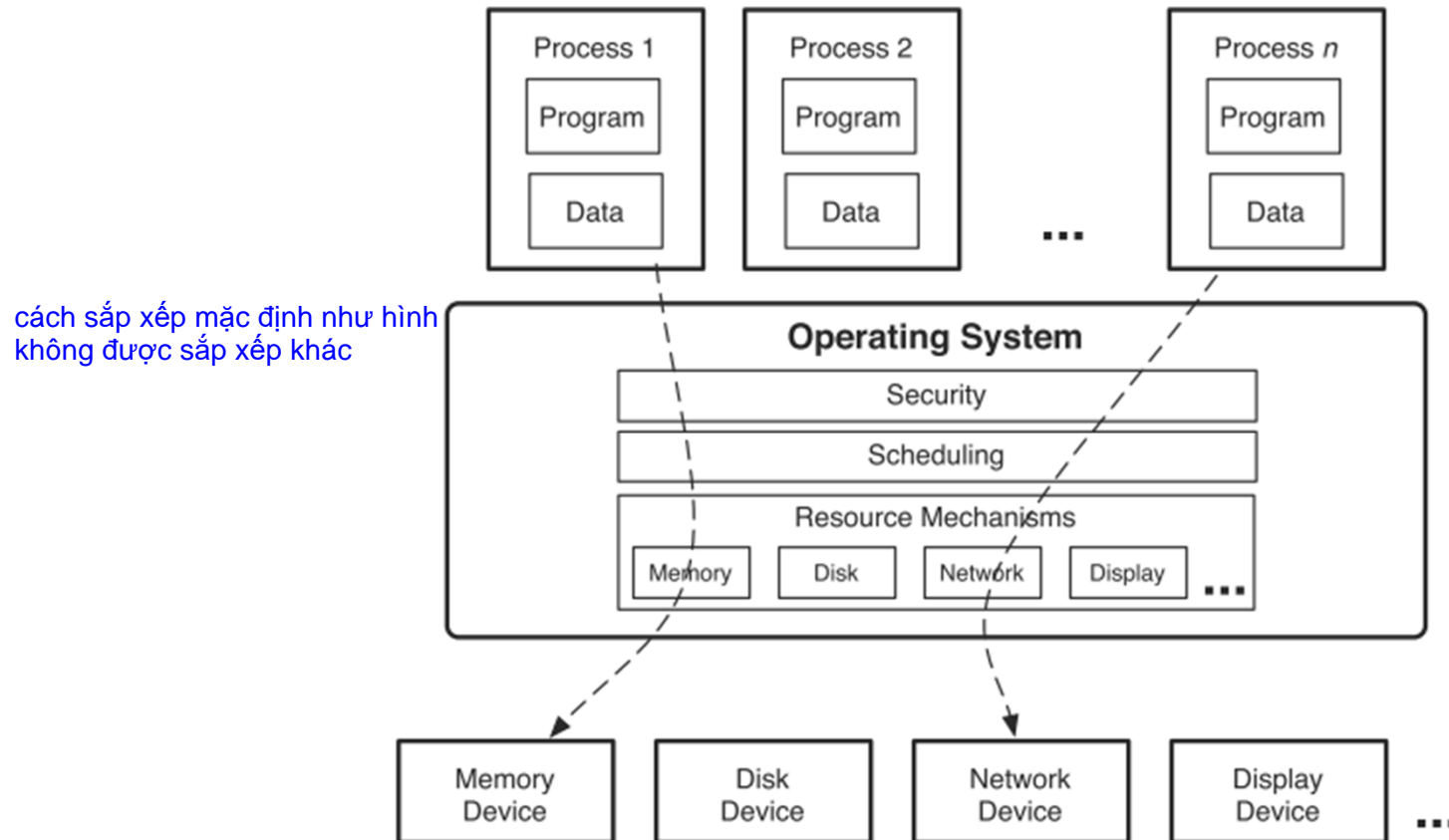
Tài liệu tham khảo

- [1] Bài giảng (slides)
- [2] Trent Jaeger, Operating System Security, The Pennsylvania State University, 2008
- [3] Peter Szor, The Art of Computer Virus Research And Defense, Addison Wesley Professional, 2005
- [4] Ric Vieler ,Professional Rootkits,Wrox Press 2007
- [5] Chris Anley,John Heasman,Gerardo Richarte, The Shellcoder's Handbook: Discovering and Exploiting Security Holes,Second Edition, Wiley Publishing, 2007


Introduction of Operating System Security

Functions of Operating Systems

- Provides access to the various hardware resources (e.g., CPU, memory, and devices)
- An operating system runs security, scheduling, and resource mechanisms to provide processes with access to the resources



Security

- đảm bảo
 Ensuring the security of all processes run on the system
- file hệ thống không cho phép tiến trình yêu cầu ghi đè lên không gian nhớ của file khác
For example, a file system **must not allow** a process request to access one file to overwrite the disk space allocated to another file.
- Also, file systems **must ensure** that one write operation is not impacted by the data being read or written in another operation.
- Scheduling mechanisms **must ensure** availability of resources to processes to prevent denial of service attacks.
- tấn công hdh
OS Attacks: The **misuse of OS's mechanisms to maliciously impact** the execution of another process

SECURITY GOALS

- The system implements accesses to system resources that satisfy the following:
tính bí mật, tính toàn vẹn và tính khả dụng
secrecy, integrity, and availability
- A system access is traditionally stated in terms of **which subjects** (e.g., processes and users) can perform **which operations** (e.g., read and write) on **which objects** (e.g., files and sockets).
- Secrecy requirements hạn chế đối tượng có thể truy cập (Phân quyền) **limit the objects** Hạn chế khả năng đọc that individual **subjects can read** because objects may contain secrets that not all subjects are permitted to know.
- Integrity requirements Giới hạn khả năng sửa chữa(phân quyền sửa chữa) **limit the objects** hạn chế khả năng ghi that **subjects can write** because objects may contain information that other subjects depend on for their correct operation. Some subjects may not be trusted to modify those objects.
- Availability requirements Giới hạn nguồn tài nguyên hệ thống 1 chủ thể có thể sử dụng(Không cho phép chiếm dụng -> cạn kiệt tài nguyên => vi phạm nguyên tắc thiết kế hđh) **limit the system resources** (e.g., storage and CPU) that qui định mức tài nguyên tối đa một tiến trình có thể sử dụng **subjects may consume** because they may exhaust these resources.

Threats of Security Goals

Lỗi hỏng về cơ chế hdh

- Vulnerabilities of OS's mechanisms

Lỗi hỏng về cơ chế của phần cứng

- Vulnerabilities of Hardware's mechanisms

Cơ chế liên kết giữa An Toàn Hệ Điều Hành với An Toàn Máy Tính

- OS security in association with Computer security