Access control activities

Overview

The exercise here is a simple implementation from a problem statement. You will produce the schema for a simple database (three tables), populate it with data, and then establish the access controls, test them and review the effect. Suggestions are then made for you to investigate some of the system tables.

The problem

You have received the following account of the access security requirements for an SQL database system.

> The database has three tables: CUSTOMER (keyed on name and street num- ber); ORDER (keyed on date-of-receipt and the foreign key from CUSTOMER), and ORDER-ITEM (keyed on item-name and the foreign key from ORDER).
>
> The system is to process sales orders. Entry and access to documents and the progressing of orders is handled by the sales office. There are currently seven staff in this office. Tracey, the supervisor, needs to be able to see and change everything. Bill, Sheila and Govind do most of the routine work, but especially they cannot create new customers.
>
> There are a few other things. Make sure that large orders, say above £1000, cannot be handled by anyone except Tracey and Govind. Also ensure that a temporary member of staff can process orders but cannot see the customer details.

1. Produce an analysis and the necessary SQL statements to handle the problems.
2. Implement the database, populate it with test data and apply your security statements.
3. Test your access control mechanism thoroughly.
4. If, when you see the sample solution, either your analysis or testing are faulty, you need to find out why.
5. Indicate any additional SQL security measures that could be taken.
6. Comment on the strengths and weaknesses of the measures you have taken. The

following activities will help you through solving the problem, step by step.

Activity 1 – Creating the database schema

Using the data definition statements from SQL, produce a script to create three tables (table 1 is related to many rows of table 2 which is related to many rows of table 3).

You may already have a database schema which can be used for this purpose, but in any case you must ensure that the primary and foreign keys are correctly declared.

Activity 2 – Populating the database

This is a security exercise so the data itself need not be to normal test data standards. Make sure that the data is easily recognisable – use meaningful values and remember that foreign key fields should be present.

Activity 3 – Analysing the problem

Treat the names given as user-roles (otherwise the problem becomes too obscure for a first attempt). Develop a matrix of user against database resource. For this exercise, the database resources in question are the base tables and views (virtual tables).

Your matrix will make it clear where access is to be permitted and to whom. These requirements translate directly to an SQL script of GRANT statements. Produce this script on paper and check it manually.

Activity 4 – Executing the security script (if you have a DBMS that permits this)

If you don't have an executing environment, then get a friend to critique your work so far.

Activity 5 – Testing the access control (if you have a DBMS that permits this)

Formulate SELECT statements from the problem specification and issue SE- LECT statements to check that they have been correctly implemented. If you find problems, correct them at the point they occurred.

Activity 6 – Conclusion

Indicate any additional SQL security measures that could be taken, and comment on the strengths and weaknesses of the measures you have taken.

Activity 7 – Postscript

Well, how well did you do? Remember

Tracey?

After your work, she thought she should have a raise. She asked and was refused and then returned to her desk. To answer these questions, refer to your database design and security script.

1. Tracey then tried to delete the CUSTOMER table. Did she succeed?
2. I hope not, but if so, why? Did you not inadvertently give her SYSADM privileges?
3. She then tried to delete some customers. Did she succeed? Did the deletes cascade?

4. She tried to insert a line in all orders over £1000 for 500 coffee Machines.
Did she succeed?

5. And how was the problem detected?
6. She tried to change her password? Did she succeed?
7. How much privilege can any one individual ever be given?