الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1361

(2018/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (2) – أمن إنترنت الأشياء (IoT)

الإطار الأمني لإنترنت الأشياء القائم على نموذج البوابة

التوصية ITU-T X.1361

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب	X.1140–X.1149
بروتوكولات الأمن (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	**X.1360–X.1369**
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1389
أمن سجل الحسابات الموزع	X.1400–X.1429
أمن سجل الحسابات الموزع	X.1430–X.1449
البروتوكول الأمني (2)	X.1450–X.1459
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1361

الإطار الأمني لإنترنت الأشياء القائم على نموذج البوابة

ملخص

تصف التوصية ITU-T X.1361 إطاراً أمنياً لإنترنت الأشياء (IoT) استناداً إلى البوابات الأمنية. وإنترنت الأشياء (IoT) بنية تحتية عالمية لمجتمع المعلومات تمكّن الخدمات المتقدمة عن طريق التوصيل البيني للأشياء (المادية والافتراضية) استناداً إلى تكنولوجيات المعلومات والاتصالات القابلة للتشغيل البيني القائمة والمتطورة.

وتحلل هذه التوصية التهديدات والتحديات الأمنية في بيئة لإنترنت الأشياء وتصف القدرات الأمنية التي يمكن أن تعالج هذه التهديدات والتحديات وتخفف من حدتها. وتقدم منهجية إطارية لتحديد القدرات الأمنية المطلوبة للتخفيف من حدة التهديدات والتحديات التي تواجه إنترنت الأشياء والتصدي لها.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1361	2018-09-07	17	11.1002/1000/13607

مصطلحات أساسية

إنترنت الأشياء (IoT)، الإطار الأمني، المتطلبات الأمنية.

* للنفاذ إلى توصية، يرجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1361

الإطار الأمني لإنترنت الأشياء القائم على نموذج البوابة

1 مجال التطبيق

تصف هذه التوصية إطاراً أمنياً لإنترنت الأشياء (IoT) باستعمال البوابات الأمنية.

وتقدم هذه التوصية تحليلاً للتهديدات والتحديات الأمنية في بيئة إنترنت الأشياء وتصف القدرات الأمنية التي تعالج هذه التهديدات والتحديات الأمنية وتخفف من حدتها. وتقدم منهجية إطارية لتحديد القدرات الأمنية المطلوبة للتخفيف من حدة التهديدات والتحديات الأمنية لإنترنت الأشياء والتصدي لها.

وتركز هذه التوصية على القدرات الأمنية لإنترنت الأشياء باستعمال البوابات الأمنية وتبحث النموذج المرجعي المبين في التوصية [b-ITU-T Y.4401] مع التركيز على الجوانب التقنية وليس على الجوانب الإدارية.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجَعة، يُشجع جميع مستعملي هذه التوصية على بحث إمكانية تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T Y.4100] التوصية ITU-T Y.4100/Y.2066 (2014)، *المتطلبات المشتركة لإنترنت الأشياء*.

3 المصطلحات والتعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 هجوم (attack) [b-ISO13491-1]: محاولة الحصول على معلومات حساسة أو خدمة أو تعديلهما من جانب أحد الخصوم غير المرخص لهم بذلك.

2.1.3 استيقان (authentication) [b-NIST-SP-800-53]: التحقّق من هوية المستعمل أو العملية أو الجهاز، غالباً كشرط أساسي للسماح بالنفاذ إلى الموارد في نظام المعلومات.

3.1.3 المقدرة (capability) [b-ISO 19440]: مفهوم يمثل مجموعة من خصائص المقدرات (معبر عنها بنعوت المقدرة) لمورد (مقدرته المعروضة) أو نشاط مؤسسة (مقدرته المطلوبة).

ملاحظة – يمكن تجميع المقدرات.

4.1.3 السياق (context) [b-ITU-T X.1252]: بيئة محدَّدة الحدود توجد فيها الكيانات وتتفاعل.

5.1.3 خوارزمية التشفير (cryptographic algorithm) [b-ISO/IEC 19790]: إجراء حسابي محدد جيداً يمكن أن يتضمن مفاتيح تجفير وينتج ناتجاً من خلال متغيرات المدخلات.

6.1.3 عدد عشوائي ذي نوعية تجفيرية (cryptographic-quality random-number) [b-ITU-T X.667]: رقم عشوائي أو رقم عشوائي زائف تولده آلية ويضمن نشراً كافياً للقيم المولدة بشكلٍ متكرر لتكون مقبولة للاستخدام في عمليات التجفير (ويستخدم في هذه العمليات).

7.1.3 علم التجفير (cryptography) [b-ITU-T X.800]: التخصص الذي يجسد مبادئ ووسائل وطرائق تحويل البيانات من أجل إخفاء محتواها من المعلومات ومنع تعديلها خلسة و/أو منع استخدامها غير المرخص به.

ملاحظة – يحدد علم التجفير الطرائق المستخدمة في التجفير وفك التجفير. ويعتبر الهجوم على أي مبدأ أو وسيلة أو طريقة للتجفير بمثابة تحليل للتجفير.

8.1.3 نظام تجفير (cryptosystem) [b-ISO 11568-1]: مجموعة بدائيات التجفير التي تُستخدم لتوفير خدمات أمن المعلومات.

9.1.3 الجهاز (device) [b-ITU-T Y.4000]: في إنترنت الأشياء، هو معدة بقدرات اتصالات إلزامية وقدرات اختيارية للاستشعار والتفعيل ونقل البيانات وتخزينها ومعالجتها.

10.1.3 إدارة الهوية (identity management) [b-ITU-T X.1250]: مجموعة من الوظائف والمقدرات (مثل عمليات الإدارة والصيانة والكشف وتبادل الاتصالات والربط وإنفاذ السياسة والاستيقان والتأكيد) التي تستعمل للأغراض التالية:

- ضمان معلومات الهوية (من قبيل المعرفات والإثباتات والنعوت)؛
- ضمان هوية كيان ما (من قبيل المستعملين/المشتركين والمجموعات وأجهزة المستعمل والمنظمات وموردي الشبكات والخدمات وعناصر الشبكة وأغراضها والأغراض الافتراضية)؛
- توفير تطبيقات الأعمال التجارية والأمن.

11.1.3 إنترنت الأشياء (IoT) (Internet of things) [b-ITU-T Y.4000]: بنية تحتية عالمية لمجتمع المعلومات، تمكّن الخدمات المتطورة عن طريق التوصيل البيني للأشياء (المادية والافتراضية) استناداً إلى تكنولوجيات المعلومات والاتصالات القابلة للتشغيل البيني القائمة والمتطورة.

الملاحظة 1 – من خلال استغلال إمكانيات تعرّف الهوية ونقل البيانات ومعالجتها واتصالاتها، تستخدم إنترنت الأشياء استخداماً كاملاً لإتاحة الخدمات لجميع أنواع التطبيقات، مع ضمان الحفاظ على الخصوصية المطلوبة.

الملاحظة 2 – يمكن النظر إلى إنترنت الأشياء، من منظور أوسع، باعتبارها رؤية تنطوي على آثار تكنولوجية ومجتمعية.

12.1.3 كشف الاقتحام (intrusion detection) [b-ISO/IEC 27039]: عملية نظامية للكشف عن عمليات الاقتحام تتميز عموماً بجمع المعارف بشأن أنماط الاستعمال غير المعتادة، بالإضافة إلى تحديد نقاط الضعف وكيف تستغل وأي منها قد استغل بهدف تحديد كيفية استغلالها ومتى استغلت.

13.1.3 نظام كشف الاقتحام (intrusion detection system) [b-ISO/IEC 27039]: أنظمة معلومات تستخدم للكشف عن محاولة اقتحام أو عن الاقتحام أثناء حدوثه أو بعد حدوثه.

14.1.3 منع الاقتحام (intrusion prevention) [b-ISO/IEC 27033-1]: عملية نظامية لتقديم استجابة نشطة لمنع حالات الاقتحام.

15.1.3 نظام منع الاقتحام (intrusion prevention system) [b-ISO/IEC 27039]: شكل من أشكال أنظمة كشف الاقتحام مصمم خصيصاً لتوفير القدرة على الاستجابة النشطة.

16.1.3 إدارة المفاتيح (key management) [b-ITU-T X.800]: توليد المفاتيح وتخزينها وتوزيعها وإلغاؤها وأرشفتها وتطبيقها طبقاً لسياسة الأمن.

17.1.3 التجفير الخفيف (lightweight cryptography) [b-ISO/IEC 29192-1]: خوارزمية تجفير مصممة لكي تطبّق في بيئات مقيدة.

18.1.3 البرمجيات الضارة (malware) [b-ISO/IEC 27033-1]: برمجيات خبيثة مصممة خصيصاً لإلحاق الضرر بنظام أو تعطيله، مهاجمةً السرية و/أو السلامة و/أو التيسر.

ملاحظة – تشمل الأمثلة على البرمجيات الضارة الفيروسات وأحصنة طروادة.

19.1.3 مراقبة الشبكة (network monitoring) [b-ISO/IEC 27033-1]: عملية المراقبة والاستعراض المستمرين للبيانات المسجلة بشأن نشاط الشبكة وعملياتها، بما في ذلك سجلات التدقيق والإنذارات والتحليلات ذات الصلة.

20.1.3 المعلومات المحدِّدة لهوية شخص (personally identifiable information) (PII) [b-ISO/IEC 29100]: معلومات (أ) يمكن أن تستخدم للتعرّف على هوية الشخص الذي تتعلق به هذه المعلومات، أو (ب) قد تكون مرتبطة بشكل مباشر أو غير مباشر بهوية الشخص المراد التعرف عليه من خلالها.

ملاحظة – لتحديد إمكانية التعرف على هوية الشخص، يجب مراعاة جميع الوسائل التي يمكن لصاحب المصلحة في الخصوصية الذي يحوز البيانات أو أي طرف آخر أن يستعملوها استعمالاً معقولاً لتحديد هذا الشخص الطبيعي.

21.1.3 رابطة الأمن بقناع (security association with mask) (SAM) [b-ITU-T X.1362]: مجموعة من المعلمات المخصصة لبروتوكول الأمن. وتحدد الرابطة SAM الخدمات والآليات اللازمة لحماية الحركة بإجراء التجفير ببيانات قناع مصاحب (EAMD). ويشار إلى الرابطة SAM بالبروتوكول المرتبط بها، بحسب طبقات البروتوكول مثل طبقة النقل أو طبقة بروتوكول الإنترنت (IP). ويمكن أن تدرج ضمن هذه المعلمات معرفات هوية الخوارزميات، والأساليب، ومعرفات هوية الطبقات التي يطبق عليها التجفير EAMD، ومفاتيح التشفير.

22.1.3 جهاز الاستشعار (sensor) [b-ITU-T Y.4105]: جهاز إلكتروني يستشعر ظرفاً مادياً أو مركباً كيميائياً ويخرج إشارة كهربائية تتناسب مع الخاصية المرصودة.

23.1.3 الشيء (thing) [b-ITU-T Y.4000]: في إنترنت الأشياء، هو كائن من العالم المادي (أشياء مادية) أو من عالم المعلومات (أشياء افتراضية)، يتسم بإمكانية تحديده ودمجه في شبكات الاتصالات.

24.1.3 تهديد (threat) [b-ISO/IEC 27000]: سبب محتمل لحادث غير مرغوب قد يُلحق ضرراً بالنظام أو المنظمة.

25.1.3 مواطن الضعف (vulnerability) [b-ISO/IEC 27000]: مكمن ضعف في أصل من الأصول أو في وسيلة تحكم يمكن استغلاله من جانب تهديد واحد أو أكثر.

2.3 المصطلحات المعرفة في هذه التوصية

تعرف هذه التوصية المصطلح التالي:

1.2.3 تفاوض خوارزمية التشفير (cryptographic algorithm negotiation): آلية لتحديد نوع خوارزمية التشفير وطول مفاتيح التشفير لاستخدامها في دورة اتصالات مشفرة ومتكاملة والتحقق من خوارزمية التشفير الأكثر ملاءمة في كلا الجانبين.

ملاحظة – اقتبس هذا التعريف بتصرف من التوصية [b-ISO/IEC 27033-1] ويشار إليه في هذه التوصية بمصطلح "بوابة".

2.2.3 إدارة البرمجيات التصحيحية (patch management): عملية تشمل الحصول على برمجيات تصحيحية متعددة واختبارها وتثبيتها على أنظمة المعلومات.

ملاحظة – يمكن استعمال قدرات إدارة مكامن الضعف.

3.2.3 انتهاك المعلومات المحدِّدة لهوية شخص (PII breach): الحالة التي تحدث فيها معالجة للمعلومات المحددة لهوية شخص بالمخالفة لشرط واحد أو أكثر من شروط حماية هذه المعلومات.

4.2.3 نموذج تفضيلات الخصوصية (privacy preference model): نموذج يسمح لمواقع الويب بالإفصاح عن الغرض من استعمال البيانات التي تجمعها عن الأفراد، لمنحهم قدرة أكبر على التحكم في معلوماتهم الشخصية.

5.2.3 التشكيل الآمن (secure configuration): العملية التي ينبغي أن يتم بها تشكيل أجهزة الشبكة للحد من نقاط الضعف الكامنة والاقتصار على توفير الخدمات المطلوبة لكي تؤدي هذه الأجهزة دورها.

ملاحظة – يشمل ذلك إزالة أو تعطيل حسابات المستعملين غير الضروريين والبرمجيات غير الضرورية، وتغيير أي كلمة مرور افتراضية إلى كلمة مرور بديلة وحصينة، وتفعيل جدار الحماية والتشكيل لتعطيل (منع) التوصيلات غير المصرح بها بشكل تلقائي، وتعطيل ميزة التشغيل التلقائي.

6.2.3 بوابة الأمن (security gateway): نقطة توصيل بين الشبكات، أو بين المجموعات الفرعية داخل الشبكات، أو بين تطبيقات البرمجيات داخل ميادين أمنية مختلفة بغرض حماية الشبكة وفقاً لسياسة أمنية معينة في بيئة إنترنت الأشياء.

7.2.3 هجمة القنوات الجانبية (side-channel attack): هجمة باستعمال المعلومات التي يتحصل عليها من التطبيق المادي لنظام تجفير.

ملاحظة – يمكن استغلال معلومات عن التوقيت الحاسوبي واستهلاك الطاقة والتسريبات الكهرومغناطيسية لاختراق نظام التجفير.

8.2.3 إدارة مواطن الضعف (vulnerability management): عملية تشمل تحديد مواطن الضعف وتصنيفها وعلاجها والتخفيف من حدتها.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية المختصرات التالية:

DoS رفض الخدمة *(Denial of Service)*

EAMD التجفير ببيانات قناع مصاحب *(Encryption with Associated Mask Data)*

IDS نظام كشف الاقتحام *(Intrusion Detection System)*

IoT إنترنت الأشياء *(Internet of things)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPS نظام منع الاقتحام *(Intrusion Prevention System)*

PII المعلومات المحددة لهوية الشخص *(Personally Identifiable Information)*

5 الاصطلاحات

لا توجد

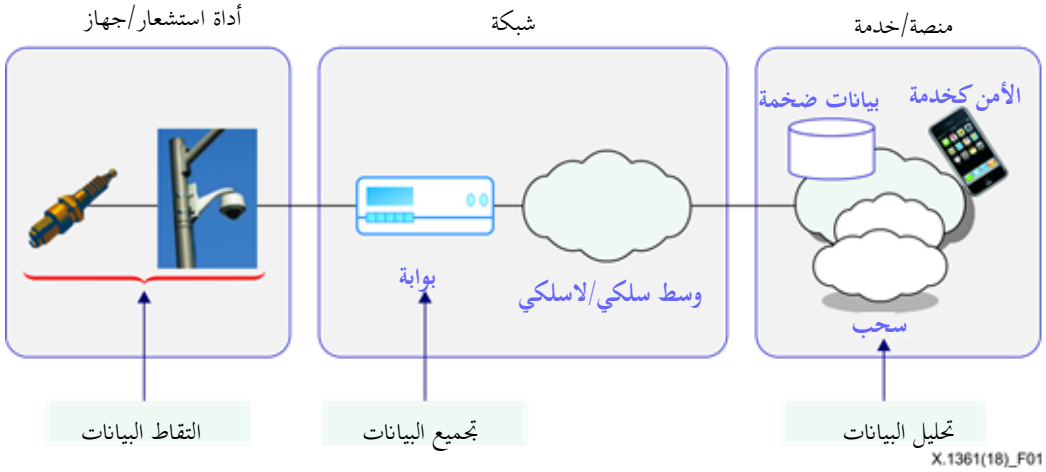
6 لمحة عامة

تُعرف إنترنت الأشياء (IoT) بأنها بنية تحتية عالمية لمجتمع المعلومات تمكّن الخدمات المتقدمة عن طريق التوصيل البيني للأشياء (المادية والافتراضية) استناداً إلى تكنولوجيات المعلومات والاتصالات القابلة للتشغيل البيني القائمة والمتطورة.

وتتألف أي حالة نشر نمطية لإنترنت الأشياء من أجهزة طرفية مزودة بوسائل استشعار على شبكة سلكية أو لاسلكية تقوم بإرسال البيانات عبر بوابة إلى سحابة عامة أو خاصة. وتختلف جوانب الطوبولوجيا اختلافاً كبيراً من تطبيق إلى آخر؛ فمثلا قد تكون البوابة في بعض الحالات على الجهاز. ويمكن بناء أجهزة قائمة بكاملها على هذه الطوبولوجيات للاستفادة من إنترنت الأشياء أو استعمال أجهزة تقليدية تضاف إليها قدرات إنترنت الأشياء بعد نشرها.

7 المعمارية الوظيفية والإطار

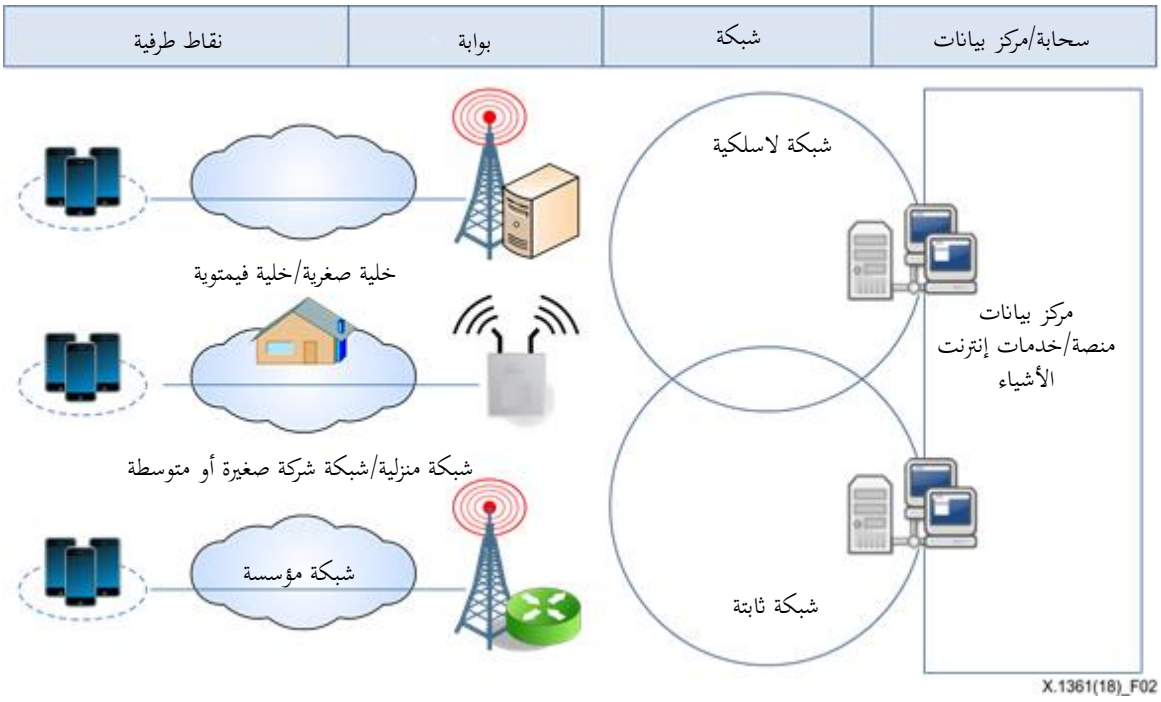
تستند هذه التوصية إلى المعمارية الوظيفية لإنترنت الأشياء المعروضة في الشكل 1.



الشكل 1 – المعمارية الوظيفية لإنترنت الأشياء (مبسّطة)

يمكن نقل البيانات بين نقطة طرفية لإنترنت الأشياء (أداة استشعار أو جهاز) والبوابة عبر نوعين من شبكات الاتصالات: شبكة قائمة على بروتوكول الإنترنت (IP) أو شبكة غير قائمة على بروتوكول الإنترنت. ويفترض أن يستعمَل بروتوكول قائم على بروتوكول الإنترنت من أجل إقامة الاتصال بين البوابة ومكون إنترنت الأشياء في منصة إنترنت الأشياء المنشورة في مركز للبيانات. ولذلك ينبغي في حالة الشبكة غير القائمة على بروتوكول الإنترنت أن يتم إنهاء التوصيل عبر الشبكة غير القائمة على بروتوكول الإنترنت وأن يعاد إقامته عبر شبكة قائمة على بروتوكول الإنترنت عند البوابة.

ويمكن تفصيل المعمارية الوظيفية على النحو المبين في الشكل 2.



الشكل 2 – المعمارية الوظيفية العملية

في أي نظام ذكي للنقل مثلا، يمكن للبوابة، كما هو مبين في الشكل 2، أن تؤدي وظيفة بوابة الاتصالات المتنقلة للمركبة للتوصيل بين شبكة منطقة داخلية (لسيارة) وشبكة خارجية مفتوحة.

وينبغي وجود مقدرة جدار حماية في البوابة للتحكم في الحركة المقصود إنهاؤها عند الجهاز. ولبعض أجهزة إنترنت الأشياء بروتوكولات نقل فريدة تختلف عن بروتوكول التحكم في الإرسال (TCP)/البروتوكولات القائمة على بروتوكول الإنترنت. ويمكن استعمال

بروتوكولات مشمولة بحقوق الملكية لتنظيم كيفية الاتصال بين أجهزة إنترنت الأشياء. ولذلك ينبغي وجود مقدرات ترشيح البروتوكولات الخاصة بالصناعة تحديداً لتحديد الحمولات النافعة الخبيثة التي يمكن أن تندس في البروتوكولات غير القائمة على بروتوكول الإنترنت.

وينبغي أن تنفذ البوابة وظيفة لترشيح البيانات المحددة المقصود إنهاؤها على هذا الجهاز بطريقة تحقق الاستخدام الأمثل للموارد الحاسوبية المحدودة المتاحة.

وتشارك البوابة كعنصر فريد في المعمارية الوظيفية. وغالباً ما تكون البوابة هي نقطة الأمان الأولى الموثوقة في نظام إنترنت الأشياء، لأن النقاط الطرفية هي الأكثر تعرضاً للعبث المادي. وتؤدي البوابة دوراً في إنترنت الأشياء يقتضي تمييزها كأصل من الأصول الأمنية المحددة، بعيداً عن الشبكة. ويجب أن تراعي البوابة القيود المفروضة على عُقد أدوات الاستشعار. ويمكن للبوابة في معظم الأحيان أن تؤدي بعض الوظائف الأمنية بالنيابة عن النقاط الطرفية المقيدة مثل: إدارة المفاتيح، وتفاوض التجفير، ومنع الاقتحام، وغير ذلك.

وستتمتع البوابة بإمكانات أمنية شديدة التنوع رهناً بعوامل مثل: قدرة وإمكانات النقاط الطرفية وتصميم الخدمات وتصميم الشبكة والمواقع المادية وبيئة الاستعمال.

8 التهديدات الأمنية التي تواجه إنترنت الأشياء

1.8 التهديدات الأمنية التي تواجه أدوات الاستشعار/أجهزة إنترنت الأشياء

التهديدات الخاصة بأدوات الاستشعار/الأجهزة

- الاستيلاء على الجهاز: يشير إلى الانتهاك المادي لجهاز أو فقدانه لمفاتيحه.
- هجمة الثقب الأسود (Sinkhole): تشير إلى هجمة يجتذب فيها الجهاز المنتهَك حركة الاتصالات لتكوين ثقب أسود أو بدء إعادة تسيير انتقائية. وفي هجمة الثقب الأسود، ينتهك الشخص الدخيل جهازاً أو يدس جهازاً مزيفاً داخل الشبكة ويستخدمه لشن هجمة ثقب أسود. ويحاول الجهاز المنتهَك أن يجتذب جميع حركة البيانات من العقد المجاورة استناداً إلى مقياس التسيير المستعمل في بروتوكول التسيير. وعندما يتحقق ذلك، يشنّ الجهاز المنتهَك هجمة. وهجمات الثقب الأسود هي نوع من الهجمات على طبقة الشبكة حيث يرسل الجهاز المنتهَك معلومات تسيير مزيفة إلى الأجهزة المجاورة له لجذب حركة الشبكة إليه. وبسبب الشبكات المخصصة وأنماط الاتصالات من عدة نقاط إلى نقطة في الشبكة اللاسلكية حيث ترسل العديد من العقد بيانات إلى محطة قاعدة وحيدة، تكون الشبكة اللاسلكية بوجه خاص معرضة لهجمات الثقب الأسود. واستناداً إلى تدفقات الاتصالات في أي شبكة لاسلكية، لا يحتاج الثقب الأسود إلى استهداف جميع العقد في الشبكة، بل فقط تلك العقد القريبة من المحطة القاعدة.
- الهجمات بهويات مزورة (Sybil): تشير إلى هجمة ينتحل فيها جهاز خبيث هويات متعددة بصورة غير مشروعة. ويُشار إلى الهوية الإضافية للجهاز الخبيث بعقدة الهوية المزورة. وتُشنُّ هذه الهجمة بالاقتران مع هجمات أخرى، للحد من فعالية آليات تحمل الأعطال، مثل التخزين الموزع، والتسيير المتعدد المسيرات وصيانة الطوبولوجيا.
- هجوم الإغراق: هجوم الإغراق هو شكل من هجمات رفض الخدمة (DoS) يرسل فيه المهاجم سلسلة متعاقبة من رزم 'hello' إلى الجهاز المستهدف في محاولة لاستهلاك قدرٍ كافٍ من موارد الجهاز لجعل الجهاز لا يستجيب للحركة المشروعة.
- هجمات إعادة التسيير الانتقائي: في هذه الهجمة، ترشح العقدة المنتهَكة عشوائياً الرزم المستقبَلة وتعيد تسيير بعض منها إلى العقدة التالية. وعندما ترشح العقدة (تُسقِط) جميع الرزم التي تتلقاها، فإن هذه الهجمة تسمى هجمة 'ثقب أسود'.
- هجمة الثقب الدودي (Wormhole): تحدث هجمات الثقب الدودي عندما تعلن عقدتان خبيثتان/منتهَكتان أن هناك مسيراً قصيراً جداً بينهما. والمسار البيني هو مسير بيانات بين جهازين موصلين شبكياً، يقام عبر بنية تحتية شبكية قائمة. وتحصل الشبكة التي تمرر البيانات إلى شبكة أخرى على البيانات من شبكة ما وتستنسخها في شبكة أخرى من خلال المسار البيني وقد يختلط الأمر على تلك الشبكة بعينها بسبب هذا الإجراء. وأثناء ذلك، قد يدخل القرصان الشبكة

بسهولة ويسيء استخدامها. وبالاقتران مع هجمة الثقب الأسود والهجمة بهوية مزورة، يمكن أن تؤدي هذه الهجمة إلى إعادة تسيير انتقائي أو إلى تكوين ثقب أسود.

- انتحال هوية أداة الاستشعار/الجهاز. تحدث هذه الهجمة عندما ينجح مهاجم في انتحال هوية أداة استشعار مشروعة/جهاز مشروع.

2.8 التهديدات الأمنية التي تواجه بوابات إنترنت الأشياء

التهديدات التي تواجه البوابات تحديداً:

- النفاذ غير المرخص به: قد يتسبب النفاذ غير المرخص به إلى البوابة في إفشاء معلومات حساسة، وتغيير البيانات، ورفض الخدمة والاستخدام غير المشروع للموارد. فمثلاً، بمجرد نفاذ مهاجم ما إلى بوابة ما، يمكن أن يؤدي رصد البيانات غير المشفرة في هذه اللحظة إلى انتهاك بيانات أسماء المستعملين وكلمات المرور والتشكيلة الآمنة.
- البوابة الاحتيالية: حتى وإن كانت جميع البوابات اللاسلكية آمنة، فمن السهل على المهاجمين أن يطلقوا بوابة احتيالية خاصة بهم. فمثلاً، قد يثبت موظف شديد الفضول نقطة نفاذ لاسلكية في مكتبه دون الاهتمام بالأمن. ويمكن أن يساهم ذلك بفعالية في الالتفاف على العديد من الإجراءات الأمنية القائمة، بل وربما التسبب في التداخل الراديوي مع عملية التثبيت النظامية في المنظمة و/أو الشركة. ويمكن تثبيت نقطة نفاذ لاسلكية احتيالية بصورة مقصودة وسرية لتمكين المجرم من النفاذ بسهولة إلى الشبكة سواء محلياً أو عن بُعد. ويمكن للمجرم (المعروف أيضاً باسم 'التوأم الشرير') أن يستبدل نقطة نفاذ لاسلكية قائمة بنقطة أخرى يمكنه تشكيلها ومراقبة النفاذ إليها بشكل كامل أو حتى تشكيل نقطة نفاذ لاسلكية، احتيالية، بإعدادات مماثلة، ولكن بنسبة أعلى من القدرة اللازمة للتغلب على إشارة نقطة النفاذ اللاسلكية المشروعة. وبعد أن يُضلِّل الجهاز المشروع ويُستدرَج إلى التوصيل ببوابة احتيالية، يمكن جمع معلومات التوصيل السرية.
- هجمة رفض الخدمة: تؤدي هجمة رفض الخدمة إلى جعل الهدف شديد البطء أو التوقف تماماً عما يقدمه من خدمات باستنفاد ذاكرة الأهداف و/أو السعة. وتصبح الأهداف منشغلة بالاستجابة إلى الحركة غير المشروعة التي يرسلها المهاجمون. وتكون شبكة أجهزة الاستشعار اللاسلكية معرضة بوجه خاص لهجمات رفض الخدمة بسبب سماتها التي تشمل الوسط المفتوح والطوبولوجيا المتغيرة بصورة دينامية وغياب خط واضح للدفاع. وتطرح هجمات رفض الخدمة مشكلة متزايدة في شبكات اليوم. ولا تنطبق الكثير من تقنيات الدفاع المطورة لشبكة الاتصالات السلكية الثابتة على بيئات شبكات الاتصالات المتنقلة.

3.8 التهديدات الأمنية التي تواجه الشبكة

التهديدات الخاصة التي تواجه الشبكة

- النفاذ غير المرخص به: يمكن أن يتسبب النفاذ غير المرخص به إلى شبكة استشعار لاسلكية في الكشف عن معلومات حساسة وتغيير البيانات ورفض الخدمة والاستخدام غير المشروع للموارد. فمثلاً، كلما حصل المهاجم على النفاذ إلى شبكة من شبكات الاستشعار، فإن رصد البيانات غير المشفرة حينها قد يؤدي إلى انتهاك أسماء المستعملين وكلمات مرورهم.
- استشفاف الرزم: في شبكات الاستشعار غير اللاسلكية غير المزودة بقدرات تجفير، من السهل عموماً على المهاجمين أن يتنصتوا على اتصالات الشبكة. ويتطلب التنصت على هذا النوع من شبكة الاستشعار اللاسلكية وجود هوائي مع أدوات توصيل شبكي لاسلكية وجهاز لاستشفاف رزم الشبكة. وجهاز استشفاف رزم الشبكة هو أداة تضبط بطاقة الشبكة على "الأسلوب المشوش". ويعني ذلك أن السطح البيني سيتقبل ويعالج كل الحركة وليس فقط الحركة الموجهة إليها. ويُظهر المتجسس على الشبكة لمستعملها جميع رزم الشبكة ويفكك شفرتها لقراءتها بسهولة. وكل حركة نصية تُفهم بسهولة ويمكن أن توضع مراشيح للبحث عن بعض الكلمات المفتاحية أو القيم.

- سطو ببلوتوث (Bluejacking): هذه هجمة تُشنُّ على الأجهزة المتنقلة المزودة بإمكانية البلوتوث، مثل الهواتف الخلوية. ويبدأ المهاجم هذه الهجمة بإرسال رسائل غير مرغوب فيها إلى مستعملي الأجهزة المزودة بإمكانية البلوتوث. ولا تُلحق هذه الرسائل المرسلة ضرراً بالجهاز المستهدَف، لكنها قد تستدرج المستعمل إلى الرد بصورة ما أو إضافة بيانات اتصال جديدة إلى مجلد عناوين الجهاز.
- التهام ببلوتوث (Bluesnarfing): تؤدي هذه الهجمة إلى نفاذ غير مرخص به إلى المعلومات من جهاز لاسلكي مستهدَف عن طريق توصيل بلوتوث، ويحدث ذلك غالباً بين الهواتف، أو الحواسيب المكتبية، أو الحواسيب المحمولة، أو المساعدات الرقمية الشخصية (PDA). وقد يؤدي نجاح هذه الهجمة إلى النفاذ غير المرخص به إلى معلومات خصوصية وسرية على هذه الأجهزة.

4.8 التهديدات الأمنية التي تواجه المنصة/الخدمات

في الإنترنت، تكون المهمة الرئيسية لطبقة التطبيقات هي جمع ومعالجة عدد كبير من بيانات المستعملين، بما فيها المعلومات الشخصية للمستعملين أو المعلومات السرية لمختلف المعاملات. وهذه البيانات هي الهدف الرئيسي للمهاجم بغرض سرقتها أو العبث بها أو إتلافها. ومن الضروري حماية البيانات باستعمال آليات حماية الخصوصية. وتشمل التهديدات المحدقة بطبقة التطبيقات ما يلي: معالجة البيانات الضخمة، والأجهزة الذكية الخارجة عن السيطرة، والتدخل البشري غير المرخص به، وعدم قدرة الأجهزة الخارجة عن السيطرة على التعافي من الكوارث.

التهديدات الخاصة التي تواجه المنصات/الخدمات

- تحديد المواصفات: عملية استكشافية تستخدم لجمع معلومات عن المنصة/الخدمات.
- رفض الخدمة: هجمة تصبح فيها المنصة/الخدمة مغمورة بطلبات كثيفة على الخدمة بحيث تصبح مشغولة إلى درجة يتعذر عليها الاستجابة لطلبات العملاء الشرعيين.
- تنفيذ شفرة عشوائية: هجمة تحاول تشغيل شفرة خبيثة على منصة/خدمة لانتهاك مواردها ثم بعد ذلك شنّ هجمات إضافية.
- تنفيذ شفرة خبيثة: أي جزء من نظام برمجيات أو نص الغرض منه إحداث تأثيرات غير مرغوب فيها، وانتهاكات للأمن أو للمعلومات المحددة لهوية الشخص (PII)، أو الإضرار بنظام. ومن الأمثلة الشائعة الفيروسات والديدان وأحصنة طروادة.
- زيادة الامتيازات: هجمة تنفذ فيها الشفرة، باستعمال حساب عملية مميزة، لزيادة امتيازات المهاجم.
- حقن لغة الاستعمال البنيوية (SQL): هجمة تستغل مكامن الضعف في عملية التحقق من مدخلات تطبيق ما وشفرة النفاذ إلى البيانات لتنفيذ أوامر عشوائية تحقن معلومات أو تستخرجها.
- التنصت على الشبكة: هجمة تلتقط الرزم المرسلة من الشبكة وتقرأ محتوى البيانات بحثاً عن المعلومات الحساسة مثل كلمات المرور وتأشيرات الدورة أو أي نوع من المعلومات السرية.
- النفاذ غير المرخص به: هجمة تمكّن من النفاذ إلى منصة/خدمة باستعمال حساب شخص آخر أو طريقة أخرى للنفاذ. فمثلاً، إذا استمر شخص في تخمين كلمة مرور أو اسم المستعمل لحساب ليس حسابه إلى أن يحصل على النفاذ، فإن ذلك يعد نفاذاً غير مرخص به.
- القوة الغاشمة: هجمة يتم من خلالها التجريب المنهجي لجميع المفاتيح الممكنة إلى حين إيجاد المفتاح الصحيح.
- هجمات قاموس أسماء المستعملين/كلمات المرور: هجمة تعمل بصورة نظامية على إبطال آليات التجفير أو الاستيقان بتكرار محاولات كلمات المرور، باستعمال كلمات في قاموس.
- استعمال أسماء للمستعملين وكلمات مرور افتراضية/استعمال كلمات مرور ضعيفة: هجمة تُستغل فيها أسماء المستعملين وكلمات المرور الافتراضية/كلمات المرور الضعيفة للنفاذ إلى المنصة/الخدمات.
- هجمة بالتخمين: تحدث هذه الهجمة كلما تمكن المستعمل من تخمين معلومات محمية من قطع من المعلومات المنخفضة التصنيف التي يمكن النفاذ إليها بطريقة مشروعة.

– تسرب المعلومات المحدِّدة لهوية الشخص: إرسال المعلومات المحدِّدة لهوية الشخص عن قصد أو بدون قصد إلى بيئة غير موثوق بها.

9 متطلبات من أجل إنترنت الأشياء

تستند هذه التوصية إلى المتطلبات الرفيعة المستوى المبينة في التوصية [ITU-T Y 4100]، كما ترد مناقشتها في الملحق A.

10 القدرات الأمنية لإنترنت الأشياء

1.10 لمحة عامة

لا تتناول هذه التوصية سوى المتطلبات الأمنية وتراعي اعتمادية الخدمات وجودتها. وقد تم تفصيل القدرات الأمنية لإنترنت الأشياء انطلاقاً من القدرات المبينة في التوصية [b-ITU-T Y 4401].

القدرات العامة

ينبغي أن تتضمن معمارية إنترنت الأشياء ما يلي:

– قدرة اتصالات آمنة لدعم الاتصالات الآمنة والموثوقة والمحمية الخصوصية؛

– قدرة آمنة لإدارة المفاتيح لدعم الاتصالات الآمنة؛

– قدرة إدارة آمنة للبيانات لتوفير إدارة بيانات آمنة وموثوق بها ومحمية الخصوصية للبيانات؛

– قدرة استيقان من أجل الاستيقان من الأجهزة؛

– قدرة تخويل (مراقبة النفاذ) لتخويل الأجهزة؛

– قدرة تدقيق لرصد النفاذ إلى البيانات أو محاولات النفاذ إلى تطبيقات إنترنت الأشياء بصورة شفافة يمكن تعقبها وإعادة إنتاجها على نحوٍ كامل، استناداً إلى اللوائح والقوانين المناسبة؛

– قدرة آمنة لتوفير الخدمة من أجل تقديم خدمة آمنة وموثوق بها ومحمية الخصوصية؛

– قدرة تكامل آمنة من أجل دمج مختلف السياسات والتقنيات الأمنية المتعلقة بالمجموعة المتنوعة من المكونات الوظيفية لإنترنت الأشياء؛

– قدرة لتنفيذ البروتوكولات الآمنة التي تستعمل خوارزميات تجفير مقيسة ومتاحة لعامة الجمهور؛

– قدرة لتنفيذ البروتوكولات الآمنة استناداً إلى تجفير خفيف؛

– قدرة آمنة ومتينة لتحديث البرمجيات من أجل تحديث الوحدات النمطية للبرمجيات أو تطبيقاتها؛

– قدرة لإدارة الهوية من أجل أجهزة/أدوات استشعار إنترنت الأشياء والبوابات والمنصات/الخدمات؛

– قدرة للكشف عن مواطن الضعف؛

– قدرة لمراقبة النفاذ إلى البيانات أو محاولات النفاذ إلى تطبيقات إنترنت الأشياء بصورة شفافة يمكن تعقبها وإعادة إنتاجها بشكلٍ كامل؛

– قدرة أمنية قائمة على العتاد (مثل وحدة نمطية لمنصة موثوقة) لمنع حدوث المخاطر الأمنية المادية المصاحبة للتمثيل الافتراضي للشبكة والبوابة؛

– قدرة تسيير متعدد المسيرات لمنع هجمات إعادة التسيير الانتقائية؛

– قدرة لحماية المعلومات المحدِّدة لهوية الشخص من انتهاكات هذه المعلومات في جميع مراحل دورة حياة هذه المعلومات؛

– قدرة إمكانية تشكيل آمنة؛

- قدرة استعمال تجفير خفيف؛
- قدرة تجفير بسيط بإجراء التجفير ببيانات قناع مصاحب (EAMD) [b-ITU-T X.1362] للاتصال بالكيانات الأخرى بما في ذلك البوابة.

القدرات المتعلقة بخوارزمية التجفير

ينبغي أن تتضمن معمارية إنترنت الأشياء ما يلي:

- قدرة لإنتاج عدد عشوائي بجودة تجفيرية لدعم إدارة المفاتيح [b-IETF RFC 4086]؛
- قدرة للتحديث الدوري لمفاتيح التجفير الضرورية لتدفقات الإذاعة؛
- قدرة لاستعمال خوارزميات التجفير المقيسة.

القدرات المتعلقة بالسياق

ينبغي أن تشمل معمارية إنترنت الأشياء ما يلي:

- قدرة لمقاومة هجمات القنوات الجانبية؛
- قدرة لدعم ممارسات التشفير الآمن التي تقوم بإنفاذ تحقق صارم من مدخلات البيانات في الأنظمة والخدمات وتطبيقات قواعد البيانات وخدمات الويب؛
- قدرة لإجراء تقييم مخاطر مخطط له لتحديد المخاطر التي تواجهها السياقات التشغيلية.

2.10 القدرات الأمنية لأدوات الاستشعار/الأجهزة

يجب أن تتضمن أدوات استشعار/أجهزة إنترنت الأشياء ما يلي:

- قدرة لإدارة المفاتيح؛
- قدرة تفاوض لخوارزمية التجفير؛
- قدرة لتجفير البيانات وفي بعض الحالات بيانات مستوي التشوير والتحكم والإدارة من أجل التخفيف من حدة الشواغل الأمنية بشأن سرية البيانات المرسلة عبر الشبكات اللاسلكية؛
- قدرة لسلامة البيانات فيما يتعلق بالبيانات المرسلة عبر الشبكات اللاسلكية باستعمال مخططات مناسبة لحماية السلامة تعطي تأكيدات بأن بيانات المستعمل أو بيانات التشوير أو التحكم أو الإدارة لم يتم العبث بها أو تغييرها؛
- قدرة للاستيقان من منشأ البيانات أو هويات أدوات استشعار/أجهزة إنترنت الأشياء وهويات الإداريين وموظفي صيانة شبكات الاستشعار؛
- قدرة لإدارة البرمجيات التصحيحية، بما في ذلك تحديث وترقية الوحدات النمطية للبرمجيات الآمنة؛
- قدرة لتنفيذ بروتوكولات آمنة قائمة على تجفير خفيف؛
- قدرة للتحكم في النفاذ لضمان أن يقتصر النفاذ إلى عناصر الشبكة والمعلومات المخزنة وتدفقات المعلومات والخدمات والتطبيقات على المخوَّل له بذلك من الأشخاص أو الأجهزة؛
- قدرة لكشف العبث و/أو منع العبث؛
- قدرة لإنتاج أرقام عشوائية بجودة تجفيرية لدعم إدارة المفاتيح؛
- قدرة لمقاومة هجمات القنوات الجانبية؛
- قدرة للكشف عن البرامج الضارة والحماية منها؛
- قدرة لحماية المعلومات المحددة لهوية الشخص من التسرب؛

ينبغي أن تتضمن أجهزة إنترنت الأشياء ما يلي:

- قدرة للتحقق من استيقان وسلامة البرمجيات المثبتة على الأجهزة باستعمال التوقيعات الرقمية المولدة تجفيرياً [b-ISO/IEC 9796-3]؛
- قدرة جدار حماية أو كشف الاقتحام أو الحماية من الاقتحام أو القدرة على الفحص العميق للرزم لمراقبة الحركة المقصود إنهاؤها في جهاز ما؛
- قدرة لإجراء تشكيلات آمنة.

3.10 القدرات الأمنية للبوابات

يجب أن تتضمن البوابة ما يلي:

- قدرة نظام للكشف عن الاقتحام (IDS)/نظام لمنع الاقتحام (IPS)؛
- قدرة لإدارة المفاتيح؛
- قدرة لإجراء تشكيلات آمنة؛
- قدرة تفاوض لخوارزمية التجفير؛
- قدرة لتجفير البيانات وفي بعض الحالات بيانات مستوي التشوير والتحكم والإدارة مع أجهزة ومكونات إنترنت الأشياء في مركز البيانات من أجل التخفيف من حدة الشواغل الأمنية بشأن سرية البيانات المرسلة عبر الشبكات اللاسلكية؛
- قدرة لسلامة البيانات فيما يتعلق بالبيانات المرسلة عبر الشبكات اللاسلكية باستعمال مخططات مناسبة لحماية السلامة تعطي تأكيدات بعدم العبث ببيانات المستعمل أو بيانات التشوير أو التحكم أو الإدارة أو تغييرها؛
- قدرة تيسير للتعامل مع هجمات رفض الخدمة تتراوح بين استعمال تقنيات التشفير الآمن للمصدر واختبار تحليل شفرة المصدر واختبار قابلية التعرض واستعمال نظام للكشف عن الاقتحام (IDS)/نظام لمنع الاقتحام (IPS) قائم على الشبكة أو المضيف؛
- قدرة للاستيقان من منشأ البيانات أو هويات أدوات استشعار/أجهزة إنترنت الأشياء وهويات الإداريين وموظفي صيانة شبكات الاستشعار؛
- قدرة للتحكم في النفاذ لضمان أن يقتصر النفاذ إلى عناصر الشبكة والمعلومات المخزنة وتدفقات المعلومات والخدمات والتطبيقات على المخوَّل له بذلك من الأشخاص أو الأجهزة؛
- قدرة مساءلة لأجهزة إنترنت الأشياء لضمان إمكانية تتبع الجهاز المسؤول عن أي انتهاك للسياسة الأمنية.

ويتعين أن تتوفر في البوابة إمكانية لتحديث الوحدات النمطية للبرمجيات الآمنة.

4.10 القدرات الأمنية للشبكة

لا تندرج القدرات الأمنية للشبكة ضمن نطاق هذه التوصية.

ملاحظة – يمكن استعمال القدرات الأمنية للوفاء بالأبعاد الأمنية المبينة في التوصية [b-ITU-T X.805].

5.10 القدرات الأمنية للمنصات/الخدمات

ينبغي أن تتضمن المنصة/ الخدمة الإمكانات التالية:

- قدرة لحماية بيانات الاعتماد لأغراض عمليات التجفير، وهي مجموعة من البيانات المقدمة كدليل للهوية و/أو المستحقات المدعاة؛
- قدرة لتغيير أسماء المستعملين وكلمات المرور الافتراضية أثناء الإعداد الأولي؛
- قدرة لتنفيذ كلمات مرور قوية وسياسة دقيقة للتحكم في النفاذ؛

- قدرة لإلغاء تيسر المنافذ غير الضرورية؛
- قدرة لدعم التشكيل الآمن لإزالة الخدمات والبرمجيات غير الضرورية مثلاً؛
- قدرة للحماية من الإصابة بالبرمجيات الضارة من خلال استعمال برمجيات الحماية من البرمجيات الضارة؛
- قدرة لتنفيذ سياسات إدارة البرمجيات التصحيحية؛
- قدرة لإدارة مواطن الضعف؛
- قدرة لتحديث الوحدات النمطية للبرمجيات الآمنة وتطبيقاتها؛
- قدرة لإدارة المفاتيح لأغراض النقل الآمن للرسائل بين بوابة ومنصة/خدمة؛
- قدرة مفاوضات لخوارزمية التجفير لإقامة مسيرات آمنة بين البوابة والمنصة/الخدمة، في حالة الحاجة إلى نقل آمن للرسائل بين البوابة والمنصة/الخدمة؛
- قدرة تيسر للتعامل مع هجمات رفض الخدمة؛
- قدرة لمراقبة الشبكة؛
- قدرة لحماية المعلومات المحدِّدة لهوية شخص أثناء السكون؛
- قدرة لأمن مستوى التطبيقات لمنع التهديدات والهجمات على مستوى التطبيقات، على النحو المبين في الفقرة 4.8؛
- قدرة لتقديم الدعم للتخفيف من حدة هجمات التخمين.

الملحق A

متطلبات الأمن والخصوصية المبينة في التوصية ITU-T Y.4100/Y.2066

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية.)

تشير متطلبات حماية الأمن والخصوصية إلى المتطلبات الوظيفية أثناء التقاط بيانات الأشياء وتخزينها ونقلها وتجميعها ومعالجتها، فضلا عن توفير الخدمات التي تتضمن الأشياء. وتتعلق هذه المتطلبات بجميع الجهات الفاعلة في إنترنت الأشياء.

ويقدم هذا الملحق المتطلبات العالية المستوى المتعلقة بالأمن والخصوصية كما هي مبينة في الملحق A من التوصية [ITU-T Y.4100] وتشير المصطلحات الواردة بين الأقواس في كل فقرة أدناه إلى العنصر الخاص بها في الملحق A من التوصية [ITU-T Y.4100].

1.A أمن الاتصالات

يلزم توفير قدرة للاتصالات الآمنة والموثوقة والمحمية الخصوصية لكي يُحظر كل نفاذ غير مرخص به إلى محتوى البيانات، ولكي يتسنى ضمان سلامة البيانات وحماية محتويات البيانات المتعلقة بالخصوصية أثناء إرسال البيانات أو نقلها في إنترنت الأشياء [SP1].

2.A أمن إدارة البيانات

يلزم توفير قدرة لإدارة البيانات الآمنة والموثوقة والمحمية الخصوصية لكي يُحظر كل نفاذ غير مرخص به إلى محتوى البيانات، ولكي يتسنى ضمان سلامة البيانات وحماية محتويات البيانات المتعلقة بالخصوصية أثناء تخزين البيانات أو معالجتها في إنترنت الأشياء [SP2].

3.A أمن توفير الخدمات

يلزم توفير قدرة لتوفير الخدمة الآمنة والموثوقة والمحمية الخصوصية لكي يُحظر كل نفاذ غير مرخص به إلى الخدمة وتقديم الخدمات الاحتيالية، ولكي يتسنى حماية المعلومات المتعلقة بخصوصية مستعملي إنترنت الأشياء [SP3].

4.A تكامل السياسات والتقنيات الأمنية

يلزم توفر القدرة على دمج مختلف السياسات والتقنيات الأمنية، لكي يتسنى ضمان الاتساق في المراقبة الأمنية على مجموعة متنوعة من الأجهزة وشبكات المستعملين في إنترنت الأشياء [SP4].

5.A الاستيقان والتخويل المتبادل

قبل أن يتمكن أي جهاز (أو مستعمل لإنترنت الأشياء) من النفاذ إلى إنترنت الأشياء، يلزم إجراء استيقان وتخويل متبادل بين الجهاز (أو مستعمل إنترنت الأشياء) وإنترنت الأشياء وفقاً للسياسات الأمنية المحددة سلفاً [SP5].

6.A التدقيق الأمني

يلزم دعم التدقيق الأمني في إنترنت الأشياء. ويلزم أن يتسم كل نفاذ إلى البيانات أو محاولة نفاذ إلى تطبيقات إنترنت الأشياء بالشفافية وإمكانية التتبع وإعادة الإنتاج بشكلٍ كامل وفقاً للوائح والقوانين ذات الصلة. وبوجهٍ خاص، يلزم أن تدعم إنترنت الأشياء التدقيق الأمني لأغراض إرسال البيانات وتخزينها ومعالجتها والنفاذ إلى التطبيقات [SP6].

التذييل I

قدرات الأمن والخصوصية المبينة في التوصية ITU-T Y.4401/Y.2068

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم هذا التذييل القدرات عالية المستوى المتعلقة بالأمن والخصوصية المبينة في التوصية [ITU-T Y.4401] وتشير المصطلحات الواردة بين الأقواس في كل فقرة أدناه إلى العنصر الخاص بها في التوصية [b-ITU-T Y.4401].

1.I قدرة أمن الاتصالات

تشمل قدرة أمن الاتصالات قدرات دعم الاتصالات الآمنة والموثوقة والمحمية الخصوصية [C-7-1].

2.I قدرة أمن إدارة البيانات

تشمل قدرة أمن إدارة البيانات قدرات توفير إدارة البيانات الآمنة والموثوقة والمحمية الخصوصية [C-7-2].

3.I قدرة أمن توفير الخدمة

تشمل قدرة أمن توفير الخدمة قدرات توفير الخدمة الآمنة والموثوقة والمحمية الخصوصية [C-7-3].

4.I قدرة التكامل الأمني

تشمل قدرة التكامل الأمني قدرات دمج مختلف السياسات والتقنيات الأمنية المتعلقة بمجموعة متنوعة من المكونات الوظيفية لإنترنت الأشياء [C-7-4].

5.I قدرة الاستيقان والتخويل المتبادل

تشمل قدرة الاستيقان والتخويل المتبادل قدرات استيقان وتخويل كل جهاز قبل أن ينفذ هذا الجهاز إلى إنترنت الأشياء استناداً إلى سياسات أمنية محددة سلفاً [C-7-5].

6.I قدرة التدقيق الأمني

تشمل قدرة التدقيق الأمني قدرات مراقبة النفاذ إلى البيانات أو محاولات النفاذ إلى تطبيقات إنترنت الأشياء بصورة تتسم بالشفافية وإمكانية التتبع وإعادة الإنتاج بشكل كامل وفقاً للوائح والقوانين ذات الصلة [C-7-6].

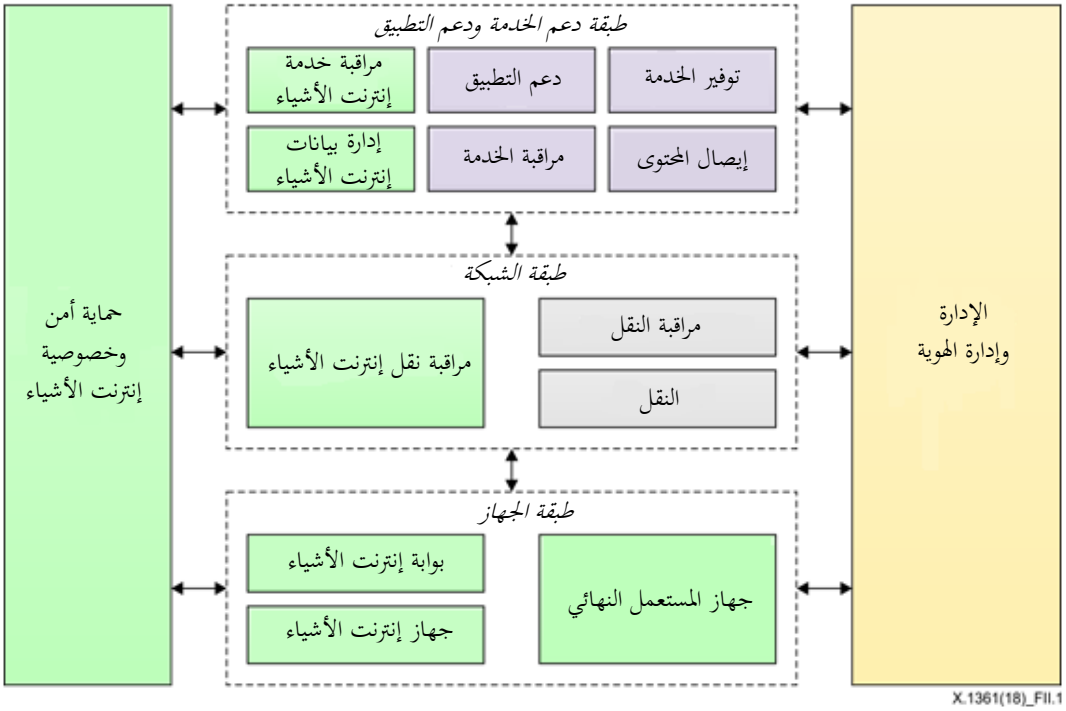
ملاحظة - تشمل قدرات حماية الأمن والخصوصية هذه أيضاً القدرة على التعامل مع المسائل المرتبطة بحماية الأمن والخصوصية في عمليات تشمل ميادين مختلفة.

التذييل II

نظرة التنفيذ لبناء الإطار الوظيفي لإنترنت الأشياء عبر المعمارية الوظيفية لشبكات الجيل التالي كما وردت في التوصية ITU-T Y.4401/Y.2068

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يوضح الشكل 1.II نظرة تنفيذ للإطار الوظيفي لإنترنت الأشياء، بناءً على الكيانات الوظيفية المبينة في المعمارية الوظيفية لشبكات الجيل التالي (NGN) الواردة في التوصية [b-ITU-T Y.4401] والتي ترتبط بالإطار الوظيفي الأمني الوارد في هذه التوصية. وتعرض هذه التوصية قدرات طبقة دعم الخدمة وطبقة الجهاز المبينة في الشكل 7-2 من التوصية [b-ITU-T Y.4401].



الشكل 1.II – نظرة التنفيذ لبناء الإطار الوظيفي لإنترنت الأشياء فيما يتعلق بالمعمارية الوظيفية لشبكة الجيل التالي

بيبليوغرافيا

[b-ITU-T X.667] Recommendation ITU-T X.667 (2012), *Information technology – Procedures for the operation of object identifier registration authorities: Generation of universally unique identifiers and their use in object identifiers*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-IUT-T X.1250] Recommendation ITU-T X.1250 (2009), *Baseline capabilities for enhanced global identity management and interoperability*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1311] Recommendation ITU-T X.1311 (2011) | ISO/IEC 29180:2012, *Information technology – Security framework for ubiquitous sensor networks*.

[b-ITU-T X.1362] Recommendation ITU-T X.1362 (2017), *Simple encryption procedure for Internet of things (IoT) environments*.

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ITU-T Y.4050] Recommendation ITU-T Y.4050/Y.2069 (2012), *Terms and definitions for the Internet of things*.

[b-ITU-T Y.4105] Recommendation ITU-T Y.4105/Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment*.

[b-ITU-T Y.4113] Recommendation ITU-T Y.4113 (2016), *Requirements of the network for the Internet of things*.

[b-ITU-T Y.4400] Recommendation ITU-T Y.4400/Y.2063 (2012), *Framework of the web of things*.

[b-ITU-T Y.4401] Recommendation ITU-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things*.

[b-IETF RFC 4086] IETF RFC 4086 (2005), *Randomness Requirements for Security*.

[b-ISO 11568-1] ISO 11568-1:2005, *Banking – Key management (retail) – Part 1: Principles*.

[b-ISO 13491-1] ISO 13491-1:2016, *Financial services – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods*.

[b-ISO 19440] ISO 19440:2007, *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/IEC 9796-3] ISO/IEC 9796-3:2006, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms*.

[b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules.*

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/IEC 27033-6] ISO/IEC 27033-6:2016, *Information technology – Security techniques – Network security – Part 6: Securing wireless IP network access*.

[b-ISO/IEC 27039] ISO/IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS).*

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

[b-ISO/IEC 29192-1] ISO/IEC 29192-1:2012, *Information technology – Security techniques – Lightweight cryptography – Part 1: General*.

[b-NIST SP 800-53] NIST Special Publication 800-53 (2013), *Security and Privacy Controls for Federal Information Systems and Organizations*.

[b-ZT] Zhang Li, Tong Xin (2013), *Threat Modeling and Countermeasures Study for the Internet of Things*, Journal of Convergence Information Technology (JCIT), *Vol. 8, No. 5, March.*

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2019