**Introduction to database Security**

Database management systems are increasingly being used to store information about all aspects of an enterprise. The data stored in a DBMS is often vital to the business interests of the organization and is regarded as a corporate asset

**Database Security**

**Database security** refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks. OR

Is the means of ensuring that data is kept from corruption and that access to it is suitable controlled. Thus data security helps to ensure privacy. It also helps in protecting personal data. Data security is part of the larger practice of Information security.

Data is the raw form of information stored as columns and rows in our databases, network servers and personal computers.

**Objectives to be considered**

There are three main objectives to consider while designing a secure database application.

1. **Secrecy:**Information should not be disclosed to unauthorized users. E.g. a student should not be allowed to examine other students' grades.
2. **Integrity:**Only authorized users should be allowed to modify data. E.g. students may be allowed to see their grades, yet not allowed (obviously!) to modify them.
3. **Availability:** Authorized users should not be denied access. E.g. an instructor who wishes to change a grade should be allowed to do so.

To achieve these objectives, a clear and consistent *security policy* should be developed to described what security measures must be enforced. In particular, we must determine what part of the data is to be protected and which users get access to which portions of the data.

Next, the security mechanisms of the underlying DBMS (and OS, as well as external mechanisms such as securing access to buildings and so on) must be utilized to enforce the policy. We emphasize that security measures must be taken at several levels. Security leaks in the operating system or network connections can circumvent database security mechanisms.

**Types of Database Security Control**

- Access Control
- Database Audit
- Authentication
- Backup
- Password
- Encryption

**Access Control**

An Access Control mechanism is a system of controlling data that is accessible to a given giver. This implies the use of authentication and authorization. A computer system that is meant to be used by those authorized to do so must attempt to detect and exclude the unauthorized users.

**Approach to Access Control**

A DBMS offers two main approaches to access control

1. **Discretionary Access Control:**Discretionary access control (DAC) is a type of security access control that grants or restricts object access via an access policy determined by an object's owner group and/or subjects. DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password. DACs are

discretionary because the subject (owner) can transfer authenticated objects or information access to other users. In other words, the owner determines object access privileges.

2. **Mandatory Access Control**: is a type of access controlin which only the administrator manages the access controls. The administrator defines the usage and access policy, which cannot be modified or changed by users, and the policy will indicate who has access to which programs and files. MAC is most often used in systems where priority is placed on confidentiality.

**Database Audit**

It involves observing a database so as to be aware of the actions of database users. Database administrators and consultants often set up auditing for security purposes, for example, to ensure that those without the permission to access information do not access it

**Authentication**

Is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. In contrast with identification, which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the authenticity of a website with a digital certificate, determining the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

**Backup**

Is the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. The verb form is to **back up** in two words, whereas the noun is backup.

**Password**

This is an un-spaced sequence of secret characters used to enable access to a file, program, computer system and other resources.

**Encryption**

Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text ; encrypted data is referred to as cipher text.

**Roles of the database administrator in security**

The database administrator (DBA) plays an important role in enforcing the security-related aspects of a database design. In conjunction with the owners of the data, DBA will probably also contribute to developing a security policy. The DBA has a special account, which we will call the system account, and is responsible for the overall security of the system.

DBA deals with the following:

- Back up and recover the database.
- Install and configure Oracle software.
- Create new databases.
- Design the database schema and create any necessary database objects.
- Formulate optimal application SQL.
- Ensure database security is implemented to safeguard the data.
- Work closely with application developers and system administrators to ensure all database needs are being met.
- Apply patches or upgrades to the database as needed.
- Maintaining archiveddata
- Contacting database vendorfor technical support
- Generating various reports by querying from database as per need
- Managing and monitoring data replication

**Encryption**

The basic idea behind encryption is to apply an *encryption algorithm*, which may be accessible to the intruder, to the original data and a user-specified or DBA-specified *encryption key* which is kept secret.

Another approach to encryption, called public-key encryption, has become increasingly popular in recent years. The encryption scheme proposed by Rivest, Shamir and Adleman, called RSA, is a well-known example of public-key encryption. Each authorized user has a public encryption key, known to everyone, and a private description key (used by the decryption algorithm), chosen by the user and known only to him or her.