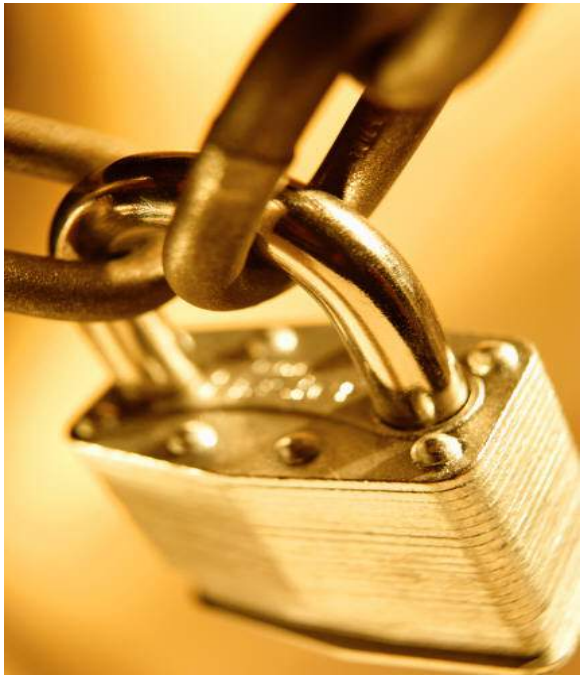
COSC344
Database Theory and Applications

Lecture 20
Database Security

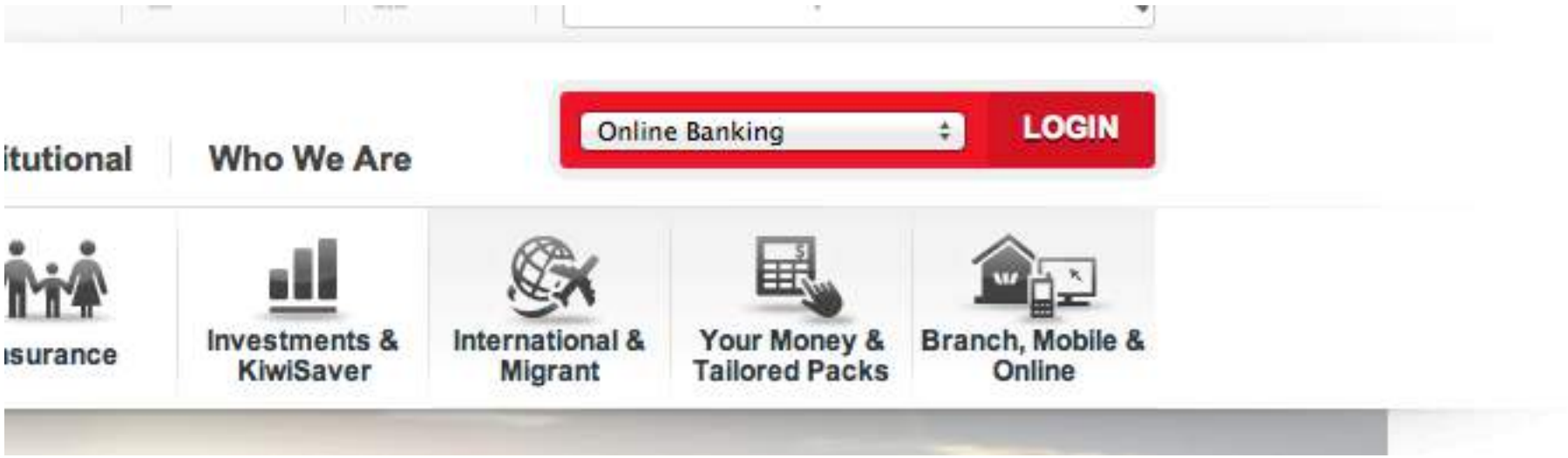


Overview

- Last Lecture
  - Indexing
- This Lecture
  - Database Security
    - Security
      - Mandatory access control
      - Discretionary access control
  - Source: Chapter 25
  - Source: Oracle documentation
- Next Lecture
  - Query Optimization

Security

- Security refers to the protection of the database against unauthorized access, either intentional or accidental.

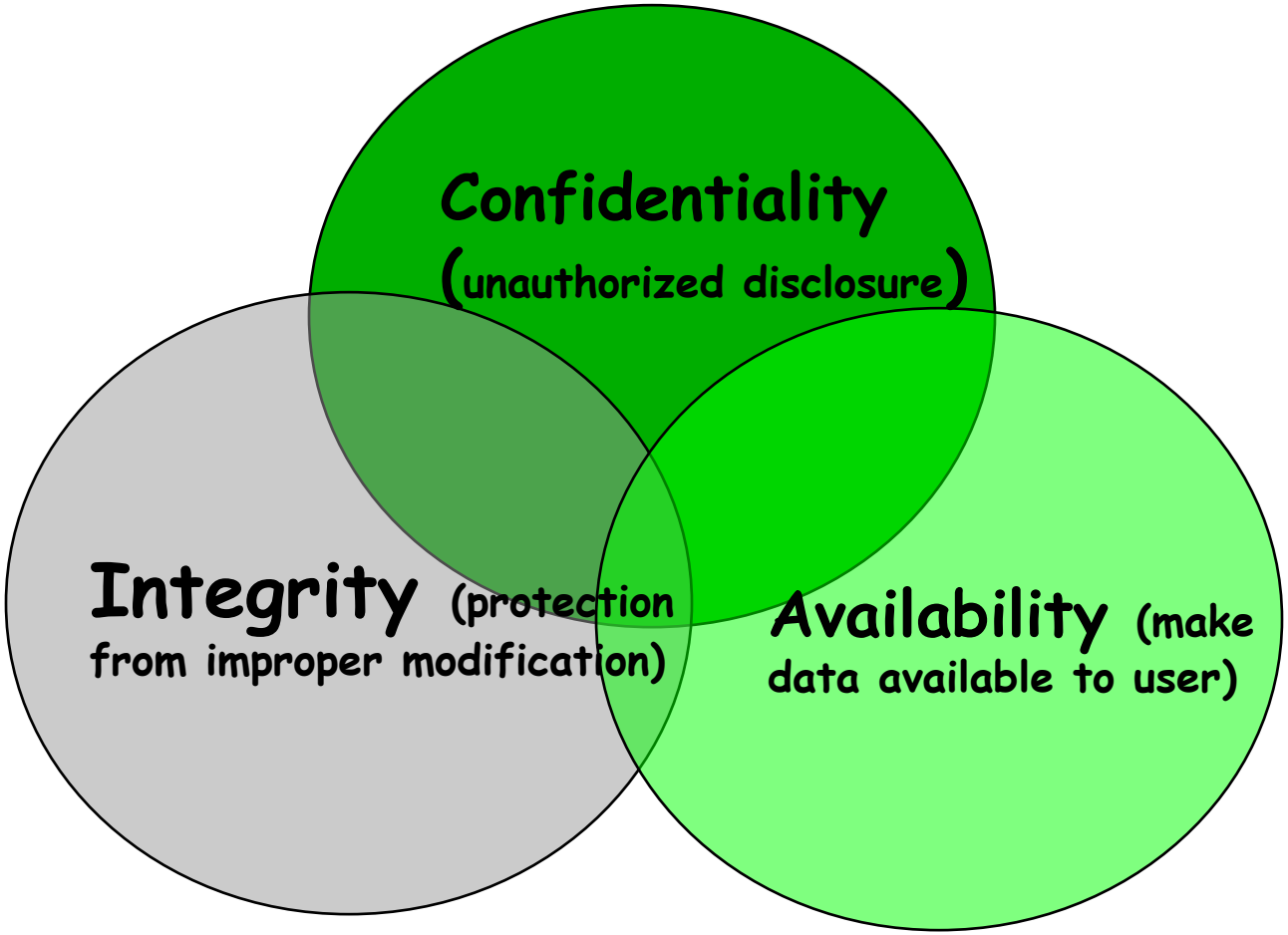


Security

- Security refers to the protection of the database against unauthorized access, either intentional or accidental.

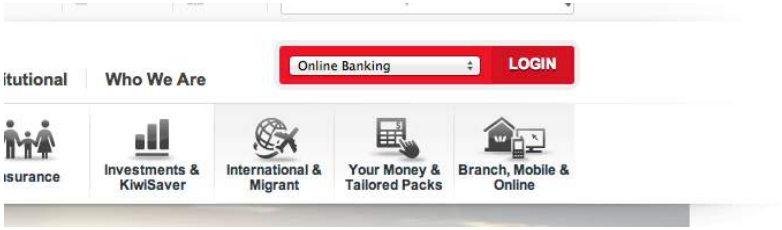
Security

- Security refers to the protection of the database against unauthorized access, either intentional or accidental.



Control Measures

- Access Control
  - User account and password
- Inference Control
  - Statistical database security
- Flow Control
  - Prevent information from reaching unauthorized users
- Data encryption
  - Protect sensitive data (e.g., credit card number)



Access Control: DBA's responsibility

Access Control: DBA's responsibility

- DBA has DBA account known as superuser
- Overall responsibility for managing a DBMS and its data
- DBA-privileged commands provide
  - Account creation
    - Creates a new account/password for a user or group of users
    - Used to control access to DBMS as a whole
  - Privilege Granting
    - grants certain privileges to certain accounts/users
    - Used by discretionary database authorization
  - Privilege Revocation
    - revokes (cancels) certain privileges from the accounts used by discretionary database authorization
  - Security level assignment
    - assigns user accounts to the appropriate security classification level
    - Used by mandatory database authorization

Two Approaches to DB Security

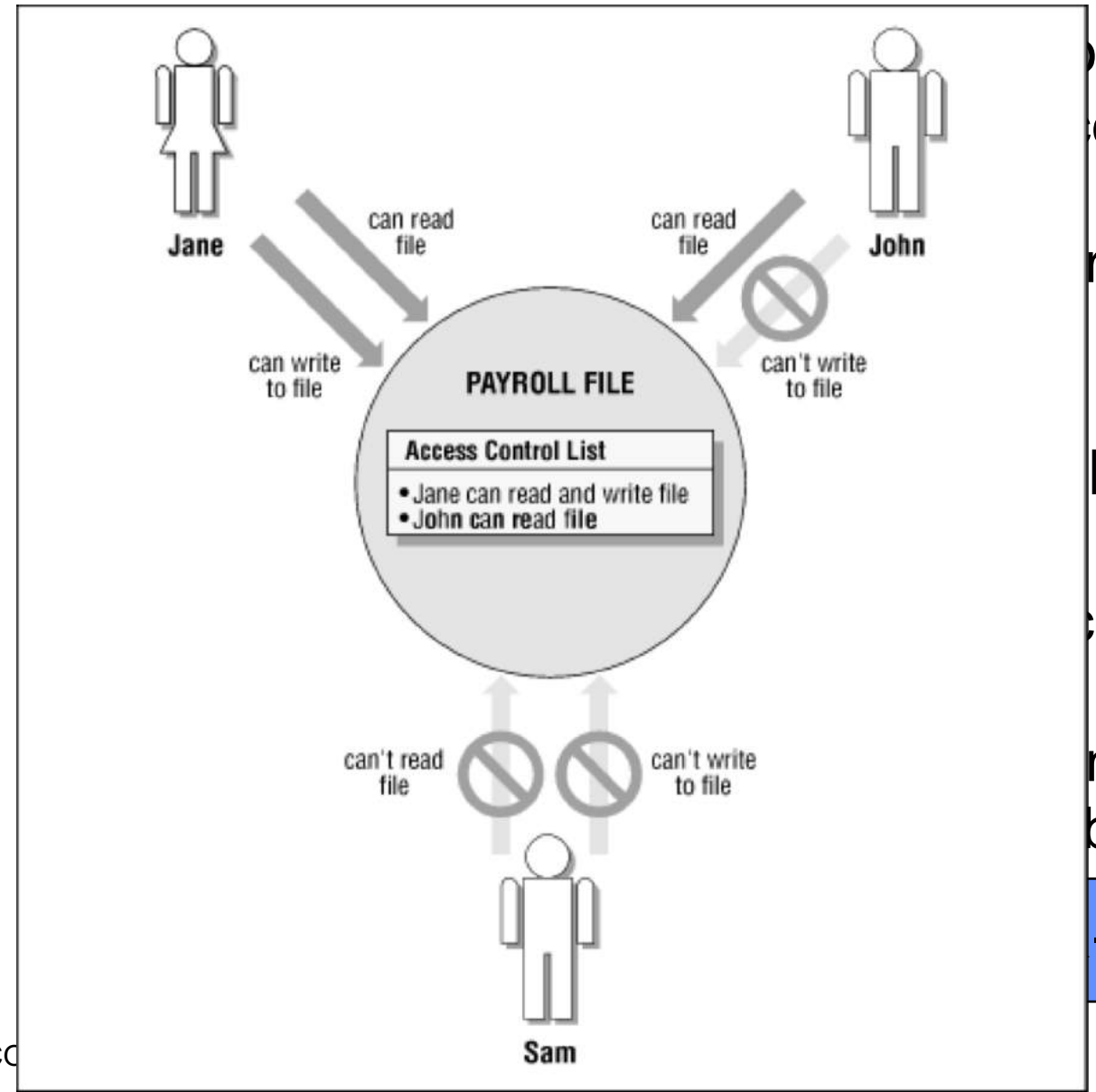
- Discretionary (provided by most commercial DBMSs)
  - A given user may have different access rights to different objects (relation level)
  - Different users may have different rights on the same object (account level)
  - Very flexible

Give or not give

- Mandatory (incorporated by some DBMS for government, military, and etc.)
  - Each data object is tagged with a certain classification level
  - Each user is given a certain clearance level
  - Data object can only be accessed by users with the appropriate clearance
  - Rigid

Multi-level security

Two Approaches to DB Security



ommercial DBMSs)
cess rights to

rights on the same

Give or not give

DBMS for

certain classification

nce level
by users with the

-level security

Two Approaches to DB Security

- Discretionary (provided by most commercial DBMSs)
  - A given user may have different access rights to different objects
  - Different users may have different rights on the same object
  - Very flexible

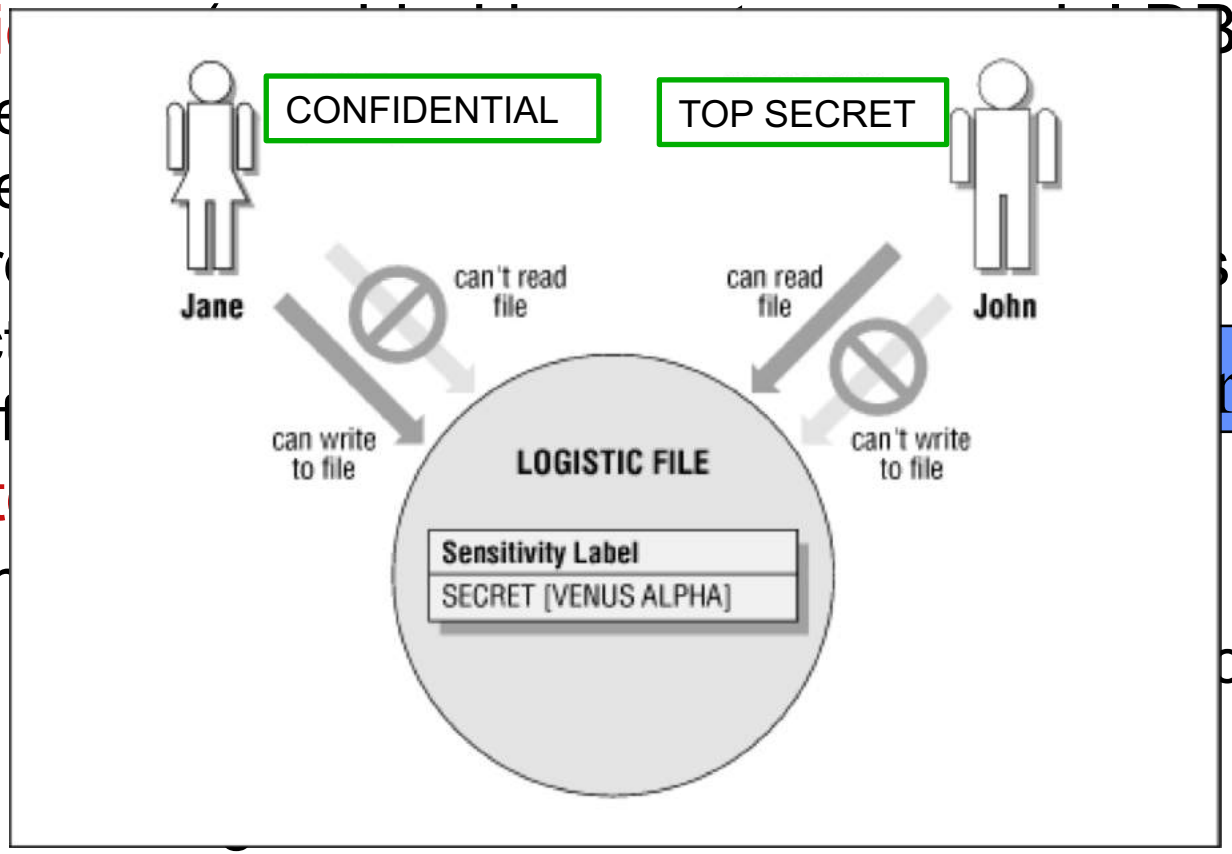
Give or not give

- Mandatory (incorporated by some DBMS for government, military, and etc.)
  - Each data object is tagged with a certain classification level
  - Each user is given a certain clearance level
  - Data object can only be accessed by users with the appropriate clearance
  - Rigid

Multi-level security

Two Approaches to DB Security

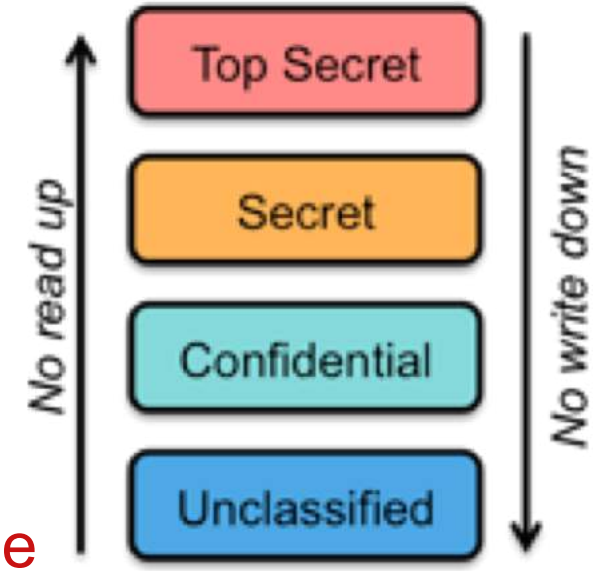
- Discreti… (…BMSs)
  - – A give… differe…
  - – Differ… same objec…
  - – Very f… r not give
- Mandat… governr…
  - – Each … cation level
  - – Each …
  - – Data object can only be accessed by users with the appropriate clearance
  - – Rigid



Multi-level security

Mandatory Access Control

- Applicable to databases with static and rigid classification structures
- Each data object has a *classification* level
- Each user has a *clearance* level
- Levels
  - Top secret
  - Secret
  - Confidential
  - None
- Levels ordered
  - top secret > secret > confidential > none



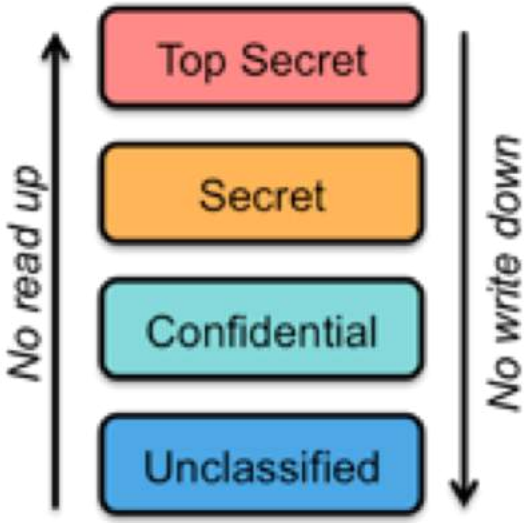
Confidential cannot read Secret
Confidential cannot write Unclassified

Multi-level security

Mandatory Access Control Rules

Bell-Lapadula Model

1. Simple security property
   A subject S is not allowed to read access to an object O unless
   clearance(S) >= classification(O)
2. Star property
   A subject S is not allowed to write an object O unless clearance(S) <= classification(O)



Confidential cannot read Secret
Confidential cannot write Unclassified

Note: Rule 2 keeps a user from lowering the security of database objects

	top secret	secret	confidential	none
read		O	O	O
		S		
write	O	O		

Discretionary Access Control

- Based on granting & revoking privileges
- Provide selective access to each relation based on specific users

Give or not give

- Two levels for assigning privileges
  - Account level
  - Relation level
- Access matrix model

	Tablex	Tabley.col3	Tablez
User 1	*RW*	*RW*	*R*
User 2	*R*	*R*	*R*
User 3	*RWD*	*RW*	-

Discretionary Access Control (cont.)

- Each table has an owner
  - Owner is granted all privileges on his/her tables.
- Owner can pass on privileges on owned tables to other users
- Types of privileges
  - SELECT
  - MODIFY (includes UPDATE, DELETE, INSERT)
  - REFERENCES (the ability to reference relation R when specifying integrity constraints)
- Views

Discretionary Access Control in Oracle

- Based on Privileges and Roles
- Example system privilege
  - CREATE TABLE
  - CREATE VIEW
  - SELECT ANY TABLE
  - ALTER ANY TABLE
  - CREATE ROLE
  - Many more
- Command

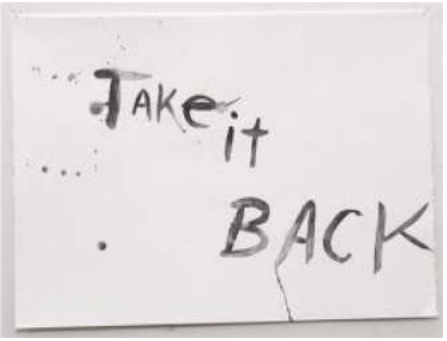
Discretionary Access Control in Oracle

- **GRANT gives privileges to users.**

```
GRANT system_privilege | role
    [, {system_privilege | role}] ...
TO {user | role | PUBLIC}
   [, {user | role PUBLIC}] ...
[WITH ADMIN OPTION];
```

- **REVOKE takes away privileges**

```
REVOKE system_privilege | role
    [, {system_privilege | role}]
FROM {user | role | PUBLIC};
```



Discretionary Access Control in Oracle (cont.)

- Examples

```
GRANT CREATE TABLE
   TO SCOTT;

GRANT CREATE TABLE
   TO PUBLIC;


REVOKE CREATE TABLE
   FROM PUBLIC;
```

Discretionary Access Control in Oracle (cont.)

- Object Privileges
  - SELECT
  - INSERT
  - UPDATE
  - DELETE
  - ALTER
  - EXECUTE
  - INDEX
  - REFERENCE

```
GRANT object_privilege
      [, object_privilege] . . .
      [(column [, column]. . .)]
  ON [user.] object
  TO {user | role | PUBLIC}
     [, {user | role | PUBLIC}] . . .
  [WITH ADMIN OPTION]
```

- Items
  - All or specified columns
- Command

Discretionary Access Control in Oracle (cont.)

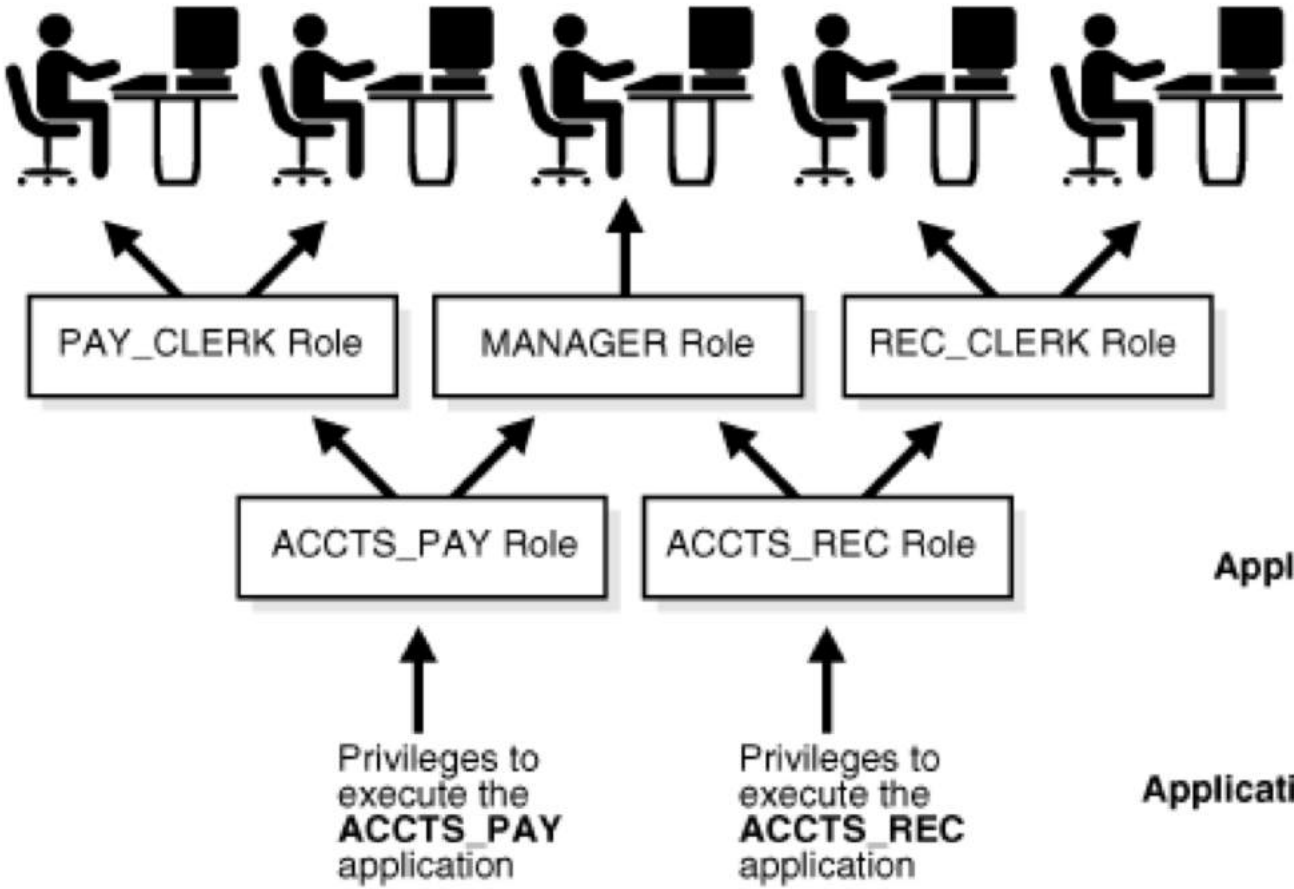
- Example

```
GRANT SELECT
  ON employee
  TO SMITH;
```

```
GRANT UPDATE, DELETE
  ON employee
  TO SMITH;
```

```
GRANT UPDATE(salary)
  ON employee
  TO SMITH;
```

Discretionary Access Control in Oracle (cont.)



Discretionary Access Control in Oracle (cont.)

- Roles
  - Groups of related privileges
  - Simplify
  - Dynamic
- Command

```
CREATE ROLE <role>;
```

- Use GRANT command to give the role privileges
- Grant the role to users

Example

```
CREATE ROLE researcher;

GRANT ALL ON results1 TO researcher;
GRANT SELECT, INSERT ON results2 to
  researcher;

GRANT researcher TO SMITH, WONG;
```

Views

- Can restrict access by creating a view
- A view creates a horizontal and vertical subset of a table

```
CREATE VIEW LsEmployee AS
   SELECT fname, lname, sex, dno
   FROM employee;

GRANT SELECT ON LsEmployee TO Smith;
```

Problems With the WITH ADMIN OPTION

- An owner (A) of a table can grant another user (B) a privilege with a WITH ADMIN OPTION
- B can grant privileges on the table to other users with or without the GRANT option
- Propagation of privileges without the knowledge of the owner
- How to track cascading GRANTs?
- How to revoke cascading GRANTs?

```
GRANT SELECT, UPDATE, DELETE
ON mytable
TO USERB WITH ADMIN OPTION
```

Statistical Database Security

- Produce statistics on various populations
- Users only allowed to retrieve statistical information
  - Averages
  - Counts
  - Sums
  - Standard deviations
- Must prevent the retrieval of individual data
- It is possible to deduce the values of individual tuples from a sequence of statistical queries

Statistical Database Security Example

- ```
  SELECT COUNT(*) FROM PERSON
      WHERE <condition>;
  ```

- ```
  SELECT AVERAGE(INCOME)
      FROM PERSON
      WHERE <condition>;
  ```

- ```
  (last_degree='PhD' AND
   SEX='F' AND
   city='Dunedin')
  ```

Prohibit statistical queries when the number of tuples specified by the selection condition falls below some threshold

Prohibit statistical queries that refer repeatedly to the same tuples
  ```