HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC

An toàn hệ điều hành

Security Models – Các mô hình an toàn

Giảng viên: TS. Phạm Hoàng Duy

Điện thoại/E-mail: phamhduy@gmail.com

Bộ môn: An toàn thông tin - Khoa CNTT1

Nội dung

- Vai trò và đặc trưng của mô hình an toàn
- Mô hình máy trạng thái
- Mô hình Harrison-Ruzzo-Ullman
- Các mô hình khác

Mô hình an toàn

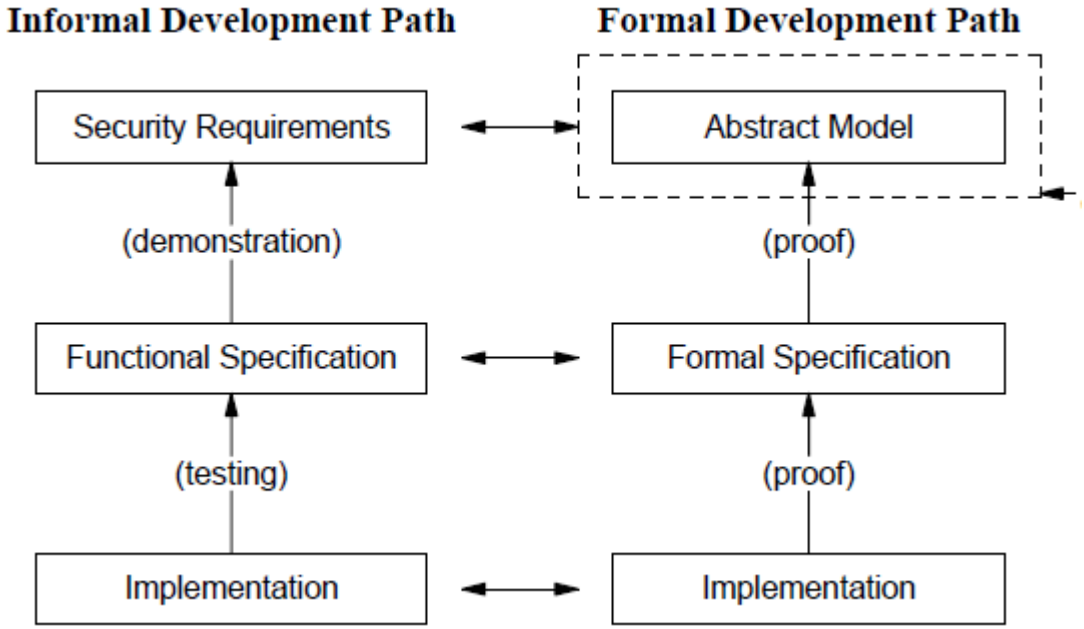
- Thành công trong việc đạt được mức độ an toàn cao trong hệ thống tùy thuộc vào mức độ cẩn thận trong quá trình thiết kế và triển khai các biện phận kiểm soát an ninh. Mục tiêu của mô hình an ninh là biểu diễn các yêu cầu về an toàn của hệ thống một cách chính xác.

Đặc trưng

- Mô hình an toàn có các thuộc tính cơ bản sau
  - Chính xác và không mơ hồ
  - Đơn giản và khái quát do vậy dễ hiểu
  - Căn bản: xử lý các thuộc tính an toàn và không hạn chế một cách quá đáng (không thích đáng) các chức năng hay việc triển khai của hệ thống
  - Thể hiện rõ ràng chính sách an toàn

Vai trò

- Một trong những vấn đề khiến cho hệ thống mất an toàn là người thiết kế không xác định được một cách chính xác và đúng đắn yêu cầu về an toàn. Mô hình an toàn đóng vai trò then chốt trong cách thức phát triển hệ thống một cách chính tắc.



Vai trò

- Mục tiêu phát triển hệ thống nhằm đảm bảo với mức độ chắc chắn nhất định rằng việc triển khai hệ thống phù hợp với mô hình lựa chọn
- Mức độ khác biệt về chi tiết giữa mô hình và triển khai thường rất lớn nên cần thêm bước trung gian nhằm đảm bảo sự tương ứng giữa yêu cầu an toàn và triển khai thực tế
- Các mô tả chính tắc (formal specification) cung cấp các cơ sở cho các chứng minh toán học rằng các mô tả phù hợp với mô hình đề ra

Vai trò

- Mô hình an toàn có thể dùng như các mô tả về an ninh cho hệ thống. Việc này giúp hạn chế các lỗ hổng an toàn khi người thiết kế quá tập trung vào chức năng.
- Việc lập mô hình an toàn tiêu tốn nhiều công sức và nhân lực. Các mô hình an toàn đóng vai trò gợi ý cho người thiết kế để phát triển hệ thống phù hợp

Các mô hình an toàn

- Mô hình máy trạng thái
- Mô hình Harrison-Ruzzo-Ullman
- Các mô hình khác

Mô hình máy trạng thái

- Mô hình máy trạng thái thường được sử dụng vì mô hình này biểu diễn hệ thống máy tính gần giống cách thức thực hiện của hệ điều hành
- Một biến trạng thái là khái niệm trừu tượng của bit hay byte trong hệ thống thay đổi khi hệ thống hoạt động
- Người thiết kế lựa chọn các biến liên quan đến vấn đề an ninh để lập mô hình

Mô hình máy trạng thái

1. Xác định các biến trạng thái 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 nhập giữa chủ thể và đối tượng
2. Xác định trạng thái an toàn
   - Mô tả một bất biến (invariant) biểu diễn quan hệ giữa các giá trị của biến mà luôn được đảm bảo trong khi thay đổi trạng thái

Mô hình máy trạng thái

3. Xác định hàm chuyển dịch trạng thái
   - Các hàm này mô tả các thay đổi tới các biến trạng thái còn gọi là các nguyên tắc hoạt động (rule of operation). Mục tiêu của các hàm là hạn chế các thay đổi mà hệ thống có thể thực hiện.
4. Chứng minh các hàm đảm bảo trạng thái an toàn
   - Để đảm bảo mô hình nhất quán với các mô tả về trạng thái an toàn, cần chức minh với mỗi hàm hệ thống ở trạng thái an toàn trước và sau mỗi thao tác

Mô hình máy trạng thái

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

- Chính sách:
  - Người dùng có thể đọc tài liệu khi và chỉ khi quyền (clearance) có được lớn hơn hoặc bằng phân loại (classification) của tài liệu
- Mô tả
  - Chủ thể có đọc đối tượng khi và chỉ khi lớp truy nhập của chủ thể lớn hơn hoặc bằng lớp truy nhập của đối tượng
  - Chủ thể có ghi vào đối tượng khi và chỉ khi lớp truy nhập của chủ thể lớn hơn hoặc bằng lớp truy nhập của đối tượng

Ví dụ

- Mô tả các biến trạng thái

S = set of current subjects
O = set of current objects
$sclass(s)$ = access class of subject s
$oclass(o)$ = access class of object o
$A(s,o)$ = set of modes, equal to one of:
- {r} if subject s can read object o
- {w} if subject s can write object o
- {r,w} if both read and write
- ∅ if neither read nor write

$contents(o)$ = contents of object o
$subj$ = active subject

- Trạng thái hệ thống

$\{S, O, sclass, oclass, A, contents, subj\}$

Ví dụ

- Trạng thái an toàn

Invariant: The system is secure if and only if, for all $s \in S$, $o \in O$,
if $\mathbf{r} \in A(s,o)$, then $sclass(s) \geq oclass(o)$,
if $\mathbf{w} \in A(s,o)$, then $oclass(o) \geq sclass(s)$.

- Các hàm chuyên dịch trạng thái

1. **Create_object** (*o, c*)
2. **Set_access** (*s, o, modes*)
3. **Create / Change_object** (*o, c*)
4. **Write_object** (*o, d*)
5. **Copy_object** (*from, to*)
6. **Append_data** (*o, d*)

Ví dụ

Function 1: **Create_object** (o,c)
if $o \notin O$
then $'O = O \cup \{o\}$ and
$'oclass(o) = c$ and
for all $s \in S$, $'A(s,o) = \varnothing$.

Function 2. **Set_access** $(s,o,$ *modes*$)$
if $s \in S$ and $o \in O$
and if $\{[\mathbf{r} \in modes$ and $sclass(s) \geq oclass(o)]$ or $\mathbf{r} \notin modes)$ and
$\{[\mathbf{w} \in modes$ and $oclass(o) \geq sclass(s)]$ or $\mathbf{w} \notin modes\}$
then $'A(s,o) = modes$.

Ví dụ

- Trạng thái ban đầu

$$\{S_0, O_0, sclass_0, oclass_0, contents_0, subj_0\}$$

Initial State (2): For all $s \in S_0$, $o \in O_0$

$$sclass_0(s) = c_0$$
$$oclass_0(o) = c_0$$
$$A_0(s,o) = \{\mathbf{r},\mathbf{w}\}$$

Mô hình Harrison-Ruzzo-Ullman

- Mô hình HRU xử lý quyền truy nhập của các chủ thể và tính toàn vẹn của các quyền này
  - Cho phép quyền truy nhập thay đổi và xác định chủ thể và đối tượng cần được tạo và xóa thế nào

Mô hình Harrison-Ruzzo-Ullman

- Mô hình HRU bao gồm
  - Tập chủ thể S
  - Tập đối tượng O
  - Tập quyền truy nhập R
  - Ma trận truy nhập M
    - $M = (M_{so})_{s \in S,\, o \in O} \mid M_{so} \in R$

Các thao tác gốc

- enter r into (X_s, X_o)
- delete r from (X_s, X_o)
- create subject X_s
- create object X_o
- destroy subject X_s
- destroy object X_o

Câu lệnh c

$c(x_1,\ldots,x_k)$

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

Ví dụ

- 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
```

- Chủ sở hữu *s* của *f* cấp quyền truy nhập *r* cho chủ thể *p*

```
command grant_read(s,p,f)
   if o in M_{s,f}
   then enter r into M_{p,f}
end
```

Mô hình Harrison-Ruzzo-Ullman

- Các câu lệnh (*command*) làm thay đổi quyền truy nhập đối tượng được lưu lại thông qua sự thay đổi của ma trận truy nhập
  - Như vậy ma trận truy nhập thể hiện trạng thái của hệ thống
- Mô hình HRU biểu diễn các chính sách an toàn thông qua việc điều chỉnh cấp quyền truy nhập. Để kiểm tra hệ thống tuân thủ chính sách an toàn, cần chứng minh không tồn tại cách cấp quyền truy nhập không mong muốn
- Ma trận *M* 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*

HRU Trạng thái an toàn

- Trạng thái an toàn của hệ thống được diễn giải như sau
  - Truy nhập 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.
- Hệ thống có các câu lệnh sau có an toàn

```
command grant_execute (s,p,f)
    if o in M_{s,f}
    then enter x into M_{p,f}
end

command modify_own_right (s,f)
    if x in M_{s,f}
    then enter w into M_{s,f}
end
```

Các thuộc tính an toàn của HRU

- Với ma trận truy nhập 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, có thể giải quyết được
- Với hệ thống mà các lệnh chỉ chứa 1 thao tác (toán tử), với ma trận truy nhập 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

Các mô hình khác

- Information flow
  - Bí mật
  - Toàn vẹn

Mô hình luồng thông tin

- Một trong những hạn chế của kỹ thuật dựa trên máy tạng thái là sự thiếu mô tả về luồng thông tin hơn là việc thiếu mô tả các ràng buộc hay bất biến của các thuộc tính an ninh của các đối tượng và chủ thể.
- 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. Và bí mật có thể bị lộ khi chủ thể ghi bí mật này ra đối tượng.

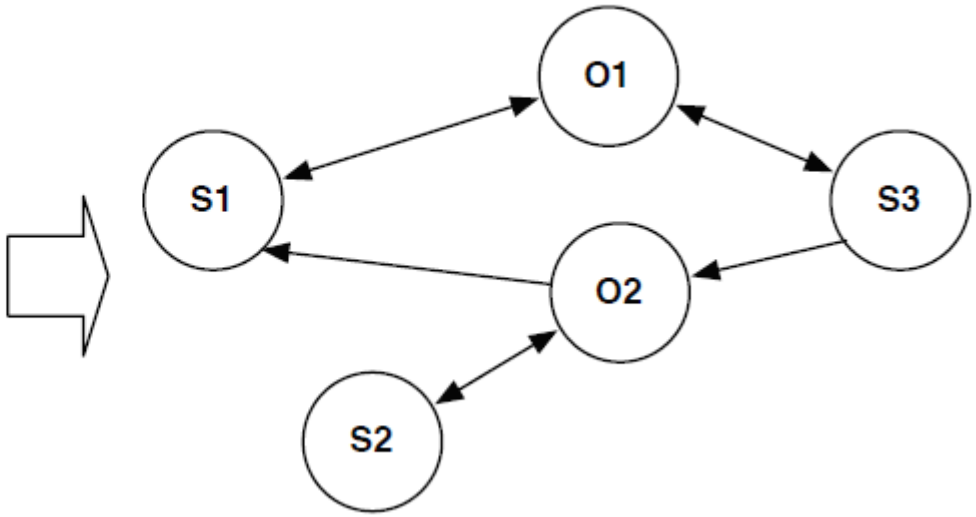
Mô hình luồng thông tin

- Đồ thị luồng thông tin gồm các đỉnh là các chủ thể và đối tượng, các cung biểu diễn các thao tác giữa các chủ thể và đối tượng, chiều thể hiện hướng đi của dữ liệu tới đối tượng hay vào bộ nhớ của chủ thể

Access Matrix

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

Information Flow Graph



Mục tiêu an toàn – Bí mật

- Các cung trong đồ thị biểu diễn toàn bộ các đường dẫn mà dữ liệu có thể bị rò rỉ qua đó.
- Chúng ta 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

Mục tiêu an toàn – Tính toàn vẹn

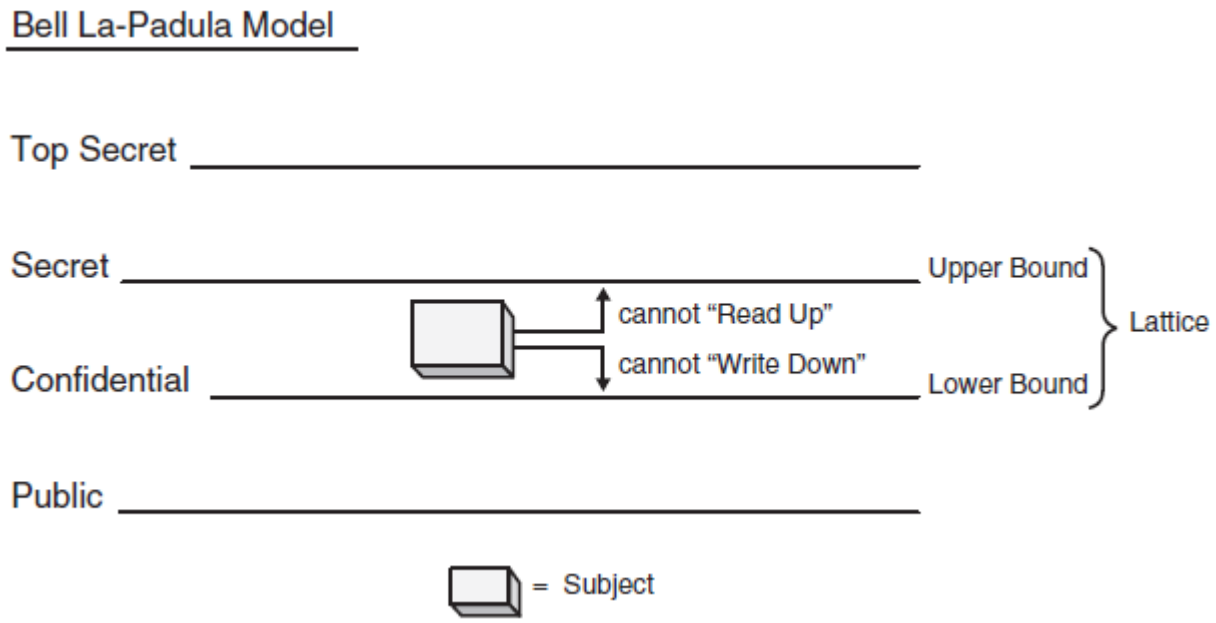
- Không một chủ thể với mức độ toàn vẹn cao lệ thuộc vào bất cứ chủ thể hay đối tượng nào có mức toàn vẹn thấp.
- Chúng ta dùng đồ thị để xác định liệu chủ thể *s1* có nhận đầu vào từ chủ thể *s2* mà có mức độ toàn vẹn thấp hơn không. Nếu có tồn tại một đường dẫn từ *s2* tới *s1* thì không đảm bảo độ toàn vẹn

- Mô hình đảm bảo tính bí mật
  - Bell-La Padula

Mô hình Bell-LaPadula

- Quyền truy nhập được định nghĩa thông qua ma trận truy nhập 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

Mô hình Bell-LaPadula



Mô hình Bell-LaPadula

- Hạn chế cho tính bí mật
- Không có chính sách thay đổi quyền truy nhập
- Chứa kênh ngầm (*covert channel*): đối tượng mức thấp có thể phát hiện sự tồn tại của đối tượng mức cao khi bị từ chối truy nhập

- Mô hình đảm bảo tính toàn vẹn
  - Biba
  - Clark-Winson

Mô hình Biba

- Mô hình này xử lý việc tính toàn vẹn của dữ liệu bị đe dọa khi chủ thể ở mức toàn vẹn thấp có khả năng ghi vào đối tượng có mức toàn vẹn cao hơn và khi chủ thể có thể đọc dữ liệu ở mức thấp
- Biba áp dụng hai quy tắc
  - Không ghi lên: Chủ thể có thể không thể ghi dữ liệu vào đối tượng có mức toang vẹn cao hơn
  - Không đọc xuống: Chủ thể không thể đọc dữ liệu từ mức toàn vẹn thấp hơn

Mô hình Clark-Winson

- Mô hình này tập trung vào việc ngăn chặn người dùng không hợp lệ 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 được thực hiện lên đối tượng và như vậy bảo vệ tính toàn vẹn của đối tượng
- Tính toàn vẹn được dựa trên việc các thủ tục được định nghĩa tường minh và việc tách biệt trách nhiệm

Xây dựng mô hình

- 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 nhập được thực hiện nhờ
  - Định nghĩa các thao tác truy nhập có thể được thực hiện lên từng mục dữ liệu
  - Định nghĩa các thao tác truy nhập 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

Quy định chứng thực

- Thủ tục kiểm tra ban đầu IVP (Initial Verification Procedures) phải đảm bảo các mục dữ liệu hạn chế CDI (Constrained Data Items) ở trạng thái hợp lệ khi IVP chạy
- Thủ tục chuyển đổi TP (Transformation Procedures) phải được chứng thực là hợp lệ tức là CDI bắt buộc phải chuyển đổi thành CDI hợp lệ
- Các luật truy nhập này 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 ky 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

Quy định thực thi (Enforcement rules)

- Bốn quy định thực thi mô tả cơ chế an ninh của hệ thống
  - Hệ thống phải duy trì và bảo vệ danh sách các mục {TP,CDI_i,CDI_j,...} cho phép TP được xác thực truy nhập 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 chạy
  - Hệ thống phải xác thực từng người dùng khi yêu cầu thực hiện TP
  - Chỉ có chủ thể xác thực qui định truy nhập TP mới có thể sửa đổi mục tương ứng trong danh sách. Chủ thể này phải không có quyền thực thi trên TP đó.