المحاضرة السابعة و الثامنة و التاسعة

مادة علم الحاسوب#

- عناصر أمن المعلومات #
- وسائل تحقيق أمن المعلومات
- أمن الحاسبات و البرمجيات والملفات

امن المعلومات
عناصر أمن المعلومات

أعداد

د.قيس سلطان

التعريف بأمن المعلومات

1- مفهوم أمن المعلومات

* يعني أمن المعلومات إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر دون إذن منك، وان تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصة.
* (منع وصول الأفراد الغير مصرح لهم – منع تعديل البيانات – منع أخذ المعلومات – حماية المصادر وذلك بعرقلة الهجمات)

التعريف بأمن المعلومات

إنّ علم أمن المعلومات هو العلم الذي يُعنى بحماية المعلومات من المخاطر التي قد تتعرّض لها. ويمكن تعريف أمن المعلومات بشكل مختصر بأنه: «حماية المعلومات من الوصول غير المسموح به». ويمكن تعريفه بتفصيل أكثر بأنه: «المفاهيم والتقنيات والتدابير التقنية والإداريّة المستخدمة لحماية أصول المعلومات من الوصول غير المأذون به عمدًا أو سهوًا أو حيازتها أو الإضرار بها، أو كشفها، أو التلاعب بها، أو تعديلها، أو فقدها أو إساءة استخدامها»[١]. تعرّف لجنة أنظمة الأمن القومي الأمريكية(Committee on National Security Systems-CNSS)[٢] أمن المعلومات بأنه: «حماية المعلومات وعناصرها المهمة(الحرجة) بما في ذلك الأنظمة والأجهزة التي تَستخدِم هذه المعلومات وتخزنها وترسلها»[٣]. ويُعدُّ هذا التعريف هو

المحاور الاساسية التي يشملها امن المعلومات

- حماية المعلومات من الضرر بأشكاله كافة، سواءً أكان مصدره أشخاص(كالمخترقين)، أم برامج(كفيروسات الحاسب الآلي)، وسواءً أكان متعمّدًا أم عن طريق الخطأ.
- حماية المعلومات من الوصول غير المصرّح به، أو السرقة، أو الالتقاط، أو التغيير، أو إعادة التوجيه، أو سوء الاستخدام.
- حماية قدرة المنشأة على الاستمرار وأداء أعمالها على أحسن وجه.
- تمكين أنظمة تقنيّة المعلومات والبرامج التطبيقيّة لدى المنشأة من العمل بشكل آمن.

الحاجة لأمن المعلومات

١. حماية الأصول المعلوماتيّة الحرجة:

ومن الأمثلة على الأصول المعلوماتيّة الحرجة ما يلي:

- مراكز البيانات(Data Centers).
- قواعد البيانات(Databases).
- أجهزة الخوادم الرئيسة(Severs).
- شبكات المعلومات المحلية(LAN) والواسعة(WAN).
- أنظمة التشغيل(Operating Systems).
- البرامج التطبيقيّة(Application Programs).
- أجهزة تخزين المعلومات(Storage Devices).
- المواقع والبوابات الإلكترونيّة سواءً داخلية أو على شبكة الإنترنت.

الحاجة لأمن المعلومات

٢. حاجة أعمال المنشآت وأنشطتها إلى ذلك: حيث أصبحت المعلومات تشكّل ثروة حقيقيّة للمنشآت ومورداً مهمًّا من مواردها، بل إنّ المعلومات في بعض المنشآت هي مصدر الدّخل الأول لها، ويقوم عليها نشاط المنشأة الأساسي، والتجارة الإلكترونيّة خير مثال لذلك.

٣. حاجة المستفيدين من الخدمات الإلكترونيّة إلى ذلك: ومعنى ذلك أنّ المستفيدين من الخدمات الإلكترونيّة بحاجة إلى حماية معلوماتهم من كلّ ما يضرّ بها.

الحاجة لأمن المعلومات

٤. انتشار الخدمات الإلكترونيّة عن بعد: مثل خدمات الحكومات الإلكترونيّة والتعليم عن بُعد، لدرجة أنّ المواطن يستطيع أن يُنهي جلّ أو جميع إجراءاته، وأن يحصل على درجته العلمية المناسبة من منزله. ولإتمام هذا النوع من الخدمات فلا بدّ من توفير الحماية اللازمة للمعلومات ولجميع الأنظمة والتجهيزات التي تخزّنها أو تعالجها أو تنقلها لدى كل من مقدِّم الخدمة والمستفيد على حدٍّ سواء.

الحاجة لأمن المعلومات

٥. الحاجة إلى معرفة إمكانيّات المنشآت ومدى قدرتها على حماية معلوماتها ومعرفة التهديدات التي تواجهها: فلكي تكون آمنًا، فلا بدّ أن تعرف نفسك، وتعرف التهديدات التي تواجهك. ومن هنا جاءت الحاجة إلى أمن المعلومات التي من خلالها يمكن تقويم وضع الحماية في المنشأة، ومعرفة التهديدات التي تواجهها، وتحليل المخاطر المحيطة بها، من أجل أخذ التدابير اللازمة لمجابهة تلك التهديدات والمخاطر.

الحاجة لأمن المعلومات

٦. كثرة التهديدات المعلوماتيّة وتنوّعها، وتعدّد مصادرها: والخطورة في ذلك أنّه قد توجد جُملة من التهديدات داخل المنشأة، في أنظمتها المعلوماتيّة أو في موظّفيها، إذا لم يُحتاط لها فقد تضر بالمعلومات. ولأهميّة ذلك فقد أفردتُ له موضوعًا مستقلًّا

٧. انتشار الهجمات الإلكترونيّة:

تهديدات المعلومات و انظمتها

A. تهديدات فنية

- **تهديدات عيوب التصميم و التشغيل .**
- **تهديد تشتت المعلومات .**

B. تهديدات بشرية

C. تهديدات طبيعية

الهدف من التهديد

- تدمير وإتلاف الأجهزة أو المعلومات.
- سرقة أو تعديل المعلومات.
- وضع أنظمة للتجسس والمراقبة، ويتم مكافحة ذلك النوع بالتأمين المادي للأجهزة.

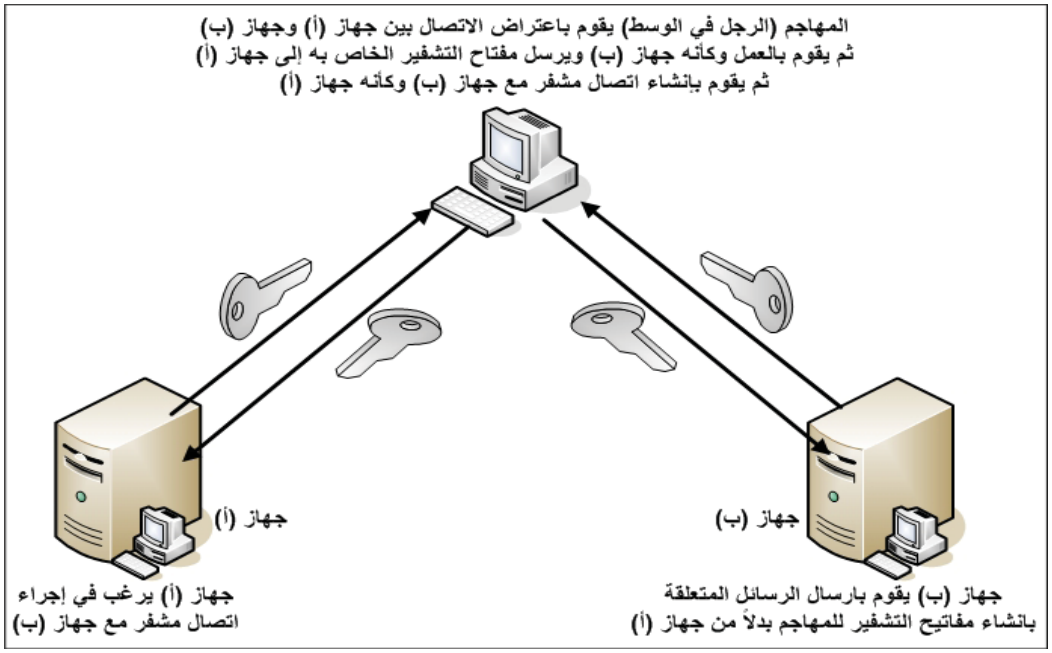
الهجمات الالكترونية و الحاجة للحماية منها

I. **هجمات البرامج او الاكواد الخبيثة (Malicious Code Attacks)**

- الفيروسات .
- ديدان الحاسب الألي .
- برامج أحصنة طروادة .
- برامج الاختراق .
- برامج التجسس الالكتروني .

الهجمات الالكترونية و الحاجة للحماية منها

II. هجمات الابواب الخلفية (Back Door Attacks).
III. كسر كلمات المرور (Password Crack).
IV. الهجوم الأعمى الاستقصائي (Brute Force Attack).
V. هجمات المعجم (Dictionary Attacks).
VI. هجمات الرجل في الوسط (Man-in-the-Middle Attacks) .
VII. هجوم تعطيل الخدمة (Denial of Service (DoS) Attack) .
VIII. هجمات الخداع (Spoofing Attacks) .
IX. الرسائل المزعجة او غير المرغوب فيها (Spam).
X. تفجير البريد الألكتروني (Mail Bombing) .
XI. هجمات التشمم أو الالتقاط (Sniffer Attacks).
XII. هجمات الهندسة الأجتماعية (Social Engineering Attacks) .
XIII. هجوم تصفح الكتف (Shoulder Surfing Attack) .
XIV. هجمات المعلومات الجانبية (Side-channel Attacks)



عناصر أمن المعلومات

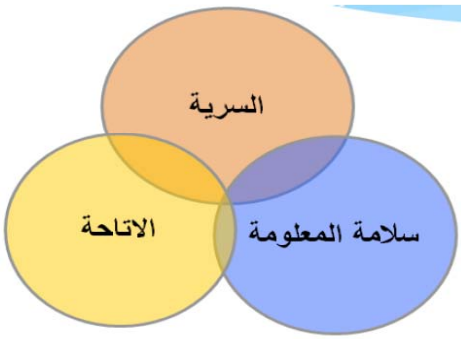
عناصر امن المعلومات هي :

- السرية .
- التحقق من الهوية .
- عدم الأنكار .
- التحكم بالوصول .
- سلامة المعلومة و تكاملها .

عناصر أمن المعلومات

2– عناصر أمن المعلومات:

الشكل رقم16: عناصر أمن المعلومات



عناصر أمن المعلومات

من أجل حماية المعلومات من المخاطر التي تتعرض لها لا بد من توفر مجموعة من العناصر التي يجب أخذها بعين الاعتبار لتوفير الحماية الكافية للمعلومات، ولقد صنف تلك العناصر إلى خمسة عناصر وهي:

أولا: السرية أو الموثوقية :(**Confidentiality**) : وهي تعني التأكد من أن المعلومات لا يمكن الاطلاع عليها أو كشفها من قبل أشخاص غير مصرح لهم بذلك ولتجسيد هذا الأمر يجب على المؤسسة استخدام طرق الحماية المناسبة من خلال استخدام وسائل عديدة مثل عمليات تشفير الرسائل أو منع التعرف على حجم تلك المعلومات أو مسار إرسالها.

عناصر أمن المعلومات

ثانيا: التعرف أو التحقق من هوية الشخصية:(**Authentication**) : وهذا يعني التأكد من هوية الشخص الذي يحاول استخدام المعلومات الموجودة ومعرفة ما إذا كان هو المستخدم الصحيح لتلك المعلومات أم لا، ويتم ذلك من خلال استخدام كلمات السر الخاصة بكل مستخدم، وتوضح مؤسسة(RSA) لأمن المعلومات RSA Security Inc ثلاث طرق للتحقق من الشخصية وهي:

1– عن طريق شيء يعرفه الشخص مثل كلمة المرور .

2– عن طريق شيء يملكه مثل رسالة الشيفرة (Token) : وهي عبارة عن كود يقوم بإدخاله المستخدم للحاسوب للحيازة على صلاحيات التشغيل أو الشهادة الإلكترونية.

3– عن طريق شيئ يتصف به الشخص من الصفات الفيزيائية مثل بصمة الإصبع أو المسح الشبكي أو نبرة الصوت، وكل طريقة لها إيجابياتها وسلبياتها، وتنصح مؤسسة RSA باستخدام طريقتين مع بعضهما البعض من هذه الطرق الثلاثة.

عناصر أمن المعلومات

. **ثالثا: سلامة المحتوى:** (Integrity) : وهي تعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو تدميره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواء كان التعامل داخليا في المشروع أو خارجيا من قبل أشخاص غير مصرح لهم بذلك ويتم ذلك غالبا بسبب الاختراقات الغير مشروعة مثل الفيروسات حيث لا يمكن لأحد أن يكسر قاعدة بيانات البنك ويقوم بتغيير رصيد حسابه لذلك يقع على عاتق المؤسسة تأمين سلامة المحتوى من خلال إتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزات المضادة للاختراقات أو الفيروسات.

عناصر أمن المعلومات

رابعا: استمرارية توفر المعلومات أو الخدمة: (Availability) : وهي تعني التأكد من استمرارية عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمات لمواقع المعلومات وضمان عدم تعرض مستخدمي تلك المعلومات إلى منع استخدامها أو الوصول إليها بطرق غير مشروعة يقوم بها أشخاص لإيقاف الخدمة بواسطة كم هائل من الرسائل العبثية عبر الشبكة إلى الأجهزة الخاصة لدى المؤسسة.

عناصر أمن المعلومات

خامسا: عدم الإنكار: (No repudiation) : ويقصد به ضمان عدم إنكار الشخص الذي قام بإجراء معين متصل بالمعلومات لهذا الإجراء، ولذلك لا بد من توفر طريقة أو وسيلة لإثبات أي تصرف يقوم به أي شخص للشخص الذي قام به في وقت معين، ومثال ذلك للتأكد من وصول بضاعة تم شراؤها عبر شبكة الإنترنت إلى صاحبها، ولإثبات تحويل المبالغ إلكترونيا يتم استخدام عدة رسائل مثل التوقيع الإلكتروني والمصادقة الإلكترونية.

وسائل تحقيق عناصر أمن المعلومات

أعداد

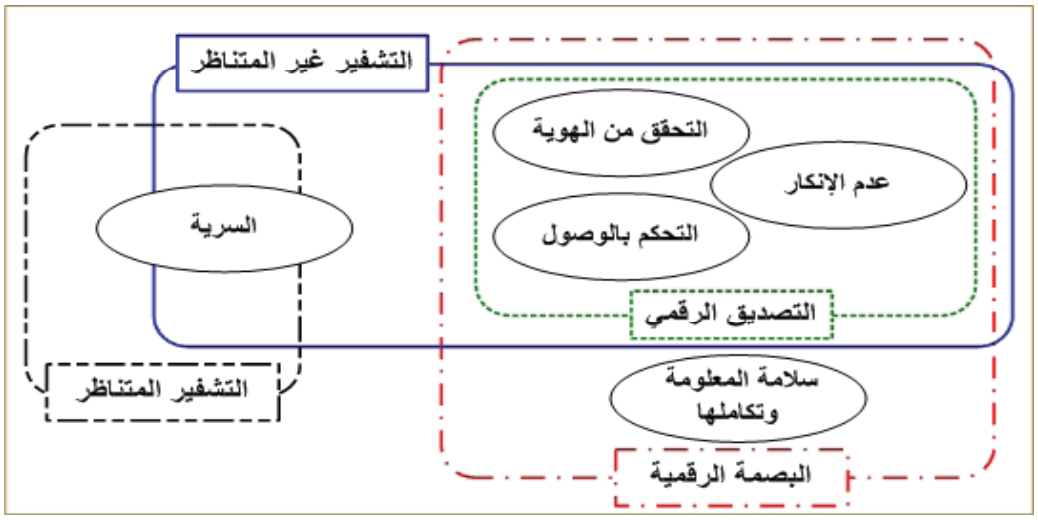
د.قيس سلطان

وسائل تحقيق عناصر أمن المعلومات

- هناك ثلاث تقنيات رئيسة يمكن استخدامها كوحدات بناء اساسية لتحقيق بعض عناصر امن المعلومات :

A. التشفير (Encryption) بنوعيه المتناظر و الغير متناظر .
B. التصديق الرقمي (Digital Signature) .
C. البصمة الرقمية (Hash Value).

وسائل تحقيق عناصر أمن المعلومات



التشفير (Encryption)

- التشفير هو العملية التي يتم من خلالها تغيير البيانات و جعلها في شكل غير مفهوم او غير مقروء (أي تعميتها) .

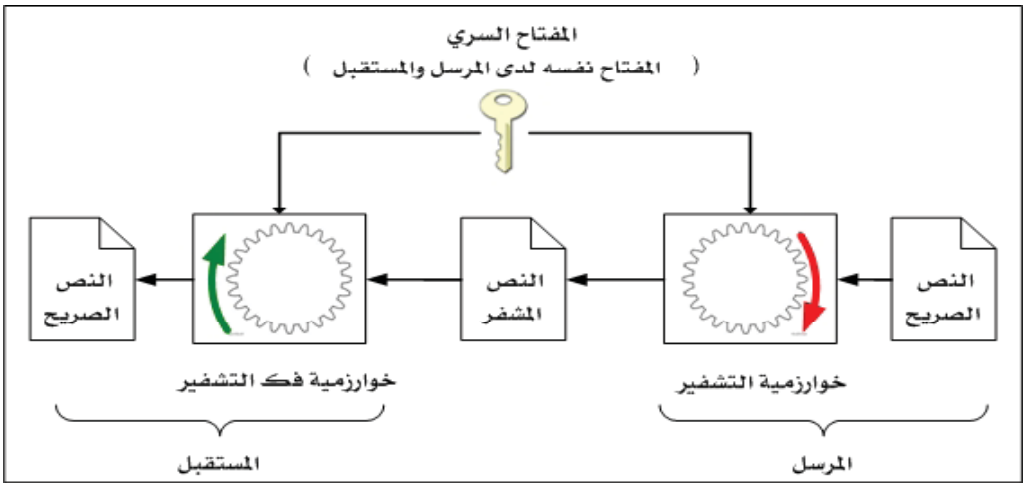
التشفير (Encryption)

A. التشفير المتناظر (Symmetric Encryption)
   - التشفير التسلسلي (Stream Cipher).
   - التشفير الكتلي (Block Cipher).
B. التشفير غير المتناظر او التشفير باستخدام المفتاح العام .

مصطلحات التشفير (Encryption)

- «النّص الصريح»(Plain Text): وهو الرسالة أو(البيانات) الأصليّة قبل إجراء أيّ عمليّة عليها.
- "النص المشفّر"(Cipher Text) : يطلق على الرسالة المشفّرة بعد أن تشفّر.
- "التّشفير"(Encryption): تحويل الرسالة من نصّ صريح إلى نص مشفّر.
- "فك التّشفير"(Decryption): استرجاع النّصّ الصريح من النصّ المشفّر.
- "خوارزميّة التّشفير"(Encryption Algorithm): مجموعة الخطوات والعمليّات الرياضيّة التي يتم اتّباعها لتحويل النّص الصريح إلى نص مشفّر.
- "خوارزميّة فكّ التّشفير"(Decryption Algorithm): وهي الخوارزميّة العكسيّة لخوارزميّة التّشفير؛ لاسترجاع النّص الصريح من النّص المشفّر.
- "تحليل الشيفرة"(Cryptanalysis)، ويطلق عليها أيضًا(كسر الشيفرة)، وتعني التقنيات المستخدمة لفكّ تشفير رسالة بطريقة غير شرعيّة، أي كسر تشفيرها بوساطة طرف غير مصرّح له، ولا يعرف المفاتيح اللازمة لذلك[1].
- «المفتاح السِّرّي»(Key) : وهو عبارة عن قيمة غير معتمدة على الرسالة يختارها نظام التّشفير أو المستخدم.

١ـ التشفير المتناظر



١ـ التشفير المتناظر

- نظام التشفير المتناظر يتكون من خمسة مكونات رئسية هي :

A. النص الصريح .

B. خوارزمية التشفير . تتكون مدخلات خوارزمية التشفير من النص الصريح والمفتاح السري ومخرجاتها من النص المشفر . ومن اشهر خوارزميات التشفير:

- **خوارزمية التشفير القياسي الثلاثي (Triple Data Encryption Standard(3DES)) .**
- **خوارزمية التشفير القياسي المتقدم (Advanced Encryption Standard-AES) .**

A. المفتاح السري .

B. النص المشفر .

C. خوارزمية فك التشفير .

١ـ التشفير المتناظر

إنّ قوّة نظام التّشفير (سواءً أكان متناظرًا، أم غير متناظر) تكمن في سريّة المفتاح السِّريّ وقوّته، وليس في إبقاء خوارزميّة التّشفير سريّة. فمن المعروف أن لا تبقى الخوارزميّة سريّة وأن تكون معروفة حتى يمكن تطويرها من حين لآخر[١]. وللحصول على مفاتيح سرّ قوية فإنّه يمكن اتباع الآتي:

١. إنتاج المفاتيح السِّريّة بشكل آلي من قِبل النظام، وليس من قِبل المستخدم.

٢. استخدام مفاتيح سريّة عشوائيّة مختلفة لكلّ عمليّة إرسال مختلفة.

٣. استخدام مفاتيح سريّة طويلة لا تقل عن ٢٥٦ بت (Bit).

٤. استخدام مفاتيح سريّة في صيغتها الثنائيّة (٠ ، ١) فقط وليس في صيغتها المعتادة (الحروف والأرقام المعتادة).

١ـ التشفير المتناظر باستخدام استبدال الحروف الهجائية

النّص الصريح	أ	ب	ت	ث	ج	ح	خ	د	ذ	ر	ز	س	ش	ص
النّص المشفّر	ث	ج	ح	خ	د	ذ	ر	ز	س	ش	ص	ض	ط	ظ

النّص الصريح	ض	ط	ظ	ع	غ	ف	ق	ك	ل	م	ن	هـ	و	ي
النّص المشفّر	ع	غ	ف	ق	ك	ل	م	ن	هـ	و	ي	أ	ب	ت

١ـ التشفير المتناظر باستخدام استبدال الحروف الهجائية

يتكوّن هذا النظام البسيط من المكوّنات الأساسيّة الآتية:

١. النّص الصريح: أيّ كلمة أو جملة في اللّغة العربيّة.

٢. خوارزميّة التّشفير: استبدال الحرف بالحرف الثالث الذي يليه في الترتيب الهجائي.

٣. المفتاح السِّريّ للتشفير: (+٣).

٤. النّص المشفّر: أيّ كلمة أو جملة في اللّغة العربيّة.

٥. خوارزميّة فك التّشفير: استبدال الحرف بالحرف الثالث الذي يسبقه في الترتيب الأبجدي.

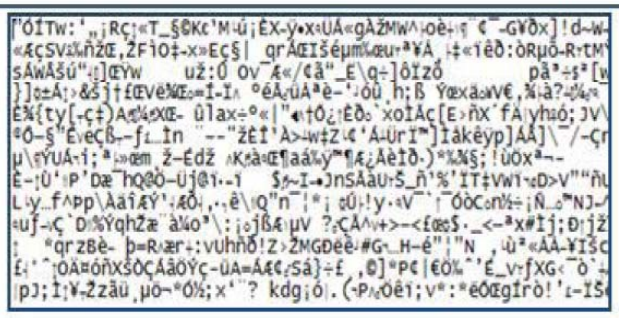
٦. المفتاح السِّريّ لفك التّشفير: (-٣).

١- التشفير المتناظر باستخدام استبدال الحروف الهجائية

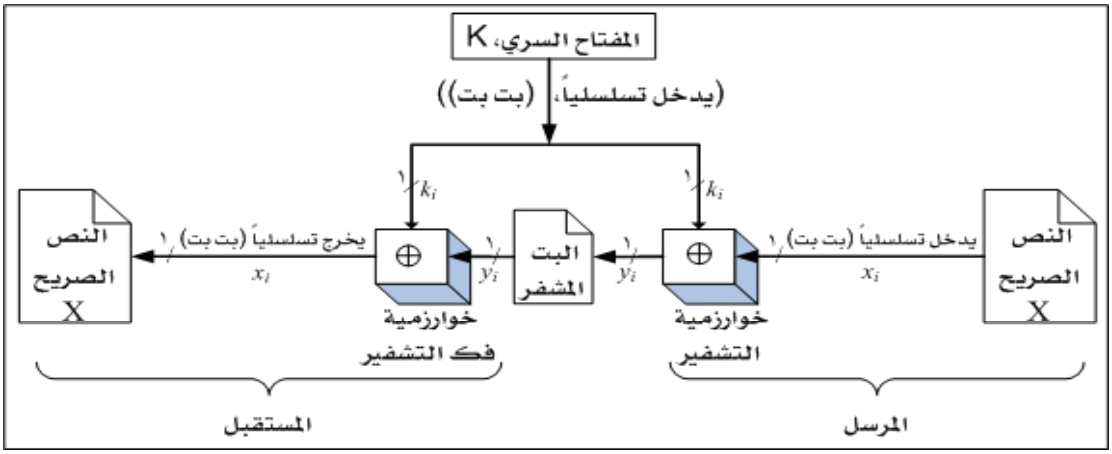
بتشفير الجملة «أمن المعلومات» باستخدام النظام أعلاه فإنّنا نحصل على النّص المشفّر «ثوي ثهوقهبوثح»، كما أنه يمكن الحصول على الجملة (أمن المعلومات) مرّة أخرى بفكّ تشفير النّص المشفّر «ثوي ثهوقهبوثح» باستخدام النظام نفسه.

١- التشفير المتناظر باستخدام التشفير القياسي المتقدم AES

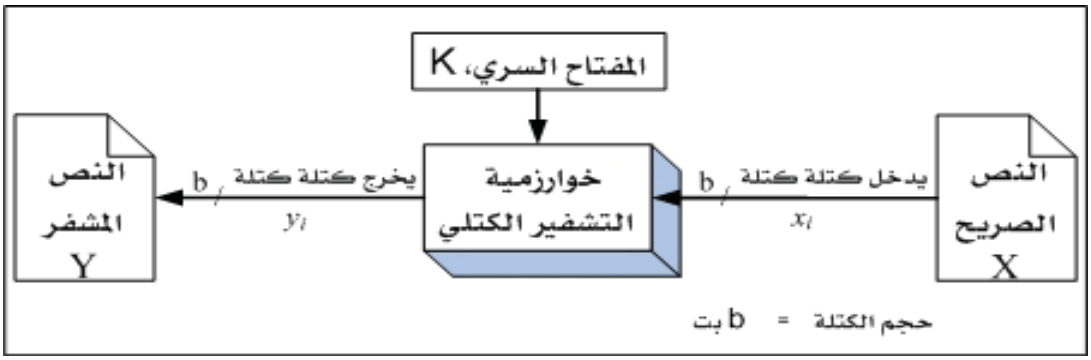
مر التاريخ البشري بمراحل تطور عديدة منذ نشأته. وفي القرون الأخيرة، ظهرت عدة ثورات كبيرة أثّرت في حياة البشر بدرجة كبيرة وغيّرت في منحى حياتهم اليومية، ومنها ثورة السكك الحديدية، ثم ثورة الكهرباء، وبعدها ثورة الهاتف والاتصالات الفضائية. وفي عصرنا الحاضر، أصبحت تتردد كثيراً عبارات "عصر المعلومات" و "ثورة المعلومات".



١ـ التشفير المتناظر
التشفير التسلسلي (Stream Cipher)



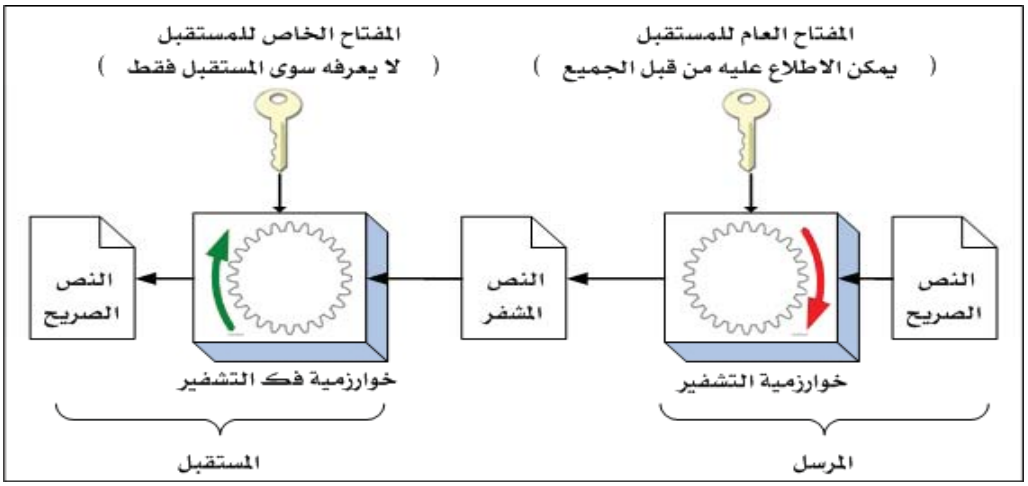
١ـ التشفير المتناظر
التشفير الكتلي (Block Cipher)



١ـ التشفير المتناظر
التشفير الكتلي (Block Cipher)

- يختلف حجم الكتلة و طول مفتاح التشفير من خوارزمية الى أخرى :
- في خوارزمية تشفير البيانات القياسي (DES) كل كتلة ٦٤ بت (٨ بايت) ، و طول مفتاح التشفير ٥٦ بت .
- خوارزمية التشفير القياسي المتقدم (AES) كل كتلة ١٢٨ بت (١٦ بايت) ، و طول مفتاح التشفير ١٢٨ بت أو ١٩٢ بت أو ٢٥٦ بت و إن كان ١٢٨ بت هو الأكثر انتشارا .

٢ـ التشفير غير المتناظر



٢- التشفير غير المتناظر

كما هو موضح في الشكل (٤-١٢)، يتكوّن نظام التّشفير غير المتناظر من ست مكوّنات رئيسة، هي:

١. النّص الصريح: وهو النّص أو الرسالة الأصليّة المقروءة التي يتم إدخالها إلى خوارزميّة التّشفير.

٢. خوارزميّة التّشفير: وهي الطريقة التي تشتمل على مجموعة الخطوات التي تُنفّذ على النّص الصريح لإنتاج النّص المشفّر باستخدام المفتاح العام للمستقبل، وتكون مدخلات خوارزميّة التّشفير هي النّص الصريح والمفتاح العام للمستقبل، ومخرجاتها هي النّص المشفّر، ومن أشهر خوارزميّات التّشفير بالمفتاح العام خوارزميّة آر إس أيه(RSA)، وخوارزميّة المنحنى البيضاوي(الإهليليجي) (Elliptic Curve).

٢- التشفير غير المتناظر

٣. المفتاح العام(Public Key): وهو مفتاح عام (مشاع) بحيث يكون لكّل طرف مفتاح عام يستخدم لتشفير إي رساله ترسل إليه. ويمكن لأيّ شخص الاطّلاع على المفتاح العام واستخدامه في تشفير البيانات المرسلة إلى صاحب ذلك المفتاح العام، و يُفكّ تشفير الرسالة المشفّرة عن طريق المفتاح الخاص بالمستقبل (صاحب المفتاح العام الذي جرى التّشفير به).

٤. المفتاح الخاص(Private Key): وهو عبارة عن مفتاح خاص سرّي، بحيث يكون لكلّ طرف مفتاح خاص سرّي خاص به يتم استخدامه لفكّ تشفير الرسائل الواردة إليه، ويكون هذا المفتاح مرتبطًا بالمفتاح العام الخاص بالشخص نفسه.

٢- التشفير غير المتناظر

٥. النّص المشفّر: وهو عبارة عن الرسالة التي تنتجها خوارزميّة التّشفير من كلّ من النّص الصريح والمفتاح العام للمرسل إليه.

٦. خوارزميّة فكّ التّشفير: وهي مجموعة الخطوات التي يتم تنفيذها على النّص المشفّر لإنتاج النّص الصريح، باستخدام المفتاح السِّريّ الخاص للمستقبل. وتكون مدخلات خوارزميّة فكّ التّشفير هي النّص المشفّر والمفتاح السِّريّ للمستقبل، ومخرجاتها هي النّص الصريح.

مقارنة بين التشفير المتناظر و غير المتناظر

التّشفير المتناظر	التّشفير غير المتناظر
١. يتم استخدام نفس المفتاح عند المرسل والمستقبل ونفس الخوارزميّة لكل من عمليّة التّشفير وفك التّشفير.	١. يتم استخدام نفس الخوارزميّة للتشفير وفك التّشفير.
٢. يجب إن يتم توزيع المفتاح السِّريّ بطريقة آمنة.	٢. يستخدم زوج من المفاتيح أحدهما عام يطلع عليه الآخرون، والآخر سري خاص بكل مستخدم (ليس نفس المفتاح عند المرسل والمستقبل)
٣. يحتاج إلى عمليّة توزيع آمنة للمفاتيح السِّريّة.	٣. لا يحتاج إلى عمليّة توزيع المفاتيح.

مقارنة بين التشفير المتناظر و غير المتناظر

نوع التّشفير	الخوارزميّة	مستوى السِّريّة (بت)			
		٨٠	١٢٨	١٩٢	٢٥٦
متناظر	التّشفير القياسي المتقدم (AES)	٨٠	١٢٨	١٩٢	٢٥٦
غير متناظر	آر إس أيه (RSA)	١٠٢٤	٣٠٧٢	٧٦٨٠	١٥٣٦٠
	المنحنى البضاوي (Elliptic Curve)	١٦٠	٢٥٦	٣٨٤	٥١٢

التصديق أو التوقيع الرقمي

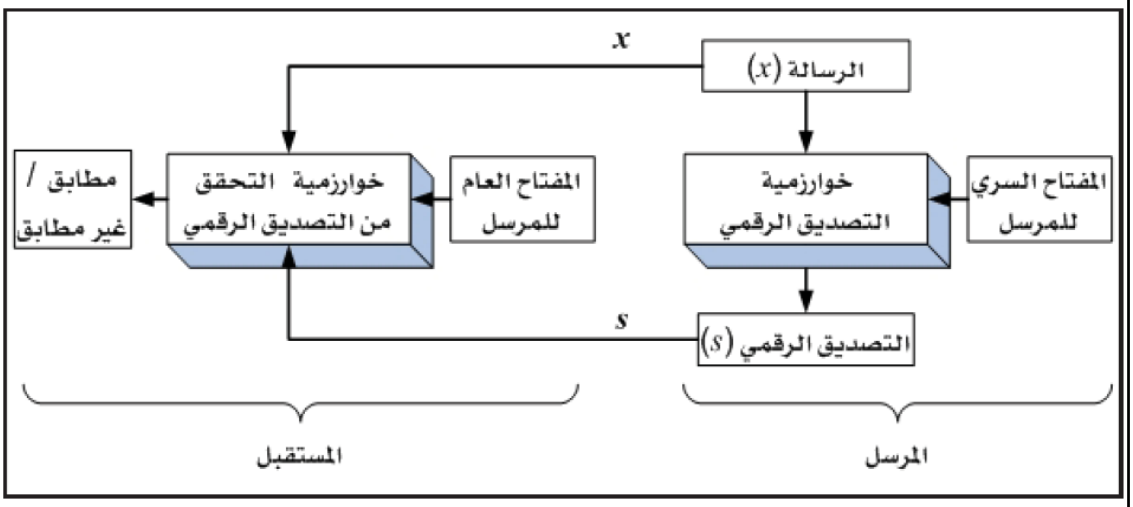
يعتمد التصديق الرقمي بشكل أساسي على نظام التّشفير بالمفتاح العام، لكن بطريقة عكسيّة له، حيث توقيع الرسالة من قبل معد الرسالة باستخدام مفتاحه السِّريّ (وليس المفتاح العام للمستقبل كما هي الحال في التّشفير بالمفتاح العام)، ويتم التحقّق من صحة التوقيع من قبل مستلم الرسالة باستخدام المفتاح العام للموقِّع. لاحظ أنّ الطرف الآخر- وهو مستلم الرسالة- يستخدم المفتاح العام للموقِّع للتّحقق من صحّة التوقيع، وليس من أجل تشفير الرسالة كما هي الحال في التّشفير بالمفتاح العام.

التصديق أو التوقيع الرقمي

إذن فالتصديق الرقمي يتكوّن من عمليتين أساسيتين، كما هو موضح في الشكل (٤-١٦)، وهما:

- التوقيع (Sign): وهو عمليّة إجراء (إنتاج) التصديق الرقمي، ومدخلاتها هي: الرسالة والمفتاح السِّريّ للموقِّع، ونتيجتها هي التوقيع الرقمي نفسه، وهو رقم صحيح (طويل)، (٢٠٤٨) بت مثلًا.
- التحقّق من صحة التوقيع (Verify): وهو عمليّة التحقّق من أنّ التوقيع تم من الشخص المعنى على الرسالة المعنيّة. ومدخلاتها هي: الرسالة والمفتاح العام للموقِّع، ونتيجتها إحدى حالتين: إمّا مطابق، أو غير مطابق.

التصديق أو التوقيع الرقمي



التصديق أو التوقيع الرقمي

من أشهر طُـرُق التوقيع الرقمي هي الطريقة التي تعتمد علـى تصديق البصمة الرقميّة للرسالة وليس الرسالة الأصلية؛ لأنّه عادة ما تكون الرسائل الأصليّة طويلة،(قد يصل طول بعضها إلى مئات الصفحات)، وهو ما يجعل عمليّة التصديق طويلة أيضًا. وتتلخص عمليتا التوقيع، والتحقق من صحّته بهذه الطريقة في الخطوات التالية،

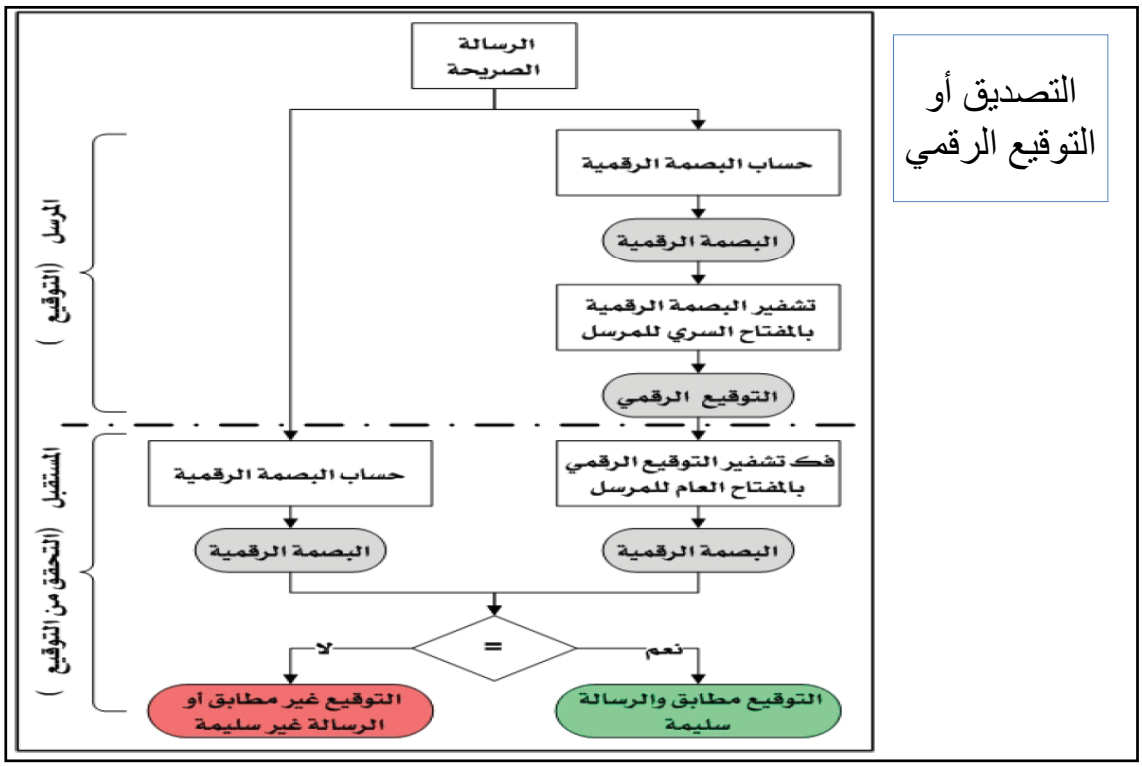
التصديق أو التوقيع الرقمي

- عمليّة التوقيع:

١. يتم حساب البصمة الرقميّة (Hash Value) للرسالة (انظر موضوع: البصمة الرقميّة) المراد التوقيع عليها.

٢. يتم تشفير هذه البصمة الرقميّة باستخدام المفتاح السِّريّ للمرسل (الموقِّع) لإنتاج "التوقيع الرقمي" للرسالة.

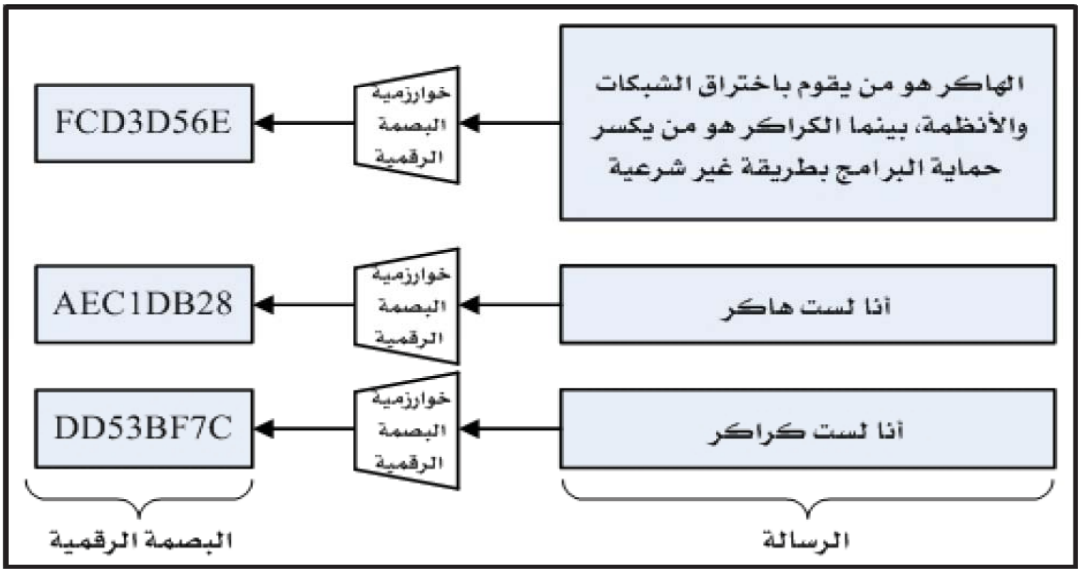
٣. يتم إرسالها مع الرسالة الصريحة إلى المرسل إليه.



البصمة الرقمية (Hash Value)

على الرغم من وجود تطبيقات كثيرة ومهمّة للبصمة الرقميّة، إلّا أنّ أشهرها هو استخدامها في التصديق الرقمي، كما مرّ معنا آنفًا. فعادة ما تكون الرسائل طويلة، قد يصل طول بعضها إلى مئات الصفحات، وهو ما يجعل تطبيق التصديق الرقمي عليها صعبًا جدًّا. ومن هنا جاءت البصمة الرقميّة(أو القيمة المركّزة) لتحلّ مشكلة التعامل مع الرسائل الطويلة. فالبصمة الرقميّة هي «سلسلة قصيرة وثابتة الطول من البتّات تشكّل بصمة فريدة لكل رسالة» ومعنى ذلك أن يكون لدينا بصمة رقميّة مختلفة لكلّ رسالة، لكن جميع البصمات طولها واحد مكوّن من العدد نفسه من البتّات، ١٦٠ بت مثـلًا ، مهما كان طول الرسالة.

البصمة الرقمية (Hash Value)



البصمة الرقمية (Hash Value)

تحسب البصمة الرقميّة باستخدام خوارزميّات خاصّة بذلك، بحيث يتم الحصول من خلالها على بصمة رقميّة فريدة لكل رسالة، من أشهرها: خوارزميّة (Message Digest-5-MD5)، وخوارزميّة (Secure Hash Algorithm-1-SHA-1)، وخوارزميّة (SHA-2)، وهناك خوارزميّة حديثة تحت التصميم والتجربة يتوقّع أن تُقنّن لتصبح قياسيّة عالميًّا في العام ٢٠١٢م، هي خوارزميّة (SHA-3).

البصمة الرقمية (Hash Value)

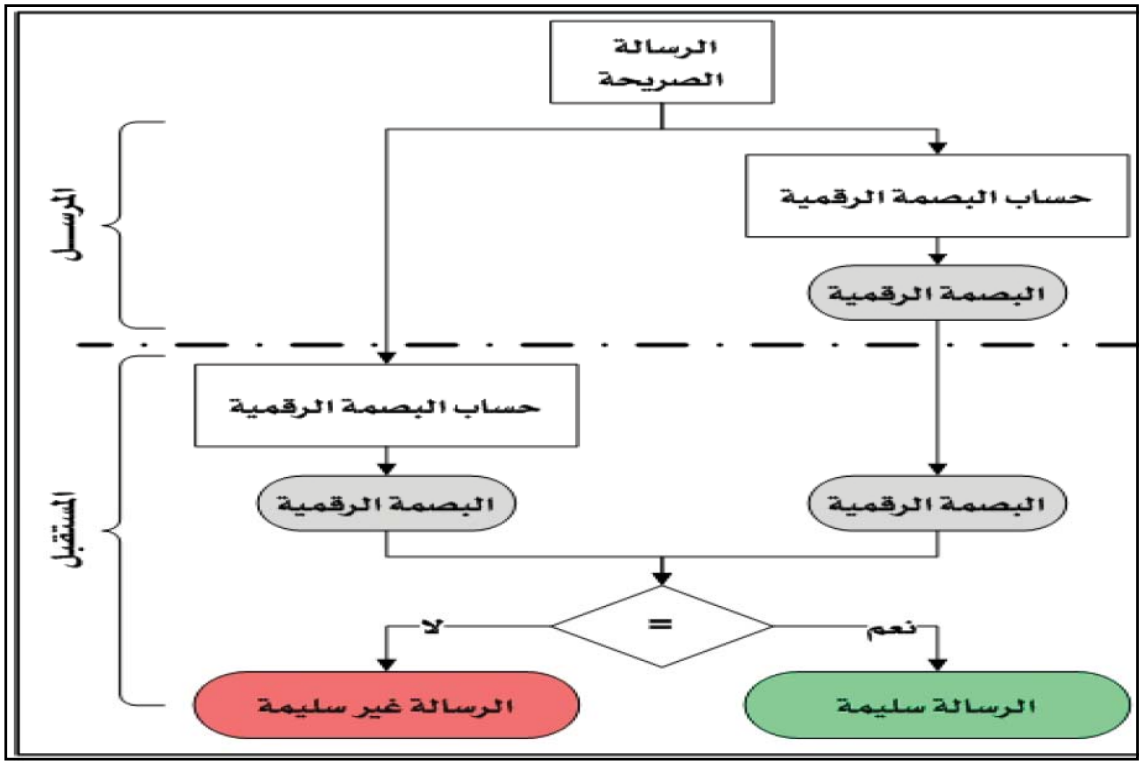
وتتلخص طريقة استخدام البصمة الرقميّة للتحقق مـن سلامة محتوى الرسالة فيما يلي، انظر الشكل(٤-١٩):

١. يحسب المرسل البصمة الرقميّة للرسالة باستخدام إحدى خوارزميّات البصمة الرقميّة.

٢. يرسل المرسل الرسالة الأصليّة متبوعة بالبصمة الرقميّة.

٣. عند استلام الرسالة من قبل المستقبل يُعيد حساب البصمة الرقميّة للرسالة التي استلمها.

٤. يقارن المستقبل البصمة الرقميّة التي حصل عليها في الخطوة السابقة(رقم ٣) مع البصمة الرقميّة التي استلمها مع الرسالة، فإذا تطابقت القيمتان، فهذا دليل على أنّ الرسالة سليمة ولم يطرأ عليها أيّ تغيير، أمّا إذا لم تتطابق فهذا دليل على أنّ الرسالة غير سليمة، أو أنه طرأ عليها تغيير ما.



الملخص

فيمكن تحقيق عنصر السِّريّة باستخدام التّشفير المتناظر أو غير المتناظر أو بهما معًا. ويمكن تحقيق عناصر التحقّق من الهُويّة، والتحكم بالوصول للمنشآت الصغيرة، وعدم الإنكار باستخدام التّشفير غير المتناظر والتصديق الرقمي معًا. ويمكن تحقيق عنصر سلامة المعلومة وتكاملها باستخدام البصمة الرقميّة. كما يمكن استخدام التصديق الرقمي للتحقق من هويّة الشخص(Entity Authentication) ويستخدم مع البصمة الرقميّة للتحقق من هويّة الرسالة أو المعلومة(Data Origin Authentication).

أمن الحاسبات و البرمجيات و الملفات

أعداد

د.قيس سلطان

تعريف

يقصد بأمـن الحاسبات هنا، أمن أجهـزة الحاسب الآلي(كعتاد صلـد)، ويقصد بأمن البرمجيات أمن أنظمة التشغيل التي تتحكم بالأجهزة، وأمن البرامج التطبيقيّة التي يتعامل معها المستخدم لأداء مهامه اليومية، ويقصد بأمن الملفّات أمن الملفّات نفسها كأوعية لتخزين المعلومات، مثل: ملفات معالجة النصوص، والجداول الإلكترونيّة، وقواعد البيانات، ورسائل البريد الإلكتروني، وأمن نظام الملفّات(File System) الذي يتحكم بإدارة جميع الملفّات.

التهديدات الرقمية للحاسبات والبرمجيات والملفات

يكمن التهديد الرئيس لجهاز الحاسب الآلي(الصلد) في وفرته. فالجهاز هو أكثر المناطق ضعفًا في مواجهـة الهجمات، وأكثرها طاعـة لضوابط الرقابة التلقائيـة. وتشمل تهديدات أجهزة الحاسب الآلي كذلك: السرقة، وإلحاق الضرر بها سواءً عن طريق الخطأ أم العمد.

التهديدات الرقمية للحاسبات والبرمجيات والملفات

يكمن التهديد الرئيس للبرمجيات في الهجمات على توفر البرنامج، خاصّة البرامج التطبيقيّة، حيث غالبًا ما تكون سهلة الحذف، ومن التهديدات كذلك تغيير البرامج التطبيقيّة أو إتلافها؛ لتصبح غير مفيدة. ومن أكثر المشكلات التي يجب التعامل معها في مجال البرمجيات هو التعديلات التي تحدث في البرنامج الذي لا يزال يعمل، لكنه يجري تحديثه بطريقة مختلفة عن الطريقة السابقة. ولحل هذه المشكلة يجب توزيع البرامج بعناية عن طريق إنشاء النسخ وفق إصدارات تدريجية، وتوزيع النسخ الأحدث منها. المشكلة الأخيرة التي تواجه البرمجيات هي الخصوصية، ومع أن هنالك كثيرًا من الاحتياطات التي اتخذت، إلّا أنّ مشكلة النسخ غير المرخّص له للبرامج ما زالت بدون حل.

التهديدات الرقمية للحاسبات والبرمجيات والملفات

إنّ التهديدات الأمنيّة بخصوص البيانات واسعة جدًّا لدرجة أنها تشمل تهديدات توفرها وتهديدات سرّيّتها، وتهديدات سلامتها وتكاملها. ففي حالة التوفر، فإنّ التهديدات تكمن في إتلاف ملفات البيانات، التي قد تحدث إمّا عن طريق الخطأ أو بشكل متعمّد، وفي حالة السِّريّة، تكمن التهديدات في القراءة غير المسموح بها لملفات البيانات أو قواعد البيانات، وفي حالة سلامة البيانات وتكاملها، تكمن التهديدات في تغيير البيانات، إمّا بحذف أو إضافة أو تعديل، وهذا المجال قد أضحى أكثر المجالات اهتمامًا بالأبحاث والجهود المبذولة من جانب المختصين في أمن المعلومات.

التهديدات الرقمية للحاسبات والبرمجيات والملفات

وهناك تهديد آخر لكنه أقل ظهورًا، وهو تحليل البيانات وتحليل تصاميم قواعد البيانات من أجل كسر حمايتها، ويمكن القول إن سلامة البيانات هي الهاجس الأكبر في معظم المنشآت؛ لأن التعديلات التي تجرى على ملفات البيانات قد تترتب عليها نتائج تتراوح بين المخاطر الصغيرة إلى المخاطر الكارثية.

التهديدات الرقمية للحاسبات والبرمجيات والملفات

هناك تهديدات رئيسة تُعدُّ قاسمًا مشتركًا بين تهديدات الحاسبات والبرمجيات والبيانات، وتهدّد كلًّا منها إمّا بشكل منفصل أو بشكل تكاملي، وهذه التهديدات هي: البرامج الضارة (Malware)، وبرامج التجسّس (Spyware) ولأهمية هذه التهديدات فقد أفردنا لكل منها موضوعًا مستقلًا نتعرف فيه ماهيّة هذه التهديدات، وأنواعها، وطريقة عملها، وطرق مكافحتها.

التهديدات الرقمية للحاسبات والبرمجيات والملفات

هنـاك تهديـدات رئيسة تُعـدُّ قاسمًـا مشتركًا بـين تهديـدات الحاسبـات والبرمجيات والبيانات، وتهدّد كلًّا منها إمّا بشكل منفصل أو بشكل تكاملي، وهذه التهديدات هي: البرامج الضارة(Malware)، وبرامج التجسّس(Spyware) ولأهمية هذه التهديدات فقد أفردنا لكل منهـا موضوعًا مستقلًا نتعرف فيـه ماهيّة هذه التهديدات، وأنواعهـا، وطريقة عملها، وطرق مكافحتها.

التهديدات الرقمية للحاسبات والبرمجيات والملفات

هنـاك تهديـدات رئيسة تُعـدُّ قاسمًـا مشتركًا بـين تهديـدات الحاسبـات والبرمجيات والبيانات، وتهدّد كلًّا منها إمّا بشكل منفصل أو بشكل تكاملي، وهذه التهديدات هي: البرامج الضارة(Malware)، وبرامج التجسّس(Spyware) ولأهمية هذه التهديدات فقد أفردنا لكل منهـا موضوعًا مستقلًا نتعرف فيـه ماهيّة هذه التهديدات، وأنواعهـا، وطريقة عملها، وطرق مكافحتها.

البرامج الضارة – Malware

رغم أنّ مصطلح "البرامج الضارّة" عادة ما يستخدم بطريقة عمومية؛ ليكون مرادفًا للفيروس، إلا أنه بنفس الطريقة أصبح يطلق اسم "فيروس" ببساطة لوصف أي نوع من مشكلات الحاسب الآلي؛ مما سبب بعض اللبس وصعوبة التفريق بين أنواع البرامج الضارة. ولم يقف الأمر عند ذلك الحد، بل أصبح هناك خلط واضح بين الفيروسات، والديدان، وأحصنة طروادة، رغم أن لكل منها خصائصه التي تميزه من غيره، وإن كان القاسم المشترك بينها هو إلحاق الضرر.

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

فيروس الحاسب الآلي هو برنامج يُعدُّ لينسخ وينشر نفسه، وينتشر ذاتيًّا دون علم وتعاون مع المالك أو المستخدم للجهاز، ولم يتم التوصل بعد لتعريف موحد للفيروسات متفق عليه من الباحثين كافّة، والتعريف العام هو تعريف فريد كوهين[١]، الذي يعرّف الفيروس بأنه: «برنامج يعدّل البرامج الأخرى لكي تحتوي نسخة معدّلة من نفسها» ورغم أنّ هذا التعريف يصف جُلّ الفيروسات، وأن كثيرًا من الباحثين ما زالوا يصرّون على استخدامه، إلّا أنّه يقتصر على البرامج التي تقحم نفسها بنفسها في البرامج الأخرى فقط، وهو بذلك يهمل كثيرًا من الفيروسات التي تقحم نفسها في الملفّات التي ليست برامج بطبيعتها، كالوثائق مثلًا.

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

يمكن تعريف الفيروسات بصورة عامة بأنّها: «البرامج التي تُقحم نفسها بنفسها في مادّة أخرى قد تكون برنامجًا أو قرصًا أو وثيقة أو رسالة بريد إلكتروني أو نظام كمبيوتر أو أيَّ صيغة معلوماتيّة».

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

خصائص الفيروسات

لا تحدث فيروسات الحاسب الآلي أو تنتج طبيعيًّا، وإنّما هي برامج يكتبها مبرمجون، وكذلك فهي لا تظهر من خلال بعض التطورات الإلكترونيّة فقط، وإنّما تكتب بصورة متعمّدة عن طريق أناس متخصّصين، وتبقى الفيروسات مختبئة داخل الجهاز المصاب حتى يستثيرها المستخدم، كفتح الملف المصاب، أو تشغيل البرنامج المصاب؛ لتبدأ بالعمل والتكاثر والانتشار. أي أنّها لا تبدأ بعملها حتى يستثيرها المستخدم، وهناك عدّة خصائص لفيروسات الحاسب الآلي تميزها من غيرها من البرامج الضارّة، وتساعدها على الانتشار وإصابة أجهزة الحاسب الآلي دون علم مستخدميها، وهي:

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

خصائص الفيروسات

- التخفّي: ويعني القدرة على الارتباط ببرامج أو ملفّات أخرى تبدو سليمة ومألوفة للمستخدم، بحيث يلحق الفيروس نفسه بالملف المصاب خفية ليصبح جزءًا منه.

ومن أشهر طُرُق تخفي الفيروسات ما يلي:

- التخفّي في مرفقات البريد الإلكتروني.
- التخفّي في الملفّات التي يجري تحميلها من مواقع الإنترنت، خاصّة تلك التي تشغّل ملفات الصوتيات والفيديو وتتبادلها.
- التخفي وراء الروابط والأوامر الموجودة في صفحات الإنترنت والبريد الإلكتروني.
- التخفّي وراء روابط وملفات الإعلانات والبريد الدعائي.
- التخفّي مع البرامج المنسوخة بشكل غير قانوني.

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

خصائص الفيروسات

- التضاعف: ويعني ذلك أن ينسخ الفيروس نفسه عدّة نسخ تصل في بعض الأحيان إلى ملايين النسخ، بمعنى أنه يتكاثر ليصيب أكبر قدر ممكن من الملفّات والبرامج داخل جهاز الحاسب الآلي نفسه أو داخل الأجهزة الأخرى المرتبطة به. وتبدأ عمليّة التضاعف عندما يتم تحميل برنامج الفيروس إلى ذاكرة الحاسب الآلي وينفّذه المعالج المركزي.

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

خصائص الفيروسات

- الانتشار: ويعني انتقال الفيروس من جهاز إلى آخر عبر شبكات الحاسب الآلي أو وسائط التخزين المختلفة، ومعنى ذلك أنّ لدى الفيروس القدرة على نقل نفسه عند استثارته، كتشغيل أمر النسخ، أو عند اكتشاف اتصال الحاسب الآلي المصاب بحاسب آلي آخر، ومن أشهر طُرُق انتشار الفيروسات ما يلي:

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

خصائص الفيروسات

- تحميل ملفات مصابة من مواقع شبكة الإنترنت أو زيارة مواقع تنشر الفيروسات بشكل تلقائي.
- فتح مرفقات بريد إلكتروني مصابة.
- أن ينسخ المستخدم ملفات مصابة دون علمه، ويخزّنها على وسائط تخزين خارجية تنتشر معها، أو يرسلها عبر الشبكة(كاستخدام المجلّدات المشتركة)، فتنتشر عبرها.
- أن ينسخ الفيروس نفسه، ثم يرفق تلك النسخة مع أيّ ملف آخر عند استثارته.

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

أنواع الفيروسات

ثمة أنواع كثيرة جدًا من الفيروسات. لكن ما يهمنا هنا هو الأنواع (أو المجموعات) الرئيسة الأكثر انتشارًا، التي يشكّل كلّ نوع منها مجموعة من الفيروسات لها البُنية نفسها وتؤدي مهام متشابهة إلى حدّ كبير، وهذه الأنواع هي:

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

أنواع الفيروسات

- فيروسات قطاع بدء التشغيل (الإقلاع): يوجد لكل نظام تشغيل قطاع في قرص التخزين الصلب، مخصّص لبدء عمليّة التشغيل (الإقلاع) وعادة ما يكون هذا القطاع هو القطاع الأول (Track 0)، وعند وجود أيّ خلل فيه فإنّ الحاسب الآلي لن يستطيع البدء بالتشغيل. وفيروسات قطاع بدء التشغيل (Boot Sector Viruses) هي الفيروسات التي تصيب قطاع بدء التشغيل في قرص التخزين الصلب، وتكمن خطورة هذا النوع من الفيروسات في إصابتها لمكان مهم جدًّا يتم من خلاله توجيه الجهاز لتنفيذ البرامج التي يجري من خلالها استكمال تجهيز جهاز الحاسب الآلي للعمل، وبدلًا من ذلك يوجّه الفيروس الحاسب الآلي لتنفيذ الكود الخاص بالفيروس، و من ثَمَّ يفشل الجهاز في عمليّة الإقلاع ولا يمكنه العمل.

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

أنواع الفيروسات

- فيروسات الملفّات(File Infecting Viruses): هي الفيروسات التي تصيب الملفّات بشتى أنواعها؛ فيمكن أن تصيب ملفّات نظام التشغيل كملف(Command.com) في نظام الوينـدوز أو أيّ ملف آخـر، وعادة ما ينتج عن هـذه الفيروسات زيادة في أحجام الملفّات.

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

أنواع الفيروسات

- الفيروسـات الجزئيّة الكبـيرة: تستخـدم الفيروسات الجزئيّـة الكبيرة(Macro Viruses) البرمجة الجزئيـة الخاصة بتطبيق معيّن، مثل معالـج الكلمات، للبدء بنشاطها. وتضرب هذه النوعيّة من الفيروسات ملفات البيانات(مثل ملفات برامج وورد وإكسل وأكسس)، وتظل ساكنة أو مقيمـة في التطبيق نفسه عن طريق إصابة حقل التهيئة الخاص به. وعلى الرغم مـن أنّ الفيروسات الجزئية الكبيرة تصيب ملفات البيانـات، إلا أنّها عمومًا لا تعدّ من فيروسات الملفّـات، والسبب في ذلك أن فيروسات الملفّات قد تصيب البرامج وملفات البيانـات، بينما لا تصيب فيروسات الجزئية الكبيرة إلا ملفات البيانات فقط.

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

أنواع الفيروسات

- فيروسات البريد الإلكتروني: هي الفيروسات التي تنتقل بوساطة البريد الإلكتروني. فبإضافة بعض الوظائف (عن طريق الفيروس) لبرنامج مقدم خدمة البريد الإلكتروني القياسي (مثل أوتلوك (Outlook)) أصبح للفيروسات إمكانية الانتشار عبر العالم خلال ساعات فقط، بدلًا من شهور. ومن أشهر فيروسات البريد الإلكتروني فيروس ماليسا (Melissa) وماليسا ليس أول فيروس بريد إلكتروني، بل أول فيروس بريد إلكتروني انتشر بنجاح بصورة شرسة هو فيروس كريستما إكسك (Christma Exec) في خريف ١٩٨٧م[١]. لكن فيروس ماليسا هو أول فيروسات البريد الإلكتروني السّريعة التكاثر والانتشار، وكذلك الأول الذي صار معروفًا لشريحة واسعة من عامّة الناس. ويُعدُّ ماليسا من الفيروسات الجزئية الكبيرة، فبالإضافة إلى أنّه فيروس بريد إلكتروني، إلا أنه يمكن أن يرسل نفسه ذاتيًّا في شكل وثيقة مصابة بالفيروس.

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

أعراض الإصابة بالفيروسات

عندما يصاب جهاز الحاسب الآلي بفيروس فإنّه قد يظهر عليه بعض الأعراض الآتية:

- البطء الشديد: يعمل الحاسب الآلي ببطء ملحوظ، وتصبح سرعة البرامج المركبة عليه أبطأ من المعتاد، ومن ذلك أن نظام التشغيل يعمل ببطء شديد عند بداية التشغيل، أو عند إيقاف التشغيل، وقد يكون سبب هذا البطء هو النقص الشديد في الذاكرة العشوائية (RAM).
- تعليق (أو تجمد) الحاسب الآلي: يدخل الحاسب الآلي في حالة من الجمود وعدم الاستجابة لأيّ أمر؛ فلا يمكن في هذه الحالة تشغيل أيّ برنامج، أو حتى إيقاف عمل الجهاز.

البرامج الضارة – Malware
١- فيروسات الحاسب الآلي

أعراض الإصابة بالفيروسات

- انهيار الحاسب الآلي: في أغلب حالات انهيار الحاسب الآلي تظهر شاشة غريبة (كالشاشات الزرقاء في نظام التشغيل ويندوز)، وعندئذ يتوقف الحاسب الآلي عن العمل.
- إضاءة لمبة القرص الصلب بشكل عشوائي ومتّصل.
- زيادة أحجام الملفّات وزيادة الزمن اللازم لفتح الملفّات أو تشغيل البرامج.
- وجود بيانات تالفة كانت صالحة من قبل.
- ظهور رسائل خطأ، ومربعات حوار غير مألوفة وغير متوقعة.
- إعادة تشغيل الحاسب الآلي بشكل آلي ومستمر دون تدخل المستخدم.

البرامج الضارة – Malware
٢- ديدان الحاسب الآلي

دودة الحاسب الآلي (Worm Computer) هي عبارة عن برنامج مستقل بذاته، وله ملف خاص به. فالدودة تُعدُّ برنامجًا تطبيقيًّا متكاملًا يمكن أن يعمل لوحده، ولا يحتاج لأن يضيف نفسه لملف آخر، كما هي الحال في الفيروسات. ويمكن للدودة أيضًا أن تعمل بمفردها وتحمّل نفسها إلى ذاكرة الحاسب الآلي، وتبدأ بالعمل بشكل آلي.

البرامج الضارة – Malware
٢- ديدان الحاسب الآلي

من الفوارق الأصليّة، هي أن الديدان تستخدم الشبكات وروابط الاتصالات لكي تنتشر، وهي خلافًا للفيروسات لا تلتحم مباشرة بالملفّات القابلة للتنفيذ. وتصيب الديدان أجهزة الحاسب الآلي المرتبطة بشبكات الحاسب الآلي المصابة دون تدخل المستخدم أو قيامه باستثارتها كفتح ملف معين أو تشغيل برنامج، كما هي الحال في الفيروسات. فقد تنتقل إلى الجهاز بمجرّد تصفّح بعض مواقع الإنترنت، أو بمجرّد فتح بريد إلكتروني(إذا لم يكن الجهاز محميًا ببرنامج حماية محدّث) وهذا الأمر يجعلها تنتشر بشكل أسرع وأوسع من الفيروسات.

البرامج الضارة – Malware
٢- ديدان الحاسب الآلي

طُرُق انتشار الديدان

من أهم خصائص الديدان هي قدرتها على الانتشار والتكاثر عبر الاتصال بشبكات الحاسب الآلي، ومن أهم الطرق التي تنتشر بها الديدان ما يلي:

- مرفقات البريد الإلكتروني المصابة.
- التحميل التلقائي عند زيارة بعض مواقع الإنترنت التي من خلالها تنتشر الديدان، أو عند استخدام أحد الارتباطات داخل البريد الإلكتروني.
- التسلل عبر الثغرات الأمنيّة في أنظمة التشغيل أو برامج الحماية.

البرامج الضارة – Malware
٢- ديدان الحاسب الآلي

أضرار الديدان

- لا تقل أضرار الديدان عن الفيروسات من ناحية التلف، أو فقْد البيانات التي تسببها، ومن أهم أضرار الديدان ما يلي:
- تتيح للمهاجم أن يستخدم الحاسب الآلي المصاب لمهاجمة أجهزة أخرى، أو مواقع الإنترنت، أو إرسال بريد إلكتروني، أو تحميل برامج ضارّة إليه.
- يمكن من خلالها فتح باب خلفي (Back Door) في الجهاز المصاب، حيث يمكن التحكّم به من خلال ذلك الباب.
- يمكن للديدان أن تنسخ نفسها، وترسل نسخة إلى كل بريد إلكتروني في عناوين البريد المخزّنة في جهاز الحاسب الآلي المصاب.

البرامج الضارة – Malware
٣- برامج أحصنة طروادة

في مجال أمان الحاسب الآلي، يعرّف حصان طروادة بأنّه جزء من برنامج (كود) قابل للتنفيذ يؤدي بعض المهام لا يتوقعها المستخدم، ويقيم في البرنامج المصاب. وطروادة يمكن أن يوضع في برنامج بريء عند تأليفه وجمعه، أو يمكن إضافته للبرنامج بعد جمعه. وسبب تسمية هذا البرنامج الضار بهذا الاسم هو تشابه عمله مع أسطورة الحصان الخشبي الذي اختبأ به عدد من الجنود اليونانيين، وكانوا سببًا في فتح مدينة طروادة[١]. فبرنامج حصان طروادة هو برنامج ضار (الجنود)، مختبئ داخل برنامج بريء (حصان خشبي).

البرامج الضارة – Malware
٣- برامج أحصنة طروادة

إنّ مصطلح حصان طروادة يحمل في طيّاته دلالة سالبة جدًّا، بسبب وفرة أحصنة طروادة المنتشرة، التي صُمّمت بغرض إغراق أجهزة الكمبيوتر. وعلى الأقل يمكن لحصان طروادة ألا يكون أكثر من مجرد إزعاج، وفي أسوأ مراحله يمكن لحصان طروادة أن يدمّر بالكامل عمل الجهاز الذي يسكنه. وكمثال لحصان طروادة الذي يكون مجـرّد مصدر إزعاج هو "وحش خاصية الاسترجاع"، الذي يحثّ المستخدم على الدخول إلى الكلمة (cookie) بصورة دوريّة، بذاته)، الذي يتم نشره بواسطة مورد البرامج؛ ليرسل معلومات تتعلّق بالمستخدم لجهة تستغل هذه المعلومات بصفة غير شرعيّة. وبعض برامج حصان طروادة الماكرة تسجّل الضغطات على أزرار لوحة المفاتيح الخاصة بالمستخدمين وتحفظها في ملف مخفي يمكن من خلاله انتحال شخصية المستخدمين عند الحصول على ذلك الملف المخفي في وقت لاحق.

البرامج الضارة – Malware
٣- برامج أحصنة طروادة

عمومًـا يمكـن تقسيم برامـج حصان طـروادة إلـى تلك التـي تنتشر عـن طريق تغيير شيفرة (كود) المصدر (Source Code)، وتلك التي تنتشـر عن طريق إصابة الملف القابل للتنفيذ يدويًّا. وطريقة الانتشار السابقة تفترض أنّ لدى مؤلّف حصان طروادة لديه القدرة على تحوير شيفرة المصدر لكي تحتوي برنامج حصان طـروادة، وأنّ لديه القدرة بعد ذلك على جمـع البرنامج البريء ونشره، وهذا الخيـار لا يكون دائما ممكنًـا، ولذلك فإنّ مؤلفي أحصنة طروادة قد يلجؤون في بعض الأحيان لتحوير الملفّات الموجودة مسبقًا والقابلة للتنفيذ. والبرامج التي يجري تحويرها بهذه الطريقة هي البرامـج العامّة، التي توفّر بغرض تحميل برامج أخرى، أو برامج نظم التشغيل التي تكون في الجهاز محل الهجوم.

البرامج الضارة – Malware
٣- برامج أحصنة طروادة

تختلف أحصنة طروادة عن فيروسات وديدان الحاسب الآلي بأنها لا تتكاثر أو تتضاعف. ففيروسات الحاسب الآلي هي برامج تتضاعف عن طريق إصابة البرامج الأخرى، وتحتاج إلى استثارتها من قبل المستخدم لكي تنتشر، والديدان قد تصيب البرامج التنفيذية أو لا تصيبها، ولا تتطلّب عادة استثارتها من قبل المستخدم بصورة واضحة لكي تتضاعف، إلا أنّها تتضاعف وتنتشر بطريقة أسرع من الفيروسات. وقد ظهر الفرق بين الفيروس والدودة بمرور السنوات، لكن الفارق الرئيس بينهما وبين حصان طروادة هو أنّ هذا الأخير لا يتكاثر.

البرامج الضارة – Malware
مكافحة البرامج الضارة

بدأت تظهر في الآونة الأخيرة إصابات ليست فيروسيّة صرفة ولا دوديّة محضة، وإنّما خليط من تقنيات الفيروسات والديدان لكي تنتشر بصورة أسرع وأكثر نجاعة، و"رسالة حب" هي مثال لهذا التحول في تقنيات الإنتاج لهذه الآفات. وكذلك فإنّ "نيمدا" هو مثال للدودة، لكنه أيضًا ينتشر بطرق أخرى كثيرة؛ لذا يمكن عدّها فيروس بريد إلكترونيًّا في الوقت نفسه. وهذا التحول في التقنيات سيكون مشكلة إضافية في المستقبل، ويجب مراعاة ذلك في طُرُق الحماية المتبعة.

البرامج الضارة – Malware
مكافحة البرامج الضارة

يمكن مكافحة البرامج الضارّة باستخدام حزمة برامج واحدة لمكافحة كل من الفيروسات والديدان وأحصنة طروادة في آن واحد؛ لذا لا بدّ من تثبيت برنامج مكافحة جيّد وتحديثه دوريًّا لتوفير الحماية المطلوبة. ولا بدّ أن تشتمل برامج الحماية ليس فقط على كشف الإصابات فقط، وإنّما إزالتها أيضًا، وهناك عدّة برامج (أو حزم) مشهورة لمكافحة البرامج الضارّة يمكن الاعتماد عليها، ومن أشهرها:

- حزمة برامج مكافي (McAfee).
- حزمة برامج سيمانتك (Symantec).
- حزمة برامج كاسبر سكاي (Kasper SKY).
- حزمة برامج نورتون (NORTON).

البرامج الضارة – Malware
مكافحة البرامج الضارة

- وفي جميع الحالات لا بدّ من اتّباع الخطوات الآتية للحصول على مكافحة جيدة:
- تحديث برنامج المكافحة آليًّا ودوريًّا لضمان كشف الفيروسات والديدان وأحصنة طروادة الحديثة ومنعها.
- تحديث نظام التشغيل آليًّا ودوريًّا عن طريق تنشيط خاصية التحديث التلقائي لسد الثغرات الأمنيّة عند ظهورها.
- تحميل ملفات الإصلاح الأمنيّة الخاصة بأنظمة التشغيل وبعض البرامج التطبيقيّة الأخرى، (كحزمة برامج الأوفيس) التي تصدرها الشركات المصنّعة (كشركة مايكروسوفت) بشكل مستقلّ لسدّ ثغرة أمنيّة خاصّة لم يتم سدها من خلال التحديث التلقائي، وكذلك تحميل حزم الخدمة (Service Pack) الجديدة حال ظهورها.
- عدم فتح مرفقات البريد الإلكتروني التي لها الامتدادات التشغيليّة مثل: (scr) (exe) (vbs)، أو التي لها أكثر من امتداد مثل (txt.vbs).

البرامج الضارة – Malware
مكافحة البرامج الضارة

- ويمكن أن تعمل برامج المكافحة بإحدى الطرق الآتية أو جميعها:
- باستخدام جدول زمني معيّن يحدّد من خلاله عمل برنامج المكافحة؛ ليبدأ بفحص جميع مكوّنات الجهاز عند أوقات محدّدة (عند منتصف الليل من كل يوم مثلًا).
- عند الطلب من قبل المستخدم، ويمكن أن يكون ذلك في أيّ وقت.
- عند تشغيل البرامج أو فتح الملفّات أيًّا كان نوعها، وفي هذه الحالة يفحص برنامج المكافحة الملف المراد فتحة قبل أن تتم عمليّة الفتح الفعليّة؛ للتأكد من خلوّه من الفيروسات والديدان وأحصنة طروادة، ومن الأفضل تفعيل جميع هذه الطرق لتوفير حماية أفضل وأشمل.

برامج التجسس

لقد عُرفت فيروسات الحاسب الآلي بصورة موسعة في أواخر الثمانينيّات. فهي كائنات غريبة ولافتة للنظر، وفي كل مرة يوجّه الفيروس ضرباته يكون هو موضوع الأخبار، خاصّة إذا انتشر بسرعة. وخلال السنوات القليلة الماضية ظهرت فئة جديدة من البرامج الماكرة هي برامج التجسّس، وبرنامج التجسّس ليس بفيروس، لكن فعله أقوى وأخطر من الفيروسات والديدان وأحصنة طروادة. فبالرغم من عدم تسببه في تلف البيانات، إلا أنه يفعل فعله من وراء الكواليس بكل هدوء، ودون علم المستخدم، وينقل المعلومات لمالكه. وبرنامج التجسّس هو عبارة عن خدعة ماكرة، مثله في ذلك مثل الفيروس، لكنه عمومًا أقل شهرة.

برامج التجسس

على الرغم من الجدل الذي يكتنف تعريف برنامج التجسّس الدقيق، إلا أنّه في النهاية كائن(إلكتروني) يتجسّس عليك، ونتيجة لذلك يتركز الجانب المهم من موضوع برنامج التجسّس عادةً حول مسألة الخصوصيّة. ويُعدُّ تعريف ويبوديا[٢] لبرنامج التجسّس أفضل التعريفات الموجودة، حيث عرّفه بأنه: «أيّ برنامج يحصل –سرًّا– على معلومات عن المستخدم عن طريق الربط بالإنترنت، وخاصة بدعاوى دعائية وإعلانية». عادةً ما يتم تضمين برامج التجسّس في شكل مكوّنات مجانيّة خفية، أو برامج مشاركة يمكن تنزيلها من شبكة الإنترنت، وبمجرّد تركيب برنامج التجسّس يبدأ بمراقبة حركة المستخدم على الإنترنت، وينقل المعلومات من وراء الكواليس لجهة أخرى.

برامج التجسس

أنواع برامج التجسّس

كما رأينا في تعريف برامج التجسّس، فهي برامج خطيرة تتسلل إلى الحواسيب وتعرف المعلومات الخاصة والسِّريّة المخزّنة بها، وربما ترسلها إلى أجهزة أخرى بمجرد توفر خط الاتصال، وبناءً على طريقة عملها، يمكن تصنيف برامج التجسّس إلى نوعين رئيسين: برامج رصد وتسجيل، وبرامج تتبع.

برامج التجسس

أنواع برامج التجسّس

النوع المعروف من برامج الرصد والتسجيل هو مسجل أو راصد المفاتيح (من لوحة المفاتيح) وحركات الفأرة. فهو يعمل في صمت في الخلف ويقوم بتسجيل ضغطات المفاتيح وحركات الفأرة لكي يعيد ترتيب وتكوين ما يفعله المستخدم، وهـذه الطريقة شديدة الخطورة، إذ يمكن من خلالها معرفة الأرقام السِّريّة أو الأرقام الخاصة التي يُدخلها المستخدم عبر لوحة المفاتيح. وخلافًا لراصد عمل المفاتيح، هناك أيضًا راصدات ومسجلّات للبريد الإلكتروني والدردشة. وراصدات عمل المفاتيح مشهورة؛ لأنّها هي أكثر الأنواع شيوعًا وإزعاجًا في عمليّة سرقة كلمات السر وأرقام بطاقات الائتمان.

برامج التجسس

أنواع برامج التجسّس

أمّا المتتبّعات فتراقب عادات الاستخدام وأنماطه وتخزّنها كبيانات إحصائيّة بهدف إعداد التقارير بناءً عليها. وقد تكون البيانات عبارة عن عادات التصفح للشخص المستهدف، مثل استخدام برنامج معيّن أو خاصية محدّدة في ذلك البرنامج. ويتم تجميع هذه المعلومات عن الشخص الضحية ثم تحليلها واستخدامها في الهجوم عليه أو سرقة معلوماته.

برامج التجسس

أعراض وجود برامج التجسّس وطرق انتقالها

بما أنّ برامج التجسّس تعمل على جمع المعلومات الخاصة بالحاسب الآلي ومستخدمه، وإرسالها إلى مواقع أو أجهزة أخرى، فإنّ الأمر يتطلب القيام بأعمال إضافية غير التي يقوم بها المستخدم، ولهذا تظهر لها بعض الأعراض، ومنها:

- نشاط أعلى من الحد المعتاد: ويتضح ذلك أكثر عندما يرسل الحاسب الآلي ويستقبل كميّات كبيرة من البيانات عبر الشبكة أو الإنترنت، في حين أن المستخدم لا يستخدم أيّ برامج تستوجب ذلك، ويمكن ملاحظة ذلك عن طريق مراقبة عمل جهاز المودم وعرض كميّة البيانات التي أرسلها واستقبلها.
- طلب الاتصال بالإنترنت تلقائيًا: وتظهر هذه الحالة في الأجهزة التي لا يوجد بها جهاز مودم (Digital Subscriber Line-DSL)، حيث يشغّل برنامج التجسّس طلب الاتصال الهاتفي من أجل الارتباط بالإنترنت.
- ظهور أشرطة أدوات غير مألوفة تُضاف إلى متصفّح الإنترنت.

برامج التجسس

أعراض وجود برامج التجسّس وطرق انتقالها

- اختيار صفحة بداية لمتصفّح الإنترنت خلاف الصفحة التي تم ضبط المتصفّح عليها من قبل المستخدم.

ومن أشهر الطرق التي تنتقل بها برامج التجسّس طريقتان، هما:

- تظهر كأنها برامج عادية حتى يتم تثبيتها من قبل المستخدم وبعلمه.
- الاختفاء في برامج أخرى، بحيث يجري تثبيتها مع هذه البرنامج دون علم المستخدم.

برامج التجسس

مكافحة برامج التجسّس

من أخطر ما تفعله برامج التجسّس هو أنها تُزيل برامج مكافحة التجسّس. ويمكن القول إنّه ليس هناك برنامج يحمي من برامج التجسّس بدرجة كاملة، لكن يمكن أخذ بعض التدابير الوقائية، ومنها:

١- فلاتر خصائص استرجاع البيانات

٢- حاجبات الإعلانات والنوافذ المنبثقة (Pop-UP Blockers)

٣- استخدام مضادات برامج التجسّس (Antispyware Scanners)

٤- استخدام جدار النار الشخصي وبرامج كشف التطفل

٥- تأمين متصفّح الإنترنت

٦- تأمين إدخال كلمات المرور