الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1368

(2021/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

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

التحديث الآمن للبرامج الثابتة أو البرمجيات في أجهزة إنترنت الأشياء (IoT)

التوصية ITU-T X.1368

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.600–X.699
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
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
مولّد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
أمن شبكات الجيل الخامس	X.1800–X.1819

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

التوصية ITU-T X.1368

التحديث الآمن للبرامج الثابتة أو البرمجيات في أجهزة إنترنت الأشياء (IoT)

ملخص

تحدد هذه التوصية: 1) النماذج والإجراءات الأساسية للتحديث الآمن للبرامج الثابتة أو البرمجيات (FW/SW) في أجهزة إنترنت الأشياء (IoT)؛ و2) المتطلبات والقدرات اللازمة من أجل تحديث البرامج الثابتة لإنترنت الأشياء.

وتحدد التوصية إجراءً عاماً للتحديث الآمن مع متطلبات عامة. ويسمح هذا الإجراء بالتنفيذ الآمن للتحديثات العامة للبرامج الثابتة/البرمجيات فيما بين أصحاب المصلحة في بيئة إنترنت الأشياء، مثل مطوري أجهزة إنترنت الأشياء ومقدمي أنظمة/خدمات إنترنت الأشياء.

وتركز هذه التوصية على تحديث البرامج الثابتة، ولكنها تنطبق على تحديث أي برمجيات أخرى لأجهزة إنترنت الأشياء.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X1368	2021-01-07	17	11.1002/1000/14445

مصطلحات أساسية

إنترنت الأشياء (IoT)؛ الأمن؛ تحديث برمجيات.

* للنفاذ إلى توصية، ترجى 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 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 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/.

© ITU 2021

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

1 مجال التطبيق 1
2 المراجع 1
3 التعاريف 1
1.3 مصطلحات معرَّفة في مصادر أخرى 1
2.3 المصطلحات المعرَّفة في هذه التوصية 1
4 المختصرات والأسماء المختصرة 2
5 اصطلاحات 2
6 النموذج الأساسي 2
7 إجراءات التحديث 2
8 سيناريوهات النشر 3
1.8 الكيانات الوظيفية داخل أجهزة إنترنت الأشياء 3
2.8 أنماط نشر متتبع الحالة 4
9 اكتشاف صور البرامج الثابتة الجديدة المتاحة وبدء الإجراء 6
10 المتطلبات 6
11 القدرات 7
1.11 قدرات مستهلك البرامج الثابتة 7
2.11 قدرات متتبع الحالة 7
3.11 قدرات مخدِّم البرامج الثابتة 8
4.11 قدرات المؤلف 8
التذييل I – الأنشطة ذات الصلة خارج قطاع تقييس الاتصالات 9
التذييل II – مثال سيناريو لتحديث برمجيات إنترنت الأشياء باستخدام تكنولوجيا سجل الحسابات الموزَّع 10
1.II نظرة عامة 10
2.II إجراء تحديث البرمجيات 10
بيبليوغرافيا 12

مقدمة

تزداد الهجمات السيبرانية ضد أجهزة أو أنظمة إنترنت الأشياء (IoT) تعقيداً وذكاءً وتنوعاً. وفي السابق، أصلح باعة أجهزة إنترنت الأشياء وظائف معظم هذه الأجهزة في مرحلة الإصدار الأولي. ولكن الأجهزة في الآونة الأخيرة توصَّل بالإنترنت لتقديم مجموعة محسّنة من خدمات إنترنت الأشياء. لذلك، تواجه أجهزة إنترنت الأشياء المستخدَمة تهديدات/هجمات سيبرانية. وتدعو الحاجة إلى إدراك أن البرامج الثابتة أو البرمجيات (FW/SW) المطبقة في أجهزة إنترنت الأشياء تحتاج إلى تحديث آمن لسد الثغرات الأمنية وتلافي نقاط الضعف فيها. وبدأ بعض باعة الأجهزة بالفعل في تقديم خدمة تحديث البرامج الثابتة من خلال برامجهم الخاصة.

وتقدم هذه التوصية نماذج وإجراءات أساسية للتحديث الآمن للبرمجيات/البرامج الثابتة (SW/FW) في إنترنت الأشياء، فضلاً عن المتطلبات والقدرات المرتبطة بها. وبالنماذج الأساسية وإجراء التحديث المشترَك، يمكن تبادل البرمجيات/البرامج الثابتة في إنترنت الأشياء (IoT SW/FW) بشكل آمن بين أصحاب المصلحة في بيئة إنترنت الأشياء مع تشجيع أصحاب المصلحة على تحديث القديم من هذه البرمجيات/البرامج الثابتة.

التحديث الآمن للبرامج الثابتة أو البرمجيات في أجهزة إنترنت الأشياء (IoT)

1 مجال التطبيق

تحدد هذه التوصية النماذج والإجراءات الأساسية للتحديث الآمن للبرامج الثابتة أو البرمجيات (FW/SW) في أجهزة إنترنت الأشياء. وهي تصف أيضاً متطلبات وقدرات عمليات تحديث البرامج الثابتة أو البرمجيات في أجهزة إنترنت الأشياء (IoT FW/SW). وتركز هذه التوصية على تحديث البرامج الثابتة، ولكنها تنطبق على تحديث أي برمجيات أخرى لأجهزة إنترنت الأشياء.

2 المراجع

لا توجد.

3 التعاريف

1.3 مصطلحات معرَّفة في مصادر أخرى

لا توجد.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 المؤلف (author): كيان ينتج صور البرامج الثابتة (FW) والبرمجيات لأجهزة إنترنت الأشياء. وتشمل الأمثلة عليه فرداً أو مجموعة، مثل شركة أو أي نوع آخر من المنظمات. ويمكنه تحميل الصورة إلى واحد أو أكثر من مخدمات البرامج الثابتة التي لا يلزم أن تكون موثوقاً بها بالضرورة.

2.2.3 مستهلك البرامج الثابتة (firmware consumer): كيان يقوم بتخزين صور البرامج الثابتة (FW) على جهاز إنترنت الأشياء (IoT) والتحقق منها وتشغيلها. وينبغي أن يبت في تشغيل صور البرامج الثابتة الحالية. ويحتوي جهاز إنترنت الأشياء على واحد أو أكثر من مستهلكي البرامج الثابتة.

3.2.3 مخدِّم البرامج الثابتة (firmware server): كيان يوزع صور البرامج الثابتة (FW). ويمكن أن يقبل صور البرامج الثابتة من مؤلفين متعددين؛ ويمكن أن يكون مستودعاً لمورّد معين أو مستودعاً يقبل موردين متنوعين. ومن الناحية المثالية، يكون مخدِّم البرامج الثابتة موثوقاً به، ولكن يمكن أن يكون غير موثوق به؛ ويمكنه أن يسعى إلى مشاهدة أو تعديل حزم البرامج الثابتة المستلمة من المؤلفين.

4.2.3 الكشف (manifest): سجل يحتوي على بيانات شرحية لصورة البرامج الثابتة.

5.2.3 متتبع الحالة (status tracker): كيان يقوم بالتحقق من حالة صور البرامج الثابتة (FW) ويتعقبها داخل واحد أو أكثر من مستهلكي البرامج الثابتة ويبادر بتحديثات البرامج الثابتة حسب الحاجة. ويتضمن ذلك مراقبة دقيقة للتغييرات في الجهاز، من قبيل نسخة صور البرامج الثابتة قيد التشغيل وحالة دورة تحديث البرامج الثابتة التي يمر فيها الجهاز حالياً. ويمكن أن يقع متتبع الحالة داخل جهاز إنترنت الأشياء، أو على الشبكة الداخلية، أو على شبكة الإنترنت.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

DLT تكنولوجيا سجل الحسابات الموزَّع *(Distributed Ledger Technology)*

FW البرامج الثابتة *(Firmware)*

IoT إنترنت الأشياء *(Internet of Things)*

SW البرمجيات *(Software)*

URL محدِّد موقع الموارد الموحَّد *(Uniform Resource Locator)*

5 اصطلاحات

تتبع هذه التوصية الاصطلاحات التالية التي تتماشى مع المرجع [b-IETF RFC 2119].

"يجب" هذه الكلمة معناها أن التعريف يُلزم إلزاماً مطلقاً في التوصيف.

"يجب ألا" هذه العبارة تعني أن التعريف يحظر حظراً مطلقاً في التوصيف.

"ينبغي" تعني هذه الكلمة أنه قد تكون هناك أسباب وجيهة في ظروف معينة يتم فيها التغاضي عن هذا العنصر، غير أنه ينبغي إدراك التبعات كافة وتقييم الحالة بعناية قبل اللجوء إلى مسلك مختلف.

"ينبغي ألا" تعني هذه العبارة أنه قد تكون هناك أسباب وجيهة في ظروف معينة عندما يكون السلوك الوارد مقبولاً أو حتى مفيداً، غير أنه ينبغي إدراك التبعات كافة وتقييم الحالة بعناية قبل تنفيذ أي سلوك موصوف بهذا الاسم.

"يمكن" تعني هذه الكلمة أن هذا العنصر اختياري بالفعل. فمثلاً قد يختار مورّد إدراج العنصر لأنه مطلوب في سوق معينة أو لأن المورّد يرى أنه يعزز المنتج؛ فيما يمكن لمورّد آخر إغفاله.

6 النموذج الأساسي

يمكن أن تختلف معمارية التوصيل الشبكي لأجهزة إنترنت الأشياء، ولكن ينبغي استخدام أربعة كيانات وظيفية في جميع الحالات، أي مستهلك البرامج الثابتة (انظر الفقرة 2.2.3)، ومتتبع الحالة (انظر الفقرة 5.2.3)، والمؤلف (انظر الفقرة 1.2.3)، ومخدِّم البرامج الثابتة (انظر الفقرة 3.2.3). علماً بأنه يمكن وجود كيانات وظيفية متعددة داخل العقدة الواحدة. فعلى سبيل المثال، يحتوي جهاز كاميرا الويب على مستهلكي برامج ثابتة متعددين ومتعقب واحد للحالة، بينما يحتوي مخدِّم الويب على متتبع حالة واحد ومخدِّم للبرامج الثابتة. وقد يوجد العديد من مستهلكي البرامج الثابتة داخل شبكة واحدة وتتم مراقبتهم بمتتبع حالة ينفذ داخل البوابة. ويمكن أن تختلف هذه التصاميم حسب درجة القيود المفروضة على أجهزة إنترنت الأشياء. ويرد وصف نماذج النشر النمطية في الفقرة 8.

وفي النموذج الأساسي، تؤدي هذه الكيانات أدواراً لا غنى عنها في تحديث البرمجيات/البرامج الثابتة في إنترنت الأشياء (IoT SW/FW). والسيناريو الأساسي في هذا النموذج بسيط: *إذ يقوم متتبع الحالة الذي يلمس الحاجة إلى تحديث IoT SW/FW ببدء إجراء تحديث SW/FW يسمح لمستهلكي البرامج الثابتة باستلام صورة SW/FW من مؤلف عبر مخدِّم البرامج الثابتة.*

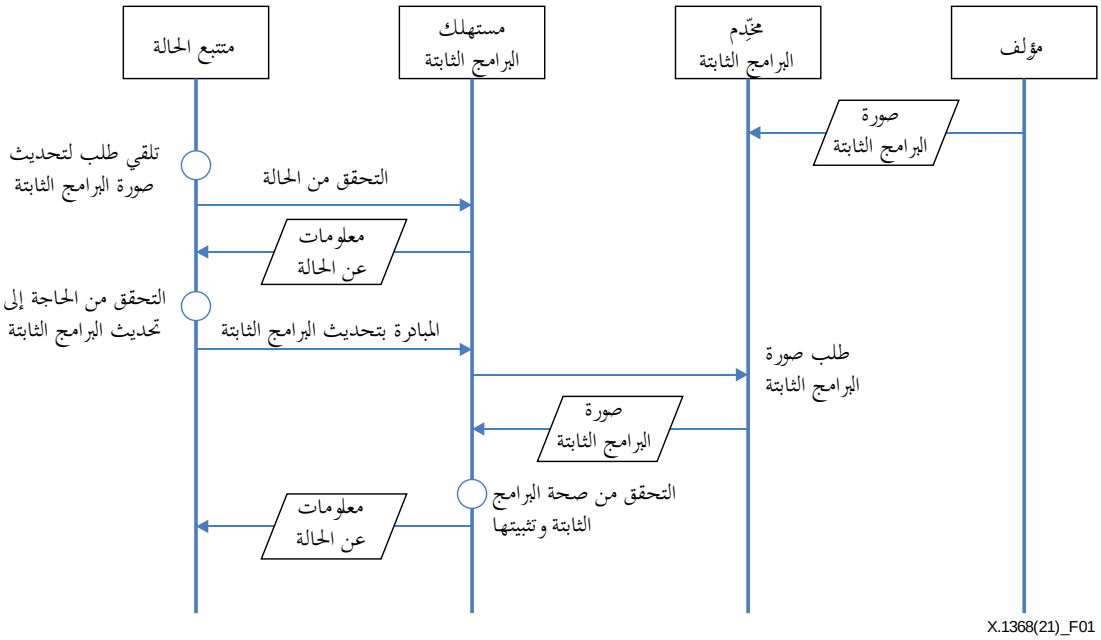
7 إجراءات التحديث

يصور الشكل 1 الإجراء الأساسي لتحديث البرامج الثابتة. وقبل الشروع في إجراء تحديث البرامج الثابتة، يحتاج المؤلف إلى تحميل صورة جديدة للبرامج الثابتة إلى مخدِّم البرامج الثابتة. ويُستحسن إرفاق الصورة بتوقيع رقمي وتجفيرها على يد المؤلف.

وعندما يتلقى متتبع الحالة طلباً لتحديث صورة البرامج الثابتة بموقعها [من قبيل محدد موقع الموارد الموحد (URL)]، فإنه يتحقق من الطلب وبعد ذلك، إذا كان الطلب صالحاً، يتحقق من حالة البرامج الثابتة من خلال التواصل مع مستهلك البرامج الثابتة لتأكيد الحاجة إلى تحديث البرامج الثابتة. ويرد سرد بعض الطرق النمطية لإرسال مثل هذه الطلبات في الفقرة 9.

وفي حال التحقق من الحاجة إلى تحديث البرامج الثابتة، يبدأ مستهلك البرامج الثابتة في تحديث البرامج الثابتة من خلال إبلاغ موقع البرامج الثابتة المتاحة. ثم يطلب مستهلك البرامج الثابتة صورة البرامج الثابتة المحدثة من مخدِّم البرامج الثابتة. ويقدم مخدِّم البرامج الثابتة صورة البرامج الثابتة إلى مستهلك البرامج الثابتة بشرط أن يكون لمستهلك البرامج الثابتة الحق الشرعي في تلقي التحديث. وخلاف ذلك، يرسل المخدِّم رسالة تحديث بشفرة خطأ.

وعند تلقي رسالة التحديث، يتحقق مستهلك البرامج الثابتة من الصورة. وفي حال عدم العثور على خطأ، يقوم مستهلك البرامج الثابتة بتثبيت البرامج الثابتة وإرسال معلومات الحالة إلى متتبع الحالة؛ علماً بأن تواصل عناصر الكيانات الوظيفية الأربعة المذكورة أعلاه يكون من عدة كيانات إلى عدة كيانات، أي أنه يمكن لمتتبعي الحالة المتعددين التواصل مع مستهلكين متعددين للبرامج الثابتة الذين يمكنهم بدورهم التواصل مع مخدمات متعددة للبرامج الثابتة، يمكنها أن تتواصل بدورها مع مؤلفين متعددين.



الشكل 1 – إجراء البروتوكول

8 سيناريوهات النشر

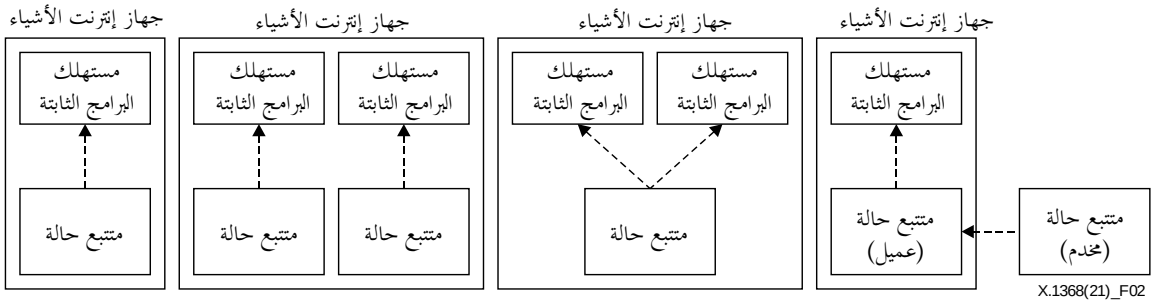
على النحو المذكور في الفقرة 6، يمكن لكيانات وظيفية متعددة أن تقع داخل عقدة واحدة، ويمكن للكيانات المتعددة أن تعمل ككيان وظيفي؛ وقد تختلف سيناريوهات النشر تبعاً للحالات. وفي هذه الفقرة، يرد توضيح عدة سيناريوهات نشر.

1.8 الكيانات الوظيفية داخل أجهزة إنترنت الأشياء

يوضح الشكل 2 أربعة أنواع من أجهزة إنترنت الأشياء. ويجب أن يحتوي جهاز إنترنت الأشياء على مستهلك واحد على الأقل للبرامج الثابتة لأن من الطبيعي أن يحتوي جهاز إنترنت الأشياء على صور متعددة للبرامج الثابتة.

ويجب أن يحتوي جهاز إنترنت الأشياء على متتبع حالة واحد على الأقل. ويمكن أن يحتوي على متتبعي حالة متعددين للتعامل مع مستهلكين متعددين للبرامج الثابتة، ولكن وجود متتبع حالة واحد يتعامل مع جميع مستهلكي البرامج الثابتة يعمل على خير ما يرام أيضاً.

ويمكن أن يرغب جهاز إنترنت الأشياء ذو الموارد المحدودة في تقليل وظائف متتبع الحالة. وهنا، تقسَّم الخواص الوظيفية لمتتبع الحالة إلى وحدة نمطية على جانب العميل ووحدة نمطية على جانب المخدِّم تقع خارج جهاز إنترنت الأشياء. ويُترك الحد الأدنى من الخواص الوظيفية، من قبيل التفاعلات مع مستهلك البرامج الثابتة، على جانب العميل، بينما تصدَّر الخواص الوظيفية الأخرى إلى جانب المخدِّم. ويمكن أن تهتم وحدة جانب المخدِّم النمطية بوحدات نمطية متعددة على جانب العميل. وكثيراً ما يكون ذلك هو النوع المفضل من النشر.



الشكل 2 – الأنواع المختلفة من إنترنت الأشياء

2.8 أنماط نشر متتبع الحالة

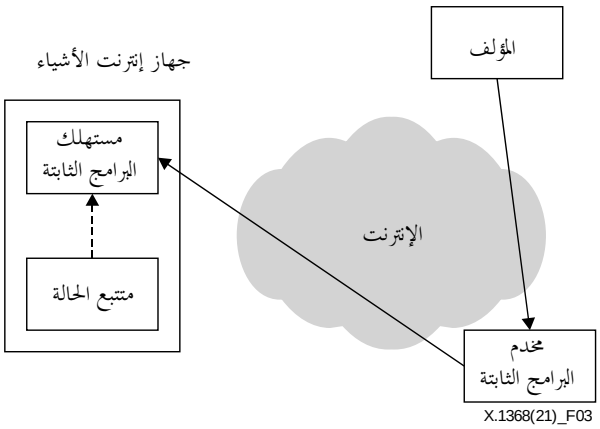
تختلف موارد أجهزة إنترنت الأشياء كثيراً؛ ويمكن أن يوجد متتبع الحالة داخل جهاز إنترنت الأشياء، ولكن قد ترغب أجهزة إنترنت الأشياء ذات الموارد المحدودة في الاحتفاظ بمتتبع حالة منفصل وتقليل استهلاك مواردها إلى الحد الأدنى. علاوةً على ذلك، قد تكون هناك حالات يفضَّل فيها لأجهزة إنترنت الأشياء أن تُدار من كيان مركزي لتيسير الإدارة.

وللتعامل مع هذه المواقف، يمكن تقسيم متتبع الحالة إلى عدة وحدات نمطية وتنفيذها بطريقة تراتبية. وفي هذه الحالة، يمكن أن تُرتب وحدات نمطية متعددة بصورة متتالية بحيث يمكن للوحدة النمطية الأولى في اتجاه المصدر أن تحدد مدى الحاجة إلى تحديث البرامج الثابتة وبدء إجراء لذلك عبر الوحدات النمطية في اتجاه المقصد.

ويرد في الفقرات من 1.2.8 إلى 3.2.8 بحث الحالات التي (1) يتواصل فيها متتبع الحالة الموجود داخل جهاز إنترنت الأشياء مباشرةً مع مخدِّم البرامج الثابتة، و(2) يتواصل فيها متتبع الحالة الموجود داخل جهاز إنترنت الأشياء مع مخدِّم البرامج الثابتة عبر متتبع حالة آخر موجود داخل نفس الشبكة، و(3) يتواصل فيها متتبع الحالة الموجود داخل جهاز إنترنت الأشياء مع مخدِّم البرامج الثابتة عبر متتبعي حالة متعددين.

1.2.8 نموذج متتبع الحالة داخل الجهاز

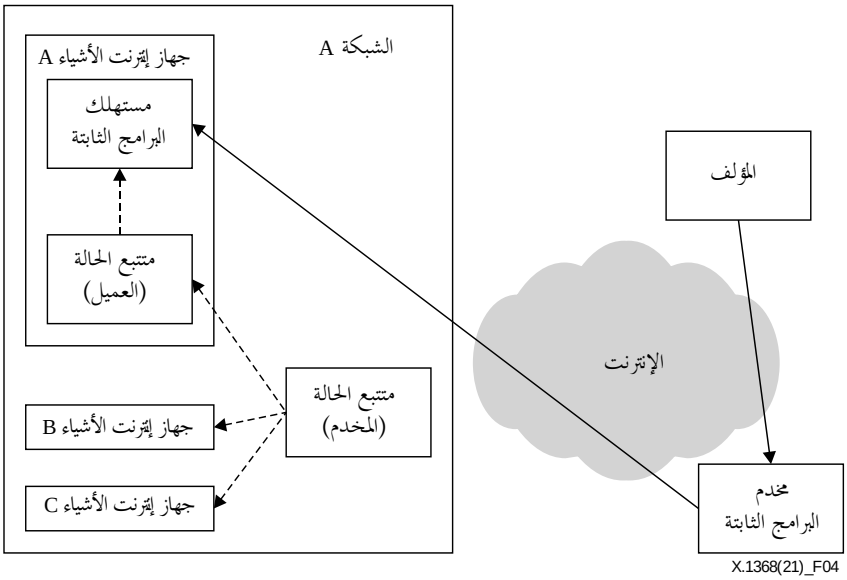
يوضح الشكل 3 نموذج متتبع الحالة داخل الجهاز. وفي هذا النموذج، يوجد مستهلك البرامج الثابتة ومتتبع حالة داخل جهاز إنترنت الأشياء. وعندما يدرك متتبع الحالة الحاجة إلى تحديث البرامج الثابتة (انظر الفقرة 9)، فإنه يطلب من مستهلك البرامج الثابتة تلقي صور البرامج الثابتة من مخدِّم البرامج الثابتة. علماً بأن قنوات الاتصال مُختصرة في هذا القسم، ولكن يمكن توصيلها عبر بروتوكول الإنترنت أو البروتوكولات الأخرى أو توليفة منهما تتطلب جسوراً للاتصالات بين الكيانات. ويُظهر الشكل 3 الإنترنت، لكن التقنيات المذكورة في هذه التوصية يمكنها التعامل أيضاً مع جميع أنواع الشبكات الأخرى.



الشكل 3 – نشر توضيحي لنموذج متتبع الحالة داخل الجهاز

2.2.8 نموذج متتبع حالة مخدِّم العميل

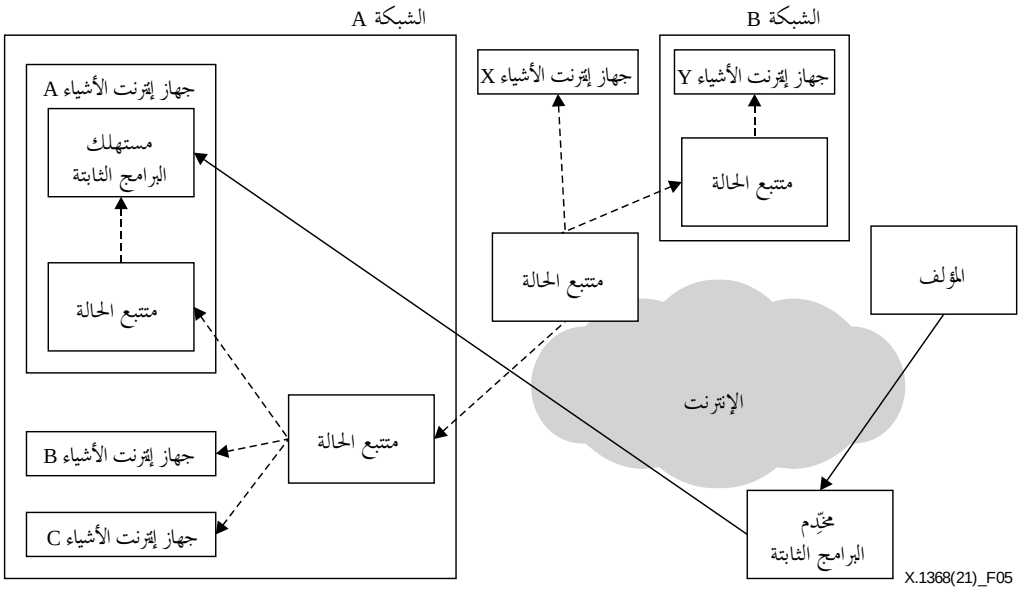
يوضح الشكل 4 نموذج متتبع حالة مخدِّم العميل. وفي هذا النموذج، يقسَّم متتبع الحالة إلى وحدة نمطية للعميل ووحدة نمطية للمخدم. وتقع الوحدات النمطية للعميل داخل أجهزة إنترنت الأشياء بينما تقع الوحدة النمطية للمخدم داخل شبكة. وتراقب الوحدة النمطية للمخدم العديد من أجهزة إنترنت الأشياء من خلال الاتصال بوحدات العميل النمطية. وتتحقق وحدات العميل النمطية ببساطة من الرسالة الواردة من وحدة المخدِّم النمطية وتتصرف وفقاً لذلك. وتبدأ وحدة المخدِّم النمطية إجراء تحديث البرامج الثابتة.



الشكل 4 – نشر توضيحي لنموذج متتبع حالة مخدِّم العميل

3.2.8 نموذج متتبع الحالة التراتبي

يوضح الشكل 5 نموذج متتبع الحالة التراتبي. وفي هذا النموذج، ينقسم متتبع الحالة إلى عدة وحدات نمطية: وحدة العميل النمطية، والوحدات النمطية الوسيطة، ووحدة المخدِّم النمطية. وتقع وحدات العميل النمطية داخل أجهزة إنترنت الأشياء، وتقع وحدة المخدِّم النمطية والوحدات النمطية الوسيطة داخل الشبكات. وتراقب الوحدات النمطية الوسيطة العديد من أجهزة إنترنت الأشياء ومن خلال الاتصال بوحدات العميل النمطية، تراقب وحدة المخدِّم النمطية جميع وحدات العميل النمطية عبر التواصل مع الوحدات النمطية الوسيطة. علماً بأن الوحدات النمطية الوسيطة يمكن أن تُرتب بصورة متتالية لمواصلة إنشاء التسلسل التراتبي. وتتحقق وحدات العميل النمطية ببساطة من الرسالة الواردة من وحدة المخدِّم النمطية وتتصرف وفقاً لذلك. وتبدأ وحدة المخدِّم النمطية إجراء تحديث البرامج الثابتة.



الشكل 5 – نشر توضيحي لنموذج متتبع الحالة التراتبي

9 اكتشاف صور البرامج الثابتة الجديدة المتاحة وبدء الإجراء

يبدأ متتبع الحالة العملية برمتها عندما يتلقى طلباً لتحديث صورة البرامج الثابتة. ويمكن أن يتخذ هذا النوع من الطلبات أشكالاً متنوعة:

أ) يجوز للمؤلف الذي ينشر نسخاً جديدة من صور البرامج الثابتة أن يرسل الطلب؛

ب) يجوز لمخدِّم البرامج الثابتة الذي يتلقى نسخة جديدة من صورة البرامج الثابتة أن يرسل الطلب؛

ج) يتعرف مدير جهاز إنترنت الأشياء على إصدار نسخة جديدة من صور البرامج الثابتة ويمكنه أن يرسل الطلب؛

د) يكتشف متتبع الحالة، أو أحد متتبعي حالة مصدر مدخلاته، الإصدار الجديد من صور البرامج الثابتة من خلال استطلاع مخدِّم البرامج الثابتة بشكل دوري؛

هـ) يتبين متتبع الحالة، أو أحد متتبعي حالة مصدر مدخلاته، وجود نسخة جديدة من صورة البرامج الثابتة من خلال مراقبة إجراء تحديث البرامج الثابتة لجهاز آخر لإنترنت الأشياء يعتني به.

ويمكن أن تصدر أحداث أخرى متنوعة الطلبات، ولكن يجب أن تقدم هذه الطلبات معلومات عن الموقع URL لصور البرامج الثابتة وإصداراتها إلى متتبع الحالة. وإذا رأى متتبع الحالة أن المعلومات موثوقة ويمكن التعويل عليها، يمكنه بدء الإجراء المذكور في الفقرة 7.

10 المتطلبات

تسرد هذه الفقرة المتطلبات الوظيفية لعمليات تحديث برمجيات إنترنت الأشياء (IoT SW). ونظراً لقيود الموارد، لا يمكن تطبيق جميع إجراءات تحديث البرامج المتاحة في بيئة غير مقيدة. وكثيراً ما لا يوجد مستخدم أو مشغل بشري بالقرب من أجهزة إنترنت الأشياء. لذلك، عند تصميم إجراء التحديث الأمني الملموس، يجب أخذ هذه الاختلافات في الاعتبار؛ علماً بأنه يتعين الحفاظ على سرية وسلامة وتيسر الكيانات الوظيفية الأربعة، فهذه شروط مسبقة لتحديث البرمجيات؛ لذا، لم يرد ذكرها من المتطلبات في القائمة التالية.

أ) يجب عدم توزيع البرمجيات/البرامج الثابتة الخبيثة:

'1' ينبغي تحديد الصور الخبيثة قبل تحميلها أو تبادلها؛

'2' يجب أن يتسنى التحقق من سلامة صور البرامج الثابتة؛

'3' يجب أن يتسنى التحقق من مقدم صور البرامج الثابتة.

ب) لا يجوز ترك البرمجيات/البرامج الثابتة المعرضة للخطر دون اتخاذ أي تدابير مناسبة حيالها:

'1' ينبغي كشف النُسخ المتقادمة من البرمجيات/البرامج الثابتة؛

'2' ينبغي كشف البرمجيات/البرامج الثابتة المعرضة للخطر.

ج) يجب أن يتسنى تدارك الفشل الحاصل أثناء إجراء التحديث:

'1' إذا فشل تحديث البرمجيات/البرامج الثابتة، ينبغي أن تكون هناك وسيلة تبليغ بذلك الموقف؛

'2' ينبغي أن تكون هناك وسائل تراجع أو وسائل حماية في حال فشل عملية التحديث.

د) ينبغي إجراء التحديث المقصود والضروري حصراً:

'1' يجب ألا تُثبت إلا الإصدارات الأحدث من البرمجيات/البرامج الثابتة في إنترنت الأشياء (IoT SW/FW)؛

'2' يجب ألا تُثبت إلا الصور الموثوقة للبرمجيات/البرامج الثابتة في إنترنت الأشياء.

هـ) تجب مراعاة قيود الموارد:

'1' ينبغي ألا يجرى التحديث إذا لم يلزم لتقليل موارد الشبكة إلى أدنى حد؛

'2' يمكن ترتيب وظائف متتبع الحالة بصورة متتالية لتقليل العبء على أجهزة إنترنت الأشياء المقيدة الموارد إلى أدنى حد.

و) يجب الحفاظ على حقوق الملكية الفكرية للمؤلفين:

'1' يجب على المؤلفين تجفير صور البرمجيات/البرامج الثابتة؛

'2' يجب الحفاظ على سرية وسلامة وتيسر صور البرمجيات/البرامج الثابتة في إنترنت الأشياء؛

'3' يجب نقل صور البرمجيات/البرامج الثابتة (SW/FW) من المؤلف إلى المقصد النهائي.

11 القدرات

تسرد هذه الفقرة قدرات الكيانات الوظيفية بناءً على المتطلبات المذكورة في الفقرة 10.

1.11 قدرات مستهلك البرامج الثابتة

أ) ينبغي أن يكون مستهلك البرامج الثابتة قادراً على ما يلي:

'1' التحقق مما إذا كان الإجراء السابق لتحديث البرامج الثابتة ناجحاً؛

'2' تداول المعلومات بشأن صور البرمجيات/البرامج الثابتة الحالية (كرقم الإصدار) مع الأطراف ذات الحقوق المشروعة في طلب هذه المعلومات؛

'3' تنفيذ وسيلة تراجع أو وسيلة حماية في حال فشل عملية التحديث؛

'4' إبلاغ متتبع الحالة بالحاجة إلى تحديث البرامج الثابتة؛

'5' تأكيد أصالة وسلامة صور البرامج الثابتة نفسها (من خلال التحقق من شهاداتها على سبيل المثال) أو بوسائل أخرى (من قبيل إسناد عملية التحقق إلى كيانات أخرى)؛

'6' اختيار عدم تثبيت الإصدار الجديد من صور البرمجيات/البرامج الثابتة.

ب) يوصى بأن يكون لدى مستهلك البرامج الثابتة "الأسلوب الآمن" الذي يقوم بتشغيل جهاز إنترنت الأشياء بالحد الأدنى من الخواص الوظيفية والذي يقدم على الأقل وسيلة لتثبيت/استعادة/تحديث البرامج الثابتة يدوياً.

2.11 قدرات متتبع الحالة

ينبغي أن يكون متتبع الحالة قادراً على ما يلي:

أ) الاحتفاظ بقوائم مستهلكي البرامج الثابتة، من الذين لديهم صور البرامج الثابتة المحدَّثة والذين لديهم صور البرامج الثابتة المتقادمة؛

'1' ينبغي أن تحتوي تلك القوائم على معرفاتها الفريدة بالحد الأدنى؛

'2' ينبغي أن يتمكن متتبع الحالة من تحديد مستهلكي البرامج الثابتة الذين لديهم برامج ثابتة متقادمة.

ب) معرفة حالة مستهلكي البرامج الثابتة الخاضعين لإدارته؛ ينبغي أن تكون هناك وسيلة:

'1' للتحقق مما إذا كان مستهلك البرامج الثابتة (وجهاز إنترنت الأشياء الذي يحتوي على مستهلك البرامج الثابتة) في حالة جيدة من خلال الاتصال بمستهلك البرامج الثابتة والتحقق من سجلات الاتصال مع مستهلك البرامج الثابتة؛

'2' للتأكد من نجاح الإجراء السابق لتحديث البرامج الثابتة لدى مستهلك البرامج الثابتة؛

'3' لمعرفة إصدارات البرامج الثابتة التي يشغِّلها مستهلكو البرامج الثابتة.

ج) تحديد ما إذا كان تحديث البرمجيات/البرامج الثابتة ضرورياً وبدء إجراء تحديث البرامج الثابتة عند الحاجة؛

د) التحقق من أصالة متتبع حالة مصدر المدخلات عند تنفيذه بطريقة تراتبية.

وعندما تُقسم الخواص الوظيفية لمتتبع الحالة إلى أكثر من وحدة نمطية واحدة، يجب أن تكون الوحدات النمطية قادرة على ما يلي:

أ) الحفاظ على سرية وسلامة الاتصالات فيما بينها؛

ب) التحقق من أصالة الإشارات المرسَلة من بعضها البعض؛

ج) الحفاظ على المعلومات اللازمة للوصول إليها.

3.11 قدرات مخدِّم البرامج الثابتة

ينبغي أن يكون مخدِّم البرامج الثابتة قادراً على ما يلي:

أ) قبول ما يقدمه المؤلفون من صور البرمجيات/البرامج الثابتة لإنترنت الأشياء (IoT SW/FW)؛

ب) تقديم صور البرمجيات/البرامج الثابتة التي يحتوي عليها إلى مستهلكي البرامج الثابتة؛

ج) تحديد صور البرمجيات/البرامج الثابتة الخبيثة واتخاذ الإجراءات المناسبة، مثل إزالتها من وحدة التخزين الداخلية وحظر تقديمها من المؤلفين الذين يقدمون هذه الصور؛

د) إدارة قائمة المؤلفين ومستهلكي البرامج الثابتة الذين يستخدمونها؛

ه) إدارة إصدارات صور البرمجيات/البرامج الثابتة لإنترنت الأشياء (IoT SW/FW)؛

و) الحفاظ على قائمة مستهلكي البرامج الثابتة وصور البرمجيات/البرامج الثابتة التي قاموا بتنزيلها في الماضي؛

ز) إبلاغ أجهزة إنترنت الأشياء التي قامت بتنزيل صور البرمجيات/البرامج الثابتة لإنترنت الأشياء (IoT SW/FW) المتقادمة في الماضي بتوفر إصدارات جديدة؛

ح) التحقق من الموقع الجغرافي أو المنطقي لأجهزة إنترنت الأشياء وإجازة أو رفض تنزيل صور البرمجيات/البرامج الثابتة لتجنب توزيعها في موقع محظور تحدده السياسات أو الوسائل الأخرى المرعية.

4.11 قدرات المؤلف

ينبغي أن يكون المؤلف قادراً على الحفاظ على أصالة وسرية وسلامة صور البرامج الثابتة التي ينتجها.

أ) ينبغي عدم تبديل البرامج الثابتة أو المساس بها على يد أطراف ثالثة (الأصالة والسلامة).

ب) ينبغي الحفاظ على الملكية الفكرية للباعة ضمن البرامج الثابتة (السرية).

ج) ينبغي للمؤلف تنفيذ تدابير لتأمين صورة البرامج الثابتة التي يقوم بتحميلها على مخدمات البرامج الثابتة لأن مخدِّم البرامج الثابتة ليس موثوقاً بالضرورة.

التذييل I

الأنشطة ذات الصلة خارج قطاع تقييس الاتصالات

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

تشمل الأنشطة المتعلقة بتحديثات برمجيات إنترنت الأشياء (IoT SW) التي دُرست خارج قطاع تقييس الاتصالات ما يلي:

1) ورشة عمل تحديث برمجيات إنترنت الأشياء (IOTSU) [b-ISOC iotsu]؛

2) فريق العمل التابع لطاقم فريق مهام هندسة الإنترنت (IETF) [b-IETF suit]:
   - المعني بملف الكشوفات [b-IETF manifest]؛
   - المعني بمعمارية تحديث البرامج الثابتة [b-IETF architecture].

3) شراكة الاتصالات من آلة إلى آلة (oneM2M): معايير الاتصالات من آلة إلى آلة (M2M) وإنترنت الأشياء [b-oneM2M] وما إلى ذلك.

التذييل II

مثال سيناريو لتحديث برمجيات إنترنت الأشياء باستخدام تكنولوجيا سجل الحسابات الموزَّع

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

1.II نظرة عامة

تحتوي البنية التحتية لإنترنت الأشياء على عدد كبير من الأجهزة التي يتعين على المدير إدارتها. ويخضع جهاز إنترنت الأشياء على مراجعات متنوعة وفقاً لسمات ما يتضمنه من عتاد، ويمكن تطبيق مختلف البرامج الثابتة وفقاً للوحة جهاز الاستشعار الإضافية. وبالإضافة إلى ذلك، تختلف نسخة البرمجيات المدعومة حسب نسخة العتاد. ويمكن أن تسبب الاختلافات في حزم البرمجيات المثبتة مشاكل التبعية. علاوة على ذلك، يمكن حل هذه المشكلة باستخدام تكنولوجيا سجل الحسابات الموزَّع (DLT).

وتمتلك تكنولوجيا سجل الحسابات الموزَّع عقداً ذكياً يسمح بإجراء تحديثات للبرامج الثابتة أو البرمجيات بناءً على العقود المكتوبة مسبقاً على يد المدير. وكذلك يمكن لحلول الثغرات الأمنية التي قد تظهر أثناء عملية التحديث أن تستند إلى خوارزميات التوافق وطبقة التجفير.

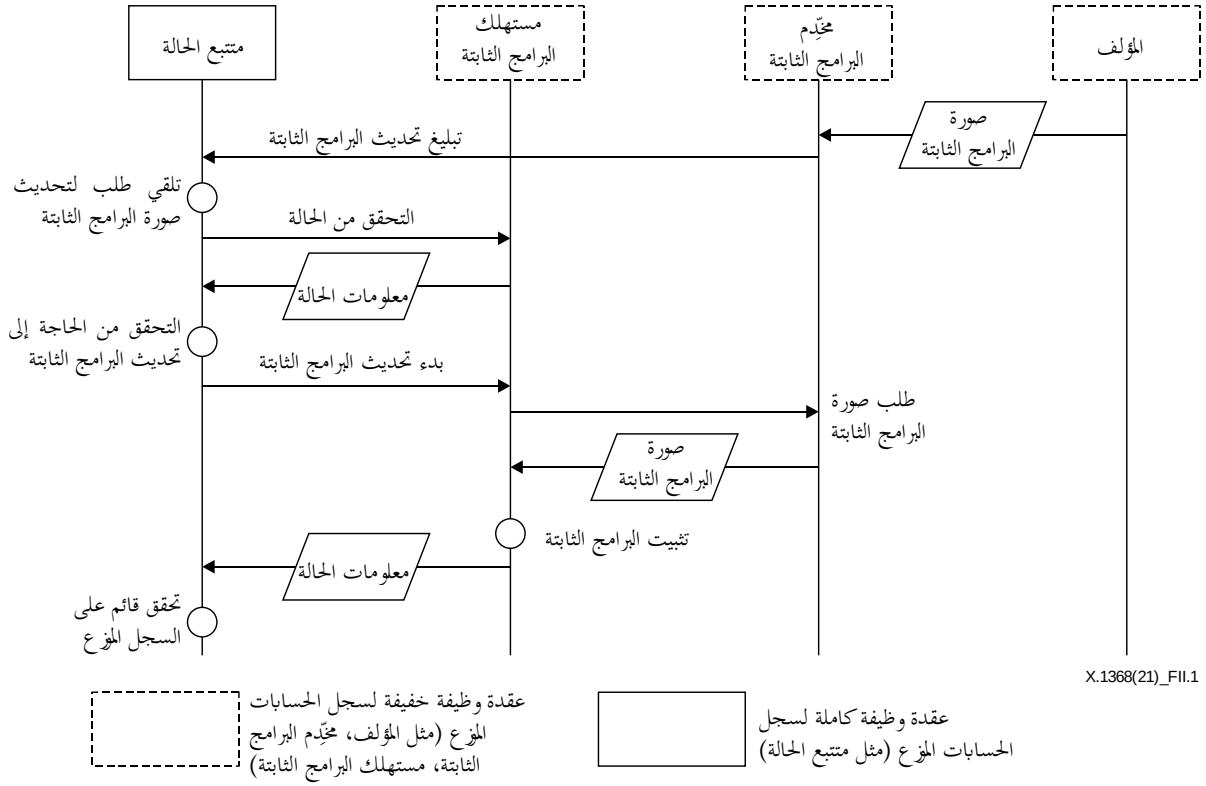
ويصف هذا المثال كيفية تقديم تحديثات البرمجيات/البرامج الثابتة الآمنة استناداً إلى سجل الحسابات الموزَّع في البيئات ذات مراجعات العتاد وإصدارات البرمجيات المختلفة، مثل البنية التحتية لإنترنت الأشياء.

2.II إجراء تحديث البرمجيات

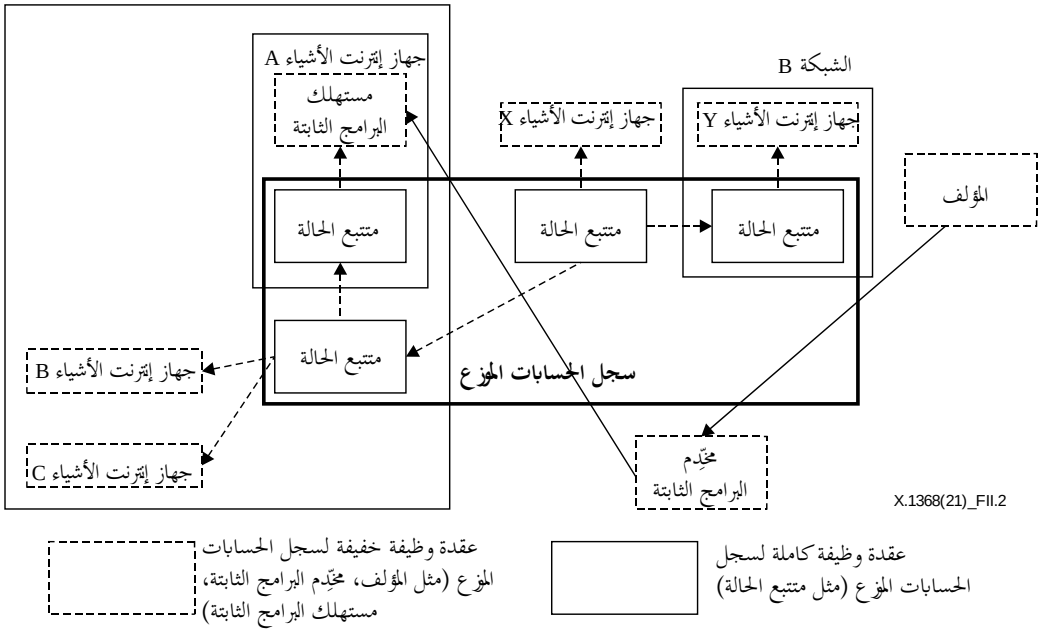
انظر الجدول II–1 والشكلين II-1 وII-2.

الجدول II–1 – هيكل الكتل لتحديث البرمجيات

رأسية الكتلة	– مقاس، إصدار الكتلة – السمة السابقة لاختزال رأسية الكتلة
بيانات الكتلة	– جذر ميركل (Merkle) – اسم المقدم، ووقت النشر، ورقم الإصدار، وشفرة اختزال الملف، ورابط الملف، واسم الملف، ومقاس الملف، وعتاد الدعم، وتبعية البرمجيات



الشكل II-1 – إجراء تحديث البرمجيات المستند إلى السجل الموزع



الشكل II-2 – تحديث البرمجيات المستند إلى السجل الموزع لشبكات متعددة

بيبليوغرافيا

[b-IETF RFC 2119] IETF RFC 2119 (1997), *Key words for use in RFCs to indicate requirement levels.*

[b-IETF architecture] *A Firmware Update Architecture for Internet of Things,* Wilmington, DE: Internet Engineering Task Force. Available [viewed 2021-02-19] at: https://tools.ietf.org/html/draft-ietf-suit-architecture-08

[b-IETF manifest] Moran, B., Tschofenig, H., Birkholz, H. (2019). *Firmware updates for Internet of things devices – An information model for manifests.* Wilmington, DE: Internet Engineering Task Force. Available [viewed 2021-02-19] at: https://tools.ietf.org/id/draft-ietf-suit-information-model-02.html

[b-IETF suit] IETF (2021). *Software updates for the internet of things (suit),* version 7.26.0. Wilmington, DE: Internet Engineering Task Force. Available [viewed 2021-02-19] at: https://datatracker.ietf.org/wg/suit/about/

[b-ISOC iotsu] Internet Architecture Board (Internet), *Internet of things software update workshop (IoTSU) 2016.* Reston, VA: Internet Society. Available [viewed 2021-02-20] at: https://www.iab.org/activities/workshops/iotsu/

[b-oneM2M] oneM2M (2017), *Standards for M2M and the Internet of things.* oneM2M. Available [viewed 2021-02-20] at: http://www.onem2m.org/technical/published-drafts

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، 2021