HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC

AN TOÀN HỆ ĐIỀU HÀNH

CHƯƠNG 4 – CÁC MÔ HÌNH AN TOÀN CỦA HĐH

Giảng viên: PGS.TS. Hoàng Xuân Dậu

E-mail: dauhx@ptit.edu.vn

Khoa: An toàn thông tin

NỘI DUNG CHƯƠNG 4

1. Giới thiệu
2. Các đặc trưng của mô hình an toàn
3. Mô hình máy trạng thái
4. Mô hình Harrison-Ruzzo-Ullman
5. Các mô hình an toàn khác

4.1 Giới thiệu

- Mô hình an toàn là khái niệm quan trọng trong thiết kế và phân tích an toàn của hệ thống do nó tích hợp chính sách an toàn hay các mục tiêu cần phải được thực thi và đảm bảo trong hệ thống;
- Mô hình an toàn là biểu diễn dạng ký hiệu của các chính sách và ánh xạ mong muốn của người đề ra chính sách thành tập các luật phải được tuân thủ trong hệ thống.
- Chính sách là thuật ngữ trừu tượng mô tả mục tiêu và các kết quả mà hệ thống phải đáp ứng và hoàn thành theo cách an toàn và chấp nhận được.

Giới thiệu

- Mô hình an toàn ánh xạ các mục tiêu khái quát và trừu tượng của chính sách vào các bộ phận của hệ thống máy tính bằng cách mô tả các cấu trúc dữ liệu và kỹ thuật cụ thể để thực thi chính sách an toàn.
- Thông thường, mô hình an toàn được biểu diễn bằng các ký hiệu toán học, các ý tưởng được phân tích, tiếp theo chúng được chuyển thành các đặc tả của hệ thống, và sau đó được phát triển thành các đoạn mã chương trình.

Giới thiệu

- Một số mô hình an toàn thực thi các quy định và luật nhằm bảo vệ:
  - Tính bí mật dữ liệu;
  - Tính toàn vẹn dữ liệu.
- Các mô hình chính tắc thường được dùng nhằm đảm bảo an ninh ở mức độ cao, như Bell-LaPadula;
- Các mô hình phi chính tắc như Clark-Winson thường sử dụng như cấu trúc khung cho biết cách thức các chính sách an toàn được biểu diễn và thực thi.

4.2 Các đặc trưng của mô hình an toàn

- Chính xác và rõ ràng
- Đơn giản, khái quát và dễ hiểu
- Căn bản/cơ bản
- Thể hiện rõ ràng chính sách an toàn.

Các đặc trưng - Chính xác và rõ ràng

- Mô hình an toàn biểu diễn và thực thi chính sách an toàn của hệ thống chính vì vậy đặc trưng đầu tiên là tính chính xác và rõ ràng để có thể mô tả một cách đầy đủ và trọn vẹn chính sách cần thực thi của hệ thống.
  - Với các hệ thống an toàn cao, mô hình được diễn giải bằng các ký hiệu toán học.
  - Tuy vậy, các khái niệm của việc lập mô hình hệ thống không nhất thiết cần các công cụ toán học, đặc biệt là khi sử dụng lại mô hình sẵn có.
    - Khi đó, việc biểu diễn mô hình bằng ngôn ngữ thông thường hoàn toàn có thể đủ thỏa mãn đặc trưng này.

Các đặc trưng - Đơn giản, khái quát và dễ hiểu

- Đặc trưng này giúp cho mô hình có thể được nắm bắt và triển khai một cách nhanh chóng và đầy đủ không chỉ với người thiết kế hay triển khai mà cả với người dùng cuối của hệ thống.
  - Nếu không ai có thể hiểu được yêu cầu an toàn thì không công cụ toán học nào có thể chứng minh sự phù hợp của mô hình an toàn.

Các đặc trưng

- Căn bản/cơ sở: Hệ thống xử lý các thuộc tính an toàn và không hạn chế một cách quá mức các chức năng khác hay việc triển khai hệ thống;
- Thể hiện rõ ràng chính sách an toàn: Mô hình an toàn cần chứa đựng đầy đủ và rõ ràng các mong muốn cũng như yêu cầu thiết yếu về việc vận hành hệ thống.

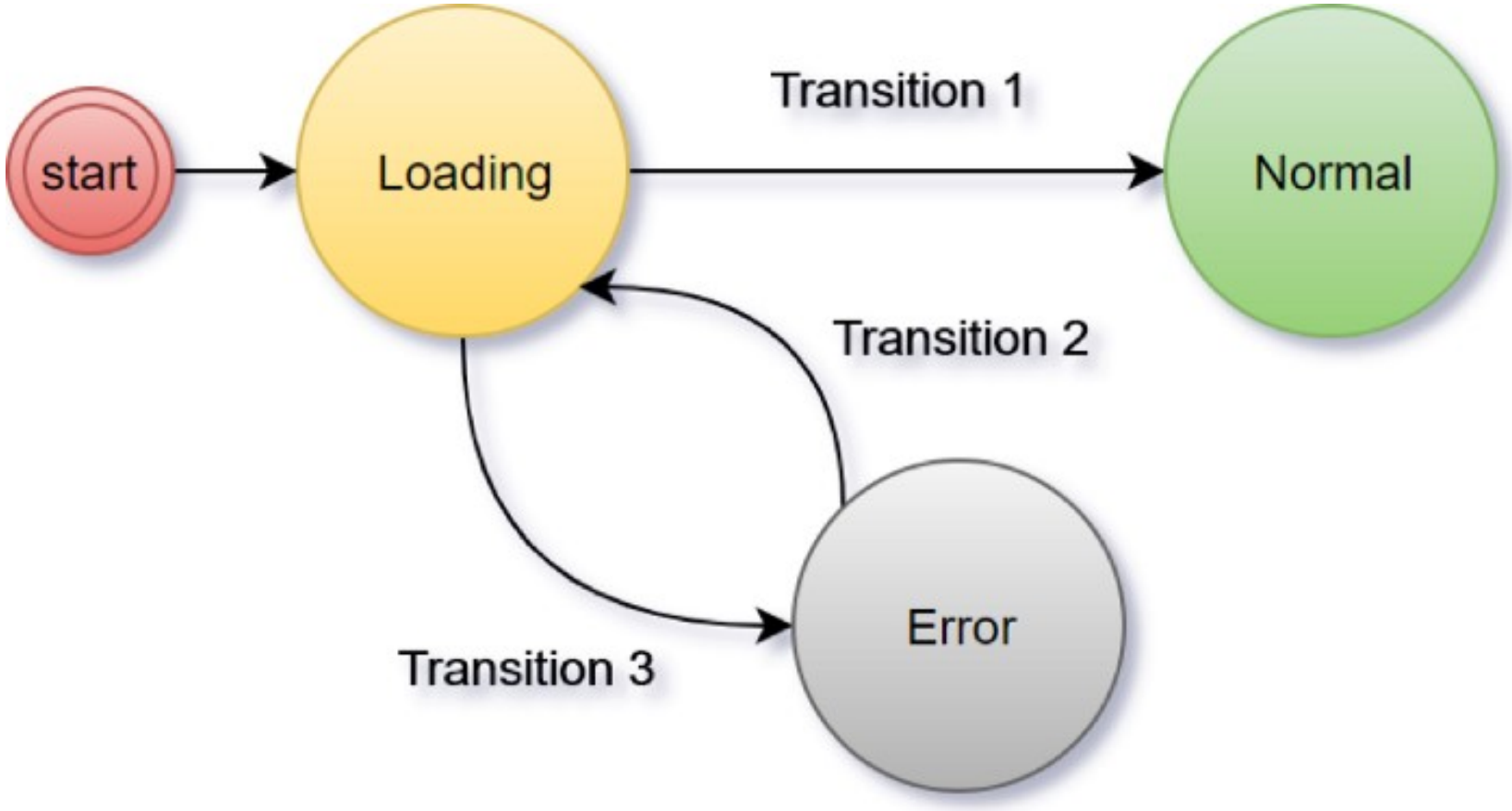
4.3 Mô hình máy trạng thái

- Khái quát
- Các bước xây dựng mô hình
- Ví dụ xây dựng mô hình

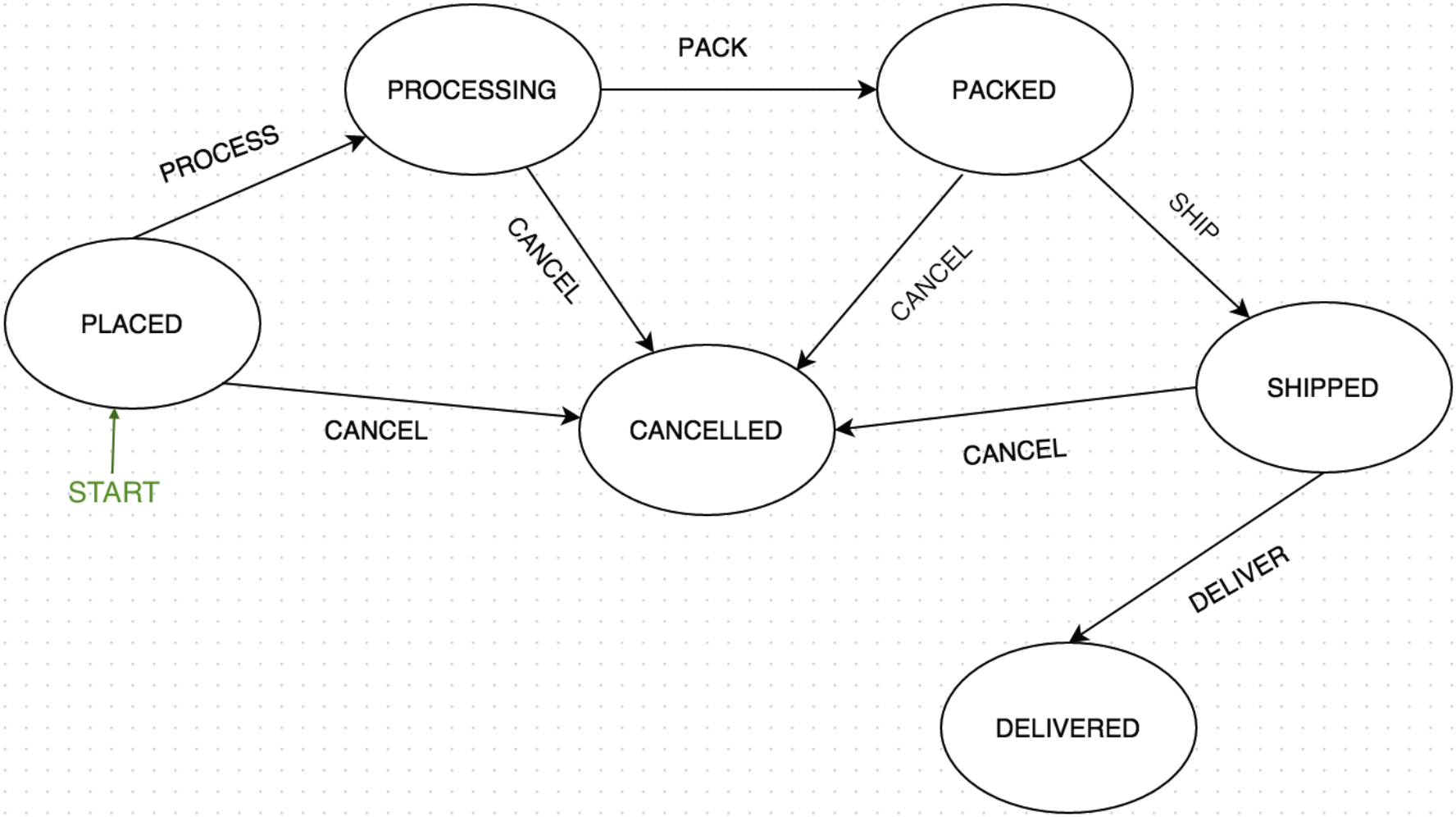
Khái quát mô hình máy trạng thái

- Mô hình máy trạng thái (State-machine model) được sử dụng khá rộng rãi trong hệ thống máy tính để biểu diễn quá trình vận hành, xử lý dữ liệu. Mô hình máy trạng thái gồm:
  - Các trạng thái;
  - Các thao tác/hàm dịch chuyển trạng thái.

Một mô hình máy trạng thái đơn giản



Một mô hình máy trạng thái đặt hàng - xử lý - giao hàng



Khái quát mô hình máy trạng thái

- Mô hình an toàn không sử dụng tất cả các trạng thái và các chức năng của hệ thống mà người thiết kế lựa chọn các biến liên quan đến vấn đề an ninh để lập mô hình.
- Việc xây dựng mô hình an toàn máy trạng thái liên quan đến:
  - Việc xác định các thành phần của mô hình bao gồm các biến, các chức năng, các quy định,... và
  - Trạng thái an toàn khởi đầu.
- Khi đã xác định được tính an toàn của trạng thái khởi đầu và các chức năng an toàn, việc suy diễn toán học cho phép xác định tình trạng an toàn của hệ thống bất kể các chức năng được sử dụng như thế nào.

Các bước xây dựng mô hình

1. Xác định các biến trạng thái có liên quan:
   - Các biến mô tả các chủ thể và đối tượng bên trong hệ thống, các thuộc tính an toàn của chúng cũng như quyền truy cập của chủ thể đến đối tượng.
2. Xác định trạng thái an toàn:
   - Mô tả một bất biến (invariant) biểu diễn quan hệ giữa các giá trị của các biến mà luôn được đảm bảo trong khi thay đổi trạng thái.
3. Xác định hàm dịch chuyển trạng thái:
   - Các hàm mô tả các thay đổi tới các biến trạng thái còn gọi là các nguyên tắc hoạt động. Mục tiêu của các hàm là hạn chế các thay đổi mà hệ thống có thể thực hiện.

Các bước xây dựng mô hình

4. Chứng minh các hàm đảm bảo trạng thái an toàn
   - Đảm bảo mô hình nhất quán với các mô tả về trạng thái an toàn, cần chứng minh với mỗi hàm hệ thống ở trạng thái an toàn trước và sau mỗi thao tác.
5. Xác định trạng thái khởi tạo:
   - Lựa chọn các giá trị cho các biến trạng thái mà hệ thống bắt đầu ở trạng thái an toàn.
6. Chứng minh trạng thái khởi tạo an toàn theo các mô tả về trạng thái an toàn.

Ví dụ xây dựng mô hình máy trạng thái

- Chính sách:
  - Người dùng có thể đọc tài liệu khi và chỉ khi quyền truy cập có được lớn hơn hoặc bằng nhãn phân loại của tài liệu;
    - Đây là một dạng yêu cầu truy cập tiêu biểu với cơ quan có áp dụng cơ chế đảm bảo an toàn thông tin trong cơ quan.
    - Mục tiêu là xác định mô hình sử dụng cho hệ thống máy tính nhằm thực thi chính sách trên.
- Mô tả chi tiết chính sách:
  - Chủ thể có thể đọc đối tượng khi và chỉ khi lớp truy cập của chủ thể lớn hơn hoặc bằng lớp truy cập của đối tượng;
  - Chủ thể có thể ghi vào đối tượng khi và chỉ khi lớp truy cập của chủ thể nhỏ hơn hoặc bằng lớp truy cập của đối tượng.

Ví dụ xây dựng mô hình máy trạng thái

- Mô tả các biến trạng thái:

S = Tập các chủ thể

O = Tập các đối tượng

sclass(s) = lớp truy cập của chủ thể *s*

oclass(o) = lớp truy cập của đối tượng *o*

A(s,o) = Tập các chế độ truy cập, nhận các giá trị sau

{**r**} Nếu chủ thể s có thể đọc đối tượng *o*

{**w**} Nếu chủ thể s có thể ghi lên đối tượng *o*

{**r,w**} Nếu cả đọc và ghi

Ø Nếu không được đọc và không được ghi

contents(o) = nội dung của đối tượng *o*

subj = chủ thể hoạt động

Ví dụ xây dựng mô hình máy trạng thái

- Trạng thái hệ thống tại một thời điểm bất kỳ được biểu diễn bằng tập giá trị của tất cả các biến trạng thái:

  {*S, O, sclass, oclass, A, contents, subj*}

- Trạng thái an toàn chính là biểu diễn toán học của các mô tả thể hiện chính sách truy cập mong muốn. Trạng thái này thể hiện tính bất biến của hệ thống.
- Hệ thống an toàn khi và chỉ khi $\forall s \in S, \forall o \in O$,

  Nếu r $\in A(s,o)$, thì $sclass(s) \geq oclass(o)$,

  Nếu w $\in A(s,o)$, thì $oclass(o) \geq sclass(s)$.

Ví dụ xây dựng mô hình máy trạng thái

- Các hàm chuyển dịch trạng thái có thể coi như các lời gọi hàm tới các tiện ích của hệ thống mà các tiện ích này làm thay đổi các biến trạng thái.
- Một số hàm chuyển dịch trạng thái tiêu biểu:

1. Create_object (*o, c*): Tạo đối tượng o với lớp truy cập *c*.
2. Set_access (*s, o, modes*): Thiết lập chế độ truy cập cho chủ thể *s* tới đối tượng *o*.
3. Change_object (*o, c*): Thiết lập lớp truy cập của *o* tới *c*.
4. Write_object (*o, d*): Ghi dữ liệu *d* vào *contents(o)*.
5. Copy_object (*from, to*): Sao chép *contents(from)* tới *contents(to)*.
6. Append_data (*o, d*): Thêm dữ liệu *d* tới *contents(o)*.

Ví dụ xây dựng mô hình máy trạng thái

- Nội dung hàm khởi tạo:

Create_object (*o*, *c*)

Nếu $o \notin O$

thì $'O = O \cup \{o\}$ và

$'oclass(o) = c$ và

Với mọi $s \in S$, $'A(s,o) = \emptyset$.

Ví dụ xây dựng mô hình máy trạng thái

- Nội dung hàm thiết lập:

Set_access (*s, o, modes*)

Nếu $s \in S$ và $o \in O$

và nếu {[$r \in modes$ và $sclass(s) \geq oclass(o)$] hoặc $r \notin modes$} và

{[$w \in modes$ và $oclass(o) \geq sclass(s)$] hoặc $w \notin modes$}

thì $'A(s,o) = modes$.

Ví dụ xây dựng mô hình máy trạng thái

- Trạng thái ban đầu thể hiện giá trị khởi tạo của các biến trong hệ thống:

  $\{S_0, O_0, sclass_0, oclass_0, contents_0, subj_0\}$ hay có thể biểu diễn như sau:

  $\forall s \in S_0, o \in O_0$

  $sclass_0(s) = c_0$

  $oclass_0(o) = c_0$

  $A_0(s, o) = \{r,w\}$

4.4 Mô hình Harrison-Ruzzo-Ullman (HRU)

- Định nghĩa
- Các đặc trưng
- Các kết quả.

Mô hình HRU - Định nghĩa

- Mô hình HRU hướng tới xử lý quyền truy cập của các chủ thể và tính toàn vẹn của các quyền này.
- Mô hình HRU cho phép quyền truy cập thay đổi và xác định chủ thể và đối tượng cần được tạo và xóa thế nào.
- Mô hình HRU cũng cho phép kiểm chứng các thay đổi về quyền có tác động như thế nào đến các yêu cầu về an toàn đặt ra.
  - Nói cách khác, mô hình cho phép đánh giá tính an toàn của các thao tác thay đổi quyền này.

Mô hình HRU - Định nghĩa

- Mô hình HRU được định nghĩa như sau:
  - Tập chủ thể *S*
  - Tập đối tượng *O*
  - Tập quyền truy cập *R*
  - Ma trận truy cập *M* | $M = (M_{so})_{s \in S,\, o \in O} \mid M_{so} \in R$

Mô hình HRU - Định nghĩa

- Mô hình HRU được định nghĩa như sau:
  - Tập các câu lệnh *C* với mỗi câu lệnh *c* dưới dạng:

$c(x_1,\ldots,x_k)$
if r_1 *in* $M_{s1,o1}$ *and*
if r_2 *in* $M_{s2,o2}$ *and*
...
if r_m *in* $M_{sm,om}$
then
op_1
op_2
....
op_n
end

Mô hình HRU - Định nghĩa

Các thao tác op_i có thể là một trong các thao tác nguyên thủy như sau:

1. ***enter r into*** $(x_s; x_o)$**:** Thêm r vào $M[x_s, x_o]$
2. ***delete r from*** $(x_s; x_o)$ **:** Loại bỏ r khỏi $M[x_s, x_o]$
3. ***create subject*** x_s **:** Tạo hàng mới trong M
4. ***create object*** x_o **:** Tạo cột mới trong M
5. ***destroy subject*** x_s **:** Loại bỏ hàng tương ứng với x_s
6. ***destroy object*** x_o **:** Loại bỏ cột tương ứng với x_o

Ví dụ minh hoạ mô hình HRU

- Chủ thể *s* tạo file *f* (có quyền sở hữu *o* file này) và có quyền đọc *r*, ghi *w* với file:

command create_files(s,f)

create f

enter o into $M_{s,f}$

enter r into $M_{s,f}$

enter w into $M_{s,f}$

end

Ví dụ minh hoạ mô hình HRU

- Chủ thể *s* của file *f* cấp quyền đọc *r* cho chủ thể *p*:

command grant_read(s,p,f)

if o in $M_{s,f}$ *// o là quyền sở hữu*

then enter r into $M_{p,f}$

end

Các đặc trưng của mô hình HRU

- Các câu lệnh làm thay đổi quyền truy cập đối tượng được lưu lại thông qua sự thay đổi của ma trận truy cập. Như vậy, ma trận truy cập thể hiện trạng thái của hệ thống. Nói cách khác mô hình HRU sử dụng cách kiểm soát thông qua ma trận truy cập.

Các đặc trưng của mô hình HRU

- Mô hình HRU biểu diễn các chính sách an toàn thông qua việc điều chỉnh cấp quyền truy cập. Để kiểm tra hệ thống tuân thủ chính sách an toàn, cần chứng minh không tồn tại cách cấp quyền truy cập không mong muốn:
  - Ma trận *M* được coi là rò rỉ quyền *r* nếu tồn tại thao tác *c* thêm quyền *r* vào một vị trí của *M* mà trước đó không chứa *r*.
  - Ma trận *M* là an toàn với quyền *r* nếu không có chuỗi lệnh *c* nào có thể chuyển *M* sang trạng thái rò rỉ *r.*

Các đặc trưng của mô hình HRU

- Trạng thái an toàn của hệ thống được mô hình HRU diễn giải không chính tắc như sau:
  - Truy cập tài nguyên của hệ thống mà không có sự đồng ý của chủ sở hữu là không thể.
  - Người dùng cần có khả năng xác định liệu việc họ định làm có thể dẫn đến việc rò rỉ quyền tới các chủ thể không được phép.

Các kết quả của HRU

- Mục tiêu mà mô hình HRU hướng tới là xây dựng mô hình đơn giản có thể áp dụng được cho nhiều hệ thống an toàn khác nhau. Mô hình này đã chứng tỏ:
  - Với ma trận truy cập *M* và quyền *r*, việc kiểm chứng tính an toàn của *M* với *r* là không xác định được. Bài toán an toàn không giải quyết được trong trường hợp tổng quát đầy đủ. Với mô hình hạn chế hơn thì có thể giải quyết được.
  - Với hệ thống mà các lệnh chỉ chứa 1 thao tác, với ma trận truy cập *M* và quyền *r*, việc kiểm chứng tính an toàn của *M* là xác định được. Với hệ thống lệnh chứa 2 thao tác, việc kiểm chứng là không xác định được.
  - Bài toán an toàn cho hệ thống xác thực bất kỳ là xác định được nếu số lượng các chủ thể là hữu hạn.

4.5 Các mô hình an toàn khác

- Mô hình luồng thông tin
- Mô hình Bell-La Padula
- Mô hình Biba
- Mô hình Clark-Winson

Mô hình luồng thông tin

- Lý do mô hình luồng thông tin ra đời:
  - Nhằm khắc phục hạn chế của mô hình dựa trên máy trạng thái là sự thiếu mô tả về luồng thông tin;
  - Giúp giải quyết vấn đề an toàn liên quan tới việc luân chuyển của dữ liệu cần được xử lý bằng các ràng buộc;

Mô hình luồng thông tin

- Mô hình luồng thông tin biểu diễn cách thức dữ liệu di chuyển giữa đối tượng và chủ thể trong hệ thống:
  - Khi chủ thể (chương trình) đọc từ một đối tượng (file), dữ liệu từ đối tượng di chuyển vào bộ nhớ của chủ thể.
  - Nếu có bí mật trong đối tượng thì bí mật này chuyển tới bộ nhớ của chủ thể khi đọc.
  - Như vậy, bí mật có thể bị lộ khi chủ thể ghi bí mật này ra đối tượng (file) khác.

Mô hình luồng thông tin

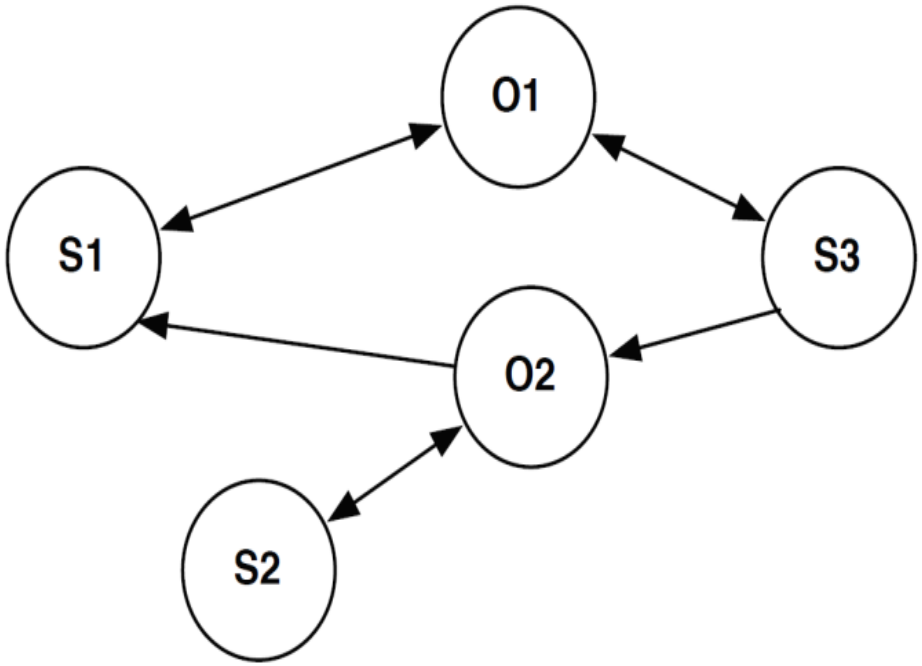
- Với mỗi thao tác trên một đối tượng trong mô hình này thì thao tác này có thể là:
  - Đọc luồng thông tin (tức là lấy dữ liệu ra khỏi chủ thể) hay
  - Ghi luồng thông tin (tức là cập nhật đối tượng với dữ liệu mới), hoặc kết hợp cả hai.
- Đồ thị luồng thông tin gồm:
  - Các đỉnh là các chủ thể và đối tượng;
  - Các cung/liên kết biểu diễn các thao tác giữa các chủ thể và đối tượng;
  - Chiều liên kết thể hiện hướng đi của dữ liệu tới đối tượng hay vào bộ nhớ của chủ thể.

Luồng thông tin giữa chủ thể và đối tượng

Ma trận truy nhập

	O1	O2
S1	read append	read getattr
S2		read ioctl
S3	read write	append

Đồ thị luồng thông tin



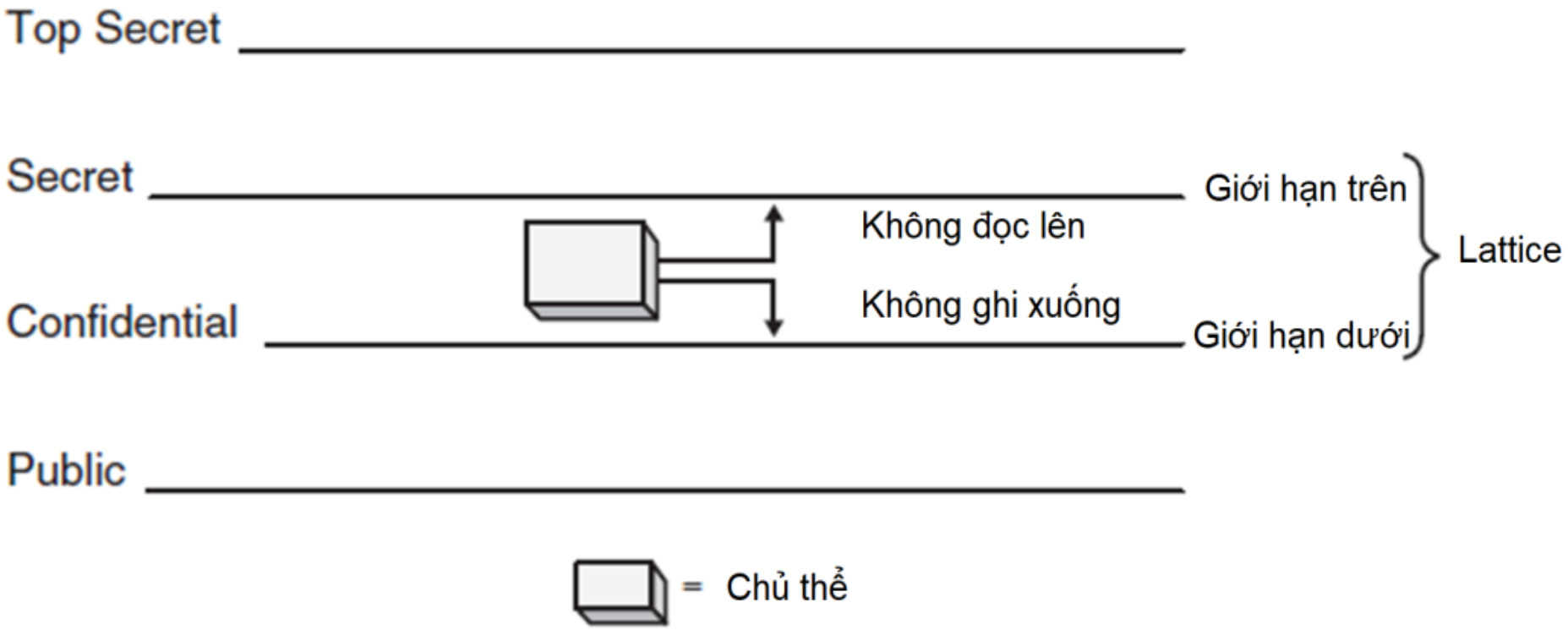
Mô hình luồng thông tin

- Luồng thông tin được sử dụng để mô tả các mục tiêu an toàn của hệ thống (tính bí mật và toàn vẹn) bằng cách phân tích các cung trong đồ thị luồng thông tin:
  - Tính bí mật: Các cung trong đồ thị biểu diễn toàn bộ các đường dẫn mà dữ liệu có thể bị rò rỉ qua đó;
    - Có thể dùng đồ thị để xác định liệu có một đối tượng bí mật *o* rò rỉ tới chủ thể không được phép *s*. Nếu tồn tại một đường dẫn từ *o* tới *s* thì tính bí mật của hệ thống bị xâm phạm.
  - Tính toàn vẹn: Không một chủ thể với mức độ toàn vẹn cao lệ thuộc vào bất cứ chủ thể hay đối tượng nào có mức toàn vẹn thấp:
    - Có thể dùng đồ thị để xác định liệu chủ thể *s1* có nhận đầu vào từ chủ thể *s2* mà có mức độ toàn vẹn thấp hơn không. Nếu có tồn tại một đường dẫn từ *s2* tới *s1* thì không đảm bảo mức độ toàn vẹn.

Mô hình Bell-La Padula

- Mô hình Bell-La Padula là mô hình luồng thông tin phổ biến nhất hướng tới việc bảo vệ tính bí mật.
  - Để thực hiện việc kiểm soát truy cập, mô hình này định nghĩa mức độ an toàn cho các đối tượng dữ liệu.
- Các đặc trưng của mô hình Bell-La Padula như sau:
  - Quyền truy cập được định nghĩa thông qua ma trận truy cập và thứ tự mức an toàn;
  - Các chính sách an toàn ngăn chặn luồng thông tin đi xuống từ mức an toàn cao xuống mức thấp;
  - Mô hình này chỉ xem xét luồng thông tin xảy ra khi có sự thay đổi hay quan sát một đối tượng.

Nguyên tắc an toàn trong Bell-La Padula



Nguyên tắc an toàn trong Bell-La Padula

- Các chủ thể và đối tượng đều được gán các nhãn an toàn;
- Các nhãn an toàn theo cấp độ bảo mật từ cao xuống thấp gồm:
  - Top Secret
  - Secret
  - Confidential
  - Public.
- Nguyên tắc an toàn: không đọc lên và không ghi xuống (hoặc chỉ đọc xuống và chỉ ghi lên).
  - Chủ thể chỉ được phép đọc dữ liệu mà nhãn an toàn của dữ liệu thấp hơn nhãn an toàn của chủ thể và chỉ được phép ghi khi nhãn an toàn của chủ thể không lớn hơn nhãn an toàn của dữ liệu.

Nguyên tắc an toàn trong Bell-La Padula

- Nguyên tắc an toàn của mô hình Bell-La Padula được biểu diễn như sau:

  SC(o) và *SC(s)* là các nhãn an toàn của dữ liệu *o* và chủ thể *s*. Các nhãn này tuân thủ trật tự nhất định, khi này các thao tác đọc ghi được phép của chủ thể *s* lên đối tượng *o* khi và chỉ khi:

  - đọc: $SC(s) \geq SC(o)$
  - ghi: $SC(s) \leq SC(o)$

Điểm yếu của mô hình Bell-La Padula

- Mô hình Bell-La Padula được phát triển tập trung cho việc đảm bảo tính bí mật của các đối tượng (dữ liệu).
- Mô hình không đề cập đến việc thay đổi quyền truy cập của các người dùng (chủ thể) của hệ thống.
- Mô hình này chứa kênh ngầm (covert channel) thể hiện qua việc đối tượng mức thấp có thể phát hiện sự tồn tại của đối tượng mức cao khi bị từ chối truy cập.
  - Vấn đề này xâm phạm trực tiếp đến tính bí mật của đối tượng.

Mô hình Biba

- Mô hình Biba đảm bảo tính toàn vẹn theo cách thức tính toàn vẹn của dữ liệu bị đe dọa khi:
  - Chủ thể ở mức toàn vẹn thấp có khả năng ghi vào đối tượng (dữ liệu) có mức toàn vẹn cao hơn và khi
  - Chủ thể có thể đọc dữ liệu ở mức toàn vẹn thấp hơn.
- Mô hình Biba áp dụng hai quy tắc:
  - Không ghi lên: Chủ thể không thể ghi dữ liệu vào đối tượng có mức toàn vẹn cao hơn;
  - Không đọc xuống: Chủ thể không thể đọc dữ liệu có mức toàn vẹn thấp hơn.

Mô hình Biba

- Mô hình Biba tương tự như Bell-LaPadula sử dụng các nhãn an ninh để biểu diễn mức độ an toàn mong muốn và kiểm soát các thao tác của chủ thể lên đối tượng.
- Tuy nhiên, luồng thông tin trong mô hình Biba được kiểm soát ngược với mô hình Bell-LaPadula.
  - Các đối tượng có mức độ an ninh thấp có nghĩa là độ toàn vẹn thấp và chủ thể có mức độ an ninh cao không được sử dụng thông tin từ các đối tượng này.
  - Nói cách khác chủ thể có yêu cầu an ninh cao không được sử dụng thông tin từ nguồn có độ tin cậy thấp.
    - Tình huống này có thể thấy trong việc tiếp nhận dữ liệu đầu vào của các máy chủ web, cơ sở dữ liệu hay dịch vụ hệ thống từ các nguồn không tin cậy.

Mô hình Clark-Winson

- Mô hình Clark-Winson cung cấp một cách tiếp cận khác cho vấn đề toàn vẹn dữ liệu.
- Mô hình này tập trung vào việc ngăn chặn người dùng sửa đổi trái phép dữ liệu.
  - Trong mô hình này, người dùng không thao tác trực tiếp với các đối tượng mà thông qua một chương trình.
  - Chương trình này hạn chế các thao tác người dùng được thực hiện lên đối tượng và như vậy bảo vệ tính toàn vẹn của đối tượng.

Mô hình Clark-Winson

- Tính toàn vẹn được dựa trên nguyên tắc các công việc (thủ tục) được định nghĩa tường minh và việc tách biệt trách nhiệm.
- Nói cách khác, mô hình dựa trên cơ sở qui trình công việc được xây dựng một cách rõ ràng và nguyên tắc tách biệt trách nhiệm của người dùng tham gia vào qui trình xử lý công việc.

Mô hình Clark-Winson

- Mô hình Clark-Winson được mô tả như sau:
  - Chủ thể và đối tượng được dán nhãn theo chương trình;
  - Chương trình đóng vai trò như lớp trung gian giữa chủ thể và đối tượng;
  - Việc kiểm soát truy cập được thực hiện nhờ:
    - Định nghĩa các thao tác truy cập có thể được thực hiện lên từng mục dữ liệu;
    - Định nghĩa các thao tác truy cập có thể được thực hiện bởi chủ thể.
  - Các thuộc tính an toàn được mô tả qua các luật chứng thực và cần kiểm tra để đảm bảo các chính sách an ninh nhất quán với yêu cầu của chương trình.

Mô hình Clark-Winson

- Các dữ liệu có mức độ toàn vẹn cao, gọi là các mục dữ liệu hạn chế CDI (Constrained Data Items), phải được kiểm chứng nhờ các chương trình đặc biệt có mức độ toàn vẹn tương đương.
  - Các chương trình này gọi là các thủ tục kiểm chứng toàn vẹn IVP (Integrity Verfication Procedure).
  - Các mục dữ liệu này cũng chỉ được sửa đổi qua các thủ tục chuyển đổi TP (Transformation Procedure) có mức toàn vẹn tương đương.
  - Các chương trình IVP đảm bảo các dữ liệu CDI thỏa mãn các yêu cầu nhất định để hệ thống đảm bảo được mức độ toàn vẹn mong muốn khi khởi động.
  - Các thủ tục chuyển đổi có vai trò tương tự như các chủ thể trong mô hình Biba ở chỗ chúng chỉ có thể sửa đổi các dữ liệu có mức toàn vẹn tương đương.

Mô hình Clark-Winson

- Mô hình Clark-Winson xây dựng các qui định chứng thực và thực thi để đảm bảo tính toàn vẹn của hệ thống như sau:
  - Qui định chứng thực:
    - Thủ tục kiểm chứng toàn vẹn IVP phải đảm bảo các mục dữ liệu hạn chế CDI ở trạng thái hợp lệ khi IVP chạy;
    - Thủ tục chuyển đổi TP phải được chứng thực là hợp lệ tức là CDI bắt buộc phải chuyển đổi thành CDI hợp lệ;
    - Các qui định truy cập phải thỏa mãn bất kỳ yêu cầu về việc tách biệt trách nhiệm;
    - Tất cả các thủ tục TP phải ghi vào log chỉ ghi thêm;
    - Bất kỳ TP có đầu vào dữ liệu không hạn chế UDI (unconstrained data items) thì phải chuyển đổi sang dạng CDI hoặc loại bỏ UDI đó và không thực hiện việc chuyển đổi nào.

Mô hình Clark-Winson

- Mô hình Clark-Winson xây dựng các qui định chứng thực và thực thi để đảm bảo tính toàn vẹn của hệ thống như sau:
  - Qui định thực thi:
    - Hệ thống phải duy trì và bảo vệ danh sách các mục {TP, CDI_i, CDI_j,...} cho phép TP được xác thực truy cập tới các CDI;
    - Hệ thống phải duy trì và bảo vệ danh sách {UserID,TP_i, CDI_i,CDI_j,...} chỉ định các TP mà người dùng được thực thi;
    - Hệ thống phải xác thực từng người dùng khi yêu cầu thực hiện TP;
    - Chỉ có chủ thể xác thực qui định truy cập TP mới có thể sửa đổi mục tương ứng trong danh sách. Chủ thể này phải không có quyền thực thi trên TP đó.

Mô hình Clark-Winson

- Các qui định chứng thực và thực thi cho thấy mô hình Clark-Winson yêu cầu cả ba thành phần xác thực, kiểm toán, và quản trị.
  - Vấn đề xác thực thể hiện rõ ràng trong qui định thực thi.
  - Vấn đề kiểm toán thể hiện ở việc các TP phải cung cấp đủ thông tin về việc thực hiện để có thể mô tả lại các thao tác sửa đổi dữ liệu hạn chế CDI.
  - Yêu cầu về quản trị thực hiện qua việc hạn chế các người dùng được quyền chứng thực không được phép chạy các chương trình thay đổi dữ liệu.
- Hơn thế nữa, mô hình này cũng hạn chế người dùng được phép thực thi tất cả các thao tác của một công việc.