DATABASE MANAGEMENT SYSTEMS

Subject Teacher: Zartasha Baloch

CREATING USERS & PERMISSIONS ON OBJECTS

Lecture 28

Disclaimer: The material used in this presentation to deliver the lecture i.e., definitions/text and pictures/graphs etc. does not solely belong to the author/presenter. The presenter has gathered this lecture material from various sources on web/textbooks. Following sources are especially acknowledged:

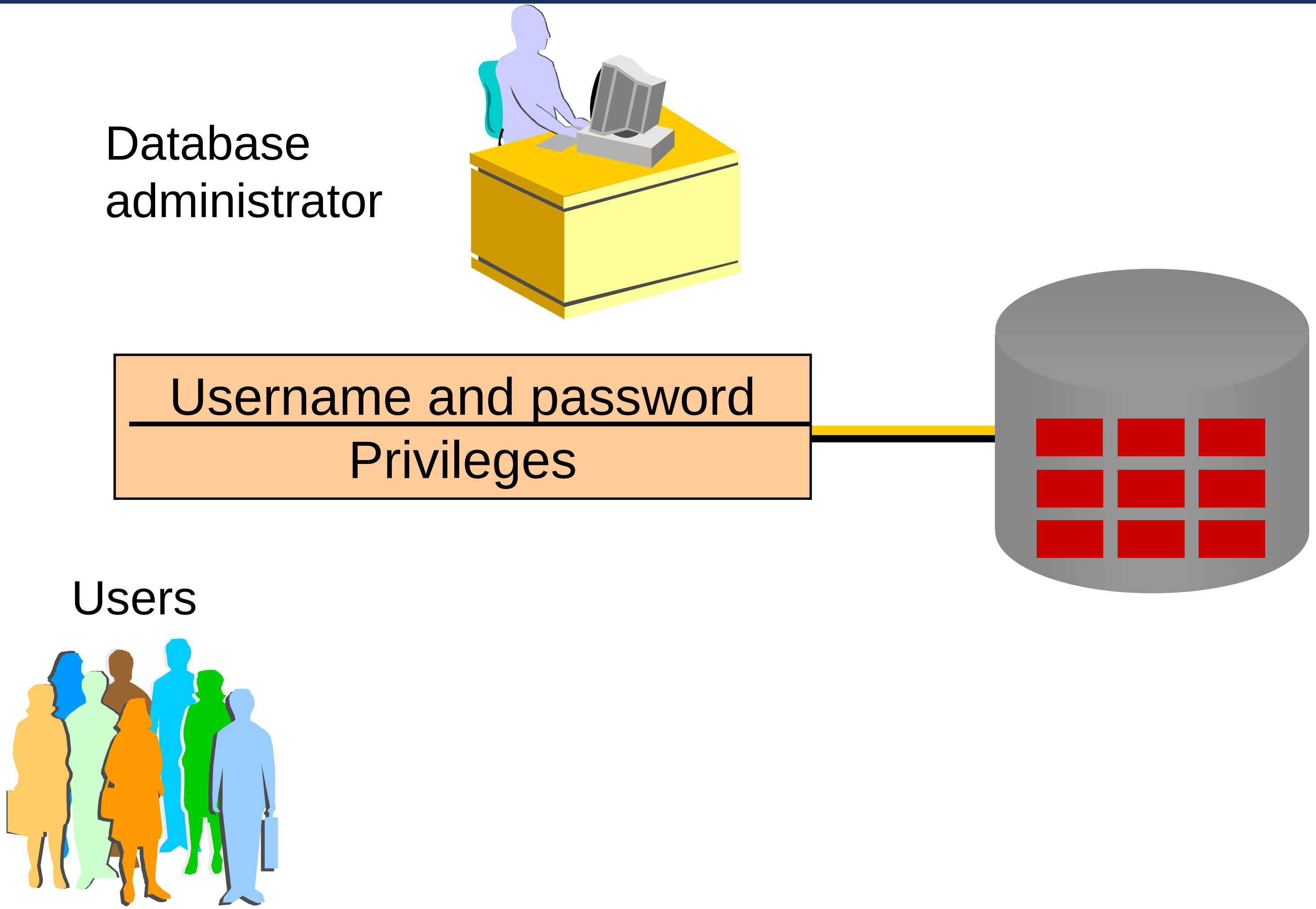
1. Connolly, Thomas M., and Carolyn E. Begg. *Database systems: a practical approach to design, implementation, and management*. Pearson Education, 2005.
2. Gorman, Tim, Inger Jorgensen, Melanie Caffrey, and Lex deHaan. Beginning Oracle SQL: For Oracle Database 12c. Apress, 2014.
3. Greenberg, Nancy, and Instructor Guide PriyaNathan. "Introduction to Oracle9i: SQL." ORACLE, USA (2001).

OBJECTIVES

After completing this lesson, you should be able to do the following:

- Create users
- Create roles to ease setup and maintenance of the security model
- Use the `GRANT` and `REVOKE` statements to grant and revoke object privileges
- Create and access database links

CONTROLLING USER ACCESS



Database administrator

Username and password

Privileges

Users

PRIVILEGES

- Database security:
  - System security
  - Data security
- System privileges: Gaining access to the database
- Object privileges: Manipulating the content of the database objects
- Schemas: Collections of objects, such as tables, views, and sequences

SYSTEM PRIVILEGES

- More than 100 privileges are available.
- The database administrator has high-level system privileges for tasks such as:
  - Creating new users
  - Removing users
  - Removing tables
  - Backing up tables

CREATING USERS

The DBA creates users by using the `CREATE USER` statement.

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

```
CREATE USER  scott
IDENTIFIED BY   tiger;
User created.
```

USER SYSTEM PRIVILEGES

- Once a user is created, the DBA can grant specific system privileges to a user.

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

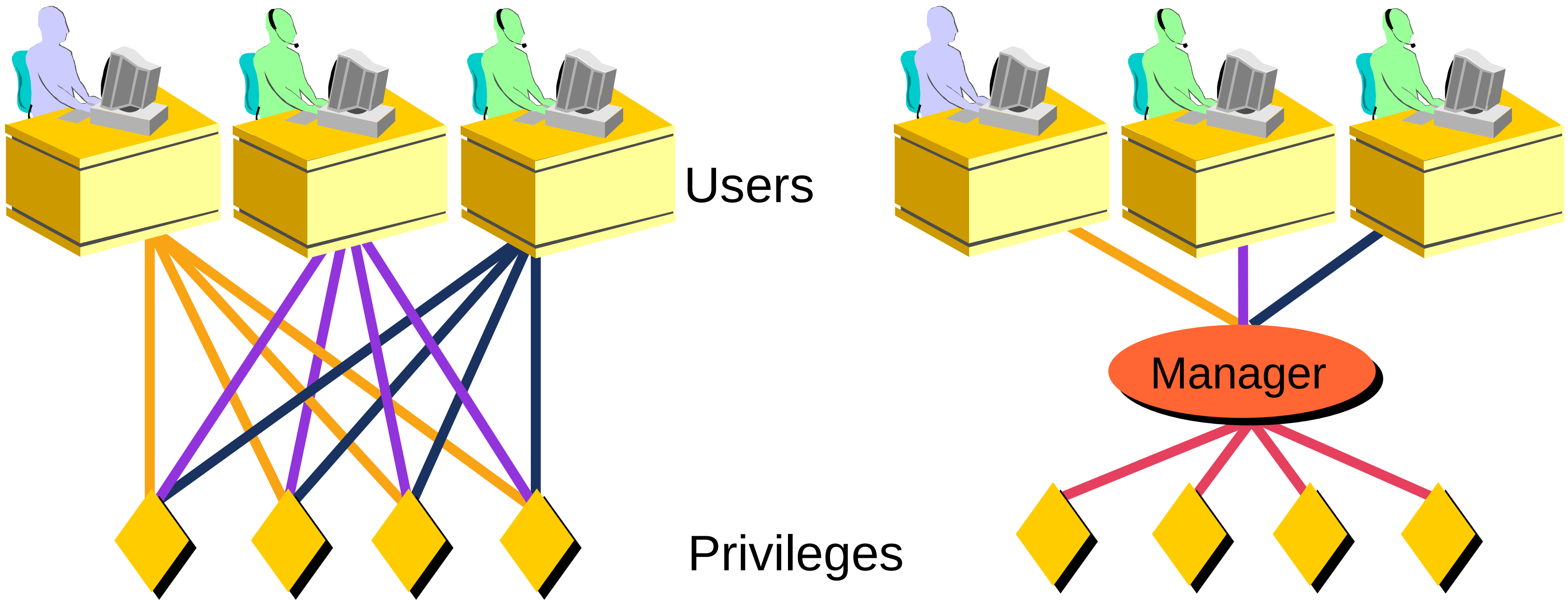
- An application developer, for example, may have the following system privileges:
  - `CREATE SESSION`
  - `CREATE TABLE`
  - `CREATE SEQUENCE`
  - `CREATE VIEW`
  - `CREATE PROCEDURE`

GRANTING SYSTEM PRIVILEGES

The DBA can grant a user specific system privileges.

```
GRANT  create session, create table,
       create sequence, create view
TO     scott;
Grant succeeded.
```

WHAT IS A ROLE?



Allocating privileges
without a role

Allocating privileges
with a role

CREATING AND GRANTING PRIVILEGES TO A ROLE

- Create a role

```
CREATE ROLE manager;
Role created.
```

- Grant privileges to a role

```
GRANT create table, create view
TO manager;
Grant succeeded.
```

- Grant a role to users

```
GRANT manager TO DEHAAN, KOCHHAR;
Grant succeeded.
```

SYSTEM ROLES PRE-DEFINED BY ORACLE

System Role	Privileges Granted to the Role
CONNECT	CREATE TABLE, CREATE VIEW, CREATE SYNONYM, CREATE SEQUENCE, CREATE SESSION etc.
RESOURCE	CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER etc. The primary usage of the RESOURCE role is to restrict access to database objects.
DBA	ALL SYSTEM PRIVILEGES

CHANGING YOUR PASSWORD

- The DBA creates your user account and initializes your password.
- You can change your password by using the `ALTER USER` statement.

```
ALTER USER scott
IDENTIFIED BY lion;
User altered.
```

OBJECT PRIVILEGES

Object Privilege	Table	View	Sequence	Procedure
ALTER	√		√	
DELETE	√	√		
EXECUTE				√
INDEX	√			
INSERT	√	√		
REFERENCES	√	√		
SELECT	√	√	√	
UPDATE	√	√		

OBJECT PRIVILEGES

- Object privileges vary from object to object.
- An owner has all the privileges on the object.
- An owner can give specific privileges on that owner’s object.

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

GRANTING OBJECT PRIVILEGES

- Grant query privileges on the `EMPLOYEES` table.

```
GRANT  select
ON     employees
TO     sue, rich;
Grant succeeded.
```

- Grant privileges to update specific columns to users and roles.

```
GRANT  update (department_name, location_id)
ON     departments
TO     scott, manager;
Grant succeeded.
```

USING THE WITH GRANT OPTION AND PUBLIC KEYWORDS

- Give a user authority to pass along privileges.

```
GRANT  select, insert
ON     departments
TO     scott
WITH   GRANT OPTION;
Grant succeeded.
```

- Allow all users on the system to query data from Alice's DEPARTMENTS table.

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

CONFIRMING PRIVILEGES GRANTED

Data Dictionary View	Description
`ROLE_SYS_PRIVS`	System privileges granted to roles
`ROLE_TAB_PRIVS`	Table privileges granted to roles
`USER_ROLE_PRIVS`	Roles accessible by the user
`USER_TAB_PRIVS_MADE`	Object privileges granted on the user’s objects
`USER_TAB_PRIVS_RECD`	Object privileges granted to the user
`USER_COL_PRIVS_MADE`	Object privileges granted on the columns of the user’s objects
`USER_COL_PRIVS_RECD`	Object privileges granted to the user on specific columns
`USER_SYS_PRIVS`	Lists system privileges granted to the user

HOW TO REVOKE OBJECT PRIVILEGES

- You use the `REVOKE` statement to revoke privileges granted to other users.
- Privileges granted to others through the `WITH GRANT OPTION` clause are also revoked.

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

REVOKING OBJECT PRIVILEGES

As user Alice, revoke the SELECT and INSERT privileges given to user Scott on the DEPARTMENTS table.

```
REVOKE  select, insert
ON      departments
FROM    scott;
Revoke succeeded.
```

PRACTICE QUESTIONS

1. Create a user SMITH and assign a password JONES.
2. Assign the privilege to start a session to SMITH.
3. Write a query to grant SELECT, INSERT, UPDATE, and DELETE privileges on a table called *suppliers* to a user *smith*.
4. *Cancel the INSERT and DELETE privileges for user SMITH.*

SUMMARY

In this lesson, you should have learned about DCL statements that control access to the database and database objects.

Statement	Action
`CREATE USER`	Creates a user (usually performed by a DBA)
`GRANT`	Gives other users privileges to access the your objects
`CREATE ROLE`	Creates a collection of privileges (usually performed by a DBA)
`ALTER USER`	Changes a user’s password
`REVOKE`	Removes privileges on an object from users