

Sean Poston
4/14/2020
CY201 Database HW

Homework - Database Security
Total = 30 points

Instructions:

- 1) Each new question should start from a new page. Pls copy-paste the question before your response.
- 2) Although you can work in a group, the final submission is an individual assignment.
- 3) Simple and clear arguments or comments in Bullet points about the solution Well-labeled block diagram as and when required
- 4) Keywords are highlighted/underlined
- 5) Please, submit a typed response. Handwritten response is unacceptable.

Pls follow above policies, otherwise you will lose 10% for each violation.

1. (10 points) Consider the following scenario:

Student “John Smith” receiving read access of his college transcript from the university registrar for Spring 2020

The legitimate representation in **System R authorization model** for the above is:

<John_Smith, READ, transcript, Spring 2020, Registrar, YES>

For the following cases, provide the sample System R authorization representation:

- a) Student “Jane Doe” receiving read access of her college transcript from the university registrar for Spring 2020

<Jane_Doe, READ, transcript, Spring 2020, Registrar, NO>

- b) Assistant Registrar “Jack Roy” receiving write access for student transcripts from the university registrar for Spring 2020

<Jack_Roy, WRITE, transcript, Spring 2020, Registrar, YES>

- c) Student “Jane Doe” receiving read access of assignment 1 from Moodle for Spring 2020

<Jane_Doe, READ, assignment 1, Spring 2020, Moodle, NO>

- d) Professor “Aubrey Paul” receiving read and write access of assignment 1 from Moodle for Spring 2020

<Aubrey_Paul, READ_WRITE, assignment 1, Spring 2020, Moodle, NO>

- e) Professor “Aubrey Paul” receiving read and write access of college transcript from the university registrar for Spring 2020

<Aubrey_Paul, RW, transcript, Spring 2020, Registrar, NO>

2. (10+10 points) Sample SQL commands - consider the following scenario:

Incoming freshman student “John Smith” receiving read access of his Comp Science transcript from the university registrar for Spring 2020

This action can be expressed with the following table:

Grant or revoke	Type of rights	Table name	User list name
Grant	Read	Spring2020_CS_Transcript	Incoming freshman students

Sample command:

```
grant read on Spring2020_CS_Transcript to freshman2020
```

For the following cases, provide the sample table (see template below) **and** SQL commands:

- a) Student “Jane Doe” receiving read access of her MBA degree transcript for Spring 2020

GRANT read ON Spring2020_CS_Transcript TO Jane_Doe

- b) Graduating student “Jack Roy” will be unable to access his MBA degree transcript after Spring 2020

REVOKE read ON Spring2020_MBA_Transcript TO Jack_Roy

- c) Professor “Jack Darcy” receiving read and write access of “Intro to CS” course for Spring 2020

GRANT read_write ON Intro_to_CS TO Jack_Darcy

- d) Professor “Aubrey Paul” will no longer have any access for “Intro to CS” course in Spring 2021 (because another faculty is teaching this course)

REVOKE read_write ON Intro_to_CS TO Aubrey_Paul

- e) Assistant Registrar “Jack Roy” receiving read and write access for transcripts belonging to multiple student groups such as Management and CS.

	Grant or revoke	Type of rights (read or write or both)	Table name	User list name
a)	GRANT	read	Spring2020_MBA_Transcript	Student
b)	REVOKE	read	Spring2020_MBA_Transcript	Student
c)	GRANT	read_write	Intro_to_CS	Faculty
d)	REVOKE	read_write	Intro_to_CS	Faculty
e)	GRANT	read_write	Management Transcript, CS Transcript	Faculty

3. (5 points) In few sentences explain the difference between Auditability and Availability requirements w.r.t. databases.

Auditability is the power of a system to track what users have done. A good system will be able to log whenever a user opens or updates a file. **Availability** is simply the ability of a system to be accessed by authorized parties. A good system will have 99% uptime and will have granted all the users their correct privileges.

4. (15 points) Database Administrator can assign an owner to an entire schema and grant the appropriate access privileges. The owner of a database object can grant privileges to another user. This second user can then pass along the privileges to a third user and so on. The DBMS keeps track of the cycle of granting of privileges.

Authorization Matrix

We can think of the two levels of users and database objects forming a matrix for the purpose of granting access privileges. Set the users as columns and the database objects as rows. Then in the cells formed by the intersection of these columns and rows we can specify the type of privilege granted.

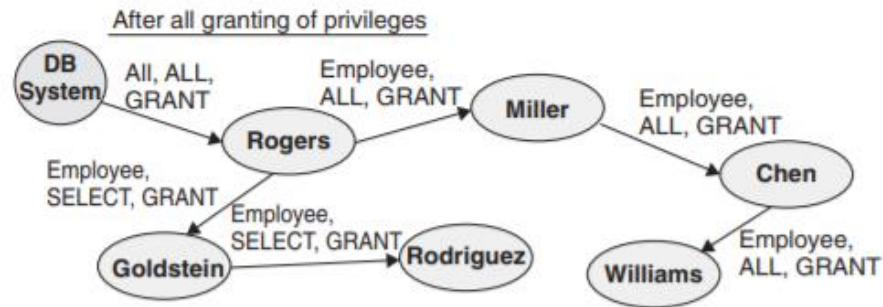
Now consider Company X where at the level of users, access privileges include the following:

CREATE privilege	To create a database schema, a table or relation, or a user view
ALTER privilege	To alter and make changes to schema such as adding or eliminating columns
DROP privilege	To delete a table or view
SELECT privilege	To retrieve data
MODIFY privilege	To add or insert, update, or delete data

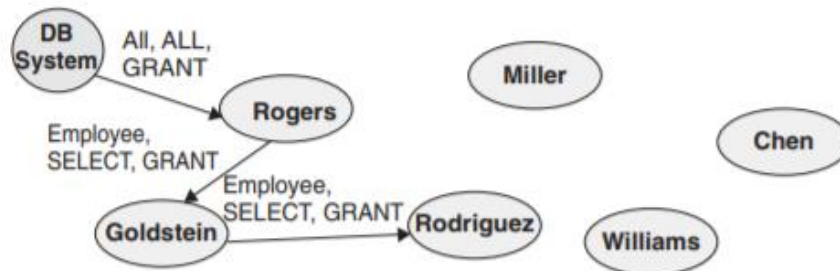
Here is an example of a cycle of privileges passed along from Rogers who is the head of the IT department in Company X, who is the owner of table EMPLOYEE:

By Rogers	GRANT ALL PRIVILEGES ON EMPLOYEE TO Miller WITH GRANT OPTION
By Miller	GRANT ALL PRIVILEGES ON EMPLOYEE TO Chen WITH GRANT OPTION
By Chen	GRANT ALL PRIVILEGES ON EMPLOYEE TO Williams WITH GRANT OPTION
By Rogers	GRANT SELECT ON EMPLOYEE TO Goldstein WITH GRANT OPTION
By Goldstein	GRANT SELECT ON EMPLOYEE TO Rodriguez WITH GRANT OPTION
By Rogers	REVOKE ALL PRIVILEGES ON EMPLOYEE FROM Miller CASCADE

Study the authorization graph below.



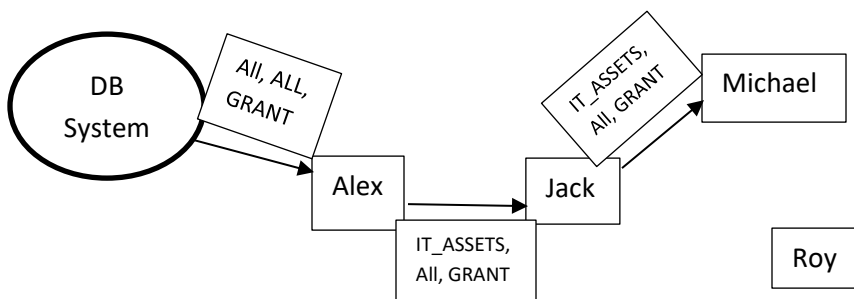
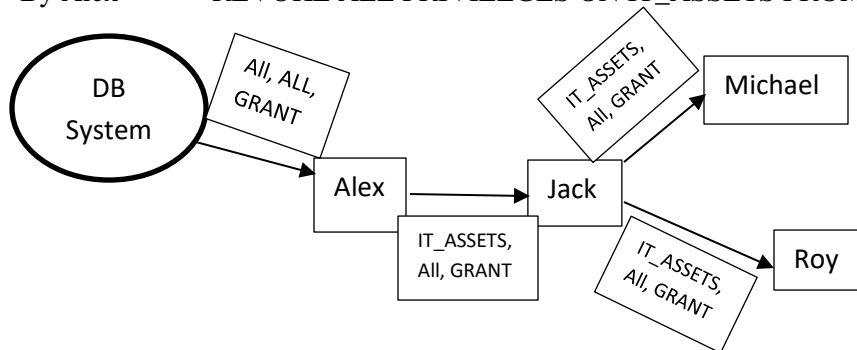
After revoking of privileges from Miller by Rogers with cascade option



Authorization Graph

Using above authorization graph as a reference, create a similar graph with Alex as the head of Testing department with the following cycle of privileges (5 points):

By Alex GRANT ALL PRIVILEGES ON IT_ASSETS TO Jack WITH GRANT OPTION
 By Jack GRANT ALL PRIVILEGES ON IT_ASSETS TO Michael WITH GRANT OPTION
 By Jack GRANT ALL PRIVILEGES ON IT_ASSETS TO Roy WITH GRANT OPTION
 By Alex REVOKE ALL PRIVILEGES ON IT_ASSETS FROM Roy CASCADE



Create the authorization matrix for all the employees of Company X and explain your choice in a sentence **(10 points)**:

Employee name	Database Object	Privilege	Your comments
Rogers	Employee Record	Modify	Rogers is the admin.
Miller	Miller was revoked from the system.
Chen	Chen's revocation was cascaded from Miller.
Williams	Williams's revocation was cascaded from Miller through Chen.
Goldstein	Employee Record	Select	Goldstein was granted select privileges by Rogers.
Rodriguez	Employee Record	Select	Rodriguez was granted select privileges by Goldstein.