



www.itsci.mju.ac.th/sayan

LEC 06: USERS & SECURITY

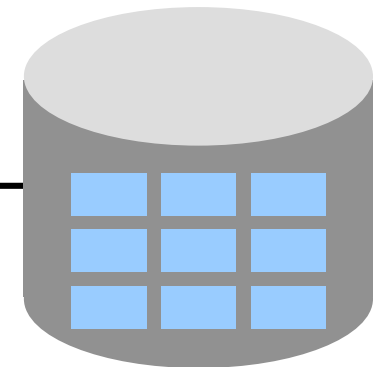
SAYAN UNANKARD
1/2558

CONTROLLING USER ACCESS

Database administrator



Username and password
Privileges



Users



PRIVILEGES

การกำหนดความปลอดภัยของฐานข้อมูล

- System security
- Data security

การกำหนดสิทธิ์ของระบบ (System privileges)

การกำหนดสิทธิ์ของวัตถุ (Object privileges) จัดการ database objects ต่าง ๆ เช่น ตาราง วิว เป็นต้น

SYSTEM PRIVILEGES

สิทธิ์ต่างๆ มีมากกว่า 100 privileges

ผู้ดูแลระบบฐานข้อมูล (database administrator) มีสิทธิ์ในการจัดการระดับสูง (high-level system privileges) เช่น

- Creating new users
- Removing users
- Removing tables
- Backing up tables

CREATING USERS

Database administrator (DBA) สร้างผู้ใช้ด้วยคำสั่ง CREATE USER

```
CREATE USER user  
IDENTIFIED BY password;
```

```
CREATE USER demo  
IDENTIFIED BY demo;
```

USER SYSTEM PRIVILEGES

หลังจากที่ผู้ใช้ถูกสร้างแล้ว ผู้ดูแลระบบสามารถจะกำหนดสิทธิ์การทำงานของระบบได้

```
GRANT privilege [, privilege...]  
TO user [, user/ role, PUBLIC...];
```

สำหรับนักพัฒนาระบบ สิทธิ์ที่อาจจะกำหนดให้ใช้งานได้ เช่น

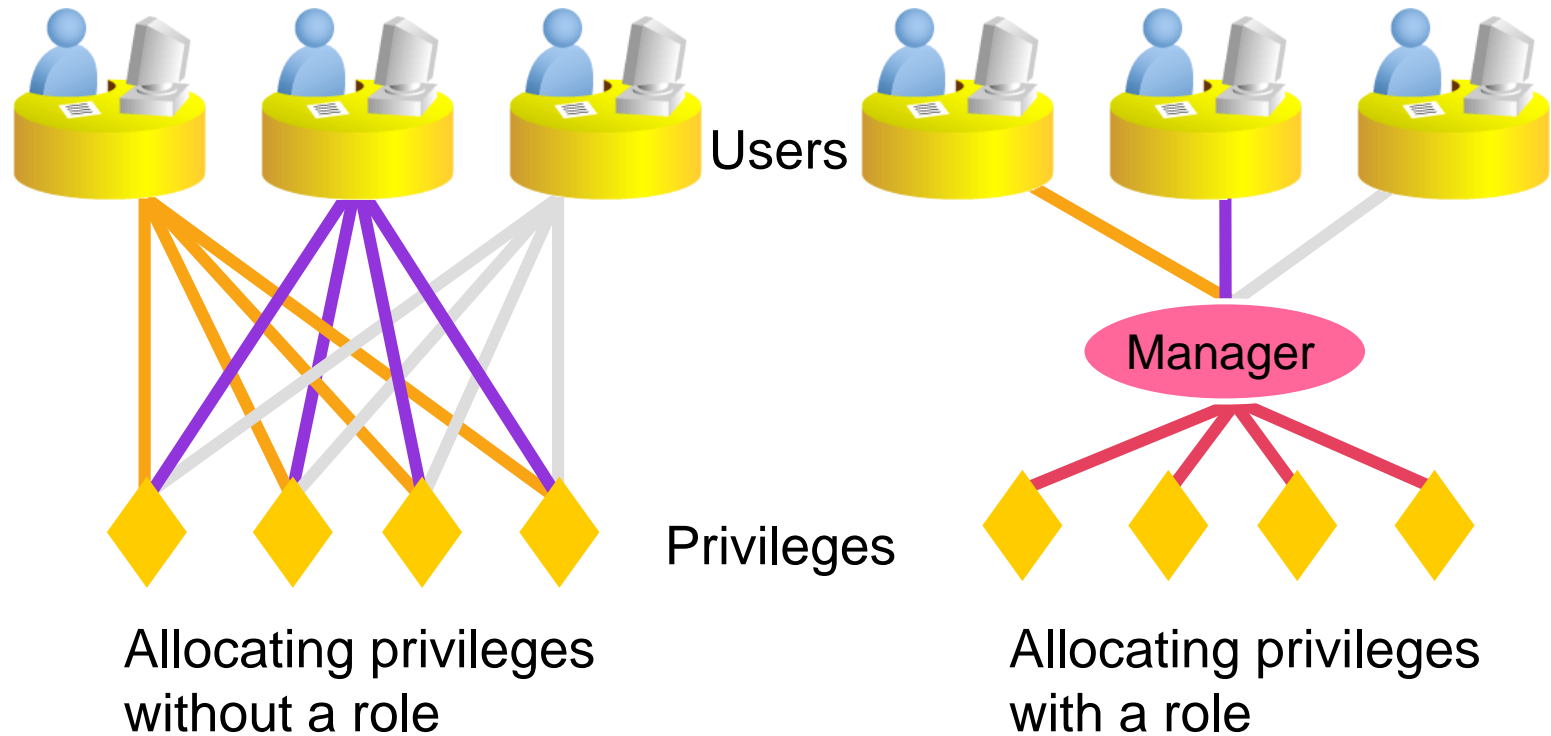
- CREATE SESSION – เข้าใช้ฐานข้อมูลได้
- CREATE TABLE
- CREATE SEQUENCE
- CREATE VIEW
- CREATE PROCEDURE

GRANTING SYSTEM PRIVILEGES

ตัวอย่างการกำหนดสิทธิ์ของผู้ใช้

```
GRANT create session, create table,  
      create sequence, create view  
TO    demo;
```

WHAT IS A ROLE?



CREATING AND GRANTING PRIVILEGES TO A ROLE

Create a role:

```
CREATE ROLE manager;
```

Grant privileges to a role:

```
GRANT create table, create view  
TO manager;
```

Grant a role to users:

```
GRANT manager TO SAYAN, JIRAWAN;
```



CHANGING YOUR PASSWORD

DBA สร้างบัญชีผู้ใช้และกำหนดรหัสผ่านเริ่มต้นให้

เราสามารถเปลี่ยนรหัสผ่านได้โดยใช้คำสั่ง ALTER USER statement

```
ALTER USER demo  
IDENTIFIED BY employ;
```

OBJECT PRIVILEGES

Object privilege	Table	View	Sequence
ALTER	✓		✓
DELETE	✓	✓	
INDEX	✓		
INSERT	✓	✓	
REFERENCES	✓		
SELECT	✓	✓	✓
UPDATE	✓	✓	

OBJECT PRIVILEGES

การกำหนดสิทธิ์ให้กับวัตถุใด ๆ

เจ้าของวัตถุนั้น ๆ มีสิทธิ์ทั้งหมดในการจัดการ

เจ้าของวัตถุนั้น ๆ สามารถกำหนดสิทธิ์ต่อให้กับผู้ใช้คนอื่น ๆ ต่อไปได้

```
GRANT object_priv [(columns)]  
ON object  
TO {user|role|PUBLIC}  
[WITH GRANT OPTION];
```

GRANTING OBJECT PRIVILEGES

การกำหนดสิทธิ์ในการ SELECT ตาราง EMPLOYEES

```
GRANT select
ON employees
TO demo;
```

การกำหนดสิทธิ์ในการ update บางคอลัมน์

```
GRANT update (department_name, location_id)
ON departments
TO demo, manager;
```

PASSING ON YOUR PRIVILEGES

การกำหนดสิทธิ์ พร้อมทั้งให้สิทธิ์ในการอนุญาตให้สิทธิ์ต่อได้

```
GRANT select, insert  
ON departments  
TO demo  
WITH GRANT OPTION;
```

อนุญาตผู้ใช้ทุกคนเข้ามาเลือกดูข้อมูลของผู้ใช้ที่ชื่อว่า Alice ในตาราง DEPARTMENTS

```
GRANT select  
ON alice.departments  
TO PUBLIC;
```

REVOKING OBJECT PRIVILEGES

สามารถยกเลิกสิทธิ์การใช้งานต่าง ๆ ของผู้ใช้ โดยใช้คำสั่ง REVOKE

การกำหนดสิทธิ์ใด ๆ ที่ทำด้วยคำสั่ง WITH GRANT OPTION จะถูกยกเลิกไปด้วย

```
REVOKE {privilege [, privilege...]|ALL}
ON      object
FROM    {user[, user...]|role|PUBLIC}
[CASCADE CONSTRAINTS];
```

ตัวอย่างการยกเลิกสิทธิ์การ SELECT และ INSERT สำหรับผู้ใช้ demo บนตาราง DEPARTMENTS

```
REVOKE select, insert
ON      departments
FROM    demo;
```