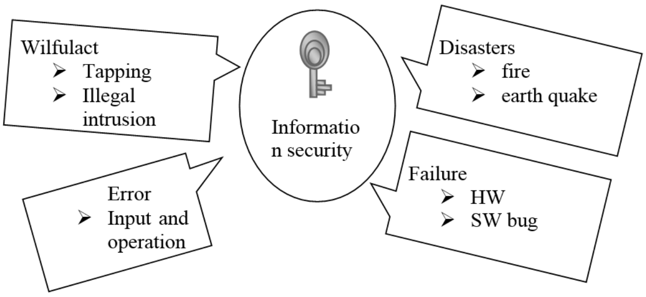
CHAPTER - 6

Security

6.1 Introduction

Any organizational information must be secured because every decision are based on information. *Information security* means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information.

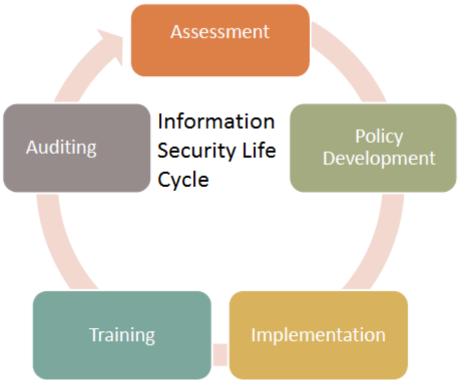


Database Security

Security is the protection of information and systems and hardware that use, store, and transmit that information. Database security is primarily concerned with the secrecy of data against intentional or unintentional threats. Designing and implementing a secure database involves achieving the following objectives:

- **Confidentiality:** Prevent the disclosure or leak of sensitive information from unauthorized people, resources, and processes.
- **Integrity:** The protection of system information or processes from intentional or accidental modification.
- **Availability:** The assurance that systems and data are accessible by authorized users when needed.
- **Authentication:** Making sure the data is from where it is supposed to be from.

The attack on information may be from diversified field such as insiders, ex-employee, competitors, customers, disasters, hackers or crackers, and cyber terrorists. To maintain the security, the security policy must be continuously monitored, tested, improved, and secured. This re-engineering process form a cycle called security wheel.



- **Security:** Means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. To provide security means to disclose only non-sensitive data, and reject any query that references a sensitive field.
- **Precision**: To protect all sensitive data while disclosing as much non-sensitive data as possible.

Security Attacks: Categorization

A. Interruption

- This is an attack on availability.
- Example: Cutting of a communication line or the disabling of the file management system.

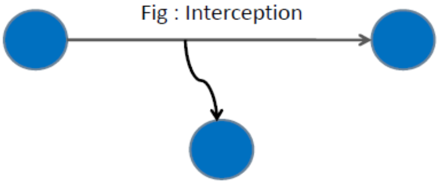


Fig : Interception

B. Interception

- This is an attack on confidentiality.
- Example: Wiretapping to capture data in a network and unauthorized copying of files or programs.

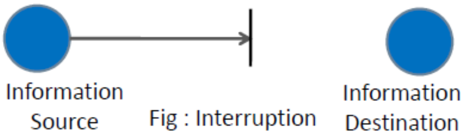


Fig : Interruption

C. Modification

- This is an attack of Integrity
- Example: Changing values in a data or modifying the content of message being transmitted.

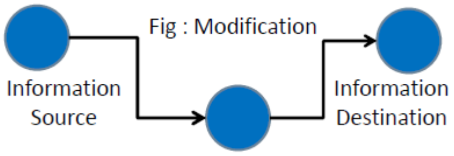


Fig : Modification

D. Fabrication

- This is an attack on authenticity
- Example: Insertion of fake messages in a network.

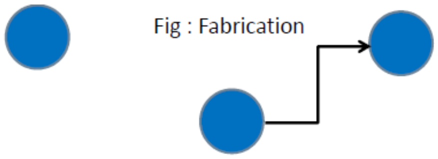


Fig : Fabrication

Security Classification for Information

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification. Common information security classification labels used by the business sector are: public, sensitive, private, confidential. Common information security classification labels used by government are: *Unclassified, Sensitive But Unclassified, Restricted, Confidential, Secret, Top Secret* and *their non-English equivalents.*

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification a particular information asset has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place.

6.2 Database Security and the DBA

The database administrator (DBA) is the central authority for managing a database system. The DBA’s responsibilities include granting privileges to users who need to use the system and classifying users and data in accordance with the policy of the organization. The DBA has a **DBA account** in the DBMS, sometimes called a **system** or **superuser account**, which provides powerful capabilities that are not made available to regular database accounts and users. DBA-privileged commands include commands for granting and revoking privileges to individual accounts, users, or user groups and for performing the following types of actions:

1. **Account creation.** This action creates a new account and password for a user or a group of users to enable access to the DBMS.
2. **Privilege granting.** This action permits the DBA to grant certain privileges to certain accounts.
3. **Privilege revocation.** This action permits the DBA to revoke (cancel) certain privileges that were previously given to certain accounts.
4. **Security level assignment.** This action consists of assigning user accounts to the appropriate security clearance level.

Whenever a person or group of person s need to access a database system, the individual or group must first apply for a user account. The DBA will then create a new account number and password for the user if there is a legitimate need to access the database. The user must log in to the DBMS by entering account number and password whenever database access is needed. The database system must also keep track of all operations on the database that are applied by a certain user throughout each login session. To keep a record of all updates applied to the database and of the particular user who applied each update, we can modify *system log*, which includes an entry for each operation applied to the database that may be required for recovery from a transaction failure or system crash. If any tampering with the database is suspected, a database audit is performed, which consists of reviewing the log to examine all accesses and operations applied to the database during a certain time period. A database log that is used mainly for security purposes is sometimes called an *audit trail*.

A. Access control

A security problem common to computer systems is that of preventing unauthorized persons from accessing the system itself, either to obtain information or to make malicious changes in a portion of the database. The security mechanism of a DBMS must include provisions for restricting access to the database system as a whole. This function, called **access control**, is handled by creating *user accounts* and *passwords* to control the login process by the DBMS.

In practice, there are two major approaches to data security.

- **Discretionary control**: In this type of security, a user will have different access rights, also known as privileges on individual items. Obviously, there are various limitations in terms of rights that different users have on various objects. For ***example***, in a system for which the discretionary control is used, a user may be able to access object X of the database, but cannot access object Y, while user B can access object Y, but cannot access object X. Discretionary control schemes are very flexible. We can combine rights and assign to users and objects according to our needs.

- **Mandatory control**: In this case, each data object is associated with a certain classification level and each user is given a certain permission level. A given data object can then be accessed only by users with the appropriate permission. Mandatory schemes are hierarchic in nature and are hence more rigid than discretionary ones.

B. Authentication

Authentication is the process by which users are identified by the DBMS and prove their identity to access the database. User and group identity validation is achieved through security facilities located outside of the DBMS that is, they are performed as part of the operating system or using a third-party security facility, such as Kerberos or Lightweight Directory Access Protocol (LDAP). Authentication of a user requires two elements: a *user ID* and an *authentication token*. The user ID allows the security component to identify the user and by supplying the correct authentication token (a password known only by the user and the security component), the user identity is verified. After successful authentication of a user, the authenticated user ID is mapped to an authorization ID. This mapping is determined by the authentication security plug-in.

If the default IBM (in DB2) shipped authentication security plug-in is used, there are two derived authorization IDs provided: system and session IDs. In this case both authorization IDs are derived in the same way from the user ID and are identical. The system authorization ID is used for checking the connect privilege to establish a connection. The session authorization ID is the primary ID for the next connection.

C. Authorization

After a user is authenticated, it is necessary to determine whether that user is authorized to access certain data or resources. Authorization is the process of granting privileges, which allows a subject to have legitimate access to a system or an object in a system. The definition of authorization contains the terms subject and object. The subject refers to a user or program and the term object addresses a table, a view, an application, procedure or any other object that can be created in the system.

Authorization control can be implemented by software elements and it can regulate both systems and objects to which a user has access and what a user can do with them. For this reason, the authorization is also called access control. For example, a user may be authorized to read records in a database, but cannot modify or insert a record.

Authorization rules are controls incorporated in the DBMS that restrict the action that user may take when they access data. When an authenticated user tries to access data, the authorization name of the user and the set of privileges granted to them, directly or indirectly through a group or a role, are compared with the recorded permissions. The result of the compare is used to decide whether to allow or reject the requested access. In order to perform different tasks, the DBMS requires that each user be specifically, implicitly, or explicitly authorized.

D. View-Based Access Control

Views allow the database to be conceptually divided into pieces in ways that allow sensitive data to be hidden from unauthorized users. In the relational model, views provide a powerful mechanism for specifying data-dependent authorizations for data retrieval.

Views allow a user to see information while hiding any information that the user should not be given access to. A view is the dynamic result of one or more relational operations that apply to one or more base tables to produce another table. A view is always based on the current data in the base tables from which it is built. The advantage of a view is that it can be built to present only the data to which the user requires access and prevent the viewing of other data that may be private or confidential. A user may be granted the right to access the view but not to access the base tables upon which the view is based.

E. Integrity Control

The aim of integrity control is to protect data from unauthorized use and update, by restricting the values that may be held and the operations that can be performed on data. Integrity controls may also trigger the execution of some procedure, such as placing an entry in a log that records what users have done what with which data. There are more forms of integrity controls.

The first form that we discuss is the integrity of the domain. A domain may be viewed like a way to create a user-defined data type. Once a domain is created it may be assigned to any field as its data type. Consequently any value inserted in the field must belong to the domain assigned. When a domain is created, it may use constraints (for example a CHECK constraint) to restrict the values to those which satisfy the imposed condition. An important advantage of a domain is that if it must change then it can be modified in a single place – the domain definition.

Assertions are also powerful constraints that enforce some desirable database conditions. They are checked automatically by the DBMS when transactions are run involving tables or fields on which assertion exists. If the assertion fails, the DBMS will generate an error message.

For security purposes one can use triggers as well. Triggers consist of blocks of procedural code that are stored in a database and which run only in response to an INSERT, UPDATE or DELETE command. A trigger, which includes an event, condition, and action, may be more complex than an assertion. It may prohibit inappropriate actions, it may cause special handling procedures to be executed, or it may cause a row to be written to a log file in order to store important information about the user and transactions made to sensitive data.

6.3 Encryption and Decryption

Sensitive and personal data stored within the database tables and critical data transmitted across the network, such as user credentials (user ID and password), are vulnerable and should be protected against intruders.

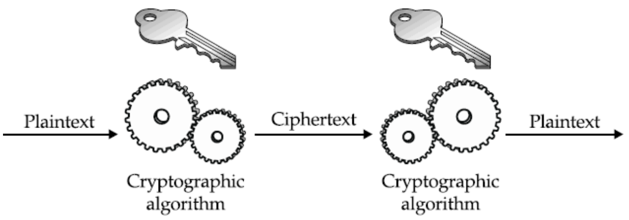
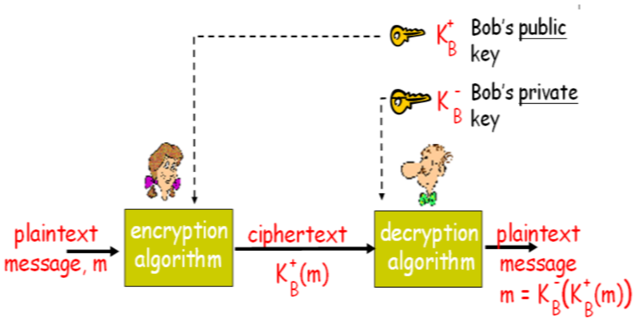
Encryption is the process of encoding data by a particular algorithm, which makes it impossible for a program to read data without the decryption key. Usually encryption protects data transmitted through communication lines.

Cryptography in Greek means “*Secret Writing*”. It is a Science and Art of transforming message by which it make them secure and immune to attack. Cipher refers to different categories of algorithm (encryption & decryption algorithm) in Cryptography. The secret key is also input to the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key. The traditional ciphers are character oriented but the modern one is the bit-oriented.

- Original message or data that is fed into the algorithm as input => Plaintext.
- An Encryption algorithm transforms + Secret Key => Plaintext to Ciphertext
- Decryption algorithm transforms + Secret Key => Ciphertext to Plaintext

Encryption Operations used	**No of Keys Use**	**Way in which Plaintext is Processed**
Substitution Transposition Product	Single Key or Private Key or Symmetric Key Two key or Public Key or Asymmetric Key	Block Cipher => Process one Block at a time Stream Cipher => Process the Input Elements Continuously.

- A **substitution technique** is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- **Transposition** (or **permutation**) is the process of inter-changing the position of symbol or number.

Private Key cryptography	***Public Key cryptography***
 Plaintext Cryptographic algorithm Ciphertext Cryptographic algorithm Plaintext	 K_B^+ Bob's public key K_B^- Bob's private key plaintext message, m encryption algorithm ciphertext $K_B^+(m)$ decryption algorithm plaintext message $m = K_B^-(K_B^+(m))$
In the private key encryption method, the same key is used by the sender (for encryption) and the receiver (for decryption). Thus, the key is shared. This method requires maximum number of keys in the internet as individual requires a secrete key.	To remove the limitation of public key, the asymmetric or public key encryption method is come in existence in which a public key and a private key is used. The private key is kept by the receiver and the public key is announced to the public by the same receiver to encrypt all the sanding data for him by the general public or any one.