Database Authorization

Harman Gill
SJSU

Content from Database Systems-The Complete Book and Oracle Administration SQL guide

Database Authorization

- Make sure users see only the data they are supposed to see.
- Guard the database access against modifications by malicious users.

Database Security

- Maintain security of the database access and use in multiple-user environment.
  - System level security
    - Access to database (username/password)
    - Disk space allocated to users
  - Data level security
    - Access and use of database objects

Privileges

- User have privileges
  - user can only operate on data which they are authorized
  - Privileges on database objects
- Similar to File system privileges
  - Database privileges more fine grained
  - e.g. For Relation R1(A1,A2,A3,A4,A5) and user Foo, Foo may be authorized for:
    - UPDATE(A1,A4) ON R1

Example

DELETE FROM instructor

WHERE id IN (SELECT id FROM teaches

WHERE course_id = 'CS157A')

- Relation : Object Privileges (Columns)
- instructor : DELETE
- instructor : SELECT (id)
- teaches : SELECT (id, course_id)

Privileges

- Right to execute particular SQL statements
- System Privileges
  - Gaining access to the database
    - CREATE/DROP USER, CREATE/DROP ANY TABLE, CREATE/DROP VIEW
  - Typically provided by DBA
- Object Privileges
  - Manipulating the content of database objects
  - ALTER, DELETE, UPDATE, INSERT, INDEX, SELECT

System Privileges

CREATE USER user

IDENTIFIED by password;

- User does not have any privileges on creation
- DBA can grant privileges to the new User

Note: Schema is collection of objects like table, views, and indexes. The schema is owned by database user and has the same name as that user.

Granting System Privileges

GRANT privilege [, privilege…]

TO user [, user/ role, PUBLIC,…];

- *privilege – create table, create view, etc.*
- PUBLIC designates that every user is granted the privilege
- System privileges saved in Catalog(System tables)

Privileges manageability (ROLE)

- ROLE is a named group of related privileges that can be granted to the user.
  - Makes it easier to maintain privileges
  - A user can have access to several ROLEs
  - Several users can be assigned the same ROLE

CREATE ROLE manager;

GRANT create table, create view TO manager;

GRANT manager TO foo, bar;

Object Privileges

GRANT object_priv [(columns)]

ON object

TO {user|role|PUBLIC}

[WITH GRANT OPTION]

- Object creator is owner
- Owner has all privileges and can grant any object privileges to other user or role
- WITH GRANT OPTION allows the grantee to grant the object privileges to other users and roles

Object Privileges

GRANT delete, update(id, dept_name)

ON instructor

TO foo, manager

WITH GRANT OPTION;

- To grant privileges on an database object
  - Object must be in your own schema
  - Or you must have granted the object privileges WITH GRANT OPTION

Revoking Object Privileges

REVOKE {privilege [, privilege…]|ALL}

ON object

FROM user [, user/ role, PUBLIC,…]

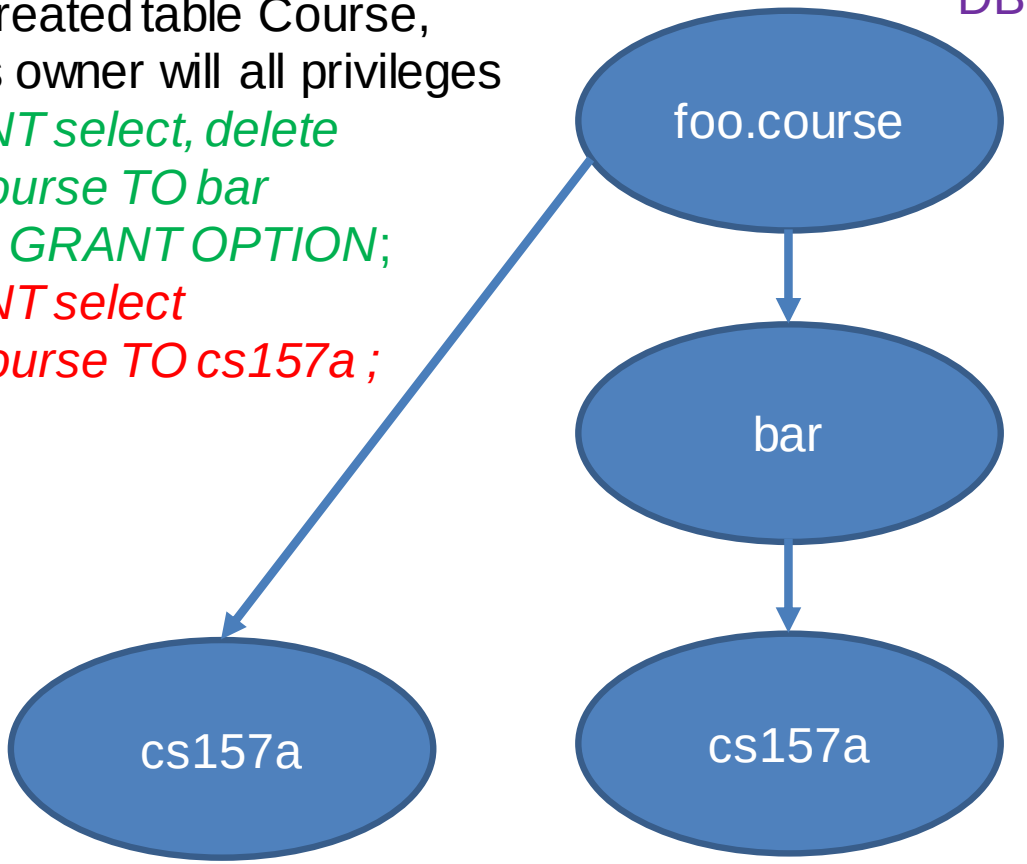
[CASCADE]

- CASCADE – privileges granted to others through the WITH GRANT OPTION are also revoked (transitively)
  - Except privileges granted from other sources
- Oracle does not permit circular grants

GRANT diagram

DB Users: foo, bar, and cs157a

Foo created table Course,
Foo is owner will all privileges
GRANT select, delete
ON course TO bar
WITH GRANT OPTION;
GRANT select
ON course TO cs157a ;

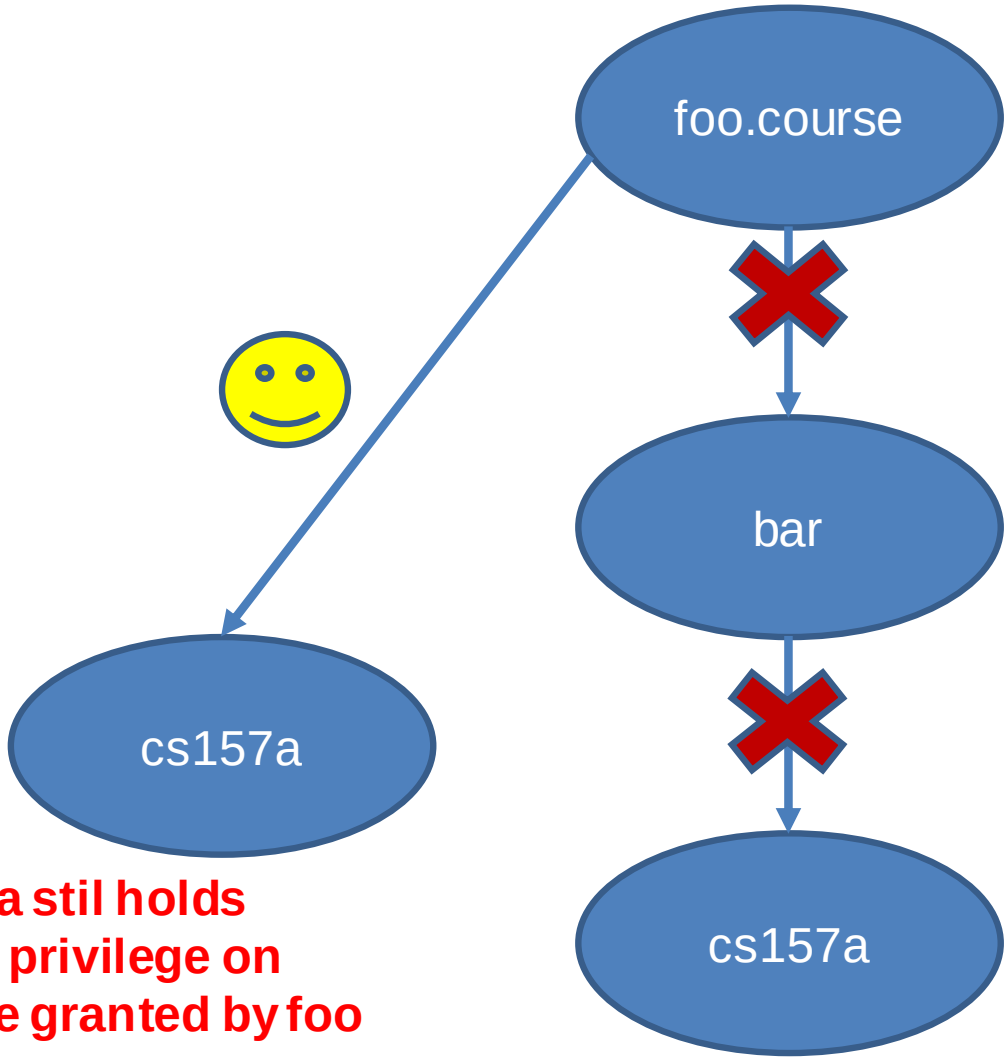


bar:
GRANT select
ON course TO cs157
WITH GRANT OPTION;

cs157a holds select privilege (with ability to grant to others)

cs157a also holds select privilege granted by foo

GRANT diagram



foo:
REVOKE select,delete
ON course
FROM bar;

cs157a stil holds select privilege on course granted by foo

Leveraging object-level privileges

- Are object-level operational privileges on single relation enough?
  - Allow user Foo to select information of Computer Sci. instructors only?
  - Foo (instructors : Select, Delete)
    - Foo will be able to access all tuples (all instructors)
    - How do we filter out tuples? So, that Foo can only see tuples with Computer Sci. department name.

Privileges on Views rather than Tables

- Solution:
  - *CREATE VIEW instrCS as*

    *SELECT * FROM instructor*

    WHERE dept_name = 'Computer Sci.'
  - Foo (instrCS : Select, Delete)
  - Question: Allow Foo to only delete instructors who belong to Computer Sci. department?
    - Will above solution (using Views) work?