Chapter 6
Some Issues on Databases

Database Security and Integrity

- A database represents an essential corporate resource that should be properly secured using appropriate controls.
- Database security encompasses hardware, software, people and data
- Database security and integrity is about protecting the database from being inconsistent and being disrupted.
- Multi-user database system - DBMS must provide a database security and authorization subsystem to enforce limits on individual and group access rights and privileges.

- Database misuse could be
  - Intentional or accidental,
- Accidental inconsistency could occur due to:
  - System crash during transaction processing
  - Anomalies due to concurrent access
  - Anomalies due to redundancy
  - Logical errors
- Intentional misuse could be:
  - Unauthorized reading of data
  - Unauthorized modification of data or
  - Unauthorized destruction of data
- Accidental misuse is easier to cope than intentional misuse.

- Database security is considered in relation to the following situations:
  - Theft and fraud
  - Loss of confidentiality (secrecy)
  - Loss of integrity
  - Loss of availability

- **Database security** - the mechanisms that protect the database against intentional or accidental ***threats.***

- Examples of threats:
  - Unauthorized modification or copying of data
  - Program alteration
  - Wire-tapping
  - Illegal entry by hacker
  - Theft of data, programs, and equipment
  - Failure of security mechanisms, giving greater access than normal
  - Inadequate staff training
  - Electronic interference and radiation
  - Data corruption owing to power loss or surge
  - Fire (electrical fault, lightning strike, arson), flood, bomb
  - Physical damage to equipment
  - Breaking cables or disconnection of cables
  - Introduction of viruses

Computer-based security controls for a multi-user environment:

- **Authorization**
  - The granting of a right or privilege that enables a subject to have legitimate access to a system or a system's object
  - Authorization controls can be built into the software, and govern not only what system or object a specified user can access, but also what the user may do with it
  - Authorization controls are sometimes referred to as ***access controls***
  - The process of authorization involves authentication of ***subjects*** (i.e. a user or program) requesting access to ***objects*** (i.e. a database table, view, procedure, trigger, or any other object that can be created within the system)

- **Backup and recovery**
  - Backup is the process of periodically taking a copy of the database and log file (and possibly programs) on to offline storage media
  - A DBMS should provide backup facilities to assist with the recovery of a database following failure
  - Database recovery is the process of restoring the database to a correct state in the event of a failure
  - Journaling is the process of keeping and maintaining a log file (or journal) of all changes made to the database to enable recovery to be undertaken effectively in the event of a failure
  - The advantage of journaling is that, in the event of a failure, the database can be recovered to its last known consistent state using a backup copy of the database and the information contained in the log file
  - If no journaling is enabled on a failed system, the only means of recovery is to restore the database using the latest backup version of the database
  - However, without a log file, any changes made after the last backup to the database will be lost

- **Integrity**
  - Integrity constraints contribute to maintaining a secure database system by preventing data from becoming invalid and hence giving misleading or incorrect results
    - Domain Integrity
    - Entity integrity
    - Referential integrity
    - Key constraints

Levels of Security Measures

- Security measures can be implemented at several levels

  - **Physical Level:** concerned with securing the site containing the computer system should be physically secured. The backup systems should also be physically protected from access except for authorized users.

  - **Human Level:** concerned with authorization of database users for access the content at different levels and privileges.

  - **Operating System:** concerned with the weakness and strength of the operating system security on data files. Weakness may serve as a means of unauthorized access to the database. This also includes protection of data in primary and secondary memory from unauthorized access.

  - **Database System:** concerned with data access limit enforced by the database system. Access limit like password, isolated transaction and etc.

- Even though we can have different levels of security and authorization on data objects and users, ***who access which data is a policy matter rather than technical.***

Authentication

- All users of the database will have different access levels and permission for different data objects, and authentication is the process of checking whether the user is the one with the privilege for the access level.
- Is the process of checking the users are who they say they are.
- System checks whether the user with a specific username and password is trying to use the resource.
- Associated with each identifier is a password, chosen by the user and known to the operation system, which must be supplied to enable the operating system to authenticate who the user claims to be

Forms of user authorization on the data

- **Read Authorization**: the user with this privilege is allowed only to read the content of the data object.
- **Insert Authorization**: the user with this privilege is allowed only to insert new records or items to the data object.
- **Update Authorization**: users with this privilege are allowed to modify content of attributes but are not authorized to delete the records.
- **Delete Authorization**: users with this privilege are only allowed to delete a record and not anything else.

- Different users, depending on the power of the user, can have one or the combination of the above forms of authorization on different data objects.

- Major responsibilities of DBA in relation to authorization of users :
  - ***Account Creation:*** involves creating different accounts for different **USERS** as well as **USER GROUPS.**
  - ***Security Level Assignment***: involves assigning different users at different categories of access levels.
  - ***Privilege Grant:*** involves giving different levels of privileges for different users and user groups.
  - ***Privilege Revocation:*** involves denying or canceling previously granted privileges for users due to various reasons.
  - ***Account Deletion:*** involves in deleting an existing account of users or user groups.