Chapter 6
Security

Introduction

Database security means the protection of data or information from accidental loss, unauthorized access, modification, destruction and unintended activities. In any organization, certain class of data should be available only to those persons who are authorized to access it. So data stored in database need to be protected from authorized access and from any kind of intentional or accidental corruption.

Needs of database security

Database security is needed for a database due to the following reasons.

1. Unauthorized disclose of information.
2. Unauthorized modification or destruction of valuable information.
3. Unauthorized use of service.
4. Denial of service to the authorized users.

To protect database, we must make security measures at several levels.

1. **Physical Security**
    a. The room where the computer storing a database must be itself strong and secured.
    b. Unknown person must be restricted to enter into system room.
    c. Placing backup copies of database in a separate location so that they remain safe in case of any disaster in office area.
    d. It also includes protection of database against fire, earthquake.
2. **Human**

    The unauthorized access of data should be prevented. There are many measures to protect data from unauthorized access like as password system. Also the employee of a company should not leak valuable information about the organization to outsiders.
3. **Operation System**

    No matter how secure the database system is, weakness in OS security may serve as a means of unauthorized access to the database.
4. **Network**

    The database information must be protected from hackers and attack of viruses, leakages of data while being transferred from one computer to other in a network or internet.
5. **Database System**

    Database system users may be authorized to access only limited portion of the database. Here user may be allowed to issue queries without any modification. Also several views can be utilized as a form of security in the database because it can be used to suppress the confidential columns from viewing and manipulation.

6. **Administrative Controls**

Administrative controls are the security and access control policy that determines what information will be accessible to what class of users.

Authorization

Authorization is the process of giving someone permission to do or have something.

In multi-user database systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is getting access. A user may have several form of authorization on parts of database.

- Read Authorization allows reading but not modification to database.
- Insert Authorization allows insertion of new data but not modification of existing data.
- Update Authorization allows modification of data not deletion of data.
- Delete Authorization allows deletion of data.

A database user may be assigned all, none, or combination of these types of authorization. In addition to these form of authorization for access to data, we may grant user authorization to modify the database schema.

- Index Authorization allows creation and deletion of indices.
- Resource Authorization allows the creation of new relations.
- Alteration Authorization allows the addition or deletions of attributes in relations.
- Drop Authorization allows the deletion of relations and attributes.

Logically, authorization is preceded by authentication.

Authentication

Authorization is the process to confirm what you are authorized to perform but Authentication confirms who you are. So the primary goal of authentication system is to allow access to the legal system users and deny access to unauthorized access. The most widely used authentication techniques are

1. **Password Based Authentication:**

   A **password** is a secret word or string of characters used for user authentication to prove identity to a resource, which should be kept secret from those not allowed access. It is not much reliable than other authentication system because if a weak password is chosen then it can be easily guessed. Google released a list of most common password types, all of which are considered unsecured because they are too easy to guess.

   Good criteria when choosing a password or setting up password guidelines includes the following:

   - Don't pick a password that someone can easily guess if they know who you are (for example, not your Social Security number, birthday, or maiden name)
   - Don't pick a word that can be found in the dictionary (since there are programs that can rapidly try every word in the dictionary!)
   - Don't pick a word that is currently newsworthy

- Don't pick a password that is similar to your previous password
- Do pick a mixture of letters and at least one number
- Do pick a word that you can easily remember

2. **Artifact Based Authentication:**

   It includes machine-readable batches and electronics cards. These cards consist of magnetic strip, which represents a unique identification number. Card reader may be installed in or near the terminal and users are required to supply the artifact for authentication. This form of authentication is common in ATMs in bank. Some companies also provide cards to their employee for authentication.

3. **Biometric Technique:**

   In this technique, the major groups of authentication mechanism are based on the unique characteristic of each user. This falls into two basic categories.

   a. Physiological Characteristics: Characteristics such as finger prints, facial characteristics, retina characteristics etc.
   b. Behavioral Characteristics: Characteristics such as voice pattern, signature pattern etc.

Access Control

Access control mechanism enforces rules who can perform what operation or who can access which data. This access control mechanism must concern with three basic components.

1. **Accessor (Subject):**

   A subject is an active element in the security mechanism that operates on the object. A subject is a user who is given some right to access a data object. A subject may be a class of users or even an application program. To provide security to object, identification and authentication of accessor is required. The process of identification may be performed with the help of password, finger print or voice pattern etc.

2. **Object to be accessed:**

   An object is something that needs protection. A typical object in a database environment could be a unit of data that need to be protected. Object can be classified as

   a. Data: These are prime candidates for protection. Data object may be file, record, table etc.
   b. Access Path: Access path to be followed for accessing a particular data item or service is an important object by itself in any security mechanism.
   c. Schema: The database schema is another object for protection. Since schema declaration defines access right to different data object, anyone having access to schema declaration can eventually attain access right to different data items also. This is highest level of security.
   d. Views: The views may involve read only facility of the data items and no modification will be permitted for one class of users while other call of user might be able to update view also.
   e. Communication Object: In a distributed database environment, some communication protocols have to be maintained for reliable communication of environment. The communication protocol may include necessary information for the identification and authentication of the sender and receiver.

3. **Types of Access Control:**

   Once an object is created, the owner may grant the following rights to object to the other authorized users.

   Read, insert, delete, update, run, create and destroy

Discretionary Access Control Vs Mandatory Access Control

In discretionary access control (DAC), the owner of the object specifies which subjects can access the object. This model is called discretionary because the control of access is based on the discretion of the owner. Most operating systems such as all Windows, Linux, and Macintosh and most flavors of UNIX are based on DAC models.

In these operating systems, when we create a file, we decide what access privileges we want to give to other users; when they access our file, the operating system will make the access control decision based on the access privileges our created.

Mandatory access control (MAC) is a security strategy that restricts the ability individual resource owners have to grant or deny access to resource objects in a file system. MAC criteria are defined by the system administrator, strictly enforced by the operating system (OS) or security kernel, and are unable to be altered by end users

Mandatory access control works by assigning a classification label to each file system object. Classifications include confidential, secret and top secret. Each user and device on the system is assigned a similar classification and clearance level. When a person or device tries to access a specific resource, the OS or security kernel will check the entity's credentials to determine whether access will be granted.

For example, if a user has a security clearance of secret, and he requests a data object with a security classification of top secret, then the user will be denied access because his clearance is lower than the classification of the object.

Cryptography

Simply cryptography means hidden secret.

Cryptography is one of the techniques to improve security in computer system by encrypting sensitive data and information.

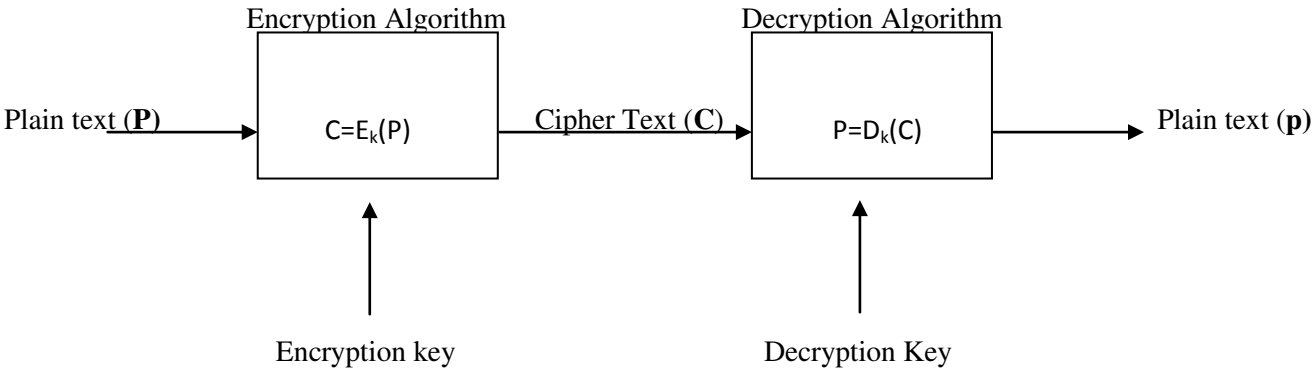
Encryption means modifying the data such a way that it becomes useless or unidentifiable or unreadable to the intruder (undesired person, program) but only the desired receiver can view the actual data. The original unencrypted data is called plain text or clear text. It can be encrypted using some encryption method parameterized by encryption key. The result is cipher text which is unreadable. The cipher text may be stored or transmitted over the secured communication medium. Now a plain text can be obtained by decrypting the cipher text using the decryption key. So use of key to reverse this encryption process and return the data to its original form is called **decryption**. Cryptography is used to protect e-mail messages, credit card information, computer password, electronic commerce etc.

Most practical cryptographic systems combine two elements:

- A process or algorithm which is a set of rules that specify the mathematical steps needed to encipher or decipher data.

- A cryptographic key (a string of numbers or characters), or keys. The algorithm uses the key to select one relationship between plaintext and cipher text out of the many possible relationships the algorithm provides. The selected relationship determines the composition of the algorithm's result.

A general model of cryptography system is shown below.



Types of Cryptography

There are two types of cryptography.

1. Private Key Cryptography (Symmetric Cryptography)

   A cryptography system that uses the same key for both encryption and decryption is called symmetric cryptography. The key used for encrypt and decrypt must only be know by the sender and receiver i.e. key must be private hence called as private key cryptography.

2. Public Key Cryptography (Asymmetric Cryptography)

   The main disadvantage of private key cryptography is key management since it requires greater number of keys because each distinct pair of communicating parties has to share different key. A cryptography system that used different keys for encryption and decryption are known as public key cryptography. In this system every user has two keys know as public key and private key. It is also called as asymmetric cryptography because the two keys are not identical. The public key is open for all interested users and a particular user only knows the private key. In public key encryption, encryption uses public key and decryption is performed using private key. When two part A and B wish to communicate they proceed as follows.

   The sender A looks for the receiver's public key E_b and uses it to generate cipher text $C=E_b(P)$ where P is the plain text. The receiver then receives the encrypted cipher text and decrypts the cipher text using his private key Db as $P= D_b(C)$ to get plain text P.

   Public key cryptography systems are often used to generate and verify digital signatures on electronic documents. The sender uses his or her private key to generate the digital signature. The receiver then uses the sender's public key to verify the identity of the sender. On the emerging information highway, the digital signature replaces the handwritten signature as a legal proof of authenticity.

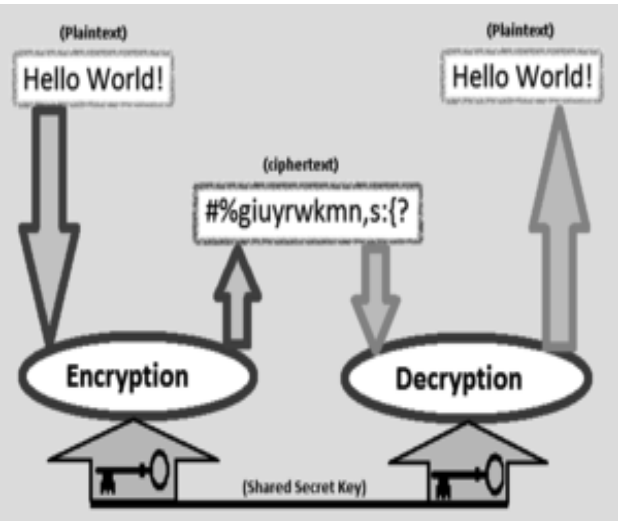


Fig : Private key Cryptography

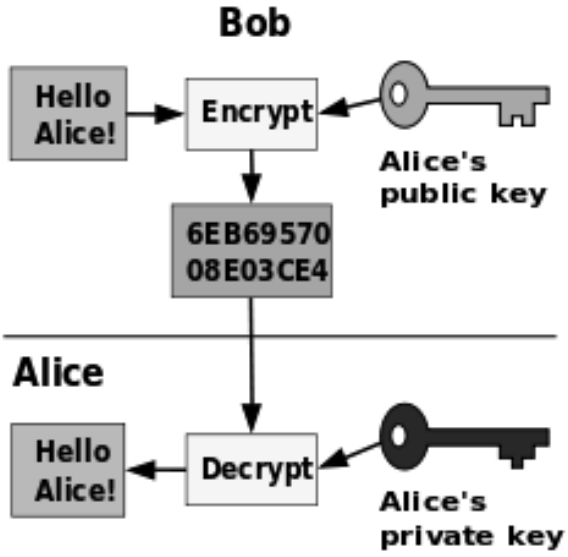


Fig: Public Key Cryptography