**Why is the Computer Security Important?**

1. Provide support for the critical business processes.

2. Provide protection for the personal and sensitive information.

**What will happen if your computer gets hacked?**

1. It could be used to hide some programs.

2. It could generate a large amount of unwanted traffic.

3. Some one could send illegal software from your computer to others without you realize it.

4. Someone could access personal information.

5. Someone could record all your keys that are used like passwords.

**Good Security Standards :-**

If follows the rule of 90/10, it means that 10% of security are *technical* while 90% of security depends on *computer user* (you).

For example:- the lock of the door represent the 10% while the remembering to lock the door, checking if the door is closed, etc., this represents the 90%. So we need the both 90 and 10 to get the effective security.

**The Effective Security** :-

Means the following:-

1. Everyone who uses a computer needs to understand how to keep their computer and data secure.

2. Learn the good computing security procedures.

3. Report anything unusual and notify the appropriate persons.

**The Consequences of Security Violation :-**

1. Loss of employee trust.

2. It causes risks to security and integrity of personal information.

3. Loss of business information.

**Internet Privacy and Security:-**

**1. *Privacy on Internet :-*** It means the measures to protect data during their transmission over a collection of interconnected networks. Social networking sites like Facebook, personal web pages have also become public sources of personal information. So :-

 Do not write personal details online. Assume that anything you post to those websites is public and could be used against you.

 The good rule is to post only the information that you desire to be public in that websites.

 Put in your mind that anything you will post in public website is more difficult to take it back even if you delete it, since copies of this information will still exist on other computer or websites.

**Cautions when using Social Network:-**

1. Remember that the internet is not private.

2. Do not give out personal or sensitive information to anyone you don’t know.

3. Don’t provide personal or sensitive information to internet site unless you are using trusted and secure web pages.

4. Some web pages display an internet address directly, so don’t click on such address.

5. A little lock is putting at the end of "http" address; this means that website is secure.

**2. *Internet Security Cautions :-***

1. Make sure you know where you are going before clicking on a link.

2. Use only known, trusted and secure websites when you enter sensitive or personal information.

3. To help avoid viruses don’t use internet explorer and use instead more secure alternative way like *Firefox* or *Safari*.

**Security Involving Programs :-**

Programs may cause two types of problems:-

1. These programs may transform of data to serve the users who must have no access to such data.

2. Theses programs may possible to penetrate by other systems leading to prevent authorized person from accessing them and at the same time allow unauthorized access to it.

**Information Access Problems :-**

There are several types of software that can be used to gain access to unauthorized data or information:-

**a) *Trapdoors***

A set of access points that are put in the system by programmer for the following possibility points:-

1. To identify future modification of the system.

2. To access to mistakes in the future.

3. Allowing the designer of accessing to the program after the completion of its design.

**Causes of Trapdoors:-**

Usually the programmer must remove these points during program development but it can be found in the programs for the following reasons:-

1. The programmer forgot to delete these points.

2. Programmer usually leaves these points in order to help the rest of the parts of the program test or to assist in the maintenance of that program.

So we note that the advantage of ***Trapdoors*** is that we can test the performance of the system, while the disadvantages are that it is used by the programmer for a break.

**b) *Trojan Horse***

For the similarity of his work with the legend of Trojan Horse wooden which hid by a number of soldiers Greeks and they were the reason to open the city of Trojan.

It is a kind of software which is loaded with major program and doing some hidden functions that are often concentrated to penetrate the system.

Trojan horses may steal information or damage the host computer systems and may be used for the download by search engines or by installing online games or applications based on internet taking advantage of security gaps that allow unauthorized access to the system.

**c) *Salami Attack***

Is a process similar to the process slicer where small deducted (يستقطع ) money from each account an amount so that this part is not observed in the normal case.

This type of software is attacking the banks where the decimals deduct each amount daily and will be transferred to another account without being noticed and within days or months will get the beneficiary on the huge amounts of money.

Also the customer who will be deducted from his account decimals will not demanding to clarify the matter because it will be regarded as the amount deducted is worthwhile.

**Programs that leak information**

This type of software is leaking the information and delivery it to person not authorized to get it.

The generic name for this type of program is (Covert or Hidden Channels).

Are a hidden channels or programs used to penetrate the system and leaking of information from the system.

For example; a programmer when designing a specific program for the bank, is entitled to deal with the data and its size as required by the banking program, but access to that data after completion the designing of the program is unacceptable.

**How to Create Covert Channels**

1. The programmer can encode data through a formula to replace the output, for example replace the word (total) with (totals) by adding (s) to the end of the word as it is represents the bit itself Covert Channel through which is part of the information transfer.

2. In same case, the programmer can not access the data through the program, but it calls another program that converts the data to the first program and is not observable.

3. The smart programmer can develop Covert Channel, for example, assume that the program reached a confidential data (بجانات سريٌ ) during execution and that the programmer will create of dual-coding and through which passes the information to that coding.

**Service Problems**

This kind of problem depends on designing programs to influence the work of the system and the services provided by the user, causing stops these services and the failure of this is called " ***fail of service***".

**Types of service problems:-**

**a) *Greedy Programs***

Programs that are change the sequence of important for programs to implement, for example, in multi-processes systems, there is a time to run each program so when one program waiting for input data for input devices, the CPU will enter in the waiting state, leading to wait for the implementation od other programs.

**b) Viruses**

Are programs that impact on other programs by making adjustments.

These programs are considered an extension for Greedy Programs.

Its problems:-

1. Viruses interference to systems that have a number of users to access data, for example e-mail.

2. Viruses can multiply in the system a very short time and often can not determine the source and the small size of these programs help to hide in complex programs such as Data Base.

**c) Worms**

Is malicious software that repeats them in order to spread into the rest of the computers that are used in computer network depending on the failure in the security system that is used.

Worms differ from viruses that viruses make changes on programs that are dominated by, while worms causing harm in a simple computer networking through the destruction of ***bandwidth***.

Worms don’t make any change in files but only settle in the memory and repeat them and are often used parts of the operating system specially the invisible parts for the users.

**Program Development Controls against Program Attacks**

(a) Modularity (b) Encapsulation (c) information Hiding

**a) *Modularity*:-** is the process of dividing a program into subtasks called (Modules), each task do certain function. There are several advantages from writing program into partial tasks:-

**1. Maintainability**

The maintenance of the system be directed process where only the specific module maintenance.

**2. Understandability**

Program which consists of several parts is easy to understand and know his work compared to if large.

**3. Correctability**

Easy follow-up errors as they arise and this will lead to speed in correcting these errors.

**b) *Encapsulation***

The concept of modularity lead to the independence of each module from the other, where each module is an independent object and this is known as the principle of encapsulation.

When making a program, each module will be surrounded by a shield preventing unwanted access from the outside, so that the process of encapsulation does not mean isolating modules from other parts of the program but sets handle modules with each other, and this will reduce the covert channel used to penetrate the system.

**c) *Information Hiding***

Means hide the data and instructions of a module and this will lead to hide the function of module.

This process is desired in terms prevents the programmer from doing penetrate the module unless it is to know how the module works.

**Independent Testing**

The purpose of the test is to determine the validity of the program and during the test we can see the errors.

The purpose of the test:-

1. Test that shows errors is more accurate than the test you can not find something.

2. The testing process will assure us that the system works and is designed according to its purpose.

3. From a security stand point, the testing is very important because the programmer may hide another program within the system as a weakness to serve its own purposes.

**Security Mechanism** :- means the mechanism that is designed to detect, prevent, or recover from security attack. Remember that no single mechanism will support all functions required.

**Data Hiding**

**Steganography and Watermarking**



• Information Hiding is a general term encompassing many sub-disciplines

• Two important sub-disciplines are:

Steganography and Watermarking

**– Steganography**:

Hiding: keeping the existence of the information secret

– **Watermarking**

Hiding: making the information imperceptible

• Information hiding is different than cryptography (cryptography is about protecting the content of essages)

**The Need for Data Hiding:**

• Covert communication using images (secret message is hidden in a carrier image)

• Ownership of digital images, authentication, copyright

• Data integrity, fraud detection, self-correcting images

• Traitor-tracing (fingerprinting video-tapes)

• Adding captions to images, additional information, such as subtitles, to video, embedding subtitles or audio tracks to video (video-in-video)

• Intelligent browsers, automatic copyright information, viewing a movie in a given rated version

• Copy control (secondary protection for DVD)

**Issues in Data Hiding**

Perceptibility: does embedding information ―distort‖ cover medium to a visually unacceptable level (subjective)

Capacity: how much information can be hidden relative to its perceptibility (information theory)

Robustness to attacks: can embedded data survive manipulation of the stego medium in an effort to destroy, remove, or change the embedded data

Trade-offs between the three:

1. More robust => lower capacity
2. Lower perceptibility => lower capacity

**Section 1: Steganography**

**Introduction:-**

The word steganography is derived from the Greek words “***stegos***” meaning “cover” and “***grafia***” meaning “writing” defining it as “covered writing”. **Steganography** is one such pro-security innovation in which secret data is embedded in a cover.

**Steganography** deals with composing hidden messages so that only the sender and the receiver know that the message even exists. Since nobody except the sender and the receiver knows the existence of the message, it does not attract unwanted attention.

The study of hiding information is called **Cryptography**. When communicating over an untrusted medium such as internet, it is very important to protect information and **Cryptography** plays an important role in this. Today, **Cryptography** uses principles from several disciplines such as mathematics, computer science, etc. **Steganography** deals with composing hidden messages so that only the sender and the receiver know that the message even exists.

**Steganography** and **Cryptography** are closely related. **Cryptography** scrambles (تخلط ) messages so they cannot be understood.

**Steganography** on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion (تثير الشك ) while an

"invisible” message will not do so. Both sciences can be combined to produce better protection of the message. In this case, when the **Steganography** fails and the message can be detected, it is still of no use as it is encrypted using **Cryptography** techniques.

There exist two types of materials in steganography: message and carrier. Message is the secret data that should be hidden and carrier is the material that takes the message in it.

Figure below shows the different categories of file formats that can be used for steganography techniques.

**Differences between Steganography and Cryptography:-** 1. Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. 2. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message.

3. Steganography hides a message within another message normally called as a cover and looks like a normal graphic, video, or sound file. In cryptography, encrypted message looks like meaningless jumble of characters.

4. Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content.

5. Steganography requires caution when reusing pictures or sound files. In cryptography caution is required when reusing keys. By combining Steganography and Cryptography one can achieve better security.

**Types of Steganography:-**

1. Hiding a message inside text.

2. Hiding a message inside images.

3. Hiding a message inside audio or video files.

Computer Security M.Sc .Shaimaa A. Al-Obaidy

**Section 2: Digital Watermarking**

**2.1: Introduction**

Digital Watermarks are imperceptible or barely perceptible transformations of digital data. Watermarking principles are used whenever cover *work[[1]](#footnote-1)* is available to parties that may be interested to remove it. The watermarking schemes should be robust against manipulations that attempt to remove it. A principal application of watermarking is to provide proof of ownership of digital data by embedding copyright statements. Digital watermarking may also be used for fingerprinting applications in order to distinguish distributed data sets.

**2.2: Watermark Properties**

Watermarks can be characterized by a number of properties. The relative importance of properties depends on the application and the role that the watermark will play in that application. Some properties are associated with the watermark embedding process, some with detection and others with keys.

**2.2.1: Effectiveness**

The effectiveness of a watermark is the probability of detection immediately after watermarking. Although one hundred percent effectiveness is desirable it may not be feasible in practice without sacrificing other properties such as fidelity. Some applications may necessitate sacrificing on effectiveness so that other more important characteristics are realized.

**2.2.2: Fidelity**

Fidelity is the closeness between the original and watermarked versions of the cover. As the watermarked cover may degrade during transmission before being seen by a person, fidelity may also be defined as the closeness between the original and watermarked covers when it is being viewed by the consumer.

**2.2.3: Payload**

Payload refers to the number of bits a watermark encodes within a unit of time or within a cover. For a photograph the data payload would refer to the number of bits encoded within the image. In audio transmissions data payload refers to the number of embedded bits per second that are transmitted. For video transmissions the data payload may refer to the number of bits per frame or the number of bits per second. The requirements for data payload are application dependent.

**2.2.4: Blind/Informed Detection**

In some applications the original cover may be available during watermark detection while in others it may not make sense to have the original available for e.g. in a copy control application. The detectors that need the original cover in order to detect a watermark are called *informed detectors*. Conversely detectors that do not need information about the original cover are *blind detectors*. Informed detection is also referred as *private watermarking system* where detection is available to only a select group of individuals whereas blind detection is referred as *public watermarking system* where everyone must be allowed to detect the watermark.

**2.2.5: False Positive Rate**

This refers to the detection of watermark in a cover that does not contain one. With respect to a detector application, this refers to the number of false positives we expect to occur in a given number of runs of the detector. The requirement of false positives will depend on the application. In a proof of ownership application a small number of false positives may be acceptable. However in a copy control application where huge numbers of detectors are active we may not want any false positives during the lifetime of the cover.

**2.2.6: Robustness**

The watermark must be detectable after common signal processing operation. This is the robustness of the watermark. Some operations on images that test robustness are spatial filtering, lossy compression, scanning and geometric distortions. Audio watermarks need to be robust to recording on audio tape and variations in playback speed.

**2.2.7: Security**

The security of a watermark is its resistance to hostile attacks. The types of attacks are unauthorized detection, embedding and removal. Removal of a watermark prevents its detection. These could be the total elimination of the watermark or changing so that it escapes detection. Unauthorized detection and removal are active attacks. In contrast the passive attack is unauthorized detection where an adversary can detect and distinguish watermarks.

**2.2.8: Cipher and Keys**

In modern cryptographic algorithms, security is derived from the key as the algorithm is made public. Similarly it should not be possible to detect the watermark in a cover without the key even if the watermarking algorithm is known. Also, without the key, an adversary should not be able to remove or damage the watermark without significant degradation of fidelity. In some systems the watermark message is first encrypted with a cryptographic key and then embedded with a watermark key.

**Kinds of security breaches (penetration)**

**Vulnerability** is a weakness in the security system, for example, in procedures, design, or implementation that might be exploited to cause loss or harm.

**A threat** to a computing system is a set of circumstances that has the potential to cause loss or harm

A human who exploits vulnerability perpetrates an **attack** on the system. An attack can also be launched by another system.

**Kinds of threats**

1) **Interception:** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network.

2) **Interruption**: an asset of the system becomes lost, unavailable, or unusable. An example is malicious destruction of a hardware device, erasure of a program or data file or malfunction of an operating system file manager so that it cannot find a particular disk file.

3) **Modification** means an unauthorized party not only accesses but tampers with an asset,. For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted electronically.

4) **Fabrication**: an unauthorized party might create a fabrication of counterfeit objects on a computing system. The intruder may insert spurious transactions to a network communication system or add records to an existing database.

1. A picture, music or video or other object that can have watermarks embedded in it. [↑](#footnote-ref-1)