أمن الشبكات اللاسلكية

إعداد : Alberto Escudero Pascual/ IT +46
النسخة العربيةأنس طويلة

المحتويات

- الجزء I
  مقدمة إلى أمن الشبكات اللاسلكية وأمن أنظمة المعلومات
  مقدمة موجزة إلى نموذج OSI والتشفير على مستوى الوصلة

- الجزء II
  الخصائص الأمنية الخمس في سياق الشبكات اللاسلكية

- الجزء III
  عشرة مخاطر أمنية للشبكات اللاسلكية

تعريف أمن الشبكات اللاسلكية

- يتصف مفهوم الأمن بأنه واسع وعام إلى حد كبير.
- أي "أمن" نقصد؟
- علينا البدء بتعريف "السياق" الصحيح للأمن لدراسة أمن الشبكات اللاسلكية
- سنستعرض أمن الشبكات اللاسلكية ضمن سياق أمن المعلومات.

ماهو أمن المعلومات؟ 3\1 COMSEC

- كان يعرف في السبعينات باسم " أمن الإتصالات" Communication Security – COMSEC
- حددت توصيات أمن أنظمة المعلومات والإتصالات لوكالة الأمن القومي في الولايات المتحدة أمن الإتصالات COMSEC بأنه:

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

- تضمّن أمن الإتصالات خاصيتين تتعلقان بموضوع هذه الوحدة: السرية Confidentiality والتحقق من الهوية Authentication.

السرية

التأكيدبأن المعلومات لم تصل لأشخاص، عمليات أو أجهزة غير مخولة بالحصول على هذه المعلومات."

الحماية من إفشاء المعلومات غير المرخص

التحقق من الهوية

"إجراء أمني للتأكد من صلاحية الإتصال، الرسالة أو المصدر أو وسيلة للتحقق من صلاحية شخص ما لاستقبال معلومات ذات تصنيف محدد."

التحقق من مصدر المعلومات

ماهو أمن المعلومات؟ 3\2 COMPUSEC

- بدأت في الثمانينات مع النمو المضطرد للحاسبات الشخصية حقبة جديدة من الأمن.
- تم تعريف أمن الحواسيب Computer Security – COMPUSEC ضمن توصيات NSTISSI بما يلي:

"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.

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."

لا يمكن تعديل البيانات دون السماح بذلك

التوفر

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

" وثوقية "الوصول إلى المعلومات

ماهو أمن المعلومات؟ 3\3

- في 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.
- يتضمن مفهوم أمن أنظمة المعلومات أيضاً خاصية جديدة بمكافحة الإنكار.

مكافحة الإنكار - المسؤولية

التأكيدبأن مرسل البيانات قدحصل على إثبات بوصول البيانات إلى المرسل إليهوبأن المستقبل قدحصل على إثبات لشخصية المرسل مما يمنع إحتمال إنكار أي من الطرفين بأنه قدعالج هذهالبيانات."

أمن المعلومات في الشبكات 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".

المنهجية

ماذا سيتم استعراض أمن الشبكات اللاسلكية من وجهة نظر أمن المعلومات.

لماذا التعرف على أسلوب منهجي لتصميم الشبكات اللاسلكية الآمنة.

كيف سنستعرض جميع الخصائص الأمنية الخمس لأمن المعلومات وسنناقش كيف يتم (تطبيق كل منها في الشبكات اللاسلكية.

ملاحظتين

- تذكر قبل البدء بالخصائص الأمنية الخمس الملاحظتين التاليتين من وحدة التشبيك المتقدم:
  - نموذج OSI ومعايير الشبكات اللاسلكية
  - التشفير على مستوى الوصلة

تذكير بنموذج OSI
وأمن الشبكات اللاسلكية

- ترتبط معايير الشبكات اللاسلكية عادة بالطبقتين الأولى والثانية من حزمة بروتوكولات OSI

- عندما نتحدث عن أمن الشبكات اللاسلكية فإننا نعني غالباً الإعداد الصحيح لـ "التشفير على مستوى الوصلة اللاسلكية".

- لا تنتمي آليات الأمن ضمن الطبقة الثالثة فما فوق من حزمة بروتوكولات OSI إلى "أمن الشبكات اللاسلكية" وينبغي اعتبارها كجزء من "وحدة أمن الشبكة أو التطبيقات".

التشفير على مستوى الوصلة 2\1 تذكير

- تعريف: آلية تأمين البيانات على مستوى الوصلة أثناء انتقال هذه البيانات بين نقطتين متصلتين بنفس الوصلة الفيزيائية.
- المتطلبات: توفر مفتاح محدد أو سر مشترك بين الأطراف التي ستشترك في عملية التشفير بالإضافة إلى الإتفاق عل خوارزمية مشتركة للتشفير.
- أمثلة: من غير الشائع استخدام التشفير على مستوى الوصلة في شبكات الأقمار الصناعية على الرغم من أن حلف الناتو ووزارة الدفاع الأمريكية تستخدمه.

للمزيد من المعلومات: حلول الأمن العالي للشبكات ViaSat
http://www.viasat.com/refresh/secure

التشفير على مستوى الوصلة 2\2

- في حال عدم تشارك المرسل والمستقبل في نفس الناقل الفيزيائي ينبغي فك تشفير البيانات وإعادة تشفيرها عند كل نقطة مرور أثناء انتقالها إلى المستقبل. يعمل التشفير على مستوى الوصلة بين نقطتين فقط HOP-BY-HOP.

- يستخدم التشفير على مستوى الوصلة عادة عند غياب التشفير على مستويات أعلى أو في التطبيقات عالية الحساسية.

التشفير على مستوى الوصلة في الشبكات اللاسلكية 802.11 – 1 \ 2

- تعتبر خوارزمية السرية المكافئة للشبكة السلكية Wired Equivalent Privacy (WEP) أكثر خوارزميات التشفير شيوعاً في الشبكات اللاسلكية العاملة وفق معايير 802.11 (1999-2004).
- لقد ثبت عملياً أن WEP غير آمن، وهي نتيجة بديهية لأن هذا المعيار لم يخضع للتدقيق من قبل العموم.
- استحدثت بدائل أخرى خلال السنوات الخمس الماضية وتم اعتماد هذه الصيغة المعيارية للوصول المحمي للشبكة اللاسلكية Wi-Fi Protected Access (WPA)
- سيتضمن المعيار الجديد للشبكات اللاسلكية 802.11 i إصدارةً مطورةً من WPA تدعى WPA2.

التشفير على مستوى الوصلة في الشبكات اللاسلكية 802.11 – 2\2

- لا يوفر التشفير على مستوى الوصلة أمناً مطلقاً خارج مجال الوصلة الفيزيائية.
- يجب اعتبار التشفير على مستوى الوصلة 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.

الخصائص الأمنية الخمس في الشبكات اللاسلكية

- السرية Confidentiality.
- التحقق من الهوية Authentication.
- الكمال Integrity.
- التوفر Availability.
- مكافحة الإنكار – المسؤولية Non-repudation.

سريةالشبكات اللاسلكية

- سنعرّف سريةالشبكات اللاسلكيةبضمان أنالمعلومات المرسلةبين نقاط الولوجوحواسب المستخدمين لن تصل إلىأشخاص غير مخولين.

- يجب أن تضمن سريةالشبكات اللاسلكيةبأن:

1-الإتصالات الجاريةبين مجموعةمن نقاط الولوج ضمن نظامتوزيع لاسلكي Wireless Distribution System (WDS) محمية أو

2-الإتصالات الجاريةبين نقطةولوج APوحاسب متصل بها STAتبقى محمية.

WEP

- شكلت "السرية المكافئة للشبكة السلكية "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.
- لم يستغرق الأمر سوى عدة أشهر من إطلاق البروتوكول حتى تم خرقه وهجرانه.
- لقد أثبت هذا البروتوكول ضعفه بغض النظر عن طول مفتاح التشفير المستخدم.
- لقد ساهم عدم توفر نظام لإدارة مفاتيح التشفير ضمن هذا البروتوكول في إفشاله أيضاً.
- سرعان ما طورت بدائل جديدة لهذا البروتوكول مثل WEP+ من شركة Lucent وبروتوكول WEP2 من شركة Cisco.

WEP

- يعتبر بروتوكول السرية المكافئة للشبكة السلكية WEP وتعديلاته WEP+ و WEP2 حالياً خارج الخدمة.
- يعتمد بروتوكول السرية المكافئة للشبكة السلكية على شيفرة سيل RC4.
- هناك العديد من البرمجيات المتاحة لاختراق بروتوكول السرية المكافئة للشبكة السلكية منها aircrack، kismac، wepcrack، Airsnort
- إذا كنت مهتماً بتاريخ بروتوكول السرية المكافئة للشبكة السلكية ننصحك بمراجعة (موارد إضافية للمعلومات) المرفقة مع هذه الوحدة.

ولادةبروتوكولي الوصول المحمي للشبكة اللاسلكية WPA و WPA2

- تم اقتراح بروتوكول الوصول المحمي للشبكة اللاسلكية WPA في العام 2003 أثناء مناقشة معيار الشبكات اللاسلكية IEEE 802.11i

- لقد تم التركيز أثناء تصميم بروتوكول WPA على تسهيل تحديث التجهيزات القديمة في العام 2004 طور بروتوكول WPA ليتضمن AES وتم اعتماده كجزء من معيار الشبكات اللاسلكية IEEE 802.11i تحت اسم WPA2.

- لقد تم تصميم بروتوكولي WPA و WPA2 للعمل مع أو دون وجود مخدم لإدارة مفاتيح التشفير.

ولادةبروتوكولي الوصول المحمي للشبكة اللاسلكية WPA و WPA2

- في حال غياب مخدم إدارة مفاتيح التشفير فإن جميع المحطات ستستخدم "مفتاح تشفير مشترك مسبقاً Pre-Shared Key PSK".
- يعرف نمط التشغيل PSK باسم بروتوكول WPA أو WPA2 الشخصي.
- يعرف بروتوكول WPA2 عند استخدام مخدم لمفاتيح التشفير ببروتوكول WPA المؤسساتي.
- من أهم التطويرات المضمنة في بروتوكول WPA2 مقارنة بسلفه WEP هو إمكانية تبادل مفاتيح التشفير ديناميكياً.

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.

حق إرسال (توجيه) البيانات عبر نقطة الولوج

- لاستيعاب مفهوم التحقق من الهوية في الشبكات اللاسلكية لابد من فهم ما يحدث عند بدء جلسة الإتصال بين نقطة ولوج و/أو محطة لاسلكية STA.

آليات الربط

- التحقق المفتوح من الهوية:

- لايوجدأي آليةللأمن ممايمكن أيشخص كان من الإتصال مع نقطةالولوج.

- التحقق من الهوية باستخدامالمفتاح المشترك:
  - يتمتشارك سر)كلمةسر(بين محطة المستخدم ونقطةالولوج.
  - تتيح آليةطلب الإستجابةللتحدي لنقطةالولوج بالتحقق من أن المستخدمعرف السر المشترك وستسمح لهبالتالي الوصول إلى الشبكة اللاسلكية.

بروتوكول السرية المكافئة للشبكة السلكية والتحقق من الهويةفي الطبقة الثانية

- تعتبر آليةالتحقق من الهوية باستخدامفتاح التشفير المشترك والمستخدمةفي بروتوكول السرية المكافئة للشبكة اللاسلكية WEP بائدةً.
- يمكن بسهولةاختراق آليةالتشفير المستخدمةفي بروتوكول WEP باستخدامهجماتنصوص تشفير بسيطة.
- مفتاح التشفير ومفتاح التحقق من الهويةيستخدمانفس السر المشترك.
- فإناكتشاف أي من هذين المفتاحين سيؤدي إلىاكتشاف الآخر.

بروتوكول السرية المكافئة للشبكة السلكية والتحقق من الهوية في الطبقة الثانية

نصائح:

- استخدم 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).
- لابد 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.

إيقاف إرسال معرّف مجموعة الخدمات SSID

- من مشتقات آلية التحقق المفتوح من الهوية "الشبكة المغلقة Closed Network".
- لا ترسل نقاط الولوج في الشبكات المغلقة إطارات إرشاد معرّف مجموعة الخدمات SSID بشكل دوري وهي إطارات إدارة مستوى الوصلة ضمن معيار IEEE 802.11).
- إن إيقاف إرسال معرف مجموعة الخدمات SSID يعني ضمنياً أن على مستخدمي الشبكة اللاسلكية الحصول مقدماً على معرّف مجموعة الخدمات.

إيقاف إرسال معرّف مجموعة الخدمات SSID

حماية "أمنية"؟

- لن تمنع إيقاف معرّف مجموعة الخدمات باستخدام برمجيات التجسس على إطارات الربط المرسلة من محطات أخرى.
- إن إيقاف معرف مجموعة الخدمات لشبكة مغلقة يعني ببساطة انتظار أحد ما ليقوم بالربط بالشبكة اللاسلكية واستخلاص معرّف مجموعة الخدمات من إطار الربط المرسل.
- ينبغي اعتماد إيقاف إرسال معرّف مجموعة الخدمات كتدبيرٍ وقائي إضافي وليس كإجراءٍ أمني بحد ذاته.

استخدام فلترة العناوين الفيزيائية كإجراء لتعزيز أمن الشبكة اللاسلكية

- يستخدم الكثير من مزودي خدمات الإنترنت اللاسلكية فلترة العنوان الفيزيائي لبطاقة الشبكة اللاسلكية كآلية لتحديد أو توفير الوصول إلى الشبكة اللاسلكية على اعتبار أن العناوين الفيزيائية MAC مسجلة ضمن المكونات الإلكترونية لبطاقة الشبكة وبالتالي يستحيل تغييرها من قبل المستخدمين العاديين.
- المشكلة: يمكن ببساطة تغيير العناوين الفيزيائية في معظم بطاقات الشبكة اللاسلكية.
- لا يمكن اعتبار أية آلية للتحقق من الهوية تعتمد فقط على العناوين الفيزيائية MAC إجراءً آمناً.

البوابات المقيّدة للشبكات اللاسلكية

- إزالة التحقق من الهوية من الشبكة اللاسلكية: البوابات المقيّدة.
- هناك العديد من أساليب تطبيق البوابات المقيّدة للشبكات اللاسلكية.
- أغلب هذه الأساليب تعتمد على نفس المبدأ: إعادة توجيه طلبات HTTP والجدران النارية الديناميكية.

البوابات المقيّدة للشبكات اللاسلكية

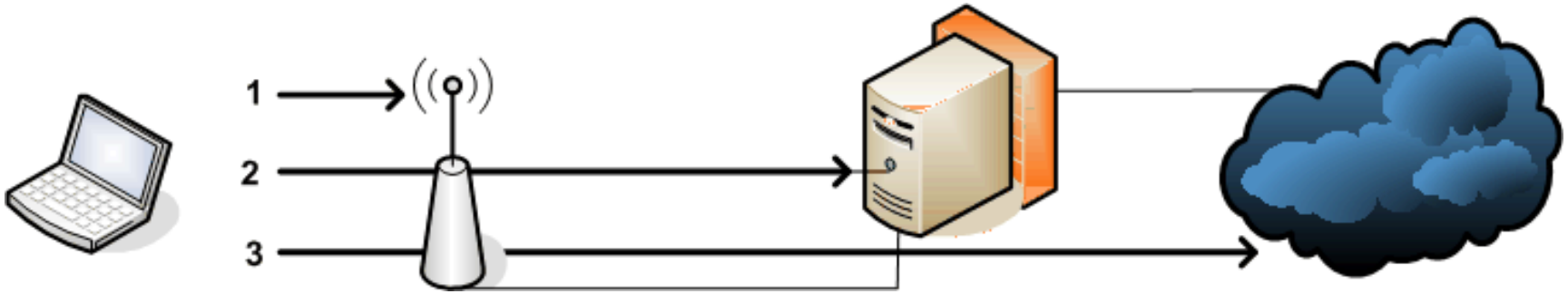
1) يسمح لمستخدمي الشبكة بالربط مع أية نقطة ولوج والحصول على عنوان IP عبر بروتوكول الإعداد التلقائي للمضيف DHCP إنترنت.

2) بعد حصول المستخدم على عنوان IP إنترنت تقوم الشبكة بالتقاط جميع طلبات الوصول إلى الإنترنت عبر بروتوكول HTTP لإجبار المستخدم على تسجيل الدخول" إلى صفحة إنترنت.

3) تضطلع البوابات المقيّدة بمهمة التأكد من صحة كلمة السر التي أدخلها المستخدم وتعديل حالة الجدار الناري (والذي غالباً ما يتوضع ضمن نفس الجهاز).

4) تعتمد قواعد الجدار الناري على قيم العنوان الفيزيائي MAC وعنوان الإنترنت IP الذي حصل عليه المستخدم عبر بروتوكول DHCP.

البوابات المقيّدةللشبكات اللاسلكية التحقق من الهويةفي ثلاث خطوات



كمال المعلومات في الشبكات اللاسلكية

- قدرة بروتوكول الإتصال اللاسلكي على كشف أي تحريف في البيانات المنقولة من قبل أشخاص غير مخولين.
- كان من المفترض ببروتوكول السرية المكافئة للشبكة السلكية WEP أن يضمن كمال البيانات المنقولة.
- إن آلية كمال البيانات المستخدمة في بروتوكول WEP (التحقق الدوري من الأخطاء Cyclic Redundancy Check – CRC) لم تكن آمنة أمر متوقع!
- يمكن تعديل البيانات المنقولة وتحديث قيمة CRC الخاصة بهذه البيانات حتى دون معرفة مفتاح تشفير WEP.

كمال المعلومات في الشبكات اللاسلكية

النتيجة: يمكن تحريف البيانات المنقولة دون أن يتم كشف هذا التحريف.

WPA و **WPA2** تضمنت شيفرة أكثر أمناً لتحقق من الرسالة إضافة إلى عداد للإطارات والذي يمنع ما يسمى بـ "هجمات الإعادة Replay Attacks".

كمال المعلومات في الشبكات اللاسلكية

WPA مقارنةً مع WPA2

- يعتبر كمال البيانات عبر بروتوكول WEP منقرضاً .
- يجب استخدام بروتوكول الوصول المحمي للشبكة اللاسلكية WPA أو WPA2 لتحقيق كمال البيانات في الشبكات اللاسلكية عبر التشفير على مستوى الوصلة.

توفر الشبكات اللاسلكية

" قدرة التقنية على ضمان الوصول الموثوق إلى خدمات البيانات والمعلومات للمستخدمين المخولين."

التشويش على القنوات الراديوية للشبكات اللاسلكية

- تعمل الشبكات اللاسلكية ضمن نطاق محدد للقنوات الراديوية يمكن استخدامه من قبل أي شخص لإرسال إشاراتٍ لاسلكيةٍ.
- من شبه المستحيل منع الأشخاص غير المخولين من التشويش على شبكتك.
- نصيحة: راقب وصلاتك اللاسلكية بعناية لتحديد المصادر المحتملة للتشويش.

إيقاف الخدمة

- تعتبر الشبكات اللاسلكية عرضة لإيقاف الخدمة Denial of Service (DoS) بسبب التشويش اللاسلكي، من الممكن أن يبدأ أي شخص باستخدام:
  - نفس القنوات الراديوية المستخدمة في شبكتك.
  - نفس معرّف مجموعة الخدمات SSID الخاص بشبكتك.
- يمكن أن تكون هذه الهجمات مقصودة أو غير مقصودة.
- الإحتياطات:
  - حاول القيام بمسح دوري للترددات اللاسلكية.
  - لا تفرط في زيادة طاقة وصلاتك اللاسلكية.

تهديدات أخرى لتوفرالشبكات اللاسلكية

- وجود نقاطٍ مخفيةٍ Hidden Nodes)تكراركثيف للإرسال(.
- فيروسات) مسحكثيف(.
- برمجيات الند للند Peer-to-Peer)كثافةفي المعلومات المنقولة(.
- الرسائل المرسلة عشوائياً SPAM)كثافةفي البريد الوارد / الصادر(.

مكافحة الإنكار (المسؤولية) في الشبكات اللاسلكية

- لا تحتوي بروتوكولات الشبكات اللاسلكية على آلية للتأكيد على أن مرسل البيانات قد حصل على إثبات لتسلم المستقبل لرسالته أو على أن المستقبل قد حصل على إثبات لهوية المرسل.

- يجب إعداد المسؤولية ضمن بروتوكولات الطبقات العليا.

عشرة تهديدات أمنية للشبكات اللاسلكية

1	السرية	خطر التجسس	• WPA2 • "التشفير" ضمن الطبقات ذات المستوى الأعلى
2	السرية	خطر اختطاف البيانات المنقولة، 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	• WPA2 • لا تعتمد على أساليب التحقق من الهوية باستخدام العنوان الفيزيائي MAC فقط. • لا ترسل معرّف مجموعة الخدمات SSID الخاص بشبكتك.

عشرة تهديدات أمنية للشبكات اللاسلكية

4	السرية	خطر الوصول غير المخول إلى شبكتك وإلى الإنترنت	• IEEE 802.11X • البوابة المقيدة Captive Portal
5	التكامل	خطر تحريف البيانات أثناء نقلها لاسلكياً	• "التشفير" ضمن الطبقات ذات المستوى الأعلى • 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.

عشرة تهديدات أمنية للشبكات اللاسلكية

8	التوفر	خطر انخفاض سعة النقل نتيجة البرمجيات المؤذية	• راقب البيانات المنقولة لبروتوكول الإنترنت IP وبشكل خاص بروتوكولي ICMP و UDP. • ركب أنظمة كشف التسلل Intrusion Detection Systems
9	التحقق من الهوية المسؤولية	خطر الوصول غير المخول لشبكتك الداخلية	• قم بتركيب الشبكة اللاسلكية خارج حدود الجدار الناري. • استخدم الشبكة الخاصة الإفتراضية VPN • اسمح بالوصول إلى شبكتك الداخلية عبر مركز الشبكة الخاصة الإفتراضية فقط.
1	الوصول إلى الشبكة - المسؤولية	خطر الإستخدام غير المخول لموارد الشبكة والشبكة اللاسلكية	• IEEE 802.11X • البوابات المقيدة المعتمدة على التواقيع الإلكترونية Digital Signature.

الخلاصة

- يمكن تطبيق الخصائص الأمنية الموصّفة في أمن المعلومات INFOSEC ضمن عدة طبقات من نموذج OSI المرجعي.
- إذا ما احتجت إلى الأمن على مستوى الوصلة تجنب WEP واستخدم بروتوكول WPA2 في معيار IEEE 802.11i.
- عليك تحديد متطلباتك الأمنية بدقة وتطبيق الحلول الملائمة لخصوصية كل حالة.