Information Security

أمن المعلومات

Dr. Bashar M. Al-Essawi

Dr Jamal Nasir Hasoon

Mustansiriyah University

Department Of CS

IRAQ, Baghdad

2021

List Of CONTENTS

Chapter One

INTRODUCTION TO COMUTER SECURITY

1.1 Introduction:

With the introduction of computer and computer networks, the use of automated tools for protecting stored and transmitted files and other information on computer or on the internet has become evident. Therefore, one may come up with the following definitions:

- ***Computer security*** - Generic name for the collection of tools designed to protect data and to thwart (احباط المتسللين) hackers.
- **Network Security** - Measures to protect data during their transmission
- **Internet Security** - Measures to protect data during their transmission over a collection of interconnected networks

i.e. there might be no clear boundaries between ***PC security*** and ***internet security***. For example, one of the most common types of attacks on information system is the computer virus. A virus may be introduced into a system physically when it arrives on a diskette or USB. Virus may arrive over the internet. In either case, once the virus is resident on the computer, internal security tools are needed to recover the system.

1.2 Attacks, Services and Mechanisms

To understand the security problem, three aspects must be considered, they are ***security attack***, ***security services*** and ***security mechanism***.

- **Security Attack**: Any action that compromises the security of information owned by an organization.

- **Security Service**: A service that enhances the security of the data processing system and the information transfer of an organization. The services are intended to counter security

attacks and they make use of one or more security mechanisms to provide the service.

- **Security Mechanism**: A measure that is designed to detect, prevent or recover a security attack.

A. Security attacks:

Any action that compromises the security of information owned by a person or an organization is considered a security attack. Attack on security of computer system or computer network is best characterized by viewing the function of the computer system as information provider. In general, ***normal*** information flows from a source, such as a site or a place in the memory to a destination, such as another site or a user, as depicted in **Figure 1-1** below:

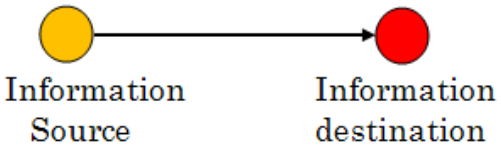

Fig.1-1 Normal information flow from source to destination.

When an asset of the system is destroyed or becomes unavailable or unusable, it results into an ***Interruption***, see **Figure 1-2**. This is considered as an attack on the (***Availability)***. **Examples** include the destruction of a piece of hardware such as hard disc, communication line cut or disabling of file management system.

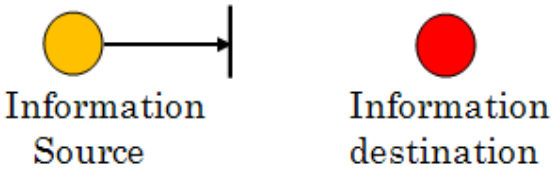

Fig. 1-2 Interruption of information flow.

When an unauthorized party gains an access to an asset, it results into an ***Interception***, see **Figure 1-3**. This is considered as an attack on the ***(Confidentiality)***. The unauthorized party could be a person, a program or a computer. **Examples** include wiretapping to capture data in a network and the elicit copying of files or programs.

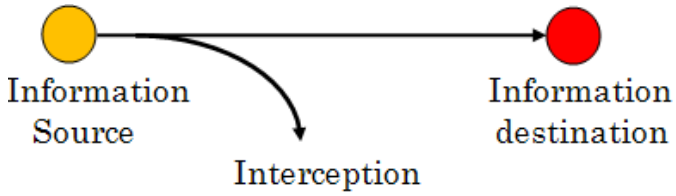

Fig. 1-3 Interception of information flow.

When an unauthorized party not only gains an access to but tempers with an asset, it results into ***Modification***, see **Figure 1-4**. This is considered as an attack on the (***Integrity)***. **Examples** include changing values in a data file or altering a program.

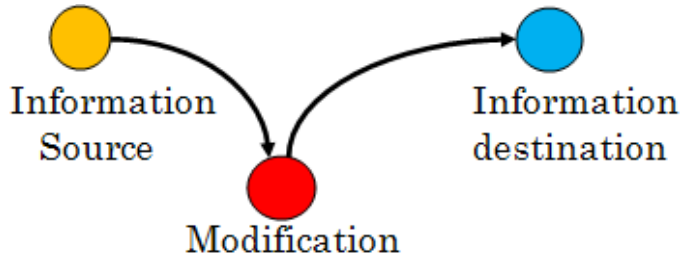

Fig. 1-4 Modification of information.

When an unauthorized party insert counterfeit object into the system, it results into ***Fabrication***, see **Figure 1-5**. This is considered as an ***(Authenticity).*** **Examples** include insertion of spurious messages in a network or the addition of records to a file.

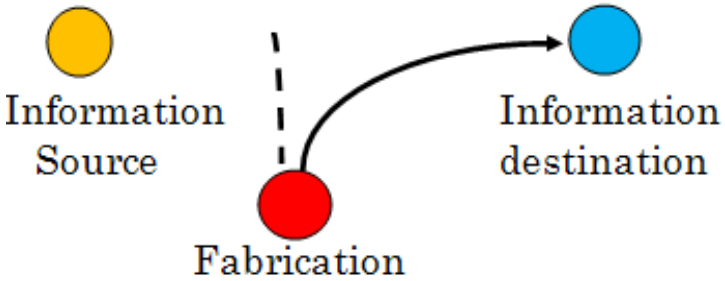

Fig. 1-5 Fabrication of information.

Attack categorization:

Attacks can be categorized as follows and illustrated in figure 1-6.

1- Passive attack or threats.
2- Active attack or threats.

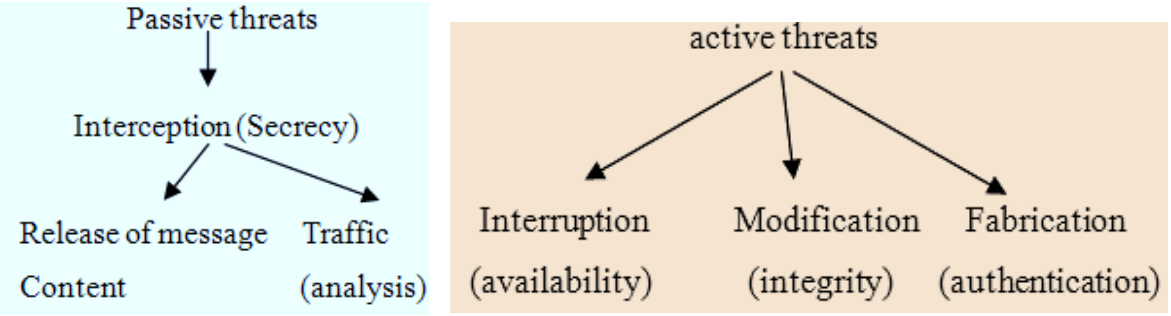

Fig. 1-6 Passive and Active security threat.

Passive attacks:

Passive attacks are the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information that is being transmitted. Two types of threats resulting from passive attack, they are:

1-Release of message contents and
2-Traffic analysis.

Passive attacks are very difficult to detect because they do not involve any alteration of the data.

Active attacks:

The second major category of attack is active attack. These kinds of attacks involve some modification in the data stream or the creation of false stream and can be subdivided into four categories:

- ***Masquerade***: it takes place when one entity pretends to be different entity.
- ***Replay:*** involves the passive capture of a data unit and its subsequent representation to produce any un-authorized effect.

- ***Modification of messages***: it means parts of the message is removed or changed.

DDoS

- ***Denial of service (DoS)***: it prevents or inhibits the arrival of a message to the recipient or management of communication facilities.

B. Security Services:

Confidentiality:

It is the protection of transmitted data from passive attacks.

- With respect to the ***release of message contents***, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. For example, if a virtual circuit is set up between two systems, this broad protection would prevent the release of any user data transmitted over the virtual circuit.

- The other aspect of confidentiality is the ***protection of traffic flow from analysis***. This requires that an attacker shall not be able to observe the source and destination, frequency, length or other characteristics of the traffic on a communication facility.

Authentication:

The authentication service is concerned with securing that a communication is authentic. In case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved:

1. At the time of connection initiation, the service assures that the two entities are ***authentic*** (i.e. making sure that the messages are coming from the same person, that claims, he is sending them, or it insures the ***signature*** of the sender).

2. The service must assure that communication is not interfered with in such a way that third party can ***masquerade*** as one of the two legitimate parties for the message exchange.

Integrity:

As with confidentiality, integrity applies to a stream of messages, single message or selected fields within the message. It means preventing data from being ***corrupted*** or made otherwise ***unavailable*** due to any combination of system failure or user's mistakes (i.e. ***un-authorized modification***)
Connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, recording or replay. Because the integrity service relates to active attacks, we are concerned with detection rather than prevention.

Nonrepudiation:

Prevents either sender or receiver from ***denying*** a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender.

Access control:

It is the ability to limit and control the access to host systems and application via communication links. To achieve this control, each entity tries to gain access must first be identified or authenticated.

Availability:

A variety of attacks can result into the loss or reduction in availability of the data being stored or sent over a communication link.

C. Security Mechanism:

A measure that is designed to detect, prevent or recover a security attack. However, there is no single mechanism that can support all the security services listed above. Examples of mechanisms in use: ***cryptographic*** techniques, ***encryption*** and encryption-like transformation (e.g. ***hash function***).

1.3 A Model for network Security:

Most of what we are going to discuss in the computer networks security can be summarized in the diagram of **Figure 1-7**.

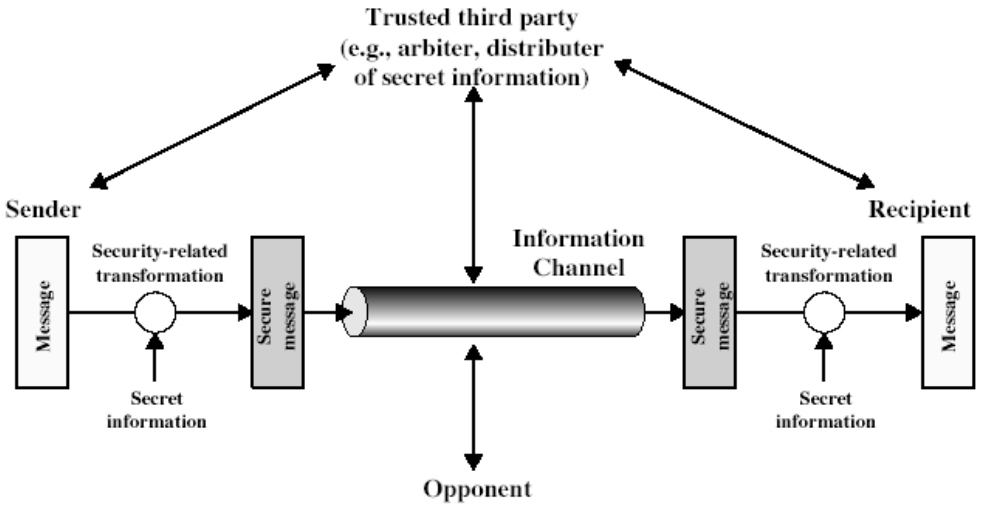

Fig. 1-7 Network Security model.

All techniques for providing security have two components:

1-**Security–Related Transformation** on the **information** to be sent. Examples include the encryption of the message and using some code based on the content of the message that can be used to verify the sender identity.

2-**Some Secret Information** shared by the two principals, **sender** and **receiver**, and it is hoped un-known to the opponent. Example is an encryption key used in conjunction with transformation to scramble the message before transmission.

A trusted third party may be needed to achieve secure transmission. He may be responsible for distributing the secret information to the two principals while keeping it from any opponent.

This general model shows that there are four basic tasks in designing a particular security service.

- **Design an algorithm** for performing the security related transformation. The algorithm should be designed in such a way that an opponent can not defeat its purpose.
- **Generate the secret information** to be used with the aid of an algorithm.
- Develop methods for the **distribution and sharing** of the secret information.
- **Specify a protocol** to be used by the two principals that makes use of the secrecy algorithm and the secret information to achieve a particular security service.

1.4 Network Access Security Model:

Another security related situation that do not neatly fit the above mentioned network security model is the general situation of access model shown in **Figure 1-8**. It is generally suitable for protection against unauthorized or unwanted access.

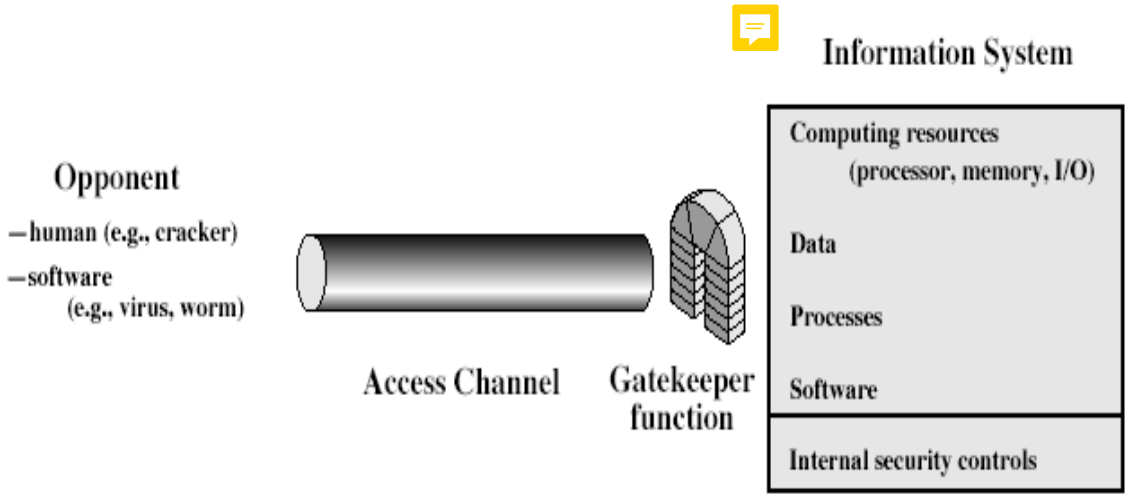

Fig. 1-8 Network Access Security

The security mechanisms needed to cope with unwanted access fall into two broad categories:

Ethical **Hacker:**

Someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system.

Intruder:

Someone who can be disgruntled employee who wishes to do damage to the system or data.

Criminal:

Someone who seek to exploit computer assets for functional gain (e.g. obtaining credit card numbers or performing illegal transfers).

1.5 Cryptographic system (Data Security):

Practically, cryptography employs two operations, i.e.

Encryption (encipherment)

Converting ***plaintext*** (or clear) into ***ciphertext*** *(scrumbled).*

Decryption (decipherment)

Converting back ***ciphertext*** into ***plaintext***, as shown in figure 1-9 below.

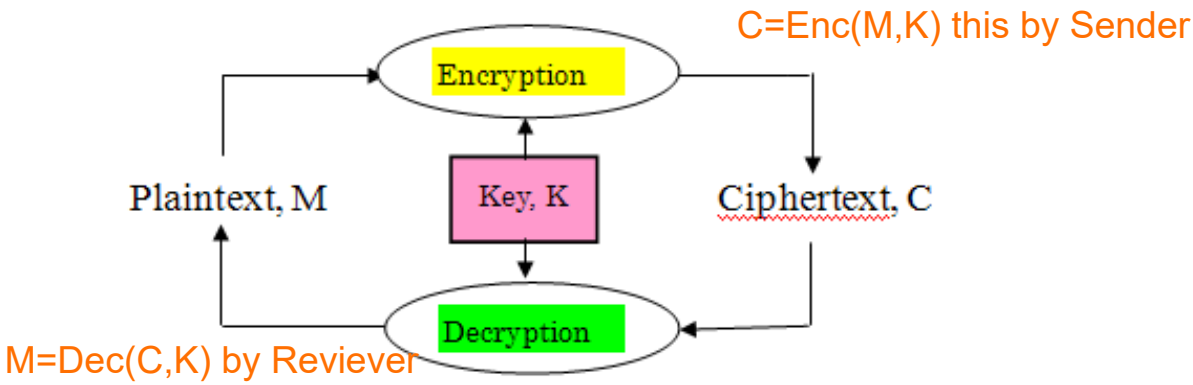

Fig.1-9 Traditional Encryption and decryption cycle.

Cryptography:
The science and study of secret writing, This name came from the Greek words **crypto** (secret) and **graph** (writing), which means converting the clear plaintext to ***ciphertext .***

Message:
Multimedia
It can be some text, numerical data, an executable program, photo or any kind of information → → called ***plaintext.***

Cipher:
It is the secret method of writing whereby ***plaintext*** (Clear text) is transformed into ***ciphertext*** (may be called Cryptogram).

** Encryption key(s) may be used for both encryption and decryption.

Cryptography is generally used to protect valuable and important data from unauthorized disclosure and modification. This problem is mainly a communication problem which consists of **three** factors, see **Figure 1-10**. **Sender,** (b) **Receiver** and (c) **Channel.**

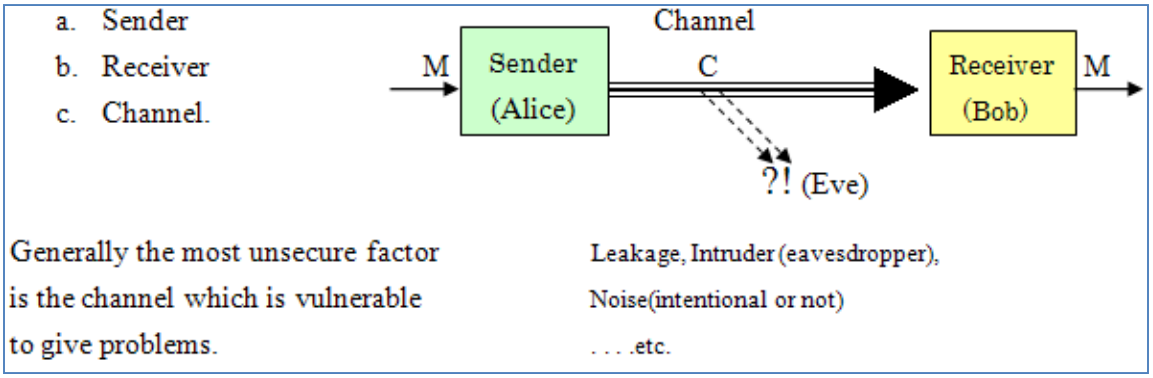

Fig. 1-10 Communication System.

Example:

1- ***Alice encrypts the message M by using encryption key K, obtaining ciphertext C, then transmitted to Bob.***
2- ***Bob turns C into M be decrypting it. He needs decryption key K (secret).***
3- ***Adversary, Eve still may intercept the ciphertext, however, encryption prevents her.***

1.6 Cryptanalysis

✓ It is the study of principles and methods of deciphering ciphertext without knowing key. There are two approaches for code breakers or cryptanalysis:

1. It relies on the nature of algorithm plus some knowledge of the general characteristic of text, such those in the followings:
   - **a.** Ciphertext only.
   - **b.** Known plaintext.
   - **c.** Chosen plaintext.
   - **d.** Chosen ciphertext.
   - **e.** Chosen text.
2. **Brute-Force Attack**: Trying every possible key until intelligible translation of the ciphertext to plaintext is obtained.

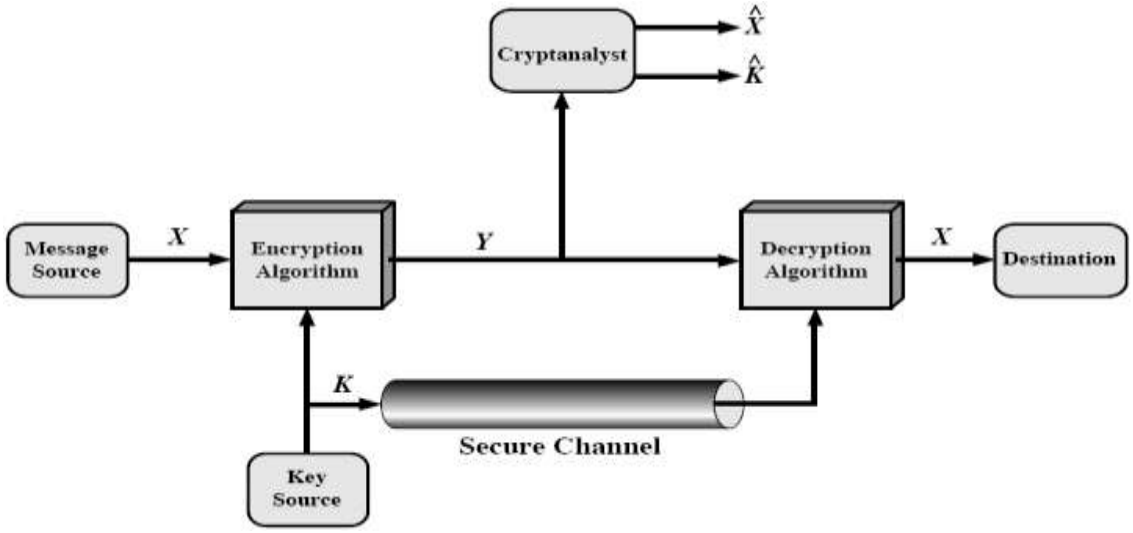

Fig 1-11. Model of symmetric cryptosystem.

- With the message X and the encryption key k as input, the encryption algorithm forms the ciphertext Y = [Y_1, Y_2, Y_3, . . . , Y_n], We can write this as $Y = E_k(X)$
- The receiver in possession of the key K, is able to invert the transformation, i.e. $X = D_k(Y)$
- An opponent, observing Y but not having access to k or X may attempt to recover plaintext X, key k or both of them. It is assumed that the opponent knows the encryption algorithm E and decryption algorithm D.
- If the opponent focus is on the effort to recover X by generating a plaintext estimate X^ , and to recover k by generating an estimate k^.