

BCA Part II

Paper XI: DBMS using Access

Topic: Security in Database

Compiled by: Dr. Kiran Pandey

(School of Computer Science)

Email-id: kiranpandey.nou@gmail.com

Database security has many different layers, but the key aspects are:

Authentication

User authentication is to make sure that the person accessing the database is who he claims to be. Authentication can be done at the operating system level or even the database level itself. Many authentication systems such as retina scanners or bio-metrics are used to make sure unauthorized people cannot access the database.

Authorization

Authorization is a privilege provided by the Database Administer. Users of the database can only view the contents they are authorized to view. The rest of the database is out of bounds to them.

The different permissions for authorizations available are:

- **Primary Permission** - This is granted to users publicly and directly.
- **Secondary Permission** - This is granted to groups and automatically awarded to a user if he is a member of the group.
- **Public Permission** - This is publicly granted to all the users.
- **Context sensitive permission** - This is related to sensitive content and only granted to a select users.

The categories of authorization that can be given to users are:

- **System Administrator** - This is the highest administrative authorization for a user. Users with this authorization can also execute some database administrator commands such as restore or upgrade a database.
- **System Control** - This is the highest control authorization for a user. This allows maintenance operations on the database but not direct access to data.

- **System Maintenance** - This is the lower level of system control authority. It also allows users to maintain the database but within a database manager instance.
- **System Monitor** - Using this authority, the user can monitor the database and take snapshots of it.

Database Integrity

Data integrity in the database is the correctness, consistency and completeness of data. Data integrity is enforced using the following three integrity constraints:

- **Entity Integrity** - This is related to the concept of primary keys. All tables should have their own primary keys which should uniquely identify a row and not be NULL.
- **Referential Integrity** - This is related to the concept of foreign keys. A foreign key is a key of a relation that is referred in another relation.
- **Domain Integrity** - This means that there should be a defined domain for all the columns in a database.