HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC

AN TOÀN HỆ ĐIỀU HÀNH

CHƯƠNG 1 – TỔNG QUAN VỀ AN TOÀN HỆ ĐIỀU HÀNH

Giảng viên: TS. Hoàng Xuân Dậu

Điện thoại/E-mail: dauhx@ptit.edu.vn

Bộ môn: An toàn thông tin - Khoa CNTT1

TÀI LIỆU THAM KHẢO

1. Phạm Hoàng Duy, *Bài giảng An toàn hệ điều hành*, Học viện Công nghệ BC-VT, 2017.
2. Andrew S. Tanenbaum, Herbert Bos, Modern Operating Systems 4th Edition, Pearson Education, Inc 2015.
3. Abraham Silberschatz, Peter B. Galvin, Greg Gagne, Operating System Concepts Essentials, John Wiley & Sons Inc., 2014.
4. Daniel Jackson, “Alloy: a lightweight object modelling notation,” ACM Transactionson Software Engineering and Methodology (TOSEM), vol. 11, no. 2, pp. 256–290, 2002.
5. Gustavo Duarte, CPU Rings, Privilege, and Protection, 2008.
6. Intel Co., Intel x64 and IA-32 Architectures Software Developer’s Manual, Intel Co. 2016.

TÀI LIỆU THAM KHẢO

7. Morrie Gasser, Building a secure computer system, Library of congress, ISBN 0-442-23022-2.
8. Mehedi Al Mamun, Operating Systems Security: Linux, LAP Lambert Acad. Publishing, 2011.
9. Seymour Bosworth. M.E. Kabay, Eric Whyne, Computer Security Handbook 6th Edition, John Wiley & Sons, 2014.
10. Trent Jaeger, Operating System Security, Morgan & Claypool Publishers, 2008.
11. Will Arthur & David Challener, A Practical Guide to TPM 2.0: Using the New Trusted Platform Module in the New Age of Security, 2015, Apress Media.

ĐÁNH GIÁ MÔN HỌC

- Các điểm thành phần:
  - Chuyên cần: 10%
  - Kiểm tra: 10%
  - Bài tập/thảo luận: 20%
  - Thi cuối kỳ: 60%

NỘI DUNG MÔN HỌC

1. Tổng quan về an toàn hệ điều hành
2. Các cơ chế an toàn phần cứng
3. An toàn các dịch vụ cơ bản của HĐH
4. Các mô hình an toàn HĐH
5. Đánh giá an toàn HĐH

NỘI DUNG CHƯƠNG 1

1. Giới thiệu an toàn HĐH
2. Các vấn đề về kiến trúc an toàn
3. Chính sách an toàn
4. Nhân an toàn

1.1 Giới thiệu an toàn HĐH

- Khái quát về Hệ điều hành
- Tổng quan về an toàn hệ điều hành

Khái quát về Hệ điều hành

- Hệ điều hành là gì?
- Một số họ HĐH thông dụng
- Các thành phần của HĐH
- Các chức năng của HĐH
- Vấn đề điều phối truy cập tài nguyên

Hệ điều hành là gì?

- Hệ điều hành (Operating system - OS) là một chương trình quản lý các tài nguyên phần cứng và phần mềm của một thiết bị tính toán (theo Wikipedia).
- Hệ điều hành cung cấp:
  - Môi trường cho các chương trình ứng dụng hoạt động
  - Giao diện giữa người dùng và phần cứng máy tính/ thiết bị tính toán
  - Một số các dịch vụ và ứng dụng cơ bản cho người dùng (tùy chọn).

Một số họ HĐH thông dụng

- DOS
  - MS-DOS
  - PC-DOS, FreeDOS
- Microsoft Windows
  - Windows 3.0, 3.1
  - Windows 95, 98, Me
  - Windows 2000
  - Windows NT 3, 4
  - Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10
  - Windows NT 3, 4 Server, Windows 2000 servers
  - Windows 2003, 2008 servers, Windows 2003, 2008 R2 servers
  - Windows 2012, 2012 R2 server, Windows 2016, 2019 servers

Một số họ HĐH thông dụng

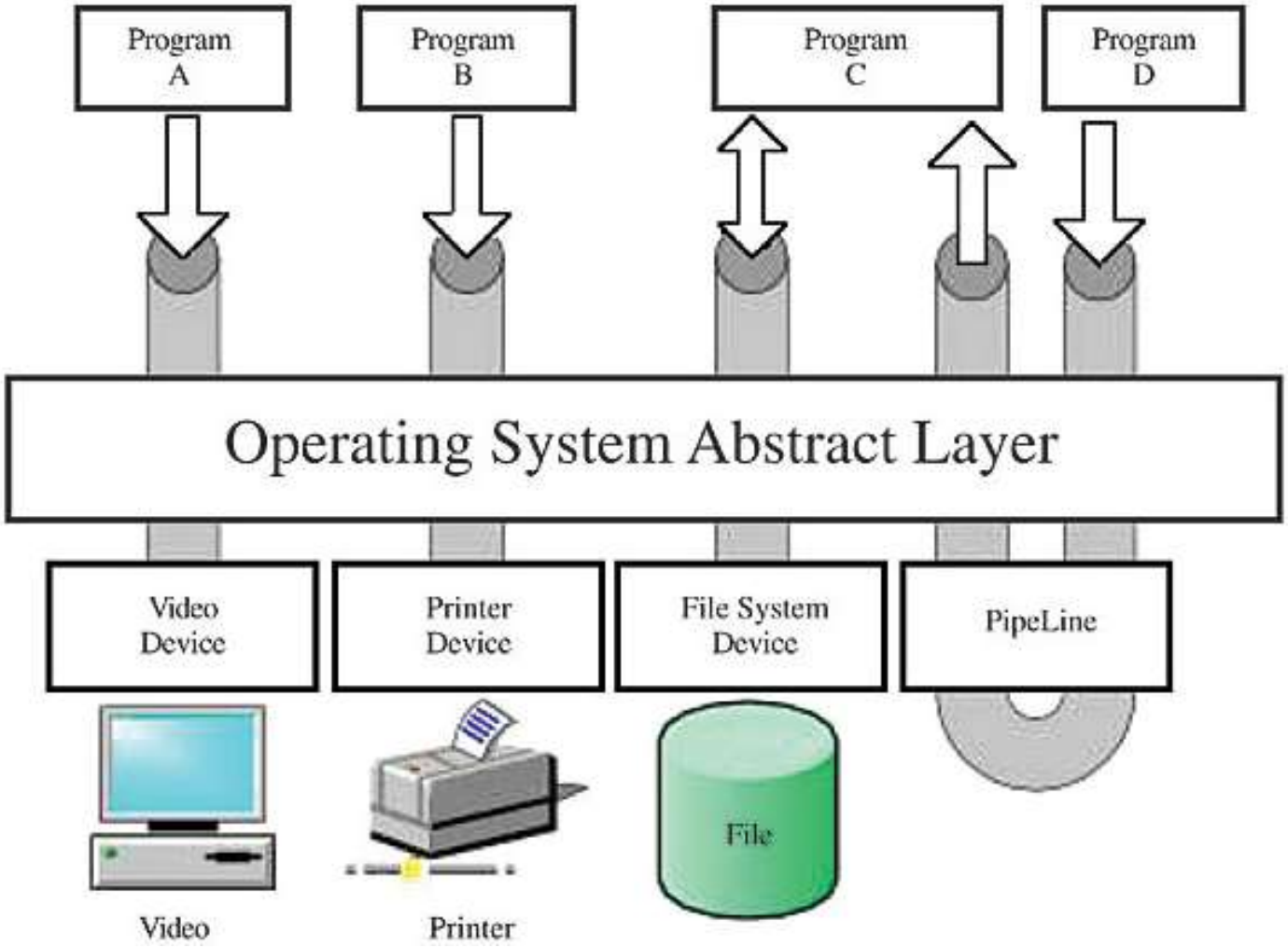
- Unix
  - System V
  - BSD, FreeBSD, OpenBSD
  - Solaris, OpenSolaris, illumos
  - HP Unix, IBM Unix
- Linux
  - Debian Linux: Ubuntu, Kloppix, Linux Mint,...
  - RedHat Linux: RedHat Enterprise, Fedora, CentOS, Oracle Linux,...
  - SUSE Linux, OpenSUSE.
- MacOS

Một số họ HĐH thông dụng

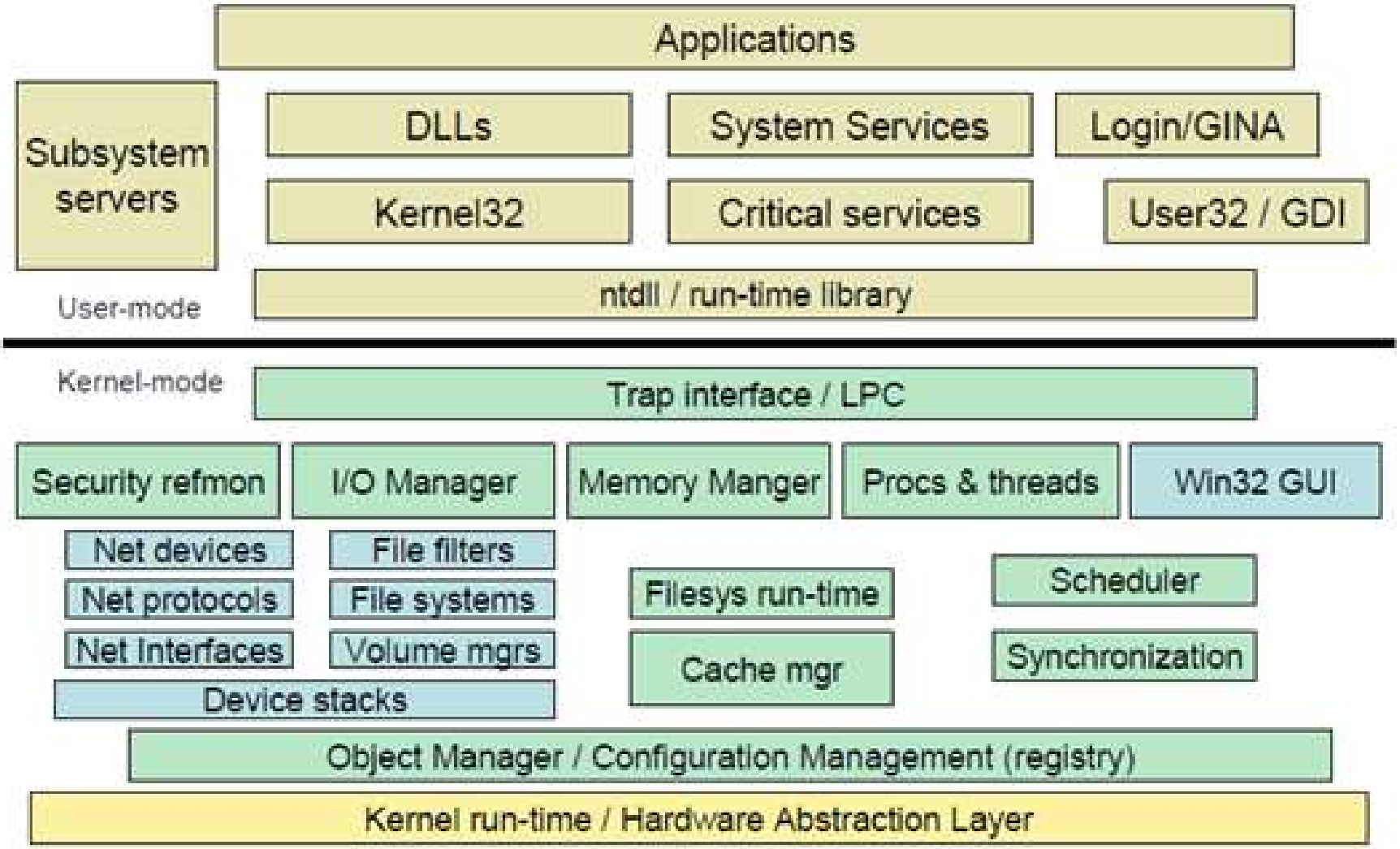
- HĐH di động, nhúng:
  - Apple iOS
  - Android
  - ChromeOS
  - Raspberry Pi OS,...
  - Cisco IOS
- HĐH ảo hoá:
  - VMWare ESX, ESXi
  - Microsoft Hyper-V
  - Oracle VM Server.

Các thành phần của HĐH

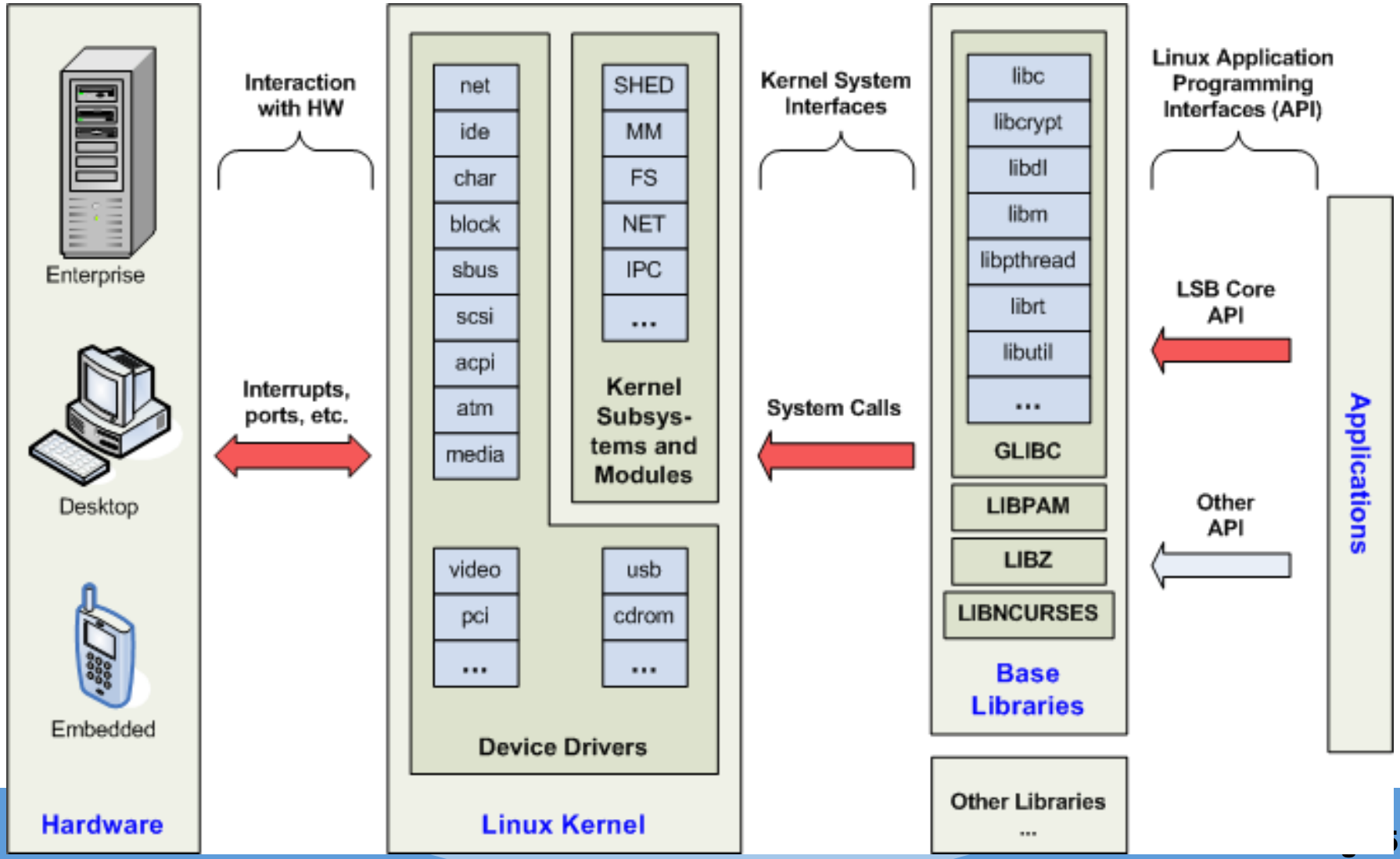
Các thành phần chính của hệ điều hành



Các thành phần chính của Microsoft Windows



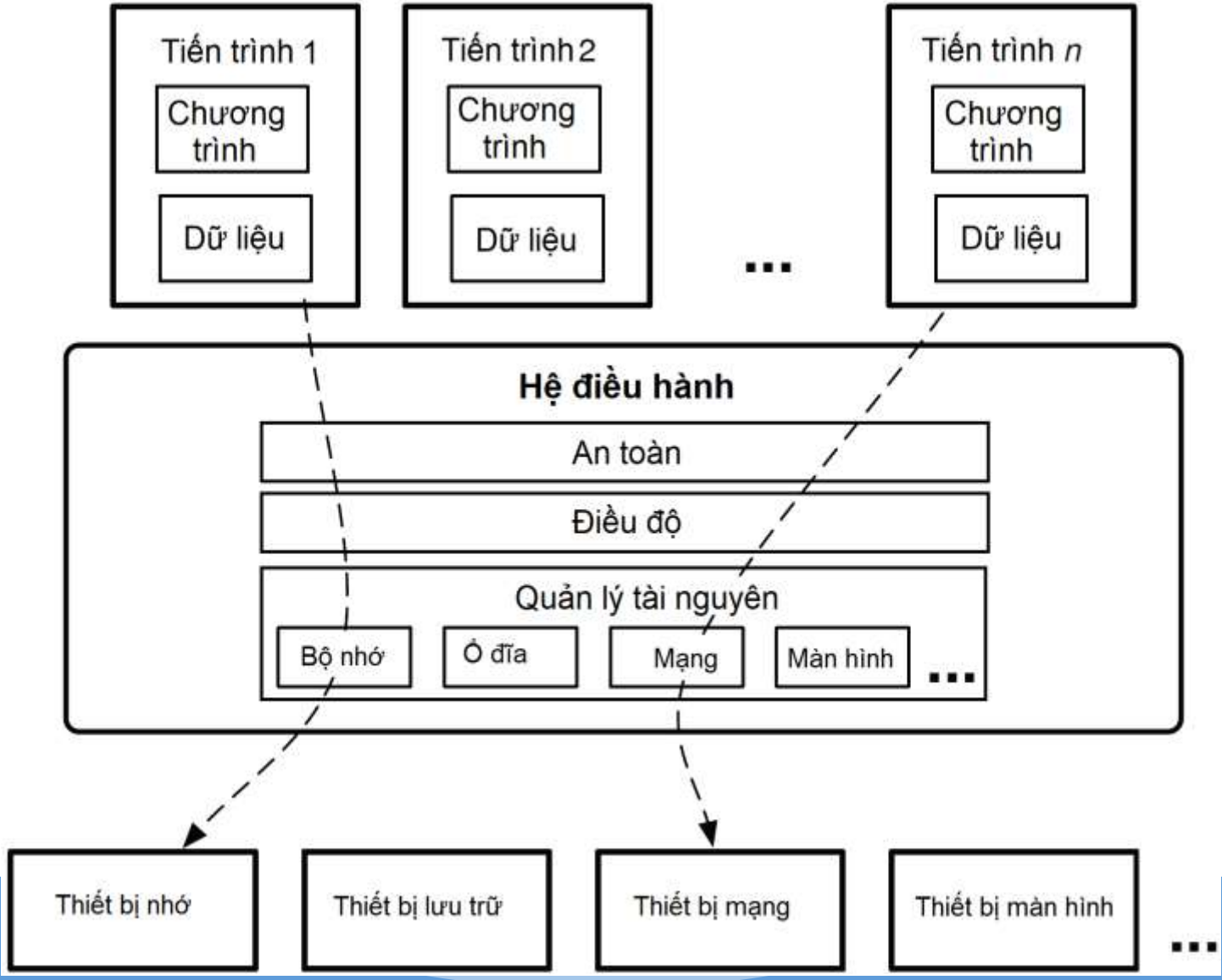
Các thành phần chính của HĐH dựa trên Linux



Các chức năng của HĐH

- Quản lý tiến trình (Process management)
- Quản lý bộ nhớ (Memory management)
- Quản lý đĩa và hệ thống files (Disk and file systems)
- Giao tiếp mạng (networking)
- Giao diện (đồ hoạ) người dùng
- Các trình điều khiển thiết bị (device drivers)
- Các tính năng an toàn và bảo mật (Security).

Vấn đề điều phối truy cập tài nguyên



Vấn đề điều phối truy cập tài nguyên

- Yêu cầu về điều phối truy cập tài nguyên:
  - Cung cấp cơ chế quản lý, sử dụng tài nguyên hiệu quả: xác định rõ phương thức cấp phát, giải phóng sử dụng tài nguyên
  - Cung cấp cơ chế điều độ giữa các chương trình người dùng đảm bảo việc sử dụng tài nguyên công bằng
  - Kiểm soát việc truy cập tới các tài nguyên sao cho chương trình người dùng không ảnh hưởng một cách vô tình hay cố ý tới chương trình khác
    - Đây chính là vấn đề đảm bảo an toàn cho các chương trình chạy trong hệ thống.

Tổng quan về an toàn hệ điều hành

- Khái niệm
- Mục tiêu an toàn
- Mô hình tin cậy
- Mô hình đe doạ
- Cơ chế an toàn.

Khái niệm an toàn hệ điều hành

- The techopedia.com: An toàn hệ điều hành (Operating System Security) là một tiến trình nhằm đảm bảo *tính bí mật*, *tính toàn vẹn* và *tính sẵn dùng* của hệ điều hành.
- An toàn hệ điều hành bao gồm:
  - Các bước hoặc biện pháp cụ thể được sử dụng để bảo vệ HĐH khỏi các mối đe dọa, vi rút, sâu, phần mềm độc hại hoặc sự xâm nhập của tin tặc từ xa.
  - Các kỹ thuật kiểm soát phòng ngừa, nhằm bảo vệ mọi tài sản máy tính có khả năng bị đánh cắp, chỉnh sửa hoặc xóa.

Khái niệm an toàn hệ điều hành

- Các yếu tố giúp xây dựng hệ điều hành an toàn bao gồm:
  - Mục tiêu an toàn
  - Mô hình tin cậy
  - Mô hình đe dọa
  - Cơ chế bảo vệ.

Mục tiêu an toàn

- Mục tiêu an toàn (security goals) xác định các thao tác có thể được thực hiện bởi hệ thống trong khi ngăn chặn các truy cập 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 thuộc tính an toàn HĐH:
  - Tính bí mật
  - Tính toàn vẹn
  - Tính sẵn dùng

Mục tiêu an toàn

- Truy cập 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/khách thể*** (file hay socket).
- Mô tả các thuộc tính an toàn HĐH:
  - Tính bí mật giới hạn các đối tượng có thể được truy cập;
  - Tính toàn vẹn hạn chế các đối tượng mà chủ thể có thể ghi/sửa đổi để đảm bảo thao tác được thực hiện 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 này có thể làm cạn kiệt các tài nguyên đó.

Mục tiêu an toàn

- Mục tiêu an toàn có thể được xây dựng dựa trên:
  - Tính bí mật: Như thực hiện trong mô hình bảo mật Bell-LaPadula (hạn chế rò rỉ thông tin thông qua biện pháp kiểm soát truy cập bắt buộc).
  - Các chức năng thông qua nguyên tắc “Đặc quyền tối thiểu”:
    - Các chương trình chỉ được thực hiện các thao tác cần thiết cho hoạt động của chúng.
    - Tuy nhiên, hạn chế chức năng không làm tăng tính an toàn của hệ thống mà chỉ làm giảm khả năng bị tấn công.

Mô hình tin cậy

- Mô hình tin cậy (Trust model) của hệ thống định nghĩa tập phần mềm và dữ liệu mà hệ thống sử dụng để đảm bảo thực hiện chính xác các mục tiêu an toàn của hệ thống.
- Các phần mềm được sử dụng trong mô hình tin cậy được gọi là *phần mềm tin cậy*.
- Các phần mềm tin cậy bao gồm:
  - Phần mềm xác định các yêu cầu an toàn của hệ thống và;
  - Phần mềm đảm bảo thực thi các yêu cầu này.

Mô hình tin cậy

- Ví dụ phần mềm tin cậy: các phần mềm đăng nhập, xác thực người dùng, truy cập tài nguyên.
- Người phát triển hệ điều hành an toàn phải chứng minh hệ thống của mình hỗ trợ mô hình tin cậy:
  - Các phần mềm tin cậy phải thực hiện toàn bộ các thao tác nhạy cảm đảm bảo 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 không nằm trong các phần mềm tin cậy;
    - Tính toàn vẹn của các phần mềm tin cậy phải được bảo vệ khỏi các mối đe dọa tới hệ thống;
    - Nếu một phần mềm bị xâm nhập thì phần mềm đó không được tin cậy.

Mô hình đe doạ

- Mô hình đe dọa (Threat model) 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 mối đe doạ trong mô hình đe dọa.
  - Chương trình người dùng có thể không tin cậy song hệ thống có thể hạn chế việc nó truy cập tới dữ liệu nhạy cảm của hệ thống nhằm hạn chế rò rỉ hay sửa đổi các thông tin này.

Mô hình đe doạ

- Mục tiêu an toàn cần được đảm bảo bất kể hành vi hay hoạt động của các chương trình người dùng.
- Người phát triển hệ thống phải:
  - Nhận biết được các mối đe dọa;
  - Đánh giá ảnh hưởng của các mối đe doạ lên an toàn hệ thống, và;
  - Cung cấp biện pháp phòng ngừa hiệu quả những đe dọa này.

Cơ chế bảo vệ

- Các cơ chế bảo vệ là các cơ chế kiểm soát thực thi truy cập đến các tài nguyên hệ thống;
  - Cụ thể là cơ chế bảo vệ, kiểm soát các chủ thể (subject) thực hiện các thao tác (operation) lên các đối tượng (object) trong hệ thống.
- Các vấn đề liên quan đến hệ thống được bảo vệ:
  - *Trạng thái bảo vệ* mô tả các thao tác mà các chủ thể của hệ thống có thể thực hiện lên các đối tượng trong hệ thống;
  - Tập các thao tác lên trạng thái bảo vệ làm thay đổi các trạng thái này;
  - Hệ thống bảo vệ xác định các yêu cầu an ninh của hệ điều hành và thực hiện việc quản lý các yêu cầu này.

Cơ chế bảo vệ

- Một số cơ chế, biện pháp bảo vệ, biểu diễn trạng thái bảo vệ:
  - Ma trận kiểm soát truy cập (Access Control Matrix – ACM);
  - Danh sách kiểm soát truy cập (Access Control List – ACL);
  - Hệ thống bảo vệ bắt buộc.

Ma trận kiểm soát truy cập

- Các trạng thái bảo vệ của hệ thống được biểu diễn bằng ma trận truy nhập được định nghĩa sử dụng:
  - Tập các chủ thể S (User, Process,...)
  - Tập các đối tượng O (File, Folder, Process,...)
  - Các thao tác được phép của chủ thể lên đối tượng Op (Read, Write,...)

  - Ma trận kiểm soát truy cập với hai tiến trình

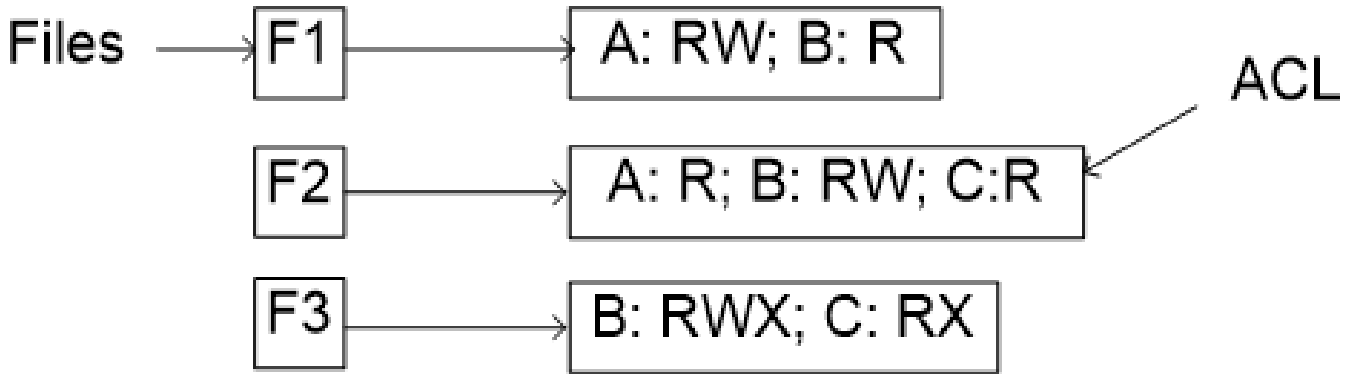
	File 1	File 2	File 3	Process 1	Process 2
Process 1	Read	Read, Write	Read, Write	Read	-
Process 2	-	Read	Read, Write	-	Read

Ma trận kiểm soát truy cập

- Ma trận kiểm soát truy cập cũng có thể được sử dụng để mô tả *miền bảo vệ* (*protection domain*);
- Miền bảo vệ gồm:
  - Tập các đối tượng (tài nguyên) mà tiến trình có thể truy cập và;
  - Các thao tác mà tiến trình có thể sử dụng để truy cập tới các đối tượng này.

Danh sách kiểm soát truy cập

- Ma trận kiểm soát truy cập có thể là ma trận thưa với nhiều ô không có nội dung:
  - Chủ thể không có quyền truy cập đến đối tượng.
- Danh sách kiểm soát truy cập được sử dụng để tăng hiệu quả sử dụng bộ nhớ;
  - Ví dụ về danh sách kiểm soát truy cập với A, B, C là các chủ thể và F1, F2 và F3 là các file (đối tượng).



Hệ thống bảo vệ bắt buộc

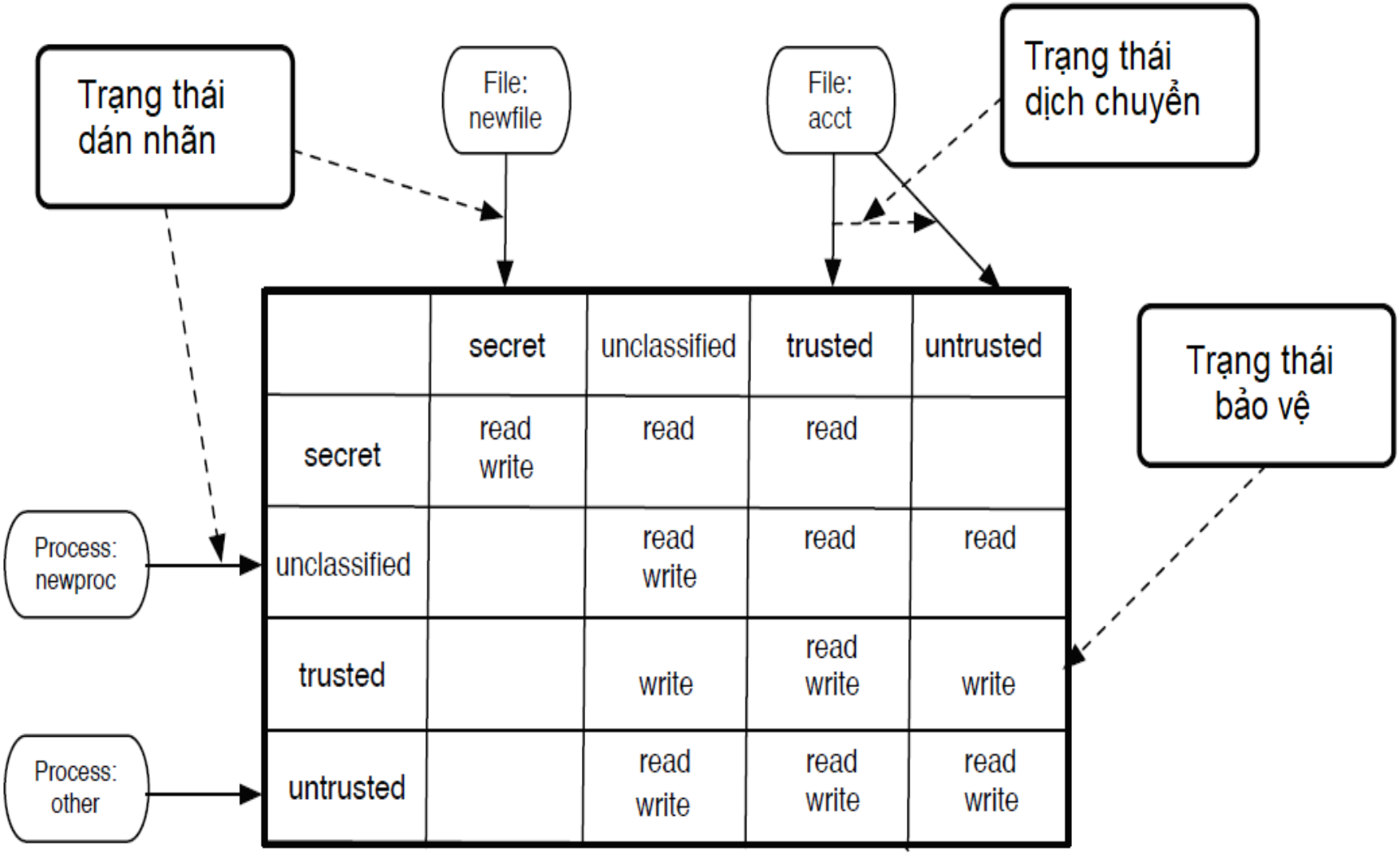
- Mô hình bảo vệ sử dụng ma trận kiểm soát truy cập làm nảy sinh vấn đề với an toàn hệ điều hành: Các tiến trình không tin cậy có thể xâm nhập hệ thống bảo vệ;
  - Lợi dụng các thao tác lên trạng thái bảo vệ, tiến trình người dùng không tin cậy có thể sửa đổi ma trận truy nhập bằng cách:
    - Thêm chủ thể, đối tượng mới, hay
    - Thực hiện các thao tác trên các ô của ma trận.
- Bài toán an toàn hệ thống yêu cầu không cho phép mọi truy cập trái phép xảy ra.

==> Cần triển khai *Hệ thống bảo vệ bắt buộc*.

Hệ thống bảo vệ bắt buộc

- Hệ thống bảo vệ bắt buộc là hệ thống chỉ có thể được sửa đổi bởi người quản trị tin cậy thông qua phần mềm tin cậy;
- Hệ thống này gồm các trạng thái:
  - *Trạng thái bảo vệ bắt buộc* là trạng thái mà các chủ thể và các đối tượng được biểu diễn bằng các nhãn. Các trạng thái mô tả các thao tác mà các nhãn chủ thể có thể thực hiện lên các nhãn đối tượng.
  - *Trạng thái dán nhãn* để ánh xạ các tiến trình và các đối tượng tài nguyên hệ thống tới các nhãn
  - *Trạng thái dịch chuyển* mô tả cách thức hợp lệ mà các tiến trình và các đối tượng có thể được dán nhãn lại (thay đổi nhãn).

Hệ thống bảo vệ bắt buộc



	secret	unclassified	trusted	untrusted
secret	read write	read	read	
unclassified		read write	read	read
trusted		write	read write	write
untrusted		read write	read write	read write

Hệ thống bảo vệ bắt buộc

- Trong hệ điều hành an toàn, nhãn là các định danh khái quát;
- Việc gán quyền cho nhãn xác định ngữ nghĩa an toàn của chúng;
- Các nhãn này chống lại việc xâm nhập nhờ:
  - Tập các nhãn này được xây dựng bởi người quản trị tin cậy sử dụng phần mềm tin cậy;
  - Tập các nhãn không thay đổi được bởi các tiến trình không tin cậy của người dùng.

Hệ thống bảo vệ bắt buộc

- Người quản trị tin cậy xây dựng các nhãn của ma trận kiểm soát truy cập và xác lập các thao tác mà chủ thể với nhãn nhất định được phép thực hiện lên trên đối tượng với nhãn cho trước;
  - Hệ thống này cho phép miễn nhiễm với các tiến trình không tin cậy.
  - Điều này là vì tập các nhãn không thể thay đổi qua việc thực thi của các tiến trình người dùng;
    - Có thể chứng minh được các mục tiêu an toàn được thực thi qua ma trận và trong suốt quá trình hoạt động của hệ thống.

Hệ thống bảo vệ bắt buộc

- Hệ điều hành an toàn cần có khả năng gán các nhãn cho các chủ thể (tiến trình) và đối tượng được tạo ra trong quá trình hoạt động và thậm chí cho phép thay đổi nhãn;
  - Trạng thái dán nhãn chỉ là quá trình gán các nhãn cho chủ thể và đối tượng mới.
- Hệ thống bảo vệ bắt buộc trên Slide 36:
  - Khi *newfile* được tạo ra cần gán cho nó một nhãn trong trạng thái an toàn cụ thể là nhãn *secret*.
  - Tiến trình *newproc* được gán nhãn *unclassified*.
  - Ma trận truy cập cho thấy tiến trình mới *newproc* không có quyền truy cập vào file *newfile* mới được tạo ra.

Hệ thống bảo vệ bắt buộc

- Trạng thái dịch chuyển cho phép hệ điều hành an toàn thay đổi nhãn của tiến trình (chủ thể) hay tài nguyên hệ thống (đối tượng):
  - Với tiến trình, việc này làm thay đổi miền bảo vệ hay các tài nguyên được phép sử dụng.
    - Việc này cần thiết khi xét đến khả năng một tiến trình kích hoạt chương trình khác chạy.
    - Nhãn gắn với tiến trình cần thay đổi thể hiện các yêu cầu truy cập hay tin cậy trong môi trường (miền) mới.
- Với hệ điều hành an toàn, trạng thái dịch chuyển phải được xác định bởi người quản trị tin cậy và không bị thay đổi trong quá trình thực thi hệ thống.

1.2 Các vấn đề về kiến trúc an toàn

- Đặt vấn đề
- Một số nguyên tắc kiến trúc an toàn

Kiến trúc an toàn - Đặt vấn đề

- Xây dựng hệ thống máy tính cần phải cân đối rất nhiều các yêu cầu như tính năng, độ linh hoạt, hiệu năng, tính dễ dùng và chi phí.
- An toàn đơn giản là một dạng yêu cầu khác và nếu có xung đột các tính năng, an toàn phải cân đối với các tính năng khác tùy theo mức độ quan trọng với hệ thống.

Kiến trúc an toàn - Đặt vấn đề

- Kiến trúc an toàn là mô tả chi tiết toàn bộ các khía cạnh của hệ thống liên quan đến vấn đề an toàn cùng với các nguyên tắc thiết kế;
  - Kiến trúc an toàn tốt giống như thiết kế tổng thể mô tả ở mức khái quát quan hệ giữa các bộ phận then chốt theo cách mà chúng phải thỏa mãn các yêu cầu về an toàn.
  - Kiến trúc an toàn cần mô tả các chi tiết của quá trình xây dựng hệ thống mà qua đó các yêu cầu an toàn được đảm bảo.

Kiến trúc an toàn - Đặt vấn đề

- Kiến trúc an toàn là mô tả chi tiết toàn bộ các khía cạnh của hệ thống liên quan đến vấn đề an toàn cùng với các nguyên tắc thiết kế;
  - Kiến trúc an toàn tốt giống như thiết kế tổng thể mô tả ở mức khái quát quan hệ giữa các bộ phận then chốt theo cách mà chúng phải thỏa mãn các yêu cầu về an toàn.
  - Kiến trúc an toàn cần mô tả các chi tiết của quá trình xây dựng hệ thống mà qua đó các yêu cầu an toàn được đảm bảo.

Kiến trúc an toàn - Đặt vấn đề

- Tại thời điểm bắt đầu xây dựng hệ thống, kiến trúc an toàn có thể được mô tả bằng các vấn đề an toàn ở mức cao:
  - Chính sách an toàn, mức độ đảm bảo mong muốn
  - Tác động của an toàn lên quá trình xây dựng hệ thống, và
  - Các nguyên tắc hướng dẫn chung.
- Ở các giai đoạn tiếp theo:
  - Kiến trúc an toàn cần phản ánh cấu trúc của hệ thống và mức độ chi tiết tăng dần theo các bước thiết kế;
  - Kiến trúc an toàn cần đi trước một bước để định hướng cho việc hoàn thành công việc thiết kế.

Một số nguyên tắc kiến trúc an toàn

1. Xem xét vấn đề an toàn ngay từ đầu
2. Lường trước các yêu cầu về an toàn
3. Giảm thiểu và cách ly các biện pháp an toàn
4. Thực hiện quyền tối thiểu
5. Giữ các tính năng an ninh thân thiện
6. An toàn không dựa trên tính bí mật

Xem xét vấn đề an toàn ngay từ đầu

- Coi trọng vấn đề an toàn ngang bằng như các tính năng vận hành của hệ thống và phải được tích hợp đầy đủ vào hệ thống;
- Việc thiếu quan tâm đến vấn đề an toàn sẽ dễ dẫn đến việc không kiểm soát được các phí tổn để bổ sung các tính năng an toàn sau này.

Lường trước các yêu cầu về an toàn

- Kiến trúc an toàn cần có tầm nhìn xa đề cập tới các tính năng an toàn tiềm năng thậm chí chưa có kế hoạch sử dụng ngay lập tức.
  - Việc này làm tăng chi phí một chút cho việc nâng cao tính an toàn.
- Điểm then chốt cho việc gắn kết hợp lý các tính năng an toàn tương lai là việc hiểu rõ các yêu cầu về an toàn của hệ thống máy tính.
  - Hơn thế cần phải mô tả một cách tường minh nhất các yêu cầu trong tương lai này trong kiến trúc an toàn.

Lường trước các yêu cầu về an toàn

- Lường trước các yêu cầu an toàn không chỉ ảnh hưởng đến mức độ cần thiết làm hệ thống an toàn hơn trong tương lai mà còn giúp xác định liệu tính an toàn của hệ thống có thể được nâng cao hay không.
- Vấn đề khác là chính sách an toàn
  - Thay đổi trong chính sách an toàn có thể dẫn đến hậu quả tai hại với các ứng dụng đang hoạt động tốt mà nay có thể xung đột với chính sách mới.

Giảm thiểu và cách ly các biện pháp an toàn

- Để đạt được độ tin cậy cao về an toàn của hệ thống, người thiết kế cần giảm thiểu kích cỡ và độ phức tạp của các phần liên quan tới an toàn của thiết kế.
  - Một lý do dẫn đến hệ điều hành không an toàn là kích cỡ quá lớn của chúng làm cho khó kiểm soát tổng thể hệ thống.
  - Vì vậy, ngay cả với hệ thống phức tạp, phần cốt lõi (liên quan đến an toàn) nên có kích thước nhỏ và được định nghĩa rõ ràng.

Giảm thiểu và cách ly các biện pháp an toàn

- Điểm then chốt để giảm thiểu các bộ phận liên quan tới an toàn của HĐH là chỉ dùng số ít các cơ chế thực thi an toàn.
  - Như vậy, bắt buộc các hành động liên quan tới an toàn được giữ trong một số ít phần cách ly.
  - Thực tế với hệ điều hành rất khó đạt được điều này do vấn đề an toàn liên quan tới rất nhiều chức năng khác nhau của hệ thống như quản lý file hệ thống, quản lý bộ nhớ...
  - Ví dụ như xử lý truy nhập file bằng mật khẩu, quyền truy nhập, truy nhập cơ sở dữ liệu...

Giảm thiểu và cách ly các biện pháp an toàn

- Khi các cơ chế an toàn đơn giản, dễ nhận biết và được cách ly thì dễ dàng triển khai các cơ chế bảo vệ bổ sung để tránh các thiệt hại do lỗi phát sinh bởi các phần khác của hệ thống.
  - Các đoạn mã liên quan đến an toàn có thể được bảo vệ chống ghi để không bị sửa đổi.

Thực hiện quyền tối thiểu

- Các chủ thể (người dùng hay tiến trình) cần được cấp quyền không hơn mức cần thiết để thực hiện công việc – gọi là *quyền tối thiểu*.
  - Như vậy, với *quyền tối thiểu* thiệt hại do lỗi hay phần mềm xấu được giới hạn.
- Quyền được cấp có thể được thể hiện ở:
  - Các cơ chế phần cứng hạn chế việc sử dụng các câu lệnh đặc biệt (lệnh vào ra) và truy cập tới các vùng ô nhớ.
  - Các cơ chế phần mềm, như trong hệ điều hành, cho phép chương trình người dùng qua các biện pháp kiểm soát truy cập hay thực thi các chức năng hệ thống.

Thực hiện quyền tối thiểu

- Quyền tối thiểu còn thể hiện trong nguyên tắc phát triển hệ thống.
  - Như bằng việc đặt ra các tiêu chuẩn lập trình hạn chế các truy cập tới các dữ liệu toàn cục (global data), như vậy giảm khả năng lỗi từ vùng này tác động tới vùng khác.
- Quyền tối thiểu thể hiện trong việc quản trị người dùng và hệ thống.
  - Người dùng và người quản trị không nên được cấp truy cập nhiều hơn với mức cần thiết để thực hiện công việc của họ.

Giữ các tính năng an ninh thân thiện

- Các cơ chế an toàn không được ảnh hưởng tới người dùng tuân thủ quy định:
  - Cơ chế an toàn phải trong suốt với người dùng bình thường.
  - Việc can thiệp vào công việc hàng ngày làm giảm năng suất và khiến người dùng tìm cách bỏ qua các cơ chế an toàn.
- Thuận tiện cho người dùng để cấp quyền truy cập:
  - Người dùng cần được đảm bảo cung cấp đủ truy cập khi cần thiết và tránh các thủ tục rườm rà, phức tạp.
- Thuận tiện cho người dùng để hạn chế truy cập:
  - Nhằm hạn chế các rủi ro do vô tình khi quản lý và cấp phát các quyền truy cập cho người dùng.

An toàn không dựa trên tính bí mật

- Ngoại trừ việc quản lý mật khẩu, đích chính của kiến trúc an toàn tránh phụ thuộc vào tính bí mật để đảm bảo an toàn.
  - Việc giả định người dùng không thể bẻ khóa hệ thống vì không biết mã nguồn hay tài liệu về hệ thống là không an toàn.
  - Việc công khai mã nguồn hệ thống có khả năng cải thiện tính an toàn nhờ có số lượng người dùng lớn hơn giúp phát hiện và sửa chữa các lỗi, khiếm khuyết.

1.3 Chính sách an toàn

- *Chính sách an toàn* (Security policy) mô tả các kiểm soát, hành động, và quy trình cần được thực hiện cho hệ thống thông tin.
- Các chính sách cần đề cập và xử lý các mối đe dọa tới hệ thống bao gồm cả con người, thông tin và tài sản cụ thể.
- Việc truy cập các tài nguyên hệ thống cũng như xử lý chúng chịu sự ràng buộc và hạn chế thể hiện trong các chính sách của cơ quan/tổ chức và do người quản trị thực thi thông qua các công cụ quản trị của hệ thống.

Chính sách an toàn

- Sự thành công của các biện pháp bảo vệ tài nguyên của hệ thống tùy thuộc vào:
  - Các chính sách an toàn được xây dựng và
  - Thái độ quản lý với việc đảm bảo an toàn thông tin.
- Các loại chính sách ATTT:
  - *Chính sách chung* dùng để mô tả và xây dựng định hướng và tầm nhìn chung. Nói cách khác, chính sách này xác lập mong muốn về việc bảo vệ các tài sản thông tin.
  - *Chính sách cho ứng dụng cụ thể* hướng tới các ứng dụng cụ thể sau khi đã định hình được các yêu cầu cũng như biện pháp đảm bảo an toàn cần thiết.

Chính sách an toàn

- Từ góc độ vận hành, các chính sách an toàn cần được chuyển hóa thành các luật trong các bộ phận thực hiện chức năng kiểm soát truy cập tới các tài nguyên của hệ thống như hệ thống file, mạng, bộ nhớ...
- Mặt khác, bộ phận kiểm soát cần thiết đánh giá và kiểm chứng các chính sách này có xung đột với nhau, hay vi phạm các nguyên tắc an toàn chung của hệ thống hay không?

1.4 Nhân an toàn

- Khái quát về nhân an toàn
- Các yêu cầu an toàn
- Giám sát tham chiếu
- Định hướng xây dựng nhân an toàn

Khái quát về nhân an toàn

- Nhân an toàn là phần cơ sở nền tảng có thể kiểm chứng được của hệ điều hành để đảm bảo an toàn cho hệ thống;
- Nhân an toàn được xác định bằng phần cứng và phần mềm cần thiết để thực thi các chính sách của hệ thống;
- Các quyết định truy cập được mô tả bởi các chính sách dựa trên các thông tin trong cơ sở dữ liệu về kiểm soát truy cập.

Khái quát về nhân an toàn

- CSDL về kiểm soát truy cập:
  - Thể hiện trạng thái an toàn của hệ thống và
  - Chứa các thông tin như quyền truy cập và các thuộc tính an ninh.
  - Có thể được chỉnh sửa/cập nhật do các chủ thể và đối tượng được tạo và xóa cũng như quyền truy cập của chúng được sửa đổi.
  - Yêu cầu tối quan trọng là *giám sát việc tham chiếu* của từng thao tác từ chủ thể tới đối tượng.

Các yêu cầu an toàn

- Hệ điều hành an toàn là hệ điều hành mà việc thực thi truy cập thỏa mãn các yêu cầu của *giám sát tham chiếu*.
- *Bộ giám sát tham chiếu* xác định các thuộc tính cần và đủ của bất kỳ hệ thống nào để thực thi hệ thống bảo vệ một cách an toàn.

Các yêu cầu an toàn

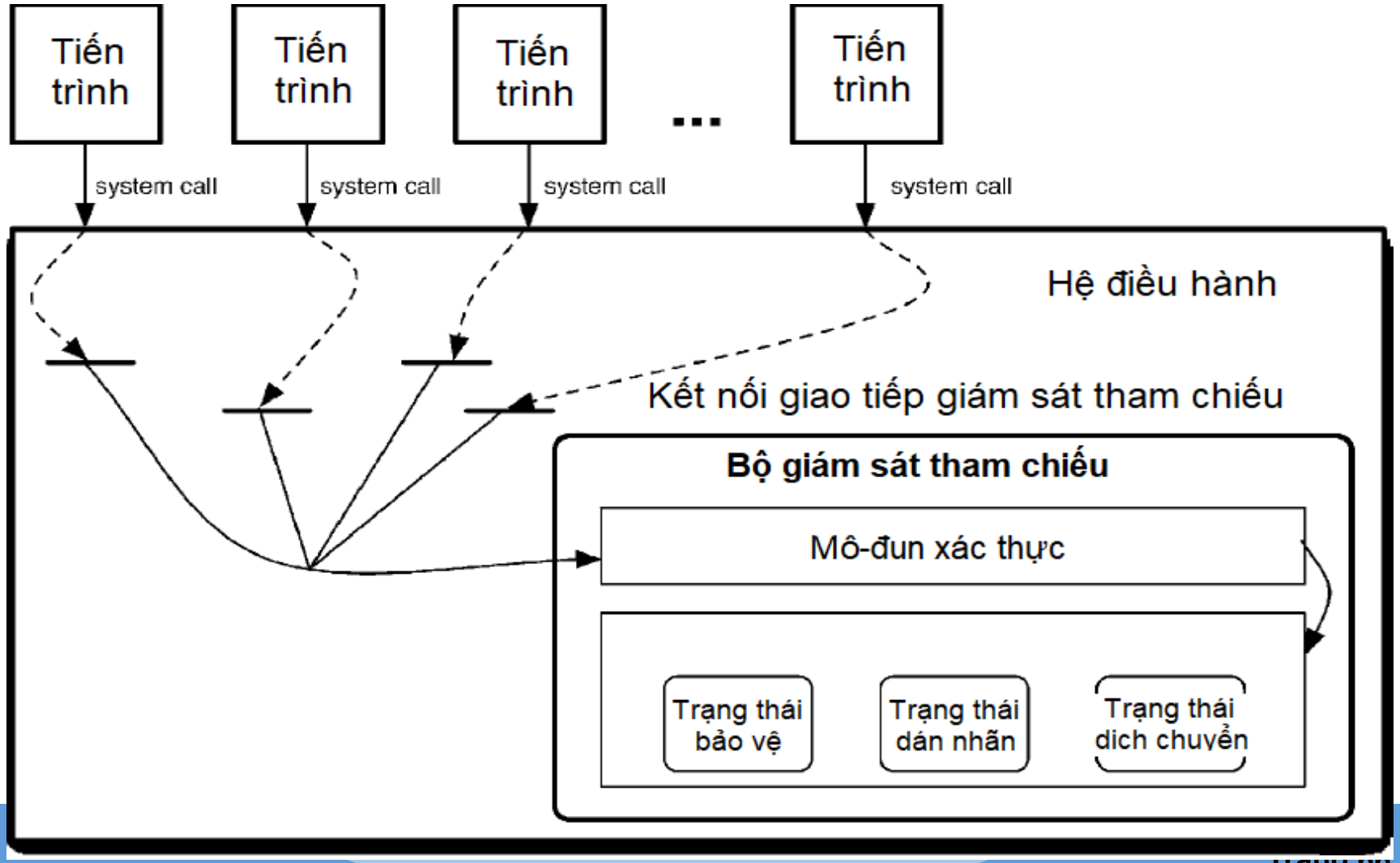
- Các thuộc tính của bộ giám sát tham chiếu đảm bảo yêu cầu an toàn:
  - Ngăn chặn hoàn toàn: hệ thống đảm bảo cơ chế thực thi truy cập ngăn chặn toàn bộ các thao tác nhạy cảm với an ninh;
  - Chống xâm nhập: hệ thống đảm bảo có chế thực thi truy cập, kể cả hệ thống bảo vệ, không thể bị sửa đổi bởi các tiến trình (chương trình) không tin cậy;
  - Xác minh được:
    - Cơ chế thực thi truy cập, kể cả hệ thống bảo vệ, phải đủ nhỏ để có thể kiểm tra và phân tích;
    - Tính đúng đắn của cơ chế thực thi truy cập có thể được đảm bảo.

  ==> Phải có khả năng chứng minh hệ thống thực thi các mục tiêu an toàn một cách đúng đắn.

Giám sát tham chiếu

- Giám sát tham chiếu (Reference Monitor) là cơ chế thực thi truy cập cổ điển:
  - Khi có yêu cầu truy cập, bộ phận giám sát trả lời chấp nhận hay từ chối truy nhập dựa vào chính sách truy cập bên trong bộ giám sát.
- Bộ giám sát tham chiếu bao gồm 3 phần:
  - *Giao tiếp* xác định vị trí mà mô-đun xác thực được gọi;
  - *Mô-đun xác thực* xác định các truy vấn chính xác cần được gửi tới kho chính sách;
  - *Kho chính sách* trả lời các truy vấn dựa trên hệ thống bảo vệ mà nó duy trì.

Tương tác giữa tiến trình và bộ giám sát tham chiếu



Giám sát tham chiếu – Giao tiếp

- Giao tiếp xác định nơi mà các truy vấn/yêu cầu hệ thống bảo vệ được gửi tới bộ giám sát.
- Về cơ bản tất cả các thao tác nhạy cảm về an ninh được xác thực bởi cơ chế thực thi truy cập.
  - Các thao tác nhạy cảm là các thao tác thực hiện trên một đối tượng cụ thể (file, socket...) mà các thao tác này có thể xâm phạm các yêu cầu an ninh của hệ thống.

Giám sát tham chiếu – Mô-đun xác thực

- Mô-đun xác thực là bộ phận cốt lõi của bộ giám sát tham chiếu.
- Mô-đun xác thực nhận các tham số đầu vào từ giao tiếp như định danh tiến trình, tham chiếu đối tượng, tên lời gọi hệ thống ... và thực hiện truy vấn kho chính sách để trả lời về tính hợp lệ của truy vấn từ giao tiếp.
  - Thách thức của mô-đun này là ánh xạ các định danh của tiến trình thành các nhãn chủ thể, các tham chiếu đối tượng thành các nhãn đối tượng và hoạt động cụ thể được chấp thuận.
  - Ví dụ như với yêu cầu mở file *open:*
    - Mô-đun này cần có nhãn chủ thể sinh yêu cầu, nhãn của đối tượng thư mục và trạng thái bảo vệ của yêu cầu (đọc hay ghi).

Giám sát tham chiếu – Kho chính sách

- *Kho chính sách* là cơ sở dữ liệu gồm:
  - Các trạng thái bảo vệ
  - Các nhãn trạng thái và
  - Các trạng thái dịch chuyển.
- Các câu truy vấn có cấu trúc {*nhãn chủ thể, nhãn đối tượng, tập thao tác*} và trả về kết quả nhị phân (*hợp lệ/không hợp lệ*).
- Các truy vấn về việc dịch chuyển có dạng {*nhãn chủ thể, nhãn đối tượng, tập thao tác, tài nguyên*}.
  - Các tài nguyên có thể là các thực thể hoạt động như bộ xử lý hay thụ động như file.

Đính hướng xây dựng nhân an toàn

- Nhân an toàn là cách tiếp cận dựa trên giám sát tham chiếu có kết hợp phần cứng và phần mềm để đảm bảo thực thi các chính sách an toàn của hệ thống.
- Giám sát tham chiếu đảm bảo việc giám sát mỗi truy cập từ các chủ thể khác nhau của hệ thống tới từng tài nguyên/đối tượng.
- Mục tiêu chính của hầu hết các nhân an toàn là kiểm chứng việc triển khai ở mức độ mã nguồn thỏa mãn các yêu cầu cầu của nhân an toàn.
  - Việc này dẫn đến ứng dụng các phương pháp chính tắc hay bán chính tắc để kiểm chứng.

Đính hướng xây dựng nhân an toàn

- Nhân an toàn – thành phần chịu trách nhiệm về an toàn thường có kích thước nhỏ trong HĐH nhiều tính năng có kích thước lớn.
- HĐH cần được cấu trúc sao cho thành phần liên quan đến an toàn được tách ra thành phần nhân an toàn/tin cậy.
  - Phần nhân an toàn chịu trách nhiệm giám sát và thực thi các chính sách an toàn lên các hoạt động của HĐH cũng như người dùng.
  - Phần nhân phải được bảo vệ một cách thích đáng (chống xâm nhập) và không thể bỏ qua các kiểm tra truy cập của nhân.
  - Phần nhân cần phải nhỏ nhất có thể được để có thể xác minh tính đúng đắn của nó một cách dễ dàng.

Đính hướng xây dựng nhân an toàn

- Nhìn chung, nhân an toàn giống HĐH sơ khai.
  - Nhân an toàn thực hiện các dịch vụ phục vụ HĐH cũng như HĐH thực thi các dịch vụ phục vụ các ứng dụng.
  - Ngay khi hệ điều hành thiết lập các hạn chế lên ứng dụng, nhân an toàn đặt ra các hạn chế với HĐH.
- Trong khi HĐH không đóng vai trò gì trong việc thực thi các chính sách an toàn được triển khai bởi nhân, HĐH cần giữ cho hệ thống hoạt động và ngăn chặn việc từ chối phục vụ do ứng dụng lỗi hay có mục đích xấu.
  - Không lỗi nào trong ứng dụng cũng như trong hệ điều hành xâm phạm đến chính sách an toàn của nhân.