الحماية من قرصنة الشبكات اللاسلكية

د. م. جمال الياسين[1]

الملخص

وَفَّرَتِ الشبكات اللاسلكية العديد من الخدمات التي لم تكن متوافرة سابقاً، وحلت معظم المشكلات التي كانت تواجه الشبكات السلكية، ولكن هذا التطور في الشبكات سمح بمجالات اختراق عديدة فكان لابدَّ من إيجاد طرائق لحماية هذه الشبكات اللاسلكية من قرصنة المتطفلين، وفي هذه الدراسة يتم تناول موضوع خوارزميات التشفير بأنواعها، والبرامج المستخدمة لاختراق الشبكات اللاسلكية وما الطرائق المثلى لحماية هذه الشبكات من الاختراق؟

الكلمات المفتاحية: الشبكات اللاسلكية، خوارزميات التشفير WPA–WEP، برامج اختراق الشبكات اللاسلكية، WPS، MAC Address.

[1]أستاذ مساعد، قسم هندسة الحواسيب والأتمتة، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق، سورية.

Protecting of Wireless Networks from Piracy

Dr. Eng. Jamal Al Yasin[(1)]

Abstract

Wireless networks provided many services that were not previously available and it solved most of the problems faced by wired networks. However, this development in networks allowed penetration in many ways. Thus made it necessary to find methods to protect wireless networks from hacking. In this study, we discuss cryptography algorithm and programs used to hack wireless networks and what are the best ways to protect these networks from hacking.

Keywords: Wireless Networks Cryptography Algorithm– WEP– WPA– Wireless Network Hacking Programs– WPS– MAC Address.

[(1)] Assistant Professor –Department of Computer& Automation Engineering - Faculty of Mechanical & Electrical Engineering Damascus University.

المقدمة:

قرصنة الشبكات اللاسلكية هي عملية اختراق للشبكات اللاسلكية دون تصريح، أو دراية لصاحب الشبكة. لأسباب كثيرة لا يقوم أصحاب تلك الشبكة بحمايتها، إمَّا عن جهل أو إهمال. وفي حالات أخرى تكون أساليب الحماية ضعيفة وسهلة الكسر؛ ممَّا يسهل تسلل أي شخص، على دراية بكيفية الولوج، بالتطفل واستغلال المعطيات والثغرات والمعلومات المتوافرة على الشبكة.

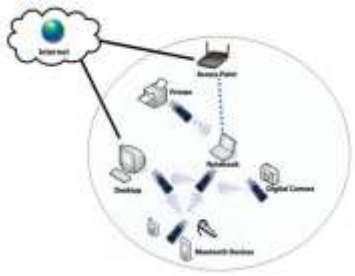
الحاجة إلى الشبكات اللاسلكية:

إن الهدف الأساسي من الشبكات اللاسلكية تحقيق الفائدة القصوى المرجوة من الموارد التي تتيحها الأجهزة على الشبكة، وبالفعل فقد وفرت هذه الشبكات العديد من الخدمات لمستخدميها، إذْ مكنتهم من التواصل مع بعضهم بعضاً عن طريق البريد الإلكتروني والإفادة من البرامج والتطبيقات فضلاً عن إمكانية الولوج إلى قواعد بيانات مشتركة. بدأ التوجه إلى استخدام الشبكات اللاسلكية (Wireless LAN) التي قدمت الحلول للمشكلات التي عانت منها الشبكات السلكية، إذْ أعطت مرونة كبيرة في عملية إضافة عقدة جديدة إلى الشبكة دون الحاجة إلى المزيد من التوصيلات السلكية، والأهم هو إمكانية التنقل بحرية مع الجهاز المحمول ضمن مجال الشبكة، هذا مع الأخذ بالحسبان الكلفة المنخفضة لهذه الشبكات.[4]

أنواع الشبكات اللاسلكية:

1- شبكة المناطق الشخصية اللاسلكية (WPAN):

شبكات WPAN هي اختصار إلى Wireless Personal Area Network وهي الشبكات التي تصل بين أجهزة ضمن مساحة صغيرة نسبياً، عادةً ما تكون هذه المساحة ضمن مجال يمكن لشخص الوصول إلى أجزائه جميعها. مثال على ذلك، تقنية الأشعة فوق الحمراء وتقنية البلوتوث التي تقوم مثلاً بربط حاسوب شخصي مع السماعات. وكذلك فإنَّ تقنية (ZigBee) تدعم تطبيقات هذا النوع من الشبكات. وقامت شركتا Intel وMicrosoft بتطوير تقنيات تعتمد على هذا النوع من الشبكات، وأصبحت مستخدمة في العديد من الأجهزة الالكترونية. يوضّح الشكل (1) مثالاً توضيحياً لشبكة المناطق الشخصية.[4]



الشكل (1) مثال توضيحي لشبكة المناطق الشخصية

2- شبكات المناطق المحلية اللاسلكية (WLAN):

شبكات WLAN هي اختصار إلى Wireless Local Area Network وهي النوع الأكثر شيوعاً من الشبكات اللاسلكية. تقوم بربط الأجهزة على مسافة أبعد من النوع السابق كمنزل أو مكتب أو حتى بناء، وفي بعض الأحيان تمتد لتغطي عدة كيلومترات. معظم الشبكات (WLAN) تعتمد على المعيار (IEEE 802.11) الذي يحتوي على معايير للشبكات اللاسلكية المحلية التي تعمل في الحزم الترددية 2.4Ghz و5Ghz، وتضم عدداً من البروتوكولات المختلفة. من الخصائص المهمة لهذه الشبكة، هي أنَّها تنقل البيانات بسرعات تصل إلى حدود عشرة آلاف ميجابت لكل ثانية. وتجدر الإشارة هنا إلى أنَّ Wi-Fi وهو الاسم المستخدم بصورة شائعة كبديل عن التسمية (IEEE 802.11) مع أنَّ هذا الاستخدام خطأ من الناحية العلمية. لأنَّ Wi-Fi هو شعار لشركة يدل على إمكانية اتصال الأجهزة التي تتبع المعيار السابق معاً. الشكل (2) يوضّح نقطة اتصال لاتصال أجهزة ضمن شبكة مناطق محلية.[4][1]

3- شـــــبكات لاســـــلكية محـــــددة (Data Wieless Fixed):

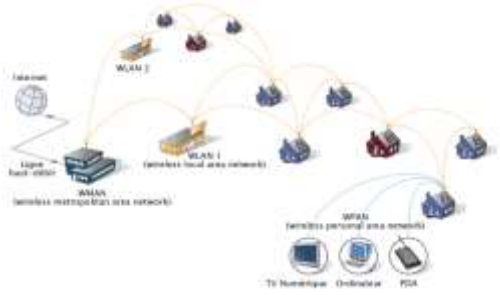
وهي شبكات لاسلكية تُستخدم لتحقيق اتصال بين جهازين أو شبكتين في مكانين مختلفين. يكون ذلك من خلال استخدام موجات صغرية أو أشعة ليزرية على مدى خط البصر، وغالباً ما يُستخدم هذا النوع من الشبكات لربط شبكات في أبنية متجاورة دون الحاجة إلى ربط هذه الأبنية فيزيائياً مع بعضها.

الشكل (2) يوضّح نقطة اتصال لاتصال أجهزة ضمن شبكة مناطق محلية.

4- شبكات المناطق الكبيرة اللاسلكية (WMAN):

وهي اختصار إلى Wireless Metropolitan Area Network ، وتربط عدة شبكات (WLAN) مع بعضها بعضاً لتحقيق شبكة لاسلكية تمتد على رقعة جغرافية متوسطة الحجم مثل حرم جامعي أو مدينة. الخدمة التي تؤديها تشابه للخدمة التي يقوم بها مزود الإنترنت Internet Service Provider(ISP).

إن التعبير المستخدم للإشارة إلى هذا النوع من الشبكات هو (WiMAX)، ويتناوله المعياران (IEEE 802.16d) و(IEEE 802.16e) الموضوعان من قبل جمعية مهندسي الكهرباء والإلكترونيات ويوضّح الشكل (3) مثالاً على شبكة مناطق كبيرة MAN.



الشكل (3) مثال على شبكة مناطق كبيرة.

5- شبكات ad hocاللاسلكية:

وهي عبارة عن شبكات لاسلكية تعتمد على العقد الراديوية التي تكون منظمة ضمن طبلوجيا الوصل المتشابك للشبكات. إذْ إنَّ كل عقدة تقوم بتمرير الرسائل إلى بقية العقد المتصلة معها، ومن ثَمَّ تقوم كل عقدة بدور موجه.

6- شـــبكات المنـــاطق الواســـعة اللاســـلكية (WWAN):

وهي اختصار إلىWireless Wide Area Network وتقوم بتغطية مساحات واسعة جداً، فمثلاً يمكن أن تغطي مسافات بين عدة مدن أو بلدات وضواحيها. يمكن أن تستخدم أيضاً لتغطية شركة لديها فروع في أكثر من دولة، وهي نوع الشبكات اللاسلكية الذي يعتمد عليه الإنترنيت.

7- شبكات الأجهزة الخلوية:

إن التطور الذي حصل في المدة الأخيرة في مجال الشبكات الخليوية مكنّنا من نقل معطيات ومعلومات عن طريق هذه الشبكات فضلاً عن الهدف الأساسي منها؛ ألا وهو نقل المحادثات بين جهازين خلويين.

إيجابيات استخدام الشبكات اللاسلكية وسلبياتها:

من أهم الإيجابيات:

المرونة: للشبكات اللاسلكيه فوائد أكثر من الشبكات السلكيه، وإحدى هذه الفوائد المرونة إذ تمر موجات الراديو بالحيطان والحاسوب اللاسلكي يمكن أنت يكون في أي مكان على نطاق نقطة الوصول (Access Point).

سـهولة الاسـتخدام: الشـبكات اللاسـلكية سـهلة الإعـداد والاسـتعمال تحتـاج فقـط تجهيـز الحاسـوب ببطاقـة شـبكة اتصالات لاسلكيه.

مـع هذه الإيجابيات فإن الشبكات اللاسلكية لا تخلو من بعض المشكلات أهمها:

مشـكلات التوافـق: فـالأجهزة المصـنوعة مـن قبـل شـركات مختلفة قد لا تتمكن من الاتصال مع بعضها، أو قد تحتاج إلى جهد إضافي للتغلب على هذه المشكلات.

تكـون الشـبكات اللاسـلكية غالبـاً أبطـأ مـن الشـبكات الموصولة مباشرةً باستخدام تقنيات Ethernet.[2][1]

الشبكات اللاسلكية أضعف من حيث حماية الخصوصية؛ لأنَّ أي شـخص ضـمن مجـال تغطيـة شـبكة لاسـلكية يمكنـه محاولة اختراق هذه الشبكة. من أجل حل هذه المشكلة، يجب استخدام خوارزميات تشفير للشبكة اللاسلكية.

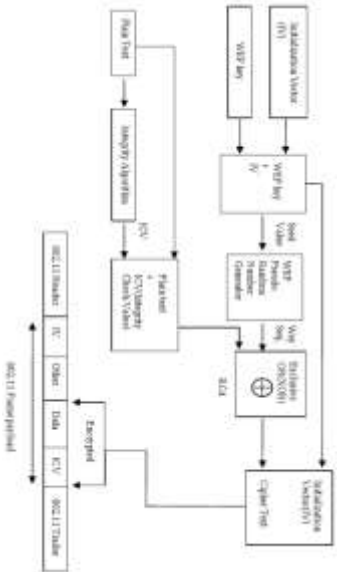
1- خوارزميات السرية المكافئةWEP:

هذا التدبير الأمني مخصص للشبكة المحلية اللاسلكية، وهو جزء من معيار الأمان IEEE 802.11.

فـي WEP، يُسْـتَخدَمُ كـود التكـرار الـدوري (CRC-32) لتوفير أمن البيانات وتكاملها، في حين يُسْتَخدَمُ تدفق RC4 ci-pher لتوفير الخصوصية. تدعم مواصفات WEP القياسية طول مفتاح 40 بتاً في حين توفر المواصفات غير القياسية طول مفتاح 128 و256 بتاً في تشفير البيانات.

آلية التشفير المستخدمة في WEP

تتكون عملية تشفير WEP لنقل البيانات من 5 خطوات كما هو مبيّن في الشكل (4). في عملية التهيئة، يرتبط متجه 24 بتاً معاً في شكل سلسلة مع مفتاحWEP40 بتاً. النتيجة تشكل المفتاح المرتبط بمنزلة قيمة أولية لمولد الأرقام العشوائية الزائفة. تُنفَّذُ خوارزمية تكامل على النص العادي بحيث يمكن إنشاء قيمة التحقق من النزاهة (ICV) التي ترتبط بعد ذلك بالنص العادي. لإنشاء نص التشفير، تُطَبَّقُ خوارزمية RC4 على النص العادي فضلاً عن ICV وتسلسل المفاتيح. يُنْشَأُ إطـار الحمولـة اللاسـلكية للـتحكم فـي الوصـول إلـى الوسـائط (MAC) عـن طريـق وضـع ناقـل التهيئـة (IV) أمـام البيانـات المشفرة التي تجمع بين ICV وحقول أخرى.

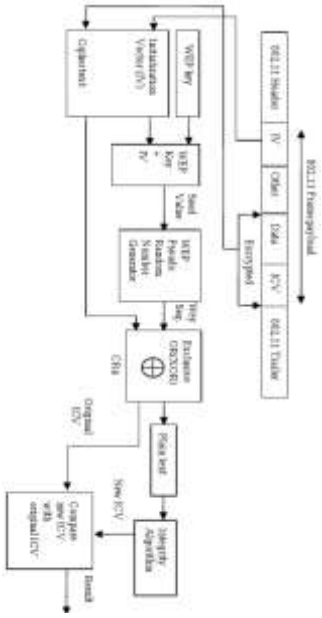


الشكل (4) خطوات آلية التشفير المستخدمة في WEP

2- آلية فك التشفير المستخدمة في WEP:

فـي عمليـة فـك تشـفير WEP، يحـدث مـا يـأتي كمـا هـو موضّـح فـي الشـكل (5). يـرتبط متجـه التهيئـة مـن الإطـار القياسي 802.11 بمفتاح WEP، الذي يعمل كقيمة أولية لمولد الأرقام العشوائية المزيفة. في الحصول على النص العادي، تُطَبَّقُ خوارزميـة CR4 علـى نـص التشـفير وتسلسـل المفـاتيح. يـتم الحصـول علـى الـنص العـادي وICV الأصـلي فـي هـذه المرحلة.

لإنشاء ICV الجديد، يُضَافُ النص العادي إلى خوارزمية النزاهة للحصول على ICV الجديد. تقارنُICV الجديدة التي تم إنشاؤها في المرحلة السابقة مع ICV الأصلي للتحقق من سلامة البيانات.



الشكل (5) آلية فك التشفير في WEP

نقاط الضعف الأمنية في WEP:

يحتوي بروتوكول WEP على بعض نقاط الضعف في الأمان مثل:

1) تشفير ضعيف: أظهرت حركة مرور الشبكة الملتقطة التي حُلِّلَتْ أنَّ المفتاح المشترك الذي اِسْتُخدمَ بواسطة WEP يمكن فك تشفيره بسهولة عند تحليل البيانات التي تم التقاطها. يمكن أن يؤدي ذلك إلى معالجة البيانات وفقدان البيانات.
2) غياب إدارة المفاتيح: لا تملك WEP ميزة إدارة المفاتيح لإدارة المفاتيح المختلفة في جدولها الرئيسي، بدلاً من ذلك يُسْتَخْدَمُ المفتاح نفسه مدة طويلة جداً من الوقت؛ وهذا يدل على جودة رديئة.
3) حجم مفتاح صغير: حجم مفتاح معيار WEP هو مفتاح 40 بتاً فقط. هذا يجعل WEP مفتوحًا للهجوم بشكل خاص على القوة الغاشمة، لأنَّ مفتاح التشفير لا يتجاوز 40 بتاً. هجوم القوة الغاشمة كنموذج لآلية القاموس غير المتصل بالشبكة التي تحقق في الشبكة باستخدام كلمات تشفير مستخدمة بشكل متكرر، وتحقق من البيانات التي تم الحصول عليها من حركة المرور الملتقطة للحصول على عبارة المرور السرية.
4) إعادة استخدام متجه التهيئة: من التوضيح في الشكل 4 والشكل 5، اِسْتُخْدِمَ متجه التهيئة نفسه. يمكن أن يؤدي ذلك إلى فك تشفير البيانات دون استخدام المفتاح المناسب، لأنَّه يمكن الحصول على IV بسهولة، ويمكن استخدام تطبيقات تشفير أخرى لفك تشفير البيانات.
5) مشكلات المصادقة: نظراً إلى خطة مواجهة التحدي المستخدمة في مصادقة المفتاح المشترك، فإنَّ هذا النوع من الهجوم الذي يمتلك كوجهة أو مصدر مطابق لبيانات في شبكة أخرى للوصول إلى المعلومات السرية التي هي في الطريق. هذا يؤدي إلى تعرض المعلومات الحساسة للخطر، وإذا أمكن ذلك يمكن أن يؤدي أيضاً إلى فقد البيانات.
6) تزوير الحزمة: لا توجد حماية ضد تزوير الحزمة في WEP. يمكن تزوير حزم البيانات باستخدام تطبيق تابع لجهة خارجية وإدخالها في الشبكة، ممَّا قد يؤدي إلى معالجة البيانات وفقدان تكامل البيانات.
7) الفيضانات: هذا هو إرسال حزم البيانات الضخمة التي تحتوي على كثير أو الرسائل إلى نقطة وصول، ومن ثَمَّ تمنع المستخدمين الشرعيين من الوصول إلى الشبكة، وكذلك الحد من نقطة الوصول من معالجة البيانات في حركة المرور.

الهجمات الشائعة في WEP:

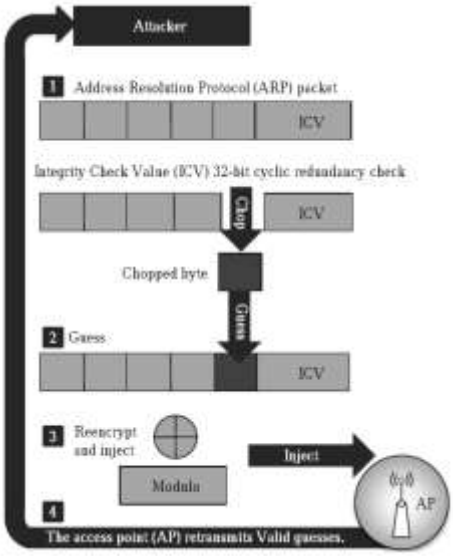
Korek Chopchop Attack: في هذا النوع من الهجوم، يمكن للمهاجم فك تشفير البايتات الأخيرة للنص غير المشفر للحزمة المشفرة عن طريق إرسال 128*s عدد الحزم على الشبكة. هذا الهجوم لا يُظهر مفتاح الجذر كما هو موضّح بالشكل 6 . يقوم المهاجم بقطع البايت الأخير عن حزمة البيانات الملتقطة، وتخمين البايت الأخير من الحزمة الملتقطة،

ويعدلها ويرسلها إلى نقطة الوصول. إذا كانت البايت المعدلة الأخيرة التي خمنها المهاجم صحيحة، فستقبل نقطة الوصول حزمة البيانات. ينتقل المهاجم إلى تخمين البايت الثاني الأخير، ويستمر حتى يتم تخمين البيانات بالكامل. ولكن إذا كانت البايت الأخيرة التي تم تخمينها من الحزمة التي اِلْتُقِطَتْ خطأ، فإن نقطة الوصول تتجاهل الحزمة.

Bittau's Fragmentation Attack:

هذه الطريقة الهجومية تمنح المهاجم الحافة في العثور على المفاتيح من الطول، بعد العثور على المفاتيح، يرسل المهاجم الحزمة ذات طول الحمولة المقابل s-4، ويزيل أربعة بايتات من ICV. إذا كانت الحزم طويلة، يمكن تقسيم ما يصل إلى 16 جزءاً بتوزيع حمولة الحزمة s-4 وفقاً لذلك. بعد استلام الحزمة وإعادة تجميعها بواسطة نقطة الوصول، تقوم حزمة البيانات بإعادة تشفيرها باستخدام دفق مفتاح جديد. يعرف المهاجم بالفعل النص العادي حتى يتمكن أيضاً من الحصول على دفق المفاتيح الجديد.

الأشكال الأخرى لهجوم WEP هي Fluhrer و Mantin و Shamir (FMS) Attack و Pyshkin و Tews و Weimann و (PTW) Attack.



الشكل (6) الهجوم على شبكات WEP

2- الوصول المحمي للشبكة اللاسلكية:

WI-FI Protected Access:
Pre Shared Key WPA: PSK

شُرِحَتْ عملية تشفير WPA في الشكل 7 أدناه. يوضح الشكل 7 عملية تشفير WPA، إذْ يُسْتَخدَمُ بروتوكول تكامل المفتاح الزمني (TKIP) بواسطة WPA لتشفير البيانات. هذا يلغي استخدام المفتاح نفسه في التشفير، ويُنْشَأُ مفتاح مختلف عشوائياً لكل حزمة بيانات، ويستخدم مفتاح 128 بتاً لتشفير حزمة البيانات. تُدْمَجُ خوارزمية Michael مع TKIP التي توفر حماية إعادة التشغيل، وتستخدم كود تكامل الرسائل (MIC) لضمان تكامل البيانات على مستوى عالٍ. هذا أكثر أماناً مقارنةً بالواحد في WEP الذي يستخدم 32 بتاً. آليات مصادقة WPA: الآليات التي يوفرها WPA هي مفتاح WPA الشخصي أو مفتاح WPA المشترك مسبقًا (WPA-PSK). مفتاح WPA المشترك مسبقًا ثابت ويُسْتَخدَمُ في بدء الاتصال بين مستخدمين. المفتاح الثابت هو المفتاح الرئيسي للزوج (PMK) في TKIP، ويجب أن يكون جاهزًا قبل أن يمكن تعيين اقتران. في WPA-PSK، خادم المصادقة غير مطلوب لأنَّه أكثر ملاءمة للشبكات الصغيرة أو المكاتب المنزلية. يُسْتَخدَمُ مفتاح 256 بتاً لمصادقة الأجهزة ومفتاح MIC 64 بتاً ويُنْشَأُ مفتاح 128 بتاً من المفتاح المشترك مسبقًا لتشفير البيانات. WPA-Enterprise: صُمِّمَ هذا أساساً لشبكات المؤسسات، إذْ يوفر EAP طريقة مصادقة أقوى. يعدُّ طلب المصادقة عن بُعد في خدمة المستخدم (RADIUS) ضرورياً لتوفير أمان ممتاز للشبكة اللاسلكية.

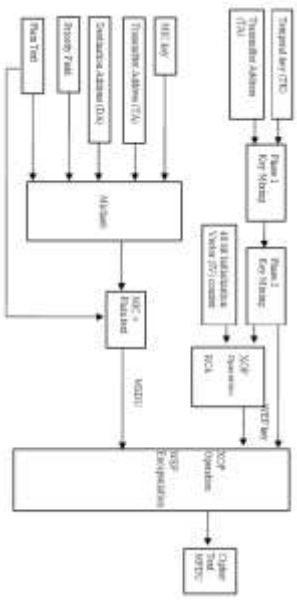
نقاط الضعف في الأمن من WPA

في WPA، توجد مجموعة متنوعة من الثغرات الأمنية المتوافرة، وهي: تستخدم WPA خوارزمية تشفير RC4 بدلاً من معيار التشفير المتقدم (AES) الأكثر أماناً والتشفير بشكل أفضل. يمكن أيضاً تنفيذ هجوم القوة الغاشمة على WPA. WPA مفتوح أيضاً لهجمات DoS. عملية الإعداد أو التكوين معقدة. في WPA، هناك عدة هجمات شائعة فيها مثل Beck

Tews Attack - و Ohigashi - Morii Attack و Micheal Reset Attack.

WPA2:

بروتوكول WPA2 هو تحسين على WPA. طُبِقَ 802.11i بالكامل في WPA2. يتعلق التغيير الرئيسي الذي تم في WPA2 على WPA بخوارزمية تشفير البيانات. يستخدم Counter Mode مع Cipher block Chaining Message Authentication Protocol (CCMP) تشفير البلوك وهو معيار التشفير المتقدم (AES) لتشفير البيانات. يوضّح الجدول 1 المقارنة بين بروتوكولات WEP و WPA و WPA2 من حيث الأمان. مجموعة متنوعة من البحوث التي أجريت في الأدب لتعزيز الأمن في الشبكات اللاسلكية. ومع ذلك، نظراً إلى طبيعة بنية الشبكات اللاسلكية الضعيفة وتنوع الهجمات، لا يمكن أن تنجح التصنيفات المختلفة وحتى المخططات المختلفة في تحقيق أهداف الأمان في الشبكات اللاسلكية.



الشكل (7) عملية تشفير TKIP

WPA Radius

نظام يتحكم بصلاحية المستخدمين للشبكة عن طريق ربط الشبكة بمزود يقوم بمراقبة الداخلين على الشبكة. يستخدم هذا النظام في معظم المطاعم والمحلات التي توفر خدمة الاتصال عبر شبكة لاسلكية. بمجرد دخول المشترك يُحَوَّلُ إلى شبكة أخرى ولكن بعد أن يدخل كلمة السر يقوم المزود بإعادة دخوله إلى الشبكة، لزيادة حماية أمن الشبكة يمكن الغاء خاصية (SSID Broadcast) التي تمكن أي شخص من العثور على الشبكة والاتصال بها. في حال إلغاء (SSID Broadcast) ستصبح الشبكة مخفية، ويجب عليك الاتصال بالشبكة يدوياً. ولكن برنامج (Kismet) يتمكن من إظهار الشبكة حتى إذا كانت مخفية. ويجدر هنا ذكر أنَّ بعض الموزعات اللاسلكية تستخدم خاصية (Wireles DistributionSystemWDS) التي تمكنها من زيادة مدى الشبكة عن طريق اتصالها بموزعات أخرى، وتقوم بالبث عن طريقها.

بعضهم يفضل بأن يحدد الأجهزة التي تستطيع أن تشبك على الشبكة اللاسلكية عن طريق تحديد عنوان للجهاز (Filter MAC address)، ولكن يمكن اختراق هذه الطريقة عن طريق ما يعرف بـ (Spoofing MAC address)؛ وهي أن تقوم بتغيير عنوان MAC بانتحال عنوان MAC لشخص يسمح له بالاتصال. ويمكن معرفة (MAC) للأجهزة الأخرى عن طريق برنامج (Airodump) .[6][3]

الفروق بين أنواع التشفير في الشبكات اللاسلكية

يعتقد كثير من الناس أنّه لا يوجد فرقٌ بين نوعي التشفير (WEP و WPA)، ولكن في الحقيقة يوجد فرقٌ شاسعٌ بينهما:

إذْ يُعدُّ WEP أقدم من WPA، فهو معيارٌ لأجهزة الجيل الأول اللاسلكية، إذ يعتمد على تشفير البيانات من خلال موجات الراديو من لحظة إرسالها لاستقبالها، بحيث تكون

محمية في أثناء إرسالها، ولكن يكمن ضعف هذا النوع في عدم منعه لأي متجسس من فك تشفير البيانات المشفرة دون معرفة كلمة المرور. كما يمكن بسهولة وضع احتمالات لمفاتيح التشفير، التي تأخذ قيمها بين A وZ، ومن 1الى 9 فقط .[3]

لحلّ هذه المشكلة، ينبغي للمستخدم تغيير كلمة المرور دورياً كل مدة معينة، وهو أمر غير مريح إطلاقاً. ويبين الجدول (1) مقارنة بين أنواع التشفير والميزات والاختلافات بينها.

الجدول (1) مقارنة بين أنواع التشفير

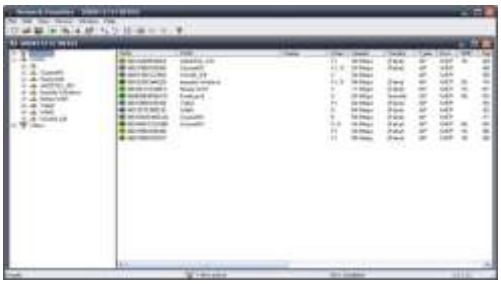
نوع التشفير	WEP	WPA	WPA2
أمن المعلومات (التشفير)	Rivest Cipher 4 (RC4)	TKIP	يتم توفير المصادقة من خلال كتل chipper مع CCMP و AES
المصادقة	WEP-Openو WEP-Shared	WPA-PSK و WPA-Enterprise	WPA2-Personal و-WPA2 enterprise
تكامل البيانات	CRC-32	من خلال رمز تكامل الرسائل	شفرة مصادقة رسائل تسلسل كتلة التشفير (CBC-MAC)
دارة المفاتيح	غير موجودة	4 طرائق مصادقة آلية	4 طرائق مصادقة آلية
قابلية الإصابة	ضعيف ضد Chop Chop، وتفتت Bittu وهجمات DoSالمتنوعة	عرضة للهجمات ضد Chop Chop و-Ohigashi Morii و-WPA Dos و PSK	عرضة للهجمات ضد DoS بسبب إطارات التحكم غير المحمية وخداع MAC
إعادة حماية الهجوم	لا حماية ضد هجمات الإعادة	تنفذ عداد تسلسل لحماية الإعادة	تنفيذ مخطط البيانات/ رقم الحزمة 48 بتاً يحمي من هجوم الإعادة

بعض برامج الاختراق:

البرامج التي اِسْتُعْرِضَتْ مُهمّتها هي اختراق Wi-Fi (للحاسوب)، وتعمل على كسر حماية بطاقات الشبكات، وحماية WEP/WPA/WPA2 وتختلف البرامج من حيث نوع التشفير وإمكانيتها لدعم أكثر من شبكة مُختلفة.

1- برنامج (Netstumbler):

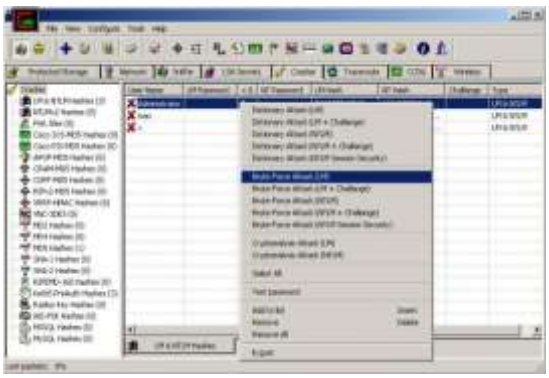
يقوم البرنامج بعمل مسح شامل لإظهار معلومات عن الشبكة وحالة الاتصال بالشبكة وقوتها، وإذا ما كانت الشبكة محمية بكلمة سر للدخول أم لا، يكتشف شبكات (b,802.11a,802.11g802.11) ويقوم بفك تشفير بيانات Wi-Fiوأجهزة نقاط الوصول Access Point، ولكن يعيبه أنه يسهل كشفه من قبل إعدادات حماية أجهزة الراوتر العادية. يبيّن الشكل (8) برنامج Netstumbler.



الشكل (8) برنامج Netstumbler.

2- برنامج (Cain and Abel):

وهو الأفضل لأنَّه يبقي على الاتصال اللاسلكي قائماً وهو يعمل، عكس باقي برامج ال WIFI scanner إذْ يقوم بفصل "WZC "Wireless Zero Configuration الذي يقوم بإعداد كروت الموزعات اللاسلكية التي تستخدم الاستاندر 802.11. برنامج cain يحتوي على خصائص كثيره مثل إمكانية عمل sniff للشبكة وعمل arp-poision.



الشكل (9) برنامج Cain and Abel.

3- برنامج (Aircrack):

يعدُّ من أشهر برامج كسر حماية الواي فاي، ويستخدم عدة خوارزميات مُختلفة لكسر تشفير شبكات الإنترنت الهوائية من نوع (WPA)، ويقوم أولاً بجمع المعلومات وفحص الشبكات، ثم البدء بعملية كسر كلمة السر. ويوضّح الشكل (10) برنامج Aircrack

الشكل (10) برنامج Aircrack

5- برنامج (Kismet):

مُتخصص في اكتشاف شبكات (802.11b,802.11a,802.11g1) ويقوم بسحب بعض البيانات من الشبكة ليتم فك التشفير ومنحك كلمة السر، كما يُمكنه اكتشاف شبكات Wi-Fiالمخفية، ويُميّز البرنامج أنَّه يُمكنه أن يعمل عبر طائرة Drone دون طيار لالتقاط شبكة Wi-Fi وكسر تشفيرها.

ويبيّن الشكل (11) برنامج Kismet. بينما يبين الشكل (12) دارة صغيرة تعمل مع برنامج Kismet يمكن وضعها على طائرة Drone.

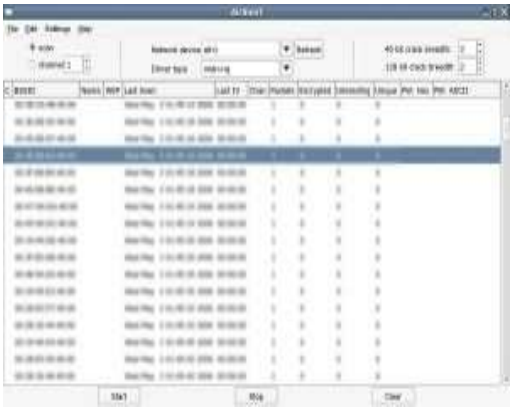
الشكل (11) برنامج Kismet.

6- برنامج (AirSnort):

يكتشف شبكات (802.11b WEP)، وهو برنامج مفتوح المصدر، ويقوم بحفظ البيانات على ملف (dump pcap)، أو على هيئة ملفات مُعدّلة. ويسهل إستخدام البرنامج حيث لن تحتاج إلّا لتشغيل عملية الفحص والتأكد من تشغيل خيار NIC Wireless.

يوضّح الشكل (13) برنامج AirSnort.

الشكل (12) دارة صغيرة تعمل مع برنامجKismet يمكن وضعها على طائرة Drone.



الشكل (13) برنامجAirSnort

ثماني خطوات من أجل حماية الشبكة اللاسلكية من الاختراق:

الخطوة الأولى: اختيار نوع التشفير

تتيح لك الراوترات عادة عدة خيارات من نظام التشفير مثل (WEP,WPA2،WPA)، قم باستخدام نظام التشفير (WPA2) الذي يعدُّ من أقوى الأنظمة المتاحة، تجنب

استخدام النظام (WEP) إذْ أنَّه غير آمن، ويمكن اختراقه ببضع دقائق من خلال أدوات مجانية يمكن تحميلها من الإنترنت، بعض الراوترات القديمة لا تملك نظام التشفير(WPA2) يمكن عندها استخدام النظام (WPA) [5][6].

الخطوة الثانية: استخدام كلمة مرور قوية

حتى إذا استخدمت نظام التشفير القوي (WPA2) فما زال من الممكن اختراق الشبكة وذلك من خلال تخمين كلمة المرور مثلاً، لذلك قم باستعمال كلمة مرور قوية، اتبع هذه التوجيهات من أجل اختيار كلمة مرور قوية:

- استخدم 10 خانات على الأقل.
- استخدم مزيجاً من الحروف الصغيرة والكبيرة والأرقام والرموز.
- ابتعد عن الكلمات السهلة والشائعة.

الخطوة الثالثة: إلغاء تفعيل WPS

إن تفعيل خاصية ال (WPS) يسهل من اتصال الأجهزة بالراوتر؛ وذلك عن طريق إدخال رقم معين (PIN)؛ وذلك عوضاً عن إدخال كلمة المرور كلّها. ولكن بالمقابل فإن هذه الخاصية تسهل الأمر كثيراً على المخترقين الذين ما عليهم سوى معرفة رقم ال (PIN) من أجل الولوج إلى الشبكة. إنَّ إلغاء تفعيل هذه الخاصية أمر مهم جداً إذا أردت الحفاظ على شبكتك من الاختراق مع الانتباه أن بعض الراوترات القديمة لا تتيح لك إمكانية التغيير، إلاَّ أنَّ معظم الراوترات الحالية إمَّا أنَّها لا تأتي مع هذه الخاصية أصلاً، أو تحوي خياراً من أجل إلغاء هذه الخاصية بسهولة.[6][5]

الخطوة الرابعة: إخفاء الشبكة

إن جعل الشبكة مخفية يصعب الأمر على المخترقين قليلاً إّذْ سيتطلب منهم معرفة اسم الشبكة المخفية أولاً، ثم محاولة الاختراق. يوجد بعض الأدوات التي تستطيع معرفة اسم الشبكة حتى إذا كانت مخفية.

الخطوة الخامسة: استخدام تصفية (MAC Address)

تُصعّب هذه الخطوة اختراق الشبكة كثيراً إذْ ستحدد عن طريق هذه الميزات الأجهزة المسموح له بالاتصال بالشبكة الخاصة بك وذلك عبر إضافة عنوان MAC الخاص بكل جهاز تسمح له باستخدام شبكتك. مع الانتباه إلى أنَّه يمكن تغيير عنوان MAC لجهاز ما ليصبح أحد عناوين MACالمسموح لها الاتصال بالشبكة.

الخطوة السادسة: تغيير اسم المستخدم وكلمة المرور الخاصة بالرواتر

قد يغفل كثير من المستخدمين عن هذه الخطوة المهمة إذْ إنِّ الراوترات جميعها تأتي باسم مستخدم وكلمة مرور افتراضية من أجل الدخول إلى إعدادات الراوتر، إن تغيير اسم المستخدم وكلمة المرور (بعض الراوترات لا تتيح تغيير المستخدم) يصعب الأمر على المخترقين الذين يحاولون اختراق الراوتر باستخدام البيانات الافتراضية.

الخطوة السابعة: قم بإلغاء تفعيل تسجيل الدخول البعيد (login Remote)

يمكن للهاكرز(المخترقين) أن يقوم بمحاولة الهجوم على الراوتر نفسه، حيث يكون اسم المستخدم الافتراضي لمعظم الراوترات (Admin)، وعندها يمكن للهاكرز (المخترقين) معرفة كلمة المرور بوسائل خاصة. ولكن لحسن الحظ فإنَّ هذه الخاصية (تسجيل الدخول البعيد) تكون غير مفعلة افتراضياً. تأكد من هذا الأمر عندما تقوم بإعداد الراوتر.[5]

الخطوة الثامنة: قم بإلغاء تفعيل إدارة الراوتر عبر الشبكة اللاسلكية

باستخدام هذه الخيار سيتيح لك فقط تغيير إعدادات الراوتر عبر الشبكة السلكية (LAN) فقط، ولن يسمح لباقي المستخدمين المتصلين عبر Wi-Fi تغيير الإعدادات حتى إذا عرفوا اسم المستخدم وكلمة المرور الخاصة بالراوتر.[6]

الخلاصة:

لا توجد حماية مطلقة للشبكات اللاسلكية ولكن هنالك طرائق وخطوات يجب علينا اتباعها لحماية الشبكة اللاسلكية من الاختراق، ويسعى العلماء جاهدين لإيجاد طريقة تشفير لا يمكن اختراقها، ولكن في النهاية لكل قفل مفتاح، وتجدر الاشارة إلى وجود ما يسمى بالقرصنة الأخلاقية التي لها أهمية كبيرة في الحفاظ على أمن المنظمات وتطبيقاتها من هجمات القرصنة الخبيثة فيمكن أن نقول إنَّ أفضل طريقة للدفاع هي جريمة كبيرة بمعنى أنه من أجل حماية النظام الذي لدينا يجب أن نحاول أن نقوم باختراقه لمعرفة نقاط الضعف والثغرات والعمل على حلها قبل أن تُسْتَخْدَم من قبل الهجمات الخبيثة التي تهدد أمن النظام، وهناك عدة تسميات تطلق على الأشخاص الذين يقومون بالقرصنة الأخلاقية مثل : قراصنة القبعة البيضاء، القراصنة القانونيين وغيرها من التسميات، وكلها تدل على قراصنة تساعد المنظمات على الكشف عن القضايا الأمنية لمنع استغلال العيوب الأمنية الموجودة في أي منظمة .

References

[1]Jing، Qi, et al. "Security of the Internet of Things: perspectives and challenges." Wireless Networks 20.8 (2014): 2481-2501.

[2]Wright, Joshua, and Johnny Cache. Hacking exposed wireless: wireless security secrets & solutions. McGraw-Hill Education Group, 2015.

[3] Adnan, Abdillahi Hassan, et al. "A comparative study of WLAN security protocols: WPA, WPA2. "Advances in Electrical Engineering (ICAEE), 2015 International Conference on.IEEE, 2015.

[4]Malgaonkar, Saurabh, et al. "Research on Wi-Fi Security Protocols." International Journal of Computer Applications 164.3 (2017).

[5]Nair, Radhi S., and Dr Ashok Babu. "A Survey on Wi-Fi Security Techniques." (2018).

[6]He, Ling, et al. "Talking about WIFI's New Security." MATEC Web of Conferences. Vol. 139.EDP Sciences, 2017.

Received	2019/1/7	إيداع البحث
Accepted for Publ.	2019/4/11	قبول البحث للنشر