Chương 5:
Điều khiển truy cập bắt buộc
Mandatory Access Controls (MAC)

Khoa Khoa học và Kỹ thuật Máy tính
Đại học Bách Khoa Tp.HCM

Nội dung

1. Giới thiệu về điều khiển truy cập bắt buộc
2. Mô hình điều khiển truy cập bắt buộc
3. Case study: Oracle Label Security

Giới thiệu về điều khiển truy cập bắt buộc

- Các lớp bảo mật (security classes)
- Các tính chất của điều khiển truy cập bắt buộc
- Quan hệ đa mức
- Ưu và khuyết điểm của điều khiển truy cập bắt buộc

Giới thiệu về điều khiển truy cập bắt buộc

- ***Điều khiển truy cập bắt buộc (Mandatory Access Control - MAC)***:
  - Được dùng để bảo vệ một khối lượng dữ liệu lớn cần được bảo mật cao trong một môi trường mà *các dữ liệu và người dùng đều có thể được phân loại rõ ràng*.
  - Là cơ chế để hiện thực mô hình bảo mật nhiều mức (multiple level).

Các lớp bảo mật

- Người dùng và dữ liệu được phân loại dựa theo các lớp bảo mật (security classes).
- Phân loại **người dùng** dựa theo mức **độ tin cậy** và lĩnh vực hoạt động của người dùng.
- Phân loại **dữ liệu** dựa theo mức **độ nhạy cảm** và lĩnh vực của dữ liệu
- Lớp bảo mật có thể được phân loại theo
  - Mức bảo mật (Classification level)
  - Lĩnh vực (Category)

Mức bảo mật

- Các mức bảo mật cơ bản:
  - Top secret (TS)
  - Secret (S)
  - Confidential (C)
  - Unclassified (U)
- Trong đó TS là mức cao nhất và U là mức thấp nhất:

  TS > S > C > U
- Người dùng ở **cấp càng cao** thì mức độ đáng **tin cậy càng lớn**.
- Dữ liệu ở **cấp càng cao** thì **càng nhạy cảm** và cần được bảo vệ nhất.

Lĩnh vực

- Phân loại người dùng và dữ liệu theo lĩnh vực hoạt động của hệ thống, hoặc theo từng phòng ban trong một tổ chức.
- Ví dụ: Một công ty có 3 phòng ban là: Phòng kinh doanh, phòng sản xuất và phòng phân phối. Như vậy thì các người dùng và dữ liệu trong công ty này có thể được phân loại theo lĩnh vực dựa theo 3 phòng ban này.

Lớp bảo mật

- Một lớp bảo mật (security class) được định nghĩa như sau:

  SC = (A, C)

  A: mức bảo mật

  C: lĩnh vực

- Hai lớp bảo mật **SC** và **SC'** có mối quan hệ *thứ tự riêng phần* **SC ≤ SC'** nếu: **A ≤ A'** và **C ⊆ C'**
- Ví dụ:
  - (C, {Sales}) ≤ (S, {Sales, Production})
  - ~~(C, {Sales, Production}) ≤ (S, {Sales})~~

Giới thiệu về điều khiển truy cập bắt buộc

- Các lớp bảo mật
- **Các tính chất của điều khiển truy cập bắt buộc**
- Quan hệ đa mức
- Ưu và khuyết điểm của điều khiển truy cập bắt buộc

Các tính chất của điều khiển truy cập bắt buộc

- ***Tính chất bảo mật đơn giản (Simple security property or ss-property)***: Một chủ thể *s* không được phép ĐỌC đối tượng *o*, trừ khi:

$$\textbf{class}(s) \geq \textbf{class}(o)$$

→ *Không đọc lên (No read-up)*

- ***Tính chất sao (Star property or *-property)***: Một chủ thể *s* không được phép GHI lên đối tượng *o*, trừ khi:

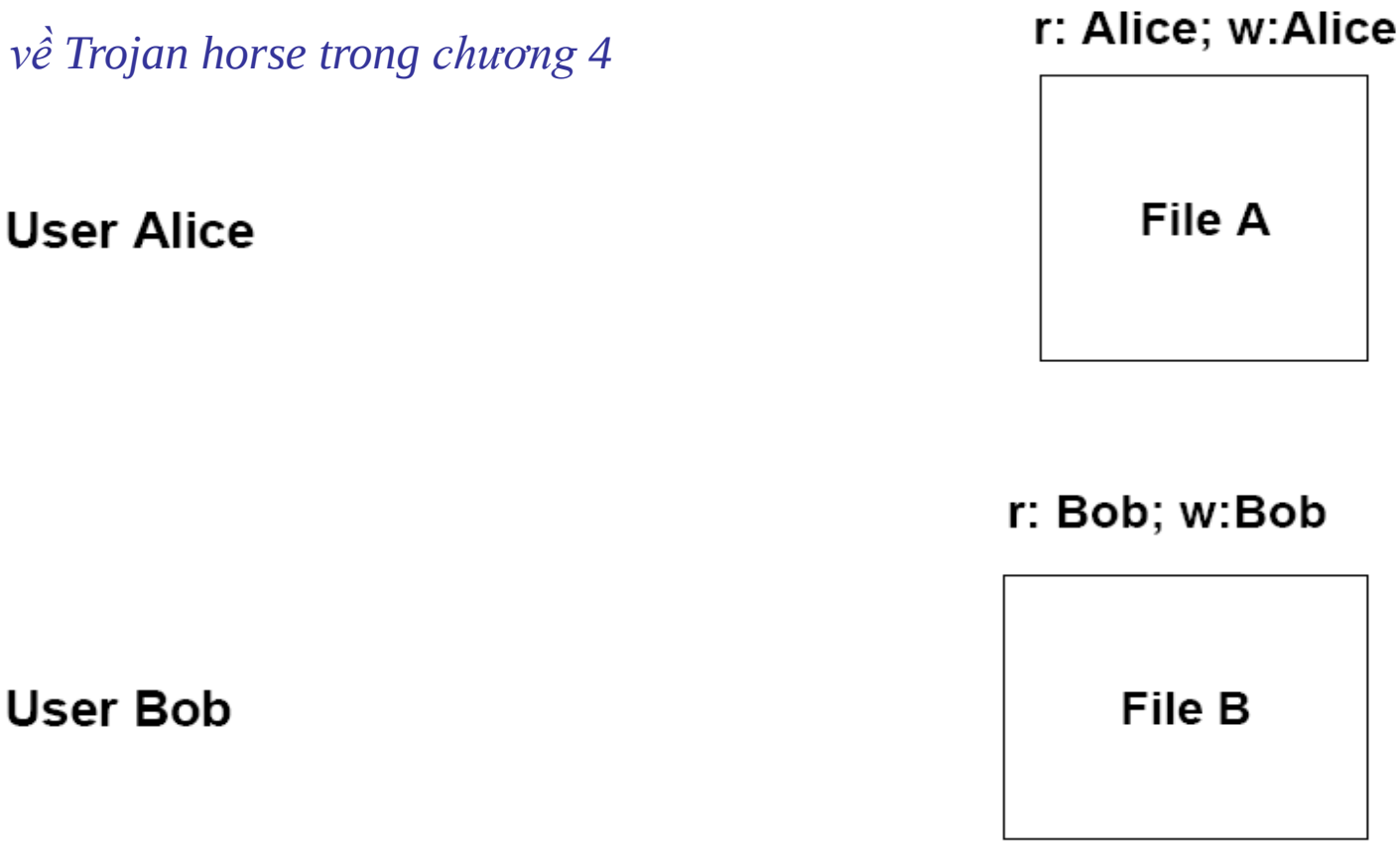
$$\textbf{class}(s) \leq \textbf{class}(o)$$

→ *Không ghi xuống (No write-down)*

Những tính chất này nhằm đảm bảo rằng không có dòng thông tin nào có thể đi từ lớp cao xuống lớp thấp!!!

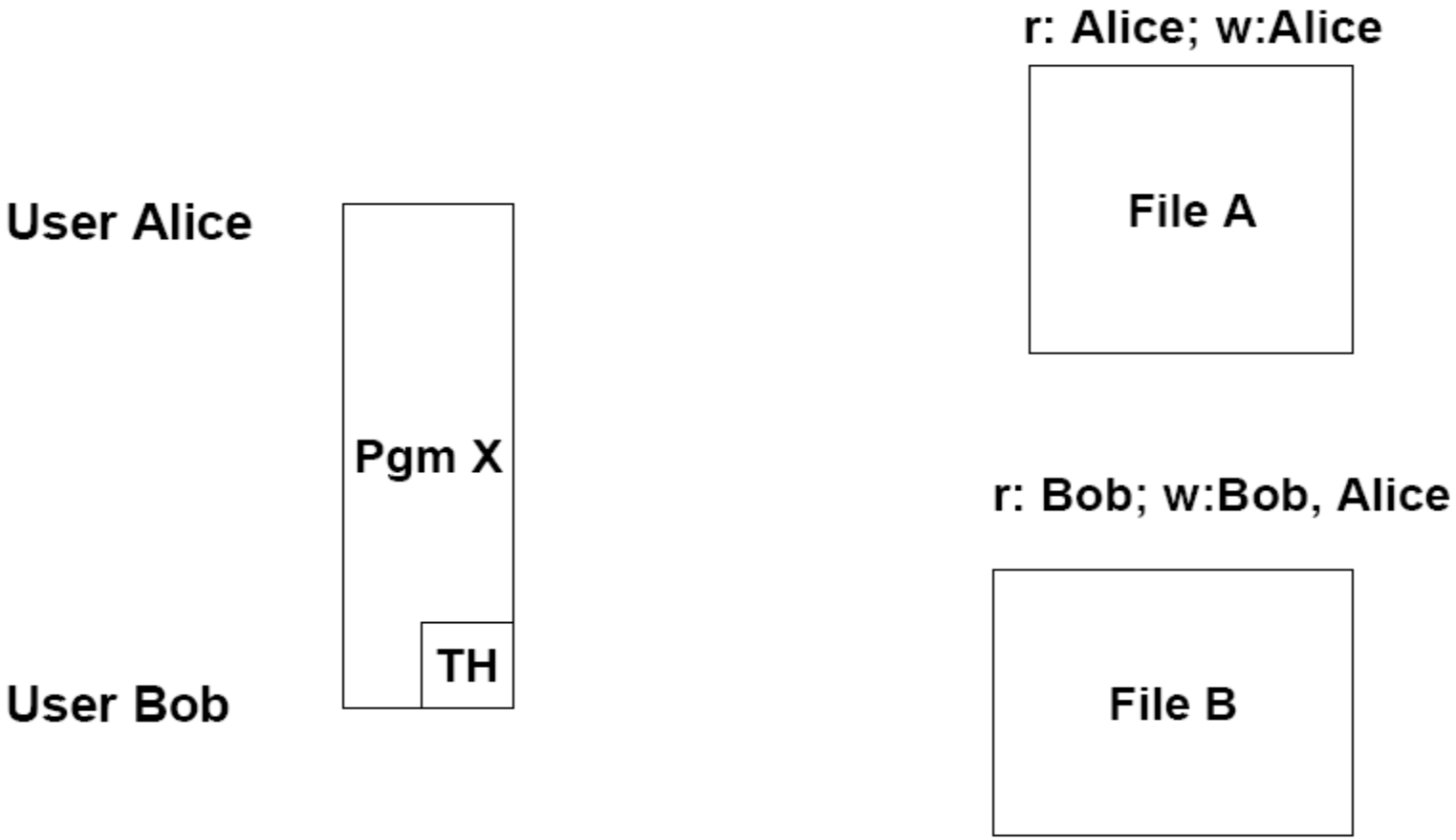
Tại sao có tính chất *

Ví dụ về Trojan horse trong chương 4

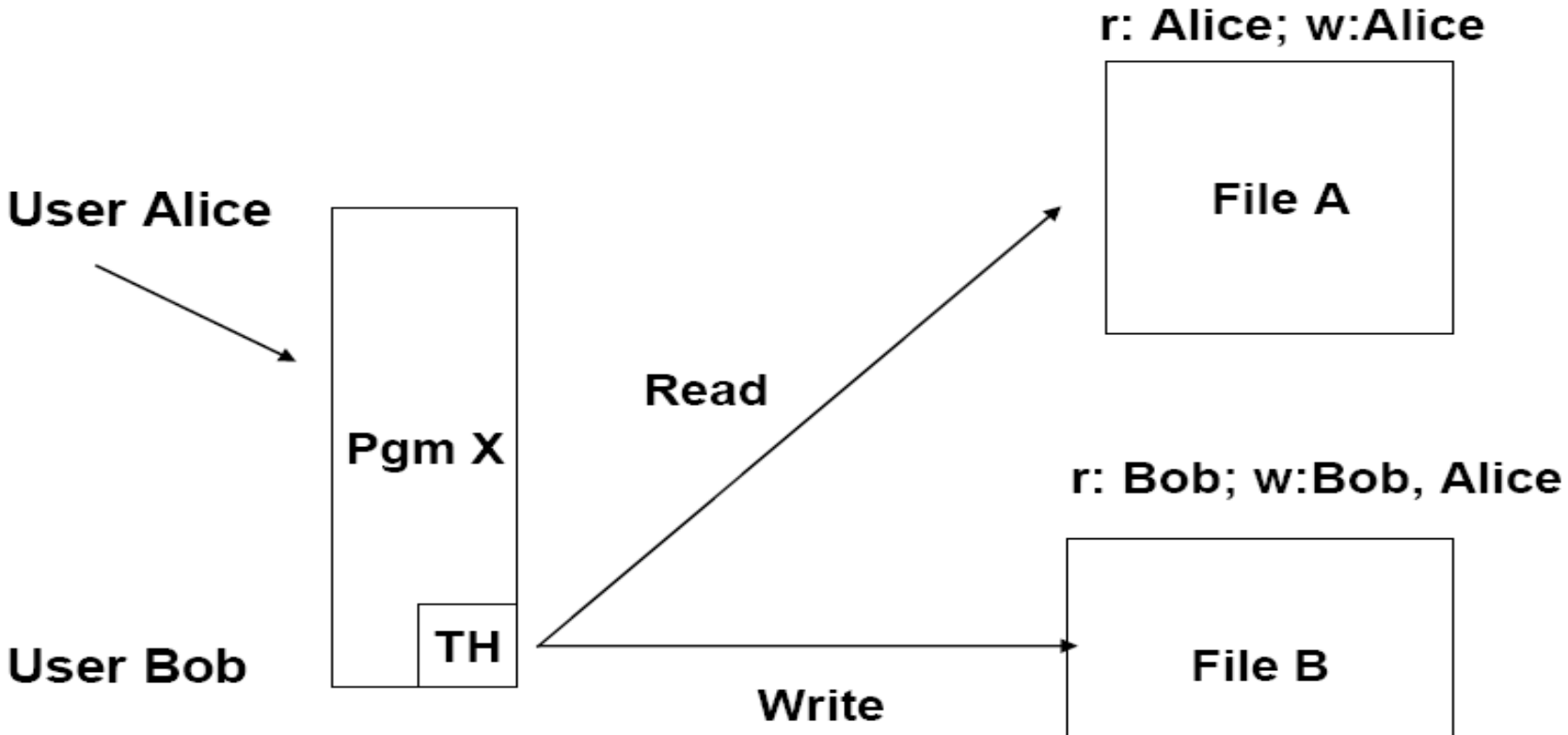


Bob không thể đọc được nội dung của file A

Tại sao có tính chất *

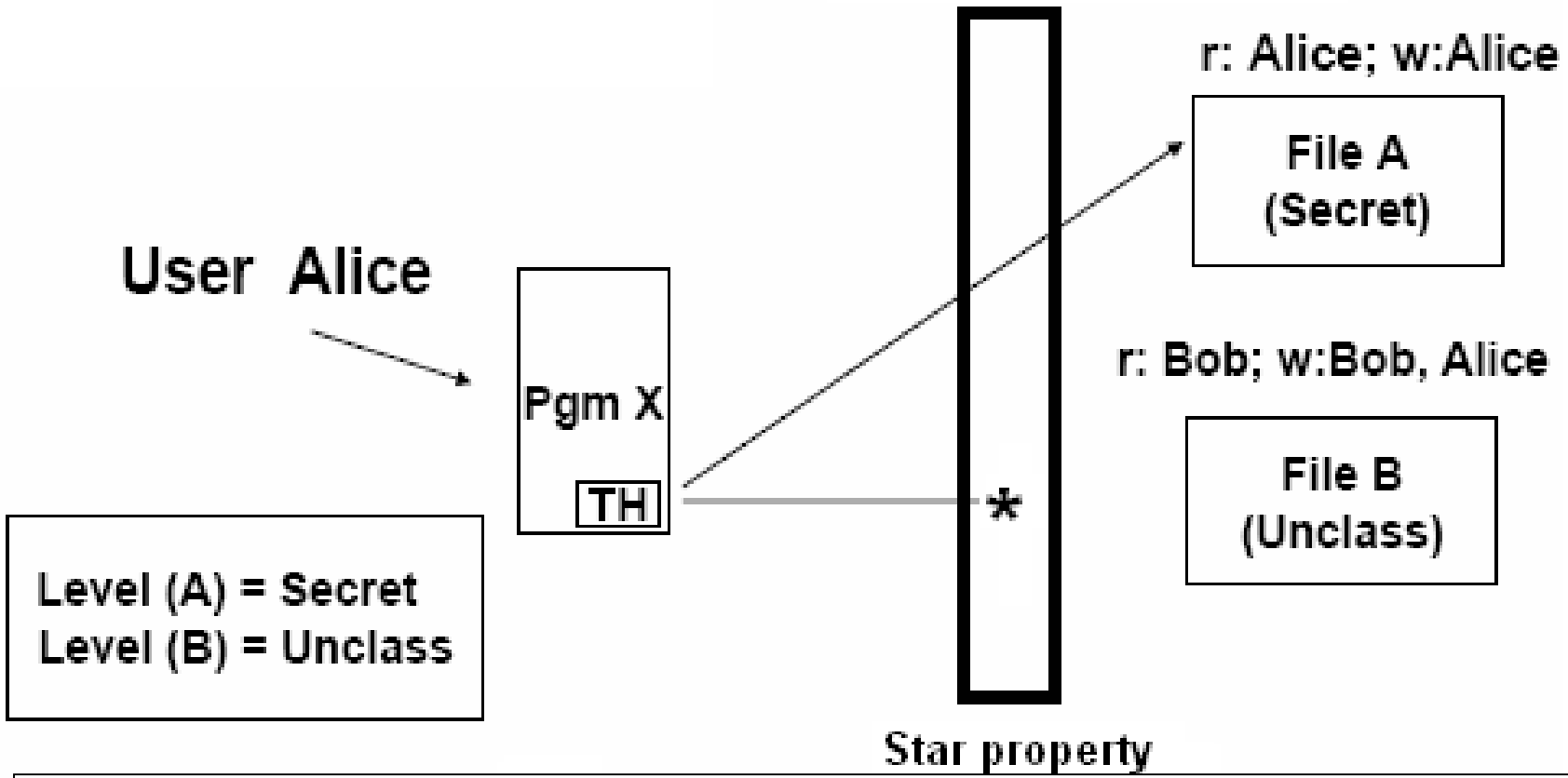


Tại sao có tính chất *



Bob có thể đọc được nội dung của file A sau khi nó được sao chép sang file B

Tại sao có tính chất *



Tính chất * ngăn chặn việc sao chép dữ liệu từ file (cấp cao hơn) sang file B (cấp thấp hơn)

Tính chất *

- ***Tính chất ****: ngăn chặn một chủ thể ở lớp bảo mật cao gửi thông điệp hợp lệ đến những chủ thể ở lớp bảo mật thấp hơn
- Có 2 giải pháp:
  - Tạm thời giảm lớp bảo mật của chủ thể đó xuống cấp thấp hơn khi gửi thông điệp
  - Đưa các chủ thể đáng tin cậy (trusted subject) vào danh sách các chủ thể không bị hạn chế bởi tính chất *

Giới thiệu về điều khiển truy cập bắt buộc

- Các lớp bảo mật
- Các tính chất của điều khiển truy cập bắt buộc
- **Quan hệ đa mức**
- Ưu và khuyết điểm của điều khiển truy cập bắt buộc

Quan hệ đa mức

- ***Quan hệ đa mức (Multilevel relation)***: MAC + mô hình CSDL quan hệ
- ***Các đối tượng dữ liệu***: thuộc tính và hàng
- Mỗi thuộc tính A_i được gắn với 1 thuộc tính **mức bảo mật** C_i
- Mỗi hàng có 1 thuộc tính **mức bảo mật chung** cho hàng đó *TC*. *TC* sẽ mang giá trị **cao nhất** của các *Ci* trong hàng đó.

$$\mathbf{R(A_1, C_1, A_2, C_2, \ldots, A_n, C_n, TC)}$$

- ***Khóa biểu kiến (apparent key)*** của một quan hệ đa mức là tập các thuộc tính mà sẽ tạo thành khóa chính như trong một quan hệ bình thường (single-level relation) (bỏ các thuộc tính mức bảo mật)

Quan hệ đa mức

EMPLOYEE

S < C < U

Name		Salary		JobPerformance		TC
Smith	U	40000	C	Fair	S	S
Brown	C	80000	S	Good	C	S

- Những chủ thể (người dùng) ở các **mức bảo mật khác nhau** sẽ thấy những **dữ liệu khác nhau** trong cùng một quan hệ đa mức.

Quan hệ đa mức

SELECT * FROM EMPLOYEE

EMPLOYEE

Name		Salary		JobPerformance		TC
Smith	U	40000	C	Fair	S	S
Brown	C	80000	S	Good	C	S

- Kết quả trả về cho người dùng ở **mức bảo mật S**

EMPLOYEE

Name		Salary		JobPerformance		TC
Smith	U	40000	C	Fair	S	S
Brown	C	80000	S	Good	C	S

Quan hệ đa mức

SELECT * FROM EMPLOYEE

EMPLOYEE

Name		Salary		JobPerformance		TC
Smith	U	40000	C	Fair	S	S
Brown	C	80000	S	Good	C	S

- Kết quả trả về cho người dùng ở **mức bảo mật C**

EMPLOYEE

Name		Salary		JobPerformance		TC
Smith	U	40000	C	null	C	C
Brown	C	null	C	Good	C	C

Quan hệ đa mức

SELECT * FROM EMPLOYEE

EMPLOYEE

Name		Salary		JobPerformance		TC
Smith	U	40000	C	Fair	S	S
Brown	C	80000	S	Good	C	S

- Kết quả trả về cho người dùng ở **mức bảo mật U**

EMPLOYEE

Name		Salary		JobPerformance		TC
Smith	U	null	U	null	U	U

Tính chất của quan hệ đa mức

- Tính chất đọc và ghi
- Tính toàn vẹn thực thể (Entity integrity)
- Tính toàn vẹn giá trị *null* (Null integrity)
- Tính đa thể hiện (Polyinstantiation)

Tính chất của quan hệ đa mức

- **Không đọc lên (No read up)**
- **Không ghi xuống (No write down)**

  → Tính chất cơ bản của MAC

Tính chất của quan hệ đa mức

- ***Tính toàn vẹn thực thể (Entity integrity)***: Tất cả các thuộc tính nằm trong khóa biểu kiến không được *null* và phải ở cùng mức bảo mật trong mỗi hàng.
- Tất cả các thuộc tính khác trong cùng một hàng phải có mức bảo mật lớn hơn hoặc bằng mức bảo mật của khóa biểu kiến.

  → Ràng buộc này đảm bảo rằng một người dùng sẽ thấy được khóa của một hàng nếu người dùng được phép xem bất kỳ phần nào của hàng đó.

Tính chất của quan hệ đa mức

- ***Tính toàn vẹn giá trị null (Null integrity)***: Tất cả các giá trị *null* đều được phân loại ở mức bảo mật bằng với mức bảo mật của khóa biểu kiến trong cùng một hàng

  → Ràng buộc này đảm bảo sự thống nhất giữa các thể hiện khác nhau (instance) của cùng một quan hệ khi nó xuất hiện ở các mức bảo mật khác nhau.

Tính chất của quan hệ đa mức

- ***Tính đa thể hiện (Polyinstantiation)***: xảy ra khi có những hàng có cùng khóa biểu kiến nhưng mang những giá trị khác nhau đối với những người dùng ở các mức bảo mật khác nhau.

Ví dụ về tính đa thể hiện

SELECT * FROM EMPLOYEE

EMPLOYEE

Name		Salary		JobPerformance		TC
Smith	U	40000	C	Fair	S	S
Brown	C	80000	S	Good	C	S

- Kết quả trả về cho người dùng ở **cấp bảo mật C**

EMPLOYEE

Name		Salary		JobPerformance		TC
Smith	U	40000	C	null	C	C
Brown	C	null	C	Good	C	C

Ví dụ về tính đa thể hiện

EMPLOYEE

Name		Salary		JobPerformance		TC
Smith	U	40000	C	null	C	C
Brown	C	null	C	Good	C	C

- Một người dùng ở mức bảo mật C thực hiện câu lệnh cập nhật giá trị của JobPerformance của Smith thành 'Excellent':

```
UPDATE EMPLOYEE
SET JobPerformance = 'Excellent'
WHERE Name = 'Smith';
```

Thực hiện câu lệnh hay báo lỗi?

Ví dụ về tính đa thể hiện

- Kết quả của câu truy vấn:
  - Name là khóa biểu kiến trong quan hệ Employee
  - Tồn tại 2 hàng có cùng khóa biểu kiến

EMPLOYEE

Name		Salary		JobPerformance		TC
Smith	U	40000	C	Fair	S	S
Smith	U	40000	C	Excellent	C	C
Brown	C	80000	S	Good	C	S

Giới thiệu về điều khiển truy cập bắt buộc

- Các lớp bảo mật
- Các tính chất của điều khiển truy cập bắt buộc
- Quan hệ đa mức
- **Ưu và khuyết điểm của điều khiển truy cập bắt buộc**

Ưu và khuyết điểm của MAC

- ***Ưu điểm:***
  - Là cơ chế điều khiển truy xuất có tính bảo mật cao trong việc ngăn chặn dòng thông tin bất hợp pháp.
  - Thích hợp cho các ứng dụng trong môi trường quân đội.
- ***Khuyết điểm:***
  - Không dễ áp dụng: đòi hỏi cả người dùng và dữ liệu phải được phân loại rõ ràng
  - Chỉ được ứng dụng trong một số ít môi trường.

Nội dung

1. Giới thiệu về điều khiển truy cập bắt buộc
2. Mô hình điều khiển truy cập bắt buộc
3. Case study: Oracle Label Security

Mô hình điều khiển truy cập bắt buộc

- Mô hình Bell-LaPadula
- Mô hình Biba

Mô hình Bell-LaPadula

- Được phát triển bởi David Elliot Bell và Leonard J. La Padula vào năm 1973.
- Để chuẩn hóa các qui định về hệ thống bảo mật nhiều mức (multilevel security system – MLS) của bộ quốc phòng Mỹ
- Áp dụng trong các ứng dụng quân đội và chính phủ

Mô hình Bell-LaPadula

- Trạng thái của hệ thống:

  $v = (b, M, f)$

- ***b:*** tập các truy cập hiện tại
  - Các loại quyền truy cập (access mode): chỉ đọc (read-only), nối (append), thực thi (excecute), đọc-ghi (read-write)
  - $b = \langle subject, object, access\ mode \rangle = \langle s, o, m \rangle$: chủ thể s đang có quyền truy cập m trên o
- ***M[s, o]:*** ma trận truy cập
  - Tương tự như trong mô hình ma trận truy cập

Bell-LaPadula model

- Trạng thái của hệ thống:

  (b, M, f)

- ***f:*** hàm xác định mức bảo mật của chủ thể/đối tượng
  - $f: O \cup S \rightarrow L$
  - $f_o(o)$: trả về mức bảo mật của đối tượng *o*
  - $f_s(s)$: trả về mức bảo mật của chủ thể *s*
  - $f_c(s)$: trả về mức bảo mật *hiện tại* của chủ thể *s*
  - $f_c(s) \leq f_s(s)$

Tính chất bảo mật đơn giản (ss-property)

- ***Không đọc lên (No read up)***
- Một trạng thái hệ thống $v = (b, M, f)$ thỏa mãn tính chất bảo mật đơn giản khi và chỉ khi:

  Với mỗi $M[s,o]$: $M[s,o] \in \{\textbf{read}, \textbf{write}\}$, $\boldsymbol{f_o(o) \leq f_s(s)}$

Tính chất *

- ***Không ghi xuống (No write down)***
- Một trạng thái hệ thống $v = (b, M, f)$ thỏa mãn tính chất * khi và chỉ khi:
  - $append \in M[s,o] \rightarrow f_c(s) \leq f_o(o)$
  - $write \in M[s,o] \rightarrow f_c(s) = f_o(o)$
  - $read \in M[s,o] \rightarrow f_c(s) \geq f_o(o)$

Hạn chế của mô hình Bell-LaPadula:

- Mô hình Bell-LaPadula chỉ tập trung vào tính mật
  - Không đảm bảo tính toàn vẹn thông tin
- Không linh động trong việc thay đổi quyền truy cập.
- Mô hình Bell-LaPadula không chặn được convert channel:
  - Không hỗ trợ tính đa thể hiện
  - Một chủ thể ở mức bảo mật thấp có thể phát hiện được sự hiện diện của một đối tượng ở mức bảo mật cao khi chủ thể đó truy xuất đến đối tượng và bị từ chối

Mô hình điều khiển truy cập bắt buộc

- Mô hình Bell-LaPadula
- **Mô hình Biba**

Mô hình Biba

- Do Biba đề nghị năm 1977
- Mô hình Biba tập trung vào việc **bảo vệ tính toàn vẹn** của dữ liệu
- Mô hình Biba phân loại chủ thể, đối tượng theo mức toàn vẹn *(integrity level)*
- Các nhóm phân loại gồm:
  - Crucial (C)
  - Very Important (VI)
  - Important (I)

  C > VI > I

Mô hình Biba

- Quyền truy xuất (access mode):
  - Chỉnh sửa (modify): ghi thông tin lên đối tượng
  - Liên hệ (invoke): quyền giữa 2 chủ thể, cho phép 2 chủ thể liên lạc với nhau
  - Quan sát (observe): đọc thông tin của đối tượng
  - Thực thi (execute): thực thi chương trình

Chính sách toàn vẹn

- ***Tính chất toàn vẹn đơn giản (Simple integrity property)***: một chủ thể *s* có thể *quan sát* được đối tượng *o* nếu và chỉ nếu:

$$i(s) \leq i(o)$$

→ *Không đọc xuống (No read down)*

i(s): mức toàn vẹn của *s*
i(o): mức toàn vẹn của *o*

- ***Tính chất toàn vẹn sao (Integrity star property)***: một chủ thể *s* có thể *chỉnh sửa* được đối tượng *o* nếu và chỉ nếu:

$$i(o) \leq i(s)$$

→ *Không ghi lên (No write up)*

Chính sách toàn vẹn

- ***Tính chất liên hệ (Invocation property)***: một chủ thể s_1 có thể *liên hệ* với chủ thể s_2 nếu và chỉ nếu:

$$i(s_2) \leq i(s_1)$$

Mô hình Biba

- Mô hình Biba bảo vệ tính **toàn vẹn** và không cung cấp **tính mật** nên cần kết hợp với những mô hình khác.
- Mô hình Lipner là mô hình kết hợp giữa mô hình Bell-LaPadula và mô hình Biba.

Nội dung

1. Giới thiệu về điều khiển truy cập bắt buộc
2. Mô hình điều khiển truy cập MAC
3. Case study: Oracle Label Security

Oracle Label Security

- Giới thiệu về Oracle Label Security (OLS)
- Các thành phần của nhãn (label)
- Cách thức hoạt động của OLS
- Ví dụ: "Order Management"

Tài liệu tham khảo: D.C. Knox (2004). ***Effective Oracle Database 10g Security by Design***, Oracle Press, ISBN 0-07-223130-0.

Giới thiệu về OLS

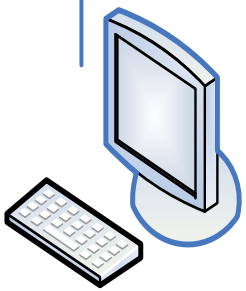
- Mô phỏng mô hình **quan hệ đa mức**
- Mỗi hàng dữ liệu được bổ sung thêm một trường **"nhãn nhạy cảm" (sensity label)** để lưu lại mức độ nhạy cảm của dữ liệu trong hàng đó.
- Quyền truy cập được xét (cho phép hoặc không) dựa vào việc so sánh danh định của người dùng, mức bảo mật của người dùng và nhãn nhạy cảm của mỗi hàng

Giới thiệu về OLS

SELECT * FROM order;

Table ORDER

Order Number	Order Location	**Row Label**
1	City	Unclassified
2	VIP	Secret
3	City	Unclassified
4	VIP	Top Secret
4	VIP	Top Secret



User
User session label
"Unclassified"

Oracle Label Security

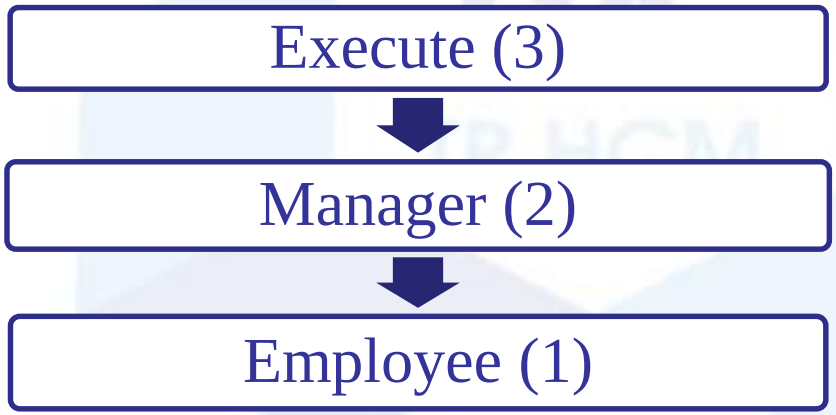
- Giới thiệu về Oracle Label Security (OLS)
- **Các thành phần của nhãn (label)**
- Cách thức hoạt động của OLS
- Ví dụ: "Order Management"

Các thành phần của nhãn

- Mỗi nhãn chứa 3 loại thành phần (component):
  - *Mức nhạy cảm (sensitivity level):* mỗi nhãn có **1** mức nhạy cảm
  - *Ngăn (horizontal compartments):* mỗi nhãn có từ **0 đến nhiều** ngăn
  - *Nhóm (hierarchical groups):* mỗi nhãn có từ **0 đến nhiều** nhóm

Mức nhạy cảm (sensitivity level)

- Mức nhạy cảm thể hiện mức độ nhạy cảm của dữ liệu hoặc mức độ bảo mật của người dùng.
- Mức nhạy cảm của dữ liệu càng cao thì càng cần phải bảo vệ. Mức nhạy cảm của người dùng càng thấp thì càng cần phải hạn chế quyền của người dùng đó.
- Mức nhạy cảm có quan hệ thứ bậc (hierachical)
- Ví dụ:

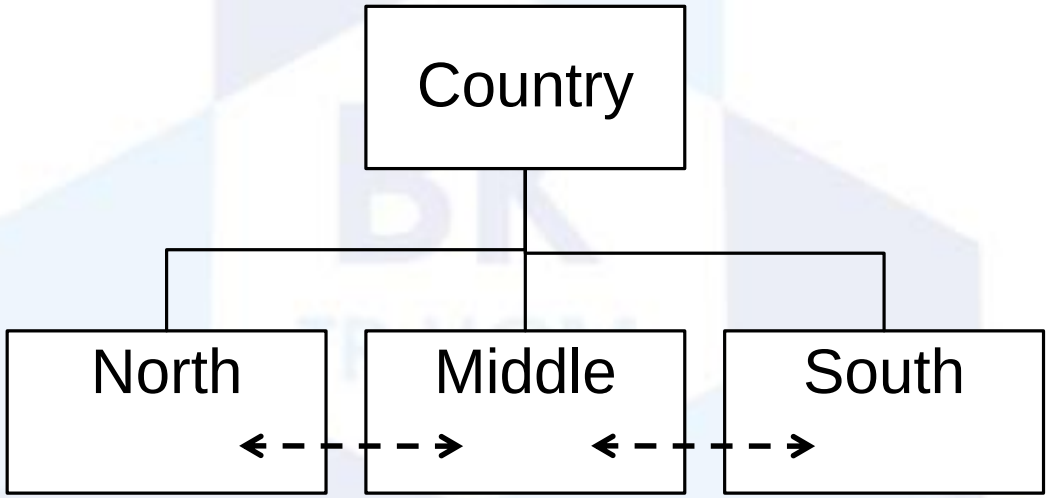


Ngăn (Compartment)

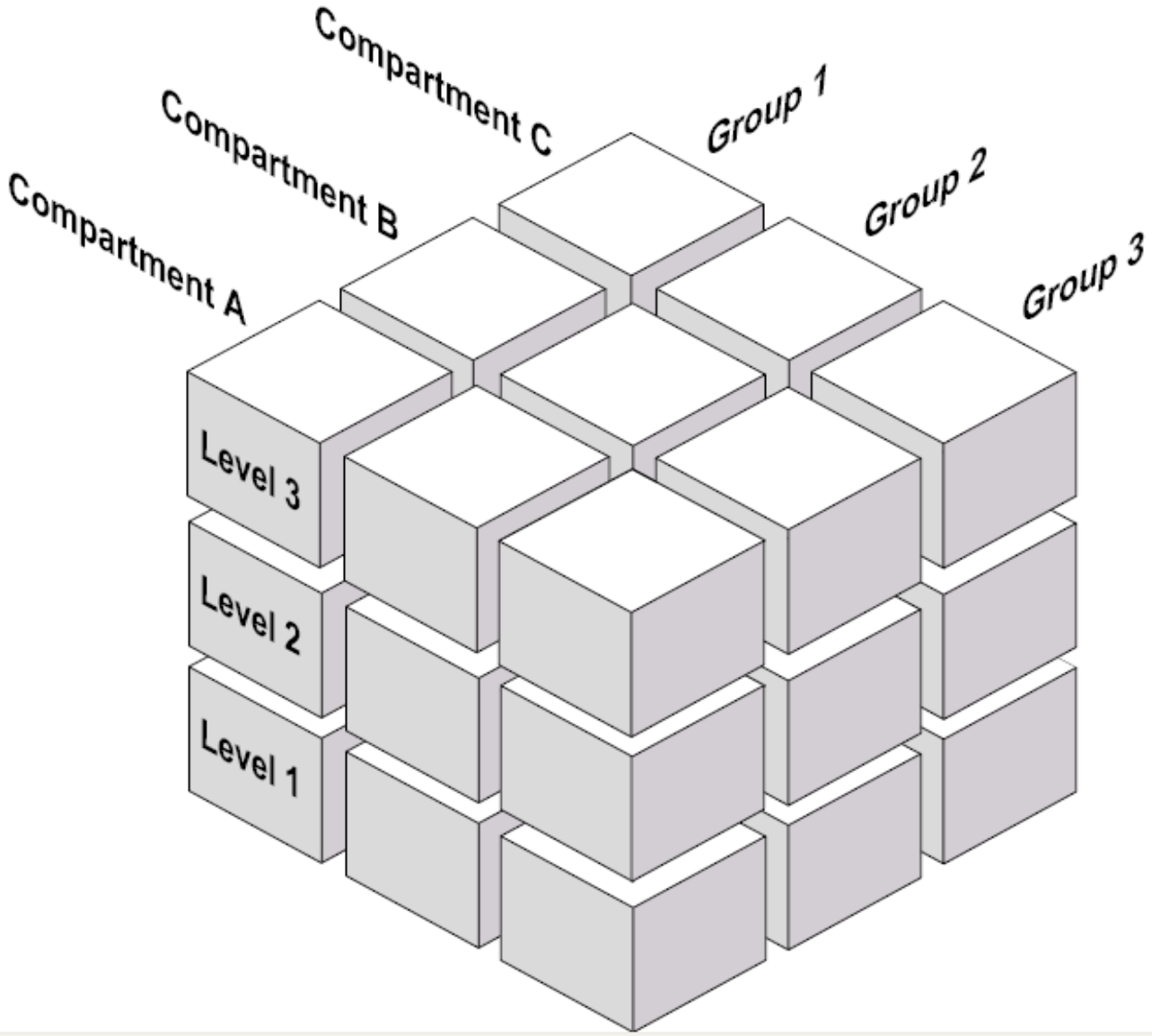
- Compartment định nghĩa các lĩnh vực liên quan đến dữ liệu.
- Thành phần compartment không có mối quan hệ thứ bậc mà là quan hệ chứa/bao gộp (tập hợp)
- Ví dụ:
  - FOOD
  - CLOTHS
  - ELECTRICAL GOODS

Nhóm (group)

- Thành phần group định nghĩa cách tổ chức dữ liệu.
- Giữa các thành phần group có mối quan hệ (so sánh) cha-con
- Ví dụ:



Các thành phần của nhãn



Cú pháp viết nhãn

- Cú pháp:

  LEV : COM_1, ..., COM_n : GRP1, ..., GRPn

- Ví dụ:
  - MGR:CS:NA
  - EXEC:CS,ES,FS:NA

Level:
MGR: Manager
EXEC: Executive

Compartment:
CS: Cloths
ES: Electrical Goods
FS: Food

Group:
NA: North

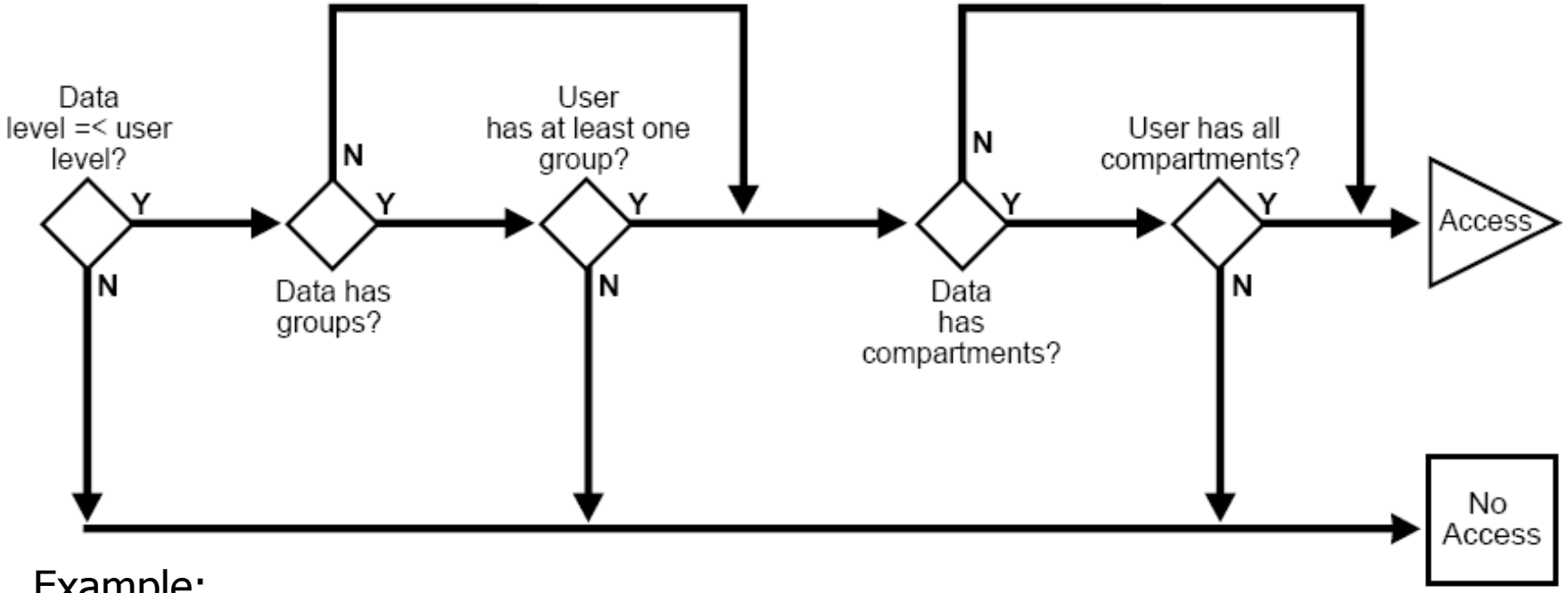
Oracle Label Security

- Giới thiệu về Oracle Label Security (OLS)
- Các thành phần của nhãn (label)
- **Cách thức hoạt động của OLS**
- Ví dụ: "Order Management"

Quản lý truy cập

- Một người dùng chỉ có thể truy cập dữ liệu nằm trong phạm vi quy định của nhãn nhạy cảm của mình
- Một người dùng có:
  - mức nhạy cảm cao nhất và thấp nhất
  - tập các compartment
  - tập các group
  - Một bản đặc tả các quyền truy cập (đọc/ghi) cho mỗi compartment và group
- Cách so sánh nhãn của người dùng với nhãn của dữ liệu?

Truy cập ĐỌC



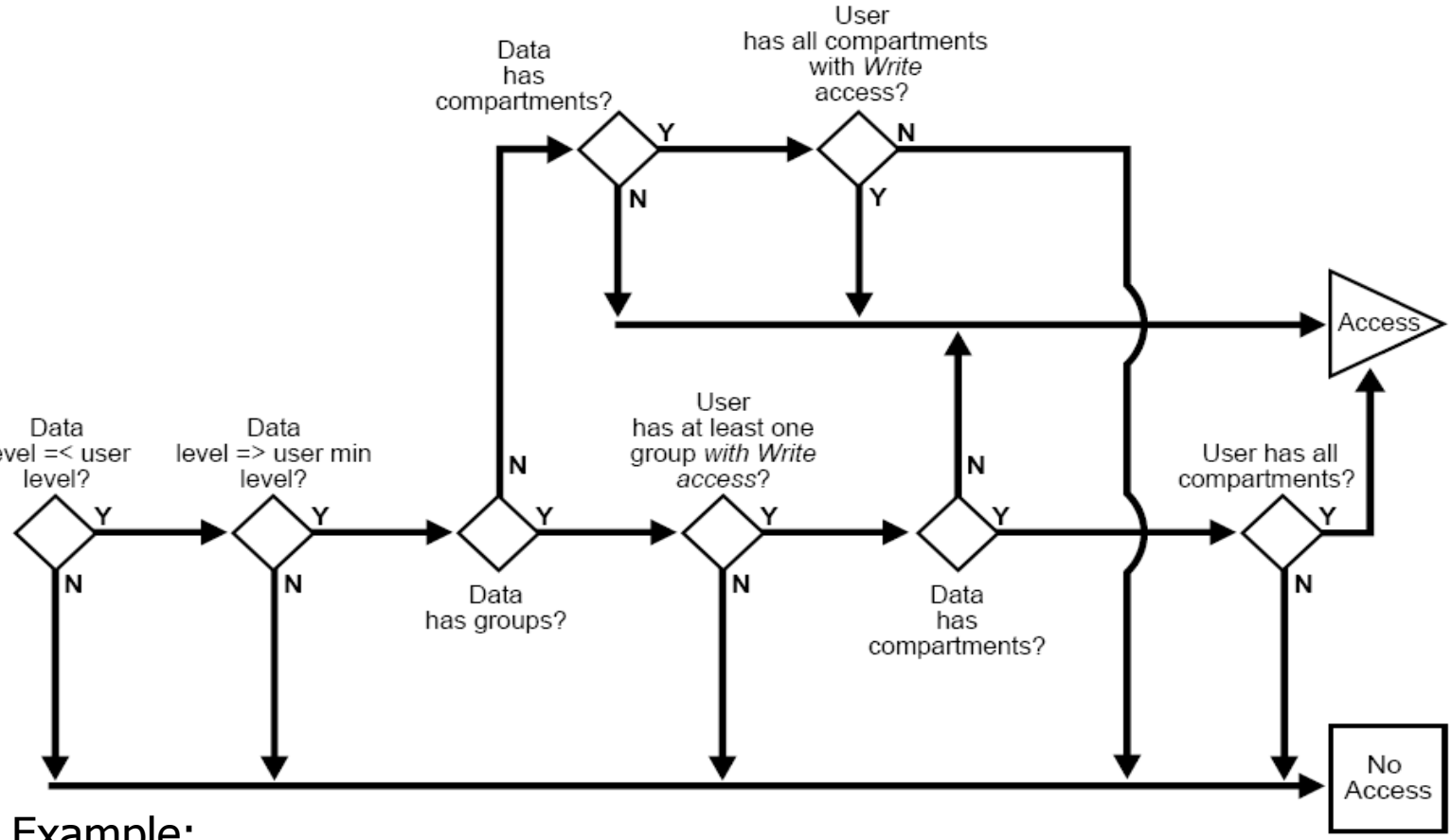
Example:

Data Label:

1	Quoc	MGR:CS:NA
2	Thai	MGR:FS:MA
3	Dan	EMP:CS:NA
4	An	EMP

User label: MGR:CS:NA
User label: EMP:FS:NA
User label: EMP:NA

Truy cập GHI



Example:

Data Label:

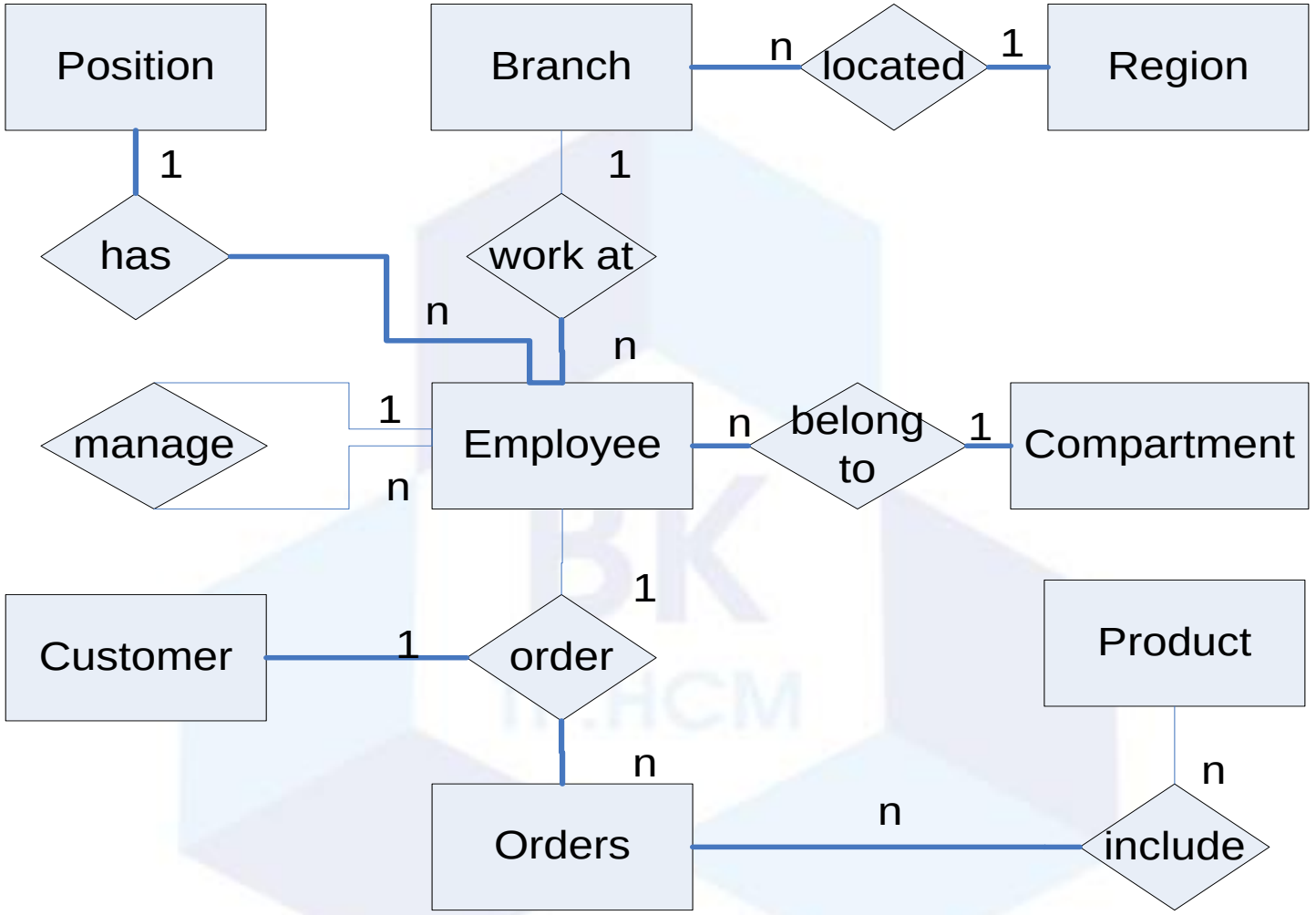
1	Quoc	MGR:CS:NA
2	Thai	MGR:FS:MA
3	Dan	EMP:CS:NA
4	An	EMP

User label: MGR:CS:NA
User label: EMP:FS:NA
User label: EMP:NA

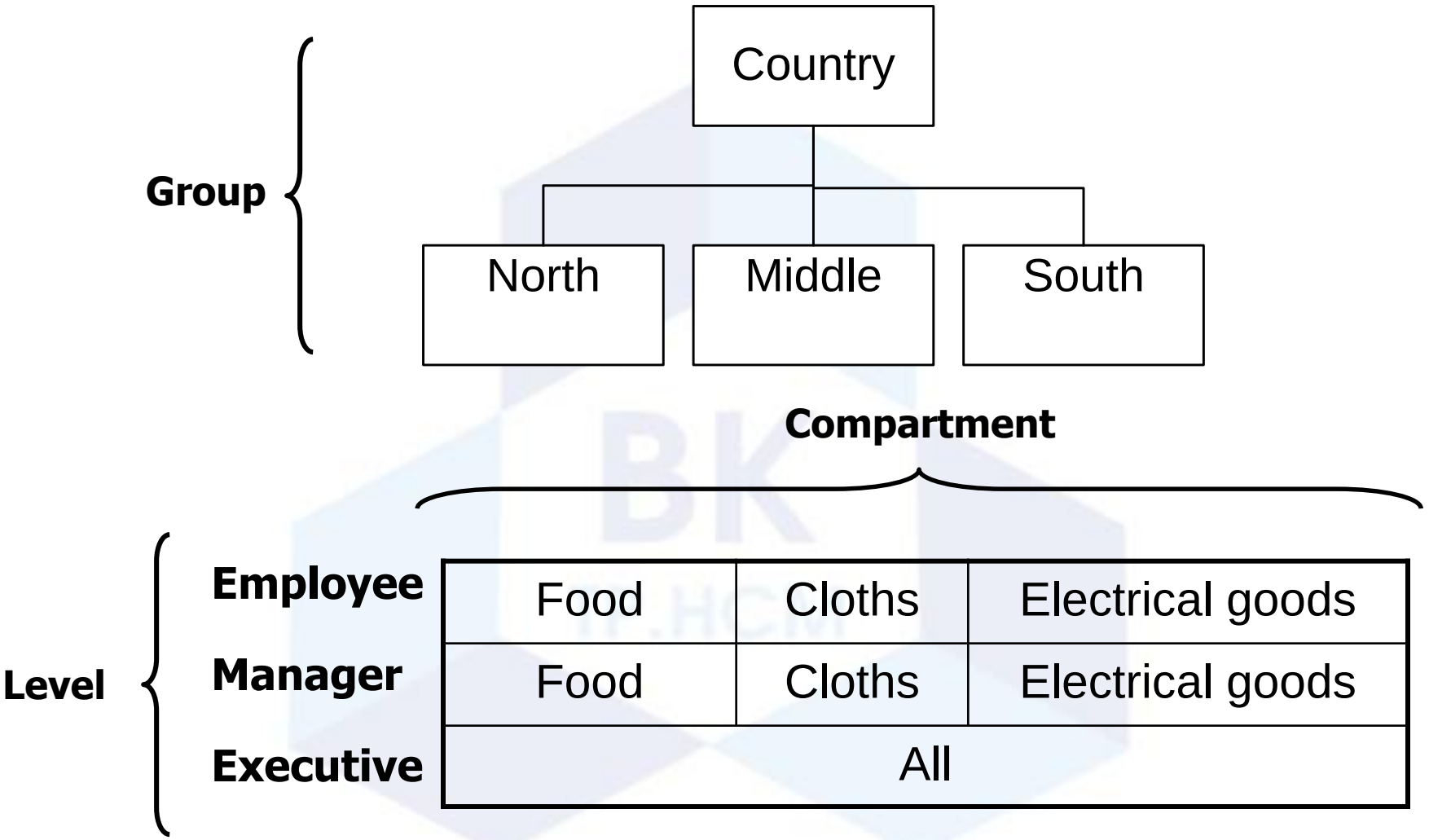
Oracle Label Security

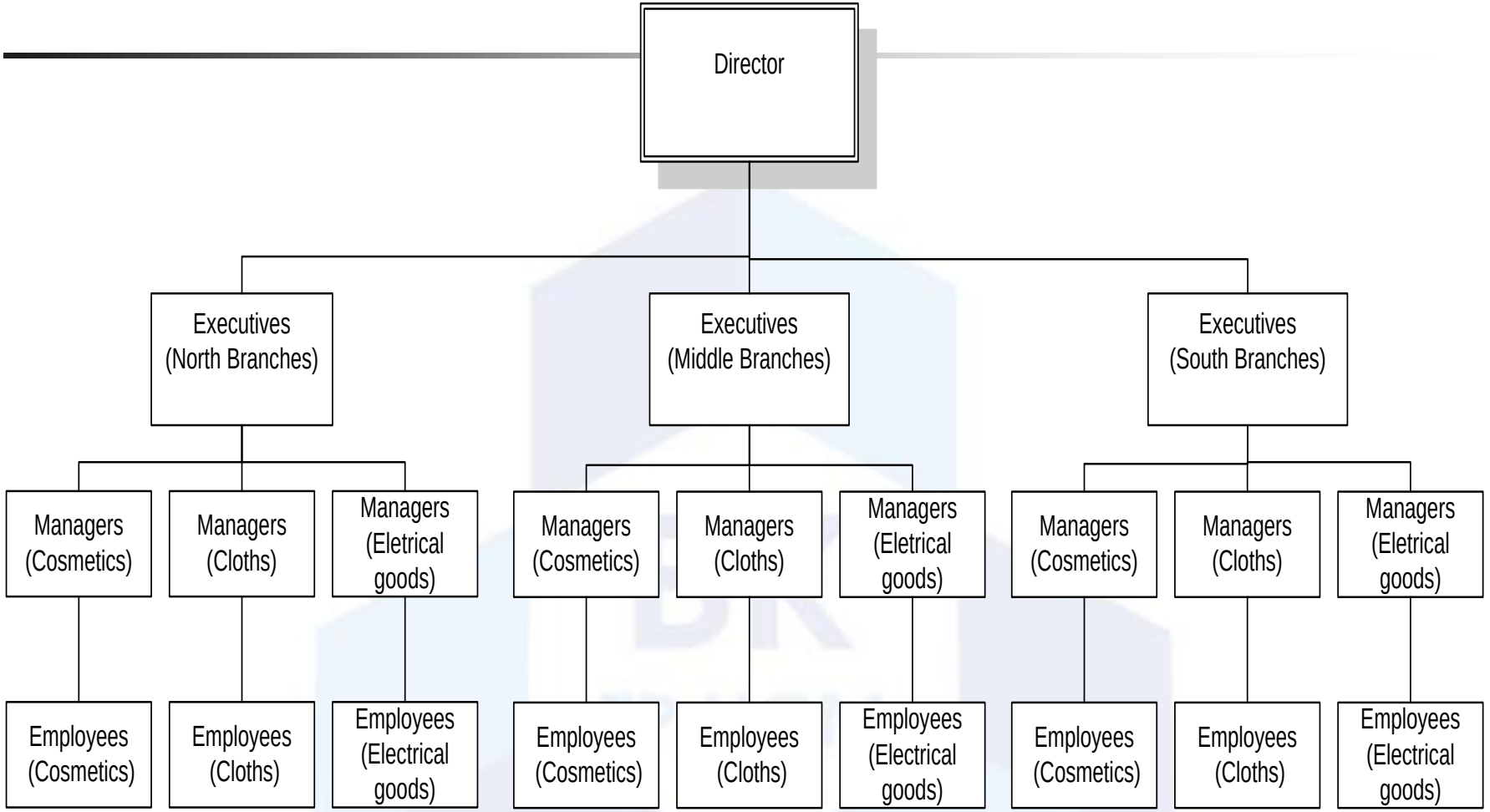
- Giới thiệu về Oracle Label Security (OLS)
- Các thành phần của nhãn (label)
- Cách thức hoạt động của OLS
- **Ví dụ: "Order Management"**

Project "Order Management"



Project "Order Management"





Cần bảo vệ đơn hàng (ORDERS) và thông tin cá nhân

Nội dung

1. Giới thiệu về điều khiển truy cập bắt buộc
2. Mô hình điều khiển truy cập bắt buộc
3. Case study: Oracle Label Security