بسم الله الرحمن الرحيم

جامعة السودان للعلوم والتكنولوجيا

كلية الهندسة – قسم العلوم العامة

اساسيات الحاسوب

الباب الرابع – الجزء الثالث

امن الشبكات

د. عصام عبدالنبي عثمان

أمن الشبكات Network Security

إن طبيعة الشبكات كشبكة الانترنت مثلا تجعلها ضعيفة أمام محاولات المخربين للوصول إلي هذه الشبكة وحواسيب مستخدميها سواء كانوا هولاء المستخدمين مستقلين أو أعضاء في شبكة خاصة.

تم تصميم شبكة الانترنت بطريقة تسمح بأكبر تبادل حر للمعلومات, وقد نجحت في ذلك علي نحو مذهل, غير إن لهذه الحرية ثمن باهظ أحيانا يدفعه مستخدمو هذه الشبكة من خلال قيام المخربين باستغلال ضعف نظم الحماية وعموميتها بالقيام بانتهاك خصوصية الآخرين في محاولة لتعطيل وإتلاف قواعد البيانات الخاصة بالشبكة، وتسبيب الأذى للبيانات والموارد المتاحة في الشبكات الخاصة المرتبطة بالانترنت.

أمن الشبكات Network Security

في عام 1988 قام احد طلبة جامعة "كورنيل" ببث برنامج خبيث عبر شبكة الانترنت أدي إلي توقف معظم عمليات التراسل عبر الشبكة ولعدة أيام ومنذ ذلك الحين دق ناقوس الخطر مؤكدا للمعنيين بأمور الشبكة ضرورة تصميم طرق لحمايتها ولحماية الرسائل المتبادلة من خلالها من العابثين المنتشرين في دول عديدة تغطيها خدمات شبكة الانترنت ولا تعتبر جرائم الحاسوب في كثير منها جريمة يعاقب عليها القانون.

هذه الثغرات الأمنية التى تشكو منها سواء البروتوكولات المستخدمة أو نظم الخدمات التي توفرها دفع البعض إلي اقتراح ضرورة إعادة هندسة هذه الشبكة لتامين قاعدة أمنية اقوي, إلا انه مقترح يستحيل تطبيقه بسبب وجود استثمارات هائلة في التجهيزات والبرمجيات المبنية والمصممة علي أساس البنية الحالية للشبكة. عندها تركزت الجهود علي ايجاد حلول جزئية تهدف إلي التغلب علي بعض الثغرات الأمنية وتوفر القدر الكافي من الحماية مع الحفاظ علي البنية الحالية للشبكة.

جرائم الانترنت

من المعروف إن جرائم الانترنت ترتبط بالسرقة والاحتيال وتغيير وحذف المعلومات وتعطيل وتخريب الأجهزة. وينطبق نموذج امن المعلومات العالمي ذو الأبعاد الثلاثة على شبكة الانترنت كأي شبكة للمعلومات والنموذج يحوي ثلاثة ابعاد هي:

1. **سرية البيانات:**

وهي ضمان تخزين البيانات والمعلومات بسرية بالاجهزة أو عند نقلها عبر الشبكة.

2. **سلامة البيانات:**

هو ضمان عدم تغيير أي بيانات في المعلومات المخزنة بالأجهزة أو المنقولة عبر الشبكة.

3. **وجود البيانات:**

هو ضمان عدم حذف المعلومات المخزنة بالأجهزة أو المنقولة عبر الشبكة وعدم الإطلاع عليها بأي نوع من أنواع التطفل.

أهم جرائم الانترنت

- **انتحال الشخصيات:**

تتميز هذه الجريمة بسرعة انتشار ارتكابها وتتمثل في استخدام هوية شخصية أخرى بطريقة غير شرعية إما للاستفادة من تلك الهوية أو لإخفاء هوية شخصية المنتحل لتسهيل ارتكاب جرائم أخرى.

- **تعطيل الأجهزة**

يقوم مرتكبو هذه الجرائم بتعطيل الأجهزة أو الشبكات عن تأدية عملها بدون إن تتم عملية اختراق فعلية لها عن طريق إرسال رسائل بطرق معينة إلى الأجهزة أو الشبكات لتعطيلها عند تأدية عملها.

أهم جرائم الانترنت

- **إساءة وتشويه السمعة:**

وهى عبارة عن نشر المجرم لمعلومات سرية أو مضلله عن ضحيته، والذي قد يكون فردا أو مجتمع أو دين أو مؤسسة تجارية أو سياسية.

- **رصد لوحة المفاتيح:**

يعتبر اخطر مصادر التهديد الأمني حيث يتم فية رصد أي ضغطة على لوحة المفاتيح ثم رصد كل مايتم كتابته على لوحة المفاتيح خاصة اسم المستخدم وكلمة المرور وذلك حتى قبل إن يتمكن جهازك من إخفاء وتشفير الكلمة.

هنالك جرائم أخرى كثيرة مثل النصب والسرقة والاحتيال وصناعة ونشر الفيروسات والاختراق.

اخطار الانترنت – البرامج المهددة للأمن

في الانترنت برامج الهجوم على الأجهزة وشبكات الكمبيوتر والتجسس وحتى وقت قريب كان تصنيف هذه البرامج ينقسم إلى الفيروسات وديدان الانترنت وأحصنة طروادة، لكن مع تطور البرامج تم تحديث طريقة تصنيف البرامج إلى:

- **البرامج سريعة التكاثر والانتشار**

منها الفيروسات وديدان الانترنت القادرة على التكاثر والانتشار بسرعة، والفرق بين الفيروسات والديدان هو أن الفيروس بحاجة إلى برنامج يحتضنه ليتمكن من التكاثر والانتشار عن طريقه، أما الديدان فليست بحاجة إلى برنامج لاحتضانها.

اخطار الانترنت – البرامج المهددة للأمن

- **برامج التجسس والإرسال**

تقوم بجمع معلومات يريدها اللصوص وتقوم بإرسال المعلومات إلى مصدر البرنامج حتى ولو كان هناك جدران نارية تحمي الجهاز وذلك لقدرة هذا النوع على استغلال نقط ضعف جدران النار التي تسمح بخروج وتصدير المعلومات من الجهاز أو الشبكة المحلية بواسطة بروتوكول HTTP أو بروتوكول FTP.

- **برامج التحكم عن بعد**

تسمح هذه البرامج في حال وصولها إلى جهاز بالتحكم الكامل بالجهاز أو القدرة على التحكم عن بعد وتستطيع تسخير الأجهزة لتنفيذ الهجوم المنسق وتعطيل عمل المواقع المشهورة.

اخطار الانترنت – البرامج المهددة للأمن

- **أحصنة طرواده الجديدة**

وهو نوع من أنواع أحصنة طرواده ويعتبر من اخطر أنواع أحصنة طرواده إذ تستفيد من ميزات كل أنواع البرامج السابقة عن طريق الدمج بين خصائص مثل تكاثر الفيروسات وعدم الحاجة إلى برنامج محتضن كالديدان ولديها القدرة على التعامل مع الملفات الصادرة أو الواردة من نوع FTP ونوع HTTP مثل برامج التجسس وخداع جدران النار، وتجمع معلومات كلمات السر وأسماء المستخدمين وأرقام بطاقات الائتمان كما يمكنها تدمير ملفات وتعديل مهامها.

الأمن على شبكة الانترنت

جميع ما ذكرناه من قبل سببه الوحيد هو عدم الاكتراث بمبادئ الأمن وضعف الإجراءات الأمنية، ولكن الأمور الآن أصبحت أكثر صعوبة أمام المخترقين والمتطفلين خاصة بعدما تم سن قوانين تجرم من يقوم بتلك الأفعال وتطور مستوى البحث والتحري لتتبع اثر المجرمين على الشبكة.

إن هدفنا جميعا هو الحصول على المعلومات من شبكة الانترنت ونقلها بشكل امن لذا كان علينا الالتزام بمجموعة من الأساسيات التي يجب أخذها في الحسبان لضمان تحقيق **مبدأ الأمن** و تنحصر في الآتي:

1. **خصوصية المعلومات.**
2. **التحقق من هوية الأطراف الأخرى.**
3. **عدم الانكار.**
4. **سلامة المعلومات.**

نصائح لتقوية امن الانترنت

- إذا كنت متصل بالانترنت بطريقة سريعة كالخطوط الرقمية فلابد من برنامج متخصص للحماية والسبب هو حصولك على رقم IP ثابت مخصص لك مما يسهل عملية تتبعك على الانترنت.
- إذا كنت تستخدم موديم للاتصال بالانترنت فان مزود الخدمة لا يخصص لك رقم IP محدد ولكنك تتحصل على رقم مختلف كلما قمت بالاتصال على الشبكة، أما لو كنت تمتلك شبكة من أجهزة الكمبيوتر المتصلة مع بعضها البعض وجهازك يعتبر جزء من هذه الشبكة المتصلة بالانترنت فانك بحاجة فورية لبرنامج حماية متخصص **(جدار ناري)** وذلك لان المخارج المخصصة لمشاركة الملفات تكون مفتوحة وجاهزة لأي هاكر.

نصائح لتقوية امن الانترنت

- حاول أن تنزل أحدث إصدار للمتصفح وذلك لان الإصدارات القديمة بها العديد من الثغرات الأمنية والتي تجعل منك هدفا سهلا وطبعا إذا كنت ممن يشترون من خلال الشبكة احصل على نسخة مدعومة بقوة تشفير 128bit.
- احم جهازك بكلمة مرور تمنع الآخرين من الدخول إلى جهازك، فيمكنك وضع كلمة عبور على جهازك ولا يتمكن اي احد غيرك من تشغيل أو استخدام الجهاز إلا بعد كتابتها، أما مستخدمي windows فيمكنهم التمتع بميزة كلمة العبور، وهناك أيضا كلمة عبور يمكن وضعها إذا كنت تريد الاتصال بشبكة معينة حيث لايتم الاتصال إلا بعد إدخالها.

الحلول المطروحة لتأمين الشبكات

نسبة لازدياد المشاكل المتعلقة بتأمين الشبكة كان لابد من البحث عن حلول لهذه المشاكل، ومن بين هذه الحلول :

- **الجدار الناري (Firewall):**

الذي يعمل كخط دفاع أول في الشبكة للتحكم في مرور البيانات من والي الشبكة المحمية.

- **التشفير (Cryptography):**

تشفير المعلومات بواسطة خوارزميات معينة حتى لا تفهم وأدت هذه الطرق إلى توفير بعض الحماية والأمن للشبكة، وبالرغم من هذه الحلول إلا أن الحماية الكافية للشبكة لم تتوفر بالمستوى المطلوبة حتى الآن.

التشفير Cryptography

التشفير أو (التعمية) استخدم في الحضارات القديمة لإخفاء المعلومات والمراسلات مثل الحضارة الفرعونية والدولة الرومانية.

التشفير كعلم مؤسس منظم يدين بولادته ونشأته للعلماء الرياضيين واللغويين العرب إبان العصر الذهبي للحضارة العربية ومن أشهرهم الفراهيدي والكندي, وقد ألف هؤلاء العلماء مفاهيم رياضية متقدمة من أهمها التوافيق والتباديل.

كذلك توظيف الكندي ومن تبعه مفاهيم الإحصاء والاحتمالات في كسر الشفرة, وقد سبقت هذه الكتابات كتابات باسكال وفيرما بحوالي ثمانية قرون.

التشفير Cryptography

شاع في أيامنا استخدام مصطلح "التشفير" ليدل على إخفاء المعلومات، ولكن كلمة "التشفير" وافدة من اللغات الأوربية وهذه بدورها جاءت أصلا من اللغة العربية ولكن **(Cipher)** بمعنى آخر لكلمة" الصفر".

فكما هو معلوم أن العرب قد تبنوا مفهوم الصفر والخانات العشرية واستخدموه في الحساب, وهو ما لم يكن الأوربيون يعرفونه في القرون الوسطى , وكان مفهوم الصفر جديدا وغريبا لدرجة أنهم أخذوه بنفس الاسم فأسموه "Cipher" ولأن مفهوم الصفر الجديد كان في منتهى التعقيد والغموض فقد صاروا يستخدمون كلمة "Cipher" للدلالة على الأشياء المبهمة وغير الواضحة.

التشفير Cryptography

ومن هنا تطور استخدام كلمة "Cipher" في جميع اللغات الأوربية تقريبا لتعني إخفاء المعلومات وقمنا نحن العرب بعد ستة قرون بإعادة بضاعتنا الأصلية ولكن بمعنى مختلف فنحتنا كلمة غريبة على اللغة العربية هي التشفير.

يُعرَّف التشفير بأنه عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المُرخَّص لهم من الإطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفَّرَة و من المعلوم أن الإنترنت تشكِّل في هذه الأيام الوسطَ الأضخم لنقل المعلومات.

التشفير Cryptography

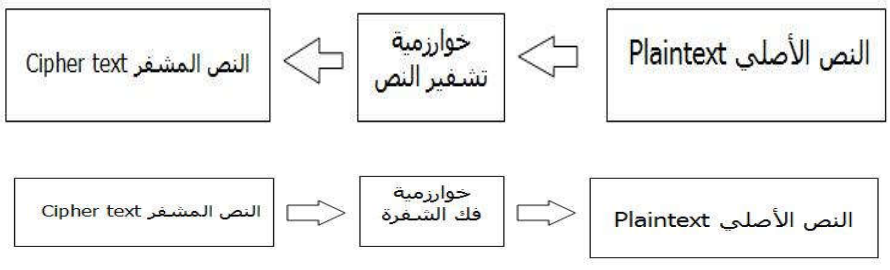
من الضروري نقل المعلومات الحساسة (مثل الحرَكات المالية) بصيغة مشفَّرة إن أُريدَ الحفاظ على سلامتها وتأمينها من عبث المتطفلين والمخربين واللصوص، وتُستخدَم المفاتيح في تشفير (encryption) الرسالة وفك تشفيرها (decryption) وتستنِد هذه المفاتيح إلى صِيَغ رياضية معقَّدة (خوارزميات).

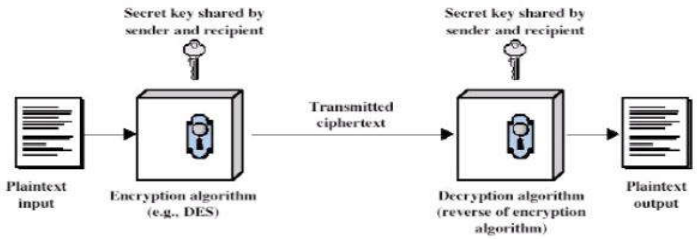
تعتمد قوة وفعالية التشفير على عاملين أساسيين:

1. **الخوارزمية**
2. **طول المفتاح (مقدَّرا بالبت (bits))**

من ناحية أخرى، فإن فك التشفير هو عملية إعادة تحويل البيانات إلى صيغتها الأصلية، وذلك باستخدام المفتاح المناسب لفك الشفرة كما مبين في الشكل التالي:

التشفير Cryptography





مثال على التشفير Cryptography

نأخذ على سبيل المثال كلمة **Arab** الخطوات أو الخوارزمية لتشفير تلك الكلمة نجعل كل حرف يساوي الحرف الذي يليه أي أن:

A = B
R = S
A = B
B = C

وفي هذا المثال النص الأصلي **Plaintext** هو **Arab** والنص المشفر هو **BSBC** وبذلك قد أخفينا النص الأصلي وعندما تصل إلى الطرف الثاني فإنه يقوم بعكس التشفير أي أننا نجعل كل حرف يساوي الحرف السابق, وبذلك نكون قد حصلنا على النص الأصلي.