## Access Control

CS1555/2055, Panos K. Chrysanthis - University of Pittsburgh

## Access Control

Grant command

GRANT <privilege list> | ALL PRIVILEGES
ON <object\_names>
TO <user-name list> | <role-name list> | PUBLIC
[WITH GRANT OPTION]

- rivilege list>: privilege [(attribute list)]
  - Privileges:
  - SELECT, DELETE, INSERT, UPDATE
  - REFERENCE (with CREATE TABLE)
  - List all privileges (Oracle): select name from system\_privilege\_map;
- □ [WITH GRANT OPTION]
  - Can grant other uses this authorization

CS1555/2055, Panos K. Chrysanthis - University of Pittsburgh

Reliability...

#### Ensuring <u>data integrity</u> ...

- Security
  - Encryption
  - Authentication
  - Compartmentalization
- Access control
  - Who (user/role), what (data), how (operations)
  - Mandatory and discretional
  - Access permissions in the catalog

CS1555/2055, Panos K. Chrysanthis - University of Pittsburgh

2

### Access Control

ON STUDENT

TO Znati, Ramirez, Pat

WITH GRANT OPTION;

CS1555/2055, Panos K. Chrysanthis - University of Pittsburgh

4

## RBAC: Role-based access control Roles are similar to user groups CREATE ROLE < role\_name>; DROP ROLE < role\_name>; Users can be given the privilege to be part of a role □ E.g., CREATE ROLE UG Director; GRANT UG Director TO Ramirez; GRANT UG Director TO Znati; GRANT ALL PRIVILEGES ON STUDENT TO UG DIRECTOR; CS1555/2055, Panos K, Chrysanthis - University of Pittsburgh

## Revoking Privileges REVOKE UPDATE (Major, SID) ON STUDENT FROM Matt, Angela CASCADE: REVOKE UG Director FROM Mosse; CS1555/2055, Panos K. Chrysanthis - University of Pittsburgh

# Revoking Privileges

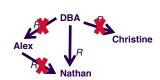
Revoke command is similar to the Grant command REVOKE <privilege list> | ALL PRIVILEGES ON <object\_names> FROM (user-name list) | (role-name list) | PUBLIC [CASCADE | RESTRICT]

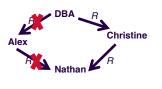
- ¬ <pri>privilege list>: privilege[(attribute list)]
- □ Cascade: revokes privileges from <u>all users</u> who got the privileges from a user in the user-name list
  - It revokes only the privileges derived/granted by the user invoking the Revoke statement

CS1555/2055, Panos K. Chrysanthis - University of Pittsburgh

### Access Control Lattice

- Example scenario:
  - DBA grants R to Alex and Christine with grant option;
  - Alex grants R to Nathan with grant option;
  - Christine grants R to Nathan with grant option;
  - DBA revokes R from Alex CASCADE:
- Nathan still has access to R
  - DBA revokes R from Christine





CS1555/2055, Panos K. Chrysanthis - University of Pittsburgh