- **Computer Security :-** is the protection of computing systems and the data that they store or access. It refers to the technological safeguards (ضمانات) and managerial procedures that can be applied to computer hardware, programs, and data.

هي حماية انظمة التشغيل والبيانات والتي من الممكن الوصول اليها، فهي تشير الى الضمانات التقنية والاجراءات الادارية التي من الممكن تطبيقها على الاجزاء المادية للحاسبة وعلى البرامج والبيانات.

- **Data Security :-** refers to the protection of data from accidental, or unauthorized modifications or destructions, or disclosure to unauthorized persons.

حماية البيانات من اتلافها او من التعديل غير المخول او تدميرها او الكشف عنها من قبل الاشخاص غير المخولين.

- **Privacy :-** it is the right of an individual to decide what information he wish to share with others and what information he will accept from others.

تمثل حق الشخص لتحديد ما هي المعلومات التي يرغب بمشاركتها مع الاخرين وكذلك ما هي المعلومات التي سوف يستقبلها من الاخرين.

- **Integrity :-** it refers not only to the correctness of data (message or file) but its resources and validity.

تشير الى صحة البيانات وكذلك الى مصدرها واصل تلك البيانات ومدى صلاحيتها.

- **Data Integrity :-** is the property that data has not been changed or destroyed in an unauthorized manner.

هي خاصية البيانات التي لم يتم تغييرها او اتلافها بطريقة غير مخولة

- **Authentication :-** is the granting a user of right access to a protected program, or a process.

هو عملية منح حق الوصول للمصادر المحمية من قبل الاشخاص او البرامج.

- **System Integrity :-** is the ability of a system to operate according to some specifications even in the face of deliberate (متعمدة) attempts to make the system behave differently.

هو قدرة النظام على ان يعمل وفقا لمواصفات معينة في مواجهة المحاولات المتعمدة من اجل جعل النظام يتصرف بشكل مختلف.

- **Confidentiality (السرية) :-** is the property that information is not made available or disclosed to unauthorized persons.

هي الخاصية التي تكون فيها البيانات او المعلومات غير متوفرة وغير مكشوفة بالنسبة للاشخاص غير المخولين.

- **Identification :-** the identification of a user, file, program, or other object is the unique name or number assigned to that object.

الهوية التعريفية للمستخدم او للملف او للبرنامج او اي عنصر اخر، معناه اسم او رقم وحيد يتم تحديده او اعطاءه لذلك العنصر.

Why is the Computer Security Important?

1. Provide support for the critical business processes.

توفير دعم واسناد للعمليات التجارية الحرجة.

2. Provide protection for the personal and sensitive information.

توفير الحماية للمعلومات الشخصية الحساسة.

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 :- مقاييس الامنية الجيدة

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.

   اي شخص يستخدم الحاسبة يحتاج الى فهم كيفية الحفاظ على الحاسبة والبيانات بشكل امن.

2. Learn the good computing security procedures.

   تعلم الطرق او الاجراءات الامنية الجيدة.

3. Report anything unusual and notify the appropriate persons.

   سجل اي حالة تكون غير اعتيادية وابلاغ الاشخاص المعنيين بها.

The Consequences of Security Violation :- عواقب الانتهاك الامني

1. Loss of employee trust. فقدان الثقة بالموظف
2. It causes risks to security and integrity of personal information.

   تسبب خطر على امنية وتكامل المعلومات الشخصية.

3. Loss of business information. فقدان المعلومات الخاصة بالعمل

Internet Privacy and Security:- امنية وخصوصية الانترنت

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 :-

ويعني ذلك تدابير حماية البيانات أثناء إرسالها عبر مجموعة من الشبكات المترابطة. مواقع التواصل الاجتماعي مثل فيس بوك ايضا تعتبر مصدر عام للعلومات الشخصية، لذلك:-

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

لا تكتب التفاصيل الشخصية عبر الإنترنت. افترض أن أي شيء تنشره على تلك المواقع هو عام ويمكن استخدامه ضدك

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

القاعدة الجيدة هي نشر المعلومات التي ترغب في أن تكون عامة في تلك المواقع فقط

- ❖ 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.

اي شيء ينشر على مواقع عامة من الصعب جدا استرجاعها حتى وان قمت بحذفها لانه سوف يكون هنالك نسخ منها موجودة في حاسبات اخرى.

Cautions when using Social Network:-

تحذيرات من استخدام مواقع التواصل الاجتماعي

1. Remember that the internet is not private.

تذكر دائما ان الانترنت ليس خاص

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

لا تعطي معلومات شخصية أو حساسة لأي شخص لا تعرفه.

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

لا تقدم معلومات شخصية أو حساسة على موقع الإنترنت إلا إذا كنت تستخدم صفحات ويب موثوق بها وآمنة.

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

تعرض بعض صفحات الويب عنوان الإنترنت مباشرة، لذا لا تنقر على هذا العنوان

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

يتم وضع قفل صغير في نهاية عنوان "http "؛ وهذا يعني أن الموقع آمن.

2. *Internet Security Cautions :-*

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

تأكد من أنك تعرف أين أنت ذاهب قبل النقر على الرابط.

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

استخدم مواقع ويب معروفة وموثوقة وآمنة فقط عند إدخال معلومات حساسة أو شخصية

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

للمساعدة في تجنب الفيروسات لا تستخدم *internet explorer* واستخدام بدلا من ذلك طريقة بديلة أكثر أمنا مثل *Firefox* أو *Safari*

Security Involving Programs :- الحماية المتعلقة بالبرامج

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 (تخترق) by other systems leading to prevent authorized person from accessing them and at the same time allow unauthorized access to it.

البرامج ممكن ان تسبب نوعين من المشاكل:-

1. هذه البرامج ممكن ان تحول البيانات لخدمة الـ users الذي يجب ان لا تصل اليهم تلك البيانات.

2. هذه البرامج ممكن ان تخترق من قبل انظمة اخرى مما يؤدي الى ان تمنع الاشخاص المخولين من الوصول اليها او تسمح للاشخاص غير المخولين من الوصول اليها.

Information Access Problems :- مشاكل الوصول الى البيانات

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

هنالك عدة انواع من البرامج التي من الممكن ان تستخدم للوصول غير المخول الى البيانات او المعلومات:-

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.

مجموعة من نقاط الوصول يضعها المبرمج في النظام لهذه الاحتمالات:-

1. لتحديد التعديلات المستقبلية للنظام.
2. للوصول الى الاخطاء في المستقبل.
3. تسمح للمصمم من الوصول الى البرنامج بعد الانتهاء من تصميمه.

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.

عادة المبرمج يجب ان يزيل هذه النقاط اثناء عملية التطوير للبرنامج لكنها من الممكن ان تكون موجودة في البرامج للاسباب التالية:-

1. المبرمج نسي حذف تلك النقاط.
2. المبرمج عادة يترك هذه النقاط عمدا من اجل المساعدة في اختبار بقية اجزاء البرنامج او للمساعدة في صيانة ذلك البرنامج او من اجل سهولة الوصول الى البرنامج من قبله او من قبل الجهة المستفيدة.

لذلك نلاحظ ان ***Trapdoors*** فيه محاسن من خلالها نستطيع اختبار اداء النظام لكن من مساوئه انه يستخدم من قبل الجهة المستفيدة او من قبل المبرمج لاختراقه.

b) *Trojan Horse*

For the similarity of his work with the legend (اسطورة) 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 (تسرق) information or damage the host computer systems and may be used for the download by search engines (محركات البحث) or by installing online games or applications based on internet taking advantage of security gaps that allow unauthorized access to the system.

لتشابه عمله مع أسطورة حصان طروادة الخشبي الذي اختبأ به عدد من الجنود اليونانيين وكانوا سببا في فتح مدينة طروادة.

هي شفرة صغيرة يتم تحميلها مع برنامج رئيسي، ويقوم ببعض المهام الخفية، غالباً ما تتركز على إضعاف قوى الدفاع لدى الضحية أو اختراق جهازه وسرقة بياناته.

فهو نوع من البرمجيات الخبيثة التي لا تتناسخ من تلقاء نفسها والذي يظهر لكي يؤدي وظيفة مرغوب فيها ولكن بدلا من ذلك ينسخ حمولته الخبيثة. وفي كثير من الأحيان يعتمد على الثغرات الأمنية التي تتيح الوصول الغير المصرح به إلى الكمبيوتر. وهذه الثغرات الأمنية تميل إلى أن تكون غير مرئية للمستخدمين العاديين. أحصنة طروادة لا تحاول حقن نفسها في ملفات أخرى مثل فيروسات الكمبيوتر. أحصنة طروادة قد تسرق المعلومات، أو تضر بأنظمة الكمبيوتر المضيف. وقد تستخدم التنزيلات بواسطة المحركات أو عن طريق تثبيت الألعاب عبر الإنترنت أو التطبيقات القائمة على الإنترنت من أجل الوصول إلى أجهزة الكمبيوتر الهدف. والمصطلح مشتق من قصة حصان طروادة في الأساطير اليونانية لأن أحصنة طروادة تستخدم شكلا

من أشكال "الهندسة الاجتماعية"، وتقوم بتقديم نفسها على أنها غير مؤذية، ومفيدة، من أجل إقناع الضحايا لتثبيتها على أجهزة الكمبيوتر الخاصة بهم.

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 (الجهة المستفيدة) 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 (غير جدير بالاهتمام).

عملية مشابهة الى عملية تقطيع شرائح اللحم حيث يستقطع مبلغ صغير من المال من كل حساب جاري بحيث ان هذا الجزء المستقطع لا يلاحظ في الحالات الطبيعية.

هذا النوع من البرامج تهاجم المصارف حيث يقوم باستقطاع الكسور العشرية لكل مبلغ وبشكل يومي ويتم تحويله الى حساب اخر بدون ان يتم ملاحظته وخلال ايام او اشهر سوف تحصل الجهة المستفيدة على مبالغ طائلة.

ايضا الزبون الذي سوف يتم استقطاع الكسور العشرية من حسابه سوف لن يطالب بتوضيح الامر لانه سوف يعتبر المبلغ المستقطع غير جدير بالاهتمام.

Programs that leak information برامج تسريب المعلومات

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 (اختراق) the system and leaking of information from the system.

For example; a programmer when designing a specific program for the bank, is entitled to (يحق له) 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 (غير مقبول).

هذا النوع من البرامج يقوم بتسريب المعلومات وايصالها الى اشخاص لا يحق لهم الحصول عليها.

التسمية العامة لهذا النوع من البرامج او المسارات غير الطبيعية هو (***Covert or Hidden Channels***).

Covert or Hidden Channels عبارة عن قنوات مخفية او برامج مخفية تستخدم لاختراق النظام وتسريب المعلومات منه.

مثلا:- ان المبرمج عند تصميم برنامج معين الى (البنك) يحق له التعامل مع البيانات وحجمها بما يتطلبه البرنامج المصرفي لكن الوصول الى تلك البيانات بعد الانتهاء من تصميم البرنامج يكون غير مقبول.

How to Create Covert Channels كيفية انشاء هذه القنوات (البرامج) المخفية

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.

المبرمج يستطيع ترميز البيانات من خلال ابدال صيغة المخرجات مثلا ابدال كلمة Total الى Totals اي اضافة (s) الى نهاية الكلمة الخاصة بالمخرجات وان هذا (s) يمثل bit واحد وهو بحد ذاته عبارة عن ***Covert Channel*** والذي من خلاله يتم نقل جزء من المعلومات.

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.

في بعض الحالات فان المبرمج لا يستطيع الوصول الى البيانات عن طريق البرنامج وانما يقوم باستدعاء برنامج اخر يقوم بتحويل البيانات الى البرنامج الاول وبشكل غير قابل للملاحظة.

3. The smart programmer can develop Covert Channel, for example, assume that the program reached a confidential data (بيانات سرية) during execution

and that the programmer will create of dual-coding and through which passes the information to that coding.

ان المبرمج الذكي يستطيع خلق (***Covert Channel***) مثلا نفترض ان البرنامج وصل الى بيانات سرية اثناء التنفيذ وان المبرمج لا يستطيع الحصول على تقرير بهذا لذلك فان المبرمج سوف يقوم باستحداث ترميز ثنائي الذي من خلاله يقوم بامرار المعلومات الى ذلك الترميز.

Service Problems مشاكل الخدمات

This kind of problem depends on designing programs to influence (تاثير) 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***".

هذا النوع من المشاكل تصمم برامج للتاثير على عمل النظام والخدمات التي يقدمها للمستخدمين مسببة توقف هذه الخدمات وفشلها وهذا ما يسمى (***fail of service***).

Types of service problems:- **انواع مشاكل الخدمات**

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.

البرامج الطماعة وهي البرامج التي تقوم بتغيير تسلسل الاهمية للبرامج للتنفيذ. مثلا في الانظمة متعددة البرامج (*multi-processes system*) هنالك وقت لتشغيل كل برنامج وذلك عند انتظار احد البرامج لبيانات مدخلة من اجهزة الادخال فان CPU سوف يدخل في حالة انتظار (*waiting*) مما يؤدي الى حصول حالة توقف تنفيذ بقية البرامج.

b) Viruses

Are programs that impact (تؤثر) 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.

عبارة عن برامج تقوم بالتاثير على البرامج الاخرى من خلال اجراء تعديلات عليها. هذه البرامج تعتبر امتداد للـ (*Greedy Programs*).

مشاكلها:-

1. الفايروسات تدخل الى الانظمة التي لها عدد من المستخدمين للوصول الى البيانات مثلا البريد الالكتروني (*email*).
2. الفايروسات تستطيع ان تتكاثر في النظام بوقت جدا قصير وفي الغالب لا يمكن تحديد مصدرها وان صغر حجم هذه البرامج يمكنها من الاختباء في البرامج المعقدة مثلا (*Data Base*).

c) Worms

Is malicious software (برمجيات خبيثة) 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 (تستقر) in the memory and repeat them and are often used parts of the operating system specially the invisible parts for the users.

هي من البرمجيات الخبيثة التي تكرر(Replicate) نفسها من اجل ان تتنشر(Spread) في بقية الحاسبات لذلك تستخدم شبكة الحاسبات (Computer Network) من خلال الاعتماد على الفشل في نظام الامنية المستخدم في الحاسبات الاخرى.

فهي تختلف عن الفيروسات كون الفايروسات تقوم باجراء تعديل على البرامج التي سيطرت عليها بينما Worms تسبب اذى بسيط في (Computer Network) من خلال اتلاف (Bandwidth)

لا تحدث اي تغيير في الملفات لكن فقط تستقر في الذاكرة وتكرر نفسها وغالبا تستخدم اجزاء من نظام التشغيل (Operating System) وتحديدا تلك الاجزاء التي تكون غير مرئية (Invisible) بالنسبة للـ User

غالبا ما يتم اكتشافها عندما هذه البرمجيات تفشل في السيطرة على عملية تكرار نفسها (Replicate) مسببة بذلك بطىء في عمل مصادر الكومبيوتر (Computer Resources) بالاضافة الى توقف بعض المهام.

Program Development Controls against Program Attacks

ضوابط تطوير برنامج ضد الهجمات حيث يتم ذلك من خلال ثلاث مراحل:-

(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:-

هي عملية تقسيم المهمة الكبيرة الى مهام جزئية تسمى (modules) وان كل مهمة تقوم بوظيفة معينة. هنالك عدة فوائد من كتابة البرنامج على شكل مكونات صغيرة متعددة:-

1. Maintainability قابلية الصيانة

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

ان صيانة النظام تكون عملية موجهة حيث يتم صيانة الـ (Module) المحدد فقط.

2. Understandability قابلية الفهم

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

البرنامج المكون من عدة اجزاء (modules) يكون من السهل فهمه ومعرفة عمله مقارنة لو كان كبير.

3. Correctability قابلية التصحيح

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

من السهولة متابعة الاخطاء عند ظهورها وهذا سوف يؤدي الى السرعة في تصحيح تلك الاخطاء.

b) *Encapsulation* الاحاطة

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 (درع) 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.

ان مفهوم (Modularity) يؤدي الى استقلالية كل (Module) عن الاخر حيث ان كل (Module) عبارة عن (Independent Object) وهذا ما يعرف بمبدا الـ (Encapsulation).

اي عند عمل برنامج فان كل (Module) سوف يحاط بدرع يمنع الوصول غير المرغوب به من الخارج. وبذلك ان عملية (Encapsulation) لا تعني عزل (Modules) عن بقية اجزاء البرنامج لكنها تحدد تعامل (Modules) الموجودة في البرنامج مع بعض وهذا سوف يقلل من القنوات الخفية (Covert Channels) المستخدمة لاختراق النظام.

c) *Information Hiding* اخفاء المعلومات

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.

هو اخفاء بيانات وايعازات (Module) وبالتالي سوف يؤدي الى اخفاء وظيفته.

هذه العملية تكون مرغوب بها حيث يمنع المبرمج من القيام باختراق الـ (Module) ما لم يكن على معرفة بكيفية عمل الـ (Module).

ان المبادئ الثلاثة (Modularity , Encapsulation, information Hiding) هي مبادئ اساسية في هندسة البرامجيات وانها ممارسات امنية للحفاظ على النظام بالكامل حيث تجعل النماذج (Modules) مفهومة ومحللة وموثوقة.

Independent Testing استقلالية الاختبار

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.

الغرض من الاختبار هو معرفة مدى صحة البرنامج ومن خلال الاختبار نستطيع معرفة الاخطاء.

الغاية من هذا الاختبار:-

1. الاختبار الذي يظهر الاخطاء هو اكثر دقة من الاختبار الذي لا يجد شيء.
2. ان عملية الاختبار سوف تؤكد لنا بأن النظام يعمل وفقا لما صمم له.
3. من الناحية الامنية اجراء الاختبار مهم جدا لان المبرمج قد يخفي برنامج اخر ضمن النظام كنقطة ضعف لخدمة اغراض خاصة به.

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.

تعني الآلية التي تم تصميمها للكشف عن الهجوم الأمني أو منعه أو معالجتها في حالة حدوثها. تذكر أن أي آلية مفردة سوف لن تكون كافية لتوفير كل تلك الوظائف المطلوبة.