HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC

An toàn hệ điều hành

Giới thiệu chung

Giảng viên: TS. Phạm Hoàng Duy

Điện thoại/E-mail: phamhduy@gmail.com

Bộ môn: An toàn thông tin - Khoa CNTT1

- Đường dẫn môn học
  - https://drive.google.com/open?id=0B_rgEztHXVWJY1Q4Y2pLbG85VzA
- Chia nhóm bài tập lớn
  - Mỗi nhóm 4-5 người

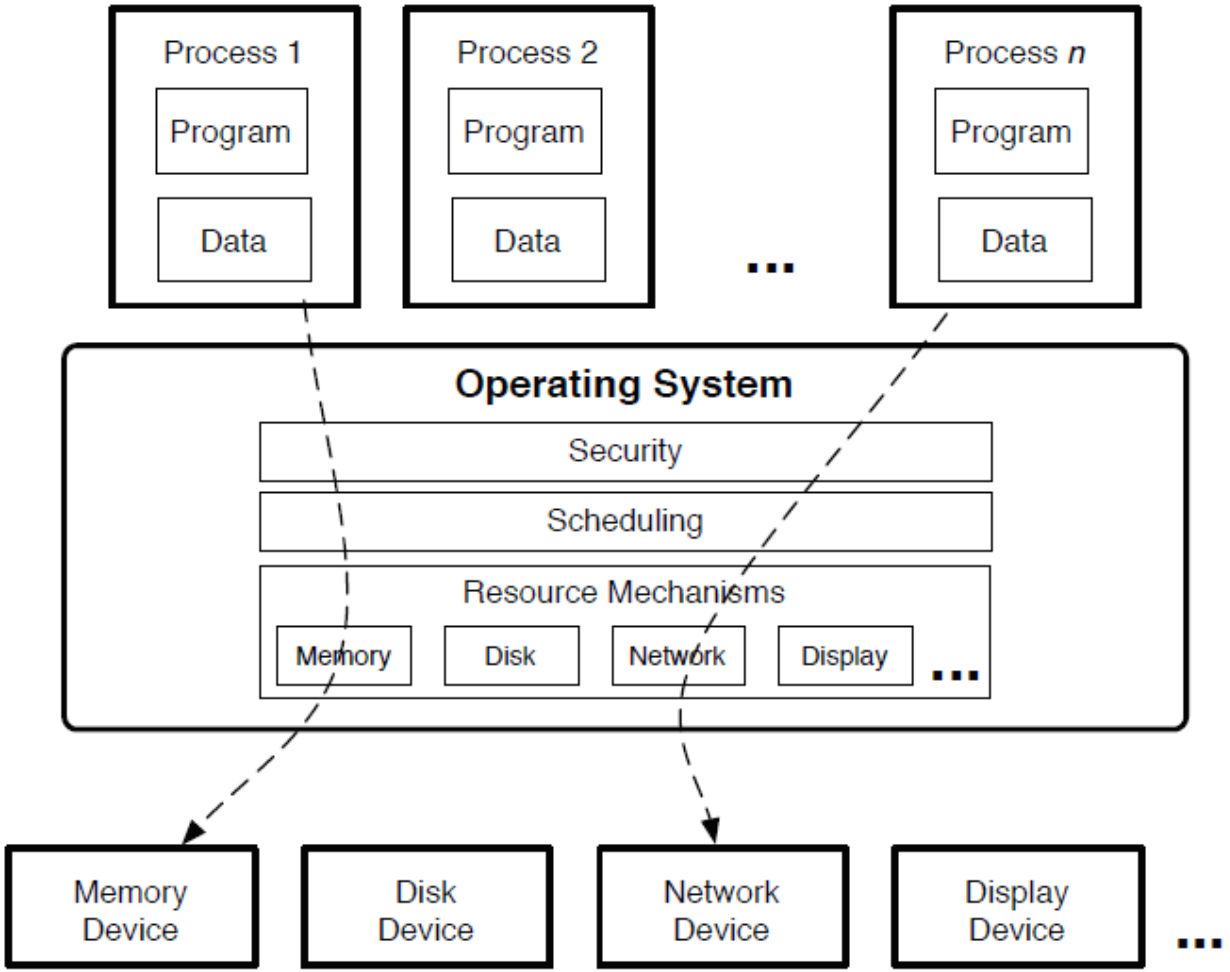
Nội dung

- Giới thiệu chung
- Hệ điều hành an toàn

Giới thiệu hệ điều hành

- Hệ điều hành là phần mềm đặc biệt cho phép người dùng truy nhập tới các tài nguyên phần cứng khác nhau như bộ xử lý, bộ nhớ, các thiết bị
  - Người dùng thông qua các chương trình để sử dụng phần cứng máy tính
  - Các chương trình thực thi nhờ các CPU
  - Việc thực thi của các chương trình cần truy nhập tới các tài nguyên khác (phần cứng)

Giới thiệu hệ điều hành



Chức năng quan trọng

- Hệ điều hành phải cung cấp cơ chế sử dụng tài nguyên hiệu quả
  - Quản lý CPU,
  - Quản lý bộ nhớ
  - Hệ thống file
  - Giao thức mạng
  - ...
- Hệ điều hành phải cung cấp cơ chế điều độ giữa các chương trình người dùng đảm bảo việc sử dụng tài nguyên công bằng

Chức năng quan trọng

- Hệ điều hành phải kiểm soát việc truy nhập tới các tài nguyên sao cho chương trình người dùng không ảnh hưởng vô tình hay xấu tới chương trình khác.
  - Đây chính là vấn đề đảm bảo an toàn cho các chương trình chạy trong hệ thống

Vấn đề an toàn

- Việc đảm bảo các chương trình hoạt động một cách an toàn lệ thuộc vào việc triển khai đúng đắn các cơ chế chia sẻ và điều độ tài nguyên
  - Các cơ chế truy nhập tài nguyên phải xác định ranh giới các tài nguyên và đảm bảo các thao tác tới các tài nguyên này không xung đột với nhau.
  - Cơ chế điều độ phải đảm bảo tính sẵn sàng của tài nguyên cho các chương trình để ngăn chặn tấn công từ chối dịch vụ.

Vấn đề an toàn

- An toàn được quan tâm do các chương trình trong máy tính hiện đại tương tác với nhau theo nhiều cách và việc chia sẻ dữ liệu giữa các người dùng là hành vi căn bản và phổ biến với hệ thống máy tính.
- Thách thức với việc thiết kế an toàn cho hệ điều hành là thiết kế các cơ chế an toàn để bảo vệ việc thực thi của các chương trình và dữ liệu của chúng trong môi trường phức tạp.
  - Các cơ chế an toàn chính tắc (*formal security mechanism*) giúp chứng minh hệ thống đạt được các mục tiêu an toàn song không tính đến độ phức tạp của hệ thống

Vấn đề an toàn

- An toàn hệ điều hành được tiếp cập theo hai hướng chủ yếu
  - Hệ thống có ràng buộc: đảm bảo các mục tiêu an toàn được thỏa mãn với mức độ cao
  - Hệ thống dùng chung (general-purpose): chỉ đảm bảo các mục tiêu an toàn một cách hạn chế với mức độ thấp
- Các hệ thống dùng chung hướng tới cung cấp các chức năng mềm dẻo, thân thiện người dùng, dễ triển khai và có hiệu năng cao. Các đặc điểm này dẫn đến nhiều thách thức với việc đảm bảo an toàn cho hệ thống.

An toàn hệ điều hành

An toàn hệ điều hành

- Khái niệm
- Mục tiêu an toàn (security goal)
- Mô hình tin cậy (Trust model)
- Mô hình đe dọa

Khái niệm

- Hệ điều hành an toàn là hệ điều hành cung cấp cơ chế an toàn đảm bảo đạt được các mục tiêu an toàn của hệ thống cho dù hệ thống phải đối mặt với các mối đe dọa
- Thông thường hệ điều hành đạt được mức độ đảm bảo cao được coi là hệ điều hành an toàn hay gọi là hệ thống tin cậy (trusted system)

Mục tiêu an toàn

- Mục tiêu an toàn xác định các thao tác có thể được thực hiện bởi hệ thống trong hi ngăn chặn các truy nhập trái phép
- Các mục tiêu an toàn xác định các yêu cầu mà thiết kế hệ thống cần phải thỏa mãn và việc triển khai đúng đắn phải thỏa mãn các yêu cầu này.
- Mục tiêu an toàn cần thỏa mãn các yếu tố sau
  - Bí mật
  - Toàn vẹn
  - Sẵn dùng

Mục tiêu an toàn

- Truy nhập hệ thống được mô tả bằng ***chủ thể*** (chương trình hay người dùng) có thể thực hiện ***các thao tác*** (đọc hay ghi) lên các ***đối tượng*** (file hay socket)
  - Tính bí mật giới hạn các đối tượng có thể được truy nhập
  - Tính toàn vẹn hạn chế các đối tượng mà chủ thể có thể ghi để đảm bảo thao tác được đúng đắn trong quan hệ với các thao tác của các chủ thể khác
  - Tính sẵn dùng hạn chế các tài nguyên mà các chủ thể có thể sử dụng do các chủ thể có thể làm cạn kệt tài nguyên đó

Mục tiêu an toàn

- Mục tiêu an toàn có thể được xây dựng dựa trên tính bí mật
  - Mô hình Bell-LaPadula
- Mục tiêu an toàn có thể xây dựng dựa trên các chức năng
  - Đặc quyền tối thiểu
  - Hạn chế chức năng không làm tăng độ an toàn của hệ thống mà chỉ làm giảm rủi ro của việc tấn công

Mô hình tin cậy

- Mô hình tin cậy của hệ thống định nghĩa tập phần mềm và dữ liệu mà hệ thống dựa vào để đảm bảo thực hiện chính xác các mục tiêu an toàn của hệ thống
- Các phần mềm được tin cậy bao gồm phần mềm xác định mục tiêu an toàn và phần mềm đảm bảo các mục tiêu an toàn này
- Người phát triển hệ điều hành an toàn phải chứng minh hệ thống của mình có mô hình tin cậy tồn tại
  - Phần mềm tin cậy phải thực hiện toàn bộ các thao tác nhạy cảm với an toàn
  - Chứng minh tính đúng đắn của phần mềm và dữ liệu tin cậy
  - Chứng minh việc thực thi của các phần mềm không bị phá vỡ bởi các chương trình khác

Mô hình đe dọa

- Mô hình đe dọa xây dựng tập các thao tác mà người tấn công có thể dùng để vô hiệu hóa hệ thống
  - Tập các thao tác này không hạn chế theo nghĩa người tấn công có thể áp dụng bất cứ thao tác có thể để xâm phạm mục tiêu an toàn của hệ thống
- Nhiệm vụ của người xây dựng hệ điều hành an toàn là bảo vệ các phần mềm tin cậy khỏi các dạng đe dọa trong mô hình.
  - Chương trình người dùng có thể không tin cậy song hệ thống có thể hạn chế việc truy nhập tới dữ liệu nhạy cảm

An toàn trong UNIX và Windows

UNIX

- UNIX được viết bằng ngôn ngữ C giúp cho nó trở thành hệ điều hành đầu tiên có tính khả chuyển (chạy được trên nhiều phần cứng khác nhau) và thu hút được cộng đồng phát triển đông đảo.
- UNIX có giao diện chương trình (API) thuận tiện cho người phát triển
- UNIX hướng đến chương trình căn bản nhỏ gọi là nhân (kernel) với giao diện chuẩn để đơn giản hóa việc phát triển ứng dụng
- Mục tiêu thiết kế của UNIX là phát triển nền tảng chung chia sẽ giữa các người dùng với nhau

Mục tiêu an toàn

- Mục tiêu an toàn của UNIX là bảo vệ dữ liệu người dùng khỏi các lỗi vô tình trong chương trình người dùng.
  - Việc bảo vệ này không đảm bảo yêu cầu về tính bí mật và toàn vẹn.
- Cơ chế an toàn UNIX nhằm bảo vệ người dùng với nhau và hạ tầng tính toán tin cậy của hệ thống khỏi toàn bộ các người dùng. Hạ tầng tính toán tin cậy của UNIX bao gồm nhân và các tiến trình được chạy với đặc quyền *root* hay *superuser*

Hệ thống bảo vệ UNIX

- Hệ thống bảo vệ: sử dụng cơ chế kiểm soát truy nhập tùy chọn
  - Các tài nguyên trong hệ thống được coi như các file
  - Người dùng và nhóm người dùng được gán định danh
  - Kiểm soát truy nhập được thực hiện thông qua các bit trạng thái

Name	Owner	Group	Mode Bits
foo	alice	faculty	rwxr--r--
bar	bob	students	rw-rw-r--
baz	charlie	faculty	rwxrwxrwx

Hệ thống xác thực

- Hệ thống này kiểm soát việc truy nhập của các tiến trình tới các file và thực hiện việc dịch chuyển miền bảo vệ cho phép người dùng thay đổi định danh.
- Hệ thống này nằm ở trong nhân song phụ thuộc vào các tiến trình bên ngoài (hệ thống hay người dùng) để xác định các yêu cầu xác thực và trạng thái bảo vệ
- Quá trình xác thực diễn ra mỗi khi có yêu cầu truy nhập file và thao tác được phép trên file đó sẽ được thẩm tra.
- Vấn đề: ý nghĩa cụ thể của các thao tác read/write với dữ liệu hay các meta-data của file

- Hệ điều hành Windows

Windows

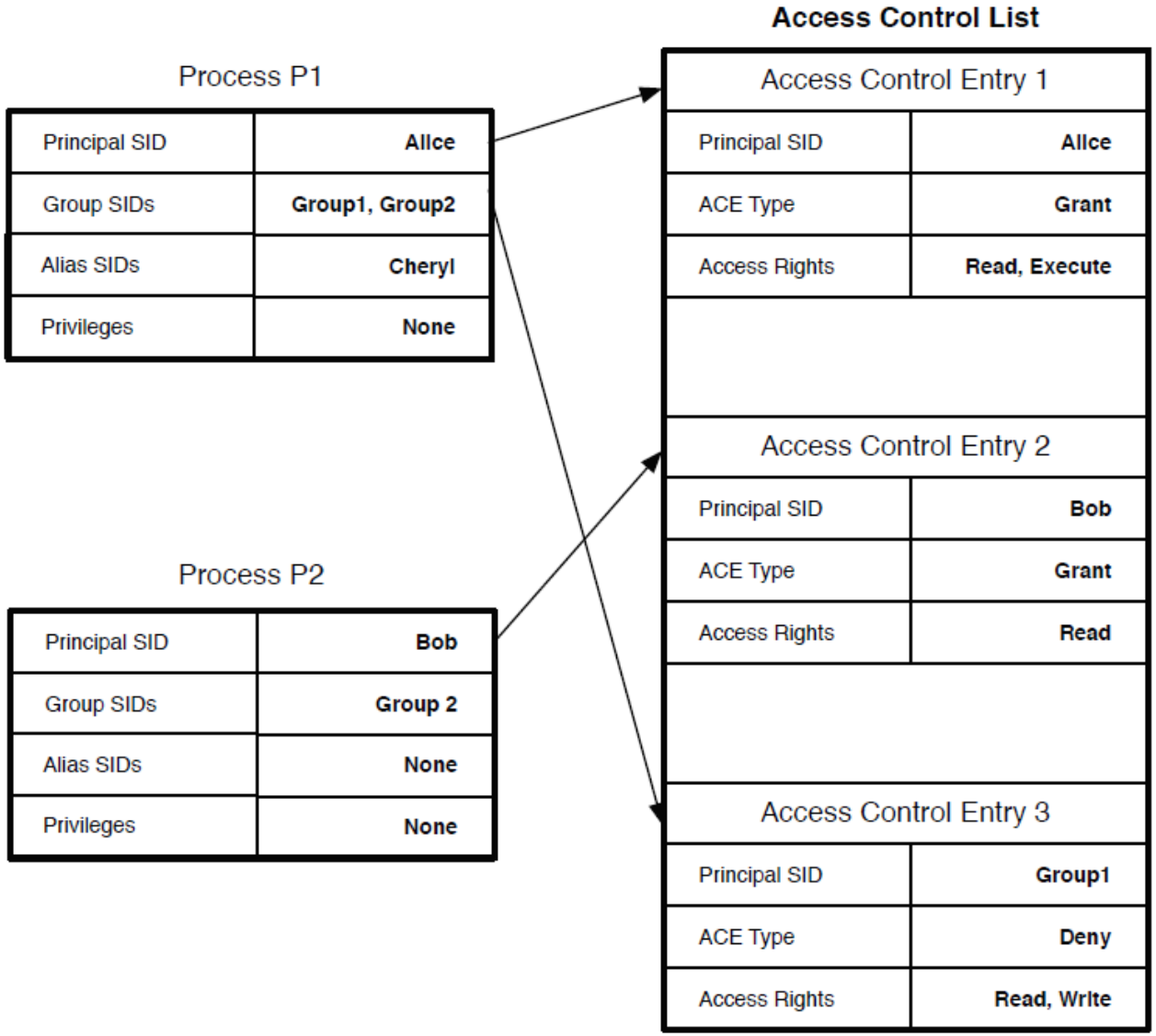
- Windows bắt nguồn từ MS-DOS. Đây là hệ điều hành rất hạn chế, không hỗ trợ đa nhiệm và không khai thác hết các tính năng của CPU x86
- Kể từ 2000, Windows phát triển dựa nhân của NT. Việc thiếu quan tâm đến vấn đề an toàn khiến cho hệ điều hành Windows (kể từ XP trở về trước) gặp phải những vấn đề nghiêm trọng về an toàn.
- Windows ban đầu được thiết kế hướng tới:
  - Người dùng máy vi tính PC riêng lẻ, không kết nối với mạng
  - Người dùng tự quản trị hệ thống của mình
  - Sử dụng mô hình mở và mềm dẻo

Các cơ chế đảm bảo an toàn

- Cơ chế ảo vệ của Windows NT cung cấp mô hình kiểm soát truy nhập theo kiểu tùy chọn để qý các trạng thái bảo vệ dán nhãn các đối tượng và dịch chuyển miền bảo vệ
- Cơ chế bảo vệ của Windows mềm dẻo và dễ biểu diễn.
- Các chủ thể của Windows cũng tương tự như Unix. Mỗi tiến trình được gán một thẻ (*token*) mô tả định danh của tiến trình.
  - Định danh bao gồm định danh an ninh (*Security Identifier Descriptor*) của người dùng, SID nhóm, bí danh SID (Alias) để hoạt động bằng định danh SID khác, danh sách các quyền

Các cơ chế đảm bảo an toàn

- Các đối tượng trong Windows có thể là nhiều kiểu dữ liệu khác với file
  - Các kiểu đối tượng mới được định nghĩa và thêm vào trong thư mục động (*active directory*)
  - Windows mô tả các kiểu thao tác khái quát mà đôi khi đối tượng không có
- Windows sử dụng danh sách kiểm soát truy nhập ACL để đảm bảo an toàn. ACL bao gồm tập các mục kiểm soát truy nhập ACE. Mỗi mục mô tả các tháo tác mà một SID có thể thực hiện trên đối tượng đó


Access Control List
Process P1
Principal SID
Alice
Group SIDs
Group1, Group2
Alias SIDs
Cheryl
Privileges
None
Process P2
Principal SID
Bob
Group SIDs
Group 2
Alias SIDs
None
Privileges
None
Access Control Entry 1
Principal SID
Alice
ACE Type
Grant
Access Rights
Read, Execute
Access Control Entry 2
Principal SID
Bob
ACE Type
Grant
Access Rights
Read
Access Control Entry 3
Principal SID
Group1
ACE Type
Deny
Access Rights
Read, Write

Cơ chế xác thực Windows

- Các yêu cầu xác thực được xử lý bởi Bộ tham chiếu an toàn (*Security Reference Monitor – SRM).* SRM là phần mềm chạy trong nhân và nhận các tham số đầu vào thẻ tiến trình, SID của đối tượng và tập thao tác, trả về kết quả của yêu cầu truy nhập (chấp nhận/từ chối)
- Bộ quản lý đối tượng đảm bảo việc đứng trung gian cho các yêu cầu truy nhập. Các bộ quản lý đối tượng chạy trong nhân song các bộ phận này là các thực thể độc lập với nhau.
  - Vì vậy cần phải chắc chắn với mỗi bộ phận quản lý đối tượng mới trung gian cho tất cả các thao tác và xác định quyền cần cho các thao tác này một cách chính xác.

Cơ chế xác thực Windows

- Windows cung cấp cách thức hạn chế quyền cho các tiến trình một cách mềm dẻo còn được gọi là ngữ cảnh hạn chế (restricted context). Quyền để tiến trình hoạt động được là giao của ngữ cảnh hạn chế và các quyền bình thường của tiến trình.