الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1367

(2020/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

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

نسق مقيَّس لسجلات الأخطاء لإنترنت الأشياء (IoT) من أجل عمليات الحوادث الأمنية

التوصية ITU-T X.1367

الاتحاد الدولي للاتصالات

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	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن (1)	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة (2)	
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.1360**
أمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن سجل الحسابات الموزع	X.1449–X.1430
البروتوكول الأمني (2)	X.1459–X.1450
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولّد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
أمن البيانات	
أمن البيانات الضخمة	X.1759–X.1750
أمن شبكات الجيل الخامس	X.1819–X.1800

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

التوصية ITU-T X.1367

نسق مقيَّس لسجلات الأخطاء لإنترنت الأشياء (IoT) من أجل عمليات الحوادث الأمنية

ملخص

هناك مسألتان لمعالجة الحوادث الأمنية من النظام الإيكولوجي لإنترنت الأشياء (IoT): الأولى هي عدم توافق البروتوكولات بين شبكات الحاسوب التي تستخدم بروتوكول التحكم في الإرسال/بروتوكول الإنترنت (TCP/IP) وأجهزة الحافة لإنترنت الأشياء. والثانية هي عدم توافق شفرات الأخطاء بين مصنعي أجهزة الحافة.

وتوصف التوصية ITU-T X.1367 نسقاً مقيَّساً لسجلات الأخطاء يمكن وضعه في الحمولة النافعة للبروتوكول، مثل سجل النظام (syslog) (انظر المعيار IETF RFC 5424) كي يستخدم في تحويل معلومات سجلات الأخطاء الصادرة عن جهاز حافة ما إلى النسق المقيَّس لسجلات الأخطاء.

وتوصف هذه التوصية أيضاً جدولاً مقيَّساً لشفرة الأخطاء لحل المسألة الثانية. ونتيجةً لذلك، فإن الحوادث الأمنية بين الشبكات الحاسوبية والشبكات الخاصة بأجهزة الحافة لإنترنت الأشياء تمكن إدارتها بشكل تكاملي.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1367	2020-09-03	17	11.1002/1000/14263

مصطلحات أساسية

جهاز الحافة، شفرة الأخطاء، نسق سجلات الأخطاء، التصدي للحوادث، إنترنت الأشياء (IoT)، عملية أمنية.

* 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 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 "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

التوصية ITU-T X.1367

نسق مقيَّس لسجلات الأخطاء لإنترنت الأشياء (IoT) من أجل عمليات الحوادث الأمنية

1 مجال التطبيق

توصِّف هذه التوصية نسقاً مقيَّساً لسجلات الأخطاء لإنترنت الأشياء (IoT) يمكن وضعه في الحمولة النافعة للبروتوكول، مثل سجل النظام (syslog) [b-IETF RFC 5424]، كي يستخدم في تحويل معلومات سجلات الأخطاء الصادرة عن جهاز الحافة إلى النسق المقيَّس لسجلات الأخطاء.

وتوصِّف هذه التوصية أيضاً جدولاً مقيَّساً لشفرة الأخطاء لحل عدم توافق شفرات الأخطاء بين الشركات المصنعة لأجهزة الحافة ونتيجةً لذلك، فإن الحوادث الأمنية بين الشبكات الحاسوبية والشبكات الخاصة بأجهزة الحافة لإنترنت الأشياء تمكن إدارتها بشكل تكاملي.

2 المراجع

لا توجد.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 المفعل (actuator) [b-ITU-T Y.4109]: جهاز يقوم بإجراءات فيزيائية بسبب إشارة دخل.

2.1.3 هجوم (attack) [b-ISO 13491-1]: محاولة الحصول على معلومات حساسة أو خدمة أو تعديلهما من جانب أحد الخصوم غير المرخص لهم بذلك.

3.1.3 الاستيقان (authentication) [b-ITU-T X.1277]: الاستيقان هو العملية التي يستخدم فيها المستخدم مستيقِن FIDO لإثبات امتلاك مفتاح مسجَّل لطرف معوِّل.

4.1.3 التخويل (authorization) [b-ITU-T X.800]: منح الحقوق، الذي يتضمن إتاحة النفاذ استناداً إلى حقوق النفاذ.

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

6.1.3 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.

7.1.3 سطح التماس بين الإنسان والآلة (HMI) (human/machine interface) [b-ITU-T H.320]: سطح تماس بين الإنسان والآلة يربط بين المستخدم وبين المطراف/النظام الذي يتكون من قسم فيزيائي (صوتي كهربائي، محول طاقة كهربائية–بصرية، مفاتيح، وما إلى ذلك) وقسم منطقي يتعامل مع حالات التشغيل الوظيفي.

8.1.3 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.

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

10.1.3 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.

11.1.3 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 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 إصدار شهادة (certification): شهادة من طرف ثالث تتعلق بالمنتجات أو العمليات أو الأنظمة أو الأشخاص.

ملاحظة – بناءً على التعريف الوارد في المرجع [b- ISO/IEC 17000].

2.2.3 مخدِّم الأوامر والتحكم (C&C) (command and control (C&C) server): مخدِّم يرسل أوامر إلى حواسيب أصبحت روبوتات بعد الإصابة ببرمجيات ضارة، ويتحكم فيها (شبكات الروبوتات).

3.2.3 التجفير (encryption): تحويل تجفيري للبيانات لإنتاج نص شفرة سرية.

ملاحظة – بناءً على تعريف التشفير السري، في التوصية [b-ITU-T X.800]، الذي يتعامل مع التجفير على أنه مرادفه.

4.2.3 جهاز الحافة لإنترنت الأشياء (Internet of things edge device): جهاز مطراف للنظام الإيكولوجي لإنترنت الأشياء يجمع البيانات من العالم الحقيقي بأجهزة استشعار أو يؤثر على العالم الحقيقي بالمفعلات.

5.2.3 بوابة إنترنت الأشياء (IoTGW) (Internet of things gateway): جهاز يوصل بين شبكة لأجهزة الحافة لإنترنت الأشياء وشبكات الحاسوب المتاحة على نطاق واسع، مثل الإنترنت.

6.2.3 وحدة تحكُّم صغرية (MCU) (microcontroller unit): معالج صغري مدمج بضم وحدات حسابية ووحدات ذاكرة ومنافذ الدخل/الخرج في دارة متكاملة واحدة.

7.2.3 فريق التصدي للحوادث الأمنية (SIRT) (security incident response team): فريق يتلقى تقارير عن "الحوادث الأمنية" ويحقق فيها ويتصدى لها.

8.2.3 مركز العمليات الأمنية (SOC) (security operations centre): قسم يراقب حالة الحواسيب والشبكات في المنظمة ويتصدى بعد اكتشاف علامات أنشطة خبيثة.

4 الاختصارات والاختزالات

تستخدم هذه التوصية المختصرات والاختزالات التالية:

C&C الأوامر والتحكم *(Command and Control)*

FW جدار الحماية *(Firewall)*

HMI سطح التماس بين الإنسان والآلة *(Human/Machine Interface)*

ID معرف *(Identifier)*

IDS نظام كشف التسلل *(Intrusion Detection System)*

IoT إنترنت الأشياء *(Internet of Things)*

IoTGW بوابة إنترنت الأشياء *(Internet of Things Gateway)*

IP بروتوكول الإنترنت *(Internet Protocol)*

JSON ترميز كائن بلغة JavaScript *(JavaScript Object Notation)*

LAN شبكة محلية *(Local Area Network)*

MCU وحدة تحكُّم صغرية *(Microcontroller Unit)*

PC حاسوب شخصي *(Personal Computer)*

SIRT فريق التصدي للحوادث الأمنية *(Security Incident Response Team)*

SOC مركز العمليات الأمنية *(Security Operation Centre)*

TCP بروتوكول التحكم في إرسال *(Transmission Control Protocol)*

5 الاصطلاحات

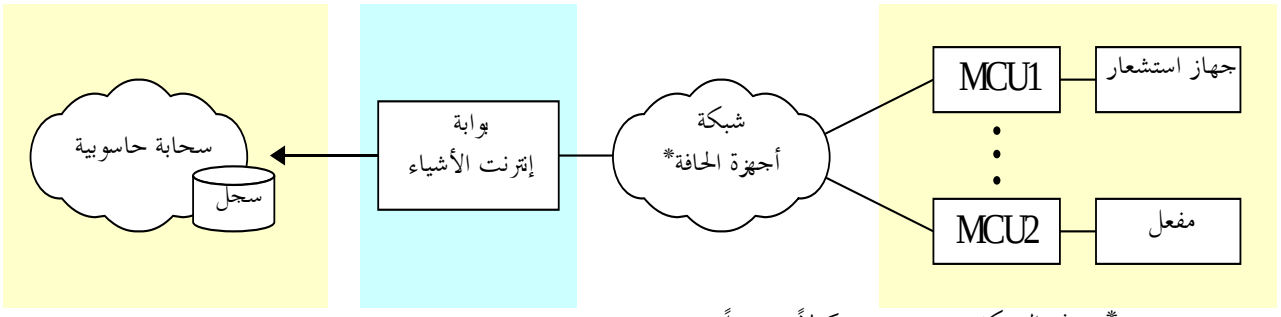
لا توجد.

6 اعتبارات عامة

1.6 معالجة الأخطاء الحالية في النظام الإيكولوجي لإنترنت الأشياء

في سياق معالجة الأخطاء في إنترنت الأشياء، إذا تعطل أحد مكونات نظام إنترنت الأشياء مثل جهاز الاستشعار أو المفعل، ستصدر شفرة الأخطاء وتسجَّل في سجلات الأخطاء. وإذا كان الخطأ نادر الحدوث، لا حاجة للتصحيح. أما إذا استمر حدوث الخطأ، فينبغي تبديل المكون لإصلاح المشكلة.

ويوضح الشكل 1 نظاماً إيكولوجياً نمطياً لإنترنت الأشياء يتكون من مكونات إنترنت الأشياء مثل وحدات التحكم الصغرية (MCU) المرتبطة بأجهزة الاستشعار والمفعلات، وبوابة إنترنت الأشياء (IoTGW) وسحابة حاسوبية.



* هذه الشبكة ستستخدم بروتوكولاً مخصصاً.

X.1367(20)_F01

الشكل 1 – النظام الإيكولوجي النمطي لإنترنت الأشياء

يعتمد الاتصال بين بوابة إنترنت الأشياء (IoTGW) وMCU1 وMCU2 في الشكل 1 على بروتوكول مخصص (انظر الملاحظة) للنظام. ويعد جهاز استشعار وحدة MCU1 ومفعل وحدة MCU2 مثالين على أجهزة الحافة لإنترنت الأشياء. وفي هذه الحالة، ترسل بوابة إنترنت الأشياء (IoTGW) طلباً إلى وحدات التحكم الصغرية (MCU) فترد وحدات التحكم الصغرية على بوابة إنترنت الأشياء (IoTGW) بمعلومات السجل. وتتواصل بوابة إنترنت الأشياء (IoTGW) أيضاً مع السحابة الحاسوبية (نظام المخدِّم).

ملاحظة – يمكن أن يكون البروتوكول المخصص بروتوكولاً للشبكات الكبيرة، مثل شبكة oneM2M [b-oneM2M] أو ECHONET Lite [b-ISO/IEC 14543-4-3] أو يمكن أن يكون بروتوكولاً للشبكات الصغيرة مثل شبكة SPI [b-SPI] أو I^2C [b-UM10204] أو Bluetooth [b-IEEE 802.15.1] أو Zigbee [b-IEEE 802.15.4] أو بروتوكولاً مسجل الملكية مصمماً حصراً لنظام إنترنت الأشياء هذا.

ونظراً لأن أجهزة الحافة لإنترنت الأشياء تتعطل أحياناً، يحتاج النظام الإيكولوجي لإنترنت الأشياء إلى معالجة الأخطاء لإدارة النظام الإيكولوجي لإنترنت الأشياء بشكل مناسب. وتتعامل هذه الأنظمة مع سجلات الأخطاء بشفرات الأخطاء وتبدأ الإصلاحات. ومن ناحية أخرى، تقوم بعض الأنظمة بتحليل سجلات الأخطاء المخزنة بشفرات الأخطاء لتجميع المعلومات الإحصائية بغية تحسينها بل وللتعامل مع الحوادث الأمنية. ولكن يصعب توحيد سجلات الأخطاء لكل نظام إيكولوجي لإنترنت الأشياء ولسجل النظام (syslog) [b-IETF RFC 5424].

2.6 نظرة عامة

من أجل التصدي للحوادث بفعالية، يعد تقديم القدرات الكافية لجمع وتحليل معلومات سجلات الأخطاء من مكونات النظام الإيكولوجي لإنترنت الأشياء أمراً أساسياً. بيد أن الشواغل التالية معروفة في حالة النظام الإيكولوجي لإنترنت الأشياء.

1) يوجد إجراء مقيَّس يشمل عملية تسليم الحوادث، وذلك باستخدام سجل النظام [b-IETF RFC 5424]، لجمع معلومات السجل من أجهزة الشبكة. ولكن لا يوجد مثل هذا الإجراء للنظام الإيكولوجي لإنترنت الأشياء.

2) لا يمكن تخزين معلومات سجلات الأخطاء لإنترنت الأشياء في مكون واحد من النظام الإيكولوجي لإنترنت الأشياء، أي ينبغي جمع معلومات السجل هذه بواسطة نظام المخدم (كالسحابة الحاسوبية) أو نظام الحافة لإنترنت الأشياء (من قبيل بوابة إنترنت الأشياء (IoTGW)) حسب تشكيلة النظام الإيكولوجي لإنترنت الأشياء.

3) يصعب تحليل تلازم معلومات سجلات الأخطاء بين مكونات إنترنت الأشياء المختلفة، لعدم وجود نسق مقيَّس لسجلات الأخطاء.

4) بدون أسلوب للتعامل مع معلومات سجلات الأخطاء، لن يتمكن النظام الإيكولوجي لإنترنت الأشياء من صيانة خدمة إنترنت الأشياء لديه بشكل فعّال.

وتصف هذه التوصية معمارية نظام إنترنت الأشياء الأساسية لجمع سجلات الأخطاء لإنترنت الأشياء ليصار إلى استخدامها في عمليات معالجة الحوادث. وهي توصِّف الشفرات المقيَّسة للأخطاء والنسق المقيَّس لسجلات الأخطاء. وبتحويل شفرات الأخطاء التي تعتمدها كل شركة مصنعة للنظام الإيكولوجي لإنترنت الأشياء إلى شفرات مقيَّسة للأخطاء، تمكن مراقبة حالة أنظمة إيكولوجية متعددة لإنترنت الأشياء بمزيد من الفعالية. علاوةً على ذلك، في عملية تحويل شفرة الأخطاء إلى شفرة مقيَّسة للأخطاء، تسجَّل الحالة التي حدث فيها الخطأ أيضاً في سجلات الأخطاء المرتبطة. ونتيجة لذلك، تمكن معالجة الحوادث الأمنية عبر أنظمة إيكولوجية متعددة لإنترنت الأشياء. (انظر المثال في التذييل I، الفقرة I.4، الأنظمة الإيكولوجية المتعددة لإنترنت الأشياء)

7 النسق المقيَّس لسجلات الأخطاء لبيئة إنترنت الأشياء

بسبب ضعف الموارد الحاسوبية، قد يصعب على أجهزة جهاز الحافة لإنترنت الأشياء تنفيذ وظائف جديدة لتسليم سجلات الأخطاء لإنترنت الأشياء. ولكن بوابة إنترنت الأشياء (IoTGW) تمتلك عادةً موارد حاسوبية أفضل للقيام بذلك. وكثيراً ما يجري تبادل الطلبات والردود بين بوابة إنترنت الأشياء (IoTGW) وأنظمة السحابة الحاسوبية، وتشمل هذه الاتصالات معلومات سجلات الأخطاء لإنترنت الأشياء. لذلك، في هذه التوصية، يُطلب قيام بوابة إنترنت الأشياء (IoTGW) بإنشاء معلومات مقيَّسة لسجلات الأخطاء وتبليغها إلى الأنظمة السحابية.

1.7 الهيكل الأساسي لنسق سجلات الأخطاء

يحتوي سجلات الأخطاء لإنترنت الأشياء على النسق الموضح في الشكل 2 باستخدام ترميز كائن بلغة JavaScript (JSON) بالتعبير العادي. ويمكن تحويل هذا النسق كي يستخدمه سجل النظام أو لغة XML (انظر الملاحظة). ويرد وصف أمثلة هذا النسق في التذييل I.

ملاحظة – لا تحدد هذه التوصية طول كل قيمة نعت. وستدعو الحاجة للاتفاق مسبقاً بين المرسل والمستلم لسجلات الأخطاء على طول كل قيمة نعت.

```
{
   "Timestamp":
        "^([0-9]{4})-(1[0-2]|0[1-9])-(3[01]|0[1-9]|[12][0-9])T
          (2[0-3]|[01][0-9]):([0-5][0-9]):([0-5][0-9])(\.[0-9]{+})Z$",
   "Reporter": {},
   "Protocol": String,
   "Requester": {},
   "Responder": {},
   "Error Code": "/^[0-9A-F]^{+}$/",
   "Error Message": String,
   "Description": String | {},
}
```

الشكل 2 – عناصر سجلات الأخطاء

في معظم الحالات، يكون مراسل سجلات الأخطاء هذا هو بوابة إنترنت الأشياء (IoTGW). ويرد تعريف النعوت المستخدمة في هذا النسق في الفقرة 2.7.

2.7 النعوت الأساسية

النعوت التالية هي عناصر في معلومات سجلات الأخطاء.

أ) الختم الزمني: يُتطلب ختم زمني (انظر الملاحظة) لإصدار سجلات الأخطاء. فعلى سبيل المثال، في حالة 20 سبتمبر 2018 – 13 ساعة و25 دقيقة و51 ثانية، ينبغي وصف الختم الزمني على أنه "2018-09-20T13:25:51.0Z." [b-ISO 8601-1].

ملاحظة – "الختم الزمني" إلزامي، على الرغم من أن بروتوكول الإرسال الذي يحمل سجلات أخطاء الموصَّف في هذه التوصية يحتوي أيضاً على حقل ختم زمني، لأن الختم الزمني يتغير عادةً بين حدوث المشكلة ووقت النقل.

ب) المراسل: مكون إنترنت الأشياء الذي يحول شفرة خطأ الجهاز إلى شفرة مقيَّسة للأخطاء ويرسلها إلى السحابة الحاسوبية. ويرد الوصف التفصيلي في الشكل 3.

```
"Reporter":{
    "IP Address":
        "(^(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}
              (?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$)
         |(^(?:[A-F0-9]{1,4}:){7}[A-F0-9]{1,4}$)"
}
```

الشكل 3 – عناصر المراسل

1) عنوان بروتوكول الإنترنت (IP): المعرف الفريد (ID) للمراسل على الإثرنت.

ج) البروتوكول: اسم البروتوكول المستخدم بين أجهزة بوابة إنترنت الأشياء (IoTGW)، وأجهزة الحافة لإنترنت الأشياء.

د) الطالب أو المجيب: مكون إنترنت الأشياء الذي يرسل طلباً إلى جهاز الحافة لإنترنت الأشياء أو مكون إنترنت الأشياء الذي يرد على الطلب. ويرد الوصف التفصيلي في الشكل 4.

```
"Requester(or Responder)": {
    "Unique ID": string,
    "Transmitted Code": "( [0-9A-F])^{+}}
```

الشكل 4 – عناصر الطالب والمجيب

1) المعرف الفريد (اختياري): هذا رقم فريد أو شفرة فريدة على صلة بكل جهاز محدد بواسطة بروتوكول شبكة جهاز الحافة لإنترنت الأشياء.

2) الشفرة المرسَلة (اختيارية): محتوى البيانات المرسَلة. ويعبَّر عنه بالسداسيات العشرية.

3) ينبغي التعبير كما في الشكل 5 عندما يحدث خطأ بدون طالب أو مجيب، من قبيل أن يرسل جهاز استشعار البيانات بشكل دوري دون طلب.

```
"Requester(or Responder)": {}
```

الشكل 5 – حالة بدون طالب أو بدون مجيب

هـ) شفرة الخطأ، ورسالة الخطأ: يرد توصيف شفرة الخطأ ورسالة الخطأ في الملحق A.

و) الوصف (اختياري): يمكن التعبير عن أي جمل وعبارات وعناصر فرعية بترميز JSON، إذا كان التبليغ عن حالة أجهزة الحافة لإنترنت الأشياء أو شبكاتها مطلوباً.

ويمكن حذف رسالة الخطأ إذا كان عرض نطاق الاتصالات ضيقاً أو مقاس التخزين محدوداً. ويمكن حذف الوصف إن لم تكن كتابة أي نص إضافي ضرورية.

الملحق A

شفرة الخطأ ورسالة الخطأ

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

يرد توصيف شفرة الخطأ ورسالة الخطأ في الجدول 1.A.

الجدول 1.A – شفرة الخطأ ورسالة الخطأ

الشفرة	الرسالة	الوصف
	لا يوجد خطأ (0x00-0x0F)	
0x00	لا يوجد خطأ	لم يحدث خطأ.
	الاتصالات (0x10-0x1F)	
0x10	لا يوجد رد	لا يوجد رد على الرغم من أن الطلب يتطلب أي رد من الردود.
0x11	فشل الاتصال	بعض المشاكل سببت فشل الاتصال.
0x12	تعطل الوصلة	تعطل وصلة السطح البيني لشبكة.
0x1E	أسباب موسّعة	شفرة البادئة لأسباب موسعة.
0x1F	أسباب الاتصالات الأخرى	أسباب أخرى تتعلق بالاتصالات.
	الأمن (0x20-0x2F)	
0x20	فشل الاستيقان	بعض مشاكل الاستيقان.
0x21	فشل إصدار الشهادة	بعض مشاكل إصدار الشهادة.
0x22	فشل التجفير	بعض مشاكل التجفير.
0x23	فشل التخويل	بعض مشاكل التخويل.
0x2E	أسباب موسّعة	شفرة البادئة لأسباب موسعة.
0x2F	أسباب أمنية أخرى	أسباب أخرى تتعلق بالاستيقان أو إصدار الشهادة أو التجفير أو التخويل.
	الأمر (0x30-0x3F)	
0x30	أمر غير صالح	الأمر غير معرَّف أو غير صالح.
0x31	وسيط غير صالح	الوسيط خارج النطاق أو غير صالح.
0x3E	أسباب موسّعة	شفرة البادئة لأسباب موسعة.
0x3F	أسباب الأمر الأخرى	أسباب أخرى تتعلق بالأمر.
	الجهاز (0x40-0x4F)	
0x40	الجهاز محطم	تحطم جزء من الجهاز بشكل غير قابل للاسترداد.
0x41	فشل الجهاز	فشل جزء من الجهاز ولكن يمكن استرداده.
0x42	نفاد الموارد	نفدت سعة التخزين والذاكرة وأي موارد حوسبة.
0x4E	أسباب موسّعة	شفرة البادئة لأسباب موسعة.
0x4F	أسباب الجهاز الأخرى	أسباب أخرى تتعلق بالجهاز.
	محجوزة للتوسيع المستقبلي (0x50-0xDF)	
	محجوزة للتطبيقات الخاصة (0xE0-0xEF)	
	رسائل أخرى (0xF0-0xFF)	
0xFF	أسباب أخرى	أسباب أخرى باستثناء الأسباب المذكورة أعلاه.

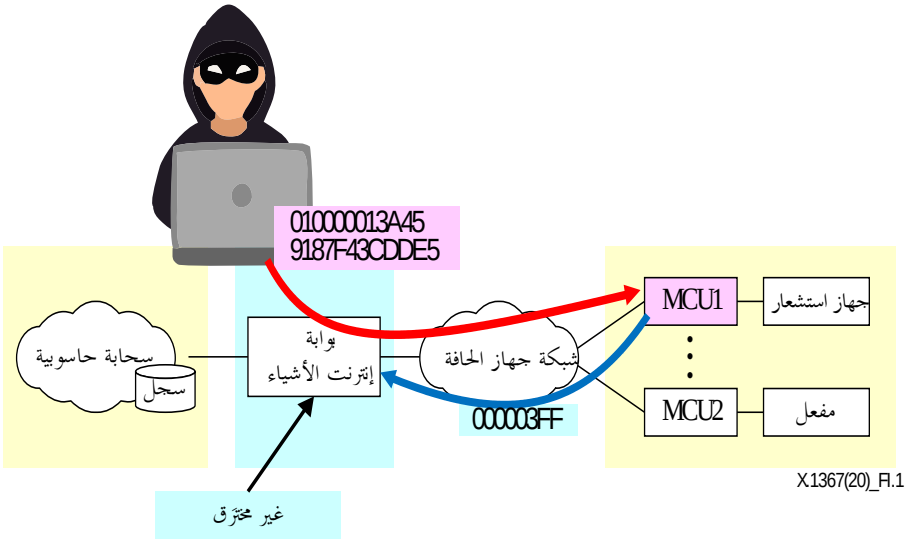
التذييل I

أمثلة على كيفية استخدام سجلات الأخطاء في عمليات الحوادث

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

1.I المهاجم يرسل سلسلة اثنينية عشوائية إلى جهاز الحافة عبر بوابة إنترنت الأشياء (IoTGW)

يوضح الشكل 1.I مهاجماً يرسل سلسلة اثنينية عشوائية إلى وحدة MCU1 وردها. ويتعرف رأس السلسلة الاثنينية العشوائية "01000001" على الجهاز رقم 0001 والوظيفة رقم 0100. وبعبارة أخرى، يسعى المهاجم إلى مهاجمة الوظيفة رقم 0100 للجهاز رقم 0001. وتعجز وحدة MCU1 عن فهم سلسلة "3A459187F43CDDE5". لذلك فهي ترد بشفرة "000003FF (أمر غير معروف)" إلى الجهاز رقم 000 (بوابة إنترنت الأشياء (IoTGW)).



الشكل 1.I – المهاجم يرسل سلسلة اثنينية عشوائية إلى وحدة MCU1

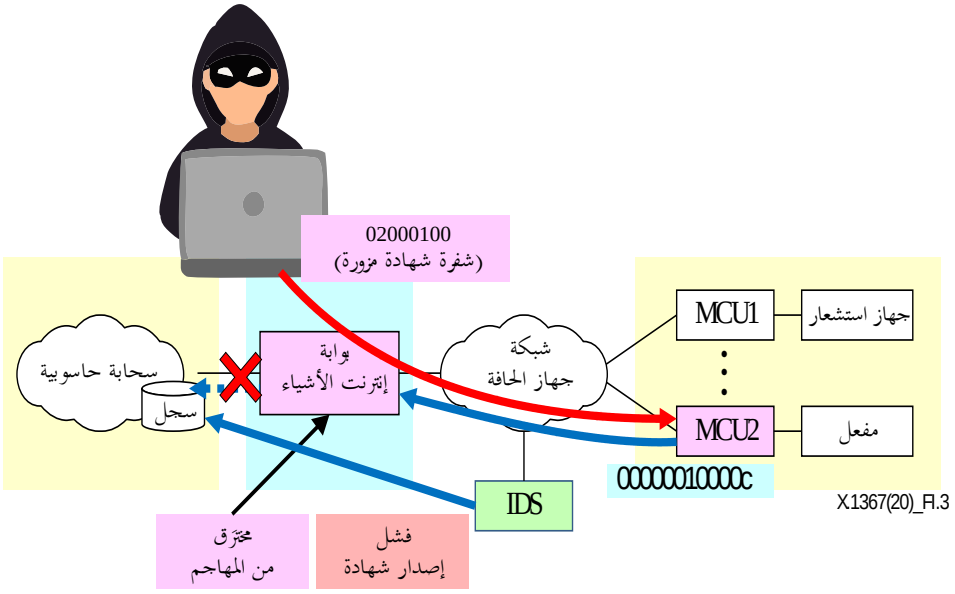
بعد أن تتلقى بوابة إنترنت الأشياء (IoTGW) سلسلة "000003FF" من وحدة MCU1، تنشئ بوابة إنترنت الأشياء السجل التالي وترسله إلى مخدِّم السجل في السحابة الحاسوبية. انظر الشكل 2.I.

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.2.11"},
    "Protocol": "ABC company protocol",
    "Requester": {
        "Unique ID": "0000",
        "Transmitted Code": "010000013A459187F43CdDE5"
    },
    "Responder": {
        "Unique ID": "0001",
        "Transmitted Code": "000003FF"
    },
    "Error Code": "30",
    "Error Message": "Invalid Command",
}
```

الشكل 2.I – (مثال) سجلات الأخطاء لإنترنت الأشياء بشأن طلب فاسد

2.I المهاجم يرسل شهادة غير صحيحة إلى جهاز الحافة عبر بوابة إنترنت الأشياء (IoTGW) مخترَق

يوضح الشكل 3.I مهاجماً يرسل شهادة غير صحيحة إلى وحدة MCU2 عبر بوابة إنترنت الأشياء (IoTGW) المخترق وردها. وتتبين وحدة MCU2 أن الشهادة غير صالحة. لذا، فإنها ترد بشفرة "00000010000c (خطأ التحقق من الشهادة)" إلى الجهاز رقم 0000 (بوابة إنترنت الأشياء (IoTGW)). ولكن بوابة إنترنت الأشياء مخترَق. وهو لن يرسل مطلقاً سجلات الأخطاء إلى مخدِّم السجل في السحابة الحاسوبية. ويرسل نظام كشف التسلل (IDS) سجلات الأخطاء لإنترنت الأشياء بدلاً من بوابة إنترنت الأشياء.



الشكل 3.I – المهاجم يرسل شفرة شهادة مزورة

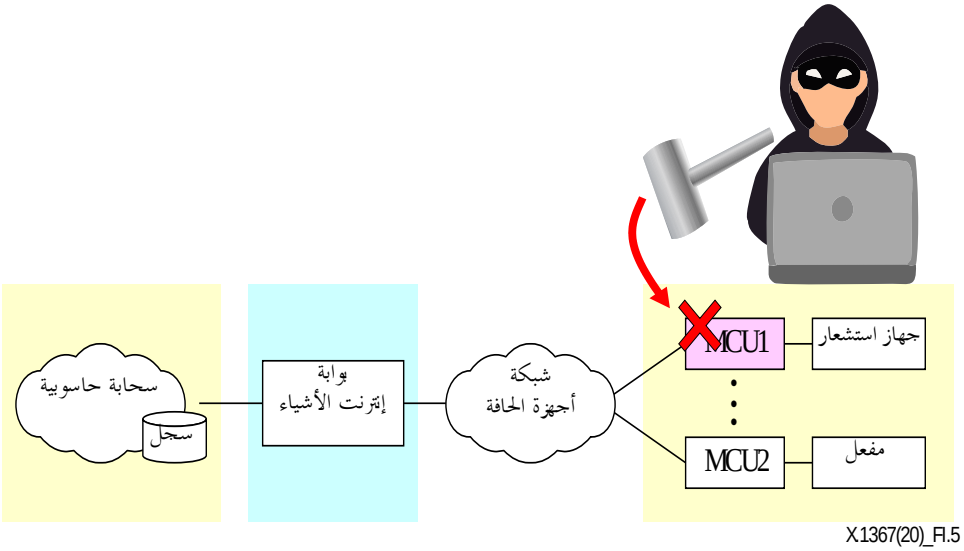
يرسل المهاجم شفرة شهادة مزورة إلى وحدة MCU2، لكن وحدة MCU2 تعجز عن التعرف عليها. لذا، ترسل وحدة MCU2 شفرة "00000010000c (خطأ التحقق من الشهادة)." وتتجاهل بوابة إنترنت الأشياء (IoTGW) رسالة الرد من وحدة MCU2، لأن المهاجم سبق أن اخترقها. ولكن إذا كان النظام مزوداً بنظام كشف تسلل (IDS)، ينشئ نظام كشف التسلل سجلات الأخطاء لإنترنت الأشياء في الشكل 4.I بدلاً من بوابة إنترنت الأشياء. وفي هذه الحالة، يقوم نظام كشف التسلل بدور المراسل.

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.100.249"},
    "Protocol": "EEE Company's protocol",
    "Requester": {
        "Unique Name": "0000",
        "Transmitted Code": "02000100... (Faked certification codes)"
    },
    "Responder": {
        "Unique Name": "0002",
        "Transmitted Code": "000000000010000c "
    },
    "Error Code": "21",
    "Error Message": "Certification Failed",
    "Description": {
        "Status": "This message was sent from IDS not IoTGW"
    },
}
```

الشكل 4.I – (مثال) سجلات الأخطاء لإنترنت الأشياء بشأن خطأ التحقق من الشهادة

3.I المهاجم يكسر فعلياً جهاز استشعار يرسل البيانات بانتظام دون أي طلب

يوضح الشكل 5.I مهاجماً يكسر فعلياً وحدة MCU1 ترسل البيانات بانتظام دون أي طلب. فلا يمكن لوحدة MCU1 إرسال أي بيانات بعد ذلك. وفي هذه الحالة، تكتشف بوابة إنترنت الأشياء (IoTGW) حالة غير طبيعية تتعلق بوحدة MCU1، وترسل سجلات الأخطاء لإنترنت الأشياء الموضح في الشكل 6.I.



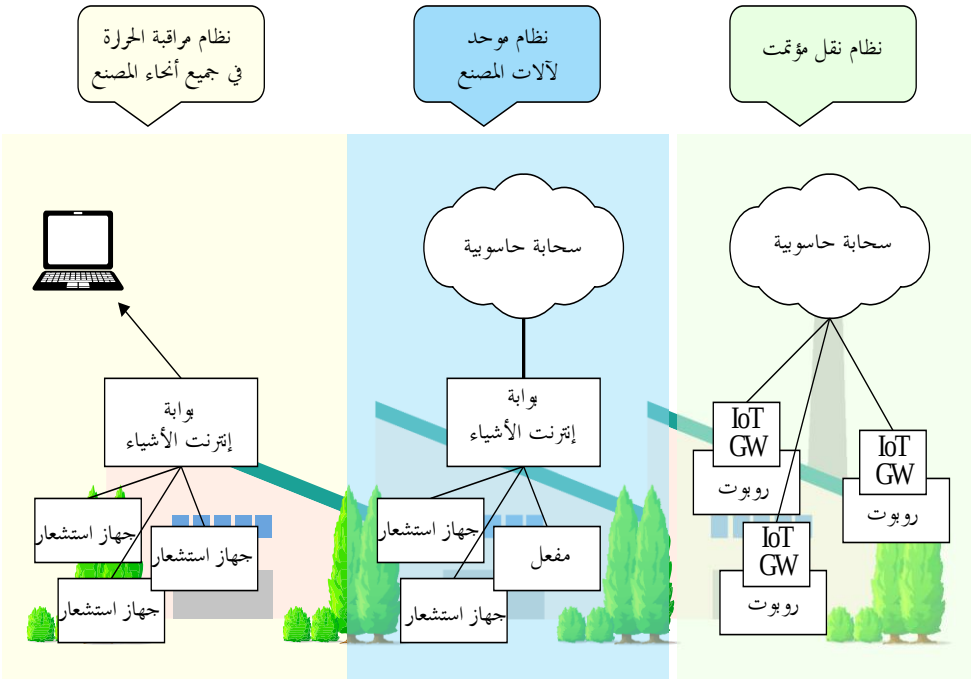
الشكل 5.I – المهاجم يكسر فعلياً وحدة MCU1

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.10.254"},
    "Protocol": "ZZZ Company's protocol",
    "Requester": {},
    "Responder": {
        "Unique Name": "0002",
        "Transmitted Code": ""
    },
    "Error Code": "11",
    "Error Message": "Communication Failed",
    "Description": {
        "Responder stopped sending data."
    },
}
```

الشكل 6.I – (مثال) إرسال سجلات الأخطاء لإنترنت الأشياء بشأن فقدان اتصال

4.I كيفية استخدام سجلات إنترنت الأشياء في التصدي لحادث

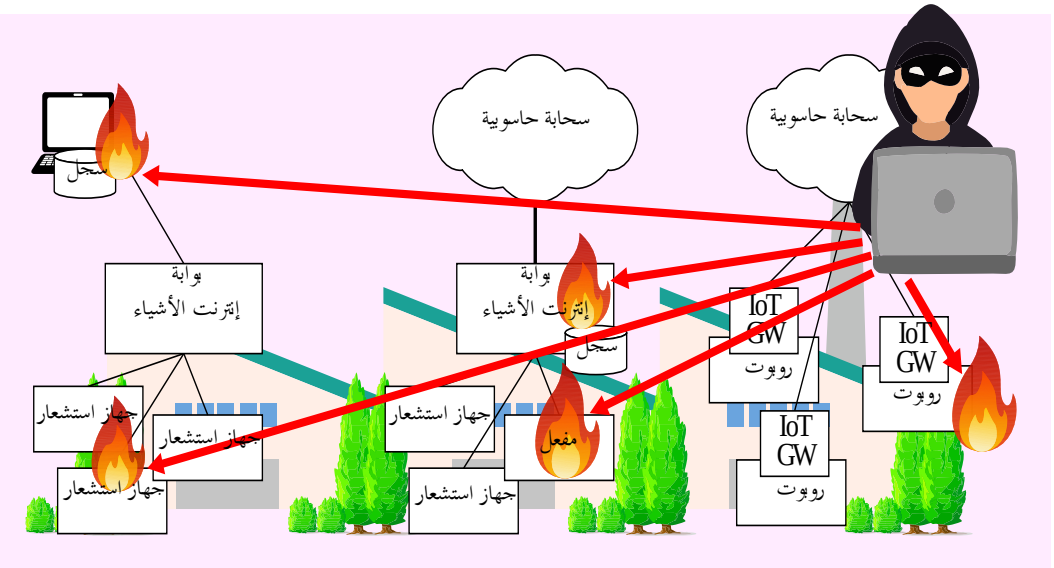
للمصنع ثلاثة أنظمة إيكولوجية لإنترنت الأشياء على نفس الشبكة المحلية (LAN) على النحو الموضح في الشكل 7.I.



X1367(20)_FI.7

الشكل 7.I – الأنظمة الإيكولوجية المتعددة لإنترنت الأشياء في مصنع

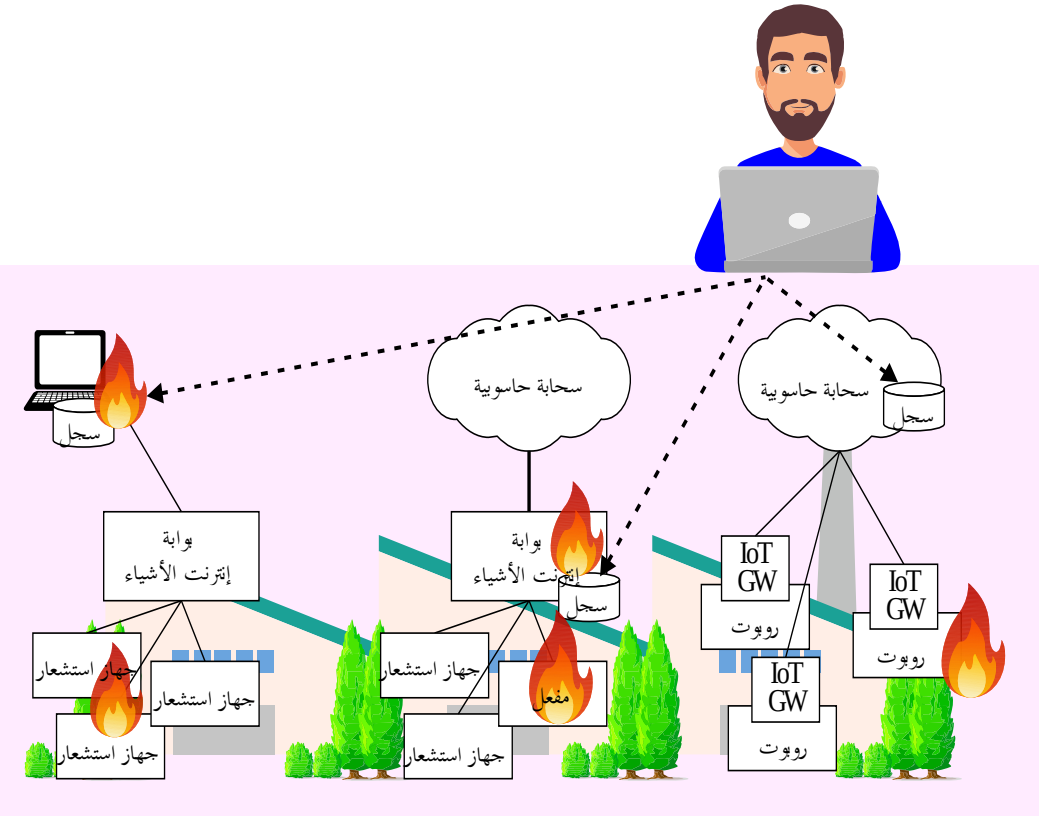
في هذه الحالة، يمكن للمهاجم أن يهاجم كل جهاز بسهولة، على النحو الموضح في الشكل 8.I. وإن لم تكن هناك سجلات الأخطاء لإنترنت الأشياء، يصعب على فريق التصدي للحوادث الأمنية (SIRT) اقتفاء آثار المهاجم، لأن الفريق لا يمكنه توحيد السجلات غير المقيَّسة لإنترنت الأشياء من كل نظام إيكولوجي لإنترنت الأشياء.



X1367(20)_FI.8

الشكل 8.I – المهاجم يستهدف جميع الأنظمة الإيكولوجية لإنترنت الأشياء في الوقت نفسه

إذا استخدمت هذه الأنظمة الإيكولوجية لإنترنت الأشياء النسق المقيَّس لسجلات الأخطاء لإنترنت الأشياء، يسهل على فريق التصدي للحوادث الأمنية (SIRT) توحيد جميع سجلات الأخطاء لإنترنت الأشياء على النحو الموضح في الشكل 9.I، بالإضافة إلى توحيد سجل النظام. ويمكن بعد ذلك اقتفاء آثار المهاجم.



X.1367(20)_FI.9

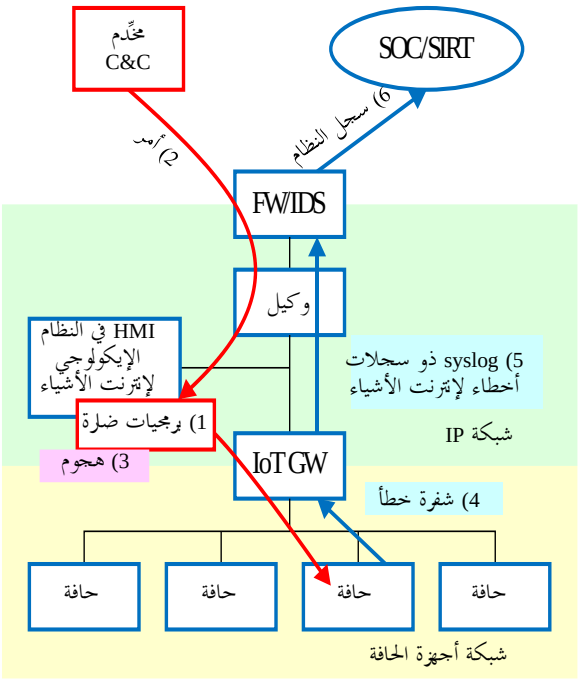
الشكل 9.I – توحيد وتحليل جميع سجلات الأخطاء لإنترنت الأشياء

التذييل II

التصدي للحوادث الأمنية المحتملة باستخدام سجلات الأخطاء لإنترنت الأشياء

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

يمكن استخدام النسق المقيَّس لسجلات الأخطاء لإنترنت الأشياء الموصوف في هذه التوصية للتصدي للحوادث الأمنية في النظام الإيكولوجي لإنترنت الأشياء. ويبين الشكل 1.II تدفق كشف الحوادث باستخدام سجلات الأخطاء لإنترنت الأشياء.



X.1367(20)_FII.1

الشكل 1.II – كشف الحوادث باستخدام سجلات الأخطاء لإنترنت الأشياء

(1) تصيب البرمجيات الضارة سطح التماس بين الإنسان والآلة (HMI)، من قبيل حاسوب شخصي مكتبي (PC)، بطريقة أو بأخرى.

(2) تتلقى البرمجيات الضارة أوامر من مخدِّم الأوامر والتحكم (C&C). ويجوز لجدار الحماية (FW) أو نظام كشف التسلل (IDS) أو الوكيل تسجيل سجل الاتصالات بين البرمجيات الضارة ومخدِّم الأوامر والتحكم (C&C).

(3) تبحث البرمجيات الضارة عن ثغرة في جهاز الحافة لإنترنت الأشياء. ويرسل جهاز الحافة لإنترنت الأشياء العديد من شفرات الأخطاء إلى بوابة إنترنت الأشياء (IoTGW)، لأن البرمجيات الضارة تحاول إرسال أوامر بمعلمات متنوعة بشكل متكرر. وتكاد معلماتها تكون غير صحيحة دائماً في جهاز الحافة لإنترنت الأشياء.

(4) ولكل شفرة الأخطاء لإنترنت الأشياء تُرسَل، ترسل بوابة إنترنت الأشياء (IoTGW) سجلات الأخطاء الإنترنت الأشياء بالنسق الموصَّف في هذه التوصية إلى جدار الحماية (FW) أو نظام كشف التسلل (IDS) باستخدام بروتوكول سجل النظام (syslog).

(5) ويرسل وكيل أيضاً سجلات الاتصالات باستخدام بروتوكول سجل النظام إلى جدار الحماية (FW) أو نظام كشف التسلل (IDS)، الذي يرسل جميع السجلات، بما في ذلك سجلات الأخطاء لإنترنت الأشياء، بواسطة بروتوكول سجل النظام إلى مركز العمليات الأمنية (SOC) أو فريق التصدي للحوادث الأمنية (SIRT).

وقد لا يرد محللو الأمن في مركز العمليات الأمنية (SOC) أو فريق التصدي للحوادث الأمنية (SIRT) على سجل واحد للأخطاء لإنترنت الأشياء لا يرتبط بسجلات الأخطاء لإنترنت الأشياء الأخرى. ولكنهم يمكن أن يلاحظوا وضعاً غير طبيعي إذا تلقى مركز العمليات الأمنية أو فريق التصدي للحوادث الأمنية عدداً كبيراً من سجلات الأخطاء لإنترنت الأشياء بشكل مستمر، لأن ذلك يمكن أن يعزى إلى مهاجم يبحث عن ثغرة في نظام إنترنت الأشياء.

وتتيح هذه التوصية لمحللي مركز العمليات الأمنية (SOC) أو فريق التصدي للحوادث الأمنية (SIRT) اكتشاف الهجمات على أجهزة جهاز الحافة لإنترنت الأشياء، لأن مركز العمليات الأمنية أو فريق التصدي للحوادث الأمنية يتلقى شفرات الأخطاء لإنترنت الأشياء بالنسق المقيَّس لسجلات الأخطاء لإنترنت الأشياء. وهم سيقومون عندئذ بالتحقق من السجلات الأخرى ذات الصلة، بما في ذلك الاتصالات بين البرمجيات الضارة ومخدِّم الأوامر والتحكم (C&C)، وبإبلاغ مشغِّل المصنع لفصل سطح التماس بين الإنسان والآلة (HMI) لذلك الحاسوب المكتبي عن الشبكة المحلية (LAN) أو إزالة البرمجيات الضارة منه.

بيبليوغرافيا

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

[b-ITU-T X.1277] Recommendation ITU-T X.1277 (2018), *Universal authentication framework*.

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of 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.4109] Recommendation ITU-T Y.4109/Y.2061 (2012), *Requirements for the support of machine-oriented communication applications in the next generation network environment*.

[b-ISO 8601-1] ISO 8601-1:2019, *Date and time – Representations for information interchange – Part 1: Basic rules*.

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

[b-ISO/IEC 14543-4-3] ISO/IEC 14543-4-3:2015, *Information technology – Home Electronic Systems (HES) architecture – Part 4-3: Application layer interface to lower communications layers for network enhanced control devices of HES Class 1*.

[b-ISO/IEC 17000] ISO/IEC 17000:2004, *Conformity assessment – Vocabulary and general principles*.

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

[b-IEEE 802.15.1] IEEE 802.15.1-2005, *IEEE Standard for information technology – Local and metropolitan area networks – Specific requirements – Part 15.1a: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPAN)*.

[b-IEEE 802.15.4] IEEE 802.15.4-2015, *IEEE Standard for low-rate wireless networks*.

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The syslog protocol*.

[b-oneM2M] oneM2M Partners (2017), Standards for M2M and Internet of things. Available [viewed 2020-02-12] at: http://www.onem2m.org/

[b-SPI] Motorola (2001), SPI block guide, V04.01. Available [viewed 2020-02-12] at: https://www.nxp.com/files-static/microcontrollers/doc/ref_manual/S12SPIV4.pdf

[b-UM10204] UM10204 (2014), *I^2C-bus specification and user manual*, Rev.6.Available[viewed 2020-02-12] at: https://www.nxp.com/docs/en/user-guide/UM10204.pdf

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