أمن المعلومات :-

هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها . ويشمل ذلك الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية .

وبشكل عام فإنه يقصد **بأمن المعلومات:**

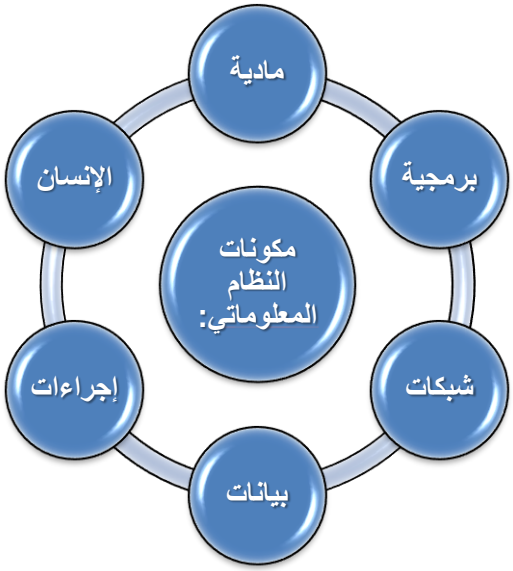
" حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث تؤمن المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسب المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة و ذلك في جميع مراحل تواجد المعلومة (التخزين – النقل – المعالجة)".

أهمية أمن المعلومات:

1. القطاعات الأمنية والعسكرية والاقتصادية تعتمد على صحة ودقة المعلومات.
2. حاجة الدول لوجود إجراءات أمنية قابلة للتطبيق تغطي المخاطر التي يمكن أن تظهر عند التعامل مع الأطراف الأخرى.
3. الحاجة المتزايدة لإنشاء بيئة إلكترونية آمنة تخدم مختلف القطاعات
4. النمو السريع في استخدامات التطبيقات الإلكترونية والتي تتطلب بيئة آمنة.
5. الحاجة إلى حماية البنية التحتية للشبكة المعلوماتية وذلك من أجل استمرارية الأعمال التجارية.
6. مع تطور التقنية المعلوماتية وازدهارها توفرت فرصاً للإجرام الإلكتروني.

مكونات النظام المعلوماتي:

1- برمجية .
2- مادية .
3- انسان .
4- اجراءات .
5- بيانات .
6- شبكات .



أركان امن المعلومات :

1- السرية

السرية هو المصطلح المستخدم لمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالأطلاع عليها أو الكشف عنها. على سبيل المثال، بطاقة الائتمان والمعاملات التجارية على شبكة الإنترنت يتطلب رقم بطاقة الائتمان على أن تنتقل من المشتري إلى التاجر ومن التاجر لانجاز وتجهيز المعاملات على الشبكة. يحاول النظام فرض السرية عن طريق تشفير رقم البطاقة أثناء الإرسال، وذلك بالحد من الأماكن ظهور تسلسل رقم البطاقة (في قواعد البيانات، وسجل الملفات، النسخ الاحتياطي، والإيصالات المطبوعة)، وذلك بتقييد الوصول إلى الأماكن التي يتم تخزين الرقم والبيانات بها. اماإذا كان الطرف غير المصرح به قد حصل على رقم البطاقة بأي شكل من الأشكال ،وبذلك فقد تم انتهاك مبدأ السرية في حفظ وتخزين البيانات.

خرق السرية يتخذ أشكالا عديدة. تجسس شخص ما على شاشة الكمبيوتر لسرقة كلمات سر الدخول ،أو رؤية بيانات سرية لديك بدون علم منك يمكن أن يكون خرقا للسرية. إذا الكمبيوتر المحمول يحتوي على معلومات حساسة عن موظفي الشركة هو سرق أو بيع، يمكن أن يسفر عن انتهاك لمبدأ السرية.

إعطاء معلومات سرية عبر الهاتف هو انتهاك لمبدأ السرية إذا كان الطالب غير مخول أن يحصل على المعلومات.

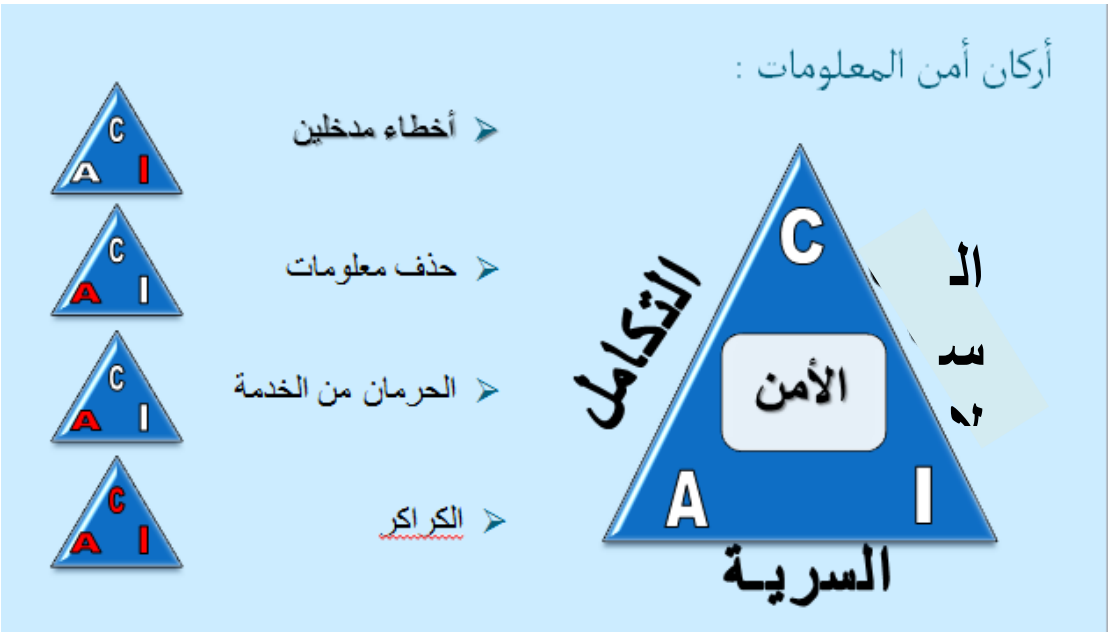
السرية أمر ضروري (لكنها غير كافية) للحفاظ على الخصوصية من الناس الذين يخترقون الأنظمة لسرقة المعلومات الشخصية في لنظام التعليق.

2- سلامة

في مجال أمن المعلومات، السلامة تعني الحفاظ على البيانات من التغيير والتعديل من الاشخاص الغير مخول لهم بذلك. عندما يقوم شخص بقصد أو بغير قصد انتهاك سلامة أو الإضرار أو حذف ملفات البيانات الهامة وهو غير مخول بذلك فهذه انتهاك لسلامة البيانات، وعندما يصيب فيروس كمبيوتر ويقوم بتعديل بيانات أو اتلافها فهذا انتهاك سلامة بيانات، وعندما يكون الموظف قادرا على تعديل راتبه في قاعدة البيانات والمرتبات، وعندما يقوم مستخدم غير مصرح له بتخريب موقع على شبكة الإنترنت، وهلم جرا.

3- توفر قاعدة البيانات

يهدف أي نظام للمعلومات لخدمة غرضه، يجب أن تكون المعلومات متوفرة عند الحاجة إليها. وهذا يعني أن الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات، والضوابط الأمنية المستخدمة لحمايته، وقنوات الاتصال المستخدمة للوصول إلى ذلك يجب أن يعمل بشكل صحيح. توافر نظم عالية السرية تهدف إلى استمرارية الحماية في جميع الأوقات، ومنع انقطاع الخدمة بسبب انقطاع التيار الكهربائي، أو تعطل الأجهزة، اونظام الترقيات والتحديث. ضمان توافر ينطوي أيضا على منع الحرمان من الخدمة الهجمات.



جرائم المعلوماتية:

هي تعبير شامل يشير إلى جريمة تتعلق باستعمال إحدى وسائل تقنية المعلومات لغرض خداع الآخرين وتضليلهم، أو من أجل تحقيق هدف معين لجهة معينة.

تُكبد جرائم المعلوماتية الحكومات والمنشآت خسائر تقدر بمليارات الدولارات سنوياً.

تصنيف جرائم المعلوماتية:

1. جرائم هدفها نشر المعلومات:

مثل الحصول على أرقام البطاقات الائتمانية، والحسابات المصرفية ومعلومات استخباراتيه.

2. جرائم هدفها نشر معلومات غير صحيحة:

مثل نشر المعتقدات والافكار الخاطئة .

3. استخدام تقنية المعلومات كوسيلة لأداء الجريمة:

مثل تزوير بطاقات الائتمان والتحويل بين الحسابات المصرفية.

4. جرائم لها علاقة بانتشار تقنية المعلومات:

مثل قرصنة البرامج الأصلية والتي تكون أسعارها $5000 لتباع بأقل من $10

المخترقون:

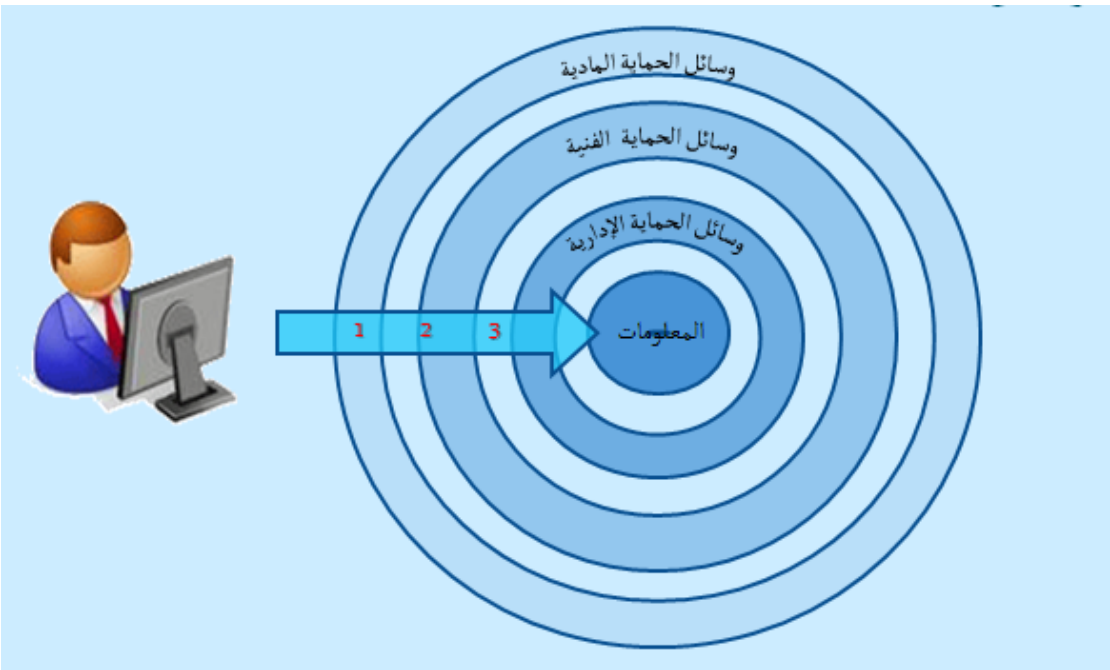
أ- الكراكر:

1. يمتلك القدرة على اختراق أنظمة التشغيل والبرامج الغير مجانية والتلاعب في برمجتها وإعطاؤها رقم خاص لكي تعمل.
2. ويقوم بكسر الأنظمة الأمنية لأهداف تخريبية، فقد يكون هدفه سرقة معلوماتك أو في أسوأ الأحيان القضاء على النظام المعلوماتي الإلكتروني، بشكل كلي.
3. كثير منهم يقوم بسرقة البرامج و توزيعها مجانا لهدف، فمنهم من يضع ملف الباتش بين ملفات هذا البرنامج.
4. الكراكر دائما عمله تخريبي ولا ينفع سوى نفسه أو من يدفع له.

ب- الهاكر:

1. يحاول فقط أن يتعرف على كيفية عمل النظام والبرامج لكي يساعد في تطويرها وتحسينها.
2. لديه القدرة الكاملة على اختراق أنظمة التشغيل عبر الانترنت.
3. يقوم الهاكر بحل المشاكل و بناء الأشياء, و يؤمن بالعمل التطوعي.
4. الهاكر دائما عمله بناء ومفيد و ينفع الآخرين.

وسائل الحماية:



أ- وسائل الحماية المادية:

وهي الأجزاء المحسوسة من وسائل الحماية.

من أمثلتها:

1. الكاميرات (الفيديو أو الفوتوغرافية)
2. أجهزة الإنذار .
3. الجدران والأسوار والمفاتيح.
4. بطاقات دخول الموظفين.
5. أجهزة اكتشاف الأصوات والحركة.

ب- وسائل الحماية الفنية:

وهي تقنيات تحديد وإثبات هوية المستخدم وصلاحياته ومسئولياته.

من أمثلتها:

1. كلمة المرور.
2. القياس الحيوي.

3. التشفير.
4. الجدران النارية.
5. البرامج المضادة للفيروسات.
6. التوقيع الالكتروني.

ج- وسائل الحماية الإدارية:

وهي إعداد وصياغة سياسات أمن المعلومات وتتضمن:

- تشريعات داخل المنشأة لتنظيم أمن المعلومات وتحديد المسئوليات والأدوار.
- تحدد ما هو مسموح به وما هو غير مسموح به للتعامل مع المعلومات ومع نظم المعلومات.

<u>من أمثلتها:</u>

1. اتفاقية صلاحيات المستخدم وقبول استخدام النظام.
2. الخصوصية.
3. كلمات المرور.
4. البريد الالكتروني.

بعض الامثلة لوسائل تحقيق أمن المعلومات:

1- كلمة المرور

أو كلمة السر هي تشكيلة من الحروف الأبجدية والأرقام والرموز الأخرى تمكن من يعرفها من الوصول أو استعمال مورد أو خدمة محمية .ومن الضروري عدم إفشاء كلمة السر لتفادي وقوعها بين أيدي آخرين فتفتح لهم الباب إلى ما لم يكن بوسعهم الوصول إليه بدونها. تقنيا، تعتبر كلمة السر من وسائل الحماية الضعيفة مقارنة مع وسائل أخرى.

لاختيار كلمة المرور:

1. يُفضل أن تحتوي على أحرف وأرقام.
2. يُفضل أن لا تقل عن 8 خانات.
3. يُفضل أن لا تكون مشهور ومتداولة.
4. يمكن استخدام معادلة بسيطة لإنشاء كلمة المرورز

2- القياس الحيوي Biometrics:

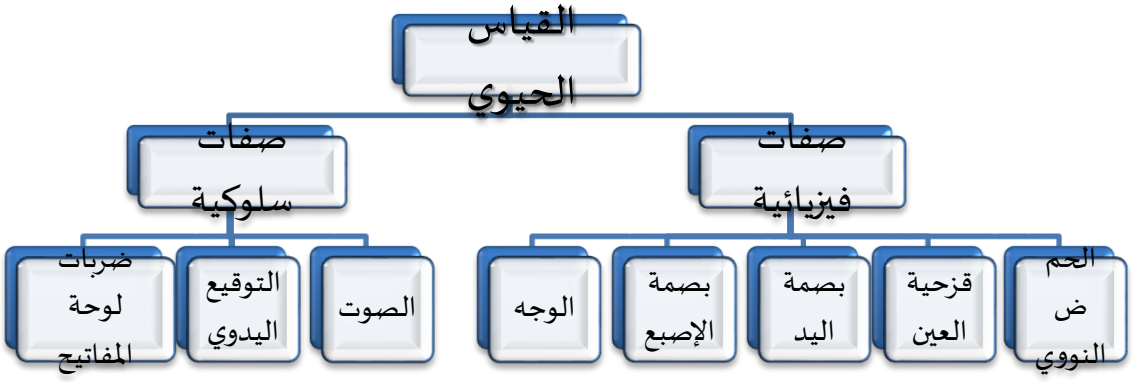
BioMetricsهي كلمة إغريقية مكونة من جزئين "BIO" ومعناها الحياة و "METRICS" ومعناها قياس.

والتعريف الدقيق للقياس الحيوي : هو العلم الذي يستخدم التحليل الإحصائي لصفات الإنسان الحيوية وذلك للتأكد من هويتهم الشخصية باستخدام صفاتهم الفريدة.

انواع القياس الحيوي

1.الصفات الفيزيائية: وهي الصفات التي تتعلق بجزء من جسم الإنسان.

2.الصفات السلوكية: وهي الصفات التي تتعلق بسلوك الإنسان.



مميزات القياس الحيوي :

يوفر لنا القياس الحيوي عدد من المزايا منها:

1. الأمن والخصوصية:

- يمنع الأشخاص الآخرين من الدخول الغير مصرح على البيانات الشخصية.
- إيقاف سرقة الهوية،مثل استخدام البطاقات الائتمانية أو الشكيات المسروقة.

2. البديل لحمل الوثائق الثبوتية مثل:

- بطاقة الهوية الوطنية.
- رخصة القيادة.
- بطاقة الائتمان.

3. البديل لحفظ وتذكر الأرقام السرية.
4. البديل لحمل المفاتيح للدخول إلى:

- السيارات.
- المنازل.
- المكاتب.

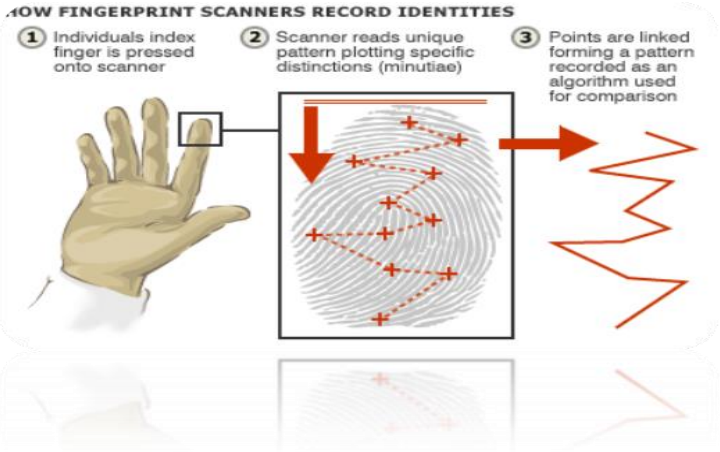
5. تأمين سرية العمليات المالية مثل:

- مكائن الصراف الآلي ATM

– التجارة الإلكترونية.

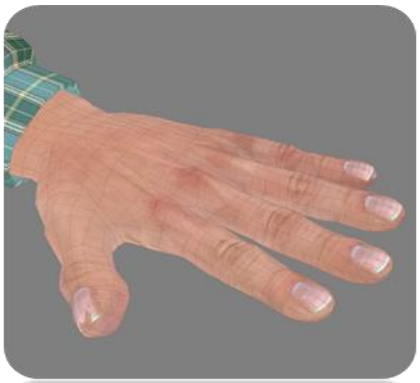
بصمة الإصبع Fingerprint Scanning:

أكثر الأنظمة شيوعًا في الاستخدام وخاصة بين المستخدمين لأجهزة تقنية المعلومات .بصمة الإصبع تمسح ضوئيًا باستخدام قارئات خاصة، ومن الأمثلة على هذه القارئات :أجهزة تربط بالكمبيوتر ، أو تأتي مدمجة مع الفأرة.



بصمة اليد Hand Geometry:

يُستخدم هذا النظام منذ سنوات عديدة وبشكل خاص في أنظمة متابعة الحضور والانصراف وتسجيل الوقت .يعطي هذا النظام توازنًا جيدًا بين الأداء والدقة وسهولة الاستخدام .ومن السهولة دمجه في أنظمة أخرى . توضع اليد على الجهاز الماسح في المكان المخصص لها، ويقوم النظام بفحص تسعين صفة من بينها شكل اليد ثلاثي الأبعاد 3D، طول وعرض الأصابع، وكذلك شكل مفاصل الأصابع.

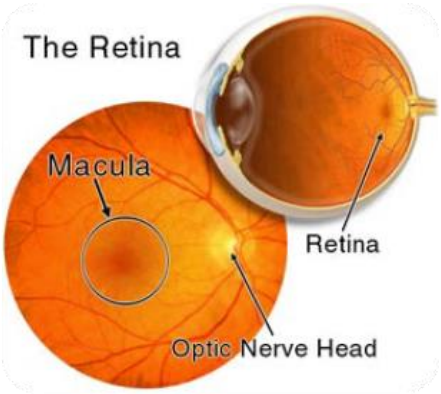


قزحية العين Iris Scanning:

يعتمد النظام المستخدم لقزحية العين على ثباتها حيث أنها الجزء الذي لا يتغير من الجسد .ولها ميزة أيضًا أنها مرئية عن بعد، ليست كصفة الشبكية .أيضًا قزحية العين اليسرى تختلف عن العين اليمنى لنفس الشخص.، ولا يحتاج المستخدم أن يقرب هذه العدسات من عينه، وهي بالتالي تعطي دقة عالية مع سهولة الاستخدام.

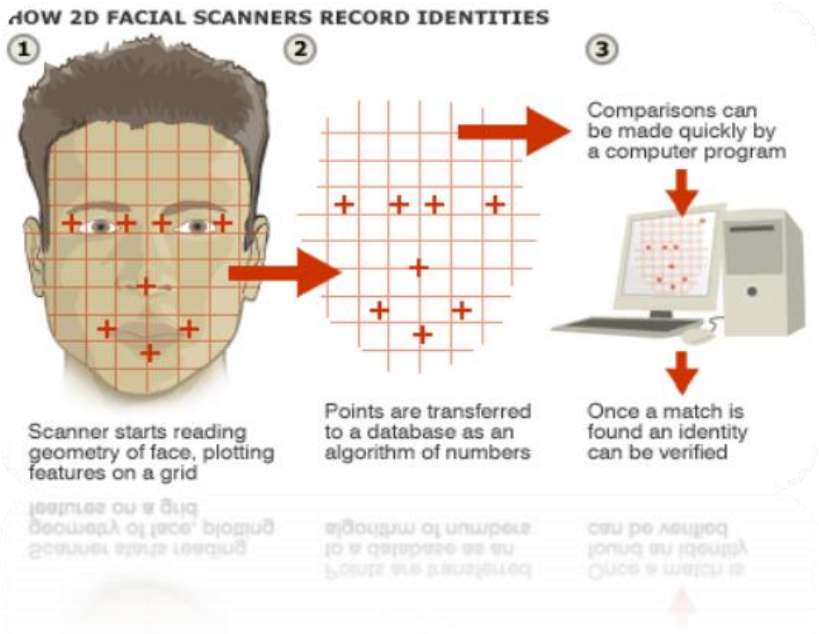
شبكية العين Retina Scanning:

هذه الطريقة تستخدم مصدر ضوء منخفض لعمل مسح للشعيرات الدموية خلف العين. عيب هذه الطريقة أن المستخدم يجب أن ينظر ويركز على الماسحة وهذا يسبب للمستخدم عدم الرغبة للتعامل مع النظام.



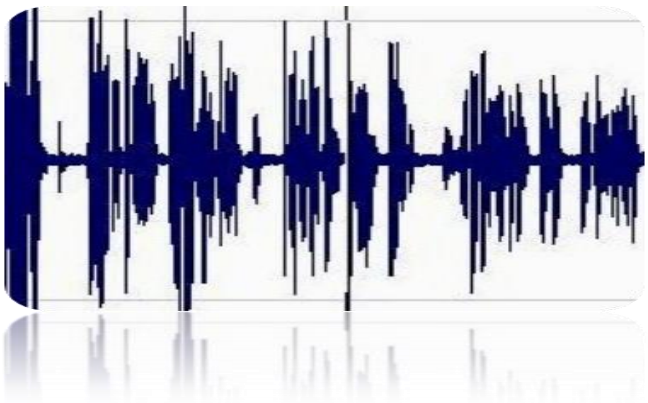
الوجه Facial Scanning:

هذا النظام يعتمد على أخذ صورة كاملة للوجه من آلة تصوير، وقيام النظام بمقارنتها مع ما خزن فيه مسبقًا .مازالت هذه التقنية في أوج التطوير، وما هو موجود حالياً من الأنظمة المعتمدة على صورة الوجه لا تعطي دقة عالية.



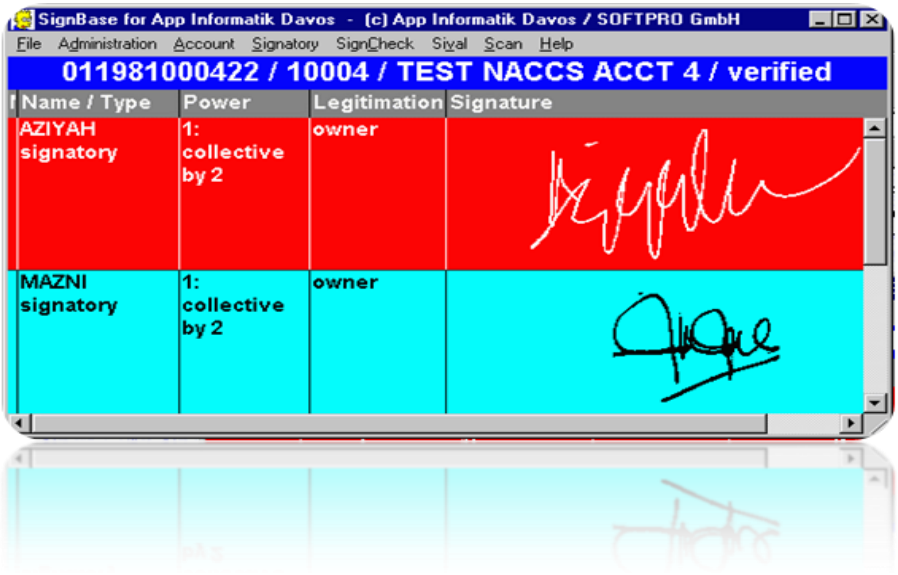
الصوت Voice Verification:

في هذه الأيام، برامج تدقيق الصوت تعد من الإضافات الشائعة لأجهزة الكمبيوترات الخاصة لدى معظم الشركات والبنوك .لكن أنظمة القياس الحيوي ألمعتمدة على الصوت، فإنها تحلل ترددات الصوت بشكل أ...كثر دقة لكي تعطي نتائج صحيحة يُعتمد عليها .ولذلك يجب أن تكون بيئة هذا النظام هادئة، حيث أن أي ضجة تؤثر على النتيجة و أجهزة هذا النظام قد تكون مستقلة بحد ذاتها أو مدمجة مع أنظمة الهاتف التي قد تساعد في مجالات عديدة منها الأنظمة المصرفية.



التوقيع اليدوي Signature Verification:

هذا النظام يعتمد على الطريقة التقليدية لتوقيع الشخص، ولكنها تتم من خلال توقيع الشخص على شاشة حساسة للمس باستخدام قلم ضوئي. ويتم من خلالها تحويل توقيعه إلى شكل رقمي ومن ثم مقارنته مع ما خزن مسبقًا في النظام.



الحمض النووي DNA Scanning:

هذا النظام يعتمد على الشريط الوراثي للشخص DNA. وهو نظام معقد جدًا ويستحيل تغييره بين الأشخاص، وهذا النظام مكلف جدًا لذلك قليلاً ما يُستخدم.

ضربات لوحة المفاتيح keystroke Dynamics:

هذا النظام يقوم تسجيل ضربات الشخص على لوحة المفاتيح .ومن خلال هذه العملية يقوم بمراقبة الوقت بين ضرب مفتاح والانتقال الأصابع لضرب مفتاح آخر .وكذلك يراقب الوقت الذي يأخذه المستخدم وهو ضاغط على المفتاح .وحيث أنه يجب على المستخدم أن يتذكر أسم المستخدم والرقم السري.

تشفير البيانات Data Encryption:

يشير مصطلح كلمة تشفير إلى تحويل النص العادي(Plaintext) من شكل مقروء, بواسطة خوارزميات التشفير ومفاتيح(Keys) التشفير , إلى هيئة نص مرمز (Ciphertext) وغير مقروءة ,ثم إعادة فك الترميز(Decryption) هذا وإعادة النص إلى أصله بواسطة الخوارزميات أيضا ومن قبل الأشخاص المسموح لهم بذلك (الذين يملكون أدوات فك التشفير).

أنواع التشفير Encryption Types :

يمكن تصنيف التشفير بناءً على المفاتيح المستخدمة في التشفير وفك التشفير إلى نوعين تشفير متماثلSymmetric Encryption وتشفير غير متماثل Asymmetric Encryption:

1- تشفير متماثل Symmetric Encryption:

يعرف أيضا بتشفير المفتاح الخاص Private Key Encryption حيث يستخدم فيه نفس المفتاح لتشفير الرسالة ولفك التشفير.يجب أن يتفق الطرفان على مفتاح التشفير مما يؤدي لمشكلة عند توزيع المفتاح عبر الشبكات فربما يحدث التقاط لهذا المفتاح وبالتالي كشف المراسلات بين الطرفين لذلك يجب تبادل المفاتيح بطريقة تضمن سريتها

2- تشفير غير متماثل Asymmetric Encryption:

يعرف أيضا بتشفير المفتاح العام Public Key Encryption حيث يستخدم فيه زوج من المفاتيح أحدهما لتشفير الرسالة والآخر لفك التشفير يعرف الأول بالمفتاح العام Public Key سمي بذلك لانه يكون معروف للمستخدمين في البيئة المعينة ويستخدم لتشفير الرسائل ,أما الثاني فيعرف بالمفتاح الخاص Private Key سمي بذلك لانه معروف لمستخدم واحد فقط هو مالكه ويستخدم لفك الرسائل المشفرة بالمفتاح العام المقابل له.يعاب على هذه الطريقة كثرة المفاتيح المستخدمة في التشفير وفك التشفير.

مثلا:

اذا اراد المستخدم A ارسال رسالة مشفرة الى المستخدم B باستخدام طريقة **التشفير غير المتماثل** فان A عليه التحصل على المفتاح العام لـ B ثم تشفير الرسالة وارسالها له وطالما الرسالة تم تشفيرها بالمفتاح العام لـ B فان المفتاح الخاص له فقط هو الذي يمكنه فك تشفير الرسالة.وبالمثل إذا أراد B إرسال رسالة الى A فعليه أن يتحصل على المفتاح العام لـ A ثم تشفير الرسالة وإرسالها الى A الذي يستخدم مفتاحه الخاص لفك تشفير الرسالة.

خوارزميات التشفير Encryption Algorithm

هي عبارة عن صيغ رياضية تستخدم لتحويل الرسالة العادية الى مكونات مشفرة Ciphered ويمكن وصف العمليتين رياضيا بالآتي :

وصف الدالة الرياضية لعملية التشفير : **C=E(P,K)** وهي تعني تشفير الرسالة الاصلية لتحويلها الى نص مشفر باستخدام المفتاح K

وصف الدالة الرياضية لعملية فك التشفير : **D(E(P,K),K)** وهي تعني اعادة الرسالة المشفرة الى اصلها بعد تحويلها بواسطة المفتاح K الثاني

حيث :

C تعني الرسالة المشفرة Ciphered

E تعني عملية التشفير Encryption

P تعني نص الرسالة Plaintext

K ترمز لمفتاحي التشفير وفك التشفير

D تعني عملية فك التشفير Decryption

خصائص السياسة الأمنية

Features of security Policy

هناك أربع خصائص رئيسية لأي سياسة أمنية فعالة يمكن تلخيصها كالتالي:

أولاً: يجب أن تضع السياسة الأمنية إطارا قويا للبرنامج الأمني، يتضمن تفاصيل شاملة للمعايير والإجراءات التقنية.

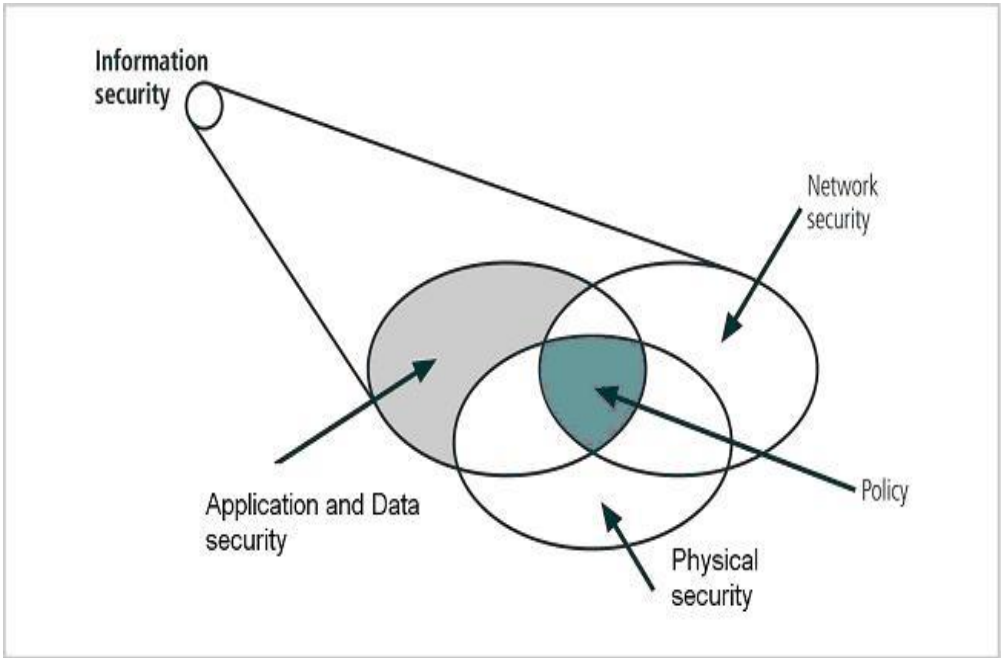
ثانياً: يجب أن تضع هذه السياسة تفاصيل توثيق السياسة وانتشارها، مع ضمان فهم المعنيين داخل المؤسسة وخارجها للسياسة وكيفية تحديدها لمسؤولياتهم

ثالثاً: إضافة إلى ذلك، من مزايا السياسة الأمنية الهامة الأخرى مراقبة التهديدات الناشئة والتعامل معها لضمان تطور السياسة والحلول التي تستند إليها أيضا.

رابعاً وأخيرا: فان السياسة الأمنية الفعالة يجب أن توفر الدليل لضمان أن جميع الأنظمة متوافقة وملتزمة بالسياسة الأمنية والتعليمات.

مما سبق لضمان أمن المعلومات لابد من تطبيق سياسة أمنية متكاملة تضمن مايلي:

1- الأمن المادي للمؤسسة و محتوياتها
2- أمن الشبكات والاتصالات
3- أمن التطبيقات والمعطيات



<u>الأمن المادي</u>

يتضمن الأمن المادي عدة أنظمة تتكامل فيما بينها لتحقيق الحماية الفزيائية وهي :

أولاً :أنظمة التحكم بالدخول Access Control Systems

هناك العديد من تقانات التحكم بالدخول سواء بالدخول إلى المباني أو الدخول إلى الحواسيب،تعتمد أنظمة التحكم بالدخول إلى المباني والغرف حالياً على الأقفال المبرمجة لفتح أو إقفال البوابات في المباني أو العربات وذلك عن

طريق قارئات Readers تقوم بالتحقق من الشخص المخوَّل للدخول أو الخروج وإعطاء الأوامر للأقفال بفتح هذا الباب أو إغلاقه .

ويمكن أن تكون هذه القارئات تقليدية تعتمد على رقم سري للدخول أو بطاقة (مغناطسية- شريط مرمز- ذكية) أو يمكن أن تكون قارئات متطورة تعتمد على مطابقة الصفات الحيوية للأشخاص(شكل الوجه، بصمة الأصبع، بصمة اليد، قزحية العين، الصوت أو مركبة المورثات DNA).

ترتبط هذه القارئات بنظام مراقبة مركزي تسمح للمسؤول عن حماية النظام والمنشاة مراجعة قواعد البيانات ومعرفة حركة الدخول والخروج في كافة أماكن وغرف المنشأة.

ثانياً :أنظمة المراقبة المرئية Video monitoring system

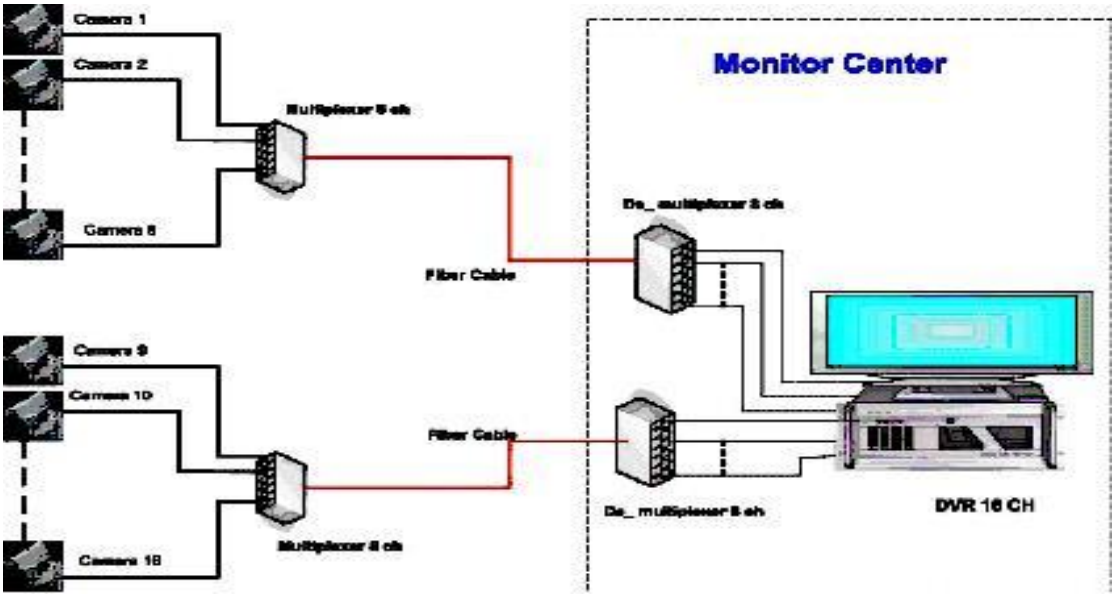
تعتمد هذه الأنظمة على كاميرات المراقبة وملحقاتها من أجهزة تسجيل وتحكم, فتوضع الكاميرات بما يتناسب مع الموقع المراد مراقبته من حيث القطاع وشدة الإضاءة. ويمكن أن تكون هذه الكاميرات ثابتة أو متحركة, ويمكن أن تكون مصمَّصمة لمراقبة المواقع داخل مبنى أو خارجه .

ويوجد تقنيتان في كاميرات المراقبة :

1- الكاميرات التمثيلية CCTVأنظمة الدارات التلفزية المغلقة

توصل الكاميرا بكبالٍ مخصصة لنقل إشارة الفيديو من الكاميرا إلى جهاز التسجيل الرقمي Digital Video Recoder (DVR) الذي يمكن أن يكون جهازاً خارجياً مستقلاً أو بطاقةَ تحصيل تركب في أحد الحواسب .

ويبين الشكل التالي مخطط ربط كاميرات عن طريق كبالٍ ضوئية



2- كاميرات عبر الشبكة الحاسوبة IP camera

توصَل مباشرة إلى الشبكة الحاسوبية الموجودة، ويكون لهذه الكاميرات عنوان شبكي خاص IP Address يولج إليها أو للتحكم عن طريق هذا العنوان وضمن سماحيات وطرق ولوج محددة .

ثالثاً : أنظمة الإنذار Alarm system

تعتمد هذه الأنظمة على توزيع مُحِسَّات تقوم بمراقبة خصائص معينة وإعطاء الإنذارات عند مستويات محددة لإعطاء الإنذارات المناسبة عند حدوث خطر معين في المبنى ويمكن استخدام :

مُحِسَّات الحريق، مُحِسَّات الدخان، مُحِسَّات الحرارة، مُحِسَّات الرطوبة، مُحِسَّات الضغط، مُحِسَّات الصوت أومُحِسَّات تغير التدفق

كما يمكن أيضاً تصميم الأبنية والغرف السرية باستخدام جدران وأسقف وأرضيات من مواد معينة تكون مقاومةً للحريق والانفجار.

إن التكامل بين الأنظمة المستخدمة في الأمن المادي هو من الأمور الأساسية الواجب أخذها بعين الإعتبار في دراسة السياسة الأأمنية للمؤسسة، كذلك تكامل هذه الأنظمة مع بقية التقانات الأمنية المستخدمة في أمن المعلومات Information Security للوصول إلى نظام أمني متكامل .

<u>الاخطار المؤثرة في المكونات المادية</u>

هناك الكثير من العوامل التي تعرض سلامة الحاسوب الشخصي للخطر والتي يمكن تصنيفها إلى :

1. الحرارة العالية

الحاسوب الشخصي شأنه شأن الأجهزة الكهربائية الاخرى، فيه الكثير من القطع التي تولد حرارة أثناء عملية التشغيل مما يؤدي إلى ارتفاع درجة الحرارة داخل الحاسوب بمعدلات أعلى من البيئة المحيطة له، لذا يتم تجهيز الحاسوب بمراوح داخلية تعمل مع بداية التشغيل، لغرض تقليل درجة الحرارة للمعدل المقبول، من خلال دفع الهواء الساخن الناتج عن ارتفاع درجة حرارة القطع والبطاقات الموجودة داخل علبة الحاسوب. وسحب تيار هواء بارد من المحيط الخارجي من خلال فتحات التهوية الموجودة في الأغطية الخارجية للعلبة. إلا ان ارتفاع درجة الحرارة الخارجية إلى أكثر من المعدلات الموصى بها (16-33) درجة مئوية. قد يؤدي إلى تضرر الحاسوب، وعليه يجب اتخاذ الإجراءات الآتية للمحافظة على الحاسوب:

أ. التأكد من وضع الحاسوب في المواضع التي تسمح للهواء بالمرور إلى داخل علبة الحاسوب من خلال فتحات التهوية.

ب. تجنب تشغيل الحاسوب عندما ترتفع درجة حرارة الغرفة إلى أكثر من (33) درجة، في حال تعطلت أجهزة التكيف.

ت. الفحص المستمر للمراوح الداخلية والتأكد من عملها بشكل صحيح. خاصة المروحة المخصصة للمعالج ومجهز القدرة.

ث. تجنب وضع أجهزة تولد طاقة حرارية بالقرب من الحاسوب المستخدم. فضلا عن تجنب وضعه في مكان تصل إليه أشعة الشمس بشكل مباشر.

ج. و لزيادة الأمان نقوم بإضافة بطاقات أو دارات متحسسة للحرارة تركب داخل الحاسوب وتطلق إشارة إنذار عند ارتفاع درجة الحرارة لحد معين خارج الحد المسموح به.

2. الغبار

يتألف الغبار من ذرات رمل صغيرة ومواد أخرى عضوية، ويسبب عدة مشاكل للمكونات الداخلية للحاسوب الشخصي، مع ملاحظة ان تشغيل الحاسوب، سيؤدي إلى وجود شحنة كهربائية تولد مجال مغناطيسي يؤدي إلى جذب الغبار والأتربة إلى داخل علبة الحاسوب، فضلا عن ان عمل المراوح الداخلية يؤدي إلى تكوين تيار هواء يسحب معه الغبار إلى داخل علبة الحاسوب. ان هذا الغبار يمكن ان يؤدي إلى :

أ. تراكم ذرات الغبار على الدارات داخل الحاسوب يؤدي إلى تشكيل طبقة عازلة حرارياً وهذا يقلل من تبديد الحاسوب للحرارة الناتجة.

ب. يسد الغبار منطقة امتصاص الهواء في وحدة الإمداد بالطاقة و القرص الصلب.

ت. يسد الغبار بين رأس القراءة والكتابة وبين القرص في مشغل الأقراص المرنة.

ولتجنب هذه المشاكل يراعى وضع الحاسوب في الغرف والقاعات التي يتم تكيفها باستخدام أجهزة التكيف، ولا يتم فيها فتح النوافذ لمنع دخول الغبار. كما يفضل وضع الحواسيب في مؤسسات المعلومات في القاعات التي لا يستخدم السجاد (والموكيت) في تغطية أرضيتها. ومن المفيد دائما تنظيف الحواسيب باستخدام أجهزة نفخ الهواء كل سنة مرة على الاقل.

3. المجال المغناطيسي

معظم الأجهزة الكهربائية تولد مجال مغناطيسي عند تشغيلها، ولكن بحدود قليلة نسبيا، لكن في حال تعرض الحاسوب الشخصي إلى مجال مغناطيسي عالي، فان المكونات الممغنطة فيه مثل القرص الصلب او الأقراص المرنة قد تتأثر، ويتم فقد المعلومات المخزنة عليها. وهو ضرر قد يحث في حال تمرير الأقراص المرنة او أجهزة الحاسوب الشخصي (المحمول) خاصة في أجهزة فحص الأمتعة في المطارات والمناطق الحساسة الاخرى. لذا يفضل دائما استخدام الأقراص الليزرية في تخزين نسخ من البيانات والمعلومات، في حال وجود تنفيذ عملية فحص الأجهزة في الأماكن المشار إليها.

4. تذبذب الطاقة

يعتبر مقبس الطاقة الجداري مصدراً لكثير من المشاكل التي يمكن ان تؤثر في المكونات المادية للحواسيب، إذ تصنف تأثيرات مصدر الطاقة إلى:

أ. المشاكل الناتجة عن ازدياد الجهد وانخفاض الجهد(تذبذب التيار). إن انخفاض الجهد يؤدي إلى زيادة التيار المستهلك وهذا بدوره يؤدي إلى زيادة القواطع الكهربائية والتوصيلات مما يؤدي إلى ارتفاع حرارة وحدة الإمداد بالطاقة وكذلك الرقائق ويمكن حل هذه المشكلة بالاستعانة بأجهزة تنظيم الكهرباء.

ب. المشاكل الناتجة عن غياب الجهد نهائياً. والتي تؤدي إلى توقف التشغيل في بعض المكونات، واستمراره في مكونات أخرى.

ت. المشاكل الناتجة عن العبور . العبور هو عبارة عن تغير طفيف في الطاقة لا يمكن أنه يكرر نفسه مرة أخرى ويأتي على شكل انخفاض في الجهد أو ارتفاع في الجهد فإذا امتلك العبور تردداً كافياً عطل مكثفات الحماية وعناصر أخرى لوحدة الإمداد بالطاقة كما أن الجهد يؤدي إلى نفس الأضرار وتعطيل رقائق الحاسوب

تشغيل الطاقة أو اندفاع الطاقة .

ث. المشاكل الناتجة عن عملية تفريغ الكهرباء الساكنة. جسم الإنسان قابل أن يشحن بشحنة ساكنة وقد تصل إلى حوالي 50 ألف فولت ويكفي 200 فولت لإفساد الرقائق الإلكترونية لذلك قبل البدء بأي عملية صيانة يجب تفريغ الشحنة التي تحملها بواسطة لمس أشياء معدنية ويمكن تجنب مشكلة الكهرباء من خلال زيادة رطوبة الجو بواسطة أجهزة زيادة الرطوبة .او زيادة رطوبة الجو عن طريق اقتناء نباتات الزينة وأحواض السمك.

5. عوامل التآكل

يعد الماء والأملاح من المواد الخطرة على الحاسوب ويجب تجنيب الحاسوب الأشياء التالية :

أ. انسكاب الماء او إي سوائل أخرى غير المقصود .

ب. الترشيح الناتج عن تسرب المياه الرطبة إلى داخل الحاسوب .

ت. فيضان المياه ودخول الماء إلى الحاسوب .

ث. ويعد التآكل عمل اخر من عوامل الأضرار بالأجهزة نتيجة تراكم الأملاح بسبب تعرق جسم الإنسان ، و تراكم الأحماض الكبريتية الناتجة عن النقل بواسطة الطائرات .

ج. إن المشكلة الكبرى التي نتعرض لها هي أكسدة نقاط الدارات وبالتالي تفقد وظيفتها في وصل الدارات ببعضها، وبالتالي تعطل الحاسوب .

لهذا السبب، يجب توخي الحذر عند التعامل مع بطاقات الدارات وعدم لمس أقطابها خوفاً من تأثير الأملاح الناتجة عن التعرق .

البيئة المناسبة لعمل الحاسوب

يجب ملاحظة بعض الامور لجعل البيئة المحيطة بالحاسوب مناسبة للتشغيل، وتحقق مستوى أمان مناسب للحفاظ على الجهاز ومن هذه الامور :

أ. تأكد من تأمين شروط حماية الطاقة الكهربائية . وذلك بعدم ربط الحاسوب مباشرة إلى مصدر طاقة، وإنما يفضل استخدام جهاز حماية UPS.

ب. يفضل عدم مشاركة الحاسوب لاي جهاز كهربائي اخر على نفس مصدر الطاقة.

ت. لا يفضل تشغل محركات ضخمة على نفس خط الطاقة الذي يغذي الحاسوب .

ث. إبعاد الحاسوب عن مصادر الضجيج .

ج. حافظ على مستوى معتدل لدرجة حرارة الغرفة.

ح. يساعد إبقاء الحاسوب في حالة عمل دائم على ضبط حرارة الحاسوب الداخلية بشكل جيد .

خ. تأكد من عدم وجود أي مصدر للاهتزاز على نفس الطاولة . التي يوجد عليها الحاسوب.

د. الحرص على تعميم إجراءات السلامة تلك على جميع العاملين في مؤسسات المعلومات الذين يستخدمون الحاسوب.

أهم الاخطار التي تهدد بيئة المعلومات الرقمية وكيفية تجنبها، و وسائل الحماية المناسبة لتأمينها.

أولا .الفيروسات Virus

فيروس الحاسوب، هو برنامج خارجي، تم تطويره من قبل مبرمجين محترفين، لغرض إلحاق الضرر في الحواسيب من خلال تغيير خصائص الملفات التي يصيبها، لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب و ما شابهها من عمليات. أي ان فيروسات الحواسيب هي برامج تتم كتابتها بغرض إلحاق الضرر بحاسوب آخر، أو السيطرة عليه.
سمي الفيروس (Virus) بهذا الاسم لتشابه آلية عمله مع تلك التي تصيب الكائنات الحية، بعدد من الخصائص، كخاصية الانتقال بالعدوى، أو كونه كائنا غريبا يقوم بتغيير حالة الكائن المصاب، إضافة إلى الضرر الذي يعقبه إن لم يتم العلاج. سُمّيت بالفيروسات، لأنها تشبه تلك الكائنات المتطفلة في صفتين رئيسيتين:

الصفة الاولى تحتاج فيروسات الحاسوب دائماً إلى ملف عائل تعيش متستّرةً فيه. فالفيروسات دائماً تتستر خلف ملف آخر، ولكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس ايضا تشبه بطريقه هذه الفيروسات ألبيولوجيه حيث لا يستطيع أي فيروس العيش بدون إصابته لخليه في جسم الكائن الحي (بدون الخلية يتلف الفيروس ويتلاشى) .

الصفة الثانية انتقالها يشبه طريقة انتقال الفيروسات البيولوجية حيث تتواجد الفيروسات في مكان أساسي في الحاسب كالذاكرة رام مثلا، وتصيب أي ملف يشغل في أثناء وجودها بالذاكرة مما يزيد عدد الملفات المصابة، كلما تأخر وقت اكتشاف الفيروس (كما الفيروس البيولوجي بعد استنزافه للخلية الحية يدمرها ويتكاثر في خلايا اخرى .ويمكن الإحساس بوجود الفيروس في جهاز الحاسوب من خلال سلسلة من الأعراض التي تظهر عند الاستخدام ومنها على سبيل المثال:

- تكرار رسائل الخطأ في أكثر من برنامج.
- ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.
- تكرار اختفاء بعض الملفات التنفيذية.
- حدوث بطء شديد في إقلاع نظام التشغيل أو تنفيذ بعض التطبيقات.
- رفض بعض التطبيقات للتنفيذ.

انواع الفيروسات

ان أهداف الفيروسات في الغالب تكون مختلفة، وحجم الضرر الذي يمكن ان تلحقه يتباين بين التدمير الشامل الى مجرد الإزعاج، وبشكل عام يمكن تصنيف الفيروسات الى ثلاث أصناف على اساس سلوكها في إحداث الضرر في المعلومات وكالآتي:

1. الفيروس

يمكن القول بأنه برنامج تنفيذي يعمل بشكل منفصل ويهدف إلى إحداث خلل في نظام الحاسوب وتتراوح خطورته حسب مهمته فمنه الخبيث الذي قد يؤدي الى إبطال عمل الحاسوب تماما، ومنه المزعج الذي لا يحدث ضرر كبير ولا يؤثر في المعلومات، لكنه يشكل مصدر إزعاج مستمر لمستخدم الحاسوب، مثل تغير اللغة او لون الشاشة او ان يكرر نفسه في مواضع خزنية مختلفة.

2. الدودة (worm)

هي فيروس ينتشر عبر الشبكات والانترنت، عن طريق دفتر عناوين البريد الالكتروني غالبا، فعند إصابة الجهاز يبحث البرنامج الخبيث عن عناوين الاشخاص المسجلين في دفتر العناوين على سبيل المثال ويرسل نفسه إلى كل شخص وهكذا ... مما يؤدي إلى انتشاره بسرعة عبر الشبكة وقد اختلف الخبراء فمنهم اعتبره فيروس ومنهم من اعتبره برنامج خبيث وذلك كون الدودة لا تنفذ أي عمل مؤذي إنما تنتشر فقط. مما يؤدي إلى إشغال موارد الشبكة بشكل كبير. ومع التطور الحاصل في ميدان الحوسبة أصبح بإمكان المبرمجين الخبيثين إضافة سطر برمجي لملف الدودة بحيث تؤدي عمل معين بعد انتشارها (مثلا بعد الانتشار إلى عدد 50000 جهاز يتم تخريب الانظمة في هذه الأجهزة) او إي شئ اخر (مثلا في يوم معين او ساعة او تاريخ ...الخ) وأصبحت الديدان من أشهر الفيروسات على الشبكة العالمية وأشهر عملياتها التخريبية وأخطرها تلك التي يكون هدفها حجب الخدمة تسمى (هجمات حجب الخدمة) حيث تنتشر الدودة على عدد كبير من الأجهزة ثم توجه طلبات وهميه لجاهز خادم معين (يكون المبرمج قد حدد الخادم المستهدف من خلال برمجته للدودة) فيغرق الخادم بكثرة الطلبات الوهمية ولا يستطيع معالجتها جميعا مما يسبب توقفه عن العمل. وهذه الديدان استهدفت مواقع لكثير من الشركات العالمية أشهرها مايكروسوفت .

3.حصان طروادة Trojan Horse

سمي هذا الفيروس بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة، حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها، وهكذا تكون آلية عمل هذا الفيروس، حيث يكون مرفقا مع أحد البرامج أي يكون جزء من برنامج ما دون ان يعلم المستخدم. فعندما يبدأ البرنامج تنفيذ عمله ويصل إلى مرحلة ما يبدأ الفيروس العمل والتخريب. وقد لا يكون هدف الفيروس التخريب هنا قد يكون هدفه ربحي مثل القرصنة على الحسابات المصرفية والكشف عن كلمات المرور.

عموما توجد عدة تصنيفات اخرى للفيروسات ، فمثلاً من حيث سرعة الانتشار هناك فيروسات سريعة الانتشار، وفيروسات بطيئة الانتشار ومن حيث توقيت النشاط ،فيروسات تنشط في أوقات محددة وفيروسات دائمة النشاط، ومن حيث مكان الإصابة فيروسات مقطع التشغيل boot sector على الأقراص وهي الأكثر شيوعاً، وفيروسات الماكرو macro التي تختص بإصابة الوثائق والبيانات الناتجة عن حزمة مايكروسوفت أوفيس، أما من حيث حجم الضرر فهناك الفيروسات المدمرة للأجهزة التي تعطل الذاكرة روم في الحاسب كما في فيروس تشرنوبل، او ان يمحي معلومات ال MBR على القرص الصلب فتعود الأقراص الصلبة كما خالية، وفي الحالتين السابقتين لا يتم إقلاع الجهاز مما يوحي للبعض ان الفيروس قد أعطب الجهاز. ومن المخاطر المحتملة للفيروسات على حواسيب مؤسسات المعلومات، إنها تتسبب في إتلاف البيانات المخزنة والتي قد تكون (البيانات) نتاج عشرات السنين مما يؤدي إلى خسائر جسيمة او إلى توقف الحاسبات عن العمل وبالتالي توقف الخدمات المقدمة للمستفيدين.

وسائل الحماية من الفيروسات

حماية الحاسوب الشخصي من الإصابة بالفيروسات تبدو مهمة شبه مستحيلة، خاصة عندما يكون الحاسوب مرتبط بشبكة الانترنت، وعلى العاملين في مؤسسات المعلومات إدراك هذه الحقيقة، والتعاطي معها كي لا يتم هدر الجهد الكبير الذي بذل في بناء محتوى قواعد المعلومات الخاصة بالمؤسسة. وعليه هناك العديد من وسائل الحماية، التي يمكن اتخاذها للحد من خطر الإصابة بالفيروسات وتقليل أثارها الى ادنى حد ممكن.

وقبل ان نناقش هذه الوسائل يجب التعرف على طرائق انتقال الفيروس الى الحاسوب الشخصي. والتي يمكن ان تكون عن طريق استخدام الأقراص المرنة في نقل الملفات، او الأقراص المدمجة المنسوخة، او الذاكرة الضوئية، او مرفقات رسائل البريد الالكتروني، او المواقع الإباحية. فضلا عن ذلك فان ذاكرة أجهزة الهاتف المحمول في حال تعريفها الى جهاز الحاسوب تعد طريقة اخرى لنقل الفيروسات مع وجود تقنية البلوتوث. وقد تلجأ بعض شركات البرمجيات الى استخدام الفيروس وسيلة لحماية منتجاتها البرمجية من النسخ والتقليد. وأمام هذه الطرائق المتعدد لانتقال الفيروسات، نؤكد القول السابق ان المهمة تكاد تكون شبه مستحلية للحفاظ على الحاسوب من خطر الإصابة، لكن يمكن الحد منها وتقليل أثارها باستخدام وسائل الحماية الآتية:

1. تنصيب برامج مكافحة الفيروسات (Antivirus) والتركيز على الإصدارات العالمية المعروفة بكفاءتها. وتجنب استخدام الإصدارات المستنسخة. او تحميلها من خارج مواقعها الرسمية على الانترنت.
2. التحديث المستمر لقاعدة بيانات برامج مكافحة الفيروسات، من خلال شبكة الانترنت.
3. تجنب تنصيب بعض برامج مكافحة الفيروسات المعروضة مجانا على الانترنت، او تجربتها.
4. منع استخدام الحاسوب الشخصي خارج الاغراض المخصص لها في مؤسسة المعلومات. وفي حال عدم الحاجة لاستخدام قارئ الأقراص المرنة، يفضل دائما فصله من داخل علبة الحاسوب.
5. توعية العاملين في مؤسسة المعلومات بمخاطر الفيروسات وتأثيرها على المعلومات والبيانات.

وفي كل الأحوال ومع وجود إي وسائل للحماية، فان الضمان الحقيقي لمؤسسة المعلومات، هو في تنفيذ عملية النسخ الاحتياطي للبيانات والمعلومات، وحفظها على أقراص تخزين مدمجة خارج الحاسوب، لضمان اعادتها في حال الإصابة الشديد التي قد تتطلب عملية اعادة التهيئة.

ثانيا: الاختراق Penetration

معنى الاختراق بشكل عام، هو القدرة على الوصول لهدف معين بطريقة غير مشروعة، عن طريق ثغرات في نظام الحماية الخاص بالهدف وبطبيعة الحال هي سمة سيئة، يتسم بها المخترق لقدرته على دخول أجهزة الاخرين عنوه ودون رغبة منهم، وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية او بنفسيتهم عند سحبة ملفات وصور تخصهم وحدهم . ولم تنتشر هذه الظاهرة لمجرد العبث وإن كان العبث وقضاء وقت الفراغ من أبرز العوامل التي ساهمت في تطورها وبروزها الي عالم الوجود . وترتبط عمليات الاختراق بجملة من الدوافع نوجزها بالآتي:

1- **الدافع السياسي والعسكري**: مما لاشك فيه أن التطور العلمي والتقني أديا

الي الاعتماد بشكل شبة كامل على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية. فمنذ الحرب الباردة والصراع ألمعلوماتي والتجسسي بين

الدولتين العظميين على أشده. ومع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية للأنظمة والدول ، اصبح الاعتماد كليا على الحاسب الآلي، وعن طريقة اصبح الاختراق من اجل الحصول على معلومات سياسية وعسكرية واقتصادية مسالة أكثر أهمية.

2- **الدافع التجاري**: من المعروف أن الشركات التجارية الكبرى تعيش هي ايضا فيما بينها حربا مستعرة وقد بينت الدراسات الحديثة أن عددا من كبريات الشركات التجارية يجرى عليها أكثر من خمسين محاولة إختراق لشبكاتها كل يوم. من قبل مبرمجين الشركات المنافسة او من قبل مبرمجين هواة بهدف الحصول على المعلومات وبيعها للشركات المنافسة.

3- **الدافع الشخصي**: تتطلب عملية الاختراق ذكاء وقدرة برمجية عالية وهي سمة دفعت العديد من الهواة في تجريب قدرتهم واثبات مهاراتهم البرمجية من خلال القيام بعمليات الاختراق، وقد تطورت هذه الحالة إلى سلوك إجرامي في أحيان كثيرة.

4. **دوافع انتقامية**. قد يلجأ بعد المبرمجين ممن يتم فصلهم من وظائفهم إلى الشعور بالظلم ومحاولة الانتقام من المؤسسة التي سرحتهم باختراق أجهزتها واللحاق الضرر في معلوماتها.

انواع الاختراق

يمكن تقسيم الاختراق من حيث الطريقة المستخدمة الي ثلاثة أقسام:

1- **إختراق المزودات او الأجهزة الرئيسية.** للشركات والمؤسسات او الجهات الحكومية وذلك باختراق الجدران النارية التي عادة توضع لحمايتها وغالبا ما يتم ذلك باستخدام المحاكاة Spoofing، وهو مصطلح يطلق على عملية انتحال شخصية للدخول الي النظام، حيث أن حزم الـ IP تحتوي على عناوين للمرسِل والمرسَل إليه، وهذه العناوين ينظر اليها على أنها عناوين مقبولة وسارية المفعول، من قبل البرامج وأجهزة الشبكة . ومن خلال طريقة تعرف بمسارات المصدر Source Routing فإن حزم الـ IP قد تم إعطائها شكلا تبدو معه وكأنها قادمة من كمبيوتر معين بينما هي في حقيقة الأمر ليست قادمة منه وعلى ذلك فإن النظام إذا وثق بهوية عنوان مصدر الحزمة فإنه يكون بذلك قد حوكي (خدع) وهذه الطريقة هي ذاتها التي نجح بها مخترقي الهوت ميل في الولوج الي معلومات النظام.

2- **إختراق الأجهزة الشخصية**. والعبث بما تحويه من معلومات وهي طريقة للأسف شائعة لسذاجة أصحاب الأجهزة الشخصية من جانب ولسهولة تعلم برامج الاختراقات وتعددها من جانب اخر.

3- **التعرض للبيانات أثناء انتقالها.** والتعرف على شفرتها إن كانت مشفرة وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات المصرفية ATM.

ثالث: التجسس Espial

قد لا يختلف التجسس عن الاختراق الا في الهدف، وتبقى الأساليب المتبعة في تنفيذ عمليات الاختراق ذاتها تقريبا. لذا يمكن تعريف التجسس في مجال الحاسوب على انه، اختراق هادف يراد من خلاله تمكين المتجسس من التعرف على محتويات الحاسوب المستهدف، أول بأول دون الإضرار بها. وغالبا ما تتم عمليات التجسس باستخدام نوع من الفيروسات التي تنقل الى الحواسيب وتعمل على إرسال نسخ من البيانات والمعلومات

الى حاسوب اخر، او تمكينه من الدخول الى الحاسوب والتعرف على محتوياته. وغالبا ما تتم عمليات التجسس الرقمي اذا صح التعبير، من خلال مؤسسات سواء كانت مؤسسات حكومية، او غير حكومية، وفي كل الأحوال، يعد التجسس شأنه شأن الاخطار سابقة الذكر عمل غير مشروع.

وسائل الاختراق لاغراض التجسس

ومن النادر بالنسبة للاشخاص قليل الخبرة والمؤسسات الصغيرة ان تدرك الإصابة بملفات التجسس، كونها لا تؤدي الى حدوث أعراض محسوسة عند الاستخدام. وهناك عدة طرائق لتنفيذ عمليات الاختراق لاغراض التجسس يمكن إيجازها بالآتي:

1. ملفات أحصنة طروادة Trojan

لتحقيق نظرية الاختراق لابد من توفر برنامج تجسسي يتم إرساله وزرعه من قبل المستفيد في جهاز الضحية ويعرف بالملف اللاصق ويسمى (الصامت) أحيانا وهو ملف باتش patch صغير الحجم مهمته الأساسية المبيت بجهاز الضحية (الخادم) وهو حلقة الوصل بينه وبين المخترق (المستفيد) . هذا الملف قد يحمل إي اسم، إلا ان الاسم الجامع له على اساس الدور الذي يقوم به وطريقة تسلله إلى حاسوب الضحية هو (حصان طروادة) لأنه يقوم بمقام الحصان الخشبي الشهير في الأسطورة المعروفة، و ربما يكون اكثر خبثا من الحصان الخشبي بالرواية، لأنه حالما يدخل لجهاز الضحية يغير من هيئته فهو خلال فترة قصيرة يغير اسمه وبشكل مستمر . لهذا السبب تكمن خطورة أحصنه طروادة، فهي من جانب تدخل للأجهزة في صمت وهدوء، ومن جانب اخر ويصعب اكتشافها . فضلا عن ذلك فهي لا تترك إي علامات دالة على وجودها.

و تتم عملية إرسال ملفات التجسس بعدة طرق من أشهرها:

- البريد الالكتروني حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر فيجد به برنامج الباتش المرسل فيظنه برنامجا مفيدا فيفتحه او أنه يفتحه بدافع الفضول فيكتشف انه لا يعمل، مع هذه العملية يكون المخترق قد وضع قدمه الأولى بداخل الجهاز.
- تتم عمليه نقله عبر المحادثة من خلال برنامج الـ ICQ.
- عن طريق إنزال بعض البرامج من المواقع الغير موثوق بها .
- كذلك يمكن اعادة تكوين حصان طروادة من خلال الماكرو الموجودة ببرامج معالجات النصوص.

2. بوابات الاتصال Contacting Gates

يتم الاتصال بين أجهزة الحواسيب عبر بوابات ports او منافذ اتصال وهذه المنافذ في واقع الأمر هي جزء من الذاكرة له عنوان معين يتعرف علية الجهاز بأنه منطقة اتصال يتم من خلاله إرسال واستقبال البيانات ويمكن استخدام عدد كبير من المنافذ للاتصال، إذ يزيد عن 65000، ويميز كل منفذ عن الأخر رقمه، فمثلا المنفذ رقم 1001 يمكن إجراء اتصال عن طريقة وفي نفس اللحظة يتم استخدام المنفذ رقم 2001 لإجراء اتصال اخر. من خلال هذه البوابات يتم زرع ملف الباتش في الحاسوب الضحية ليؤدي الدور المطلوب منه في تنفيذ عملية التجسس. ملف الباتش به ورغم خطورة وجود بجهاز الضحية فأنه يبقى في حالة خمول طالما لم يطلب منه المخترق التحرك . ولكن بدونه لا يتمكن المخترق من السيطرة على جهاز الضحية عن بعد، وحتى يتم له ذلك، فإن على المخترق بناء حلقة وصل متينة بينه وبين الخادم عن طريق برامج خاصة تعرف ببرامج الاختراق .

3.عن طريق الـ IP Address

ذكرنا سابقا بأن ملفات الباتش الحاملة لأحصنة طروادة هي حلقة الوصل بين المخترق والضحية ، ولكن في واقع الأمر فإن ملفات الباتش ليست إلا طريقة واحدة لتحقيق التواصل . عند اتصالك بالانترنت تكون معرض لكشف الكثير من المعلومات عنك، كعنوان جهازك وموقعه ومزود الخدمة الخاص بك وتسجيل كثير من تحركاتك على الشبكة. و كثيرا من المواقع التي تزورها تفتح سجلا خاصا بك يتضمن عنوان الموقع الذي جئت منه IP Address ونوع الحاسوب والمتصفح الذي استخدمته بل وحتى نوع معالج جهازك وسرعته ومواصفات شاشاتك وتفاصيل كثيرة. مبدئيا عنوانك الخاص بالانترنت Internet Protocol او IP يكشف الكثير عنك فكل جهاز متصل بالشبكة يكون له رقم معين خاص به يعرف باسم الـ IP Address . وباختصار يكون الـ IP كرقم هوية خاص بكل من يعمل على الانترنت. ومن خلاله يتمكن المخترق المحترف من الولوج الي الجهاز والسيطرة عليه خلال الفترة التي يكون فيها الضحية متصلا بالشبكة فقط ، ولكن هذا الخيار لا يخدم المخترق كثيرا لأن السيرفر الخاص بمزود الخدمة يقوم بتغيير رقم الـ IP الخاص بالمشترك تلقائيا عند كل عملية دخول للشبكة .

4. عن طريق الكوكي Cookie

يمكن ايضا تحقيق التواصل للاختراق عن طريق الكوكي Cookie وهي عبارة عن ملف صغير، تضعه بعض المواقع التي يزورها المستخدم على قرصه الصلب. هذا الملف به آليات تمكن الموقع الذي يتبع له جمع وتخزين بعض البيانات عن الجهاز، وعدد المرات التي زار المستخدم فيها الموقع، كما وأنها تسرع عمليات نقل البيانات بين جهاز المستخدم والموقع فالهدف الأساسي منها هو تجاري أصلا. ولكنه يساء استخدامه من قبل بعض المبرمجين المتمرسين بلغة الجافا Java فهذه اللغة لديها قدرات عالية للتعمق اكثر لداخل الأجهزة والحصول على معلومات اكثر عن المستخدم.

وبعد فإن آلية الاختراق تتم مبدئيا بوضع برنامج الخادم بجهاز الضحية ويتم الاتصال به عبر المنفذ port الذي فتحة للمستفيد (المخترق) في الطرف الأخر ولكن حلقة الوصل هذه تنقصها المعابر وهي البرامج المخصصة للاختراق .

بعد التعرف على طرائق المتجسس في زرع ملف التجسس، يبقى ان نقول انه من حسن الحظ ان برامج مكافحة الفيروسات تتعامل مع ملفات أحصنة طروادة على إنها فيروسات قادرة على إزالتها، اذا تم تحديثها بشكل مستمر. ولكن دائما نؤكد على ان الوقاية خير من العلاج، ولان البريد الالكتروني هو من اكثر الطرق التي يختارها المتجسسين للوصول الى الحواسيب لذا ينصح التعامل مع الرسائل التي نستلمها بحذر شديد ونتجنب فتح إي رسالة لا نعرف مصدرها مهما حملت من إغراءات، خاصة الملفات المرفقة، فملفات أحصنة طروادة لا تعمل ما لم يتم فتح الرسالة المرفقة. لذا فان حذف الرسالة هو الطريقة المثلى للتخلص من هكذا ملفات.

رابعا: البرامج الضارة - Harmful Software

الاختراق ليس الا احد انواع التدمير الممكنة عبر البرامج المؤذية ، لذلك فالمخاطر التي يتعرض لها مستخدم الحاسوب العادي تتنوع بتنوع واختلاف البرامج المؤذية وإمكاناتها. وإن كان الاختراق هو أخطرها وأبرزها. إذ تتراوح المخاطر التي يتعرض لها المستخدم من مجرد إزعاج بسيط الي مستوى الكارثة وقد صنف هذه المخاطر الي أربعة أصناف:

1- **القنابل وبرامج الطوفان** Flooders/Bombers حيث يفاجأ المستخدم بوجود مئات الرسائل في عنوانه الالكتروني او عبر برنامج الـ ICQ من أشخاص وعناوين لم يسمع بهم من قبل وهذا الصنف من المخاطر هو الأقل خطورة حيث انه يسبب إزعاجا على حساب وقت المستخدم .

2- **الخداع** Spoofing. وهو عملية تمويه وطمس للهويه حيث تتم سرقة حساب الدخول للانترنت باسم المستخدم فيجد ساعاته تنقص دون ان يستخدمها او يتم من خلاله سرقة كلمة السر في ساحات الحوار فتكتب مقالات باسمه لم يكتبها.

3- **التدمير من خلال برامج الـ** Hunkers. تقوم هذه البرامج بتعطيل نظام التشغيل ويتراوح خطرها بين تغيير الوقت بساعة النظام وبين توقف النظام كليا عن العمل وتوجد انواع منها، بعضها موجه إلى التركز على برنامج معين لتدميره دون إلحاق الضرر بنظام التشغيل ذاته.

4- **الباب الخلفي** Backdoor هذا الصنف هو الأخطر، وهو الشائع بين كل المخترقين، لأنه يجعل المخترق قادرا على الدخول لجهاز الضحية والسيطرة عليه كليا او جزئيا، بحسب البرنامج المستخدم . ويقصد بالباب الخلفي الثغرات الموجودة بقصد او دون قصد في أنظمة التشغيل وبعض البرامج او المواقع، والتي يراد منها أحيانا التعرف على عيوب النظام، لكن هذه الثغرات تستغل من قبل المخترقين للدخول إلى أجهزة الغير لتحقيق أهدافهم.

الحماية من الاختراق

للحماية من الاختراقات والتجسس هناك عدة طرق تستخدمها برامج الحماية لأداء مهامها ويمكن تصنيف هذه الطرائق الي أربعة على النحو التالي:

1- إنشاء قاعدة بيانات بأسماء أحصنه طروادة، والتي يمكن من خلالها عمل مسح لكافة الملفات الموجودة بجهاز المستخدم ومطابقتها مع الموجود بقاعدة البيانات تلك للتعرف على الملفات المطابقة . على ان يتم تحديث قاعدة البيانات دوريا اما من خلال الأقراص المرنة. وهي طريقة تعتمدها شركة مكافي ببرنامجها الشهير أنتي فيروس او يتم ذلك مباشرة من خلال الانترنت كما في برنامج Norton .

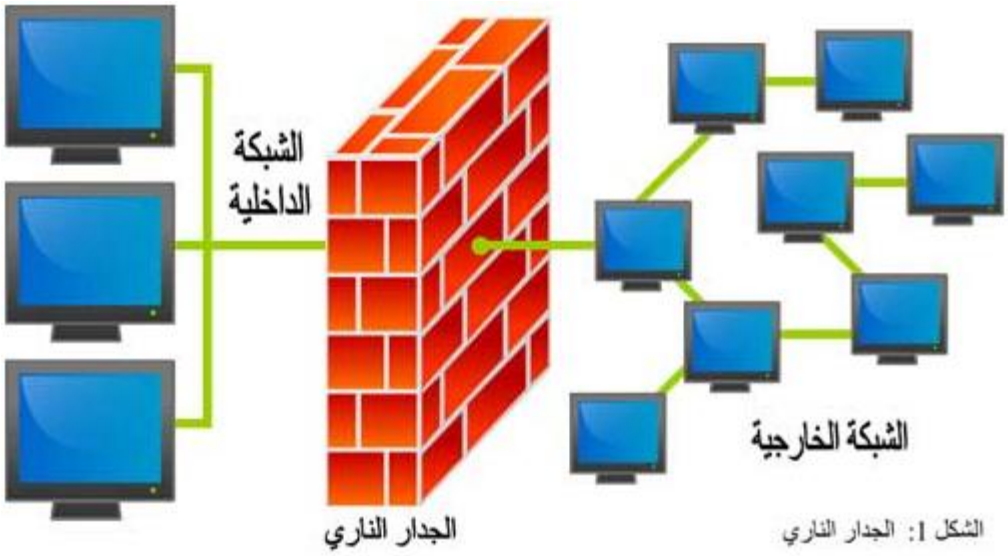
2- البحث عن وجود تسلسل محدد من الرموز التي تميز كل ملف تجسسي والتي تميز أحصنه طروادة وغيرها وهذا الملف يعرف تقنيا باسم Signature وهذه الطريقة تحدث دوريا بالطريقة التي سبق ذكرها .

3- الكشف عن التغيرات التي تطرأ على ملف التسجيل Registry وتوضيح ذلك للمستخدم لمعرفة ان كان التغيير حصل من برنامج معروف او من حصان طروادة. هذه الطريقة يتبعها برنامج Look Down الشهير.

4- مراقبة منافذ الاتصالات بالجهاز (اكثر من 65000 منفذ) لاكتشاف أي محاولة غير مسموح بها للاتصال بالجهاز المستهدف وقطع الاتصال تلقائيا وإعطاء تنبيه بذلك في حالة وجود محاولة للاختراق . هذه هي طريقة برنامج Gamer المعروف.

ما هو الجدار الناري ؟

الجدار الناري هو مجموعة من الإجراءات المتكاملة والمصممة لمنع الوصول الإلكتروني الغير معتمد (unauthorized electronic access) إلى شبكة الحاسب . وعادةً ما يكون جهاز أو مجموعة أجهزة تم إعدادها بعدد من العمليات مثل : السماح (permit) و الرفض (deny) والتشفير (encrypt) وفك التشفير (decrypt) أو أُعدت لتكون وكيل (Proxy) للتحكم في مرور البيانات بناءاً على مجموعة من القيود والمعايير.
إن الوظيفة الأساسية للجدار الناري هو تنظيم تدفق البيانات بين شبكات الحاسب المتفاوتة في مستويات الثقة ، حيث إن شبكة الإنترنت بشكل عام تعتبر معدومة الثقة (zone with no trust) فيتم ربطها بشبكة داخلية والتي هي تتمتع بمستوى عالٍ في الثقة . وعادة ما يكون بين الشبكتين منطقة تكون متوسطة الثقة وتسمى المنطقة المحايدة (Demilitarized zone (DMZ)) .



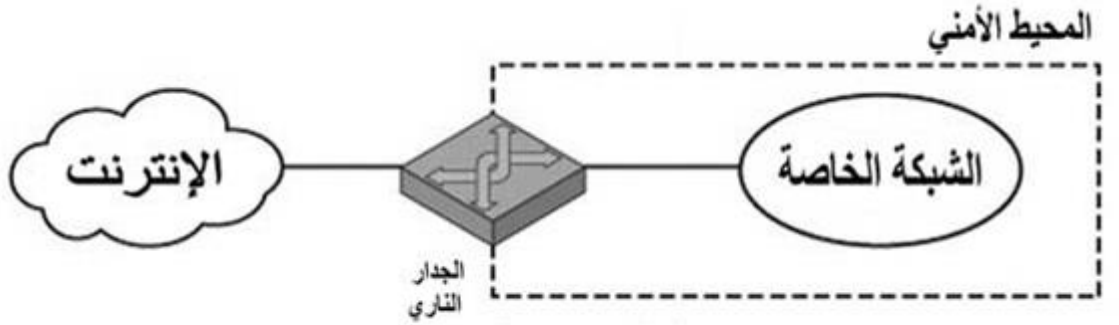
الشكل 1: الجدار الناري

: أهداف الجدار الناري

أن جميع مرور البيانات من الداخل إلى الخارج والعكس يجب أن يمر من خلال الجدار الناري ، ولن يتم تحقيق هذا الهدف إلا بوجود حاجز فيزيائي (وهو الجدار الناري Firewall) بين الشبكة الداخلية مع العالم الخارجي . يسمح فقط لمرور البيانات المصرح بها والتي تكون قد عرفت مسبقاً من خلال سياسة الأمن المحلية ، ولذلك أوجدت عدة أنواع من الجدار الناري مستخدمة الآن والتي كل منها يلبي سياسات معينة تفرضها الشركة أو المؤسسة.
بما أن الجدار الناري سيكون هو البوابة على العالم الخارجي فيجب أن يكون لديه مناعة عالية عن الإختراق ، وعادة ما يستخدم نظام تشغيل موثوق وآمن .

: أنواع الجدار الناري

أولاً : تصفية حزم البيانات(Packet filters) أو(Network Layer Firewall):



الشكل 2: تصفية حزم البيانات

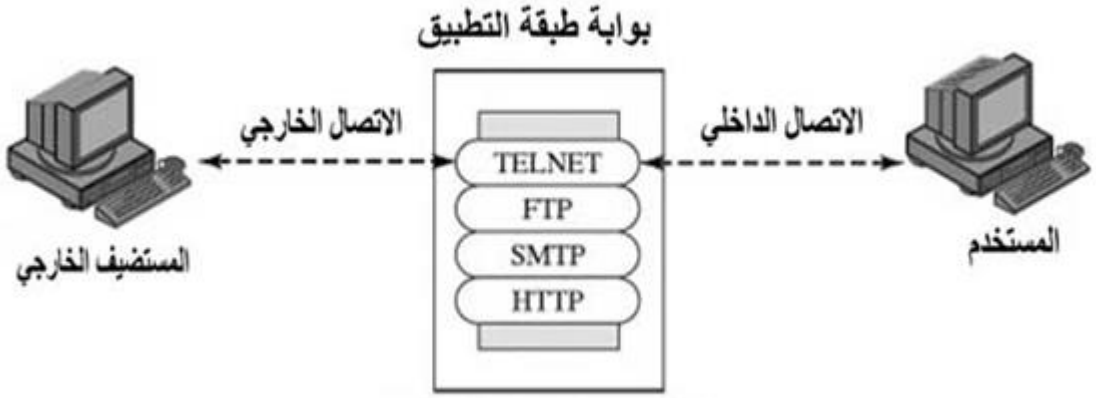
يكون عمل تصفية حزم البيانات (Packet filters) بفحص حزمة البيانات فإذا تطابقت مع مجموعة قوانين "والتي تكون عادةً مخزنة في الجدار الناري " فإنها تهمل من دون أن تعلم المرسل بذلك .
إن هذا النوع من الجدار الناري يقوم بالتصفية بناءاً على المعلومات المخزنة داخل حزمة البيانات نفسها (Packet) وغالباً ما تكون هذا المعلومات مركبة من عدة متغيرات وهي :

- عنوان المرسل (Source IP address:) .
- العنوان المرسل إليه (Destination IP address).
- نوع بروتوكل الآي بي(IP protocol field).
- عنوان المرسل والمستقبل على مستوى طبقة النقل (transport-level Source and destination address): والمقصود رقم المنفذ (port number) والتي تعرف نوع التطبيق مثل SNMP or TELNET.
- الوصلة (Interface) : وغالباً نحتاج هذا الحقل في الموجهات Routers حيث يكون لدينا العديد من وصلات RJ-45 وكذلك R232 ، ولابد من حفظ الوصلة التي ذهبت منها الحزمة والوصلة التي وصلت إليها ، ويتم التعرف على ذلك من خلال العنوان الفيزيائي MAC address لكل منهما .

إحدى الصفات الإيجابية لهذا النوع هو بساطته وسرعته ولكن هناك بعض نقاط الضعف أهمها :

- أن هذا النوع لا يفحص أعلى طبقة وهي طبقة البيانات وذلك هو غير قادر على منع الهجمات الصادرة من تلك الطبقة ، حيث لا يمكنك منع المستخدم من تنفيذ أمر معين قد تم إساءة استخدامه .
- أنه عرضة لأحدى أشهر الهجمات وهو استخدام عنوان الشبكة المزيف IP address spoofing حيث يمكن للدخيل Intruder يرسل حزمة بيانات Packet من الخارج ولكن عنوان المصدر IP Source address يحتوي على مضيف داخلي Internal host مما يجعله يستطيع المرور من خلال القوانين المكتوبة في الجدار الناري .
- بسبب قلة المتغيرات المتاحة لفرض القوانين عليها ، فإنها عرضة للتحايل وذلك باستغلال الإعدادات الخاطئة للجداري الناري . يمعنى آخر ، سهولة الوقوع في الأخطاء العرضية لدى المسئول عن الجدار الناري ،مما يساعد الدخيل Intruder على استغلال هذه الأخطاء البسيطة .

ثانياً : بوابة طبقة التطبيق ("Application Layer Gateway" ALG) وأيضاً يسمى الخادم الوكيل Proxy server:



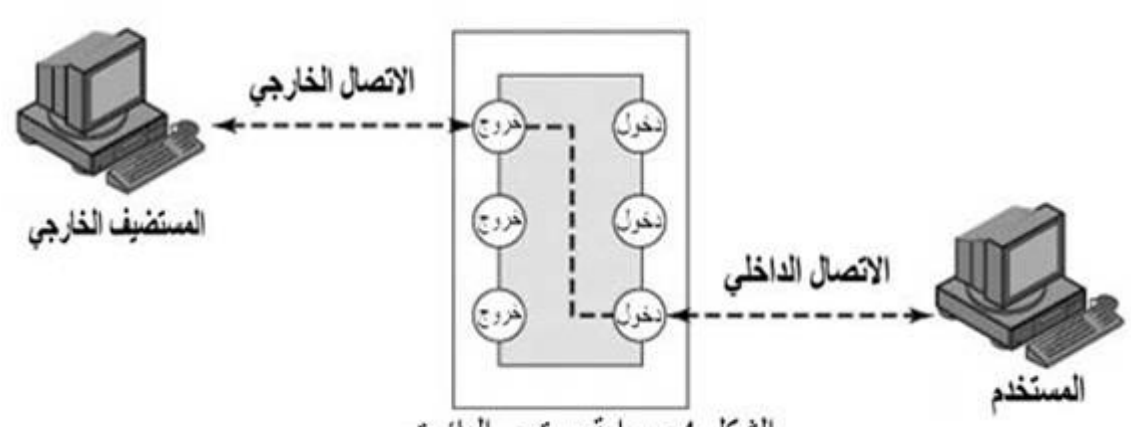
الشكل 3: بوابة طبقة التطبيق

وهو يمثل تبادل البيانات على مستوى التطبيقات (application-level) . يتصل المستخدم بالبوابة gateway باستخدام أي تطبيق من TCP/IP application مثل Telnet أو FTP . ثم تسأل البوابة gateway المستخدم عن اسم المضيف البعيد remote host ليتم الدخول عليه.
عندما يدخل المسخدم اسم صحيح ويتم التحقق منها فإن البوابة gateway تتصل مع التطبيق الموجود المضيف البعيد remote host ويتم تبادل البيانات .
الإيجابيات :

- السماح لتطبيقات العميل applications client باستخدام منافذ TCP/ UDP وقتية أو عابرة للتواصل مع منافذ معروفة known ports المستخدمة من قبل تطبيقات الخادم server applications حتى لو أن إعدادات الجدار الناري firewall-configuration فقط تسمح بعدد محدود من المنافذ . ولذلك فإن من دون وجود بوابة طبقة التطبيق ALG فإن المنافذ التي استخدمها العميل ستكون مغلقة ، وإلا فإن على مسؤول الشبكة أن يفتح عدد كبير من المنافذ مما يؤدي إلى زيادة الثغرات على الشبكة من خلال هذه المنافذ.
- ذكرنا سابقاً أن هناك أوامر في طبقة التطبيق قد يساء إستخدامها والتي لا يستطيع النوع الأول Packet filter كشفها ، ولكن هنا في هذا النوع ALG يستطيع التعرف على هذه الأوامر مما يمنح المسئول السيطرة على هذا النوع من المخاطر .
- التزامن بين فترات التعامل مع البيانات sessions بين المضيفين أثناء تبادل البيانات بينهما. ومثال ذلك : تطبيق FTP يستخدم عدة اتصالات منفصلة عن بعضها للتحكم في تمرير الأوامر لتبادل البيانات بين العميل وبين الخادم البعيد . وعندما يرسل العميل ملف كبير فإن احد تلك الإتصالات للـ FTP تكون عاطلة عن العمل وهو اتصال التحكم , control connection the. ولذلك فإن بوابة طبقة التطبيق ALG تستطيع منع هذا الإتصال من أن يحصل له انتهاء في المدة Tim out قبل أن إكتمال إرسال الملف .

أهم سلبية لهذا النوع :
بسبب المرور المتكرر في كل تطبيق على ALG فإن هذا يسبب تدهور في الأداء على عكس النوع الآخر Packet filter ميزة السرعة .

ثالثاً : بوابة مستوى الدارة (Circuit-Level Gateway :



الشكل 4: بوابة مستوى الدائرة

هذا النوع ممكن أن يكون نظام مستقل stand-alone system أو يكون على شكل دالة function تنفذ بواسطة بوابة طبقة التطبيق ALG لتطبيقات محددة .
إن هذا النوع من الجدار الناري لا يسمح باتصالات TCP والتي تكون تسمى end-to-end TCP connection؛ وبدلاً من ذلك ، فإن البوابة تبدأ باتصالين TCP :
الأول: يكون بين البوابة نفسها وبين مستخدم الـ TCP على المضيف الداخلي an inner host ، والآخر .
الثاني: بين البوابة نفسها وبين مستخدم الـ TCP على المضيف الخارجي.
عندما يؤسس الاتصالين فإنه يتم تبادل البيانات TCP segment (وهي وحدة البيانات على طبقة النقل Transport Layer) عن طريق البوابة من اتصال إلى آخر من دون فحص المحتوى . والوظيفة الأمنية في هذا النوع هي السماح أو المنع لإتصال معين .
إن الإستخدام الأمثل لهذا النوع هو في حالة أن مسئول النظام system administrator يثق بمستخدمين داخليين .
ولذلك فإنه من الممكن إعداد البوابة Gateway لأن تكون نوعين معاً:
الأول: ALG للاتصالات المتجهة للداخل inbound connections .
الثاني: circuit-level للاتصالات المتجهة للخارج outbound connections .
بهذه الطريقة، فإن البوابة تتحمل تكلفة معالجة البيانات المتجهة للداخل حتى لو تكون االبيانات أو الأوامر المطلوبة ممنوعة ، ولكن لالا تحمل تكلفة البيانات المتجهة للخارج.

Firewalls limitations : محدودية استعمال الجدار الناري :

هناك مخاطر لا يستطيع الجدار الناري منعها منها :

- أن الجدار الناري لا يمكنه حماية المخاطر الداخلية والتي تكون من مخترق موجود في داخل الشبكة وهذا المخترق قد يكون موظف ساخط عن العمل ويملك حساب خاص ومصرح له أن يعمل به فيستغله ، أو قد تكون المشكلة من خلال برنامج يكون مخفي خلال عمل تحميل برنامج آخر بواسطة الـ CD أو تحميله من الإنترنت .
- لكل جدار ناري ثغرات ولذلك يبقى ان الوضع ليس آمناً تماماً.

مفهوم التشفير

التشفير : (Encryption) هي عملية تحويل النص أو البيانات إلى شكل غير مفهوم بغرض إخفاء هذه البيانات أو هو عملية تحويل من نص صريح (Plain Text) إلى نص مشفر غير صريح(Cipher text)

مصطلح التشفير (Cryptography)هو عملية يتم فيها إخفاء المعلومات عن طريق مفتاح سري وخوارزمية.

حيث ان الشخص الذي يعلم المفتاح ويعلم خوارزمية التشفير يمكنه فك الشفرة (أي استعادة المعلومات الأصلية) ، يمكن ايضاً ان يقوم شخص لا يعرف خوارزمية التشفير ومفتاح التشفير بفك الشفرة ولكن تسمى العملية هنا عملية **غير مخولة .**

- **Plain text** النص الأصلي قبل عملية التشفير
- **Cipher text** النص المشفر بعد عملية التشفير
- **Encryption** تحويل النص العادي إلى نص مشفر
- **Decryption** فك التشفير اي تحويل النص المشفر إلى نص عادي
- **المفتاح (Key)** وهو عبارة عن كلمة السر المستخدمة في خوارزمية التشفير أو فك التشفير ويعتبر من أهم الأشياء التي يجب إخفائها حيث أنه يعتبر من الأشياء السرية التي لا يعرفها إلا المخول لهم فك الشفرة1.
- **الخوارزمية (Algorithm):** الخوارزمية هي عبارة عن الخطوات اللازمة لحل مسألة ما, و قد تكتب هذه الخوارزمية باللغة العربية أو الإنجليزيـة أو قد يعبر عنها برسم أشكال هندسيـة معينة .

أهداف التشفير:

يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كالتالي:

1. **السرية أو الخصوصية (Confidentiality):**هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.
2. **تكامل البيانات (Integrity):** وهي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.
3. **إثبات الهوية (Authentication):** وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم).
4. **عدم الجحود (Non-repudiation):** وهي خدمة تستخدم لمنع الشخص من إنكاره القيام بعمل ما، أو اثبات عمل قام به فعلاً فلا يستطيع انكاره أو التملص منه، فالتشفير يوفر الاثبات من خلال استخدامه في التوقيع الرقمي Digital Signature، والتوقيع الرقمي هو التوقيع الذي يستخدم تقنيات التشفير والذي يمتلك المفتاح العام والمفتاح الخاص والشهادة الرقمية.

إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات للأشخاص ليتم الحفاظ على أمن معلومات .

عناصر التشفير:

1- الخوارزمية .
2- مفتاح التشفير .
3- النص الاصلي .
4- نص المشفر .
5- ملاحظة :- معرفة أي ثلاثة عناصر من العناصر المذكورة سوف يؤدي إلى استنتاج العنصر الرابع.

أنواع التشفير:

أولاً: التشفير باتجاهين: :

تستخدم هذه الطريقة من التشفير عندما نكون بحاجة لاستعادة المعلومات التي قمنا بتشفيرها أي إعادتها للنص الأصل .

ويمتلك هذا النوع من التشفير خمسة أجزاء، وهي:

1. النص الصريح
2. خوارزمية التشفير
3. المفتاح السري
4. النص المشفر
5. خوارزمية فك التشفير

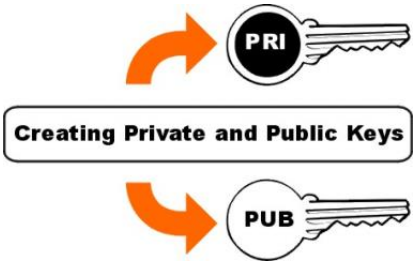
أنواع التشفير باتجاهين:

1- التشفير المتماثل: وعرف أيضاً بالتشفير بالمفتاح العام، وهو يستخدم مفتاح واحدٌلعملية التشفير وفك التشفير للبيانات. ويعتمد هذا النوع من التشفير على سرية المفتاح المستخدَم. حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل أو الملفات. من أمثلة هذا النوع: شفيرة قيصر، تشفير البيانات القياسي (DES) ، AES, IDEA, 3DES, blowfish, وهي أنظمة حديثة ومتطورة وأثبتت جدواها في عصرنا الحالي في مجال التشفير .

2- **التشفير الغير متماثل:** ويعتمد في مبدأه على وجود مفتاحين وهما المفتاح العام Public key والمفتاح الخاص Privet key، حيث أن المفتاح العام هو لتشفير الرسائل والمفتاح الخاص لفك تشفير الرسائل. ومن الأنظمة التي تستخدم هذا النوع من التشفير :
PGP, DSA, Deffie-Hellman, Elgamal, RSA

مزايا وعيوب التشفير المتماثل وغير المتماثل:

- التشفير المتماثل **أسرع** بكثير باستخدام أنظمة الكمبيوتر الحديثة، ولكنه **يستخدم مفتاح** واحد فقط. فهو **عرضة أكثر للاختراقات**.
- أما تشفير غير المتماثل فيستخدم مفتاحين في عملية التشفير وفك التشفير، وهو أقوى وأقل عرضة للاختراقات، ولكنه أبطأ من التشفير التقليدي .

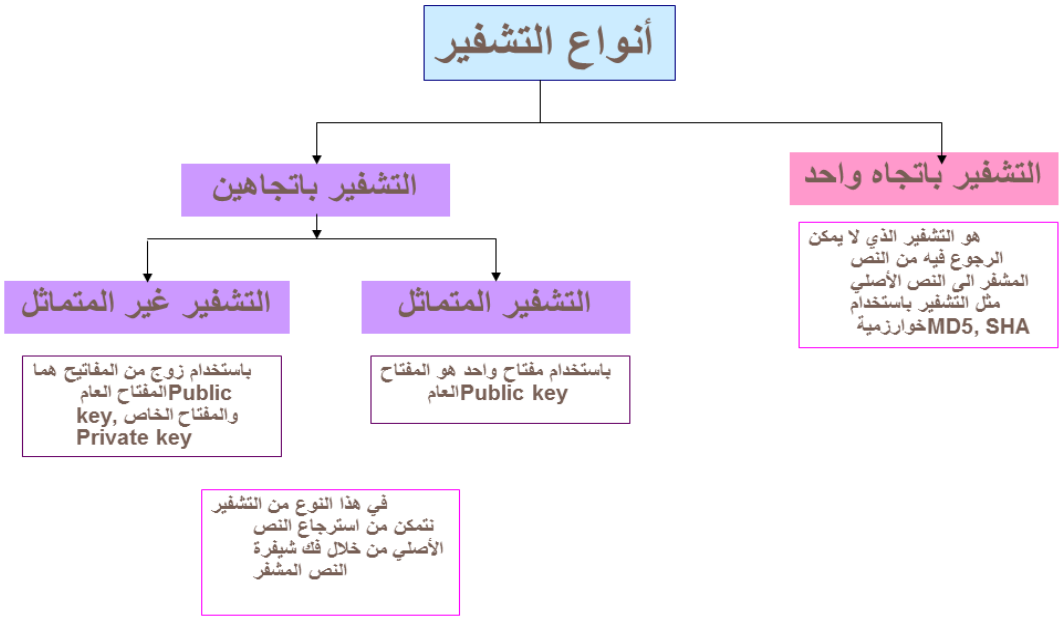


- ✓ **وتعتمد قوة التشفير في هذا النوع على عاملين أساسيين، هما:**
  - ***قوة خوارزمية التشفير***
  - ***وسرية المفتاح***

ثانياً :التشفير باتجاه واحد :

عملية يتم بموجبها تشفير المعلومات باستخدام خوارزمية التشفير ولكن لا يوجد خوارزمية فك تشفير الرسالة .

- ✓ لماذا نستخدم هذه الطريقة إن كنا غير قادرين على استعادة النص الأصلي؟
  - الجواب هو عندما لا تكون المعلومات الهامة فاننا نعمل على استرجاعها ، ولكن معرفة المعلومات مهم جدا.
- ✓ والمثال النموذجي هو السر. لا يوجد لديه كلمة مرور تستخدم.
- ✓ وفي هذا النوع من التشفير (التشفير باتجاه واحد) عادتاً يتم استخدام دالة الاختزال أو الـ **(Hash Function)** وهي عبارة عن عملية تحويل الرسالة أو البيانات إلى قيمة عددية (numeric hash value). ودالة الهاش تعتبر إما أحادية الاتجاه أو مزدوجة. فإذا كانت الدالة أحادية الاتجاه فلا تسمح للرسالة بأن تعود إلى قيمتها الأصلية، أما في حالة الدالة المزدوجة فيسمح للرسالة بأن يعاد بناءها من الهاش
- ✓ **وفي الأغلب** أكثر دالات الهاش أحادية الاتجاه أي **يستحيل فهم النص المشفر أو العودة منه للنص الأصلي**



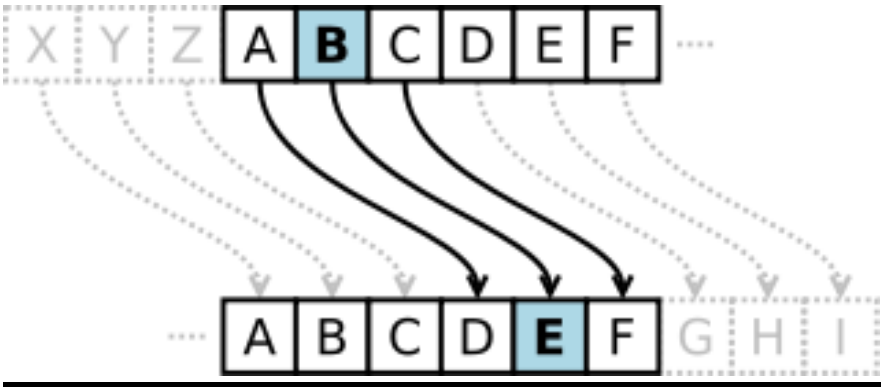
أوجه القصور في عملية التشفير:

تنقسم أوجه القصور في عملية التشفير إلى ثلاثة أنواع:

1. الأخطاء البشرية.
2. أوجه الخلل في الشفرة ذاتها.
3. عمليات الهجوم غير المنطقية.

طريقة التشفير بشيفرة قيصر (Caesar Cipher) :

- ✓ شيفرة قيصر هي من أقدم أنواع التشفير باستخدام تقنيات تبديل الحروف وأبسطها.
- ✓ يتم وفق هذه الطريقة تبديل حرف من حروف الأبجدية بالحرف الذي يقع في المرتبة الثالثة بعده، أي :
الحرف المشفر = الحرف الأصلي + 3



مثال :

النص الصريح: MR CARTER IS A COOL TEACHER

النص المشفر: PU FDUWHU LV D FRRO WHDFKHU

كيف حدث ذلك؟؟

النص الصريح:

a b c d e f g h I j k l m n o pqrstuvwxyz

النص المشفر:

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

هناك ثلاث مميزات للطريقة السابقة في التشفير، وهي:

1. خوارزميتا التشفير وفك التشفير معروفتان.
2. هناك 25 مفتاحاً محتملا فقط.
3. اللغة التي كتب فيها النص معروفة ويمكن تمييزها بسهولة.

المأخذ على خوارزمية قيصر للتشفير انها سهلة الكسر .