IT2201 / IT2601 / IT2564 / IT2621 / IT2521 / IT2323

Database Management Systems

Unit 9
Database Administration & Security

1

Unit Objectives

- At the end of this unit, you should be able to
  - Describe the purpose and tasks associated with database administration.
  - Define the scope of database security.
  - Identify the type of threats that can affect a database system.
  - Describe how to protect a computer system using computer-based security controls.
  - Implement database security using SQL statements.

2

Database Administration

- The management of physical realization of a database application, which includes :
  - physical database design and implementation,
  - setting security and integrity controls,
  - monitoring system performance, and
  - reorganizing the database.
- The tasks of a database administrator is DBMS dependent whereas those of a data administrator is DBMS independent.

3

Database Administration Tasks

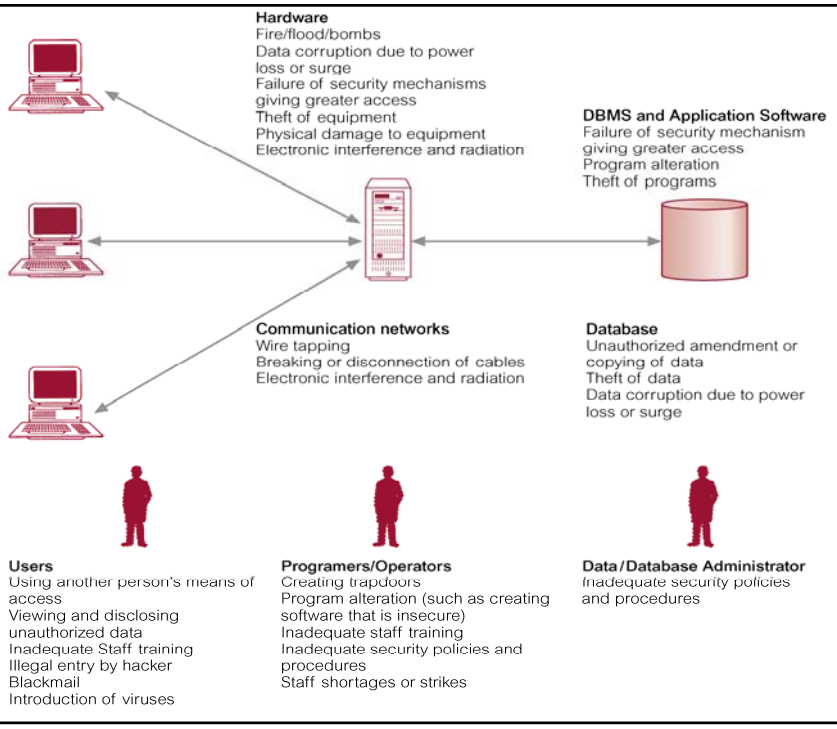
- Evaluating and selecting DBMS products.
- Implementing a physical database design using a target DBMS.
- Defining security and integrity constraints.
- Responding to changing requirements by liaising with application developers.
- Developing test strategies.
- Performing backups routinely.
- Ensuring recovery mechanisms and procedures are in place, and perform database recovery following a failure.
- Monitoring system performance and tuning the database.
- Training users.

4

Database Security

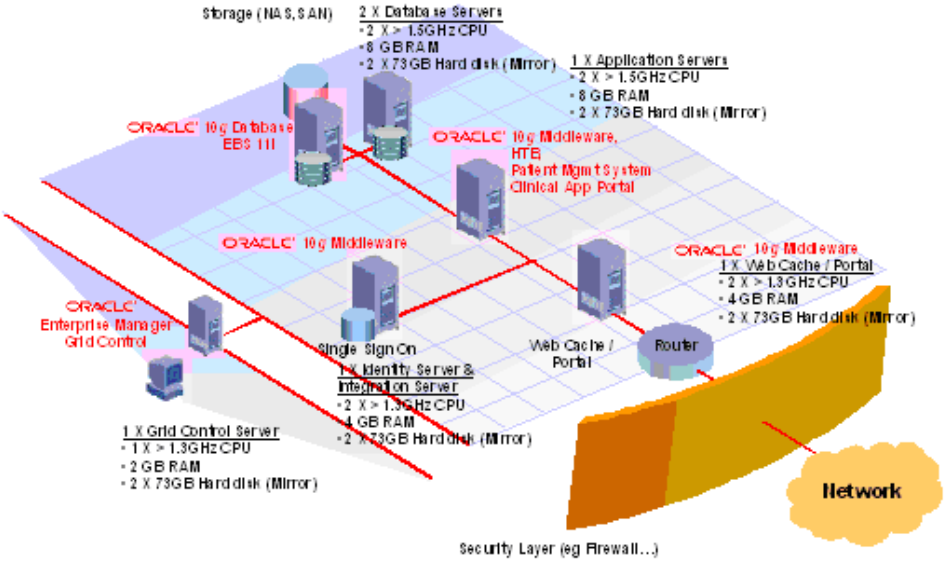
- Data is a valuable resource that must be strictly controlled and managed, as with any corporate resource.
- Part or all of the corporate data may have strategic importance and therefore needs to be kept secure and confidential.
- Database security is the mechanisms that protect the database against intentional or accidental *threats*.
- Threat
  - Any situation or event, whether intentional or unintentional, that will adversely affect a system and consequently an organization.

5



6

Typical Multi-User Environment



Review Questions 1

- Name 4 tasks for database management
- Define database security

8

Computer-Based Security Controls

- Concerned with physical controls to administrative procedures
- Includes:
  - Authorization
  - Views
  - Integrity constraints
  - Encryption
  - Auditing
  - Backup

9

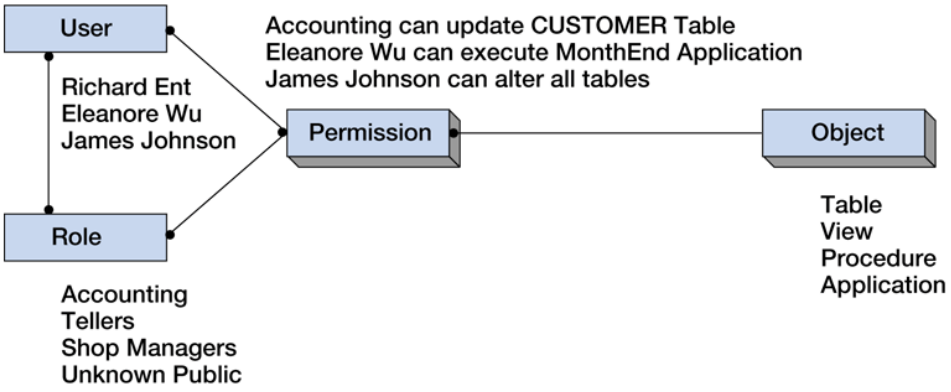
Computer-Based Security Controls

- Authorization / Privilege Management
  - The granting of a right or **privilege**, which enables a subject (a user or program) to legitimately have access to a system or a system's object (table, view, etc).
  - Also referred to as **access controls**
- Authentication
  - A mechanism that determines whether a user is who he or she claims to be.

10

Computer-Based Security Controls

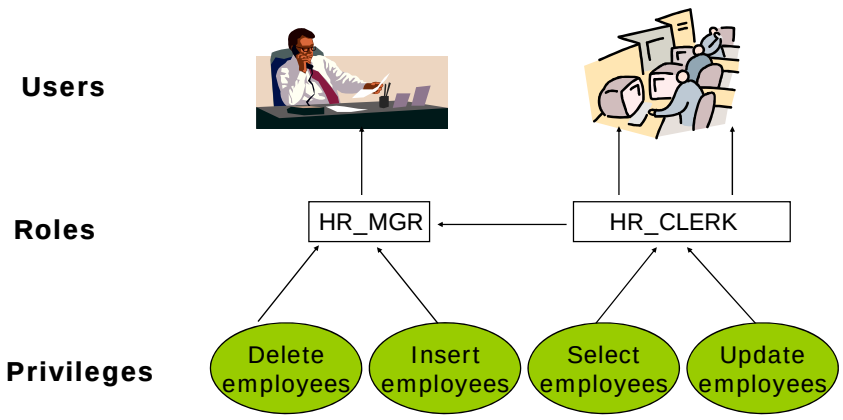
- Example illustrating privilege management



11

Computer-Based Security Controls

- Role-based implementation



12

Example of Role-based control

```
--*create HR_CLERK role
CREATE ROLE HR_CLERK;

--*grant privs to role
GRANT SELECT, UPDATE ON EMPLOYEES TO HR_CLERK;
GRANT CONNECT TO HR_CLERK;

--*grant role to users
GRANT HR_CLERK TO user1, user2, user3, user4;

--*create HR_MGR role
CREATE ROLE HR_MGR;

--*grant privs to role
GRANT DELETE, INSERT ON EMPLOYEES TO HR_MGR;

--*grant HR_CLERK role to the HR_MGR role;
GRANT HR_CLERK TO HR_MGR;

--*grant role to user
GRANT HR_MGR TO pennyLee,
```

13

Computer-Based Security Controls

- View
  - Dynamic result of one or more relational operations operating on the base relations to produce another relation.
  - A virtual relation that does not actually exist in the database, but is produced upon request by a particular user, at the time of request.

14

Computer-Based Security Controls

- Integrity constraints
  - Prevents data from becoming invalid, and hence giving misleading or incorrect results.
- Encryption
  - The encoding of the data by a special algorithm that renders the data unreadable by any program without the decryption key.
- Audit trails
  - A chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

15

Implement database security using SQL

- Views can be used for security purposes.
  - The view mechanism allows the database to be conceptually divided up into pieces (in various ways) so that sensitive information can be hidden from unauthorized users.

Example

```
CREATE VIEW     PARIS_SUPPLIERS
  AS            SELECT SNO, SNAME, STATUS, CITY
                  FROM SUPPLIER
                  WHERE CITY = 'PARIS';
```

16

Implement database security using SQL

- Two SQL statements that are used to specify operations that authorized users may execute on a particular relation or database object.
- GRANT statement
  - To give access right to a user or a group of users, to access database objects.
- REVOKE statement
  - To cancel any access rights given to a user or a group of users, to access database objects.

17

Implement database security using SQL

- Examples of GRANT Statement

```
GRANT    SELECT
  ON     SUPPLIER
  TO     USER1;

GRANT    SELECT, UPDATE (STATUS, CITY)
  ON     SUPPLIER
  TO     USER2, USER3, USER4;

GRANT    SELECT
  ON     PART
  TO     PUBLIC;

GRANT    ALL PRIVILEGES
  ON     SUPPLIER
  TO     USER5;
```

18

Implement database security using SQL

- Examples of REVOKE Statement

```
REVOKE   SELECT
  ON     SUPPLIER
  FROM   USER1;

REVOKE   UPDATE
  ON     SUPPLIER
  FROM   USER2;

REVOKE   ALL PRIVILEGES
  ON     SUPPLIER
  FROM   USER3, USER4;

REVOKE   ALL PRIVILEGES
  ON     SUPPLIER
  FROM   USER5;
```

19

Implement database security using SQL

- Example of an audit trail (using Oracle)
  - Database configuration parameter
    - audit_trail = db
  - It can be enabled by the DBA
  - System operation will be captured in the trail
    - Starting and stopping of the database
    - structural changes such as adding a datafile
    - Log-on and Log-off the database

```
SQL>
USERNAME TERMIN ACTION_N RETURNCODE TO_CHAR(TIMESTAMP,'D TO_CHAR(LOGOFF_TIME,
---------- ------ -------- ---------- ------------------- -------------------
SYS        L536P4 LOGOFF    0         09-APR-2003         20:10:46  09-APR-2003        20:16:41
SYSTEM     L536P7 LOGOFF    0         09-APR-2003         21:49:20  09-APR-2003        21:49:50
ZULIA      L536P1 LOGON     0         09-APR-2003         21:49:50
EMIL       APOLLO LOGON     0         09-APR-2003         22:49:12
```

20

Implement database security using SQL

- Examples of Encryption
  - DBMS_CRYPTO PLSQL Package
    - Available in Oracle 10g
    - Library for encryption
    - Contains more cryptographic algorithms
  - Transparent data encryption (TDE)
    - Modify existing table:
      - SQL> alter table accounts modify credit_card encrypt;
    - Create new table:
      - SQL> create table accounts (
        customer_id number(12) NOT NULL,
        credit_card varchar2(19) encrypt));

21

Review Questions 2

- Name 5 Computer-Based Security Controls
- Why are VIEWS used for security controls?
- How can integrity be achieved?
- How does the database implements authorization?

22

Reference Materials

1. Database Systems, Connolly :
   - Ch 9 (Sect 9.15)
   - Ch 18
   - Ch 6 (Sect 6.6)

23