Security & Authorization

An access control mechanism is a way to control the data accessible by a given user
Will consider in context of DBMSs.

Three main objectives:

Secrecy: Information should not be disclosed to unauthorized users.

Integrity: Only authorized users should be able to modify data

Availability: Authorized users should not be denied access.

Two approaches to Access Control:

Discretionary access control:
idea have privileges on objects and a method for granting privileges to users

Mandatory Access Control - system wide cannot be changed by individual users. Each object has a security class and each user is assigned a clearance for some security class

Most → DBMSs don't have

Discretionary Access Control in SQL

Basic command:

GRANT privileges ON object TO users [WITH GRANT OPTION]

(privileges: comma separated list)

Ex

GRANT INSERT, DELETE ON EMP TO Bob, Alice

Other Possible Privileges
INSERT (col_name)
UPDATE
UPDATE (col_name)
DELETE
REFERENCES
REFERENCES (col_name)

(foreign key references)

Often useful to use in conjunction w/ views

Ex 1st take privileges away from bob

REVOKE SELECT, GRANT OPTION FOR INSERT ON EMP FROM BOB CASCADE,

(and any user Bob granted to use RESTRICT for just bob)

2nd Create a view

CREATE VIEW YoungEmp AS
SELECT name, age FROM EMP WHERE age<30;