ITRAINONLINE MMTK

أمن الشبكات اللاسلكية – كراسة المتدرب

إعداد: ألبيرتو إسكوديرو باسكال، aep@it46.se
النسخة العربية: أنس طويلة، anas.tawileh.net

فهرس المحتويات

1. عن هذا المستند

تشكل هذه المواد التدريبية جزءاً من حزمة تدريب الوسائط المتعددة (MMTK Multimedia Training Kit). توفر هذه الحزمة مجموعةً متكاملةً من المواد التدريبية والموارد الداعمة للإعلام الإجتماعي، مراكز الوسائط المتعددة للمجتمعات، مراكز الولوج البعيد وغيرها من المبادرات باستخدام تقنيات المعلومات والإتصالات لتدعيم المجتمعات ودعم نشاطات التنمية.

1.1 معلومات حفظ الملكية الفكرية

2.1 المتطلبات المسبقة

ننصحك بقراءة وحدة "التشبيك المتقدم" قبل البدء بهذه الوحدة.

3.1 درجة الصعوبة

درجة صعوبة هذه الوحدة: متقدم.

2. مقدمة

سنستهل هذه الكراسة بتقديم ملخصٍ عن نموذج OSI المرجعي والمبادئ الأساسية لأمن الشبكات قبل استعراض أمن الشبكات اللاسلكية في سياق بروتوكول IEEE 802.11 أو WLAN.

تشرح هذه الوحدة مفاهيم الأمن في سياق أمن المعلومات. سنقوم بشرح خمسة خصائص للأمن متعلقة بالشبكات اللاسلكية (السرية Confidentiality، التحقق من الهوية Authentication، الكمال Integrity، مكافحة الإنكار Non-Repudiation والتوفر Availability) وتقييمها لاحقاً في سياق الشبكات اللاسلكية. تخلص الوحدة إلى استعراض بعض التهديدات الأمنية الهامة التي ينبغي معالجتها عند تصميم الشبكات اللاسلكية.

3. تعريف أمن الشبكات اللاسلكية

يعتمد تعريف الأمن إلى حد كبير على السياق، لأن كلمة الأمن تشير إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات. قد نتكلم مثلاً عن الأمن عند توصيف الإجراءات الوقائية على الطرق العامة

أو عند استعراض نظام حاسوبي جديد يتمتع بمناعة عالية ضد فيروسات البرمجيات. لقد تم تطوير أنظمة عدة لمعالجة الجوانب المختلفة لمفهوم الأمن.

بناء على ذلك فقد قمنا بصياغة مصطلح "أمن الشبكات اللاسلكية" ضمن تصنيف محدد للأمن بغية تسهيل مهمتنا في دراسة الأمن في مجال الشبكات اللاسلكية. تقوم هذه الوحدة بتعريف أمن الشبكات اللاسلكية ضمن سياق أمن المعلومات، أي أننا عندما نتحدث عن أمن الشبكات اللاسلكية فإننا نعني أمن المعلومات في الشبكات اللاسلكية WLAN[1].

4. ماهو أمن المعلومات؟

لكي نتمكن من استيعاب مفهوم أمن المعلومات لا بد من استعراض السياق التاريخي لتطور هذا المفهوم.

لقد ظل هذا المجال من الأمن حتى أواخر السبعينيات معروفاً بإسم أمن الإتصالات Communication Security (COMSEC) والذي حددته توصيات أمن أنظمة المعلومات والإتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:

"المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الإتصالات ولضمان أصالة وصحة هذه الإتصالات".

تضمنت النشاطات المحددة لأمن الإتصالات COMSEC أربعة أجزاء هي: أمن التشفير Cryptosecurity، أمن النقل Transmission Security، أمن الإشعاع Emission Security والأمن الفيزيائي Physical Security. كما تضمّن تعريف أمن الإتصالات خاصيتين تتعلقان بموضوع هذه الوحدة: السرية والتحقق من الهوية.

1.4. السرية

التأكيد بأن المعلومات لم تصل لأشخاص، عمليات أو أجهزة غير مخولة بالحصول على هذه المعلومات (الحماية من إفشاء المعلومات غير المرخص).

2.4. التحقق من الهوية

إجراء أمني للتأكد من صلاحية الإتصال، الرسالة أو المصدر أو وسيلة للتحقق من صلاحية شخص ما لاستقبال معلومات ذات تصنيف محدد (أو التحقق من مصدر هذه المعلومات).

بدأت في الثمانينات مع النمو المضطرد للحاسبات الشخصية حقبة جديدة من الأمن: أمن الحواسيب Computer Security (COMPUSEC) والتي حددتها توصيات أمن أنظمة المعلومات والإتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:

[1] وتعني هنا مجموعة عمل IEEE 802.11

"المعايير والإجراءات التي تضمن سرية، كمال وتوفر مكونات أنظمة المعلومات بما فيها التجهيزات، البرمجيات، البرمجيات المدمجة firmware والمعلومات التي تتم معالجتها، تخزينها ونقلها".

تضمن أمن الحواسيب الشخصية خاصيتين إضافيتين تتعلقان بموضوع هذه الوحدة: الكمال والتوفر.

3.4. الكمال

تعكس جودة أي نظام للمعلومات مدى صحة ووثوقية نظام التشغيل، التكامل المنطقي للتجهيزات والبرمجيات التي توفر آليات الحماية ومدى تناغم بنى المعلومات مع البيانات المخزنة.

4.4. التوفر

الوصول الموثوق إلى البيانات وخدمات المعلومات عند الحاجة إليها من قبل الأشخاص المخولين بذلك.

لاحقاً وفي التسعينات من القرن الماضي تم دمج مفهومي الأمن (أمن الإتصالات وأمن الحواسيب) لتشكيل ما أصبح يعرف باسم (أمن أنظمة المعلومات Information Systems Security – INFOSEC). يتضمن مفهوم أمن أنظمة المعلومات الخصائص الأربعة المعرفة مسبقاً ضمن مفاهيم أمن الإتصالات وأمن الحواسيب: السرية، التحقق من الهوية، الكمال والتوفر، كما أضيف إليها خاصية جديدة: مكافحة الإنكار.

5.4. مكافحة الإنكار (المسؤولية)

التأكيد بأن مرسل البيانات قد حصل على إثبات بوصول البيانات إلى المرسل إليه وبأن المستقبل قد حصل على إثبات لشخصية المرسل مما يمنع إحتمال إنكار أي من الطرفين بأنه قد عالج هذه البيانات.

5. أمن المعلومات والشبكات اللاسلكية

تعرّف توصيات أمن أنظمة المعلومات والإتصالات لوكالة الأمن القومي في الولايات المتحدة أمن أنظمة المعلومات كما يلي:

"حماية أنظمة المعلومات ضد أي وصول غير مرخص إلى أو تعديل المعلومات أثناء حفظها، معالجتها أو نقلها، وضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، بما في ذلك جميع الإجراءات الضرورية لكشف، توثيق ومواجهة هذه التهديدات".

سنعتمد في هذه الوحدة تعريف أمن الشبكات اللاسلكية من وجهة نظر أمن أنظمة المعلومات INFOSEC.

من الشائع في المنشورات المتعلقة بالشبكات اللاسلكية أن يتم توصيف ميزات أمن الشبكة دون تعريف إطار ملائم لمفهوم الأمن. إن مجرد سرد "الميزات" الأمنية سيترك لدى القارئ ميلاً إلى تذكر المصطلحات في حين سينسى الغاية المرجوة من كل ميزة من هذه الميزات. لتجنب ذلك فإننا لن نسرد جميع الميزات الأمنية المتوفرة في الشبكات اللاسلكية بل سنقوم باستعراض الخصائص الخمس لأمن أنظمة المعلومات ومن ثم تبيان كيفية تطبيق كل منها في الشبكات اللاسلكية.
هذا الأسلوب سيساعد القارئ على تبني طرائق منهجية أثناء تصميم الشبكات اللاسلكية الآمنة.
الخصائص الأمنية الخمس التي سنناقشها فيما يلي هي: السرية، التحقق من الهوية، الكمال، مكافحة الإنكار والتوفر.[2]

6. تطبيق الخصائص الأمنية

يقدم النموذج المرجعي OSI (ترابط الأنظمة المفتوحة Open Systems Interconnect) والذي ابتكرته منظمة المعايير الدولية ISO توصيفاً نظرياً لتصميم بروتوكولات الشبكات (الإتصالات) الحاسوبية. يقوم هذا النموذج بتقسيم وظائف الإتصال المختلفة إلى سبعة طبقات مختلفة تعمل بشكل مستقل عن بعضها البعض.

يتبع تصميم البروتوكولات وفق نموذج OSI (كما هو موضح في وحدة "مفاهيم التشبيك المتقدمة") مبدأ "التكديس Stack". إن استخدام نموذج للبروتوكولات يعمل وفق مبدأ الطبقات أو التكديس يعني أن كل طبقة ستستخدم وظائف الطبقة الأدنى منها فقط في حين تقوم بتخديم الطبقة التي تعلوها مباشرة فقط.
ينعكس أسلوب التصميم وفق مبدأ الطبقات بشكل مباشر على كيفية تطبيق الخصائص الأمنية.

[2] إذا ما كنت ترغب بالإطلاع على أسلوب رسمي أكثر عن الأمن راجع: المعايير العامة لتقييم أمن تقنية المعلومات، والذي غالباً ما يشار إليه بالإختصار "المعايير العامة CC". تحدد المعايير العامة المواصفات الوظيفية والتوكيدية لمنتجات وأنظمة الأمن.

ترتبط معايير الشبكات اللاسلكية عادة بالطبقتين الأولى والثانية من بروتوكول OSI دون المساس بالطبقات الأعلى أو حزم بروتوكول الإنترنت IP. يتم نقل "حزم بروتوكول الإنترنت IP" ضمن بروتوكولات لاسلكية خاصة بالطبقة الفيزيائية وطبقة ربط البيانات.

على سبيل المثال، إذا ما اعتبرنا "سرية البيانات المنقولة" بين نقطتي ولوج فإن تحقيق النتيجة ذاتها (سرية البيانات) يمكن أن يتم عبر عدة أساليب:

- طبقة التطبيقات (عبر بروتوكولات TLS/SSL)
- طبقة بروتوكول الإنترنت IP (عبر بروتوكول IPSEC)
- طبقة ربط البيانات (عبر التشفير اللاسلكي)

تذكر بأننا عندما نتحدث عن أمن الشبكات اللاسلكية فإننا نعني آليات الأمن المتواجدة ضمن الطبقتين الأولى والثانية، أي التشفير اللاسلكي (على مستوى الوصلة) على سبيل المثال. تشكل آليات الأمن الأخرى المتواجدة ضمن الطبقة الثالثة وما فوقها جزءاً من أمن الشبكة أو أمن التطبيقات.

1.6 ملاحظات عامة عن التشفير على مستوى الوصلة

يشكل التشفير على مستوى الوصلة آلية لتأمين البيانات أثناء انتقالها بين نقطتين متصلتين بنفس الوصلة الفيزيائية (ويمكن أيضاً أن يتصلا عبر وصلتين فيزيائيتين مربوطتين بمكرر للإشارة كما هو الحال في وصلات الأقمار الصناعية). يتيح التشفير على مستوى الوصلة حماية البروتوكولات أو البيانات المارة عبر الوصلة الفيزيائية من أعين المتطفلين.

يتطلب التشفير توفر مفتاح محدد أو سر مشترك بين الأطراف التي ستشترك في عملية التشفير بالإضافة إلى الإتفاق عل خوارزمية مشتركة للتشفير. في حال عدم تشارك المرسل والمستقبل في نفس الناقل الفيزيائي ينبغي فك تشفير البيانات وإعادة تشفيرها عند كل نقطة مرور أثناء انتقالها إلى المستقبل.

يستخدم التشفير على مستوى الوصلة عادة عند غياب التشفير على مستويات أعلى.

التشفير على مستوى الوصلة في الشبكات اللاسلكية العاملة وفق معايير 802.11

تعتبر خوارزمية السرية المكافئة للشبكة السلكية (Wired Equivalent Privacy (WEP أكثر خوارزميات التشفير استخداماً في الشبكات اللاسلكية العاملة وفق معايير 802.11 . لقد ثبت عملياً بأن هذه الخوارزمية غير آمنة، واستحدثت نتيجة ذلك بدائل أخرى عديدة منها الوصول المحمي للشبكة اللاسلكية Wi-Fi Protected Access (WPA) والتي تم اعتمادها كصيغة معيارية. سيتضمن المعيار الجديد للشبكات اللاسلكية 802.11i إصدارةً مطورةً من WPA تدعى WPA2.

لا يوفر التشفير على مستوى الوصلة أمناً مطلقاً خارج مجال الوصلة الفيزيائية، لذا يجب اعتباره على الدوام مجرد إجراء أمني إضافي لدى تصميم الشبكة اللاسلكية.

يستهلك التشفير على مستوى الوصلة مزيداً من موارد التجهيزات في نقاط الولوج كما يتطلب تصميم النواحي الأمنية المتعلقة بتوزيع وإدارة مفاتيح التشفير.

7. سرية الشبكات اللاسلكية

1.7. هل ينبغي استخدام خوارزمية السرية المكافئة للشبكة السلكية WEP أم لا؟

سنعرّف سرية الشبكات اللاسلكية بضمان أن المعلومات المرسلة بين نقاط الولوج وحواسب المستخدمين لن تصل إلى أشخاص غير مخولين. يجب أن تضمن سرية الشبكات اللاسلكية بأن الإتصالات الجارية بين مجموعة من نقاط الولوج ضمن نظام توزيع لاسلكي (Wireless Distribution System (WDS أو بين نقطة ولوج AP وحاسب متصل بها STA ستبقى محمية.

لقد ارتبط مفهوم سرية الشبكة اللاسلكية بمصطلح "السرية المكافئة للشبكة السلكية WEP". وقد شكلت WEP جزءاً من المعيار الأساسي IEEE 802.11 للشبكات اللاسلكية في العام 1999.

إن الهدف الرئيس من السرية المكافئة للشبكة السلكية WEP هو تأمين الشبكات اللاسلكية بمستوى من السرية مماثل للسرية المتوفرة في الشبكات السلكية. إن الحاجة إلى هذا البروتوكول كانت جلية: فالشبكات اللاسلكية تستخدم الأمواج اللاسلكية وبالتالي فهي أكثر عرضةً لأعين المتطفلين.

لقد كان عمر بروتوكول السرية المكافئة للشبكة السلكية WEP قصيراً للغاية، فقد أدى تصميمه الرديء وغير الشفاف إلى نجاح العديد من الهجمات في اختراق الشبكات التي تستعمل هذا البروتوكول. لم يستغرق الأمر سوى عدة أشهر من إطلاق البروتوكول حتى تم خرقه وهجرانه. على الرغم من أن طول مفاتيح التشفير كان محدوداً نتيجة بعض قوانين حظر التصدير إلا أن هذا البروتوكول قد أثبت ضعفه بغض النظر عن طول مفتاح التشفير المستخدم.

لكن العيوب التصميمية لم تكن السبب الوحيد في فشل بروتوكول السرية المكافئة للشبكة السلكية WEP، بل أن عدم توفر نظام لإدارة مفاتيح التشفير ضمن نفس البروتوكول قد ساهم أيضاً في إفشاله. لم يتضمن بروتوكول السرية المكافئة للشبكة السلكية WEP أي نظام لإدارة مفاتيح التشفير على الإطلاق، وكانت الوسيلة الوحيدة لتوزيع مفاتيح التشفير تتطلب إعداد / إدخال هذه المفاتيح يدوياً في كل وحدة من التجهيزات اللاسلكية (إلا أن السر المشترك بين عدة أشخاص لم يعد سراً!).
أدخل على بروتوكول السرية المكافئة للشبكة السلكية WEP عدد من التعديلات الخاصة ببعض منتجي التجهيزات اللاسلكية إلا أن هذه التعديلات لم ترقى إلى المستوى المطلوب لإنجاح البروتوكول (بعض الأمثلة تتضمن بروتوكول WEP+ من شركة Lucent وبروتوكول WEP2 من شركة Cisco).

يعتبر بروتوكول السرية المكافئة للشبكة السلكية WEP وتعديلاته WEP+ و WEP2 حالياً خارج الخدمة. يعتمد هذا البروتوكول على شيفرة سيل RC4 والتي أثبت تطبيقها ضمن معايير 802.11 بأنها غير آمنة.

هناك العديد من الهجمات والبرمجيات المتاحة لاختراق بروتوكول السرية المكافئة للشبكة السلكية (منها aircrack، kismac، wepcrack، Airsnort). تعتمد بعض هذه الهجمات على محدودية أرقام متجهات البدء في شيفرة سيل RC4 أو وجود ما يدعى بمتجه البدء الضعيف weak Initialization Vector في حزمة البيانات.

ننصح المهتمين بتاريخ بروتوكول السرية المكافئة للشبكة السلكية بمراجعة (موارد إضافية للمعلومات) المرفقة مع هذه الوحدة.

2.7. موت بروتوكول السرية المكافئة للشبكة السلكية WEP وولادة بروتوكولي الوصول المحمي للشبكة اللاسلكية WPA و WPA2...

بعد موت بروتوكول السرية المكافئة للشبكة السلكية WEP تم اقتراح بروتوكول الوصول المحمي للشبكة اللاسلكية WPA في العام 2003 ليتم اعتماده فيما بعد كجزء من معيار الشبكات اللاسلكية IEEE 802.11i عام 2004 تحت إسم WPA2.

لقد تم تصميم بروتوكولي WPA و WPA2 للعمل مع أو دون وجود مخدم لإدارة مفاتيح التشفير. في حال غياب مخدم إدارة مفاتيح التشفير فإن جميع المحطات ستستخدم "مفتاح تشفير مشترك مسبقاً Pre-Shared Key" (PSK). يعرف هذا النمط من التشغيل باسم بروتوكول WPA أو WPA2 الشخصي.

يعرف بروتوكول WPA2 عند استخدام مخدم لمفاتيح التشفير ببروتوكول WPA المؤسساتي. يتطلب بروتوكول WPA2 المؤسساتي وجود مخدم يعمل بمعايير IEEE 802.1X لتوزيع مفاتيح التشفير.

من أهم التطويرات المضمنة في بروتوكول WPA2 مقارنة بسلفه WEP هو إمكانية تبادل مفاتيح التشفير ديناميكياً بواسطة بروتوكول تكامل مفاتيح التشفير المؤقتة Temporal Key Integrity Protocol (TKIP).

بروتوكول الوصول المحمي إلى الشبكة اللاسلكية WPA2

وهو النسخة المعتمدة من بروتوكول WPA والذي يشكل جزءاً من معيار IEEE 802.11i للشبكات اللاسلكية. يتضمن بروتوكول WPA2 تعديلين أساسيين بالمقارنة مع سلفه WPA:

1. استبدال خوارزمية "ميخائيل" بشيفرة للتحقق من أصالة الرسائل تدعى بروتوكول النمط المعاكس / CBC-MAC (CCMP) والتي تعتبر آمنةً من ناحية التشفير.
2. استبدال شيفرة السيل RC4 بمعيار التشفير المتطور Advanced Encryption Standard (AES) المعروف أيضاً بإسم "Rijndael".

نصائح لأمن البيانات:

عند الحاجة إلى تأمين الشبكة اللاسلكية بوساطة التشفير على مستوى الوصلة فإن النمط المؤسساتي لبروتوكول الوصول الآمن إلى الشبكة اللاسلكية WPA2 هو الخيار الأمثل.
في حال اختيار الحل الأبسط باستخدام النمط الشخصي لبروتوكول WPA2 لا بد من إيلاء عناية خاصة لاختيار كلمات السر المستخدمة (مفتاح التشفير المشترك مسبقاً).
ينبغي الإبتعاد كليةً عن بروتوكول السرية المكافئة للشبكة اللاسلكية WEP وجميع مشتقاته مثل WEP+ و WEP2.

8. التحقق من الهوية في الشبكات اللاسلكية

يتم تعريف التحقق من الهوية في سياق الشبكات اللاسلكية بالإجراءات الهادفة لضمان صلاحية الإتصال بين نقاط الولوج و/أو المحطات اللاسلكية. يمكن التعبير عن التحقق من الهوية في الشبكات اللاسلكية بشكل أبسط باعتباره حق إرسال البيانات إلى وعبر الشبكة اللاسلكية.

لاستيعاب مفهوم التحقق من الهوية في الشبكات اللاسلكية لا بد من فهم ما يحدث عند بدء جلسة الإتصال بين نقطة ولوج و/أو محطة لاسلكية. يبدأ الإتصال بعملية تدعى "الربط Association". لقد تمت إضافة آليتين لعملية "الربط" عند تصميم معيار IEEE 802.11b للشبكات اللاسلكية:

- التحقق المفتوح من الهوية
- التحقق من الهوية باستخدام المفتاح المشترك

التحقق المفتوح من الهوية يعني ضمنياً عدم وجود أي آلية للأمن مما يمكن أي شخص كان من الإتصال مع نقطة الولوج.
تقوم نقطة الولوج في التحقق من الهوية باستخدام المفتاح المشترك بتشارك سر (كلمة سر) مع محطة المستخدم / نقطة الولوج. تتيح آلية طلب الإستجابة للتحدي لنقطة الولوج بالتحقق من أن المستخدم يعرف السر المشترك وستسمح له بالتالي الوصول إلى الشبكة اللاسلكية.

بروتوكول السرية المكافئة للشبكة السلكية WEP والتحقق من الهوية في الطبقة الثانية

تعتبر آلية التحقق من الهوية باستخدام مفتاح التشفير المشترك والمستخدمة في بروتوكول السرية المكافئة للشبكة اللاسلكية WEP بائدةً أيضاً. يمكن بسهولة اختراق آلية التشفير المستخدمة في بروتوكول WEP باستخدام هجمات نصوص تشفير بسيطة. نظراً لأن مفتاح التشفير ومفتاح التحقق من الهوية يستخدمان نفس السر المشترك فإن اكتشاف أي منهما سيؤدي إلى اكتشاف الآخر.

نصائح للتحقق من الهوية في الشبكات اللاسلكية

يتطلب التحقق من الهوية في الشبكات اللاسلكية ضمن الطبقة الثانية استخدام النمط المؤسساتي لبروتوكول WPA2.

يتم تنفيذ التحقق من الهوية في الشبكات اللاسلكية عادة (كما في حال مزودي خدمات الإنترنت اللاسلكية) ضمن الطبقات الأعلى لنموذج OSI المرجعي (طبقة بروتوكول الإنترنت IP) عبر بوابات مقيدة (أي تسجيل الدخول إلى موقع للإنترنت).

لا بد من الإنتباه إلى أنه عند نقل وظائف التحقق من الهوية إلى "بوابات مقيدة" فإننا سنفقد القدرة على إيقاف انتقال البيانات التي تعبر نقط الولوج الخاصة بنا.

1.8إيقاف إرسالمعرف مجموعةالخدمات SSID كإجراء لتعزيز أمن الشبكة اللاسلكية

طورت شركة لوسنت تكنولوجيز Lucent Technologies في العام 2000 نموذجاً مشتقاً من آلية التحقق المفتوح من الهوية أسمتها "الشبكة المغلقة Closed Network". تختلف الشبكات المغلقة عن الشبكات اللاسلكية المعيارية العاملة وفق معيار 802.11b بأنه نقاط الولوج لن ترسل إطارات إرشاد لمعرّف مجموعة الخدمات SSID بشكل دوري.

إن إيقاف إرسال معرف مجموعة الخدمات SSID يعني ضمنياً بأن على مستخدمي الشبكة اللاسلكية الحصول مقدماً على معرّف مجموعة الخدمات الذي يجب استخدامه للربط مع نقطة ولوج (أو مجموعة من نقاط الولوج). لقد تم استخدام هذه الميزة الجديدة من قبل الكثير من مصنعي تجهيزات الشبكات اللاسلكية كإجراء لتعزيز أمن الشبكة. في واقع الأمر فإنه وعلى الرغم من أن إيقاف إرسال معرف مجموعة الخدمات سيمنع المستخدمين غير المخولين من الحصول على هذا المعرف عبر الإطار المرشد، إلا أنها لن تمنع إيجاد معرّف مجموعة الخدمات باستخدام برمجيات التجسس على إطارات الربط المرسلة من محطات أخرى. إن إيجاد معرف مجموعة الخدمات لشبكة مغلقة يعني ببساطة انتظار أحد ما ليقوم بالربط بالشبكة اللاسلكية واستخلاص معرّف مجموعة الخدمات من إطار الربط المرسل.

إيقاف إرسال معرّف مجموعة الخدمات SSID

إن إيقاف إرسال معرف مجموعة الخدمات SSID لن يمنع شخصاً مهتماً من الحصول على المعرّف الخاص بشبكتك. كما أن إعداد شبكتك اللاسلكية كشبكةٍ مغلقةٍ لن يعدو كونه مجرد وضع عائق إضافي في درب المتطفلين العاديين. ينبغي اعتماد إيقاف إرسال معرّف مجموعة الخدمات كتدبيرٍ وقائيٍ إضافيٍ وليس كإجراءٍ أمنيٍ.

2.8. استخدام فلترة العناوين الفيزيائية MAC كإجراء لتعزيز أمن الشبكة اللاسلكية

لقد انتشر استخدام العنوان الفيزيائي لبطاقة الشبكة اللاسلكية كآلية لتحديد أو توفير الوصول إلى الشبكة اللاسلكية بين الكثير من مزودي خدمات الإنترنت اللاسلكية. يعتمد هذا الخيار على اعتبار أن العناوين الفيزيائية MAC مسجلة ضمن المكونات الإلكترونية لبطاقة الشبكة وبالتالي يستحيل تغييرها من قبل المستخدمين العاديين. إلا أن الواقع يخالف هذا الإعتبار، لأنه من الممكن وببساطة تغيير العناوين الفيزيائية في معظم بطاقات الشبكة اللاسلكية.

إستخدام العناوين الفيزيائية MAC للتحقق من الهوية

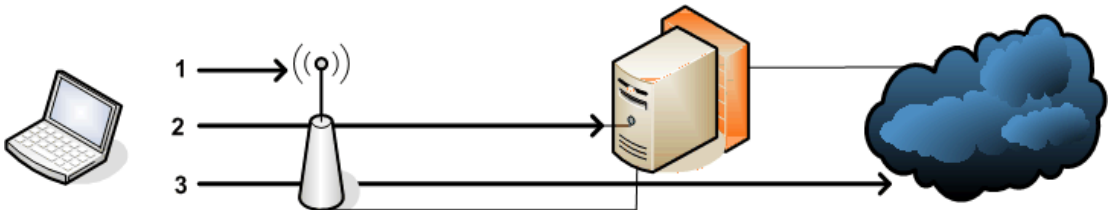
لا يمكن اعتبار أية آلية للتحقق من الهوية تعتمد فقط على العناوين الفيزيائية MAC إجراءً آمناً.

3.8. البوابات المقيّدة للشبكات اللاسلكية

يتطلب شرح "البوابات المقيّدة للشبكات اللاسلكية" تخصيص وحدة بأكملها، أما في سياق هذه الوحدة فهي تستحق مقدمةً مختصرةً على الأقل نظراً لارتباطها بأمن الشبكات اللاسلكية.

على الرغم من تعدد أساليب تطبيق البوابات المقيّدة للشبكات اللاسلكية إلا أن أغلبها يعتمد على نفس المبدأ. عند استخدام البوابات المقيدة كآلية للتحقق من الهوية في شبكةٍ ما فإن مستخدمي هذه الشبكة سيتمكنون من الربط مع أية نقطة ولوج (دون استخدام آليات التحقق من الهوية في الشبكة اللاسلكية) والحصول على عنوان إنترنت IP عبر بروتوكول الإعداد التلقائي للمضيف DHCP (دون تحققٍ من هوية المستخدم للحصول على عنوان إنترنت IP). بعد حصول المستخدم على عنوان إنترنت IP ستقوم الشبكة بالتقاط جميع طلبات الوصول إلى الإنترنت عبر بروتوكول HTTP لإجبار المستخدم على "تسجيل الدخول" إلى صفحة إنترنت.

تضطلع البوابات المقيّدة بمهمة التأكد من صحة كلمة السر التي أدخلها المستخدم وتعديل حالة الجدار الناري. تعتمد قواعد الجدار الناري على قيم العنوان الفيزيائي MAC وعنوان الإنترنت IP الذي حصل عليه المستخدم عبر بروتوكول DHCP.



الشكل 1: بوابة مقيّدة مع الخطوات الثلاث للتحقق من الهوية

يظهر الشكل السابق الخطوات الثلاث لعملية التحقق من الهوية باستخدام البوابات المقيّدة. تتطلب الخطوة الأولى أن يتم ربط المستخدم مع الشبكة اللاسلكية. لا تتطلب هذه المرحلة التحقق من هوية المستخدم عبر بروتوكولات WEP/WPA وتقوم الشبكة عادةً بإرسال معرّف مجموعة الخدمات SSID. في الخطوة الثانية يحصل المستخدم على عنوان إنترنت IP عبر بروتوكول الإعداد التلقائي للمضيف DHCP. تقوم نقطة الولوج بتمرير سيل البيانات IP دون أي تحقق من هوية المستخدم. في الخطوة الثالثة والأخيرة يتم تحويل جميع طلبات الوصول إلى الشبكة عبر بروتوكول الربط التشعبي HTTP الواردة من الزبون إلى مخدم البوابة المقيّدة. يقوم المستخدم بتسجيل الدخول إلى المخدم (ويتم ذلك عادة بإرسال إسم المستخدم وكلمة السر عبر بروتوكول HTTPS الآمن). أخيراً يقوم مخدم البوابة المقيّدة بتعديل أو إضافة قاعدة ضمن الجدار الناري للسماح للمستخدم بالوصول إلى الإنترنت.

ينطوي هذا الأسلوب على العديد من المشاكل الأمنية. للمزيد من المعلومات راجع التمارين المقترحة.

9. كمال البيانات في الشبكات اللاسلكية

سنقوم بتعريف كمال البيانات في الشبكات اللاسلكية بقدرة بروتوكول الإتصال اللاسلكي على كشف أي تحريف في البيانات المنقولة من قبل أشخاص غير مخولين.

كان من المفترض ببروتوكول السرية المكافئة للشبكة السلكية WEP في العام 1999 أن يضمن كمال البيانات المنقولة، إلا أن آلية كمال البيانات المستخدمة حينها (التحقق الدوري من الأخطاء Cyclic Redundancy Check – CRC) لم تكن آمنة. لقد أتاحت الأخطاء التصميمية في بروتوكول السرية المكافئة للشبكة السلكية WEP إمكانية تعديل البيانات المنقولة وتحديث قيمة CRC الخاصة بهذه البيانات حتى دون معرفة مفتاح تشفير WEP، أي أنه بالإمكان تحريف البيانات المنقولة دون أن يتم يكشف هذا التحريف.

حلّت بروتوكولات WPA و WPA2 مشكلة كمال البيانات الموجودة في سلفها WEP بإضافة شيفرةٍ أكثر أمناً للتحقق من الرسالة إضافةً إلى عدادٍ للإطارات والذي يمنع ما يسمى بـــ "هجمات الإعادة Replay Attacks" التي يقوم فيها المهاجم بتسجيل المحادثة بين أحد مستخدمي الشبكة اللاسلكية ونقطة الولوج بغية الحصول على وصول غير مخول إلى هذه الشبكة. بإعادة المحادثة "القديمة" لن يحتاج المهاجم إلى معرفة السر المشترك لـــ WEP أو المفتاح.

كمال البيانات: بروتوكول السرية المكافئة للشبكة السلكية WEP مقارنةً ببروتوكول الوصول المحمي للشبكة اللاسلكية WPA

يعتبر كمال البيانات عبر بروتوكول WEP منقرضاً.

نصائح لكمال البيانات:
يجب استخدام بروتوكول الوصول المحمي للشبكة اللاسلكية WPA أو WPA2 لتحقيق كمال البيانات في الشبكات اللاسلكية عبر التشفير على مستوى الوصلة.

1.9. ملاحظة حول أمن بروتوكول الوصول المحمي للشبكة اللاسلكية WPA

لقد صمم بروتوكول الوصول المحمي للشبكة اللاسلكية WPA كخطوة إنتقالية باتجاه بروتوكول WPA2 (معيار IEEE802.11i). يتضمن بروتوكول WPA جزءاً من الميزات المتوفرة في معيار IEEE802.11i ويركّز على التوافقية الرجعية مع بطاقات الشبكة العاملة وفق معايير WEP IEEE802.11b.

عالج بروتوكول الوصول المحمي للشبكة اللاسلكية WPA العيوب الموجودة في سلفه WEP عبر زيادة حجم المفاتيح المستخدمة وإضافة شيفرةٍ جديدةٍ آمنةٍ للتحقق من الرسائل. لقد تم اختيار خوارزمية ميخائيل Michael كونها أقوى الحلول القادرة على التعامل مع بطاقات الشبكة القديمة. لكن خوارزمية ميخائيل ما زالت عرضة للهجمات ولهذا السبب تحتوي الشبكات اللاسلكية المعتمدة على بروتوكول WEP آليةً لإيقاف عمل الشبكة لمدة 30 ثانية عند اكتشاف هجمةٍ ما.

		WPA	WPA2
النمط المؤسساتي	التحقق من الهوية	[3]IEEE 802.11X/EAP	IEEE 802.11X/EAP
	التشفير	TKIP[4]/MIC	AES-CCMP
النمط الشخصي	التحقق من الهوية	PSK	PSK
	التشفير	TKIP/MIC	AES-CCMP

الجدول 1: التشفير والتحقق من الهوية في بروتوكولي WPA و WPA2 (للنمطين الشخصي والمؤسساتي)

10. توفر الشبكات اللاسلكية

سنعرّف توفر الشبكة اللاسلكية بقدرة التقنية على ضمان الوصول الموثوق إلى خدمات البيانات والمعلومات للمستخدمين المخولين.

من أول الأمور الواجب أخذها بعين الإعتبار أنه من غير اليسير أن تمنع شخصاً ما من التشويش على إشارة شبكتك اللاسلكية. تعمل الشبكات اللاسلكية ضمن نطاقٍ محدد للقنوات الراديوية يمكن استخدامه من قبل أي شخص لإرسال إشاراتٍ لاسلكيةٍ. من شبه المستحيل منع الأشخاص غير المخولين من التشويش على

[3] EAP هي اختصار بروتوكول التحقق من الهوية المرن، وهو بروتوكول للأمن يستخدم في التجهيزات التي تحتوي مخدم الوصول إلى الشبكة (Network Access Server (NAS العاملة وفق معايير IEEE 802.1Xكنقاط الولوج إلى الشبكة اللاسلكية المتوافقة مع معايير IEEE 802.11 a/b/g.

[4] TKIP هي اختصار بروتوكول تكامل المفاتيح المؤقتة Temporal Key Integrity Protocol.

شبكتك. غاية ما يمكنك عمله أن تقوم بمراقبة وصلاتك لتحديد المصادر المحتملة للتشويش. (راجع وحدة المراقبة والإدارة).

إيقاف الخدمة

تعتبر الشبكات اللاسلكية عرضةً لإيقاف الخدمة Denial of Service (DoS) بسبب التشويش اللاسلكي. خذ على سبيل المثال الحالة التي يقرر بها مشغّل شبكةٍ أخرى إعداد تجهيزاته اللاسلكية لتعمل ضمن نفس القنوات الراديوية المستخدمة في شبكتك. تخيل أيضاً أن هذه الشبكة سترسل نفس معرّف مجموعة الخدمات SSID الخاص بشبكتك.

لتجنب هذه الهجمات المقصودة أو غير المقصودة ينبغي عليك القيام بمسحٍ دوريٍ للترددات اللاسلكية. لتجنب التشويش على شبكات أخرى يجب عليك ألا تفرط في زيادة طاقة وصلاتك اللاسلكية.

هناك العديد من الأسباب التي قد تخفض من أداء الشبكة اللاسلكية أو توقف عملها بالكامل. قد يتسبب وجود نقاطٍ مخفيةٍ في تدنٍ كبيرٍ في أداء الشبكات العاملة ببروتوكول IEEE 802.11. كما قد تتسبب الفيروسات، برمجيات الند للند Peer-to-Peer إضافة إلى الرسائل المرسلة عشوائياً SPAM وغيرها في تخفيض سعة نقل البيانات المتوفرة للوصول المخول إلى الخدمات الأساسية.

كما ذكرنا في فقرة "التحقق من الهوية" من هذه الوحدة فإنه من الصعب منع المستخدمين غير المخولين من الإتصال بنقطة الولوج أو البوابة المقيّدة الخاصة بك. يتطلب توفر الشبكة اللاسلكية القيام بمهام مراقبة الشبكة بشكلٍ جيدٍ.

11. مكافحة الإنكار (المسؤولية) في الشبكات اللاسلكية

لا تتعامل معايير الشبكات اللاسكية IEEE 802.11 مع (المسؤولية) عن المعلومات المنقولة عبر الشبكة اللاسلكية. لا تحتوي بروتوكولات الشبكات اللاسلكية على آليةٍ للتأكيد على أن مرسل البيانات قد حصل على إثباتٍ لتسلم المستقبل لرسالته أو على أن المستقبل قد حصل على إثباتٍ لهوية المرسل. لذلك يجب إعداد المسؤولية ضمن بروتوكولات الطبقات العليا.

12 التهديدات الأمنية للشبكات اللاسلكية

يظهر الجدول التالي المخاطر الأمنية العشر الأكثر شيوعاً في الشبكات اللاسلكية ويقدم مجموعةً من المقترحات لكل منها.

1	السرية	خطر التجسس، قد يصل المستخدمون غير المخولين إلى البيانات المنقولة عبر شبكتك اللاسلكية	استخدم التشفير على مستوى الوصلة ضمن وصلاتك اللاسلكية (WPA2). إنصح مستخدمي شبكتك باستخدام "التشفير" ضمن الطبقات ذات المستوى الأعلى (HTTPS, Secure SMTP).

2	السرية	خطر اختطاف البيانات المنقولة، قد يتمكن المستخدمون غير المخولين من تطبيق هجمات الشخص الوسيط	التوصية 1 + راقب نسبة الإشارة إلى الضجيج SNR، معرّف مجموعة الخدمات SSID إضافة إلى العنوان الفيزيائي لنقطة الولوج AP MAC المستخدمة في وصلاتك.
3	التحقق من الهوية	خطر الوصول غير المخول إلى شبكتك اللاسلكية	قم بإعداد بروتوكول IEEE 802.11X ((WPA2). لا تعتمد على أساليب التحقق من الهوية باستخدام العنوان الفيزيائي MAC فقط. لا ترسل معرّف مجموعة الخدمات SSID الخاص بشبكتك.
4	السرية	خطر الوصول غير المخول إلى شبكتك وإلى الإنترنت	قم بإعداد بروتوكول IEEE 802.11X قم بإعداد بوابة مقيدة Captive Portal.
5	التكامل	خطر تحريف البيانات أثناء نقلها لاسلكياً	إنصح مستخدمي شبكتك باستخدام "التشفير" ضمن الطبقات ذات المستوى الأعلى (HTTPS, Secure SMTP). استخدم التشفير على مستوى الوصلة ضمن وصلاتك اللاسلكية (WPA2).
6	التوفر	خطر التشويش اللاسلكي إيقاف عمل الخدمة بسبب التشويش اللاسلكي (التداخل)	راقب طيف الترددات اللاسلكية دورياً. حاذر من الزيادة المفرطة لطاقة وصلاتك.
7	التوفر	خطر انخفاض سعة النقل نتيجة الإرسال المتكرر للإشارات اللاسلكية	تأكد من عدم وجود نقاط مخفية أو مصادر أخرى للتشويش. راقب نقاط الولوج لكشف أية إرسالات متكررة على مستوى الوصلة.
8	التوفر	خطر انخفاض سعة النقل نتيجة البرمجيات المؤذية	راقب البيانات المنقولة لبروتوكول الإنترنت IP وبشكل خاص بروتوكولي ICMP و UDP. ركّب أنظمة كشف التسلل Intrusion Detection Systems إذا دعت الحاجة.
9	التحقق من الهوية المسؤولية	خطر الوصول غير المخول لشبكتك الداخلية	قم بتركيب الشبكة اللاسلكية خارج حدود الجدار الناري. استخدم الشبكة الخاصة الإفتراضية VPN واسمح بالوصول إلى شبكتك الداخلية عبر مركز الشبكة الخاصة الإفتراضية فقط.
10	(الوصول إلى الشبكة) المسؤولية	خطر الإستخدام غير المخول لموارد الشبكة والشبكة اللاسلكية	قم بإعداد بروتوكول IEEE 802.11X استخدم البوابات المقيدة المعتمدة على التواقيع الإلكترونية Digital Signature.

جدول 2: التهديدات الأمنية العشر الأكثر شيوعاً في الشبكات اللاسلكية مع نصائح للإجراءات الوقائية

13. الخلاصة

قدّمت هذه الوحدة الشبكات اللاسلكية من وجهة نظر أمن أنظمة المعلومات INFOSEC.

لقد استعرضنا خمسة خصائص أمنية: السرية، التحقق من الهوية، الكمال، مكافحة الإنكار والتوفر في سياق الشبكات اللاسلكية.

نظراً لأن معايير الشبكات اللاسلكية مثل IEEE 802.11 تتعامل فقط مع الطبقتين 1 و 2 من نموذج OSI المعياري فإن من الممكن استخدام بعض الخصائص الأمنية ضمن الطبقات الأعلى أيضاً.

يفترض بالمصمم الجيد للشبكات اللاسلكية أن يفكر ملياً في كيفية إعداد كلٍ من هذه الخصائص الأمنية. على سبيل المثال، قد يقوم بإعداد التشفير من أجل السرية ضمن مستوى الوصلة أو ضمن مستوى التطبيقات أو بروتوكول الإنترنت IP، قد يقوم بإرسال معرف مجموعة الخدمات SSID أو لا، قد يقوم بإعداد التحقق من الهوية باستخدام بروتوكول IEEE 820.1X، يمكن أيضاً إستخدام البوابات المقيّدة أو التصفية البسيطة والساكنة للعناوين الفيزيائية MAC وغيرها.

ينبغي لأي إعداد لأمن الشبكة أن يعتمد على خصوصية هذه الشبكة وتطبيقاتها.

يمكن تلخيص الأمور الخمس الرئيسية التي ينبغي عليك تذكرها من هذه الوحدة بما يلي:

1. يحتوي أمن الشبكات اللاسلكية الصرف على آليات للأمن تعمل ضمن الطبقتين الأولى والثانية فقط.
2. يعتبر التشفير على مستوى الوصلة (WEP, WPA, WPA2) من أكثر إجراءات أمن الشبكة اللاسلكية شيوعاً، إلا أنه لا يضمن السرية المطلقة من بداية الوصلة إلى نهايتها. إذا ما احتجت إلى التشفير على مستوى الوصلة، تجنّب استخدام WEP واستخدم IEEE 802.11i (WPA2).
3. لا يمكن اعتبار إيقاف إرسال معرّف مجموعة الخدمات SSID أو استخدام تصفية العناوين الفيزيائية MAC وسائل آمنة للتحقق من الهوية. لا بد من استخدام أسلوب للتحقق من الهوية على المستويات الأعلى، كالبوابات المقيّدة مثلاً.
4. قد تتوقف الشبكة اللاسلكية عن العمل نتيجة هجمات متعمدة لإيقاف عمل الخدمة DoS أو وجود برمجيات مؤذية، كما أن الشبكة قد تتعطل دون قصد بسبب وجود نقاط خفية أو مشاكل تشويش. لن تتمكّن من اكتشاف الأسباب الحقيقية وراء هذه المشاكل إلا من خلال مراقبة سير البيانات عبر شبكتك.
5. لا يوجد "حل أمني قياسي" يلائم جميع الشبكات اللاسلكية. من الضروري تحديد المتطلبات الأمنية بوضوح لأن الحلول تعتمد على خصوصية كل حالة.