التوصية

ITU-T X.1352 (2022) Amd.1 (03/2024)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة (2) - أمن إنترنت الأشياء (IoT)

المتطلبات الأمنية لأجهزة إنترنت الأشياء (IoT) وبواباتها

التعديل 1: إضافات وتصويبات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199-X.1
التوصيل البيني للأنظمة المفتوحة	X.299-X.200
التشغيل البيني للشبكات	X.399-X.300
أنظمة معالجة الرسائل	X.499-X.400
الدليل	X.599-X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699-X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799-X.700
الأمن	X.849-X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899-X.850
المعالجة الموزعة المفتوحة	X.999-X.900
أمن المعلومات والشبكات	X.1099-X.1000
تطبيقات وخدمات آمنة (1)	X.1199-X.1100
أمن الفضاء السيبراني	X.1299-X.1200
تطبيقات وخدمات آمنة (2)	X.1499-X.1300
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319-X.1310
أمن شبكة الكهرباء الذكية	X.1339-X.1330
البريد المعتمد	X.1349-X.1340
أمن إنترنت الأشياء (IoT)	**X.1369-X.1350**
أمن أنظمة النقل الذكية (ITS)	X.1399-X.1370
أمن سجل الحسابات الموزع	X.1429-X.1400
أمن التطبيقات (2)	X.1459-X.1450
أمن شبكة الويب (2)	X.1489-X.1470
تبادل معلومات الأمن السيبراني	X.1599-X.1500
أمن الحوسبة السحابية	X.1699-X.1600
الاتصالات الكمومية	X.1729-X.1700
أمن البيانات	X.1799-X.1750
أمن شبكات الاتصالات المتنقلة الدولية	X.1839–X.1800
أمن الميتافيرس والتوأمة الرقمية	X.2199-X.2000
أمن سلسلة توريد البرمجيات	X.2199-X.2150
أمن الذكاء الاصطناعي (AI) / تعلّم الآلة (ML)	X.2249-X.2200

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

التوصية ITU-T X.1352

المتطلبات الأمنية لأجهزة إنترنت الأشياء (IoT) وبواباتها

التعديل 1

إضافات وتصويبات

ملخص

تحدد التوصية ITU-T X.1352 المتطلبات التفصيلية لخمسة أبعاد أمنية تنطبق على أجهزة إنترنت الأشياء (IoT) وبواباتها: الاستيقان والتجفير وأمن البيانات وأمن منصات الأجهزة والأمن المادي. وتستند هذه المتطلبات الأمنية إلى النموذج المرجعي لإنترنت الأشياء المحدد في التوصية ITU-T Y.4100 وإلى الإطار الأمني لإنترنت الأشياء المحدد في التوصية ITU-T X.1361.

ويشمل بُعد الاستيقان استيقان المستعمل والاستخدام الآمن لبيانات اعتماد الاستيقان واستيقان الجهاز. ويشمل بُعد التجفير استخدام التجفير الآمن والإدارة الآمنة للمفاتيح والتوليد الآمن للأرقام العشوائية. وأما بُعد أمن البيانات، فهو يشمل الإرسال والتخزين الآمنين والتحكم في تدفق المعلومات والإدارة الآمنة للدورة وإدارة المعلومات المحددة لهوية الشخص (PII). ويشمل بُعد أمن منصات الأجهزة خمسة عناصر، هي: أمن البرمجيات؛ التحديث الآمن؛ إدارة الأمن؛ السجلات؛ الختم الزمني. وبالمثل، يشمل بُعد الأمن المادي سطحاً بينياً مادياً آمناً والمناعة ضد العبث.

التسلسل التاريخي*

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد
1.0	ITU-T X.1352	2022-09-02	17	11.1002/1000/14990
1.1	ITU-T X.1352 (2022) Amd.1	2024-03-01	17	11.1002/1000/15665

مصطلحات أساسية

استيقان، تجفير، أمن البيانات، أمن منصات الأجهزة، أمن أجهزة إنترنت الأشياء وبواباتها، بوابة إنترنت الأشياء، تقييم أمن إنترنت الأشياء، أمن مادي.

* للنفاذ إلى توصية، ترجى كتابة العنوان https://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة 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 "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" 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/حقوق تأليف ونشر برمجيات 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 قواعد البيانات ذات الصلة لقطاع تقييس الاتصالات (ITU-T) في موقع قطاع تقييس الاتصالات http://www.itu.int/ITU-T/ipr/.

© ITU 2024

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

التوصية ITU-T X.1352

المتطلبات الأمنية لأجهزة إنترنت الأشياء (IoT) وبواباتها

التعديل 1

إضافات وتصويبات

ملاحظة صياغية: هذا منشور كامل النص. وترد التعديلات التي أدخلها هذا التعديل بعلامات المراجعة بالنسبة إلى التوصية ITU-T X.1352 (2022).

1 مجال التطبيق

تحدد هذه التوصية المتطلبات التفصيلية لخمسة أبعاد أمنية تنطبق على أجهزة إنترنت الأشياء (IoT) وبواباتها: الاستيقان؛ والتجفير؛ وأمن البيانات؛ وأمن منصات الأجهزة؛ والأمن المادي. وتستند هذه المتطلبات الأمنية إلى النموذج المرجعي لإنترنت الأشياء المحدد في التوصية [ITU-T Y.4100] وإلى الإطار الأمني لإنترنت الأشياء المحدد في التوصية [ITU-T X.1361].

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 للمراجعة، يشجَّع مستعملو هذه التوصية على بحث إمكانية تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1361] التوصية ITU-T X.1361 (2018)، *الإطار الأمني لإنترنت الأشياء القائم على نموذج البوابة*.

[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 الاستيقان (authentication) [b-ITU-T X.1254]: تقديم ضمان للهوية التي يدعيها كيان ما.

2.1.3 القدرة (capability) [b-ISO 16100-1]: مجموعة من الوظائف والخدمات مع مجموعة من المعايير لتقييم أداء مورِّد القدرات.

3.1.3 الكتمان (confidentiality) [b-ITU-T X.800]: خاصية عدم إتاحة المعلومات أو الكشف عنها لأشخاص غير مخولين أو لكيانات، أو عمليات غير مُخَوَّلَة.

4.1.3 بيانات الاعتماد (credential) [b-ITU-T X.1252]: مجموعة بيانات تقدم كدليل على هوية و/أو استحقاقات مزعومة.

5.1.3 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).

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

7.1.3 سلامة البيانات (data integrity) [b-ITU-T X.800]: خاصية بقاء البيانات على حالتها دون أن يطرأ عليها تغيير أو تلف بطريقة غير مرخص بها.

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

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

10.1.3 إدارة البرمجيات التصحيحية (patch management) [ITU-T X.1361]: عملية تشمل الحصول على برمجيات تصحيحية متعددة واختبارها وتثبيتها على أنظمة المعلومات.

ملاحظة – يمكن استعمال قدرات إدارة مكامن الضعف.

11.1.3 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.

12.1.3 الأمن المادي (capability) [b-ITU-T X.800]: تدابير مستخدمة لتوفير حماية مادية لموارد من تهديدات متعمدة أو عارضة.

13.1.3 التشكيل الآمن (secure configuration) [ITU-T X.1361]: العملية التي ينبغي أن يتم بها تشكيل أجهزة الشبكة للحد من مواطن الضعف الكامنة والاقتصار على توفير الخدمات المطلوبة لكي تؤدي هذه الأجهزة دورها.

14.1.3 بوابة الأمن (security gateway) [ITU-T X.1361]: 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.

ملاحظة – يشار إلى المصطلح أحياناً ببوابة. واقتبس هذا التعريف بتصرف من التوصية [b-ISO/IEC 27033-1].

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

16.1.3 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.

17.1.3 إدارة مواطن الضعف (vulnerability management) [ITU-T X.1361]: عملية تشمل تحديد مواطن الضعف وتصنيفها وعلاجها والتخفيف من حدتها.

2.3 المصطلحات المعرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 الهجوم المستنفد للاحتمالات كافة (brute-force attack): محاولات التجربة والخطأ للإخلال بآلية الاستيقان بتجربة القيم الممكنة لكلمات المرور أو المفاتيح.

21.2.3 البعد الأمني (security dimension): مجموعة من التدابير الأمنية المصممة لمعالجة جانب معين من جوانب الأمن.

3.2.32 أمن منصات الأجهزة (device platform security): مجموعة أمنية من أجل البرمجيات الثابتة وقدراتها المحدثة وإدارة برمجيات طرف ثالث إلى جانب قدرة التدقيق على جهاز إنترنت الأشياء وبوابتها.

ملاحظة – يستعاض عن البرمجيات الثابتة بالبرمجيات على نظام تشغيل تبعاً لقدرات العتاد.

3.2.43 التمويه (obfuscation): أثر عملية يتم إجراؤها على شفرة البرنامج أو بيانات التطبيق تؤدي إلى إخفاء التطبيقات أو تعتيمها بطريقة ما دون التأثير على خرج الشفرة.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية المختصرات التالية:

API السطح البيني لبرمجة التطبيقات (*Application Programming Interface*)

CAPTCHA اختبار تورينغ العام المؤتمت بالكامل للتمييز بين الحواسيب والبشر (*Completely Automated Public Turing test to tell Computers and Humans Apart*)

CoAP بروتوكول التطبيق المقيد (*Constrained Application Protocol*)

DDoS الحرمان من الخدمة الموزَّع (*Distributed Denial of Service*)

DoS الحرمان من الخدمة (*Denial of Service*)

F/W برمجية ثابتة (*Firmware*)

FTP بروتوكول نقل الملفات (*File Transfer Protocol*)

H/W عتاد (*Hardware*)

ID معرِّف الهوية (*Identifier*)

IDS نظام كشف التسلل (*Intrusion Detection System*)

IMEI الهوية الدولية للمعدات المتنقلة (*International Mobile Equipment Identity*)

IoT إنترنت الأشياء (*Internet of Things*)

IPS نظام منع التسلل (*Intrusion Prevention System*)

LwM2M بروتوكول الاتصالات الخفيفة من آلة إلى آلة (*Lightweight Machine to Machine*)

MAC التحكم في النفاذ إلى الوسائط (*Media Access Control*)

MCU وحدة التحكم الصغرية (*Microcontroller Unit*)

MQTT نقل القياس عن بُعد لخدمة وضع الرسائل في قائمة انتظار (*Message Queuing Telemetry Transport*)

OS نظام تشغيل (*Operating System*)

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

PIN رقم تعرّف الهوية الشخصي (*Personal Identification Number*)

S/W برمجية (*Software*)

SD رقمي آمن/رقمية آمنة (*Secure Digital*)

SHA خوارزمية اختزال مأمونة (*Secure Hash Algorithm*)

SNMP بروتوكول بسيط لإدارة الشبكات (*Simple Network Management Protocol*)

SSA الهجوم القائم على اختلاس النظر من فوق كتف المستخدم (*Shoulder-Surfing Attack*)

SSH بروتوكول الدرع الآمن (*Secure Shell*)

SWD تصحيح سلكي تسلسلي (*Serial Wire Debug*)

TLS أمن طبقة النقل (*Transport Layer Security*)

UART مستقبِل/مرسِل عالمي غير متزامن (*Universal Asynchronous Receiver/Transmitter*)

UID معرِّف الهوية الفريد (*Unique Identifier*)

UPnP التوصيل والتشغيل الشامل (*Universal Plug and Play*)

USB ناقل تسلسلي عام (*Universal Serial Bus*)

5 الاصطلاحات

تستعمل هذه التوصية الاصطلاحات التالية:

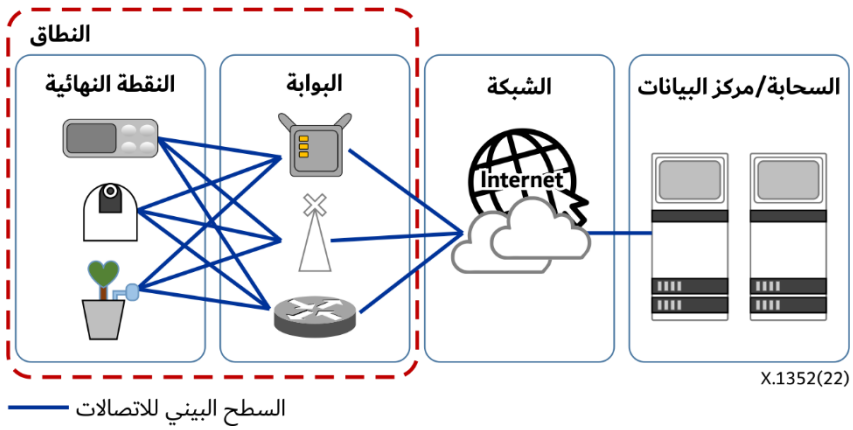
"ينبغي" فعل مساعد يدل على متطلب يوصى به لكنه غير إلزامي في المطلق.

"يجب" فعل مساعد يدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم الامتثال لهذه التوصية.

وفي متن هذه التوصية، يظهر الفعل المساعد "يمكن" أحياناً، وفي هذه الحالة يجب تفسيره على أنه يعني "يستطيع".

ولا ينطوي ظهور الفعل المساعد "ينبغي" في التذييل I على أي قصد معياري.

6 نظرة عامة



الشكل 1 – نطاق المتطلبات الأمنية

استناداً إلى القدرات الأمنية المقترحة في التوصيتين [ITU-T X.1361] و[ITU-T Y.4100] وعلى النحو المناقش في التذييل II، فإن المتطلبات الأمنية لمواجهة التحديات والتهديدات المتعلقة بأجهزة إنترنت الأشياء وبواباتها (باستثناء أنظمة الشبكات ومنصاتها) محددة لخمسة أبعاد أمنية، هي: الاستيقان، التجفير، أمن البيانات، أمن منصات الأجهزة، الأمن المادي.

ويتضمن بُعد الاستيقان استيقان المستعمل، والاستخدام الآمن لبيانات اعتماد الاستيقان، واستيقان الجهاز.

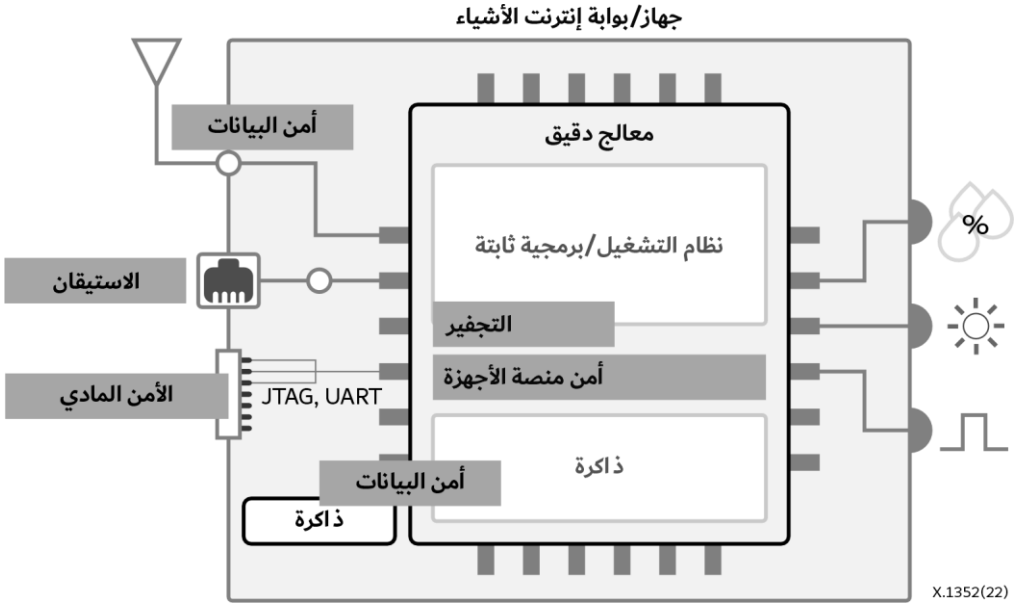
ويشمل بُعد التجفير استخدام خوارزميات تجفير آمنة، والإدارة الآمنة للمفاتيح، والتوليد الآمن للأرقام العشوائية.

ويتكون بُعد أمن البيانات من حماية بيانات الإرسال وحماية البيانات الساكنة، والتحكم في تدفق المعلومات، والإدارة الآمنة للدورة، وحماية المعلومات المحددة لهوية الشخص (PII).

وأما بُعد أمن منصات الأجهزة، فيشمل خمسة عناصر، هي: أمن البرمجيات (S/W) والتحديث الآمن وإدارة الأمن والسجلات والختم الزمني.

وبالمثل، فيما يتعلق ببُعد الأمن المادي، تم تحديد السطح البيني المادي الآمن والدفاع ضد العبث.

ويبين الشكل 2 أهداف الأبعاد الأمنية في أجهزة إنترنت الأشياء وبواباتها. وتتكون أجهزة إنترنت الأشياء وبواباتها عادةً من وحدة تحكم صغرية (MCU) ووحدة نمطية للاتصالات وذاكرة ومنافذ للدخول/الخروج. ويوجد عنصر آمن في شكل عتاد (H/W) أو برمجيات (S/W). وتحتوي وحدة MCU على برمجيات ثابتة (F/W) وسطوح بينية مادية وذاكرة. ويمكن هنا الاستعاضة عن S/W مع نظام التشغيل (OS) ببرمجيات F/W. وتتطلب الوحدة النمطية للاتصالات التجفير وأمن البيانات عند الإرسال. وتُخزن البيانات في الذاكرات المحمولة بشكل آمن من أجل الاستيقان والتجفير وكتمان/سلامة البيانات. ويتطلب النفاذ من خلال السطوح البينية المادية مثل المستقبِل/المرسِل العالمي غير المتزامن (UART) أيضاً استيقان المستعمل. وتتم إزالة السطوح البينية H/W غير المستخدمة وإيقاف تشغيلها.



الشكل 2 – مثال على أبعاد الأمن المطبقة على أجهزة الإنترنت وبواباتها

7 التهديدات/مواطن الضعف الأمنية التي تعاني منها أجهزة إنترنت الأشياء وبواباتها

يرد وصف التهديدات/مواطن الضعف الأمنية التي تعاني منها أجهزة إنترنت الأشياء وبواباتها، والتي قد تجعل منها أهدافاً ممكنة للهجمات السيبرانية، في الفقرتين 1.7 و2.7. وتشمل التهديدات الأمنية التي تواجهها البوابات التهديدات التي تواجهها أجهزة إنترنت الأشياء.

1.7 التهديدات/مواطن الضعف الأمنية التي تعاني منها أجهزة إنترنت الأشياء

تشمل التهديدات الخاصة بالأجهزة ما يلي:

- ST-D-1: تجاوز الاستيقان: عندما يتمكن مستعمل غير مرخص له من النفاذ إلى الجهاز ويستطيع بالإضافة إلى ذلك النفاذ إلى بيانات حرجة بما في ذلك بيانات المستعمل وملفات التشكيل المخزنة في الجهاز.
- ST-D-2: التوصيل غير المرخص بالجهاز: عندما يكون الجهاز معرضاً لأي جهاز غير مرخص أو يمكن إرسال بياناته، مثل بيانات المستعمل، إلى أي جهاز غير مرخص.
- ST-D-3: الامتياز المفرط: منح امتياز مفرط أو امتياز غير ضروري يمكّن المهاجم من النفاذ إلى جميع العمليات المقبولة والبيانات المتحكم فيها بما في ذلك بيانات مستعمل الجهاز.

- ST-D-4: محاولات الاستيقان غير المقيدة المتكررة: قد يتمكن المستعمل غير المرخص الذي يكرر محاولات الاستيقان من النفاذ إلى حساب مستعمل حقيقي.
- ST-D-5: الخطأ الناجم عن النفاذ المتزامن: قد يتسبب النفاذ المتزامن من حسابات مدير متعددة في تغييرات غير منسقة في تشكيل الوظائف الحرجة.
- ST-D-6: كشف معلومات الاستيقان وتخمينها: عندما تكون معلومات الاستيقان من قبيل كلمة المرور مشفرة بشكل ثابت أو ضعيفة أو مخزنة في شكل نص واضح، أو عندما تكون كلمة المرور أو رقم التعرف الشخصي (PIN) للاستيقان معروضة/معروضاً في شكل نص عادي (ما يعرف أيضاً باسم الهجوم القائم على اختلاس النظر من فوق كتف المستخدم (SSA))، أو عندما تُخترق معلومات الاستيقان بأي شكل آخر (من قبيل الهندسة الاجتماعية)، أو تُستخلص باستخدام طريقة تفتقر إلى العشوائية الكافية، فإن معلومات الاستيقان قد تكون مكشوفة للمهاجم أو يتمكن المهاجم من تخمينها نتيجة التعليق المفصل على سبب فشل العملية.
- ST-D-7: كلمة مرور ضعيفة: قد يحصل المهاجم على توليفة غير آمنة تنطوي مثلاً على كلمة مرور محددة افتراضياً، تمكن المهاجم من التظاهر بأنه مستعمل حقيقي.
- ST-D-8: مفتاح تجفير ضعيف/رقم عشوائي: مفتاح تجفير غير كاف أو رقم "عشوائي" يمكن التنبؤ به، كلها عناصر قد لا تكون قادرة على حماية البيانات الحرجة.
- ST-D-9: خوارزمية تجفير ضعيفة: يمكن أن يتنبأ المهاجم ببيانات المفتاح أو يكتشف النص العادي لرسالة مجفرة (نص مجفر) من خلال تحليل الحركة التي تستخدم خوارزمية تجفير ضعيفة.
- ST-D-10: عدم التحقق من المدخلات: يمكن أن يتسبب عدم التحقق من المدخلات في اختلال وظائف الجهاز.
- ST-D-11: كشف البيانات والتلاعب بها: قد تكون البيانات الحرجة مثل بيانات المستعمل وبيانات تشكيل الجهاز ومفتاح التجفير التي يتم إرسالها عبر جهاز أو تخزينها فيه مكشوفة للمهاجم فيتمكن من استغلالها أو التلاعب بها.
- ST-D-12: اختطاف دورة المستعمل: قد يتمكن المهاجم من النفاذ غير المرخص إلى حساب مستعمل حقيقي أغلقت دورته بطريقة غير طبيعية أو يستغل دورات صالحة لأجهزة متعددة تستخدم نفس مفتاح التجفير.
- ST-D-13: التحديث غير المأمون: عندما يكون ملف التحديث المقصود غير قابل للتنزيل، أو يكون ملف التحديث الذي تم التلاعب به ومصدره غير مصرح به/غير مستيقن قابلاً للتنفيذ.
- ST-D-14: فشل التحديث: قد يتسبب خطأ يحدث خلال التحديث في تشغيل غير طبيعي للجهاز.
- ST-D-15: خطأ في السلامة: قد يؤدي التلاعب غير المقصود بالشفرات أو قيم التشكيل القابلة للتنفيذ إلى اختلال في وظائف الجهاز.
- ST-D-16: المعدات/البرمجيات الضارة: شفرة ذات وظائف غير مقصودة يمكن استعمالها لغرض ضارة.
- ST-D-17: استغلال معلومات الذاكرة المتبقية: مفتاح التجفير وكلمة المرور والبيانات الحساسة المستخدمة في عمليات التجفير، وعمليات الاستيقان وإرسال البيانات، كلها بيانات تظل في الذاكرة ويمكن استغلالها.
- ST-D-18: تغيير غير مقصود في التشكيلات الحرجة: قد يتسبب عدم وجود ضوابط أمنية للجهاز في إجراء تغييرات غير مقصودة في التشكيلات الحرجة وعمليات غير مأمونة لتقديم الخدمة.
- ST-D-19: استجابة غير آمنة للخطأ: قد يتسبب عدم كشف الأخطاء على النحو المناسب والرد على الأخطاء والسلوك الضار للجهاز في عمليات غير مأمونة لتقديم الخدمة.
- ST-D-20: التطوير غير المأمون: قد تنشأ مواطن ضعف أمنية محتملة عن تصميم الجهاز وتنفيذه، وقد يكون تقييمها والتصدي لها خلال عملية الاختبار غير منفذيْن أو غير ملائميْن.
- ST-D-21: نظام تشغيل ضعيف: قد يتم تقويض وظائف الجهاز أو تجاوزها في بيئة نظام تشغيل ضعيف.

- ST-D-22: وحدات أو مكتبات ضعيفة لطرف ثالث: قد تؤدي وحدات أو مكتبات ضعيفة لطرف ثالث إلى تمكين المهاجم من نداء المعرضة منها للخطر.
- ST-D-23: تسجيل المعلومات الحساسة غير الآمن في سجل النظام: يمكن أن تكون المعلومات الحساسة المسجلة في سجل النظام مكشوفة للمهاجم فيتمكن استغلالها.
- ST-D-24: كشف المعلومات الحرجة من خلال تصحيح الأخطاء: يمكن أن تكون المعلومات الحساسة مكشوفة للمهاجم فيتمكن من استغلالها من خلال توليد السجلات وتصحيح الأخطاء عند إصدار الجهاز وتوزيعه.
- ST-D-25: النفاذ المادي غير المرخص: عندما يكون الجهاز معرضاً لنفاذ مادي غير مرخص وتغييرات غير مقصودة في تشكيلاته.
- ST-G-26: توصيلات الشبكة غير الآمنة: إن أجهزة إنترنت الأشياء الموصولة بشبكات غير آمنة يمكن أن تتعرض لهجمات، خاصة إذا كانت الشبكة تفتقر إلى تدابير التجفير والاستيقان المناسبة.

2.7 التهديدات الأمنية/مواطن الضعف التي تعاني منها بوابات إنترنت الأشياء

تشمل التهديدات/مواطن الضعف الخاصة بالبوابات ما يلي.

- ST-G-1: إرسال بيانات غير موثوقة: قد يتسبب إرسال بيانات غير موثوقة في اختلال وظائف الجهاز أو توزيع شفرة ضارة.
- ST-G-2: الحرمان من الخدمة (DoS) أو الحرمان من الخدمة الموزَّع: قد يتسبب الهجوم بالحرمان من الخدمة عبر فقدان الجهاز لقدرته على توفير الخدمة.
- ST-G-3: النفاذ غير المأذون إلى الأجهزة الموصولة: في الحالات التي تتسم فيها البوابة بأي قدرة تحكم في الأجهزة الموصولة، قد يتسبب النفاذ غير المأذون إلى البوابة في حدوث انتهاكات أمنية لجميع الأجهزة الموصولة.
- ST-G-4: التجفير الضعيف: الفشل في تجفير البيانات المرسَلة بين بوابات إنترنت الأشياء، مما يؤدي إلى احتمال التنصت أو اعتراض البيانات.
- ST-G-5: التلاعب المادي: يمكن للعبوات غير المؤمَّنة أو إجراءات الأمن المادية الضعيفة أن تسمح للمهاجمين بالتلاعب بعتاد البوابة، مما قد يؤدي إلى استخراج بيانات حساسة أو التلاعب بخواصها الوظيفية.

8 المتطلبات الأمنية

تحدد هذه التوصية المتطلبات الأمنية لأجهزة إنترنت الأشياء وبواباتها استناداً إلى الأبعاد الأمنية الخمسة المعرفة في القسم 6 وتُشكّل مجموعة من المتطلبات الأمنية بناءً على أحكام نموذج التهديدات والخصائص الوظيفية المحددة لإنترنت الأشياء وما إلى ذلك. وتستند القدرات الأمنية إلى التوصية [ITU-T X.1361]، على النحو المناقش في التذييل II.

1.8 الاستيقان

يتضمن بُعد الاستيقان استيقان المستعمل، والاستخدام الآمن لبيانات اعتماد الاستيقان، واستيقان الجهاز.

1.1.8 استيقان المستعمل

يجب ~~تغيير~~ توفير وظيفة لتغيير كلمة المرور المحدَّدة افتراضياً من المصنّع. (AU-1-1).

- يجب أن يقدم الجهاز وظيفة، مثل واجهة ويب، تسمح للمستعملين بتغيير ~~يجب إعداد~~ كلمة المرور للاستيقان بعدَ ~~عند~~ الاستيقان الأولي أو ~~عندما يُطلب تغييرها بعد الاستيقان الأولي. كلما كان التغيير مطلوباً.~~

- في حال كانت الإدارة عن بُعد مفعَّلة على الجهاز، يجب تغيير كلمة المرور المبدئية لحساب إدارة الجهاز قبل التهيئة على الشبكة.
- الوظيفة ينبغي أن تفرض قاعدةَ تملي اختلاف كلمة المرور الجديدة عن القيمة الأولية أو ست قِيَم سابقة. ~~التأكد من أن كلمة المرور تختلف عن القيمة الأولية أو السابقة.~~

يجب أولاً تحديد هوية المستعمل واستيقانه عند النفاذ إلى إدارة الأمن أو البيانات الحساسة (AU-1-2).

- عند النفاذ إلى إدارة الأمن، مثل إعداد جهاز لإنترنت الأشياء أو حساب مستعمل وامتياز له، يجب تحديد هوية المستعمل واستيقانه.
- تجري إدارة المستعملين الذين يتمتعون بنفاذ مميز إلى إدارة الأمن أو البيانات الحساسة بشكل منفصل عن المستعملين العاديين.
- ينبغي تنفيذ آلية آمنة لاستعادة كلمة المرور تتضمن خطوات الاستيقان لمنع النفاذ غير المخوَّل إلى استعادة الحساب.
- بالإضافة إلى كلمات المرور، ينبغي إضافة الاستيقان المتعدد العوامل لإضافة طبقة من الأمن. ويمكن تطبيق توليفة من العوامل مثل كلمات المرور أو القياسات البيومترية أو البطاقات الذكية أو كلمات المرور لمرة واحدة من أجل استيقان المستعمل.

يجب أن يكون عدد محاولات الاستيقان محدوداً (AU-1-3).

- قد يكون جهاز إنترنت الأشياء عرضة لهجمات شاملة إذا سُمح بمحاولات استيقان متكررة. لذلك، يجب أن يوفر الجهاز وظيفة للتصدي بشكل مناسب لمحاولات الاستيقان المستمرة
- يمكن توفير هذه الوظيفة باستخدام أحد الأساليب التالية:

أ) الحد من عدد محاولات الاستيقان لحظر الحساب أو إبطال وظيفة الاستيقان لمدة زمنية معينة (يوصى بحصر عدد محاولات الاستيقان في خمس محاولات أو أقل وإبطال وظيفة الاستيقان لمدة 5 دقائق على الأقل)؛

ب) يعتبر تجاوز العدد المحدد لمحاولات الاستيقان حركة غير مرخص بها للشبكة ويضاف المستعمل إلى قائمة الحظر التلقائي (يوصى بحصر عدد محاولات الاستيقان في 10 محاولات أو أقل)؛

ج) تطبيق اختبار تورينغ المؤتمت بالكامل للتمييز بين الحواسيب والبشر (CAPTCHA).

~~ينبغي~~ يجب أن تكون كلمة المرور الافتراضية المحدَّدة من المصنِّع أو كلمة المرور الموضوعة مسبقاً للجهاز فريدةً، وأن تُستحدث بطريقة عشوائية وأن تكون قويةً بدرجة كافية (AU-1-4).

ينبغي توفير وظيفة لإدارة حسابات المستعملين وامتيازاتهم (AU-1-5).

- ينبغي أن يكون من الممكن إدارة جميع حسابات المستعملين (بما في ذلك حساب المدير) المستخدمة في جهاز إنترنت الأشياء، مثلاً من أجل إضافتها أو إزالتها أو تخصيص امتيازات لها.
- في حالة استخدام نموذج قائم على الدور للتحكم في النفاذ، تحدَّد بشكل واضح امتيازات النفاذ لجميع وظائف جهاز إنترنت الأشياء وتخصَّص الامتيازات وفقاً لذلك.

ينبغي تطبيق مبدأ الحد الأدنى من الامتيازات على جميع حسابات المستعملين (AU-1-6).

- ينبغي تحصيص الامتيازات القائمة على الدور لجميع حسابات المستعملين.

ينبغي تقييد النفاذ المتزامن إلى حساب المدير (AU-1-7).

- ينبغي قصر النفاذ المتزامن لخدمات الإدارة على نفس حساب المدير، وتوفير وظيفة لقطع النفاذ السابق أو الحد من محاولات النفاذ الجديدة.

ينبغي توفير كلمة مرور آمنة من حيث الطول والدورة ودرجة التعقيد (AU-1-8).

– ينبغي أن توفر أجهزة إنترنت الأشياء وظيفة تمكن المستعمل من وضع كلمة مرور آمنة تأخذ في الاعتبار الطول والدورة ودرجة التعقيد.

في حال استيقان المستعمل باستعمال بروتوكول SSH، ينبغي أن يفرضَ الاستيقان استعمال مفاتيح البروتوكول SSH-keys. وينبغي تعطيل الاستيقان بكلمة المرور (AU-1-9).

2.1.8 الاستخدام الآمن لبيانات الاعتماد

ينبغي عدم استخدام بيانات اعتماد مشفرة بشكل ثابت (AU-2-1).

– ينبغي ألا تكون كلمة المرور (PIN، السر، إلخ.) مشفرة بشكل ثابت ولا مخزنة في شكل نص واضح.

أثناء الاستيقان بواسطة كلمة المرور، ينبغي أن تكون كلمة المرور مقنَّعة (AU-2-2).

– في حالة عرض كلمة المرور في شكل نص واضح فإنها قد تكون عرضة لهجمات SSA. ولذلك، تفادياً لهذا العرض عند إدخال كلمة المرور، ينبغي تقنيع رموز مكونات كلمة المرور باستخدام العلامات النجمية ("*").

ينبغي عدم تقديم أي تعليق محدد بشأن فشل عملية الاستيقان (AU-2-3).

3.1.8 استيقان الجهاز

يجب الحفاظ على معرِّف الهوية الفريد (UID) لكل جهاز من أجهزة العتاد. (AU-3-1). انظر الجدول 1.

– لكل جهاز من أجهزة إنترنت الأشياء معرف هوية فريد وثابت.

الجدول 1 – معرف الهوية الفريد لأجهزة إنترنت الأشياء

معرف الهوية	الوصف
عنوان التحكم في النفاذ إلى الوسائط (MAC)	معرف هوية فريد مخصص للسطح البيني لشبكة الاتصالات في طبقة وصلة البيانات لجزء الشبكة (48 بتة).
الهوية الدولية للمعدات المتنقلة (IMEI)، الرقم الدولي لاستيقان المطاريف المتنقلة	رقم فريد للهواتف الذكية. يخصصه المصنّع عند إصدار الهواتف الخلوية. يتألف من 15 رقماً في المجموع، بما في ذلك: شفرة الموافقة (ثمانية أرقام)؛ الرقم التسلسلي للنموذج (ستة أرقام)؛ رقم للتحقق (رقم واحد).

ينبغي استيقان الأجهزة بشكل متبادل قبل إرسال البيانات الحساسة أو الربط بين الأجهزة لأغراض التحكم (AU-3-2).

– فيما يلي أمثلة للاستيقان المتبادل:

أ) استخدام مفتاح خاص استناداً إلى طريقة تجفير المفاتيح العمومية؛

ب) استخدام النعوت الأمنية (معرِّف الهوية الفريد (UID)، المفتاح، إلخ.) والشرائح الأمنية؛

ج) تطبيق أمن طبقة النقل (TLS) (أو وحدات بيانات TLS) على بروتوكول الاتصالات الخفيف، مثلاً بروتوكول التطبيق المقيد (CoAP) أو بروتوكول الاتصالات الخفيفة من آلة إلى آلة (L2M2M)، أو نقل القياس عن بُعد لخدمة وضع الرسائل في قائمة انتظار (MQTT).

2.8 التجفير

– إذا كان من الصعب استخدام خوارزميات تجفير عامة بسبب محدودية الذاكرة وسعة التخزين، تُستخدم خوارزميات تجفير خفيفة.

– يجب استخدام خوارزميات تجفير للحماية من هجمات القنوات الجانبية.

يجب إدارة مفاتيح التجفير بشكل آمن طوال دورة حياتها بالكامل (CR-1-2).

– ينبغي توليد المفاتيح وتحديثها وتوزيعها واستخدامها وتخزينها وإتلافها بطريقة آمنة.

– وينبغي استعمال وظائف الاختزال الآمنة (مثل SHA-256) لأغراض التحقق من السلامة والاختزال.

ينبغي توليد رقم عشوائي في إطار خوارزمية ذات عشوائية مثبتة (CR-1-3).

3.8 أمن البيانات

يتكون بُعد أمن البيانات من حماية بيانات الإرسال وحماية البيانات الساكنة، والتحكم في تدفق المعلومات، والإدارة الآمنة للدورة، وحماية المعلومات المحددة لهوية الشخص (PII).

1.3.8 الإرسال والتخزين الآمنان

يجب أن تكون البيانات المرسَلة مجفرة (DS-1-1).

– يجب تجفير البيانات المرسَلة باستخدام خوارزمية تجفير آمنة (انظر CR-1-1).

ينبغي تطبيق أسلوب آمن عند إنشاء قناة بيانات أو تحكم (DS-1-2).

– عند إرسال البيانات، ينبغي استخدام بروتوكول أمني يكفل كتمان البيانات المرسلة وسلامتها، إلى جانب استيقان طرفي المصدر والمقصد.

– ينبغي إغفال هوية البيانات، عند الإمكان، لتقليل المخاطر المرتبطة بانكشاف البيانات.

يجب أن تكون البيانات المخزنة في الأجهزة مجفرة (DS-1-3).

– يجب تجفير أجهزة تخزين البيانات باستخدام خوارزمية تجفير آمنة (انظر CR-1-1).

ولا تُستعاد البيانات المحذوفة (DS-1-4).

– إذا كان من اللازم التخلص من جهاز أو تحديثه أو استبداله، يجب توفير قدرة حذف (الرجوع إلى الحالة الأولية المحددة من المصنّع) بحيث لا يمكن استعادة البيانات.

2.3.8 التحكم في تدفق المعلومات

ينبغي عدم السماح بحركة الشبكة غير المسموحة (DS-2-1).

يمكن لمراقبة النفاذ إلى البيانات وأنماط التدفق أن تساعد في كشف الحالات الشاذة والحوادث الأمنية المحتملة، مما يمكن من التدخل والاستجابة في الوقت المناسب (DS-2-2).

معالجة هجمات الحرمان من الخدمة أو الحرمان من الخدمة الموزَّع (DDoS) بواسطة بوابة إنترنت الأشياء (DS-2-3).

3.3.8 الإدارة الآمنة للدورة

ينبغي إنهاء الدورة بعد فترات توقف بدون استخدام (DS-3-1).

– في حالة النفاذ مجدداً بعد انتهاء الدورة، ينبغي إجراء الاستيقان مرة أخرى.

ينبغي أن تكون قيمة معرِّف هوية الدورة غير قابلة للتنبؤ (DS-3-2).

– ينبغي تطبيق خوارزمية أرقام عشوائية آمنة على توليد معرفات هوية الدورة.

– خلال الاستيقان في كل دورة، ينبغي تغيير معرف هوية الدورة وإتلاف معرفات هوية الدورة المستعملة.

ينبغي أن يبطل تنفيذُ آلية إبطال الدورة الدورات في الوقت الفعلي إذا اكتُشف نشاط مشبوه أو إذا طلب المستعمل تسجيل الخروج (DS-3-3).

– وهي تمكِّن من الاستجابة الفورية لحوادث الأمن أو إنهاء الدورة بمبادرة من المستعمل، مما يعزز التحكم في الدورات ذات النشاط المفرط.

4.3.8 إدارة المعلومات المحدِّدة لهوية الشخص (PII)

ينبغي إدارة المعلومات المحدِّدة لهوية الشخص (PII) بشكل آمن خلال دورة حياة المفتاح (DS-4-1)).

- ينبغي جمع المعلومات PII واستخدامها وتخزينها وإتلافها بطريقة آمنة.

4.8 أمن منصات الأجهزة

يشمل بُعد أمن منصات الأجهزة خمسة عناصر، هي: أمن البرمجيات (S/W)، والتحديث الآمن، وإدارة الأمن، والسجلات، والختم الزمني.

1.4.8 أمن البرمجيات

ينبغي تطبيق التشفير الآمن (PL-1-1).

- ينبغي تصميم البرمجيات وتنفيذها مع مراعاة الأمن.
- ويمكن إجراء مراجعات أمنية منتظمة واستعراضات للشفرات لتحديد مواطن الضعف في البرمجيات وتداركها.

يجب التحقق من مواطن الضعف الأمنية المعروفة وإزالتها (PL-1-2).

- في حالة تطوير البرمجية باستخدام بروتوكولات أو مكتبات، أو سطح بيني لبرمجة التطبيقات، أو رزم أو مصادر مفتوحة تنطوي على مواطن ضعف أمنية معروفة، فإن البرمجية الثابتة ونظام التشغيل قد ينطويان أيضاً على مواطن الضعف هذه.
- يجب استخدام الميدان العام لمواطن الضعف الأمنية المعروفة (مثلاً، [b-CVE]) للتحقق من مواطن الضعف الأمنية للجهاز وإزالتها.

ينبغي تطبيق التمويه (PL-1-3).

- يمكن تطبيق هذه المتطلبات غالباً على التطبيقات التي يتم تطويرها، مما يسهّل استعادة شفرة المصدر.
- نظراً لإمكانية استخدام أدوات الهندسة العكسية المفتوحة لاستخلاص معلومات منطقية أو أساسية مهمة، فإن الأمر يستحق مستوى مناسباً من الحماية.

ينبغي دعم وظيفة للتحقق من سلامة معلمات التشكيل والشفرات القابلة للتنفيذ (PL-1-4).

- لضمان صلاحية أجهزة إنترنت الأشياء، ينبغي التحقق من سلامة معلمات التشكيل والشفرات القابلة للتنفيذ في وقت التشغيل أو دورياً بأسلوب أوتوماتي أو يدوياً.

ويُضطلع باستجابة مناسبة في حالة حدوث خطأ في السلامة.

2.4.8 التحديث الآمن

يجب أن يضطلع بالتحديث مستعملون مرخصون (PL-2-1).

ينبغي دعم وظيفة التراجع في حالة فشل التحديث (PL-2-2).

ينبغي التحقق من السلامة والاستيقان قبل إجراء التحديث (PL-2-3).

- ينبغي الاستيقان من هوية المستعمل الذي يقوم بالتحديث، وينبغي إجراء عمليات تحقق من سلامة عنوان مخدم التحديث، وينبغي التحقق من كليهما مقابل ملف التحديث.
- يمكن تأكيد استيقان المستخدم من خلال إعادة الاستيقان من المستخدم قبل إجراء التحديث مباشرة.
- يمكن للمستخدم المخوَّل التحقق من سلامة عنوان مخدم التحديث عن طريق الفحص البصري.
- يمكن التحقق من سلامة ملفات التحديث والاستيقان منها عن طريق التحقق من توقيع رقمي مجفر.

3.4.8 إدارة الأمن

ينبغي تعطيل الخدمات غير الضرورية (PL-3-1).

- ينبغي تعطيل الخدمات غير الضرورية (Telnet، بروتوكول نقل الملفات (FTP)، التوصيل والتشغيل الشامل (UPnP)، البروتوكول البسيط لإدارة الشبكات (SNMP)، إلخ.) وتحديد الخدمات الضرورية التي يقدمها الجهاز.
- عندما تكون مثل هذه الخدمات ضروريةً، ينبغي أن تستخدمَ الخدمات بدائل آمنة، من قبيل بروتوكول SSH بدلاً من telnet، وSFTP بدلاً من FTP، وSNMPv3 بدلاً من SNMP.

ينبغي الاضطلاع بالإدارة عن بُعد في بيئة موثوقة (PL-3-2).

ينبغي تطبيق مكتبة طرف ثالث (PL-3-3).

- ينبغي أن تكون مكتبات ووحدات الطرف الثالث المستخدمة في التطوير أحدث نسخة وألا تعتريها أي مواطن ضعف أو عيوب أمنية معروفة.

ينبغي توفير اختبار ذاتي (PL-3-4).

- ينبغي توفير وظيفة اختبار ذاتي للكشف عن الأخطاء في المعدات والبرمجيات الرئيسية عند بدء تشغيل جهاز إنترنت الأشياء أو بعد بدء تشغيله.

4.4.8 السجلات

ينبغي توليد سجلات للأحداث المتعلقة بالأمن (PL-4-1).

- ينبغي تنفيذ السجلات، وينبغي أن يكون من الممكن كشف وتعقب أي محاولات نفاذ إلى السجلات والاستيقانات الناجحة وغير الناجحة والتغييرات في امتيازات المستعمل وأي سلوك غير طبيعي للجهاز.

ينبغي توفير آلية سجلات آمنة (PL-4-2).

- تفادياً لخسارة السجل وللتغييرات غير المرخصة (بما فيها الحذف)، ينبغي توفير آلية لحماية هذا السجل.
- ينبغي تخزين السجلات بشكل آمن وحمايتها من النفاذ غير المخوَّل أو العبث أو الحذف.

5.4.8 الختم الزمني

ينبغي توفير ختم زمني موثوق (PL-5-1).

5.8 الأمن المادي

يشمل بُعد الأمن المادي تأمين السطوح البينية وحماية أجهزة إنترنت الأشياء من العبث.

1.5.8 السطح البيني المادي الآمن

ينبغي إبطال وظائف أي سطح بيني خارجي غير ضروري (PH-1-1).

- ينبغي تحديد أبعاد ووظائف جميع السطوح البينية الخارجية (الشبكة المحلية، الناقل التسلسلي العام (USB)، منفذ البطاقة (SD) الرقمية الآمنة، إلخ.) المكشوفة للخارج.
- إذا لزم الأمر، ينبغي التحكم في النفاذ لمنع النفاذ غير المرخص.

يجب منع النفاذ غير المرخص إلى السطح البيني الداخلي (PH-1-2).

- يجب تحديد أبعاد ووظائف جميع السطوح البينية الداخلية (فريق عمل الاختبار المشترك (JTAG)، التصحيح السلكي التسلسلي (SWD)، المستقبِل/المرسِل العالمي غير المتزامن (UART)، إلخ.) المكشوفة للخارج.

- إذا لزم الأمر، يجب التحكم في النفاذ لمنع النفاذ غير المرخص.

وينبغي أن تكون الضوابط البيئية قائمة (PH-1-3).

- ينبغي تنفيذ ضوابط لحماية الأجهزة من العوامل البيئية مثل الحرارة والرطوبة والغبار.

2.5.8 المناعة ضد العبث

ينبغي دعم وظيفة لكشف التلاعب المادي غير المرخص والتصدي له (مثلاً، الأختام الكاشفة للعبث والأقفال والتصدي للعبث وبدالات ومنبهات التصفير) (PH-2-1).

الملحق A

جدول التقابل بين المتطلبات الأمنية والتهديدات/مواطن الضعف الأمنية لإنترنت الأشياء

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

ترد المتطلبات الأمنية لإنترنت الأشياء ووصفها في الفقرة 8، في حين تحدَّد تهديداتها/مواطن ضعفها الأمنية في الفقرة 7. ويبين الجدول 1.A التقابل بين المتطلبات الأمنية لإنترنت الأشياء وتهديداتها/مواطن ضعفها الأمنية.

الجدول 1.A – جدول التقابل بين المتطلبات الأمنية والتهديدات/مواطن الضعف الأمنية لإنترنت الأشياء

رقم المتطلب	بُعد المتطلب	وصف المتطلب	التهديدات/مواطن الضعف الأمنية
AU-1-1	الاستيقان	يجب توفير وظيفة لتغيير كلمة المرور المحدَّدة مبدئياً من المصنِّع. ~~يجب تغيير كلمة المرور المحددة افتراضياً من المصنِّع.~~	ST-D-6
AU-1-2	الاستيقان	يجب أولاً تحديد هوية المستعمل واستيقانه عند النفاذ إلى إدارة الأمن أو البيانات الحساسة.	ST-D-1
AU-1-3	الاستيقان	يجب أن يكون عدد محاولات الاستيقان محدوداً.	ST-D-4 ST-D-5
AU-1-4	الاستيقان	ينبغي أن تكون كلمة المرور الموضوعة مسبقاً للجهاز فريدة وأن تُستحدث بطريقة عشوائية وأن تكون قويةً بدرجة كافية.	ST-D-1
AU-1-5	الاستيقان	ينبغي توفير وظيفة لإدارة حسابات المستعملين وامتيازاتهم.	ST-D-3
AU-1-6	الاستيقان	ينبغي تطبيق مبدأ الحد الأدنى من الامتيازات على جميع حسابات المستعملين.	ST-D-3
AU-1-7	الاستيقان	ينبغي تقييد النفاذ المتزامن إلى حساب المدير.	ST-D-1
AU-1-8	الاستيقان	ينبغي توفير كلمة مرور آمنة من حيث الطول والدورة ودرجة التعقيد.	ST-D-7
AU-1-9	الاستيقان	ينبغي استخدام الاستيقان القائم على مفاتيح بروتوكول SSH-key في حال توافُر دعم للبروتوكول SSH	ST-D-4 ST-D-6 ST-D-7
AU-2-1	الاستيقان	ينبغي عدم استخدام بيانات اعتماد مشفرة بشكل ثابت.	ST-D-6
AU-2-2	الاستيقان	أثناء الاستيقان بواسطة كلمة المرور، ينبغي أن تكون كلمة المرور مقنَّعة.	ST-D-6
AU-2-3	الاستيقان	ينبغي عدم تقديم أي تعليق محدد بشأن فشل عملية الاستيقان.	ST-D-6
AU-3-1	الاستيقان	ينبغي الحفاظ على معرِّف الهوية الفريد (ID) لكل جهاز من أجهزة العتاد.	ST-D-2
AU-3-2	الاستيقان	ينبغي استيقان الأجهزة بشكل متبادل قبل إرسال البيانات الحساسة أو التحكم فيها قبل الربط فيما بينها.	ST-D-2
CR-1-1	التجفير	يجب استخدام خوارزميات تجفير آمنة عند إرسال البيانات أو تخزينها.	ST-D-8 ST-D-9
CR-1-2	التجفير	يجب إدارة مفاتيح التجفير بشكل آمن طوال دورة حياتها بالكامل.	ST-D-8
CR-1-3	التجفير	ينبغي توليد رقم عشوائي في إطار خوارزمية ذات عشوائية مثبتة.	ST-D-8

الجدول 1.A – جدول التقابل بين المتطلبات الأمنية والتهديدات/مواطن الضعف الأمنية لإنترنت الأشياء

رقم المتطلب	بُعد المتطلب	وصف المتطلب	التهديدات/مواطن الضعف الأمنية
DS-1-1	أمن البيانات	يجب أن تكون البيانات المرسَلة مجفرة.	ST-D-11
DS-1-2	أمن البيانات	ينبغي تطبيق أسلوب آمن عند إنشاء قناة بيانات أو تحكم.	ST-D-11
DS-1-3	أمن البيانات	يجب أن تكون البيانات المخزنة في الجهاز مجفرة.	ST-D-11
DS-1-4	أمن البيانات	لا تُستعاد البيانات المحذوفة.	ST-D-17
DS-2-1	أمن البيانات	ينبغي عدم السماح بحركة الشبكة غير المخوَّلة.	ST-G-1
DS-2-2	أمن البيانات	يمكن لمراقبة النفاذ إلى البيانات وأنماط التدفق أن تساعد في كشف الحالات الشاذة والحوادث الأمنية المحتملة، مما يمكن من التدخل والاستجابة في الوقت المناسب.	ST-G-1
DS-2-3	أمن البيانات	معالجة هجمات DoS أو DDoS بواسطة بوابة إنترنت الأشياء.	ST-G-2
DS-3-1	أمن البيانات	ينبغي إنهاء الدورة بعد فترات توقف بدون استخدام.	ST-D-12
DS-3-2	أمن البيانات	ينبغي أن تكون قيمة معرِّف هوية الدورة غير قابلة للتنبؤ.	ST-D-12
DS-3-3	أمن البيانات	ينبغي إبطال الدورة في الوقت الفعلي إذا اكتُشف نشاط مشبوه أو إذا طلب المستعمل تسجيل الخروج.	ST-D-12
DS-4-1	أمن البيانات	ينبغي إدارة المعلومات المحدِّدة لهوية الشخص (PII) بشكل آمن خلال دورة حياة المفتاح.	ST-D-11
PL-1-1	أمن منصات الأجهزة	ينبغي تطبيق التشفير الآمن.	ST-D-10 ST-D-20 ST-D-23 ST-D-24
PL-1-2	أمن منصات الأجهزة	يجب التحقق من مواطن الضعف الأمنية المعروفة وإزالتها.	ST-D-16 ST-D-21
PL-1-3	أمن منصات الأجهزة	ينبغي تطبيق التمويه.	ST-D-16
PL-1-4	أمن منصات الأجهزة	ينبغي دعم وظيفة للتحقق من سلامة معلمات التشكيل والشفرات القابلة للتنفيذ.	ST-D-15
PL-2-1	أمن منصات الأجهزة	يجب أن يضطلع بالتحديث مستعملون مرخصون.	ST-D-13
PL-2-2	أمن منصات الأجهزة	ينبغي دعم وظيفة التراجع في حالة فشل التحديث.	ST-D-14
PL-2-3	أمن منصات الأجهزة	ينبغي التحقق من السلامة والاستيقان قبل إجراء التحديث.	ST-D-15
PL-3-1	أمن منصات الأجهزة	ينبغي تعطيل الخدمات غير الضرورية.	ST-D-16
PL-3-2	أمن منصات الأجهزة	ينبغي الاضطلاع بالإدارة عن بُعد في بيئة موثوقة.	ST-D-18
PL-3-3	أمن منصات الأجهزة	ينبغي تطبيق مكتبة طرف ثالث.	ST-D-22
PL-3-4	أمن منصات الأجهزة	ينبغي توفير اختبار ذاتي.	ST-D-19
PL-4-1	أمن منصات الأجهزة	ينبغي توليد سجلات للأحداث المتعلقة بالأمن.	ST-D-23
PL-4-2	أمن منصات الأجهزة	ينبغي توفير آلية سجلات آمنة.	ST-D-23
PL-5-1	أمن منصات الأجهزة	ينبغي توفير ختم زمني موثوق.	ST-D-18
PH-1-1	الأمن المادي	ينبغي إبطال وظائف أي سطح بيني خارجي غير ضروري.	ST-D-24 ST-D-25

الجدول 1.A – جدول التقابل بين المتطلبات الأمنية والتهديدات/مواطن الضعف الأمنية لإنترنت الأشياء

رقم المتطلب	بُعد المتطلب	وصف المتطلب	التهديدات/مواطن الضعف الأمنية
PH-1-2	الأمن المادي	يجب منع النفاذ غير المرخص إلى السطح البيني الداخلي.	ST-D-24 ST-D-25
PH-1-3	الأمن المادي	ينبغي وجود ضوابط بيئية.	ST-D-24 ST-D-25
PH-2-1	الأمن المادي	ينبغي دعم وظيفة لكشف التلاعب المادي غير المرخص والتصدي له (مثلاً، الأختام الكاشفة للعبث والأقفال والتصدي للعبث وبدالات ومنبهات التصفير).	ST-D-24 ST-D-25

التذييل I

القدرات الأمنية لإنترنت الأشياء

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

1.I لمحة عامة

لا تتناول هذه التوصية سوى المتطلبات الأمنية، وهي تراعي موثوقية الخدمات وجودتها. وقد تم تفصيل القدرات الأمنية لإنترنت الأشياء انطلاقاً من القدرات المبينة في التوصية [ITU-T X.1361]. وينبغي أن تشمل معمارية إنترنت الأشياء القدرات العامة المدرجة في الجدول 1.I.

الجدول 1.I – جدول التقابل بين المتطلبات الأمنية والقدرات الأمنية

القدرات	المتطلبات ذات الصلة
قدرة اتصالات آمنة لدعم الاتصالات الآمنة والموثوقة والمحمية الخصوصية	DP-1-1، DS-1-2
قدرة آمنة لإدارة المفاتيح لدعم الاتصالات الآمنة	CR-2-1
قدرة إدارة آمنة للبيانات لتوفير إدارة بيانات آمنة وموثوق بها ومحمية الخصوصية للبيانات	DS-2-1، DS-1-4
قدرة استيقان من أجل الاستيقان من الأجهزة	AU-1-1، AU-1-2، AU-1-3، AU-1-4، AU-1-8، AU-1-9
قدرة تخويل (مراقبة النفاذ) لتخويل الأجهزة	AU-3-1، AU-3-2
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	PL-4-1، PL-4-2
قدرة آمنة لتوفير الخدمة من أجل تقديم خدمة آمنة وموثوق بها ومحمية الخصوصية	DS-4-1، DS-3-2
قدرة تكامل آمنة من أجل دمج مختلف السياسات والتقنيات الأمنية المتعلقة بالمكونات الوظيفية المتنوعة لإنترنت الأشياء	–
قدرة لتنفيذ البروتوكولات الآمنة التي تستعمل خوارزميات تجفير مقيسه ومتاحة لعامة الجمهور	CR-1-1
قدرة لتنفيذ البروتوكولات الآمنة استناداً إلى تجفير خفيف	CR-1-1
قدرة آمنة ومتينة لتحديث البرمجيات من أجل تحديث الوحدات النمطية للبرمجيات أو تطبيقاتها	PL-2-1، PL-2-2، PL-2-3
قدرة لإدارة الهوية من أجل أجهزة/أدوات استشعار إنترنت الأشياء والبوابات والمنصات/الخدمات	AU-2-1، AU-2-2، AU-2-3، DS-3-2، DS-4-1
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	PL-4-1، PL-4-2
قدرة أمنية قائمة على العتاد (مثل وحدة نمطية لمنصة موثوقة) لمنع حدوث المخاطر الأمنية المادية المصاحبة للتمثيل الافتراضي للشبكة والبوابة	PH-1-1، PH-1-2، PH-2-1
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	DS-4-1
قدرة إمكانية تشكيل آمنة	–
قدرة استعمال تجفير خفيف	CR-1-1
قدرة تجفير بسيط بإجراء التجفير ببيانات قناع مصاحب (EAMD) [b-ITU-T X.1362] للاتصال بالكيانات الأخرى بما في ذلك البوابة	–

وينبغي أن تشمل معمارية إنترنت الأشياء القدرات المتعلقة بخوارزمية التجفير المدرجة في الجدول 2.I.

الجدول 2.I – جدول التقابل بين المتطلبات الأمنية والقدرات الأمنية المتعلقة بخوارزمية التجفير

القدرات	المتطلبات ذات الصلة
قدرة لإنتاج عدد عشوائي بجودة تجفيرية لدعم إدارة المفاتيح [b-IETF RFC 4086]	CR-3-1
قدرة للتحديث الدوري لمفاتيح التجفير الضرورية لتدفقات الإذاعة	–
قدرة لاستعمال خوارزميات التجفير المقيسة	CR-1-1

الجدول 3.I – جدول التقابل بين المتطلبات الأمنية والقدرات الأمنية المتعلقة بالسياق

القدرات	المتطلبات ذات الصلة
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	PL-1-1، PL-1-3، PL-1-4
قدرة لإجراء تقييم مخاطر مخطط له لتحديد المخاطر التي تواجهها السياقات التشغيلية	PL-1-4

2.I القدرات الأمنية لأدوات الاستشعار/الأجهزة

ينبغي أن تشمل أدوات الاستشعار/الأجهزة لإنترنت الأشياء القدرات الأمنية المدرجة في الجدول 4.I.

الجدول 4.I – جدول التقابل بين المتطلبات الأمنية والقدرات الأمنية لأدوات الاستشعار/الأجهزة لإنترنت الأشياء

القدرات	المتطلبات ذات الصلة
قدرة لإدارة المفاتيح	CR-2-1
قدرة تفاوض لخوارزمية التجفير	CR-1-1
قدرة لتجفير البيانات وفي بعض الحالات بيانات مستوي التشوير والتحكم والإدارة من أجل التخفيف من حدة الشواغل الأمنية بشأن كتمان البيانات المرسلة عبر الشبكات اللاسلكية	CR-1-1، DS-1-1، DS-1-2
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	CR-1-1، DS-1-1، DS-1-2، PL-2-3
قدرة للاستيقان من منشأ البيانات أو هويات أدوات استشعار/أجهزة إنترنت الأشياء وهويات الإداريين وموظفي صيانة شبكات الاستشعار	AU-1-2، AU-1-6، PL-2-1
قدرة لإدارة البرمجيات التصحيحية، بما في ذلك تحديث وترقية الوحدات النمطية للبرمجيات الآمنة	PL-2-1، PL-2-2، PL-2-3
قدرة لتنفيذ بروتوكولات آمنة قائمة على تجفير خفيف	CR-1-1
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	AU-1-2، AU-3-1، AU-3-2
قدرة لكشف العبث أو منعه	PH-2-1
قدرة لإنتاج أرقام عشوائية بجودة تجفيرية لدعم إدارة المفاتيح	CR-3-1
قدرة لمقاومة هجمات القنوات الجانبية	–
قدرة للكشف عن البرامج الضارة والحماية منها	–
قدرة لحماية المعلومات المحددة لهوية الشخص من التسرب	DS-4-1

وينبغي أن تشمل أجهزة إنترنت الأشياء القدرات الأمنية المدرجة في الجدول 5.I.

الجدول I.5 – جدول التقابل بين المتطلبات الأمنية والقدرات الأمنية لأجهزة إنترنت الأشياء

القدرات	المتطلبات ذات الصلة
قدرة للتحقق من استيقان وسلامة البرمجيات المثبتة على الأجهزة باستعمال التوقيعات الرقمية المولدة تجفيرياً [b-ISO/IEC 9796-3]	PL-1-4
قدرة جدار حماية أو كشف الاقتحام أو الحماية من الاقتحام أو القدرة على الفحص العميق للرزم لمراقبة الحركة المقصود إنهاؤها في جهاز ما	DS-2-1
قدرة لإجراء تشكيلات آمنة	PL-1-4

I.3 القدرات الأمنية للبوابات

ينبغي أن تشمل المنصات/الأجهزة القدرات الأمنية المدرجة في الجدول I.6.

الجدول I.6 – جدول التقابل بين المتطلبات الأمنية والقدرات الأمنية للبوابات

القدرات	المتطلبات ذات الصلة
قدرة نظام للكشف عن الاقتحام (IDS)/نظام لمنع الاقتحام (IPS)	DS-2-1
قدرة لإدارة المفاتيح	CR-2-1
قدرة لإجراء تشكيلات آمنة	PL-1-4
قدرة تفاوض لخوارزمية التجفير	CR1-1
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 كتمان البيانات المرسلة عبر الشبكات اللاسلكية	CR-1-1، DS-1-1، DS-1-2
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	CR-1-1، DS-1-1، DS-1-2، PL-2-3
قدرة تيسير للتعامل مع هجمات الحرمان من 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	PL-1-1، DS-2-2
قدرة للاستيقان من منشأ البيانات أو هويات أدوات استشعار/أجهزة إنترنت الأشياء وهويات الإداريين وموظفي صيانة شبكات الاستشعار	AU-1-2، AU-1-6، PL 2-1
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	AU-1-2، AU-3-1، AU-3-2
قدرة مساءلة لأجهزة إنترنت الأشياء لضمان إمكانية تتبع الجهاز المسؤول عن أي انتهاك للسياسة الأمنية	PL-4-1
قدرة لتحديث الوحدات النمطية للبرمجيات الآمنة	PL-2-1، PL-2-2، PL-2-3

I.4 القدرات الأمنية للشبكة

وفقاً للتوصية [b-ITU-T X.805]، ينبغي أن تشمل الشبكة القدرات الأمنية المدرجة في الجدول I.7.

الجدول I.7 – جدول التقابل بين المتطلبات الأمنية والقدرات الأمنية للشبكة

البنود	القدرات	المتطلبات ذات الصلة
C_NT.1 [b-ITU-T X.805]	يضمن بعد أمن الاتصالات تدفق المعلومات حصراً بين النقاط الطرفية المخولة (لا يتم تحويل أو اعتراض المعلومات عند تدفقها بين هذه النقاط الطرفية).	PL-3-1

I.5 القدرات الأمنية للمنصات/الخدمات

ينبغي أن تشمل المنصات/الخدمات القدرات الأمنية المدرجة في الجدول I.8.

الجدول 8.I – جدول التقابل بين المتطلبات الأمنية والقدرات الأمنية للمنصات/الخدمات

القدرات	المتطلبات ذات الصلة
قدرة لحماية بيانات الاعتماد لأغراض عمليات التجفير، وهي مجموعة من البيانات المقدمة كدليل للهوية و/أو المستحقات المدعاة	DS-2-1
قدرة لتغيير أسماء المستعملين وكلمات المرور الافتراضية أثناء الإعداد الأولي	AU-1-1، AU-1-2
قدرة لتنفيذ كلمات مرور قوية وسياسة دقيقة للتحكم في النفاذ	AU-1-4، AU-1-6
قدرة لإلغاء تيسر المنافذ غير الضرورية	PL-3-1، PH-1-1، PH-1-2
قدرة لدعم التشكيل الآمن لإزالة الخدمات والبرمجيات غير الضرورية مثلاً	AU-1-5، PL-3-1
قدرة للحماية من الإصابة بالبرمجيات الضارة من خلال استعمال برمجيات الحماية من البرمجيات الضارة	PL-3-4
قدرة لتنفيذ سياسات إدارة البرمجيات التصحيحية	PL-2-1، PL-2-2، PL-2-3
قدرة لإدارة مواطن الضعف	PL-1-1، PL-1-2
قدرة لتحديث الوحدات النمطية للبرمجيات الآمنة وتطبيقاتها	PL-2-1، PL-2-3
قدرة لإدارة المفاتيح لأغراض النقل الآمن للرسائل بين بوابة ومنصة/خدمة	CR-1-2
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 الحرمان من الخدمة	AU-1-5، DS-1-1، DS-1-2
قدرة لمراقبة الشبكة	–
قدرة لحماية المعلومات المحدِّدة لهوية شخص أثناء السكون	DS-4-1
قدرة لأمن مستوى التطبيقات لمنع التهديدات والهجمات على مستوى التطبيقات، على النحو المبين في الفقرة 4.8 من التوصية [ITU-T X.1361]	–
قدرة لتقديم الدعم للتخفيف من حدة هجمات التخمين	–

التذييل II

حالات استعمال لتطبيق المتطلبات الأمنية لأجهزة إنترنت الأشياء وبواباتها

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

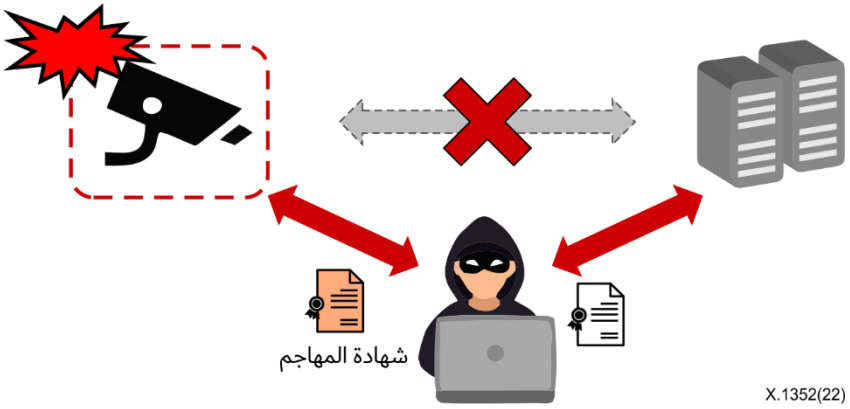
ينطوي العديد من أجهزة إنترنت الأشياء على ثغرات ومواطن ضعف أمنية فيما يتعلق بالاستيقان والتجفير وحماية البيانات. وعلاوة على ذلك، فإن معظم هذه الأجهزة عرضة للسطوح البينية المادية ومنصات تطوير الأجهزة. ويصف هذا التذييل حالات تطوير الأمن فيما يتعلق بالمتطلبات المقترحة.

1.II حالة استعمال للاستيقان – إمكانية التعرض لهجوم الاعتراض الوسيط (MITM)

ينطوي إجراء الاستيقان بين المخدّم وكاميرا الشبكة على موطن ضعف. ولا ترفض كاميرا الشبكة الشهادات غير الصالحة عند تأكيد أمن طبقة النقل (TLS). وبالتالي، يسرق المهاجم مفتاحاً مهماً. انظر الشكل 1.II.

تشمل التدابير المضادة ما يلي:

- رفض شهادة طبقة المقبس الآمن غير الصالحة؛
- استخدام تثبيت المفاتيح العمومية لبروتوكول نقل النصوص الترابطية (HTTP)؛



الشكل 1.II – حالة استعمال للاستيقان

2.II حالة استعمال لميدان التجفير – خوارزمية التجفير الضعيفة

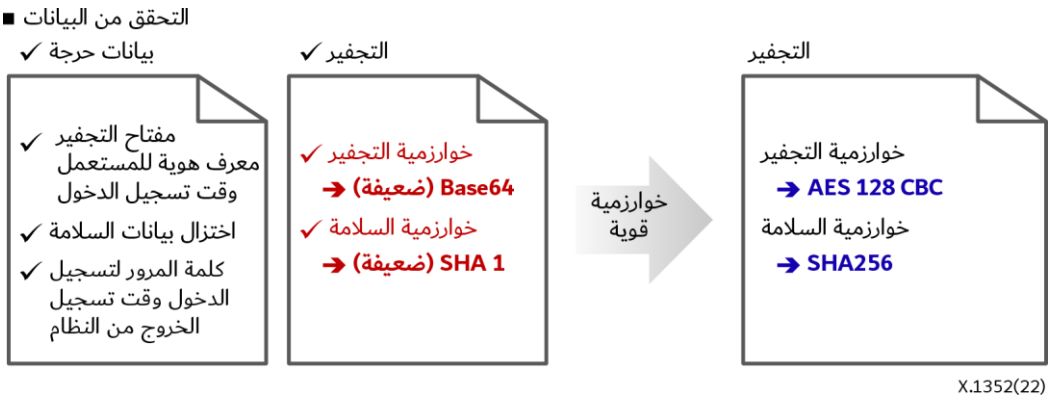
انظر الشكل 2.II.

تشمل مواطن الضعف ما يلي:

- خوارزمية تجفير ضعيفة: Base64؛
- منهجية التحقق من البيانات: خوارزمية اختزال مأمونة 1 (SHA1).

وتشمل التدابير المضادة ما يلي:

- قوة أمنية أشد من قوة خوارزمية تجفير بطول 128 بتة (انظر المعيار [b-ISO/IEC 19790])؛
- منهجية التحقق من البيانات: SHA256 [b-ISO/IEC 10118-3].



الشكل 2.II – حالة استعمال لميدان التجفير

3.II حالة استعمال لميدان أمن البيانات والتجفير – التحقق الضعيف من سلامة إرسال البيانات

انظر الشكل 3.II.

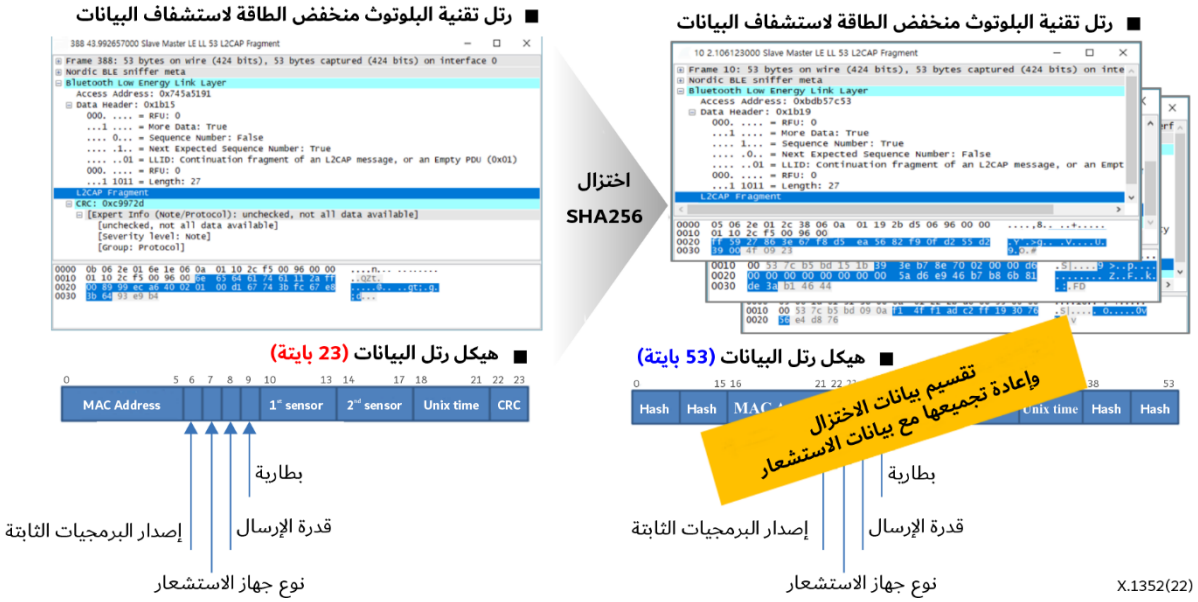
يكمن موطن الضعف في ما يلي:

– التحقق الضعيف من سلامة إرسال البيانات (منهجية التحقق من سلامة البيانات: التحقق من الإطناب الدوري)

وتشمل التدابير المضادة ما يلي:

– منهجية التحقق من البيانات: بيانات الاختزال SHA256 [b-ISO/IEC 10118-3]؛

– إعادة تجميع إجمالي تقسيمات البيانات وأرتالها.



الشكل 3.II – حالة استعمال لميدان أمن البيانات والتجفير

4.II حالة استعمال لميدان أمن منصات الأجهزة – التشفير الضعيف أمام الاستغلال

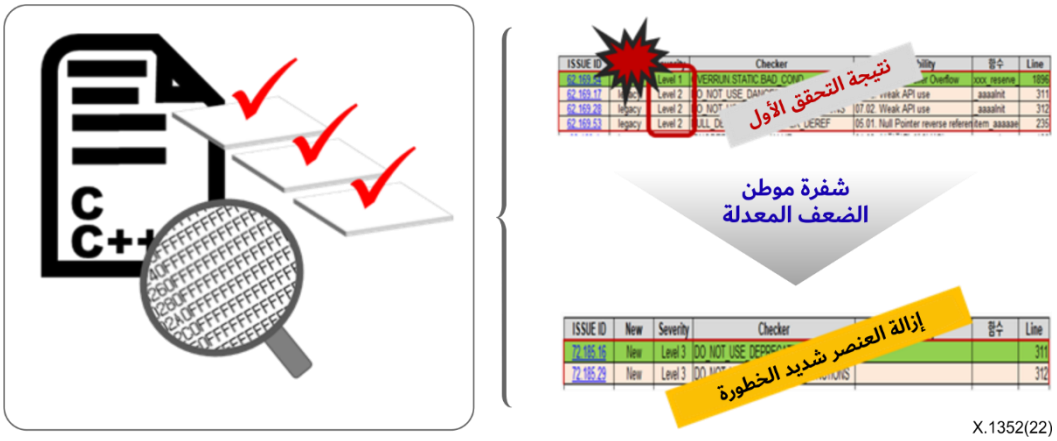
انظر الشكل 4.II.

يكمن موطن الضعف في ما يلي:

– فيض الذاكرة المؤقتة وضعف السطح البيني لبرمجة التطبيقات.

التدبير المضاد هو:

– التحقق من التشفير الآمن واقتراح إزالة الشفرات الضعيفة باستخدام أدوات التحليل الساكن.



الشكل 4.II – حالة استعمال لميدان أمن منصات الأجهزة

5.II حالة استعمال لميدان الأمن المادي – موطن ضعف في لوحة دارة مطبوعة لسطح بيني داخلي

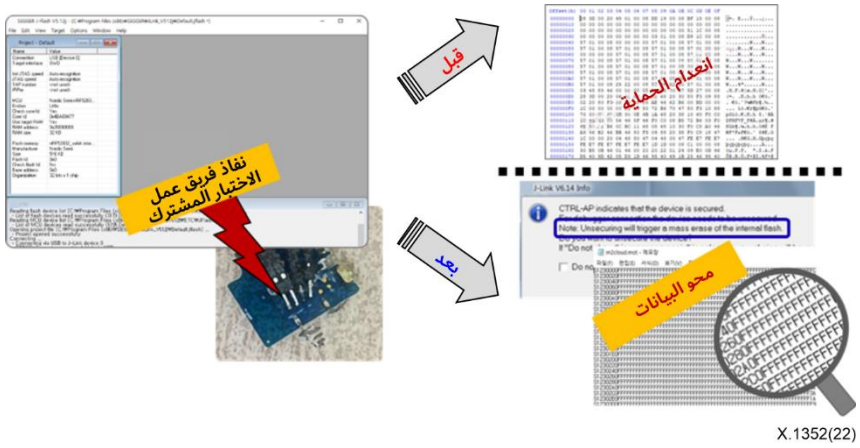
انظر الشكل 5.II.

يكمن موطن الضعف في ما يلي:

– منفذ فريق عمل الاختبار المشترك (JTAG) متاح في منتج واسع النطاق.

التدبير المضاد هو:

– تمكين حماية النفاذ إلى الذاكرة في وحدة التحكم الصغرية (MCU).



الشكل 5.II – حالة استعمال لميدان الأمن المادي

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-ITU-T X.1252] Recommendation ITU-T X.1252 (2021), *Baseline identity management terms and definitions*.

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2020), *Entity authentication assurance framework.*

[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-ISO 16100-1] ISO 16100-1:2009, *Industrial automation systems and integration – Manufacturing software capability profiling for interoperability – Part 1: Framework.*

[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 10118-3] ISO/IEC 10118-3 (2018), *IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions.*

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

[b-IETF RFC 4086] IETF RFC 4086 (2005), *Randomness requirements for security*.

[b-CVE] Mitre Corporation (Internet). *Common vulnerabilities and exposures*. Bedford, MA: Mitre Corporation. Available [viewed 2022-10-29] at: https://cve.mitre.org/

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، 2024