مقدمة في

الشبكات اللاسلكية

إعداد/ بهاء بن يوسف حلواني

جدول المحتويات :

تمهيد:

الحمد لله وحده، والصلاة والسلام على من لا نبي بعده، وبعد:
تمثل الشبكات اللاسلكية المحلية تقنية واسعة الانتشار، نظراً لما تقدمه من دعم لجميع الميزات التي تقدمها الشبكات السلكية التقليدية، وأصبح اليوم للشبكات اللاسلكية قواعدها ومعاييرها التقنية التي ساهمت في استقرار هذه التقنية وبالتالي الاعتماد عليها في الإنتاج في مختلف بيئات الأعمال، وخصوصاً مع سهولة استخدامها وأسعار نقاط الوصول (Access Point) المنخفضة، بالإضافة لدعم الشبكات اللاسلكية في معالجات الأجهزة المحمولة واتساع انتشار هذه التقنية، حيث لا يكاد يخلو منزل أو منشأة من نقاط الوصول للشبكات اللاسلكية.

وبقدر الانتشار لهذه التقنية بقدر ما تزيد أهمية العناية بتطبيق الإجراءات الأمنية لحماية الشبكات اللاسلكية، وإهمال هذا الجانب قد يعرض بيانات المستخدم والأنظمة المتصلة بالشبكة اللاسلكية لمخاطر كبيرة من المخترقين والمتسللين إلى داخلها.

لذلك كان لابد من معرفة ماهية الشبكات اللاسلكية ؟ و ما هي مكوناتها ؟ وكيف تعمل ؟ وكيف نحميها ؟ وأي طرق الحماية هي الأفضل ؟ مع بعض النصائح المهمة لحماية الشبكات اللاسلكية بشكل عام.

مقدمة في الشبكات اللاسلكية:

اكتسبت الشبكات اللاسلكية - التي تكتب بالإنجليزية اختصارا (WLAN) – و أحيانا يطلق عليها اسم (Wi-Fi) زخما لأسباب كثيرة أهمها سهولة تركيبها و المرونة التي تمتاز بها، يضاف إلى ذلك رخص تكاليف إنشائها و صيانتها، و سهولة توسعتها عند الحاجة، و تشير دراسة أعدتها مجموعة (Gartner) البحثية إلى أنه بحلول عام ٢٠٠٦م فإن أكثر من نصف الحاسبات المحمولة ستكون مزودة بالعتاد اللازم للاتصال بالشبكات اللاسلكية، و لكن دلائل الواقع تشير إلى أن نسبة الحاسبات المحمولة المزودة بالعتاد اللازم للاتصال بالشبكات اللاسلكية تفوق بكثير ما ورد في هذه التقديرات الواردة في تلك الدراسة. و مما يؤيد ما ذهبنا إليه أنه ابتداء من عام ٢٠٠٤م أحدث معهد أمن الحاسوب في الولايات المتحدة الأمريكية قسما خاصا بالمشكلات الأمنية للشبكات اللاسلكية في التقرير السنوي الذي يعده مشاركة مع مكتب التحقيقات الفدرالي.

وتعود نقطة الانطلاق الحقيقة للشبكات المحلية اللاسلكية إلى العام ١٩٩٧م الذي شهد ولادة مواصفات (IEEE 802.11) التي تعد أول مواصفات قياسية لهذا النوع من الشبكات، و كأي بداية كانت قدراتها متواضعة من حيث قدرتها على تمرير المعلومات إذ لم تتجاوز ٢ مليون نبضة في الثانية. كما أنها كانت تعمل في نطاق ترددي قدره ٢،٤ ميجاهرتز و هذا يجعلها عرضة للتداخل مع بعض الأجهزة التي تعمل في النطاق نفسه مثل بعض أجهزة المايكروويف و الهواتف المنزلية النقالة، و لتلافي هذه العيوب توالى صدور المواصفات القياسية.

المعايير القياسية للشبكات اللاسلكية:

ثلاثة أجيال من المعايير القياسية للشبكات اللاسلكية ظهرت حتى الآن ، وهي على التسلسل الزمني802.11g,802.11a,802.11b وكان التركيز على سرعة أكبر لنقل البيانات ، و لم تأخذ هذه الأجيال الثلاثة الموضوع الأمني بشكل كافي مما ساعد على كون الشبكات اللاسلكية عرضة أكثر للتهديدات الأمنية. IEEE وهي الجمعية العلمية المصدرة لهذه المعايير القياسية تعمل على إصدار معيار قياسي جديد خاص بأمن الشبكات اللاسلكية و هو 802.11i و التي لم تغطها المعايير.

اسم المواصفة القياسية	سرعة نقل البيانات	النطاق الترددي الذي تعمل فيه	المزايا	العيوب
IEEE 802.11a	54 مليون نبضة/الثانية	5 جيجا هرتز	• تدعم التطبيقات التي تحتاج وسيلة نقل كبيرة السعة مثل تطبيقات الوسائط المتعددة كملفات الصوت و الصورة • أقل عرضة للتداخل الكهرومغناطيسي من المواصفات الأخرى	• مدى عمل الشبكة قصير و بالتالي فإن إنشاء الشبكة يحتاج عددا أكبر من نقاط الدخول مقارنة بباقي المواصفات • توفر 8 قنوات فقط داخل الشبكة اللاسلكية • لا تستطيع العمل مع الأجهزة المتوافقة مع المواصفة القياسية IEEE 802.11b
IEEE 802.11b	11 مليون نبضة/الثانية	2.4 جيجا هرتز	• مدى عمل الشبكة طويل و بالتالي فإن إنشاء الشبكة يحتاج عددا أصغر من نقاط الدخول مقارنة بالمواصفة القياسية IEEE 802.11a • توفر 14 قناة داخل الشبكة اللاسلكية	• قدرتها محدودة على تشغيل التطبيقات التي تحتاج وسيلة نقل كبيرة السعة مثل تطبيقات الوسائط المتعددة كملفات الصوت و الصورة • عرضة للتداخل الكهرومغناطيسي • لا تستطيع العمل مع الأجهزة المتوافقة مع المواصفة القياسية IEEE 802.11a
IEEE 802.11g	54 مليون نبضة/الثانية	2.4 جيجا هرتز	• مدى عمل الشبكة طويل و بالتالي فإن إنشاء الشبكة يحتاج عددا أصغر من نقاط الدخول مقارنة بالمواصفة القياسية IEEE 802.11a • توفر 14 قناة داخل الشبكة اللاسلكية	• عرضة للتداخل الكهرومغناطيسي • لا تستطيع العمل مع الأجهزة المتوافقة مع المواصفة القياسية IEEE 802.11a

مكونات الشبكة اللاسلكية:

إن الشبكة المحلية اللاسلكية هي البساطة ذاتها، فهي تتألف من مكونين لا غير:

١) بطاقة الاتصال اللاسلكي: تثبت هذه البطاقة في الحاسوب أو أي جهاز نرغب أن يكون عضوا في الشبكة اللاسلكية كالطابعات مثلا، وكما مر معنا فإن معظم الحواسيب المحمولة تأتي مزودة بهذه البطاقة من مصنعها، أما الحواسيب المحمولة غير المزودة بالبطاقة أو الأجهزة الأخرى فلا بد من تزويدها بها لتكون قادرة على الاتصال، و في الشكل رقم (١) أحد أنواع كروت الاتصال اللاسلكي الذي يمكن استخدامه في الحواسيب المحمولة.

الشكل رقم (١):: بطاقة الاتصال اللاسلكي

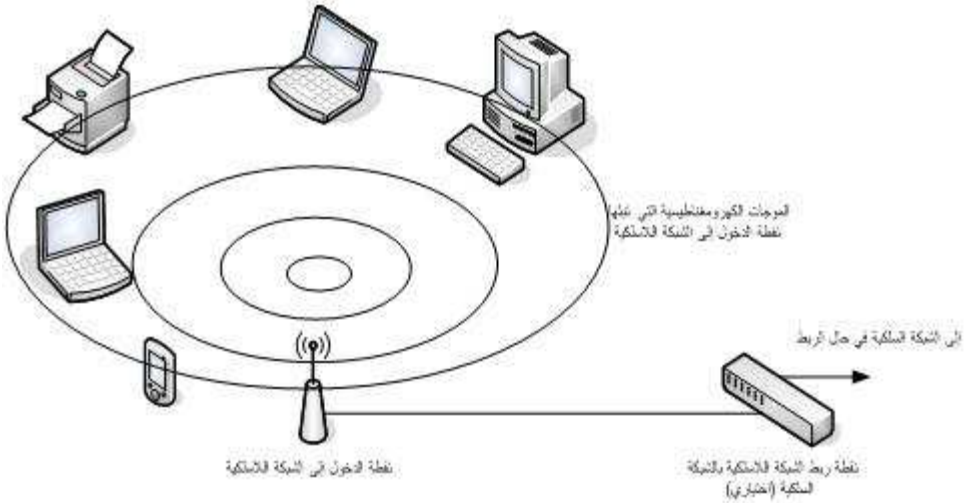
ودور بطاقة الاتصال تمرير البيانات جيئة و ذهابا بين الحاسوب و الشبكة اللاسلكية، فهي نقطة الوصل بين الطرفين.

٢) نقطة الدخول إلى الشبكة: وهذه تسمى (Access Point) و هي عبارة عن جهاز صغير به هوائي صغير كما في الشكل رقم (٢) ،و يبث الجهاز الموجات الكهرومغناطيسية لنقل البيانات بين نقطة الدخول و الأجهزة المزودة ببطاقات الاتصال بالشبكة اللاسلكية

السابق ذكرها في الفقرة السابقة، و بعمل هذه النقطة مع الأجهـزة يتألف لدينا شبكة لاسلكية كما في الشكل رقم (٢).

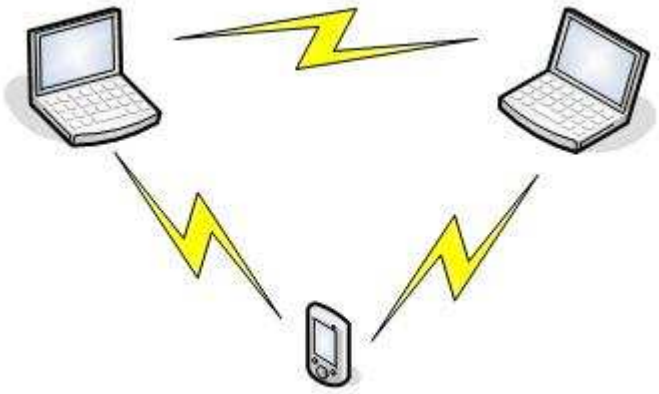
الشكل رقم (٢)

وفي معظم الأحيان نرغب في أن نـربط الـشبكة اللاسـلكية بـشبكة المعلومات الأم في المنشأة، أو بشبكة الإنترنت، و يتحقق هذا بربط نقطة الدخول بالشبكة الأم أو شبكة الانترنـت، و بهـذا يمكـن كـل جهاز في الشبكة اللاسلكية الاتـصال بالـشبكة الأم أو الـدخول إلـى شبكة الإنترنت كما يمكن للمستخدمين فـي الـشبكة الأم أو شـبكة الإنترنت الوصول إلى الأجهزة التي تؤلف الشبكة اللاسلكية.



الشكل رقم (٣): شبكة لاسلكية مزودة بنقطة دخول

كما نستطيع تكوين شبكة لاسلكية دون استخدام نقطة دخول إلى الشبكة، وفي هذه الحال فإن كل ما نحتاجه هو أجهزة مزودة ببطاقات اتصال لاسلكي، و يكون شكل الشبكة كما في الشكل رقم (٤).



الشكل رقم (٤):: شبكة لاسلكية بسيطة (بدون نقطة دخول)

كيف تعمل الشبكة اللاسلكية :

كما أن مكونات الشبكة المحلية اللاسلكية بسيطة فكذلك طريقة عملها، وذلك أنه بعد إيصال الطاقة إلى نقطة الدخول إلى الشبكة و الأجهزة المزودة ببطاقة الاتصال اللاسلكي ووضع الجميع في وضع التشغيل يحدث ما يلي:

١) ترسل نقطة الدخول إلى الشبكة نبضات إليكترونية على فترات منتظمة معلنة عن نفسها،

٢)تلتقط الأجهزة هذه النبضات التي تحوي في طياتها معلومات مهمة تساعد الأجهزة على الاستجابة و تهيئة نفسها للاتصال، ومن أهم هذه المعلومات ما يعرف باسم (Service Set Identifier) الذي يعرف اختصارا باسم (SSID)، وهو ما يميز شبكة لاسلكية عن أخرى.

٣) كما تحوي النبضات المشار إليها القناة التي ستعمل عليها الشبكة اللاسلكية.

و لحماية الرسائل المتبادلة داخل الشبكة اللاسلكية تشفر باستخدام نظام تشفير يعرف اختصارا باسم (WEP)، و لكن نظام التشفير هذا يعاني من نقاط ضعف عدة يمكن للمهاجم النفاذ من خلالها و تهديد الشبكة اللاسلكية.

نقاط ضعف الشبكات اللاسلكية :

للشبكات المحلية اللاسلكية عدد كبير من المزايا مما يضفي عليها تتميز جاذبية يصعب مقاومتها، و لن نجاوز الحقيقة إذا قلنا أن هذه الجاذبية هي وراء كثير من نقاط الضعف التي يعاني منها هذا النوع من الشبكات، وذلك لأن كثيرين يندفعون إلى تركيب شبكات لاسلكية سواء في محيط عملهم أو في منازلهم دون أن يكون لهم أدنى دراية بكيفية عمل الشبكات و الطريقة الصحيحة لتهيئتها، و هذا يقود حتما إلى إنشاء شبكات غير آمنة. و بحسب نسخة عام ٢٠٠٤م من التقرير المشترك الذي يصدره في الولايات المتحدة الأمريكية كل من معهد أمن الحاسوب و مكتب التحقيقات الفدرالي فإن١٥% من الجهات التي شملتها الدراسة التي يستند إليها التقرير أفادت بأن شبكاتها اللاسلكية تعرضت لهجمات. كما تشير بعض التقديرات إلى أن مابين ٤٠% و ٥٠% من الشبكات اللاسلكية إما أن مستوى الحماية فيها ضعيف أو أنه لا يوجد فيها أي نوع من الحماية على الإطلاق.

و مما ينبغي التأكيد عليه أن كثيرا من هذه الهجمات يمكن عملها باستخدام معدات و برامج متوفرة بأسعار في متناول كثير من الناس.

يمكن إجمال أهم نقاط ضعف الشبكات اللاسلكية المتعددة في الآتي:

١) بسبب سهولة تركيب و تشغيل الشبكات اللاسلكية فإن كثيرا ممن ينصب و يشغل هذه الشبكات هم من الأشخاص الذين ليس لهم درية كافية بأمن المعلومات، و بالتالي فإنهم – في كثير من الأحيان – لا يعرفون كيف يهيئون الإعدادات - خاصة المتعلقة بأمن الشبكة – بشكل صحيح فيتركون ثغرات أمنية كبيرة في الشبكات اللاسلكية التي أقاموها. ومن أمثلة ذلك ترك قيمة (SSID) الأصلية دون تغيير مما يسهل على المهاجم الاشتراك في الشبكة اللاسلكية. و إذا كانت المنشأة لا تملك سياسات تحدد ما يمكن و مالا يمكن عمله فيما يتعلق بأمن المعلومات فإنه كثير ما يقوم الموظفون بتركيب

شبكات لاسلكية دون علم الجهة المسؤولة عن تقنية و أمن المعلومات. و يكون الأمر أشد خطرا إذا كانت الشبكة اللاسلكية مربوطة بالشبكة الأم للمنشأة لأن ذلك يعني فتح ثغرة خفية في الدفاعات التي أقامتها الجهة المسؤولة عن تقنية و أمن المعلومات.

٢) وضع نقاط الدخول إلى الشبكة في أماكن مفتوحة مثل الممرات و القاعات، أي أنه بإمكان أي شخص أخذها من موقعها و العبث بإعداداتها بما يسهل عليه شن الهجمات ثم إعادتها في مكانها الأصلي.

٣) سهولة تعرضها للهجمات المؤدية إلى تعطيل الخدمة (Denial of Service) الذي يجعل أعضاء الشبكة اللاسلكية غير قادرين على تبادل المعلومات بينهم، هذا النوع من الهجمات يعتبر من أخطر ما تتعرض له الشبكات اللاسلكية لاعتبارات أهمها:

أ) أن الشبكات اللاسلكية تعتمد على نطاق ترددي ضمن الطيف الكهرومغناطيسي لنقل البيانات، و يمكن بسهولة التشويش على ذلك النطاق الترددي لتوفر الأجهزة اللازمة للتشويش و رخص ثمنها.

ب) وفقا لما جاء في نسخة عام ٢٠٠٤م من التقرير المشترك الذي يصدره في الولايات المتحدة الأمريكية كل من معهد أمن الحاسوب و مكتب التحقيقات الفدرالي فإن هجمات تعطيل الخدمة تبوأت المركز الأول –مشاركة مع الهجمات باستخدام البرامج السيئة – من حيث حجم الأضرار الذي تنزله، و هذا يدل على أن عددا كبيرا من المهاجمين صاروا يعتمدون هذا النوع من الهجمات.

ج) هناك ثغرات في تصميم البروتوكول الذي يدير عملية انضمام الأعضاء إلى الشبكة، وقد مر معنا أنه أثناء تأسيس الاتصال بين نقطة الدخول و الأجهزة الراغبة في الاتصال بالشبكة ترسل نقطة الدخول نبضات إليكترونية على فترات منتظمة معلنة عن نفسها، وأن هذه النبضات تحوي في طياتها معلومات مهمة تساعد الأجهزة على الاستجابة و تهيئة نفسها للاتصال. و تستمر نقطة الدخول إلى الشبكة في إرسال هذه النبضات طيلة فترة عملها

للمحافظة على الاتصال بين أعضاء الشبكة. و لكن المشكلة أن الرسائل التي تحملها هذه النبضات تبث دون أي نوع من الحماية فليس هناك ما يدل بشكل قطعي على هوية من أرسلها، و بالتالي فإنه يمكن للمهاجم إرسال نبضات مزورة تحمل هوية نقطة الدخول الحقيقة، و يحمل تلك النبضات رسالة تطلب من جميع الأجهزة المرتبطة بالشبكة إنهاء الاتصال، و هذا يقطع عمل الشبكة و يعطل الخدمة.

٤) أيضا بسبب طريقة عمل الشبكات اللاسلكية و اعتمادها على الطيف الكهرومغناطيسي فإنها عرضة بشكل خطير للتنصت إذ توجد أجهزة خاصة يمكن للمهاجم استخدامها لبث نداءات لاسلكية، و بسبب طبيعة عملها فإن نقطة الدخول إلى الشبكة تستجيب لهذه النداءات مما يكشف وجود الشبكة اللاسلكية و عندها يقوم المهاجم باستخدام أجهزة أخرى لالتقاط الرسائل المتبادلة داخل تلك الشبكة. و قد مر بنا أن الرسائل المتبادلة يمكن حمايتها باستخدام نظام تشفير (WEP)، و كما ذكرنا سابق فإن هناك نقاط ضعف في نظام التشفير هذا منها قدرة المهاجم على معرفة المفتاح المستخدم في عملية التشفير، و بالتالي يمكنه فك تشفير الرسائل التي التقطها.

الأخطار الأمنية المحتملة على الشبكات اللاسلكية:

§ اتصال أشخاص غير مصرحين بالإشارات اللاسلكية و بالتالي الاتصال بالشبكة اللاسلكية ككل.

§ بإمكان المخربين من التقاط و قراءة البيانات المرسلة على الهواء.

§ بإمكان الموظفين من تركيب شبكات لاسلكية في مكاتبهم و بالتالي خرق قوانين حماية الشبكة في منظماتهم.

§ يمكن للمخربين اختراق الشبكات اللاسلكية بسهولة بواسطة برامج اختراق بدائية جاهزة.

§ حرب الشوارع و هو مصطلح للتعبير عن التجوال بغرض اكتشاف و اختراق شبكات لاسلكية غير محمية.

وسائل حماية الشبكات اللاسلكية:

تتطلب حماية الشبكات اللاسلكية اتخاذ عدد من الخطوات الاحترازية، و لكن يمكن إجمال أهم ذلك في النقاط التالية:

١) وضع سياسات تحدد المسموح به و الممنوع فيما يتعلق بأمن المعلومات، و توفير آليات لتنفيذ تلك السياسات و اكتشاف المخالفين و التعامل معهم.

٢) التحقق من أن الشبكات اللاسلكية تنشأ و تدار من قبل أشخاص متخصصين في هذا المجال و منع الهواة و قليلي الدراية من القيام بهذه الأعمال.كما يجب التأكد أن كل ذلك يتم وفق سياسات و إجراءات تضمن أمن المعلومات.

٣) تغيير الأوضاع الأصلية لمعدات و برامج الشبكات اللاسلكية، وهذا يجب أن يكون نتيجة حتمية للخطوات السابقة.

٤) مراقبة شبكات المعلومات لاكتشاف أي أنشطة مشبوهة.

٥) حسن اختيار المواقع التي توضع فيها نقطة الاتصال بالشبكة بحيث تكون النقطة محمية، كما يكون بثها الكهرومغناطيسي موجها إلى داخل البيت أو المنشأة قدر الإمكان و تقليل ما يبث نحو الخارج لتقليل فرص التقاط البث.

٦) تشغيل بروتوكولات التحقق من الهوية و أنظمة تشفير قوية لتأمين المعلومات.

بروتوكولات تشفير الشبكات اللاسلكية:

صناعة الشبكات اللاسلكية من أسرع الصناعات تطورا في عالم الشبكات وخصوصا لدى المستخدمين ذوي نطاق محدود مثل استخدامها في المنازل والشركات الصغيرة بالرغم من قصورها من الناحية الأمنية.وهذه التقنية في تطور مستمر من حيث السرعة وسعة النقل كذلك من النواحي الأمنية.ومع كل هذا التطور مازال هناك الكثير من الشركات الكبرى لديها الكثير من المخاوف في استخدام هذه التقنية وذلك لسبب قصورها من الناحية الأمنية والخطر الذي سوف تتعرض له الشركات أثناء استخدامها.

أنواع بروتوكولات التشفير:

(١) "WEP "Wired Equivalent Privacy:

بروتوكول يستخدم في تشفير البيانات المتنقلة داخل شبكة لاسلكية وذلك لمنع المخترقين من الحصول على البيانات.

وهو من أقدم بروتوكولات تشفير الشبكات اللاسلكية وتستخدم مفتاح سري مشترك "Shared Secret Key" وله نوعين من المفاتيح إما ٤٠ بت أو ١٠٤ بت والذي يضاف إليه القيمة الابتدائية " Initial Vector" وهو عبارة عن ٢٤ بت، فيصبح إما ٦٤ بت أو النوع الشائع استخدامه وهو ١٠٤ بت "١٢٨ بت" ويسمى هذا النوع من المفاتيح مفتاح التشفير المشترك "PSK".

عيوب WEP:

بعد انتشار استخدامها قامت بحوث ودراسات هدفها كشف عيوب ال WEP ومنها:

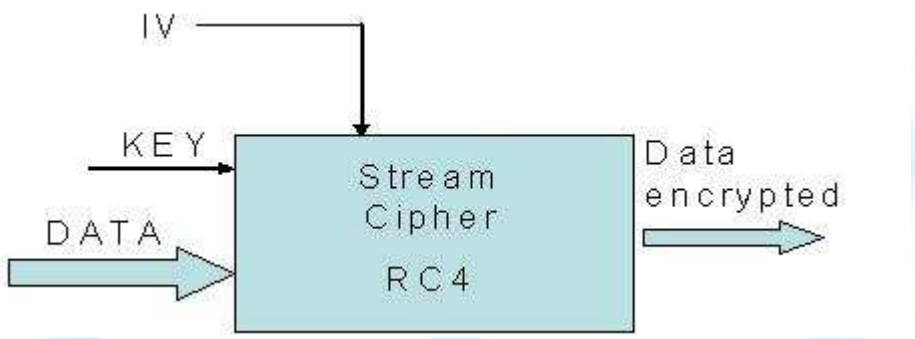
- استخدامها لمفتاح سري مشترك يتم توزيعه يدويا على جميع المستخدمين مما يجعل عملية التغير متعبة وخصوصا في الشركات

الكبرى مما يمد في عمر المفتاح السري المشترك وبالتالي يسهل عملية الاختراق وكشف المفتاح.

- قصر طول المفتاح مما يجعل اكتشاف المفتاح مهمة سهلة للمخترقين.

- رأس حزمة البيانات المرسلة غير مشفر مما يتيح معرفة عنوان المرسل والمستقبل وذلك يسهل عملية المخترقين في معرفة المفتاح.

كل ما سبق من عيوب يجعل استخدامه غير ملائم لفئة الشركات الكبرى ولكنه مناسب إلى حد ما لمستخدمي المنازل والمؤسسات.

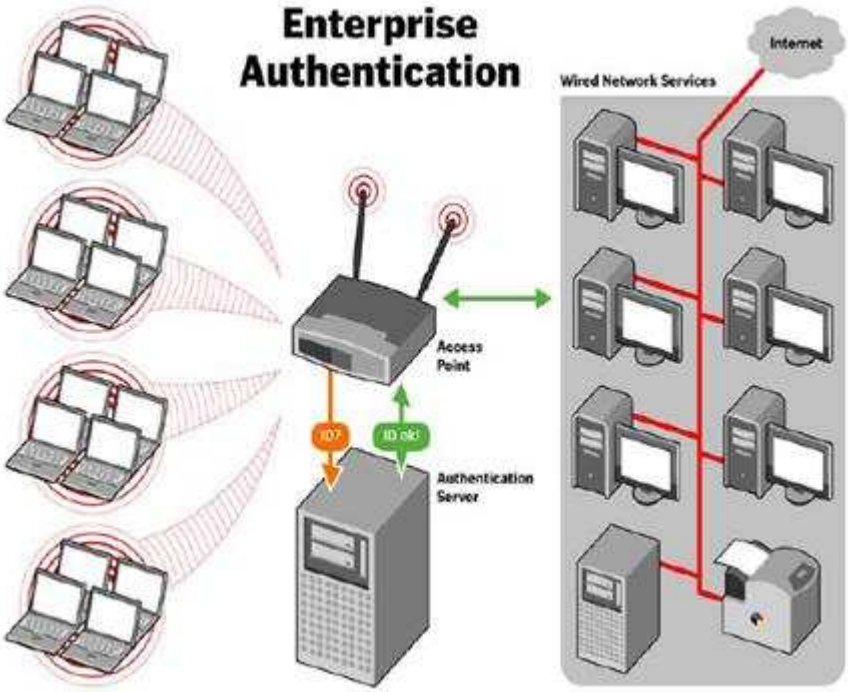


الشكل رقم (٧):: رسم يوضح طريقة عمل بروتوكول التشفير WEP

(٢) "Wi-Fi Protected Access "WPA:

هي عبارة عن برنامج "Firmware" صمم لتصحيح عيوب ال WEP يحمل على الأجهزة المستخدمة" (نقاط الوصول) "AP"أي لا يتطلب تغيرها وهو مرحلة انتقاليه أو وسيطة بين ال WEPو 802.11i ويزيد من مستوى حماية البيانات وكذلك في التحكم في الدخول إلى الشبكة اللاسلكية حيث لا يسمح إلا للأشخاص المصرح لهم مما يجذب الشركات الكبرى إلى استخدامه.

بالنسبة للاستخدام في الشركات يتطلب وجود خادم للشبكة للتحقق من هوية المستخدم" Authentication Server" من نوع 802.1x مع بروتكولEAP.



الشكل رقم (٨):: رسم يوضح طريقة عمل بروتوكول التشفير WPA

أما لمستخدمي المنازل والمؤسسات الصغيرة ليس هناك حاجة إلى توفر خادم الشبكة " Authentication Server" كل ما على المستخدم عمله هو إدخال المفتاح السري " Pre-shared Key" أو الرقم السري على جهازه الذي يريد من خلاله الدخول على الشبكة. لكل مستخدم رقم سري خاص به هو الذي يحدد هويته ومدى الصلاحيات المقدمة لهذا المستخدم وهو بعكس ال WEPالذي يستخدم مفتاح واحد لجميع المستخدمين. وللإتمام عملية ال WPAيجب إدخال جميع الأرقام السرية في نقطة الوصول " Access Point". ويتكون هذا المفتاح من ١٢٨ بت ولكن بقيمة ابتدائية مكونة من ٤٨ بت مما يجعل WPA أقوى تجاه الاختراق من WEP.

كما نلاحظ أن هذا الطول مساوي للمفتاح في ال WEP مما يعني انه ليس هناك اختلاف؟ الاختلاف هو في تغير المفتاح تلقائيا مما يعني أن مستخدم ال WPA لن يقوم باستخدام المفتاح لفترة طويلة، وهنا تكمن متانة هذا النظام.

الشكل رقم (٨):: بروتوكول WPA

عيوب WPA:

لا يوجد نظام متكامل مما يعني أن هناك بعض العيوب التي ترافق ال WPA وهي:

- ما تزال تعتمد على المفتاح الذي يمكن التقاطه في حين الإرسال ومن ثم استخدام الاختراق المعجمي "Attack dictionary" للحصول على الرقم السري.
- قد يعاني من توقف الخدمة DoS وذلك إذا أدخلت كلمة المرور أكثر من مرة بطريقة غير صحيحة سيتم حجب المستخدم عن الدخول إلى الشبكة اللاسلكية.

(٣) "Wi-Fi Protected Access 2 "WPA2:

وهو بروتوكول معزز ل WPA ويتميز بأنه يستخدم خوارزمية AES للتشفير، كما انه يستخدم في الشبكات الثنائية Ad-hoc وهو متوفر

بطريقة PSK أو باستخدام آلية توثيق 802.1X/EAP والتي يمكن من خلالها استخدام الشهادات الإلكترونية.

نصائح لحماية الشبكات اللاسلكية:

- تغيير اسم المستخدم و كلمة المرور الابتدائية لنقطة الاتصال و الموَجه ، وذلك لمنع الأشخاص الغير مصرح لهم من الاتصال بالشبكة بمجردلتخمين اسم المستخدم و كلمة المرور الموضوعة ابتدائيا من قبل الشركة المصنعة.

- تنشيط خاصية التشفير ، وذلك لمنع الأشخاص الغير مصرح لهم من التقاط الأشارات و بالتالي التعرف على البيانات المرسلة.

- تغيير اسم الشبكة الابتدائي ، لمنع معرفة اسم الشبكة بمجرد التخمين بالاسم الموضوع من قبل الشركة المصنعة.

- تنشيط خاصية فلترة العناوين للأجهزة المتصلة بالشبكة، لقصر الاتصال فقط على عناوين معروفة مسبقا ومنع الاتصال للعناوين الغير معروفة.

- إلغاء خاصية نشر اسم الشبكة ، لمنع اكتشافها و قصر الاتصال على من يعرف اسم الشبكة اللاسلكية.

- تحديد عناوين انترنت (IP) ثابته للأجهزة في الشبكة اللاسلكية ، و بالتالي سيساعد ذلك على عملية التشفير للعناوين (IPs).

- تحديد مكان مناسب لنقطة الاتصال و الموَجه من حيث مدى انتشار الإشارات اللاسلكية ، و أنها تكون قدر الإمكان داخل منطقة آمنة ولا تصل لمدى أبعد من المدى المطلوب.

§ تركيب جدار ناري (Firewall) لمنع الاتصال الغير مصرح و لإخفاء الشبكة ، وأفضل جدار ناري و هو أيضا مجاني زون آلارم و يمكن تحميله من موقع البرنامج http://www.zonelabs.com/.

§ التحديث المستمر للبرامج المشغلة لمكونات الشبكة (نقط الاتصال ، الموجهات ،...) عن طريق الشركات المصنعة.

§ متابعة أخبار الشبكات و خاصة الشبكات اللاسلكية في مجال الأمن و تطبيق التحديثات و الأنظمة الأمنية الجديدة.

مصطلحات مهمة في الشبكات اللاسلكية:

بقي لنا أن نعرف بعض المصطلحات المهمة في الشبكات اللاسلكية:

§ نقطة الاتصال (Access Point) : مركز استقبال و إرسال الإشارات اللاسلكية ، ومدى الشبكة اللاسلكية بحسب قوة إرسال الإشارة الصادرة من هذه النقطة.

الشكل رقم (٥):: -نقطة الاتصال-

§ معرف الشبكة اللاسلكية (SSID) : اسم الشبكة اللاسلكية ، و عن طريقها يتم تعريف الشبكة اللاسلكية و الاتصال بها.

§ مفتاح الحماية (WEP, WPA): خياران للحماية بتشفير البيانات المرسلة في الشبكات اللاسلكية بحيث فقط المصرح لهم الاتصال بالشبكةبامكانهم معرفة البيانات المرسلة بينما الملتقطين للإشارات اللاسلكية الغير مصرح لهم لايمكنهم معرفة البيانات المرسلة . و نظام التشفير WPA أفضل بكثير من النظام WEP لكن ليس جميع الأجهزة تدعمه ، و النسخة الأمنية الجديدة من المعايير القياسية للشبكات اللاسلكية802.11i تعزز الجانب الأمني عن طريق تطوير

نظـــام WPA وبالتـــالي ســـيكون هنـــاك نظـــام مطـــور للتـــشفير وهو WPA2 .

§ النقاط الـساخنة (Hotspots): عبـارة عـن جهـاز هـوائي موصـول بالإنترنت ويتصل لاسلكيا مع أجهزة الحاسب فـي مـداه الـذي قـد يـصل إلى ٤٥ مترا، ولاتصال جهاز الحاسب بشبكة الواي فـاي لابـد مـن تهيئتـه لدعم هذه التقنية، ومعظم الأجهـزة المحمولـة التـي تبـاع الآن مـزودة بداخلها ببطاقات واي فاي. و النقاط الساخنة هي التعبير المتداول لنقاط الاتصال.

الشكل رقم (٦):: -علامة وجود خدمة الواي فاي-

الخاتمة:

عرفنا إذن أن لشبكة الاتصال اللاسلكي مميزات كثيرة لا يمكن إنكارها، و أنه من العسير أن توجد منشأة ليس فيها شبكة لاسلكية، لما أحدثته الشبكات اللاسلكية من تغيير وتطوير كبيرين في استخدام و بناء الشبكات و طريقة الاتصال بها أيضا ، وواكب هذا التغير اهتمام متزايد بأنظمة الحماية لهذا النوع من الشبكات التي بطبيعتها نظرا للتراسل على الهواء عرضة أكبر للتهديدات الأمنية ولذلك يجب الاهتمام بالجانب الأمني و التأكد من تطبيقه بالشكل الكافي و المحدث.

المراجع:

١- كتاب أمن المعلومات بلغة ميسرة تأليف د. خالد بن سليمان الغثبر & د. مهندس محمد بن عبد الله القحطاني طبعة ١٤٢٩هـ.

٢- كتاب الشبكات اللاسلكية وتطبيقاتها مؤلف مجهول من موقع .www.abahe.co.uk

٣- أمن الشبكات اللاسلكية، إعداد : Alberto Escudero Pascual/ IT +46 النسخة العربية: أنس طويلة.

٤- أمن الشبكات اللاسلكية، إعداد : مصطفى محمد نجم.

٥- أمن الشبكات اللاسلكية، إعداد المركز الوطني الإرشادي لأمن المعلومات – هيئة الاتصالات وتقنية المعلومات.

٦- مقالة بعنوان: "WPA “Wi-Fi Protected Access ” " على هذا الرابط هنا.

٧- مقالة بعنوان: " (Wi-Fi Security) أمن الشبكات اللاسلكية قصيرة المدى " على هذا الرابط هنا.

٨- مقالة بعنوان: "كيف تعمل الشبكات اللاسلكية" على هذا الرابط هنا.

٩- مقالة بعنوان: "الشبكات اللاسلكية : أنواعها وتعريفها" على هذا الرابط هنا.

١٠- مقالة بعنوان: "الشبكة اللاسلكية" على هذا الرابط هنا.

١١- مقالة بعنوان: "حماية الشبكات اللاسلكية" على هذا الرابط هنا.

١٢- مقالة بعنوان: "الأمن في WiFi" على هذا الرابط هنا.

١٣- مقالة بعنوان: "شبكة لاسلكية آمنة" على هذا الرابط هنا.

تم بحمد الله ،،،