DATABASE MANAGEMENT SYSTEM

Subash Manandhar

Chapter 5 : Security

- Unauthorized access or manipulation of database creates problems/troubles for organization.
- Security refers to protection of data against unauthorized disclosure, alteration or destruction.
- Main objectives of designing secure database systems:
  - Secrecy
  - Integrity
  - Availability
- Database security is about controlling access to information i.e. some information be available freely and other information be available to certain authorized people or groups.
- Database security system stores authorization rules and enforces them for database access.

Chapter 5 : Security

- Database Security can be
  - **Physical security**
    - Refers to security of hardware and protection of site where computer resides.
  - **Logical security**
    - Refers to software safeguards for organization systems including user identification, password access, access rights, authority levels.
- **Database Security Levels**
  - to ensure db security, security at different levels must be maintained.
  - A weakness at low level of security allows circumvention of strict high level security measures.
  - **Database System:**
    - Database system have to be ensured that authorization restrictions are not violated.

Chapter 5 : Security

- **Operating System:**
  - Weakness in OS security is concerned with unauthorized access to db.
- **Network:**
  - s/w level security within network s/w is important.
- **Physical:**
  - Sites with computer system must be physically secured against armed entry by intruders.
- **Human:**
  - Users must be authorized carefully.

Data Security is protecting data against unauthorized users.
Data Integrity is protecting data against authorized users.
Verifying identity of user is authentication.

Chapter 5 : Security

- **Authorization:**
  - It is a security mechanism used to determine user/client privilege or access level related to system resources.
  - During authorization, system verifies authenticated user's access rule and either grant or refuse resource access.
  - Authorization includes:
    - Permitting only certain users to access , process or alter data.
    - Applying varying limitations on user's access or action. Limitations placed on users can apply to object such as schema, tables, rows etc.
  - Authorization on data include:
    - Authorization to read data
    - Authorization to insert new data
    - Authorization to update data
    - Authorization to delete data

Chapter 5 : Security

- **Authorization:**
  - Each of these type of authorization is called privilege.
  - Users are authorized all or none or combination of these types of privileges on specified parts of database such as relation or view.
  - In addition to authorization on data, users may be granted authorization on database schema, allowing them to create, modify or drop relations.
  - The ultimate form of authority is that given to DBA(Database Administrator)
  - DBA may authorize new users, restructure the database etc.

Chapter 5 : Security

- **Granting and Revoking of Privilege:**
  - SQL standard include the privileges select, insert, update, delete.
  - ‘all privileges’ can be used for all allowable privileges.
  - A user who creates a new relation is given all privileges automatically.
- **Grant Statement**

```
GRANT <privilege list>
ON <relation name or view name>
TO <user/role list>
```

  - **To read tuples in relation, ‘select’ authorization is required.**

```
e.g. GRANT select
         ON employee
         TO Ram, Hari;
```

Chapter 5 : Security

- **To update any tuple in relation, ‘update’ authorization is required.**
- **Update authorization may be given either on all attributes of relation or only some.**

```
e.g. GRANT update(salary)
     ON employee
     TO Ram, Hari ;
```

```
GRANT update
ON employee
TO Ram, Hari ;
```

- **To insert tuples in relation, ‘insert’ authorization is required.**
- **‘insert‘ privilege may also specify a list of attributes.**
- **The system either gives default value or NULL for remaining attributes.**

```
GRANT insert
ON employee
TO Ram, Hari ;
```

```
GRANT insert(name, address)
 ON employee
 TO Ram, Hari ;
```

Chapter 5 : Security

- **To delete tuple from relation, ‘delete’ authorization is required.**

```
GRANT delete
ON employee
TO Ram, Hari ;
```

- Privileges granted to ‘public‘ are implicitly granted to all current and future users.
- **To revoke an authorization, use revoke statement.**

```
REVOKE <privilege list>
ON <relation name or view name>
FROM <user/role list>
```

```
REVOKE select
ON employee
FROM Ram, Hari ;
```

```
REVOKE update(salary)
ON employee
FROM Ram, Hari ;
```

Chapter 5 : Security

- System can support user groups also known as ‘roles’ and can thus provide a way of allowing all with same role to show the same privileges on the same object.
- Role is a database object that groups one or more privileges.
- Role can be assigned to users or groups or other roles by using GRANT statement.
- Users that are member of roles have privileges that are defined for the role with which to access data.

```
CREATE role instructor

GRANT select
ON employee
TO instructor;
```

Chapter 5 : Security

- **Cryptosystem:**
  - aim to solve problem by modifying data being transmitted in a manner that it become unintelligible to anyone but not for intended recipient.
- **Data Encryption:**
  - Is storing and transmitting data in encrypted form.
  - Original data is called plain text.
  - Plaintext is encrypted using encryption algorithm; whose inputs are plain text and encryption key.
  - Output is called Cipher text.
  - Encryption refers to the process of transforming data into a form that is unreadable unless the reverse process of decryption is applied.
  - Encryption algorithm use an encryption key to perform encryption and requires a decryption key to perform decryption.
  - Encryption is widely used today for protecting data in transit in a variety of applications such as data transfer on internet, cellular phone networks.

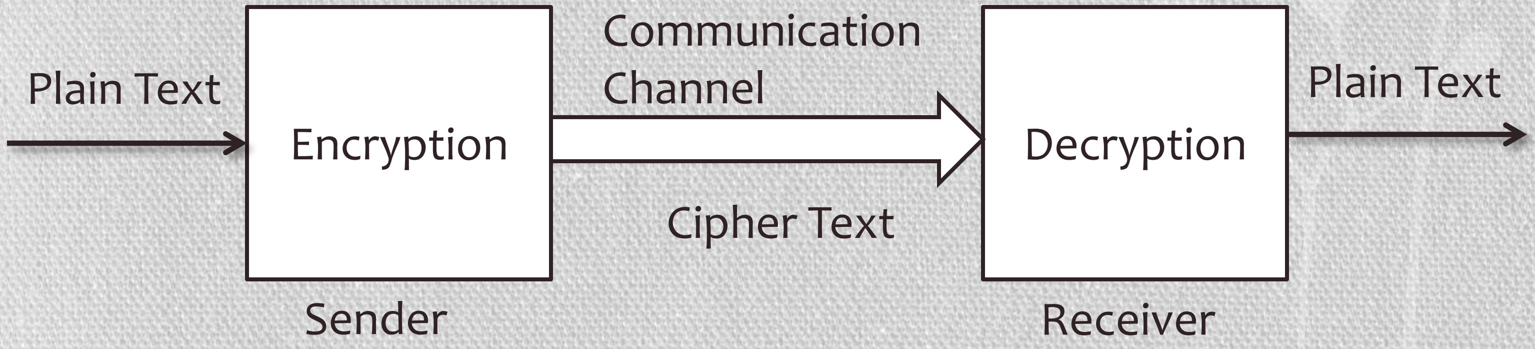
- **Data Encryption:**
  - Encryption is also used to carry out other tasks like authentication.
  - In database encryption is used to store data in secure way so that even if the data is acquired by unauthorized users, the data will not be accessible without a decryption key.
  - A good encryption technique has following properties:
    - It is relatively simple for authorized users to encrypt and decrypt data.
    - It depends on encryption key used to encrypt data.
      - In symmetric key encryption, encryption key is also used to decrypt.
      - In asymmetric key encryption, two different keys public and private key are used to encrypt and decrypt data.
    - Its decryption key is extremely difficult for an intruder to determine, even if intruder has encrypted data.
      - In asymmetric key encryption, its difficult to infer private key even if public key is available.

Chapter 5 : Security

- **Data Encryption:**
  - **Symmetric Key Encryption**
    - Authorized users must be provided with encryption key via secure mechanisms.
    - E.g. AES (Advanced Encryption Standard), DES (Data Encryption Standard)
  - **Asymmetric Key Encryption**
    - Two keys private and public
    - Public key are published
    - Private key is known to only to user to whom key belongs.
    - If user1 wants to store encrypted data, user1 encrypts them using public key E1, decryption requires private key D1.
    - E.g. RSA

Chapter 5 : Security

- **Data Encryption:**


Plain Text
Encryption
Communication Channel
Cipher Text
Decryption
Plain Text
Sender
Receiver