

بسم الله الرحمن الرحيم

جامعة الملك سعود
كلية علوم الحاسب و المعلومات
قسم نظم المعلومات

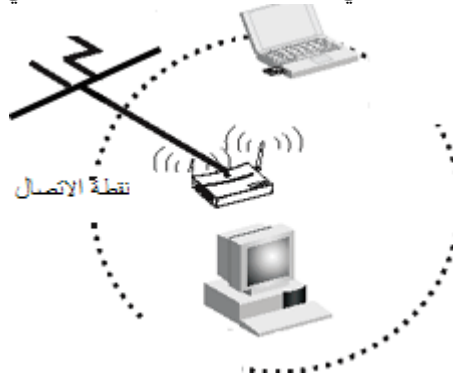
أمن الشبكات اللاسلكية قصيرة المدى (Wi-Fi Security)

إعداد : م. سليمان بن هيشة

إشراف: د. خالد الغنبر

مقدمة

بدأت الشبكات اللاسلكية بالانتشار ومن ضمنها شبكات الواي فاي (Wireless Fidelity Wi-Fi) بصورة ملحوظة و غير متوقعة ، حتى لاتكاد تذهب إلى مكان ما إلا وتجد علامة تشير الى وجود خدمة (Wi-Fi) ، وتوقعت دراسة حديثة نمو عدد مستخدمي نقاط الاتصال اللاسلكي في العالم من 9.3 ملايين مستخدم خلال العام 2004 ليصل إلى نحو 30 مليوناً بنهاية العام الجاري. وشهدت نقاط الاتصال اللاسلكي انتشاراً واسعاً على مدى السنوات القليلة الماضية من بضع مئات خلال العام 2000 لتصل إلى حوالي 40.000 نقطة اتصال ساخنة في العالم خلال العام 2004. فما هي (Wi-Fi) ؟ ، و بما أنها شبكة فهذا يعني أنها عرضة لتهديدات أمنية فما هي سبل الحماية ؟ هذا ما سنناقشه في هذه المقالة.



شبكة لاسلكية-

تعريف

(Wi-Fi) هي الشبكات اللاسلكية قصيرة المدى المكونة من مجموعة من الأجهزة المرتبطة مع بعضها البعض لتبادل المعلومات و الاستفادة من الموارد (أو المنافع) الموجودة في الشبكة من خلال وسط تراسلي لاسلكي -على الهواء- ذلك يعطي حرية تنقل الأجهزة المرتبطة بها مادامت داخل نطاق الشبكة ، لكن مقابل هذه الميزة يظهر خطر أمني يهدد هذا النوع من الشبكات ألا وهو انكشاف البيانات المرسله على الهواء و بالتالي تكون عرضة للإختراقات و غيرها من التهديدات الأمنية.

المعايير القياسية للشبكات اللاسلكية

ثلاثة أجيال من المعايير القياسية للشبكات اللاسلكية ظهرت حتى الآن ، وهي على التسلسل الزمني 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 تغطيها المعايير السابقة ، و من المتوقع طرح هذا الإصدار في الأسواق بنهاية العام 2005.

البروتوكول	السرعة	التردد
802.11b	11 ميكابت/ث	2.4 كيكاهيرتز
802.11a	54 ميكابت/ث	5 كيكاهيرتز
802.11g	54 ميكابت/ث	2.4 كيكاهيرتز

مصطلحات مهمة في الشبكة اللاسلكية

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



-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 المرسله في الشبكات اللاسلكية بحيث فقط المصرح لهم الاتصال بالشبكة بإمكانهم معرفة البيانات المرسله بينما الملتقطين للإشارات اللاسلكية الغير مصرح لهم لايمكنهم معرفة البيانات المرسله . و نظام التشفير WPA أفضل بكثير من النظام WEP لكن ليس جميع الأجهزة تدعمه ، و النسخة الأمنية الجديدة من المعايير القياسية للشبكات اللاسلكية 802.11i تعزز الجانب الأمني عن طريق تطوير نظام WPA وبالتالي سيكون هناك نظام مطور للتشفير وهو WPA2 .
- النقاط الساخنة (Hotspots) : عبارة عن جهاز هوائي موصول بالإنترنت ويتصل لاسلكيا مع أجهزة الحاسب في مده الذي قد يصل إلى 45 مترا، ولاتصال جهاز الحاسب بشبكة الواي فاي لا بد من تهيئته لدعم هذه التقنية، ومعظم الأجهزة المحمولة التي تباع الآن مزودة بداخلها ببطاقات واي فاي. و النقاط الساخنة هي التعبير المتداول لنقاط الاتصال.



-علامة وجود خدمة الواي فاي-

أخطار أمنية محتملة على الشبكات اللاسلكية

- اتصال اشخاص غير مصرحين بالإشارات اللاسلكية و بالتالي الاتصال بالشبكة اللاسلكية ككل.
- بإمكان المخربين من التقاط و قراءة البيانات المرسله على الهواء.
- بإمكان الموظفين من تركيب شبكات لاسلكية في مكاتبهم و بالتالي خرق قوانين حماية الشبكة في منظماتهم.
- يمكن للمخربين من 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.

نصائح لحماية الشبكات اللاسلكية

- تغيير اسم المستخدم وكلمة المرور الابتدائية لنقطة الاتصال و الموجه ، وذلك لمنع الأشخاص الغير مصرح لهم من الاتصال بالشبكة بمجرد لتخمين اسم المستخدم وكلمة المرور الموضوعه ابتداءيا من قبل الشركة المصنعة.
- تنشيط خاصية التشفير ، وذلك لمنع الأشخاص الغير مصرح لهم من التقاط الأشارات و بالتالي التعرف على البيانات المرسله.
- 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) ثابتة للأجهزة في الشبكة اللاسلكية ، و بالتالي سيساعد ذلك على عملية التشفير للعناوين (IPs).
- تحديد مكان مناسب لنقطة الاتصال و الموجه من حيث مدى انتشار الإشارات اللاسلكية ، و أنها تكون قدر الإمكان داخل منطقة آمنة .
- تركيب جدار ناري (Firewall) لمنع الاتصال الغير مصرح و لإخفاء الشبكة ، وأفضل جدار ناري و هو أيضا مجاني زون ألام 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.

الخاتمة

أحدثت الشبكات اللاسلكية تغير و تطور كبيرين في استخدام و بناء الشبكات و طريقة الاتصال بها أيضا ، و اكب 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

- K. Dulaney, R. Ahlawat, "Management Update: Wireless LAN Predictions for 2004", November 2003, Gartner.
- M. Ciampa, "Security+ Guide to Networking Security Fundamentals", Second Edition, Thomson Course Technology, 2004.
- J. Pescatore, J. Girard, K. Dulaney, "Wireless LAN Authentication Choices", August 2003, Gartner.
- M. Alsadhan, "المملكة الأولى بـ "13" موقعاً تليها الإمارات ثم الكويت...والعراق أكبر المرشحين للاستفادة من الواي فاي", http://www.alriyadh.com/Contents/29-05-2004/RiyadhNet/News_3275.php
- "Wi-Fi Security", Wi-fi.org, www.wi-fi.org/OpenSection/secure.asp?TID=2
- T. Krazit, "Wi-Fi Security Improves", pcworld.com, Wednesday May 05 2004, <http://www.pcworld.com/news/article/0,aid,115999,00.asp>
- M. Hines, "Worried about Wi-Fi security?", news.com, Wed Jan 19 2005 , http://news.com.com/2102-7347_3-5540969.html