King Saud University

College of Computer and Information Sciences

Department of Information System

Is591

Term Paper 4

Ali Sulaiman Al-Humaimidi 425121604

مقدمـــــــــــــــة :-

الأجهزة اللاسلكية في هذه الأيام تكاد توجد في كل مكان . كذلك نقاط الاتصال التي تسمح للأجهزة اللاسلكية بالولوج للشبكة اللاسلكية بدأ انتشارها على نطاق واسع حيث يمكن مشاهدتها في مناطق عديدة منها مقاهي الإنترنت والمطارات والأندية الرياضية .حيث يتوقع بيع ملايين الأجهزة اللاسليكة خلال السنوات القريبة القادمة .

ونظرا لهذا التطور والنمو في الشبكات اللاسلكية قابله ضعف في الإجراءات الأمنية المضمنة في البروتوكول الخاص بالشبكات اللاسلكية 802.11 , لذلك في سنة 2000 ميلادي قام معهد (IEEE) بإنشاء مجموعة خاصة بحل الثغرات الأمنية لبرتوكول 802.11 وأعطية الإسم 802.11i.

مجموعة 802.11i :-

- قامت المجموعة بدراسة نقاط الضعف الموجودة في بروتوكول WEP (Wired Equivalent Privacy) وهو بروتوكول الحماية الخاص ببروتوكول 802.11 لتوفير نظام تشفير للشبكات اللاسلكية . وبعد دراسة نقاط الضعف الموجودة في هذا البروتوكول تم التوصل إلى أربع نقاط ضعف أساسية هي :-
  1. عمليات التشفير لا تتم بدقة الكافية لتحقيق سرية البيانات .
  2. ليس هناك معنى أو فائدة من منع الرسائل المرسلة من التزوير .
  3. مفاتيح التشفير تستخدم مرة أخرى مما يتيح الفرصة لقراءة البيانات المرسلة بدون معرفة مفتاح التشفير .
  4. عملية التأكد من هوية المرسل غير عملية , لأنه يتم إرسال المعلومات التي يستفيد منها المخترق بالمفتوح .

- لذلك عمل هذه المجموعة اتجه إلى ثلاث خطوط مختلفة هي :-
  1. تحسين عملية التأكد من الهوية :

الشكل العام للتأكد من الهوية تم استبداله ببرتوكول IEEE 802.1x الذي يتطلب خادم مستقل لتأكد من الهوية فهو يقوم بتحديد ما إذا كان المستخدم مخول له الارتباط بالشبكة اللاسلكية أم لا .

  2. ابتكار خوارزميات جديدة للتشفير :

تم إبتكار بروتوكول جديد للتشفير ليحل محل بروتوكول WEP . هذا البروتوكول الجديد يعتمد على مبادئ الصوت التي قامة المجموعة باكتسابها من تطوير بروتوكول IPSEC وبروتوكولات الحماية الأخرى .

  2. التأكد من عدم استخدام المفتاح مرة أخرى :

قامت المجموعة بتصميم هيكل عام لمنع استخدام مفتاح التشفير مرة أخرى لذلك كل مرة يرتبط فيها المستخدم بنقطة اتصال جديدة يتم إعطائه مفتاح جلسة جديد لاستخدامه في عمليات التشفير .

مكونات بروتوكول 802.11i :-

1. Temporal Key Integrity Protocol (TKIP):

- وهو عبارة عن بروتوكول لسرية البيانات , تم تصميمه لتحسين مستوى الأمن في المنتجات التي تعتمد على بروتوكول WEP كبروتوكول أمن .
- بروتوكول TKIP يستخدم كود خاص لسلامة الرسالة هذا الكود يسمى Michael الذي بدوه يسمح للأجهزة من التأكد من هوية ومصدر ال packet القادمة إليه من الجهات الأخرى , كذلك يستخدم خليط من الدوال لمواجهة وإحباط أي هجوم يعتمد على ضعف المفتاح الذي يستخدمه المخترقون لكسر تشفير البيانات المرسلة .
- بروتوكول TKIP عبارة عن مجموعة من الخوارزميات التي تهيأ وتعد بروتوكول WEP لتفادي العيوب الموجودة فيه .
- بروتوكول TKIP يضيف إلي بروتوكول ثلاثة عناصر هي :

1. الكود الخاص بسلامة الرسالة (Message Integrity Code (MIC)) ويسمى Michael وذلك لإحباط أي تزوير في البيانات المرسلة .
2. وضع تسلسل لل packet بناء على قواعد وأنظمة وذلك لإحباط الهجوم المتعمد على إعادة إرسال الرسالة .
3. إضافة مفتاح لكل packet الذي يتم إنتاجه عن طريق خليط من الدوال وذلك لمنع الاختراق .

- Michael عبارة عن خوارزمية لتأكد من سلامة الرسالة حيث تقوم هذه الخوارزمية بحساب دالة المفتاح للبيانات عند المرسل ثم يتم إرسال هذه القيمة مع البيانات إلى المستقبل الذي يقوم بإعادة حساب دالة المفتاح للبيانات المستقبلة ومطابقة الناتج مع القيمة المرسلة فإذا تطابقت القيمتان تم قبول البيانات أو يتم رفضها عن اختلاف القيمتان .

2. Counter-Mode /CBC-MAC Protocol (CCMP) :

- وهو عبارة أيضا عن بروتوكول لسرية البيانات حيث يقوم بإدارة عمليات التأكد من الهوية ومصدر ال packet وكذلك تشفيرها . لسرية البيانات يقوم بروتوكول CCMP باستخدام بروتوكول AES (Advanced Encryption System) في نمط العد . كذلك يستخدم بروتوكول CBC-MAC (Cipher Block Chaining Message Authentication Code) لتأكد من هوية وسلامة البيانات .
- في بروتوكول 802.11i نستخدم بروتوكول CCMP طول مفتاح 128بت .
- بروتوكول CCMP يقوم بحماية الحقول التي لا يتم تشفيرها في ال frame الخاص ببروتوكول IEEE 802.11 , وتسمى هذه البيانات بعد تشفيرها بالبيانات الإضافية لتأكد من الهوية (Additional Authentication Data AAD) , وهي تحتوي على عنوان المرسل والمستقبل لل packet وبذلك نمنع من إعادة إرسال البيانات إلى جهة أخرى غير الجهة المراد إرسال البيانات إليها.
- يتميز هذا البرتوكول بعدة مزايا هي :-

1. أنه يستخدم مفتاح واحد لسرية وسلامة البيانات وبذلك تقليل من الجهد اللازم لإدارة المفاتيح كذلك من الوقت اللازم لحساب مفتاح بروتوكول AES .
2. يوفر حماية وسرية للبيانات المفتوحة في بروتوكول IEEE 802.11 بالإضافة إلى بيانات البروتوكول الأخرى .
3. يحتاج إلي حجم صغير لبنائه , وبذلك تقليل للتكلفة .
4. يحتاج إلي إضافات بسيطة إلي بروتوكول IEEE 802.11 لكل packet .

3. IEEE 802.1X :-

- يقوم بتوفير بنيه فعالة لتأكد من هوية البيانات والتحكم في البيانات في الشبكات المحمية , حيث يقوم بربط بروتوكول EAP (Extensible Authentication Protocol) بكلا من الشبكات اللاسلكية والسلكية وذلك لدعم الطرق المتعددة لتأكد من الهوية .
- في هذا البروتوكول يوجد ثلاثة عناصر هي :-

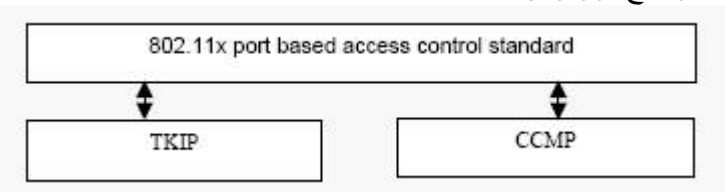
1. الطالب للخدمة (Supplicant) :
وهو عبارة عن الزبون (client) حيث يقوم بطلب الدخول إلى الشبكة اللاسلكية وذلك بالارتباط بنقطة الدخول (access point) .
2. المتأكد من الهوية (Authenticator) :
وهو عبارة عن نقطة الدخول (Wireless Access Point (AP)) أو محول للشبكة الداخلية اللاسلكية WLAN حيث يبقي الشبكة اللاسلكية الداخلية مغلقة لجميع البيانات الغير مصرح لها . وهو بدوره لا يقوم بالتأكد من الهوية مباشرة بل يقوم بإرسالها إلى الخادم المسؤول عن ذلك .
3 . الخادم المسؤول عن التأكد من الهوية (Authentication Server) :
حيث يقوم بعملية التأكد من هوية الزبون من ثم يأمر ال Authenticator أما بالسماح أو عدم السماح للزبون بالدخول للشبكة اللاسلكية . يمكن أن يكون هذا الخادم عبارة عن عنصر من عناصر محول الشبكة الداخلية اللاسلكية WLAN Switch أو عنصر مستقل بذاته مثل RADIUS Server (Remote Authentication Dial-up User Server) .

4. Encapsulation Over LANs (EAPOL) :

- هو عبارة بروتوكول مضمن في بروتوكول IEEE 802.1X لإدارة المفاتيح . حيث يوجد في بروتوكول 802.11i زوجان من EAPOL key Exchange وذلك لتبادل المفاتيح بينهما .

* بما أن بروتوكول IEEE 802.11i يحوي عدة بروتوكولات لتأكد من سرية البيانات فهو يقدم خوارزمية معينة للزبون لمخاطبة نقطة الدخول والاتفاق على البروتوكول الذي سوف يستخدم خلال جلسة الاتصال .

* رسمة توضح بروتوكول IEEE 802.11i :



الخاتـــــــــــــــمة :-

سرية وسلامة البيانات تعتبر دائما مشكلة مع التكنولوجيا اللاسلكية فهو غير مقيد بالقيود الفيزيائية مثل الكيابل أو الجدران , لذلك أنشئت مجموعة IEEE 802.11i لتضع المواصفات والمقاييس لجعل الأجهزة اللاسلكية أكثر أمنا وسلامة . لذلك نجد انه مع بروتوكول IEEE 802.11i هناك حلقة أمنية تبدأ بعملية دخول النظام ومن ثم تبادل المفاتيح ومن ثم التأكد من الهوية وأخيرا التشفير , وهذه الحلقة تعتبر أكثر فاعلية ضد أي هجوم سواء كان مقصود أم لا .

المراجـــــــــــع :

[1] R. Housley, and W. Arbaugh, , "Security problems in 802.11-based networks", *Commun. ACM 46*, 5, May, 2003 .

[2] Arbaugh, William A., Shankar, Narendar, Wan,and Justin Y.C. ,"Your 802.11 Wireless Network has No Clothes.", 30 March, 2001, URL: http://www.cs.umd.edu/~waa/wireless.pdf.

[3]Cam-Winget,and Nancy., "IEEE 802.11i Overview.", URL: http://csrc.nist.gov/wireless/S10_802.11i%20Overview-jw1.pdf

[4] Eaton, and Dennis., "Diving into the 802.11i Spec: A Tutorial.", 26 Nov, 2004, URL: http://www.commsdesign.com/printableArticle/?articleID=16506047

[5] Edney Jon , and Arbaugh William.," Real 802.11 Security: Wi-Fi Protected Access and 802.11i", Boston, Addison-Wesley,2004.

[6] Don MacVitte," 802.11i to Lock Down WLANs",URL: http://informationweek.networkingpipeline.com/specwatch/802.11i.jhtml

[7] Dan Harkins, Trapeze Networks ," Locking Down WLAN Designs with 802.11i**",** Feb 24, 2005,URL: http://www.commsdesign.com/design_corner/showArticle.jhtml?articleID=60403332

[8] Jesse Walker ," IEEE 802.11i Standard Improves Wireless LAN Security**",** May, 2005, URL: http://www.intel.com/technology/magazine/standards/80211i-0505.pdf

[9] Gast ,and Matthew, "Wireless LAN Security: A Short History.", 19 April, 2002, URL: http://www.oreillynet.com/lpt/a/1728

[10] Fleishman, and Glenn, "Caring About 802.11i.",25 June, 2004, URL: http://www.wifinetnews.com/archives/003939.html.