

Security

Security & Integrity

- Security เป็นการทำให้แน่ใจว่า users ได้รับอนุญาตให้ทำในสิ่งที่กำลังพยายามทำอยู่
- Integrity เป็นการทำให้แน่ใจว่าสิ่งที่ users กำลังทำอยู่ ถูกต้อง

เรื่องที่ต้องพิจารณาเกี่ยวกับ Security

- Legal
- Physical Controls
- Policy Questions
- Operational Problems
- Hardware Controls
- Operating System Security
- Database

ระบบรักษาความปลอดภัยของ DBMS

- Discretionary - Given user will have different access rights (privileges, authorities)
- Mandatory - Each data object is tagged with a certain classification

Discretionary

```
CREATE VIEW EX1 AS
  SELECT S.S#, S.SNAME, S.CITY
  FROM S;

GRANT SELECT ON EX1 TO Jacques, Anne;
```

Discretionary

```
CREATE VIEW EX2 AS
  SELECT S.S#, S.SNAME, S.STATUS, S.CITY
  FROM S;
  WHERE S.CITY = 'Paris';

GRANT SELECT, INSERT, UPDATE (SNAME,
  STATUS) ON EX2 TO Dan, Misha
```

Privileges

- SYSTEM Privileges: สิทธิที่ผู้ใช้สามารถกระทำการในระดับ database เช่น create, drop, alter TABLES หรือ VIEWS
- OBJECT Privileges: สิทธิที่ผู้ใช้สามารถกระทำการในระดับ object เช่น retrieve, insert, update ,delete ข้อมูลที่อยู่ใน table หรือ views

Audit Trails

It is important not to assume that the security system is perfect.

Audit Trails

The audit trail might contain the following information:

- Request (source text)
- terminal from which the operation was invoked
- user who invoked the operation
- date and time of the operation
- base relation(s), tuple(s), and attribute(s) affected
- old values
- new values

Mandatory Access Control

- เหมาะที่จะใช้กับฐานข้อมูลที่มีข้อมูลค่อนข้างคงที่ (static) และมีโครงสร้างเป็นระดับที่ชัดเจน (ตัวอย่าง ข้อมูลทางการทหารหรือราชการ)

หลักการ Mandatory Access Control

- Each data object has a **classification level** (e.g. top secret, secret, confidential, etc.)
- Each user has a **clearance level** (with the same possibilities as for the classification levels)
- The levels are assumed to form a strict ordering (e.g., top secret > secret > confidential)

กฎของการรักษาความปลอดภัยของ Mandatory Access Control

- User i can see object j only if the clearance level of i is greater than or equal to the classification level of j
- User i can modify object j only if the clearance level of i is equal to the classification level of j

Data Encryption (การเข้ารหัสข้อมูล)

- การเข้ารหัสข้อมูล เป็นวิธีรักษาความปลอดภัยที่เหมาะสมในกรณีที่ผู้ใช้ (หรือผู้ไม่หวังดี) ละเมิดระบบรักษาความปลอดภัยของ ระบบ database หรือโมยข้อมูลผ่านสายสื่อสาร

วิธีการของ data encryption

The original (unencrypted) data is called the **plaintext**.
The plaintext is encrypted by subjecting it to an **encryption algorithm**, whose inputs are the plaintext and an **encryption key**; the output from this algorithm is called the **ciphertext**.

ตัวอย่างของการ Encrypt ข้อมูล

- Plain text: AS KINGFISHERS CATCH FIRE
- Encryption key: ELIOT

ขั้นที่ 1 แบ่ง plaintext เป็นส่วนๆ ให้มีความยาวเท่า encryption key

AS+KI NGFIS HERS+ CATCH +FIRE

(เครื่องหมาย + หมายถึงช่องว่าง)

ตัวอย่างของการ Encrypt ข้อมูล

ขั้นที่ 2 แทนค่า plaintext ด้วยตัวเลขจาก 00-26 โดย 00 หมายถึงช่องว่าง A = 01, ..., Z = 26

AS+KI NGFIS HERS+ CATCH +FIRE



0119001109 1407060919 0805181900 0301200308 0006091805

ตัวอย่างของการ Encrypt ข้อมูล

ขั้นที่ 3 ทำตามขั้นที่ 2. สำหรับ Encryption key

ELIOT



0512091520

ตัวอย่างของการ Encrypt ข้อมูล

ขั้นที่ 4 นำค่า plaintext และ ค่า encryption key ที่ได้มาบวกกัน หาก
บวกได้ผลลัพธ์เกิน 27 ให้ใช้เศษที่เกิน 27

0119001109 1407060919 0805181900 0301200308 0006091805
0512091520 0512091520 0512091520 0512091520 0512091520
0604092602 1919152412 1317000720 0813021801 0518180625

ตัวอย่างของการ Encrypt ข้อมูล

ขั้นที่ 5 แทนค่าตัวเลขที่ได้กลับเป็นตัวอักษร

0604092602 1919152412 1317000720 0813021801 0518180625



FDIZB SSOXL MQ+GT HMBRA ERRFY

Classifications of Data Encryption

- Substitution - ใช้การแทนค่า ดังตัวอย่างที่แสดง
- Permutation - ใช้การสลับตำแหน่งของข้อมูล

SQL Support

- ปัจจุบัน SQL standard สนับสนุน discretionary access control เท่านั้น
- การสนับสนุนของ SQL โดยผ่าน
 - View mechanism เพื่อซ่อนข้อมูลที่สำคัญ
 - Authorization subsystem เป็นการกำหนดสิทธิและส่งต่อสิทธิให้ผู้อื่น

What Are Views For?

- Restructuring
- They allow the same data to be seen by different users in different ways at the same time
- They provide a shorthand or “macro” capability
- Automatic security is provided for hidden data

Security in Oracle

- No subversion
- Create View
- Direct privileges
- Role privileges
- Authentication mechanism
- Resource limits
- Audit trail