الفصل الثامن

الأمان والحماية

Chapter eate

Security

المقصـود بأمـــن المعلومات

أمن المعلومات يعرف من الزاوية الأكاديمية بالعلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، أما من الزاوية التقنية هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية ومن الزاوية القانونية أمن المعلومات هو محل دراسات وتدابير حماية سرية و سلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة وهوهدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات و نظمها (جرائم الكمبيوتر و الإنترنت) .

استخدام اصطلاح أمن المعلومات **Information Security** وأن كان استخداما قديما سابقا لولادة وسائل تكنولوجيا المعلومات إلا انه وجد استخدامه الشائع بل والفعلي في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال، مع شيوع الوسائل التقنية لمعالجة

وتخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات وتحديدا الإنترنت احتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات .

عناصر أمن المعلومات

إن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات سواء من الناحية التقنية أو الأدائية وهدف التدابير التشريعية في هذا الحقل ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها

- **السرية أو الموثوقية CONFIDENTIALITY** تعني التأكد من أن المعلومات ليست مكشوفة ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
- **التكاملية وسلامة المحتوى INTEGRITY** التأكد من إن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع .
- **استمرارية توفر المعلومات أو الخدمة AVAILABILITY** التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.
- **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به Nonrepudiation** يقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما هو متصل بالمعلومات أو مواقعها إنكار انه هو الذي قام بهذا التصرف بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت معين .

كيفية حماية نظام التلفونات من المخترقين و التجسس

- مراجعة فواتير الهواتف بانتظام
- الاتصال بشركات الهاتف في حالة حدوث اية مشكلة
- مراقبة فواتير الهواتف الشهرية من خلال تفقد الاتي:
  - مكالمات خارجية يتم إجراؤها.
  - زيادة مفاجئة في عدد المكالمات.
  - أي تغير في نماذج استخدام التليفون، وخاصة زيادة عدد المكالمات في أوقات توقف العمل (أثناء الليل أو عطلة نهاية الأسبوع).
  - زيادة مفاجئة في عدد المكالمات الواردة، وخاصة إغلاق الخط بدون التحدث أو غيرها من المكالمات الغريبة.
  - مكالمات يتم إجراؤها لحوالي 900 رقم هاتف، والتي يمكن أن تكون مشكلة داخلية.
  - التأخر أو الإبطاء في إجراء الاتصالات الصادرة.
  - تغيرات في نشاط بطاقة الائتمان.

استخدام كلمات المرور (Password)

على الرغم من ضرورة استخدام كلمات المرور، إلا أنها قد تشتمل على نقاط ضعف خطيرة من المفترض أن يتذكر كل مستخدم كلمة المرور الخاصة به، بالتالي فإن استخدام سلسلة من الأرقام هي أصعب كلمة مرور يمكن فكها، لأن العديد من المستخدمين لا يمكنهم تذكر أكثر من الأرقام السبعة التي يتكون منها رقم الهاتف، حتى أن البعض يواجه صعوبة في ذلك، يرى المستخدمون أن الكلمات مثل الأسماء البسيطة يكون من السهل تذكرها وذلك على العكس من الأرقام لكن الكلمات من السهل فكها.

التأمين باستخدام التشفير

على الرغم من كل الجهود التي تبذل لحماية الأنظمة، لا تتمكن نظم التأمين من منع سرقة البيانات أثناء عملية نقلها، فإذا قام أحد المخترقون بسرقة معلومات أثناء نقلها عبر الانترنت يكون بذلك قد نجح في اختراق نظام الأمان، وإذا تمكن أحدهم من المرور عبر نظام التأمين باستخدام القوة والمهارة، يجب إضافة المزيد من الأمن والحماية عن طريق تشفير المعلومات الهامة، في حالة عدم القدرة على منع الهاكرز من الحصول على البيانات، يمكن دمج الملفات بصورة محكمة حتى لا يتمكن الدخلاء من فك نظام تشفير المعلومات، يعتبر التشفير (تحويل المعلومات) من أكثر إجراءات الأمان التي يمكن الاستفادة منها، لا يجب تحويل هذه المعلومات بشدة حتى لا يتم تدميرها كليا بطريقة لا يمكن تجميعها مرة ثانية.

يمكن أن يتم تشفير البيانات قبل تخزينها على محركات الأقراص الصلبة، أو تشفيرها كجزء من عملية النقل، فعلى سبيل المثال عند القيام بكتابة رقم بطاقة الائتمان الخاصة لشراء شيء ما من شركة الانترنت تقوم الشركة غالباً بعرض رسالة اطمئنان بأن المعلومات تتم حمايتها بواسطة SSL(Secure Socket Layer)، تعتبر هذه الطبقة طريقة من طرق تشفير المعلومات قبل إرسالها عبر الانترنت، تقوم SSL بالتشفير عن طريق مفتاح خاص(Private Key) يعرف من قبل المرسل والمستقبل فقط).

إذا لم يكن أحد يختلس البيانات التي يقوم الأفراد بكتابتها، فمن أفضل وسائل الدفاع التي يمكن شنها ضد أي غزو على الخصوصيات هو استخدام فن التشفير، يجب إخفاء المعلومات الخاصة حتى لو اقتحم أي شخص محرك الأقراص الصلبة وحصل على كل الملفات فإنه لن يتمكن من قراءتها.

تشفير المعلومات يقصد به تحويلها إلى رموز غير مفهومة بحيث لا يتمكن أحد من قراءتها فيما عدا هؤلاء الذين يستطيعون فك شفرتها، كذلك يلعب التشفير دوراً بالغ الأهمية في التجارة الإلكترونية.

الاحتياطات التي يجب اتخاذها للحماية من المخترقين (الهاكرز)

1- استخدام أحدث برامج الحماية من الاختراق والفيروسات والقيام بعمل مسح دوري وشامل لجهاز الحاسوب في فترات متقاربة خاصة في حالة استخدام الانترنت بشكل يومي.

2- عدم الدخول إلى المواقع المشبوهة مثل المواقع التي تعلم التجسس والمواقع التي تحارب الحكومات لأن الهاكرز يستخدمون هذه المواقع لإدخال ملفات التجسس وإيقاع الضحايا حيث يتم تنصيب ملف التجسس(الباتش) تلقائياً في الجهاز بمجرد دخول صاحبه إلى هذا الموقع.

3- عدم فتح أي رسالة إلكترونية من مصدر مجهول لأن المخترقين يستخدمون رسائل البريد الإلكتروني لإرسال ملفات التجسس إلى الضحايا .

4- عدم استقبال أية ملفات أثناء برامج المحادثة (الشات) من أشخاص غير موثوق بهم وخاصة إذا كانت هذه الملفات تحمل امتداد (exe) أو تكون ملفات من ذوي الامتدادين gif و jpg تكون هذه الملفات عبارة عن برامج تقوم بزرع ملفات التجسس في الأجهزة المستهدفة فيستطيع المخترق بواسطتها الدخول للأجهزة وإلحاق الأذى لصاحب الجهاز.

5- عدم الاحتفاظ بأية معلومات شخصية فى داخل الجهاز كالرسائل الخاصة أو الصور الفوتوغرافية أو الملفات المهمة وغيرها من معلومات بنكية مثل أرقام الحسابات أو البطاقات الائتمانية.

6- القيام بوضع أرقام سرية على الملفات المهمة حتى لا يستطيع فتحها أي دخيل.

7- عدم التحدث الى أشخاص عبر برامج المحادثة والحذر من الإضافات الغريبة إلى البريد الإلكتروني.

8- تغيير كلمة السر بصورة دورية فهي قابلة للاختراق.

9- رفع سلك التوصيل بالإنترنت بعد الإنتهاء من استخدامها.

10- عدم القيام باستلام أي ملف وتنصيبه على القرص الصلب في الجهاز في حالة عدم التأكد من مصدره.

كيفية مواجهة الاختراق

أي شخص يكون متصلاً على الشبكة (Online) معرض للاختراق في أي وقت وبأي طريقة كانت وقد يستهدفه أحد المخترقين (الهاكرز) لسبب ما أو عشوائياً ، ربما يكون هذا المتجسس خبيراً (Expert) فيمكنه اختراق الجهاز بحيث لا يشعر به صاحب الجهاز المُخترق.

أفضل طريقة هي عدم وضع ملفات هامة وخاصة داخل جهاز الحاسوب كرقم بطاقة الائتمان أو أرقام سرية، هناك طريقة أفضل وهي استخدام جهاز خاص للاتصال بالانترنت فقط لا يحتوي على معلومات هامة، حتى لو كانت هذه الطريقة مكلفة بعض الشيء ولكن قد تقتضي للضرورة ذلك.

هناك برامج مضادة للاختراق ولكن ليست مضمونة بشكل تام، لا مانع من استخدامها حيث تفيد في التخلص من بعض المخترقين، لكن ليس الخبراء منهم.

منها البرامج المضادة للفيروسات كبرنامجي (McAfee Virus Scan Last Update) أو (Norton AntiVirus 5.0 Last Update) بحيث توفر هذه البرامج الحماية من ملفات التجسس ويعتبرانها فيروسات لذلك إذا وجد ملفات من هذا النوع تقوم هذه البرامج بتحذير صاحب الجهاز على الفور، هناك برامج أخرى مخصصة للحماية من الهاكرز فقط كبرنامج LookDown2000 أو NetBuster أو IntruderAlert'99.

الوقاية من القراصنة

الطريقة المثلى للوقاية من المخترقين والقراصنة على الإنترنت خصوصا في حالة استخدام الخط الرقمي أو ADSL السريع هي استخدام الجدران النارية الشخصية.

يعد البرنامج Tiny Personal Firewall من البرامج الناجحة في هذا الخصوص، يوفر ثلاثة مستويات من الوقاية بحيث يتم توصيف الأمان وفقاً لإرادة صاحب الجهاز.

أيضا برنامج Termi-Net هو جدار ناري، من جهة أخرى يحتاج المستخدم في كل مرة يريد فيها مراجعة بريده الالكتروني الى كلمة مرور (Password) التي بدونها لا يمكن أن الحصول على الرسائل الالكترونية، ايضاً في حالة شراء بعض السلع والحصول على الخدمات عبر الانترنت.

ان ذلك يعرض المستخدم لمخاطر القراصنة الذين قد يسرقون رقم بطاقة الائتمان الشخصية الخاصة به لاستخدامها، لهذا السبب يمكن الحفاظ على السرية والأمان في هذه الأحوال باستخدام برنامج Password 2000 حيث يقوم باختزان وحفظ كلمات المرور الخاصة، يقوم بتشفير هذه الكلمات بحيث لا يستطيع أحد فهمها، كما يمكن للبرنامج أن يعد كلمات مرور خاصة بالمستخدم صاحب الجهاز.

الوقاية من الكعكات (Cookies)

الكعكات (Cookies) هي عبارة عن ملفات لبرامج صغيرة للغاية يتم إرسالها الى جهاز الحاسوب من قبل شركات ما أثناء تصفح مواقعها على الانترنت، من المعروف أن هذه الكعكات تلتصق بالكمبيوتر

وتبدأ بإرسال معلومات الى الشركات المعنية تبين فيها طريقة المستخدم في الإبحار عبر الانترنت، الهدف من وراء ذلك الى تطوير خدماتها بحيث تلبي رغبات المستخدمين.

يمكن التخلص من الكعكات (Cookies) بواسطة برنامج Zeroclick يمنع أي نوع من الكعكات من الالتصاق بجاز المستخدم، أيضا يوجد برامج تخير المستخدم بين قبول هذه الكعكات أو رفضها منها برنامج Cookie Pal وبرنامج (شرطي الكعكات) CookieCop.

طريقة حذف ملف الباتش من الجهاز

يعتبر هذا الملف السحري بالنسبة للمخترقين، حيث يستطيع الهاكر أن يحصل على سيطرة كاملة بالجهاز المصاب بهذا الملف، منه يستطيع تغيير أو حذف أو حتى إضافة ملفات للجهاز عن طريق هذا الملف يستطيع الهاكرز أن يتحكم بالأجهزة الموجودة كفتح سواقة الاسطوانات (CDROM) أو فصل بطاقة الصوت من الجهاز.

كيفية حذف الملف

1- اختيار الأمر RUN من قائمة Start

2- كتابة هذه الكلمة في المكان المتاح REGEDIT

3- اختيار HKEY-LOCAL-MACHINE

4- بعد ذلك اختيار Software

5- ثم Microsoft

6- بعد ذلك Windows

7- ثم Current Version

8- و أخيرا Run

- مراجعة الملفات الموجودة في القائمة على اليسار و البحث عن ملف PATCH.EXE أو أي ملف تم استقباله ولم يعمل بشكل سليم وحذفه ثم إعادة تشغيل الجهاز.

الجدران النارية Firewall

الجدران النارية هي مجرد أدوات بسيطة تعمل كمنفذ للإنترنت أو كحراس على طرف الشبكة تقوم بتنظيم حركة البيانات والحفاظ على أمن الشبكة، قد ظهرت أولى الجدران النارية للشبكات في عام 1980، كانت عبارة عن موجهات تستخدم في تقسيم هذه الشبكات المصابة (الشبكات المحلية LAN) ، كانت مثل هذه الجدران النارية توضع في مواقعها هذه للحد من انتشار المشاكل التي يواجهها جزء من الشبكة المصابة للأجزاء الأخرى.

- استخدم أول الجدران النارية لتحقيق الأمن في أوائل التسعينات، كانت عبارة عن موجهات لبروتوكول IP مع قوانين فلترة.

كانت هذه الجدران النارية فعالة لكنها محدودة حيث كان من الصعب في العادة وضع قوانين فلترة للبيانات، من الصعب في بعض الأحيان تحديد أجزاء التطبيقات المراد منعها من النفاذ إلى الشبكة في أحيان أخرى كانت عناصر الشبكة مثل الموظفين العاملين ضمنها تتغير مما كان يستدعى تغيير القوانين، لذلك كان الجيل التالي من الجدران النارية أكثر قدرة وأكثر مرونة للتعديل.

الجدران النارية كانت توضع على ما يعرف بالمستضيفات الحصينة Bastion Host وأول جدار ناري من هذا النوع يستخدم الفلاتر وبوابات التطبيقات (البرمجيات الوسيطة Proxy) كان من شركة ديجيتال اكويبمنت، كان يعتمد على الجدار الناري من شركة Dec حيث أن مختبرات الشبكات التابعة لشركة Dec هي التي وضعت أول الجدران النارية التي أنتجتها الشركة، في يونيو 1991 طرحت شركة Dec في الأسواق أول الجدران النارية، خلال الشهور التي تلت ذلك ابتكر شخص يدعى ماركوس رانوم في شركة ديجيتال البرمجيات الوسيطة Proxies وأعاد كتابة جزء من الكود الخاص بالجدران النارية ليتم بعد ذلك طرح منتج Dec Seal الذي كان يتكون في بداية الأمر من نظام خارجي يدعى بحارس البوابة Gatekeeper هو النظام الوحيد الذي يمكنه مخاطبة الإنترنت، كان هناك أيضاً بوابة للفلترة ومشبك داخلي للبريد.

من هذه البدايات البسيطة دفع التنافس الحاد بين المزودين للحصول على حصة سوقية من سوق الجدران النارية المصابة المزيد من الابتكارات ليس فقط في مجال تسريع أداء الجدران النارية وتقديم خدماتها بل أيضاً في تضمينها قدرات متعددة تفوق ما كان متوفراً في تلك الأيام

تتمثل هذه القدرات بما يلي

التحقق من هوية المستخدمين

أول ما أضافه المطورون للجدران النارية الأولى كانت القدرات القوية للتحقق من الهوية إذا كانت السياسيات الأمنية التي تتبعها المؤسسة تسمح بالنفاذ إلى الشبكة من شبكة خارجية مثل الإنترنت كان لا بد من استخدام إستراتيجية ما للتحقق من هوية المستخدمين والتحقق من الهوية يعني التأكد من صحة هوية المستخدم بشكل يتجاوز مجرد التحقق من اسم المستخدم والكلمات السرية التي لا تعتبر بحد ذاتها وسيلة قوية للتحقق من هوية المستخدمين ذلك أنه على وصلة غير خاصة مثل وصلة غير مشفرة عبر الإنترنت فإن أسماء المستخدمين وكلماتهم السرية يمكن نسخها أو إعادة استخدامها Attacks Replay.

أما الأساليب القوية للتحقق من هوية المستخدمين فتستخدم أساليب التشفير مثل الشهادات الرقمية Certificates أهمية برمجيات حساب الشفرات الرقمية الخاصة بواسطة الشهادات الرقمية يمكن تفادي هجمات إعادة الاستخدام حيث يتم نسخ اسم المستخدم وكلماته السرية وإعادة استخدامها للنفاذ إلى الشبكة.

ـ الشبكات الافتراضية الخاصة

الإضافة الثانية للجدران النارية الخاصة بشبكة الانترنت هي التشفير البيني للجدران النارية Firewall to Firewall ، كان أول منتج من هذا النوع هو ans interlock هي ما تدعى اليوم بالشبكات الافتراضية الخاصة Virtual Private networks.

هذه الشبكات خاصة لأنها تستخدم التشفير وهي افتراضية لأنها تستخدم الانترنت وشبكات عامة لنقل المعلومات الخاصة، ورغم أن الشبكات الافتراضية الخاصة كانت متوفرة قبل برمجيات الجدران النارية باستخدام الموديمات لأهمية الموجهات للتشفير لكنها أصبحت تستخدم فيما بعد ضمن برمجيات الجدران النارية.

يمكن باستخدام تقنيات الشبكات الافتراضية الخاصة أن تقوم المؤسسات باستبدال مرافق الاتصالات المؤجرة وقنوات مشفرة عبر الشبكات العامة مثل الانترنت.

مراقبة المحتوى Content Screening

من خلال العامين الماضيين أصبح من الشائع استخدام الجدران النارية كأدوات لمراقبة المحتوى الوارد إلى الشبكة.

- من بعض الإضافات التي وضعت في برمجيات الجدران النارية هي البحث عن الفيروسات ومراقبة عناوين الإنترنت، منع برمجيات جافا وبرمجيات فحص ومراقبة الكلمات السرية.
- الجدران النارية الخاصة Firewall appliances

جيل جديد من الجدران النارية الذي بدأ المزودون بطرحه خلال العام الماضي وهذا الجيل يحتوي على عدد من التقنيات بما في ذلك حلول جدران نارية جاهزة turnkey، يمكن البدء باستخدامها فور الحصول عليها دون الحاجة إلى إجراء أية تعديلات خاصة على نظام التشغيل.

برامج التأمين Proxy Firewall

المعروف عن جهاز الكمبيوتر المضيف الذي يشتمل على أحد برامج التأمين الخاصة بوحدة الخدمة النائبة أنه يكون عبارة عن وحدة خدمة تشتمل على كروت شبكات ثنائية (NICs) لا تستخدم فيها إمكانيات لإرسال أو توجيه حزم بيانات بل يُكتفى باستخدام أحد برامج الخدمة التلقائية المتعلقة بوحدة الخدمة النائبة بدلاً من ذلك، لكي يتمكن كل تطبيق من تعيين مسار له عبر بوابة الاتصال هذه، يجب أن يعاد تثبيت هذا البرنامج وتشغيله ليتم تمرير التطبيق من خلاله، قد يقوم البرنامج الخاص بوحدة الخدمة النائبة مقام وحدة خدمة واحدة أو أكثر، يستخدم عادة في عمليات الاستعراض أو التأمين أو التخزين المؤقت أو جميع هذه الأغراض مجتمعة.

يستخدم مصطلح بوابة الاتصال (gateway) أحياناً كمرادف لوحدة الخدمة النائبة (Proxy) تستخدم هذه الوحدة في الأساس داخل الشركات أو المؤسسات لتجميع الطلبات الخاصة بالانترنت وإرسالها إلى وحدات الخدمة المتصلة بالانترنت وتلقي الاستجابات ثم إرسالها إلى موجه الطلب الأصلي داخل الشركة، باستخدام أحد البرامج الوسيطة الخاصة بوحدة الخدمة النائبة والذي ينوب عن المستخدم في قبول الاتصال الموجه من مستخدم ما وإتمام عملية الاتصال وحدة الخدمة المضيفة أو هذه الخدمة عن بعد.

برامج التأمين Application Proxy Gateway

عبارة عن إصدار مطوّر من برنامج التأمين Proxy Firewall، لذلك شأنه شأن هذا البرنامج يجب تثبيته وتشغيله بوحدة الخدمة النائبة مع كل تطبيق يتم إرساله إلى برنامج التأمين، الفارق الوحيد أن Application Proxy Gateway هنا يحتوي على نمطية متكاملة تقوم بفحص كل طلب والاستجابة عليه، على سبيل المثال يسمح لأي من الملفات الخاصة ببروتوكول File Transfer Protocol (FTP) بفحص البيانات داخل طبقة Application المشتملة على حزمة البرامج الخاصة ببروتوكولات الاتصال ويعمل كما لو كان عبارة عن وحدات خدمة نائبة خاصة بالمستخدمين الخارجيين، فيقوم باستقبال حزم البيانات ويرسلها إلى التطبيق التالي، لن تتاح مطلقاً الإمكانية لإنشاء اتصال فعلي ومباشر بين المستخدمين الواقعين خارج الشبكة وأي شيء فيما عدا بوابة الاتصال الخاصة بوحدة الخدمة النائبة، في الواقع إنه يقوم بفحص المعلومات المدرجة في طبقة Application لإجراء نوع من الفصل والتمييز بين المعلومات الخاصة ببروتوكول FTP والمعلومات الخاصة ببروتوكول SMTP وهكذا، لذلك يتيح هذا البرنامج قدراً جيداً من التأمين لكل تطبيق يقوم بدعمه.

حماية الانترنت من الفيروسات

النصائح المتبعة لتخفيض فرص إصابة الحاسوب بالفيروسات:

- الحصول على مضاد فيروسات: هنالك العديد من مضادات الفيروسات المعروفة يجب الحصول على واحد مناسب منها، من أمثلتها:

Norton Anti-Virus Package/MCAfee

- التحديث باستمرار: بصرف النظر عن الحل المستخدم فإنه من المهم جداً أن تبقى عملية تحديث برنامج مضاد الفيروسات مستمرة دائماً وذلك لكثرة الفيروسات التي تنشر يومياً خاصة الفيروسات الحديثة.
- الحذر من مرفقات البريد الالكتروني: على الرغم من وجود البرمجيات المضادة لفيروسات الحاسوب إلا أنه من المحتمل أن لا تكون محدثة وبالتالي فإن أحد الملفات المرفقة بالبريد الالكتروني المصابة بفيروس معين من الممكن أن تؤدي إلى ما لا يحمد عقباه.

النصائح المتبعة لتفادي الوقوع في هذه المشكلة

1. تجنب فتح المرفقات إذا كانت من شخص غريب.
2. تجنب فتح المرفقات التي تتحوي على برامج أو ماكروز (Macros) دون تفحصها لمعرفة محتوياتها حتى وإن كانت من أشخاص معروفين.
3. حماية النظام من الهجمات المفاجئة، من الممكن تقليل المخاطرة أيضاً بعدم فتح المرفقات غير المتوقعة، لكن المشكلة تكمن في كون بعض الرسائل نفسها تحوي الفيروس وليس المرفقات أو بمجرد الدخول إلى أحد مواقع الانترنت السيئة.

إرشادات كتابة كلمة السر

ارشادات لكتابة كلمة السر لرفع درجة الخصوصية والأمان:

- استخدام كلمة سر مكونة من سبعة رموز (حروف أو أرقام) على الأقل، كلما زادت فهو أفضل.
- **سهولة التذكر**: اختيار كلمة سهلة التذكر لصاحبها، صعبة التوقع على الآخرين.
- **العلامات الخاصة والأرقام**: استخدام العلامات الخاصة مثل %، $، #، وغيرها أو الأرقام ضمن كلمة السر، لا تكون كلمة السر مكونة من الحروف فقط.
- **نوع الحروف**: يمكن التنوع في استخدام الحروف الانجليزية الكبيرة والصغيرة خاصة في البرمجيات ذات الحساسية لمثل هذه الحروف.
- تجنب كتابة كلمة السر على ورقة ووضعها في المكتب، يفضل هنا تذكر كلمة السر وليس كتابتها.
- **عدم التكرار**: تجنب تكرار نفس كلمة السر في أشياء أخرى مثل رقم حساب البنك وغيرها.
- **توقيت تغيير كلمة السر**: يجب تغيير كلمة السر في الحالات الآتية:

1. إذا تم اختيار كلمة سر مخالفة للارشادات آنفة الذكر.
2. إذا استخدمت نفس كلمة السر لأكثر من ستة شهور فيجب تغييرها.
3. إذا كانت كلمة السر عرضة للوقوع في يد شخص آخر.
4. إذا استخدمت كلمة السر على حاسوب آخر.
5. إذا تم اختيار كلمة سر مغايرة لتعليمات الجهة التي يعمل لديها.

حماية الشبكات اللاسلكية

الحماية عند استخدام تقنية البلوتوث

من مساوئ استخدام الشبكات اللاسلكية سهولة اختراقها مقارنةً بالشبكات السلكية و بالتالي فإنّ إيجاد طرق لحماية المعلومات هي هاجس العلماء، حتى الآن تمكن العلماء من إيجاد طريقتين لحماية المعلومات عند استخدام البلوتوث:

1. استخدام تقنية الانتشار الطيفي الرقمي (Spectrum Technology Digital Spread) هي استخدام طيف متغير من الترددات اللاسلكية المختلفة والتي تصل إلى 1600 مرة في الثانية الواحدة بشكل عشوائي وذلك لا يمكن فهم هذه الإشارات كما أن الطريقة التي يتم فيها الاختيار العشوائي لهذه الترددات تختلف من جهاز إلى آخر ومن مستخدم إلى آخر.
2. استخدام التشفير بقوة 128 بت: تعمل على تشفير المعلومات والصوت بقوة 128 بت كذلك حماية كلمات العبور واسم المستخدم لهذه التكنولوجيا بالتشفير بنفس القوة السابقة ذكرها، بذلك يكون من الصعب جداً التنصت على المكالمات أو الدخول غير المصرح به للشبكة المتصلة باستخدام هذه التكنولوجيا، كذلك من خلال إضافة رقم سري ليتأكد من هوية المستخدم.

الحماية عند استخدام تقنية الموجات تحت الحمراء

الموجات تحت الحمراء عبارة عن اتصال نقطة–إلى–نقطة فقط، يتطلب أن يكون الجهاز الآخر في مجال رؤية الجهاز الرئيسي إضافةً إلى ذلك فإن مجال IrDA لا يتعدى المترات، لذلك فإنه حتى مع افتقار

IrDA لنظام حماية فإنها تعتبر محمية وآمنة فعلى من يريد اختراق هذه الشبكة أن يكون قريب جداً من الجهاز لأن الموجات تحت الحمراء لا تتعدى الحواجز.

سياسات الأمن والأمان العامة

مراجعة سياسات الأمن أمر ضروري فمثلاً إذا ترك موظف العمل يجب مراجعة هذه السياسات حتى لا يتمكن من الوصول إلى مصادر الشركة، كذلك فهي مهمة لتقييم النظام ومعرفة عيوبه لإصلاحها.

خطوات مراجعة سياسات الأمن الموجودة

1. مراجعة النظام الموجود: من خلال فهم هيكلية النظام وتهيئات محطات القاعدة، هذا يساعد في تحديد نقاط الضعف التي تسمح بدخول مخرب البيانات إلى النظام تتم تهيئة معظم محطات القاعدة عبر شبكة الايثرنت السلكية الأساسية وفق هذه العملية يتم إرسال كلمات السر بشكل غير مشفر، بذلك يمكن لمخرب البيانات اختراق الشبكة عن طريق مراقبة شبكة الايثرنت.
2. مقابلة المستخدمين: من خلال ذلك يمكن معرفة مقدار إدراك الموظفين لسياسات الأمن ضمن منطقة التحكم الخاصة بهم.
3. التحقق من تهيئات الأجهزة اللاسلكية: كجزء من عملية التحديد في مجال خدمة محطة القاعدة (Station range Base)، باستخدام أدوات التقاط تهيئات محطة القاعدة تهدف هذه العملية لتحديد أية آلية أمن مستخدمة فعلياً فيما إذا كانت تتوافق مع السياسات الفعالة.
4. تعريف محطات القاعدة المؤذية وإنجاز فحوصات الاختراق: تكمن مشكلة أمن الشبكة في صعوبة تحقيق التقوية والتقطيع الجيد لأمن الشبكة عند قيام موظف ما بتركيب محطة قاعدة شخصية في مكتبه، في معظم الحالات لا تتوافق هذه التركيبات مع سياسات الأمن وتقدم منفذ إدخال مفتوح غير آمن متصل مع الشبكة المتحدة باستطاعة مخرب البيانات استخدام أدوات التحري الخفية لإخبار مخربين آخرين عندما تتواجد مثل هذه الفرصة.

النصائح الأمنية المهمة عند استخدام أي شبكة لاسلكية عامةً

1. استخدام تشفير فعال: الشبكة الافتراضية تؤمن تشفير كامل للاتصالات.
2. تثبيت برنامج جدار ناري.
3. تحديد كلمات سر قوية لمحطات القاعدة.
4. تخفيض انتشار الموجات الراديوية: من الممكن عند استخدام الهوائي الموجه تقييد انتشار الموجات الراديوية ضمن منطقة العمل بحيث لا تسمح لمن خارج هذه المنطقة من التطفل على الشبكة واختراقها.

برامج مكافحة الفيروسات

أشهر وأقوى برامج مكافحة الفيروسات

Trend Micro Internet Security 17.50 Build 1366 bit64

يعرف بالبي سي سلين، من أفضل برامج مكافحة الفيروسات يتميز بوجود جدار ناري معه ومكافح لملفات التجسس، يحتوي على أداة للحماية أثناء التصفح والعديد من المميزات منها انه برنامج خفيف على الجهاز بحيث انه إذا تم تشغيل الكمبيوتر يشتغل البرنامج دون أن يدري المستخدم بذلك كما يعتبر هذا البرنامج قوي جداً بمكافحة الفيروسات ويصدر له تحديثات بشكل شبه يومي، متوافق مع جميع إصدارات الويندوز 64 bit، مرخص من قبل Trial.

Kaspersky Anti-Virus 2010 v9.0.0.735 beta

هذه النسخه تجريبيه من البرامج القوية لمكافحة الفيروسات والتي اشتهرت في الفترة الأخيرة من ميزاته وجود تحديث على مدار الساعة، كما يفحص الملفات المضغوطه، وفحص مرفقات الايميل(البريد الالكتروني) والعديد من المميزات، كما حصل على عدة جوائز، متوافق مع جميع إصدارات الويندوز مرخص من قبل Trial.

Agnitum Outpost Security Suite Pro 2009 6.7.2 bit64

برنامج قوي ومميز بحيث يقوم بحماية الحاسوب الشخصي من المخاطر من ميزاته الأمان أثناء تصفح المواقع واستخدام الانترنت،الحماية من المخترقين و من مخاطر الفيروسات والملفات الضارة الحماية من الرسائل الضارة والمزعجة، ميزة التحكم بالبرنامج بشكل بسيط ، متوافق مع ويندوز Vista bit 64 , XP Server 2003,win 2000، مرخص من قبل Trial.

Norton Internet Security 2011 18.1.0.37 Final

برنامج قوي جدا يحمي الحاسوب من الفيروسات والاختراق، يقوم بتنظيم البريد الالكتروني وحماية المستخدمين من البريد غير المرغوب به فضلا عن حماية الأطفال من المواقع الغير مرغوب فيها متوافق مع أنظمة التشغيل Vista / win 2003 / Windows XP، مرخص من قبل Trial.

AVG Anti-Virus Free 9.0.814 Build 2810

برنامج النسخة المجانية يعتبر من البرامج المشهورة للحماية من الفيروسات، من مميزاته فحص الجهاز عند بدأ التشغيل متوافق مع جميع إصدارات الويندوز، مرخص من قبل Adware.

Avast Professional Edition 4.7.871

يستخدم هذا البرنامج للحماية من الفيروسات كما يعمل على صد النوافذ والسكربتات التي قد تقوم بتحميل ملفات تضر بالجهاز، متوافق مع أنظمة التشغيل Windows NT/ Windows 2000/ Windows XP، مرخص من قبل Trial.

W32.SQLExp.Worm Removal Tool 1.03

أداة مجانية من شركة سيمانتك لحذف فيروس W32.SQLExp خاصة بالSQL SERVER يقوم بالبحث داخل الجهاز فيعمل على إيقاف sqlserver.exe ثم يظهر رسالة للتأكد من إعداد رقعة ميكروسوفت، مرخص من قبل Freewere .

Panda Antivirus Platinum7

برنامج احترافي للحماية من الفيروسات، متوافق مع جميع إصدارات الويندوز، مرخص من قبل Shareware.

ملخص برامج مكافحة الفيروسات

اسم البرنامج	الترخيص	المهام	الميزات	نظام التشغيل
Trend Micro Internet Security	Trial	مكافحة الفيروسات	وجود جدار ناري مكافح لملفات التجسس يحتوي على أداة للحماية أثناء التصفح خفيف على الجهاز	جميع إصدارات الويندوز
Kaspersky Anti-Virus	Trial	مكافحة الفيروسات	وجود تحديث على مدار الساعة فحص جميع الملفات المضغوطة و غيرها فحص مرفقات الايميل ATASHMENT	جميع إصدارات الويندوز
Agnitum Outpost Security Suite Pro	Trial	حماية الحاسوب من المخاطر الحماية من الفيروسات والملفات الضارة الحماية من الرسائل الضارة والمزعجة	الأمان أثناء تصفح مواقع الانترنت توفير الحماية من المخترقين	Vista bit 64 XP bit 64 Server 2003 Win 2000
Norton Internet Security	Trial	الحماية من الفيروسات والمخترقين الحماية من المواقع غير المرغوب فيها	تنظيم البريد الالكتروني والحماية من الرسائل غير المرغوب فيها والعناوين الغريبة	Windows XP Vista Windows 2003
Protector Plus 2007	Trial	الحماية من الفيروسات	تفحص البريد الوارد أثناء استقباله فحص الملفات أثناء تحميلها من الانترنت الحذف الفوري للملفات التي تحتوي على فيروسات جدولة المهام التي تساعد في تنظيم عملية الفحص للجهاز من الفيروسات	Windows Vista
Anti-Virus+Firewall	Trial	لإزالة الفيروسات يشكل جدار حمايه للجهاز من الاختراق	يمكن تحديثه لمدة سنتين	جميع إصدارات الويندوز
AVG Anti-Virus	Adware	الحماية من الفيروسات	فحص الجهاز عند بدأ التشغيل	جميع إصدارات الويندوز
Avast! Professional Edition 4	Trial	الحماية من الفيروسات	صد النوافذ والسكربتات التي قد تقوم بتحميل ملفات تضر بالجهاز	Windows NT Windows 2000 Windows XP
W32.SQLExp.Worm Removal Tool	Freewere	حذف فيروس W32.SQLExp	يقوم بالبحث داخل الجهاز فيعمل على إيقاف sqlserver.exe ثم يظهر رسالة للتأكد من إعداد رقعة ميكروسوفت	**Windows xp** **ME**
Panda Antivirus Platinum7	shareware	للحماية من الفيروسات	الاحتراف في مكافحة الفيروسات	جميع إصدارات الويندوز

يوجد العديد من تقنيات أمن الشبكات وحماية البيانات التي تنقل عبر الانترنت وكافة المرسلات أشهر هذه التقنيات والبرتوكولات هي:

❖ **SSH – secure shell**

هو بروتوكول مسئول عن حماية البيانات التي تنتقل عبر الشبكة عن طريق تشفيرها عند الإرسال وفك تشفيرها عند الاستقبال وهو واقع ضمن طبقة الشبكة(network protocol)، هذا البروتوكول يستخدم خوارزميات تشفير حديثة بحيث يؤمن الحماية الكاملة للبيانات عبر الشبكة له بنية (client/server) حيث يتم تنزيل برنامج (SSH server) من قبل مخدوم النظام ومن جهة أخرى يقوم المستخدم بتشغيل برنامج (SSH client) على حاسبه.

برنامج SSH شائع جدا ويأتي مع نظم التشغيل التالية: Linux distributions MacintoshOS X, Sun Solaris, OpenBSD, and virtually all other Unix-inspired operating system, Microsoft Windows، هو بروتوكول وليس منتج، يهتم بإدارة الحماية للمراسلات عبر الشبكة، يشمل التشفير والتوثيق.

يستخدم هذا البروتوكول (مثل SSL) التشفير المعتمد على المفتاح العام للتحقق من هوية المخدوم البعيد وتشفير البيانات المنقولة، كما يستبدل البنية التحتية للمفاتيح العامة PKI بمخزن مؤقت لبصمة مفتاح التشفير key fingerprint cache يتم تفقدها قبل السماح ببدء الاتصال يمكن أن يستخدم بروتوكول SSH كلمات السر، المفاتيح العامة أو غيرها من الأساليب للتحقق من هوية المستخدم، يمكن استخدام هذا البروتوكول لحماية البروتوكولات غير الآمنة من أعين المتطفلين أو هجمات المخربين عبر بناء وصلة SSH إلى موقع موثوق قريب من المخدوم البعيد، يستخدم بفاعلية من قبل مدراء الشبكات لتشفير البيانات المرسلة عبر الوصلات غير الموثوقة كالوصلات اللاسلكية بين نقطتين، يمكن لأي مستخدم تطبيق تقنية SSH بنفسه نظراً لتوفر جميع الأدوات المطلوبة مجاناً وقدرة هذه الأدوات على التعامل مع بروتوكول TCP القياسي، مما يوفر التشفير من النهاية إلى النهاية دون الحاجة إلى تدخل مدير الشبكة، يشكل برنامج Open SSH أكثر تطبيقات تقنية SSH قبولاً لأنظمة التشغيل المتوافقة مع يونيكس Unix.

استخدامات هذا البرتوكول

1- يستخدم بروتوكول SSH لتشفير البيانات المنقولة عبر أي منفذ يعمل وفق بروتوكول TCP بما فيها المنافذ المستخدمة لنقل البريد الإلكتروني.
2- يقوم SSH بضغط البيانات قبل إرسالها وبالتالي تخفيض التأخير الحاصل أثناء نقل البيانات عبر وصلات بطيئة.
3- يُستخدم من قبل مدراء الأنظمة لإدارة الخادمات الخاصة بهم على الإنترنت، لاستخدام SSH ينبغي أن يكون لدى المستخدم حساب على جهاز خادم يونيكس أو لينكس.
4- يستخدم في نقل المراسلات عبر الشبكة من خلال التحقق الأمن وتقنيات التشفير.

مزايا هذا البرتوكول

1- الدخول الآمن إلى حساب المستخدم عن بعد.
2- النقل الأمن للملفات.
3- التنفيذ الأمن للأوامر عن بعد.

❖ **SSL secure socket layer**

هو برتوكول (قوانين وقواعد تراسل بيانات) لتأمين نقل البيانات عن طريق الانترنت يضمن سرية المعلومات المرسلة عبر برتوكول HTTP (أي المرسلة عبر متصفحات الانترنت)، طور لأول مرة من قبل شركة نتسكيب لاستخدامه في إتمام العمليات التجارية على الانترنت، حيث يستخدم نظام تشفير المفتاح العام والمستخدم أيضا في الشهادات الرقمية.

يستخدم هذا البروتوكول بشكل خاص على أنظمة اليونكس له عدة برامج تعمل على تسهيل استخدامه مثل (TELNET) الهدف منه الحفاظ على ألامان والسرية بين العميل(clients) والخادم (Servers)،هو بروتوكول شائع الاستخدام .

تعتبر تقنية طبقة المنافذ الآمنة Secure Sockets Layer (SSL) أكثر تقنيات التشفير شيوعاً تعتمد هذه التقنية المستخدمة في جميع مخدومات الويب تقريباً على نظام التشفير المعتمد على المفتاح العام public key cryptography إلى جانب البنية التحتية للمفاتيح العامة public key infrastructure– PKI لحماية البيانات المنقولة عبر شبكة الإنترنت بمجرد الدخول على عنوان موقع على شبكة الإنترنت يبدأ بعبارة https يعني ذلك استخدام تقنية SSL لصفح أمن.

يحتوي الجزء المتعلق بتقنية SSL في متصفحات الويب على مجموعة من الشهادات التابعة لعدد من المصادر الموثوقة (التي تدعى بسلطات منح الشهادات certificate authorities – CA)، تضم هذه الشهادات مفاتيح التشفير العامة المستخدمة للتحقق من حقيقة مواقع الإنترنت يقوم المتصفح ومخدوم الويب، عند زيارة موقع يستخدم تقنية SSL بتبادل الشهادات يتحقق المتصفح بعد ذلك من أن الشهادة التي أرسلها إليه مخدوم الويب تتطابق مع اسم النطاق DNS المقابل لهذا الموقع وبأنها مازالت صالحة وموقعة من قبل سلطة موثوقة لمنح الشهادات، قد يتحقق مخدوم الويب أيضاً من هوية شهادة المتصفح، بعد التحقق والموافقة على الشهادات المتبادلة يتفاوض كل من المتصفح ومخدوم الويب على مفتاح تشفير أساسي لجلسة تبادل البيانات master session key، يستخدم هذا المفتاح لتشفير جميع الاتصالات إلى أن يقطع المتصفح الاتصال بمخدوم الويب، يسمى هذا النوع من تغليف البيانات بالنفق tunnel.

مجالات استخدام تقنية SSL

- تستخدم تقنية SSL في التصفح الآمن لمواقع الويب.
- تستخدم لحماية بروتوكولات البريد الإلكتروني غير الآمنة مثل (IMAP، POP وSMTP) عبر تغليفها ضمن SSL.
- تدعم غالبية برامج البريد الإلكتروني الحديثة بروتوكولات IMAPS وPOPS الآمنة.
- حماية بروتوكول SMTP باستخدام تقنيات SSL/TLS.

- حماية مخدوم البريد الإلكتروني (إذا كان غير قادر على دعم تقنية SSL).
- استخدام تقنية SSL عملياً لحماية أي خدمة تعتمد على بروتوكول TCP.

كيف يعمل برتوكول SSL

عوضاً عن استخدام برتوكول HTTP يقوم بروتوكول SSL بإنشاء طبقة إرسال خاصة بالتالي يستطيع النظام العمل مع جميع بروتوكولات الانترنت بما في ذلك HTTP و FTPو Telnet يعمل بروتوكول SSLمن خلال تأسيس قناة اتصال آمنة ومنفصلة لكافة الرسائل التي تستخدم بروتوكولHTTP ، يتم إعداد هذه القناة الآمنة على المخدوم والمتصفح بواسطة برمجيات SSL الخاصة.

استخدام المتصفحات لبرتوكول SSL

تستخدم المتصفحات بروتوكولSSL أو Secure Socket Layer لتشفير المعلومات التي تنتقل بين المتصفح ومخدوم الويب، يستخدم بروتوكول SSL في عمليات التسوق الإلكتروني وتبادل المعلومات الحساسة، عند ظهور مفتاح أو قفل في أسفل شاشة المتصفح يعني ذلك أن المتصفح قد أمن الاتصال الأمن والمشفر مع المخدوم مما يؤمن إرسال المعطيات والمعلومات.

يعد هذا البرتوكول المقياس الثاني للمعاملات الآمنة والحوارات التي تستخدم بروتوكول Secure HTTP الأمني لذلك يوضع في كل مخدومات الويب التي تقوم بتخديم زبائن التجارة الإلكترونية.

لماذا يتم اقتناء برتوكول SSL

تستخدم مواقع التجارة الالكترونية ومواقع الحكومات ومواقع البنوك برتوكول SSL لقدرته في نقل البيانات بشكل آمن مما يمنحه قوة.

الأسباب التي تميز برتوكول SSL وذلك يعود لطبيعة شبكة الانترنت

- طبيعة شبكة الانترنت غير الآمنة.
- طبيعة الشبكات الموصلة ومدى حجم الأمان التي تقدمه أو الحفاظ على سرية البيانات.
- استحالة تغيير البيانات كما نعلم أن من أسس أمن المعلومات هو وصول البيانات بشكل صحيح دون تغيير عند حصول الاختراق بالإمكان تغيير محتوى الطلب بدلا من 100 على سبيل المثال إلى 100000 من خلال عملية التشفير تمنع المخترق من تغيير البيانات عن طريق تشفيرها واستحالة فك التشفير.
- استحالة قراءة البيانات.

عيوب برتوكول SSL

- نحتاج في كل طلب التأكد من شهادة الموثوقية والقيام بعملية فك التشفير ، مما يسبب ضغط على الخادم، نتيجة للقيام بعملية أخذ نسخة من التحميل (LOAD)، مما يسبب من ارتفاع حجم الاستهلاك في CPU.
- أن عملية الاحتفاظ بالمفاتيح في كل مرة يستهلك الذاكرة العشوائية بشكل كبير.

- بسبب الحاجة للقيام بعملية فك التشفير والتأكد، فإن هيكلية وطاقة الأجهزة الصغيرة مثل أو الجوالات لا تحتمل القيام بتلك العمليات بشكل مستمر.

استخدامات هذا البرتوكول

يستخدم في تشفير وحماية قنوات الاتصال التي تنقل عبرها البيانات.

المهام التي يقوم بها

1- التحقق من النظام: يتم ذلك عن طريق استخدام تقنيات معيارية للتشفير بالمفتاح العام، حيث يتم التحقق من الشهادة الرقمية للنظام فيما إذا كانت صالحة وصادرة من جهة موثوقة بالنسبة للزبون ويتم التحقق من المفتاح العام المرتبط معها وتعد هذه العملية ذات أهمية كبرى للمستخدم حيث يحتاج ضمان عدم اختراق النظام.

2- التحقق من هوية الزبون: في هذه الحالة يتم التحقق من هوية الزبون من قبل النظام، ذلك بإتباع نفس الخطوات عند التحقق من هوية النظام لدى المستخدم.

3- الاتصال المشفر: يقوم برتوكول ssl ببناء اتصال مشفر بين الطرفين، مما يمنح سرية عالية للاتصال بحيث يضمن عدم اطلاع طرف ثالث على المعلومات المرسلة.

❖ IPSec: IP security

هو مجموعة معاير من البرتوكولات والخوارزميات طورت بواسطة لجنة خاصة لنظام الانترنت (IETF-internment engineering task force) واعتمدت كمعاير للانترنت للتحقق من سلامة وسرية المعلومات التي أرسلت عبر شبكات IP، يعتبر تقنية توفر الموثوقية والصحة والتشفير لكل شيء يمر من خلالها على مستوى IPPacket.

الفائدة الكبرى التي ظهرت في IPSec هي أنه يوفر حماية كاملة وواضحة لجميع البروتوكولات التي تعمل على الطبقة الثالثة Layer 3 of the OSI Model وما بعدها.

كيف يحمي IPSec من الهجوم على الشبكة

إن الشبكة والبيانات التي تمر فيها يمكن أن تتعرض للعديد من أنواع الهجمات المختلفة، بعض الهجمات تكون غير فعاله Passive مثل مراقبة الشبكة Network Monitoring، منها ما هو الفعال Active مما يعني أنها يمكن أن تتغير البيانات أو تسرق في طريقها عبر أسلاك الشبكة.

بعض أنواع الهجمات على الشبكات

أو لاً: التقاط حزم البيانات Eavesdropping, sniffing snooping: حيث يتم بذلك مراقبة حزم البيانات التي تمر على الشبكة بنصها الواضح دون تشفير Plain text والتقاط ما نريد منها ويعالجها IPSec عن طريق تشفير حزمة البيانات، عندها حتى لو التقطت الحزمة فإن الفاعل لن

يستطيع قراءتها أو العبث بها، لأن الطرف الوحيد الذي يملك مفتاح فك التشفير هو الطرف المستقبل.

ثانيا: تعديل البيانات Data modification: حيث يتم بذلك سرقة حزم البيانات من الشبكة ثم تعديلها وإعادة إرسالها إلى المستقبل، ويقوم IPSec بمنع ذلك.

ثالثاً: Service DoS –Denial of رفض الخدمة أو حجبها: حيث تعمل هذه الهجمة على تعطيل خدمة من خدمات الشبكة للمستخدمين والمستفيدين منها، مثلاً كإشغال السيرفر في الشبكة بعمل عليه Flood مما يشغله بالرد على هذه الأمور وعدم الاستجابة للمستخدمين، ويعمل IPSec على منع ذلك عن طريق إمكانية غلقه أو وضع قواعد للمنافذ المفتوحة Ports.

رابعاً: الهجمات على طبقة التطبيقات Application Layer Attacks : حيث تعمل هذه الهجمات على التأثير على النظام المستخدم في أجهزة الشبكة وأيضاً تعمل على التأثير على البرامج المستخدمة في الشبكة، من الأمثلة عليها الفيروسات التي تنتشر بفعل ثغرات في الأنظمة أو البرامج أو حتى أخطاء المستخدمين، يعمل IPSec على الحماية من ذلك بكونه يعمل على طبقة IP Layer فيعمل على إسقاط أي حزمة بيانات لا تتطابق مع الشروط الموضوعة لذلك تعمل الفلاتر على إسقاطها وعدم إيصالها للأنظمة أو البرامج.

مزايا برتوكول IPSEC

- يوفر حماية كاملة وواضحة.
- موجود ضمن IP packet لذلك لا يحتاج لأجهزة إضافية لانتقاله عبر الشبكة.

ينقسم هذا البرتوكول إلى ثلاث برتوكولات

1- AH:Authentication Header

يحافظ على موثوقية البيانات المرسلة من المستخدم والتأكد من صحة البيانات المرسلة أي انه لم يتم إجراء أي تعديل عليها أثناء إرسالها ، ضمان عدم إعادة الإرسال البيانات المشفرة إلى الخادم(السرفير) من قبل المخترقون بعد قيامهم بسرقة (كلمة المرور).

2-ESP:Encapsulating Payload

يوفر تشفير البيانات ويحافظ على سريتها.

مزايا هذا البرتوكول

1- تشفير البيانات لحمايتها من التعديل والتغير.

2- ضمان عدم إعادة إرسال البيانات.

3-IKE:Internet Key exchange

الوظيفة الأساسية لهذا البرتوكول توزيع المفاتيح الخاصة بين المستخدمين.

إخفاء البيانات Cryptography

علم التشفير أو الكتابة المشفرة المسماة بال (Cryptography)هو فن أو علم إخفاء المعلومات بحيث تكون بأمان عند إرسالها أو تخزينها، ويعتبر مجال ذو أهمية كبيرة للحكومات، والشركات الخاصة.

علم التشفير وعلم الإخفاء هما طريقتان لحماية المعلومات من عرضها والعبث بها من قبل الأشخاص الغير المخول لهم، لكن لو استخدمت إحداهما دون الأخرى قد لا تعتبر وسيلة حماية كافية وكاملة بالنسبة لإخفاء المعلومات حالما يكتشف أو يشك أحد المهاجمين بوجود معلومات مخفية في مكان ما فإن الهدف من عملية الإخفاء يصبح بلا جدوى، لزيادة حماية المعلومات المخفية يجب علينا استخدام التشفير والإخفاء معاً.

بالرغم من الأهمية الكبيرة والفوائد الجليلة التي يقدمها هذا العلم إلا أن انتشاره حتى هذه اللحظة لا يقارن بانتشار علم التشفير، أصبحت الكتابة المشفرة إحدى الأدوات الرئيسية لضمان السرية والثقة والتحكم في دخول المستخدمين والتسديد الإلكتروني وأمن الشركات، أصبح متوفراً لكل فرد يريد استخدامه.

أقسام إخفاء البيانات

1. الكتابة المشفرة الطبيعية (Physical Cryptography)

تتضمن الكتابة المشفَرة الطبيعية أنواع مختلفة من الطرق، الطرق الأكثر شيوعاً تستخدم الإحلال أو تبديل الحروف أو الكلمات، من الطرق الطبيعية أيضاً طريقة التشفير المسماة بفن الاختزال (Steganography) ، هي لإخفاء المعلومات ضمن معلوماتِ أخرى، كصورة، تشير الكتابة المشفرة الطبيعية إلى أي طريقة لا تعدّل القيمة باستعمال عملية رياضية.

2. الكتابة المشفرة الرياضية (Mathematical Cryptography)

تتعامل الكتابة المشفرة الرياضية مع القضايا المتعلقة باستعمال العمليات الرياضية على الحروف أو الرسالةِ، الأكثر شيوعاً هي دالة تسمى الهاش (Hashing)، هي عبارة عن عملية حسابية تتم على الرسالة وتحولها إلى قيمة عددية (numeric hash value).

كما هو ملحوظ هذه قيمة عددية (numeric hash value) وهي عدد وحيد، لا يمكن أن تستعمل لاشتقاق معنى الرسالة، هذا العددِ يمكن أن يرسل بالرسالة إلى المستلم. الطَرف الآخر يمكن أن يستعمل نفس دالة الهاش لتقرير أن الرسالةِ موثوق بها، إذا اختلفت قيمةِ الهاش فهذا يدل على أن الرسالة عُدّلت بطريقةٍ ما.

مجالات استخدام هذه التقنية

- التجارة الإلكترونية
- العلامات المائية (Watermarks) التي تستخدم في عمليات حفظ الحقوق للمنتجات الرقمية، والحد من عمليات القرصنة.

بالرغم من أن المشتري أو مستخدم هذه البرامج قد يعلم بوجود مثل هذه العلامات إلا أن اكتشاف أماكنها داخل البرنامج قد يكون صعب، على افتراض أن المستخدم قد تعرف على مكان وجود هذه العلامة سيظهر أمامه تحدٍ آخر هو معرفة البرنامج المستخدم في الإخفاء وكلمة السر ومفتاح التشفير، كلا من هذه الأشياء قد يستغرق اكتشافه وقتاً زمنياً طويلاً.

خوارزميات إخفاء البيانات

1.الهاش (Hashing)

عبارة عن عملية تحويل الرسالة أو البيانات إلى قيمة عددية (numeric hash value)

دالة الهاش تعتبر إما أحادية الاتجاه أو مزدوجة، فإذا كانت الدالة أحادية الاتجاه فلا يسمح للرسالة بالعودة إلى قيمتها الأصلية، أما في حالة الدالة المزدوجة فيسمح للرسالة بأن يعاد بناءها من الهاش، أكثر دالات الهاش أحادية الاتجاه.

2. التشفير المتناظر (Symmetric Algorithms)

يتم بتشفير الرسالة أو المعلومات باستخدام رقم واحد يسمى الرقم العام وكذلك في نفس الوقت يتم فك الشفرة وترجمة المعلومات إلى وضعها الأصلي باستخدام نفس الرقم العام، لذلك لو حصل أن شخص أخر يعرف هذا الرقم أو حصل عليه من الدليل العام فإنه يكون قادر على فك الشفرة وقراءة تلك الرسالة أو المعلومة.

3. التشفير الغير متناظر (Asymmetric Algorithms)

يتم تشفير المعلومات بالرقم العام ولكن لا يمكن فك الشفرة والوصول إلى تلك المعلومات إلا بالمفتاح الخاص لصاحب ذلك المفتاح العام الذي تم على أساسه عملية التشفير.

فوائد هذا البرتوكول

1- التحقق من هوية المستخدم.
2- السرية: ضمان وصولها إلى الشخص المعني فقط.
3- ضمان عدم دخول أشخاص غير مخول لهم للأنظمة التي تستخدم التشفير.

أساليب الإخفاء

تتمحور فكرة الإخفاء في إدخال الرسالة داخل غطاء لتكوين الهدف المخفي ويمكن تمثلية بالمعادلة التالية:

الهدف المخفي= الرسالة المراد إخفاءها + مفتاح الغطاء

وبشكل عام تقسم أساليب الإخفاء إلى أربعة أساليب أساسية:

1- **الإخفاء النصي:** يكون ذلك بكتابة نص يمكن استخلاص الرسالة المخفية منه ، أما بطريقة نصيه بان يكون أو ل حرف من كل كلمة يمثل حرف من الرسالة المخفاة، أو بطريقة نحوية أو لفظية

2- **الإخفاء الصوري:** وذلك عن طريق إخفاء الرسالة المراد إرسالها تحت ملف صوري، يعد هذا النوع من الإخفاء من أكثر الأنواع شوعيا في الاستخدام لما تتميز به الصور من صفات تجعلها الوسط المثالي للإخفاء. .

3- **الإخفاء الفيديوي:** مشتق من الإخفاء بالصور حيث أن مقاطع الفيديوليست إلا مجموعة من الصور المتتالية . لذلك فإننا نستطيع تطبيق أساليب الإخفاء.

4- **الإخفاء الصوتي:** ويتم في هذه الطريقة إخفاء الرسالة المراد إرسالها داخل إشارة صوتية ممكن أن تكون في مجال الزمن أو مجال الطيف.

أما التشفيرencryption الذي يعد من طرق حماية البيانات : هو عملية تحويل المعلومات إلى شيفرات غير مفهومة ، وذلك لمنع أشخاص غير مرخص لهم من الاطلاع على المعلومات أو فهما.[29]

الفرق بين إخفاء المعلومات والتشفير

وجه المقارنة	علم التشفير	علم الإخفاء
العلم بوجود الرسالة	يعلم	لا يعلم
الاتصال	يمنع الأطراف الأخرى من معرفة محتوى الاتصال	يمنع الآخرين من معرفة وجود الاتصال
الانتشار	شائع	غير شائع

❖ المفتاح الخاص والعامprivate & public key

هي لخوارزمية التي تطبق على النص بحيث تغير من شكل البيانات، يستخدم المفتاح العام للتشفير، والمفتاح الخاص لفك التشفير.

المفتاح الخاص:

المفتاح الذي يحتفظ به في مكان امن وسري للغاية بدونه لا يمكن فك تشفير أي رسالة ،هو مفتاح شخصي غير معروف إلا للشخص الذي يملكه، يستخدم لحل التشفير للرسائل المشفرة بواسطة المفتاح العام .

المفتاح العام:

المفتاح الذي يتم نشره بشكل واسع ليتمكن آخرون من تشفير رسائل لا يمكن إلا لصاحب المفتاح العام أن يفك تشفيرها بواسطة مفتاحه الخاص.

يقصد بالمفتاح العام: أي أنه مفتاح الشيفرة يكون معلنا للجميع وينشر على الملأ، فلا يجب أن يكون سريا لأنه يستخدم في عملية التشفير فقط، لا فائدة منه في عملية فك الشفرة، إذ يستخدم مفتاح خاص وسري في عملية فك التشفير، معنى ذلك أننا نستخدم مفتاحان في هذا النوع من التشفير على عكس أنواع التشفير السائدة والتي تستخدم مفتاحا سريا واحدا، إلا انه يمكن استخدام المفتاحين بطريقة معكوسة تماما وبالتالي تحقيق وتطبيق ما يعرف بالتوقيع الرقمي (Digital Signature)

توفر الشهادات الرقمية والتي تستخدم تشفير المفتاح العام (Public-Key Cryptography) طريقة لتجاوز أحد أهم عقبات التجارة الإلكترونية، هي تحقيق الثقة بين أولئك المتصفحين الذين قد تفصل بينهم محيطات وقارات، بالإضافة إلى تحقيق القدرة على تراسل البيانات بسرية أيضا، فحققت بالتالي أهم الشروط المطلوبة في التجارة الإلكترونية الثقة والسرية.

يتم تشفير المفتاح العامPublic Key باستخدام مفتاحين لكل طرف المفتاح العام والمفتاح الخاص، أما تشفير المفتاح السريSecret Key يتم باستخدام مفتاح واحد للطرفين يحفظ بسرية تامة بين الطرفين.

أقسام التشفير الرئيسية (نظم التشفير)

أو لا : - نظام المفتاح المتماثل (المفتاح الخاص) Symmetric key cryptography

يعتمد هذا النظام على استخدام مفتاح متماثل يتم به التشفير والحل وفقاً للخطوات التالية :

1. يتم تشفير الرسالة (المعاملة) لدى المرسل باستخدام مفتاح خاص .
2. يقوم المرسل بإرسال الرسالة المشفرة إلى المستقبل باستخدام وسائل الاتصال العادية .
3. يقوم المرسل بإرسال المفتاح باستخدام وسيلة مؤقتة إلى المستقبل منفصلاً عن الرسالة .
4. يقوم المستقبل بعد استقبال الرسالة المشفرة والحصول على المفتاح بحل الشفرة والحصول على الرسالة الأصلية.

عيوب المفتاح السري

- الحاجة إلى تبادل المفاتيح بطريقة آمنة.
- هذا غير متحقق على الانترنت.

ميزات المفتاح السري

- سرعة التشفير وفك التشفير مقارنة بالأنظمة الأخرى.
- مقارنة بالمفتاح العام فإن المفتاح المتماثل أسرع بكثير هذا الفرق غير متأثر بسرعة الحاسبات.

– طبقاً لذلك فإن هذا النظام لا يتطلب إرسال المفتاح حيث أن صاحب هذا المفتاح يحتفظ بمفتاحه الخاص، أما المفتاح العام متاح لأي مستخدم لأنه لا يمثل أي خطورة.

خطوات عملية التشفير بواسطة المفتاح العام

1. يرغب المرسل في إرسال رسالة مشفرة إلى المستقبل فيقوم باستخدام المفتاح العام للمستقبل وتشفير الرسالة .
2. يقوم المرسل بإرسال الرسالة المشفرة باستخدام القنوات العادية في الاتصال .
3. يقوم المستقبل (المرسل إليه) بتلقي الرسالة، باستخدام مفتاحه الخاص يمكنه أن يقوم بحل الشيفرة والحصول على الرسالة الأصلية.

مزايا التشفير بالمفتاح العام

ضمان درجة عالية من الأمن للمعلومات أو المعاملات التي يتم تشفيرها بهذه الطريقة .

عيوب المفتاح العام

– طول الوقت اللازم للتشفير وحل الشيفرة .
– عملية التحقق من صاحب المفتاح العام والتأكد من عدم انتحاله من قبل شخص أخر.
– صعوبة السيطرة والرقابة على المفاتيح العامة، ذلك لوجود عدد كبير منها قد يصل إلى ألاف المفاتيح العامة بالتالي يصبح من الصعب إدارتها وصيانتها.

خطوات التشفير بطريقة المزج بين المفتاح العام والمفتاح الخاص

1– تشفير الرسالة الأصلية بمفتاح متماثل (الطريقة الأولى) .
2– تشفير المفتاح المتماثل (الخاص) بالمفتاح العام للمرسل إليه (المستقبل) .
3– يتم إرسال الرسالة المشفرة بالمفتاح المتماثل والمفتاح المتماثل المشفر، بالمفتاح العام للمرسل إليه باستخدام أي شبكة اتصالات .
4– يستقبل المرسل إليه المفتاح المتماثل المشفر بالمفتاح العام ويقوم بحل شفرة هذا المفتاح باستخدام المفتاح الخاص به ليحصل على المفتاح المتماثل المشفر بها الرسالة الأصلية.
5– يقوم باستخدام المفتاح المتماثل بعد فك تشفيره في فك الرسالة الأصلية المشفرة ليحصل على الرسالة الأصلية.

نظام حماية المفتاح السري بالمفتاح العام

لحل مشكلة البطء في تشفير المفتاح العام، تصميم نظام يجمع بين حسنات التشفير بالمفتاح السري وحسنات التشفير العام يتمثل في الخطوات التالية:

• يقوم المرسل بإنتاج المفتاح السري ثم يستخدمه في تشفير الرسالة المراد إرسالها.

• يقوم المرسل بعد ذلك بتشفير المفتاح السري باستخدام المفتاح العام للمستقبل ويرفق الناتج مع الرسالة ويقوم بإرسالها.
• عند استقبال المستقبل للرسالة يستخدم مفتاحه الخاص لاستخراج المفتاح السري.
• بعد استخراج المفتاح السري يستخدمه لفك الرسالة الأصلية.[32]

مقارنة بين بعض التقنيات المستخدمة في أمن الشبكات

وجه المقارنة	برتوكول SSH	برتوكول SSL	برتوكول IPSEC	إخفاء البيانات Cryptography	المفتاح العام والخاص Public and private key
الانتشار والتوسع	شائع جداً (منتشر على نطاق واسع)	شائع الاستخدام (انتشار بشكل واسع)	منشر بشكل واسع	غير منتشر بشكل واسع	محدود الانتشار
القدرة والتحمل	قوي	معتدل	قوي	قوي	قوي
التحميل الزائد	عالي	ضعيف	عالي	عالي	ضعيف
التعقيد	بسيط وسهل (واضح)	معتدل	معقد جدا	معتدل	معقد جداً

النتائج

بعد عقد المقارنة بين تقنيات وبرتوكولات أمن حماية البيانات نرى أن

- برتوكولات SSL – SSH – IPSEC الأوسع انتشاراً
- تقنية إخفاء البيانات وبرتوكولات SSH, IPSec: الأفضل من ناحية القدرة والتحمل
- تقنية إخفاء البيانات وبرتوكولات IPSec , SSH الأفضل من ناحية التحميل الزائد
- IPSec والمفتاح الخاص والعام الأكثر تعقيدا

الأفضل بين هذه التقنيات برتوكول IPSec لأنها الأكثر تعقيدا لأنها تؤمن الحماية والأمان وبالتالي يكون صعب اختراقها أو التسلسل إليها من قبل المتطفلين(الهاكرز) بالإضافة لأنها أكثر قدرة على التحمل والتحميل العالي للبيانات.

التوصيات

تطوير هذه التقنيات لضمان حماية البيانات بشكل كامل وان تكون ذات قدرات تحميل عالية بحيث تضمن السرية والموثوقية.