الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1376

(2021/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة (2) – أمن أنظمة النقل الذكية (ITS)

آلية كشف سوء السلوك من الناحية الأمنية باستخدام البيانات الضخمة بشأن المركبات الموصولة

التوصية ITU-T X.1376

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
مولد 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.1376

آلية كشف سوء السلوك من الناحية الأمنية باستخدام البيانات الضخمة بشأن المركبات الموصولة

ملخص

وتصف التوصية ITU-T X.1376 آلية كشف سوء السلوك من الناحية الأمنية بشأن المركبات الموصولة، بهدف مساعدة أصحاب المصلحة في استعمال بيانات السيارات من أجل تحسين أمن المركبات.

مع تزايد توصيلية المركبات، يتزايد عدد نقاط الضعف بسبب تطور التكنولوجيا المعقدة. وتجلب نقاط الضعف هذه المزيد من التهديدات للمركبات الموصولة. ومن المفيد جداً تحليل كمية كبيرة من بيانات السيارات، من أجل تقييم أمن المركبات الموصولة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1376	2021-01-07	17	11.1002/1000/14448

مصطلحات أساسية

المركبات الموصولة، كشف سوء السلوك.

* 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/البرمجيات 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 المناسبة الخاصة بقطاع تقييس الاتصالات (ITU-T) المتاحة عبر الموقع الإلكتروني لقطاع تقييس الاتصالات في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1376

آلية كشف سوء السلوك من الناحية الأمنية باستخدام البيانات الضخمة بشأن المركبات الموصولة

1 مجال التطبيق

تصف هذه التوصية آلية كشف سوء السلوك من الناحية الأمنية بشأن المركبات الموصولة. وتتضمن الآلية الخطوات التالية:

أ) التقاط البيانات. وهو توصيف أنواع البيانات والمعلومات التي يمكن الحصول عليها من مصادر مختلفة لكشف سوء السلوك، بما فيها السيارات والبنية التحتية والجهات المصنعة للمعدات الأصلية (OEM) والموردون. ولا يشمل مجال تطبيق هذه التوصية أساليب وإجراءات التقاط البيانات.

ب) الكشف. تحليل البيانات الملتقَطة لاكتشاف سوء السلوك.

وتنطبق هذه التوصية على المركبات الموصولة كي يكشف المصممون ومقدمو الحلول الأمنية سوء السلوك. ولا يشمل مجال تطبيق هذه التوصية أساليب استخدام التبليغ.

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 إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

3 التعاريف

1.3 مصطلحات معرَّفة في مصادر أخرى

لا توجد.

2.3 مصطلحات معرَّفة في هذه التوصية

تعرف هذه التوصية المصطلح التالي:

1.2.3 سوء السلوك: فعل تقديم بيانات خاطئة أو مضللة، والعمل بطريقة تعيق متلقي الخدمة الآخرين أو العمل خارج النطاق المجاز. وقد ينشأ سوء السلوك عن مكونات داخلية أو خارجية لنظام المركبة.

الملاحظة 1 – على أساس المعيار [b-ISO/TR 17427-4].

الملاحظة 2 – سوك السلوك يشمل السلوك المشبوه كما في أنواع الرسائل أو الترددات الخاطئة، وعمليات تسجيل الدخول غير الصالحة والنفاذ غير المجاز، أو الرسائل الموقَّعة أو المجَّفرة بشكل غير سليم، وما إلى ذلك، سواء كان ذلك بقصد أو بغير قصد.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

ADAS أنظمة مساعدة السائق المتقدمة *(Advanced Driver-Assistance Systems)*

ABS نظام الكبح المانع للانزلاق *(Anti-skid Braking System)*

AEB الكبح المستقل في حالات الطوارئ *(Autonomous Emergency Braking)*

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

CAN شبكة منطقة وحدة التحكم *(Controller Area Network)*

GNSS النظام العالمي للملاحة الساتلية *(Global Navigation Satellite System)*

ITS نظام النقل الذكي *(Intelligent Transportation System)*

IP بروتوكول الإنترنت *(Internet Protocol)*

LiDAR الليدار أو كشف الأهداف وتحديد المدى ضوئياً *(Light Detection and Ranging)*

MCU وحدة التحكم الصغرية *(Microcontroller Unit)*

OEM جهة مصنعة للمعدات الأصلية *(Original Equipment Manufacturer)*

TCU وحدة تحكم تليماتية *(Telematics Control Unit)*

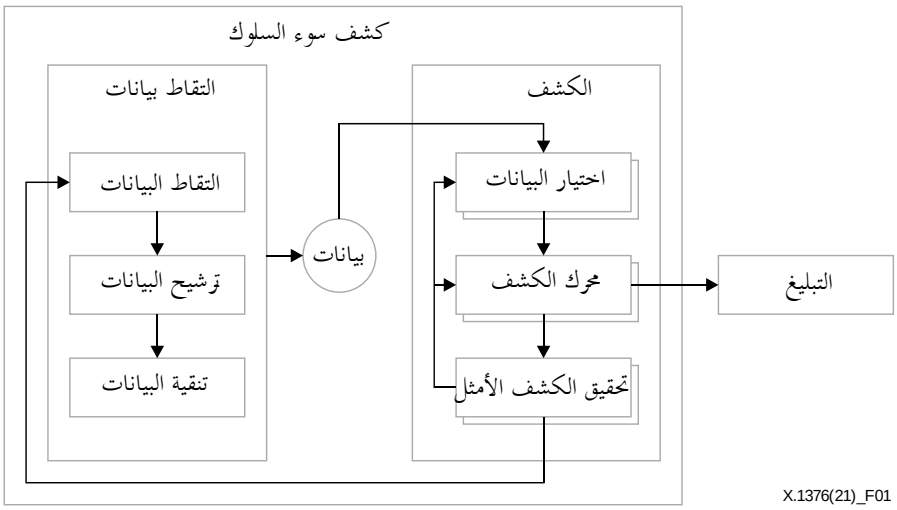
URL محدد موقع الموارد الموحّد *(Uniform Resource Locator)*

5 الاصطلاحات

لا توجد.

6 نموذج آلية كشف سوء السلوك

يقدم الشكل 1 نموذجاً لآلية كشف سوء السلوك بشأن المركبات الموصولة. وتتضمن الآلية خطوتين هما التقاط البيانات وكشفها، وينفذها نظامان.



الشكل 1 – نموذج آلية كشف سوء السلوك

نظراً لأن مجال تطبيق هذه التوصية لا يشمل أساليب وإجراءات التقاط البيانات، فإن نظام التقاط البيانات (مثل ترشيح البيانات وتنقية البيانات) في الشكل 1 هو مجرد مثال إعلامي على التنفيذ العملي لكشف سوء السلوك.

وتُرسَل البيانات من نظام الالتقاط إلى نظام الكشف، ويعالَج التقاط البيانات وفقاً للأنواع الموضحة في الفقرة 7.

ويتضمن نظام التقاط البيانات الوحدات التالية:

أ) جمع البيانات: هو جمع البيانات لكشفها من مصادر مختلفة، مثل مقدم الخدمة ونظام جسم المركبة وأجهزة الاستشعار؛

ب) ترشيح البيانات: هو ترشيح البيانات الملتقطة بناءً على تصنيف البيانات؛

ج) تنقية البيانات: تُجرى للبيانات الملتقطة عمليات إزالة البيانات المكررة وتقليل الضوضاء.

ويتضمن نظام كشف البيانات الوحدات التالية:

أ) اختيار البيانات: تُختار مجموعات البيانات بناءً على أساليب مختلفة لكشف سوء السلوك، ثم تُرسَل إلى محرك الكشف؛

ب) محرك الكشف: يُكشف سوء السلوك بناءً على أساليب الكشف، ثم تُرسَل نتائج القرارات إلى الإعداد الأمثل والتبليغ، حسب الاقتضاء؛

ج) الإعداد الأمثل: تُستخدم نتائج الكشف من محرك الكشف لتحسين اختيار البيانات ومحرك الكشف والتقاط البيانات.

والتبليغ هو وحدة نمطية تقوم بإرسال المخرجات من محرك الكشف إلى أصحاب المصلحة. ولا يشمله مجال تطبيق هذه التوصية.

7 التقاط البيانات

التقاط البيانات يتضمن عادةً التقاط البيانات وتنقية البيانات وترشيح البيانات. ونظراً لأن أساليب وإجراءات التقاط البيانات لا يشملها مجال تطبيق هذه التوصية، لا توصَّف سوى أنواع البيانات المستخدمة في إجراء الكشف. وتنبغي حماية أي بيانات شخصية حساسة باستخدام التكنولوجيات المناسبة مثل إغفال الهوية، وهي غير مشمولة بمجال تطبيق هذه التوصية.

واستناداً إلى البيانات والمعلومات الملتقَطة من مصادر مختلفة، توصِّف هذه الفقرة الأنواع المستخدمة في آلية كشف سوء السلوك، وهي بيانات الحالة وبيانات التحكم والبيانات الاستخباراتية، على النحو الموضح في الجدول 1.

الجدول 1 – أنواع البيانات

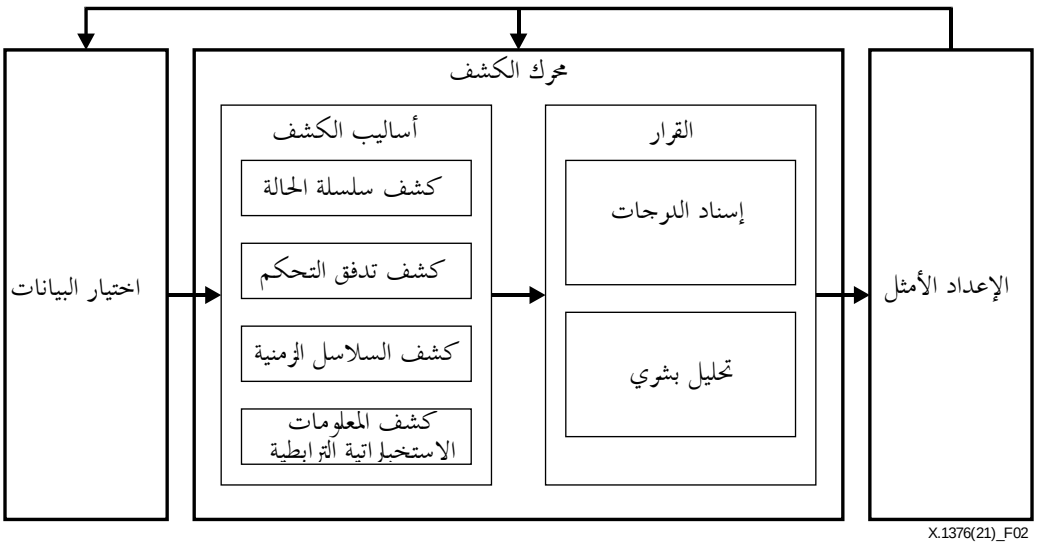
النوع	النوع الفرعي	مصادر البيانات	أمثلة البيانات
بيانات الحالة[أ]	بيانات التطبيق أو بيانات الخدمة	مقدم المحتوى أو مقدم الخدمة	بيانات المعلومات والترفيه
		بيانات خدمة الخرائط	الملاحة، تحديد الموضع
		بيانات التطبيقات المتنقلة	البيانات المتعلقة بالتطبيق
	حالة المركبة	نظام السلامة	نظام الكبح المانع للانزلاق (ABS)، وسادة هوائية، الكبح المستقل في حالات الطوارئ (AEB)، أنظمة مساعدة السائق المتقدمة (ADAS)
		نظام جسم المركبة	الأبواب، النوافذ، ممسحة الزجاج
		نظام هيكل المركبة	عزم الدوران، الزاوية
		نظام القدرة	السرعة، سرعة دوران المحرك، صمام الخانق، حالات التوقف المفاجئ
	أجهزة الاستشعار البيئية	الرادار	رادار الموجات المليمترية
		كشف الأهداف وتحديد المدى ضوئياً (LiDAR)	مجموعة نقاط بيانات في الفضاء
		أجهزة الاستشعار بالموجات فوق الصوتية (ITS)	المسافة
		كاميرا	الصورة المحيطة
		أجهزة استشعار أنظمة النقل الذكية (ITS)	علامة مَرافق على جانب الطريق

الجدول 1 – أنواع البيانات

النوع	النوع الفرعي	مصادر البيانات	أمثلة البيانات
بيانات التحكم[ب]	التحكم المحلي	وحدة التحكم داخل المركبة	فتح الباب، غلق الباب
	التحكم عن بُعد	الأتمتة، التليماتية	التشخيص عن بُعد
البيانات الاستخباراتية[ج]	البيانات الاستخباراتية الداخلية	بحث أمني، اختبار النتائج	نقاط الضعف، الأخطاء البرمجية، أحداث الأمن السيبراني الداخلية
	بيانات تناقل المعلومات الاستخباراتية الخارجية	العميل، المورد، المجتمع، المؤتمرات أو الأدبيات، الإنترنت	عنوان بروتوكول الإنترنت (IP)، قيم الاختزالات، موقع الموارد الموحّد (URL)، اسم الميدان، مواطن الضعف والتعرض الشائعة (CVE) وما إلى ذلك.
[أ] البيانات والمعلومات المتعلقة بحالة المركبات والتطبيقات والخدمات وأجهزة الاستشعار والمرافق الأخرى في نظام نقل ذكي. [ب] البيانات والمعلومات المستخدمة للتحكم في المركبات والتطبيقات والخدمات وأجهزة الاستشعار والمرافق الأخرى في نظام نقل ذكي. [ج] البيانات والمعلومات المتعلقة بالأمن السيبراني التي حُصل عليها من خارج نظام نقل ذكي. ويُفترض وجود المستوى الصحيح من السلامة لدى مصادر البيانات.			

8 الكشف

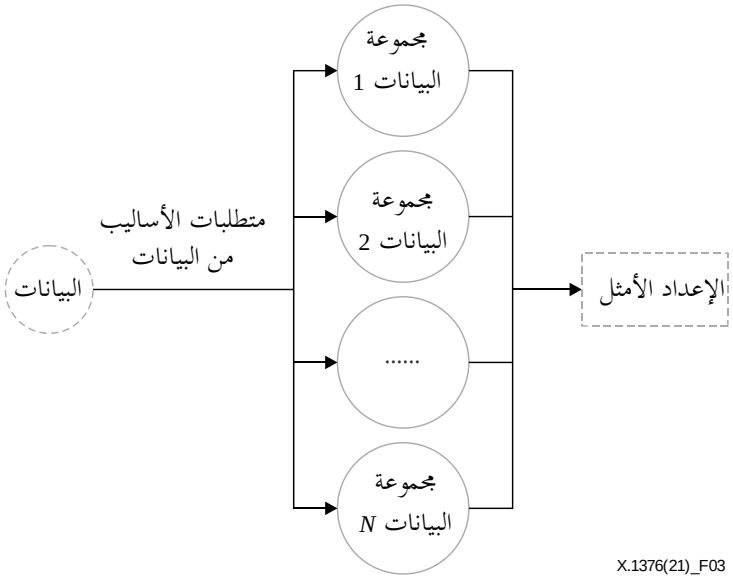
تتكون وحدة الكشف بشكل أساسي من اختيار البيانات ومحرك الكشف والإعداد الأمثل. وعلى النحو المبين في الشكل 2، يستخدم محرك الكشف، استناداً إلى بيانات ومعلومات من مصادر مختلفة، تحليل البيانات الضخمة لتحديد سوء السلوك. ويستخدم الإعداد الأمثل السلوكيات الخاطئة لاختيار البيانات الأمثل، ويعزز محرك الكشف دقة وكفاءة كشف سوء السلوك.



الشكل 2 – إجراء الكشف

1.8 اختيار البيانات

بناءً على متطلبات البيانات المختلفة من أساليب الكشف، تقوم الوحدة النمطية لاختيار البيانات بتصنيف البيانات في مجموعات بيانات مختلفة وفقاً لمتطلبات محركات الكشف، على النحو الموضح في الشكل 3. والمدخلات في الوحدة النمطية لاختيار البيانات هي بيانات من نظام الالتقاط.



الشكل 3 – إجراء اختيار البيانات

2.8 محرك الكشف

يتكون محرك الكشف من وحدتين نمطيتين فرعيتين: أساليب الكشف والقرار. وعندما تدخل مجموعات البيانات في الوحدة النمطية الفرعية لأساليب الكشف، ستحولها الأساليب إلى سمات سلوكية. ثم تتخذ الوحدة النمطية الفرعية للقرار قراراً بناءً على سمات السلوك. ولنتائج القرار ثلاثة أشكال مختلفة: محظورة؛ ومشبوهة؛ ومسموح بها. والنتيجة المحظورة تعني أنها غير مألوفة؛ أما النتيجة المشبوهة فهي تعني تعذر تحديد ما إذا كانت البيانات مرفوضة أم آمنة؛ وأما النتيجة المسموح بها فهي تعني أن البيانات آمنة.

1.2.8 أساليب الكشف

الوحدة النمطية الفرعية لأساليب الكشف هي مجموعة من أساليب الكشف المختلفة. واستناداً إلى أنواع البيانات المصنفة في الفقرة 7، صُممت أربعة أساليب لكشف سوء السلوك باستخدام هذه البيانات.

1.1.2.8 كشف سلسلة الحالة

تحتوي سلسلة الحالة على سلسلة من بيانات الحالة المتلازمة. وفي سلسلة الحالة، يؤدي التغيير في أحد البيانات إلى تغيير البيانات الأخرى في نفس الوقت.

وفيما يلي بعض خصائص سلسلة الحالة:

أ) العقدة: خدمة أو تطبيق في أنظمة النقل الذكية على صلة بإجراء ما؛

ب) التدفق: اتجاه ومسار تغيير البيانات بفعل إجراء ما.

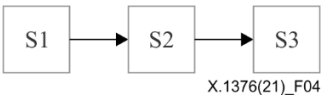
وتتولد بيانات الحالة في نظام النقل الذكي ويمكن إنشاء سياق بهذه البيانات. وتتبع قيم البيانات أيضاً اتجاهاً معيناً وتتقلب ضمن مدى معين.

وفي الأساس، يمكن تقسيم سلسلة الحالة إلى نموذجين: خط وفرع. والنموذجان هما كالتالي:

1) الخط: كل عقدة لها عقدة واحدة حصراً تستقبل إشارتها؛

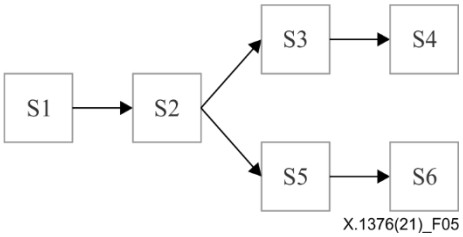
2) الفرع: تنشئ العقدة الواحدة بياني حالة أو أكثر في نفس الوقت، ثم ترسلها إلى عقد مختلفة.

وفي نموذج الخط لسلسلة الوضع، يكون للعقد توصيل أحادي الاتجاه حصراً. انظر الشكل 4.



الشكل 4 – نموذج الخط لسلسلة الحالة
S: الحالة

وفي نموذج الفرع لسلسلة الحالة، يمكن تفريع العقد إلى نموذجين أو أكثر من نماذج الخط ذات الصلة. انظر الشكل 5.



الشكل 5 – نموذج فرع لسلسلة الحالة

وبالتالي، تشمل سمات كل عقدة ما يلي:

'1' السياق في سلسلة الحالة؛

'2' قيمة واتجاه كل عقدة.

ويُحصل على السمات من العقد في سلسلة الحالة، ثم تُرسَل إلى وظيفة إسناد الدرجات.

2.1.2.8 كشف تدفق التحكم

يحتوي تدفق التحكم على سلسلة من بيانات التحكم المتلازمة. وفي تدفق التحكم، يمكن أن يتكون أمر تحكم واحد من عدة أوامر تحكم فرعية ويؤثر على أنظمة متعددة.

وفيما يلي بعض خصائص تدفق التحكم لوصف تنفيذ أمر التحكم:

أ) العقدة: خدمة أو تطبيق في أنظمة النقل الذكية على صلة بإجراء ما؛

ب) التدفق: اتجاه ومسار تغيير البيانات بفعل إجراء ما.

وعندما يبدأ إجراء التحكم، ستمر البيانات المتعلقة بالتحكم عبر العقد المتعلقة بالتحكم وتشكل تدفق تحكم.

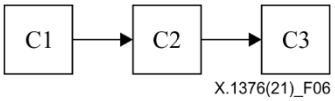
وتعمل كل عقدة تحكم بشكل مستقر ومنتظم في نظام النقل الذكي. وعندما تعمل العديد من العقد معاً، يكون تدفق التحكم مستقراً أيضاً في السلوك، بسبب الفترة المحددة للرسائل والأنواع المحددة لها وعددها.

وفي الأساس، يمكن تقسيم تدفق التحكم إلى نموذجين: خط وفرع. والنموذجان هما كالتالي:

1) الخط: كل عقدة لها عقدة واحدة حصراً تستقبل إشارتها؛

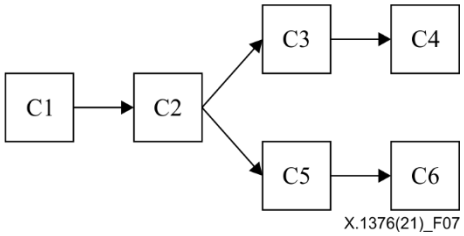
2) الفرع: تنشئ العقدة الواحدة بياني تحكم أو أكثر في نفس الوقت، ثم ترسلها إلى عقد مختلفة.

وفي نموذج الخط لتدفق التحكم، يكون للعقد توصيل أحادي الاتجاه حصراً. انظر الشكل 6.



الشكل 6 – نموذج الخط لتدفق التحكم
C: التحكم

وفي نموذج الفرع لتدفق التحكم، يمكن تفريع العقد إلى نموذجين أو أكثر من نماذج الخط ذات الصلة. انظر الشكل 7.



الشكل 7 – نموذج الفرع لتدفق التحكم

3.1.2.8 كشف السلاسل الزمنية

تُستخدم السلاسل الزمنية لوصف البيانات التي تتغير وفقاً للنوع. وطالما التزمت البيانات بالأنواع، يمكن استخدام كشف السلاسل الزمنية.

وللاتجاه المتغير لبيانات السلاسل الزمنية أربعة أنواع:

أ) الميل: تتغير البيانات مع الوقت أو مع متغيرات مستقلة، فتُظهر اتجاهاً بطيئاً وطويل الأجل نسبياً ذا الطبيعة نفسها في استمرارية الارتفاع والهبوط والمراوحة في المكان، لكن قد لا يتساوى مدى التغيير؛

ب) الدورية: هي عامل يُظهر تدريجياً خصائص متكررة بمرور الوقت، بما في ذلك الذرى والقيم الدنيا؛

ج) العشوائية: تتغير البيانات عشوائياً، لكن الوضع العام يظل إحصائياً؛

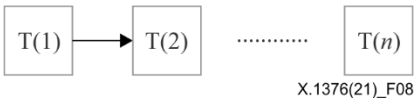
د) التراكب: التغيير الفعلي هو تراكب أو توليفة من عدة تغييرات.

وفيما يلي بعض خصائص سلوك السلاسل الزمنية:

1) العقدة: خدمة أو تطبيق في أنظمة النقل الذكية على صلة ببيانات السلاسل الزمنية؛

2) التدفق: يشير إلى الوقت بالترتيب الزمني.

وتنتمي العديد من البيانات إلى بيانات السلاسل الزمنية، مثل رسائل شبكة منطقة وحدة التحكم (CAN). ويمكن إنشاء نموذج بيانات مع نوع واحد أو أكثر من البيانات لاكتشاف سوء السلوك. انظر الشكل 8.



الشكل 8 – نموذج الخط للسلاسل الزمنية
T: الزمن

4.1.2.8 كشف المعلومات الاستخباراتية الترابطية

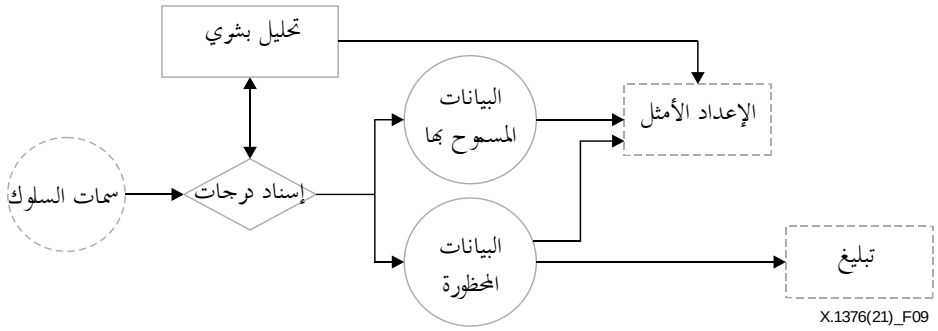
بأسلوب كشف المعلومات الاستخباراتية الترابطية، يمكن كشف سوء السلوك بشكل مباشر أو غير مباشر. لذلك يمكن تقسيم البيانات الاستخباراتية الترابطية إلى فئتين: مباشرة وغير مباشرة.

المعلومات الاستخباراتية الترابطية المباشرة: يمكن كشف سوء السلوك بشكل مباشر بناءً على هذه المعلومات الاستخباراتية، من قبيل تقرير نقاط الضعف الخارجية، وبحوث الأمن السيبراني الداخلي، وكشف نقاط الضعف الشائعة.

المعلومات الاستخباراتية الترابطية غير المباشرة: لا يمكن كشف سوء السلوك بشكل مباشر بناءً على هذه المعلومات الاستخباراتية، حيث تُستخدم هذا المعلومات الاستخباراتية لوصف الأحداث العادية، مثل إصلاح الأخطاء البرمجية وإصدار ميزة جديدة وتحديث البرمجيات وتبديل الشريحة. وبالجمع بين المعلومات الاستخباراتية الترابطية غير المباشرة والبيانات الأخرى الملتقَطة، يمكن كشف سوء السلوك.

2.2.8 القرار

تعرِّف هذه الفقرة بإجراءات الوحدة النمطية الفرعية للقرار الموضحة في الشكل 9.

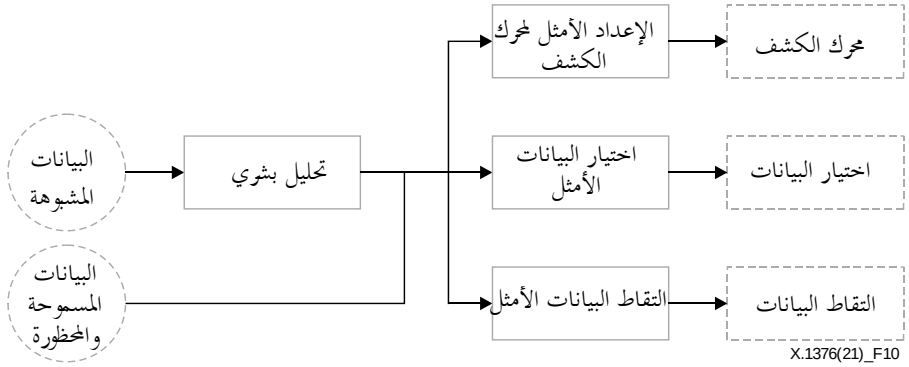


الشكل 9 – الإجراء في الوحدة الفرعية للقرار

تُستخدم الوحدة النمطية الفرعية للقرار لتحديد النتائج من أساليب الكشف. وهي تشمل وظيفتين: إسناد الدرجات والتحليل البشري. وتحدد وظيفة إسناد الدرجات أنواع البيانات حسب سمات السلوك، ثم تسند درجات إليها. وإذا حدث سوء سلوك مثل هجوم للاختطاف أو العبث، فإنها تنحرف عن خط أساس الاستقرار. وإذا لم تستوف الدرجة عتبة المسموح به أو المحظور، فسيُصنف السلوك على أنه مشبوه. وسيتدخل المحللون البشريون بعد ذلك ويساعدون في اتخاذ قرار حتى تستوفي الدرجة عتبة المسموح به أو المحظور.

3.8 الإعداد الأمثل

الإعداد الأمثل هو عبارة عن وحدة نمطية للردود التقييمية، تتلقى البيانات من محرك الكشف وتستخدمها لتحسينها. انظر الشكل 10.



الشكل 10 – الإجراء في الإعداد الأمثل

1.3.8 الإعداد الأمثل لمحرك الكشف

السمة هي القيمة الأساسية في كل بيان يُرسَل في التدفق. وفي بداية كشف سوء السلوك، تتولد خطوط أساس الاستقرار بالسمات العادية من البيئة العادية. وتتهيأ وظيفة إسناد الدرجات.

ويتحقق محرك الكشف الأمثل من خلال مخرجاته. فتضاف أساليب الكشف أو تُعدَّل أو تُحذَف لتحسين كفاءة الكشف؛ وتتحقق الوظيفة المثلى لإسناد الدرجات أيضاً من خلال إضافة معارف جديدة مستمدة من التحليل البشري.

2.3.8 اختيار البيانات الأمثل

تضاف مجموعات البيانات أو تُعدَّل أو تُحذَف لتحسين دقة الكشف.

3.3.8 التقاط البيانات الأمثل

تضاف البيانات الملتقَطة أو تُعدَّل أو تُحذَف لتحسين دقة الكشف.

التذييل I

حالات استخدام أساليب الكشف المختلفة

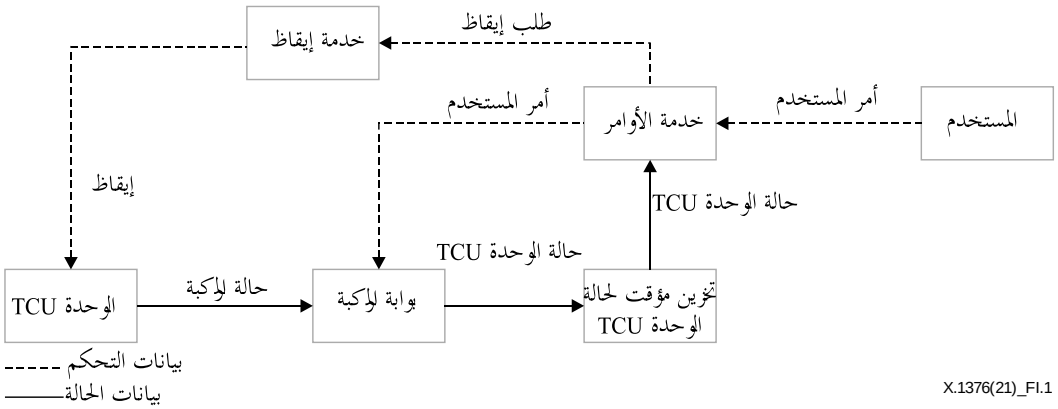
(لا يشكل هذا التذييل جزءاً من هذه التوصية.)

يقدم هذا الملحق حالات استخدام لكيفية اكتشاف سوء السلوك وفقاً لأساليب الكشف المختلفة المذكورة في الفقرة 1.2.8.

1.I حالة استخدام لسلسلة الحالة

هذه حالة كشف لسلسلة الحالة للفقرة 1.1.2.8.

تحتوي مركبة على وحدة اتصالات نمطية للنفاذ إلى الإنترنت تسمى وحدة تحكم تليماتية (TCU). ولا تشغَّل وحدة التحكم التليماتية طوال الوقت، لذلك فهي تبدل إلى أسلوب القدرة المنخفضة بعد إيقاف محرك المركبة لتوفير الطاقة. وقبل أسلوب القدرة المنخفضة، ترسل وحدة التحكم التليماتية حالة المركبة إلى بوابة المركبة (خدمة الطرف الخلفي) التي تزامن هذه الحالة مع ذاكرة التخزين المؤقت لوضع وحدة التحكم التليماتية. ثم تحصل خدمة الأوامر على هذا الوضع من ذاكرة التخزين المؤقت لحالة وحدة التحكم التليماتية. وعندما يرسل المستخدم أمراً إلى مركبته، تتفاعل خدمة الأوامر وفقاً لحالة وحدة التحكم التليماتية. وإذا كانت وحدة التحكم التليماتية في وضع القدرة المنخفضة، ترسل خدمة الأوامر طلباً إلى خدمة الإيقاظ التي توقظ بدورها وحدة التحكم التليماتية. ويوضح الشكل 1.I السلوك العادي. ويوضح الجدول 1.I بيانات الحالة المشمولة في هذا السلوك العادي.



الشكل 1.I – سلسلة وضع السلوك العادي

عندما يرغب المهاجمون في اكتشاف هذا الإجراء، سيحاولون تعديل حالة وحدة التحكم التليماتية (TCU) لرؤية السلوكيات المختلفة التي تبديها خدمة الأوامر. وسيكون هناك بعد ذلك فرق بين ذاكرة التخزين المؤقت لحالة وحدة التحكم التليماتية وبوابة المركبة.

وفي هذه الحالة، يمكن لكشف سلسلة الحالة اكتشاف سوء السلوك من خلال مقارنة حالة المركبة في بوابة المركبة بحالة وحدة التحكم التليماتية (TCU) في ذاكرة التخزين المؤقت لحالة وحدة التحكم التليماتية. وإذا وجد اختلاف، فهذا سوء سلوك. ولا يمكن أن تعمل وحدة التحكم التليماتية بأسلوب القدرة المنخفضة عندما تكون المركبة قيد التشغيل.

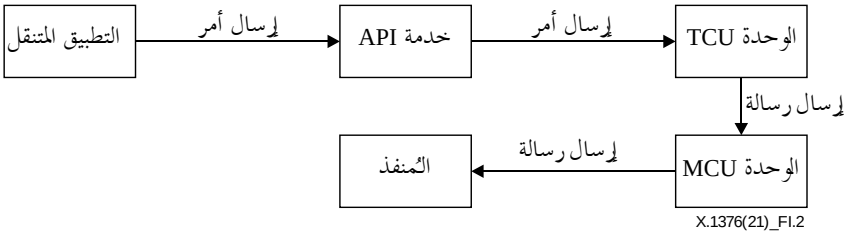
الجدول 1.I – بيانات وضع قيادة المركبة

العقدة	البيانات
بوابة المركبة	حالة المركبة
التخزين المؤقت لحالة الوحدة TCU	حالة الوحدة TCU
خدمة الأوامر	حالة الوحدة TCU

2.I حالة تدفق التحكم

هذه حالة كشف لتدفق التحكم بالفقرة 2.1.2.8.

عندما يريد المستخدم التحكم في المركبة عن بُعد، تقتضي الضرورة استخدام التطبيق المثبت على الهاتف الذكي للمستخدم لتشغيل هذه الوظيفة. وسيقوم التطبيق بإنشاء سجل التشغيل. ثم سيرسل التطبيق طلباً إلى خدمة السطح البيني لبرمجة التطبيقات (API)، في الطرف الخلفي، التي ستسجل هذا الطلب في سجل النفاذ. وستقوم خدمة السطح البيني لبرمجة التطبيقات بعد ذلك بمعالجة أولية للطلب وإعادة توجيهه إلى النقطة الطرفية للمركبة، من قبيل وحدة التحكم التليماتية (TCU) التي ستستدعي وحدة التحكم الصغرية (MCU) بجهاز مرسِل–مستقبِل وسترسل أمراً إلى المنفذ ذي الصلة. وأخيراً، سيقوم المفعِّل بتنفيذ أمر التحكم من جانب المستخدم. انظر الشكل 3.I. ويوضح الجدول 2.I بيانات التحكم المشمولة في هذا السلوك العادي.



الشكل 2.I – السلوك العادي لتدفق التحكم

في هذه الحالة، لا ترسل وحدة التحكم التليماتية (TCU) رسائل إلى وحدة التحكم الصغرية (MCU) إلا عندما تطلبها خدمة السطح البيني لبرمجة التطبيقات (API). وفي حال استدعاء وحدة التحكم الصغرية من مسار غير مألوف، لن يكون هناك سجل تشغيل في التطبيق المتنقل وخدمة السطح البيني لبرمجة التطبيقات. وعندئذ يُكشف سوء السلوك.

الجدول 2.I – بيانات التحكم في التليماتية

العقدة	البيانات
التطبيق المتنقل	سجل التشغيل
خدمة API	سجل النفاذ
TCU	البيانات المستقبَلة
MCU	سجل الاستدعاء
المنفذ	سجل المنفذ

3.I حالة السلاسل الزمنية

هذه حالة كشف للسلاسل الزمنية للفقرة 3.1.2.8.

وفي هذه الحالة، ترسل وحدة التحكم التليماتية (TCU) موضع المركبة إلى خدمة الطرف الخلفي بشكل دوري. انظر الشكل 3.I.

الفاصل الزمني (بالثواني)	خط العرض (º)
10.4015592431	39.9544
10.2439587253	39.9566
10.5735141799	39.9594
10.3234362303	39.9502
10.0973092011	39.9528
10.5066656864	39.9538
10.4945798327	39.9558
10.1209659368	39.9556
10.2163646279	39.9506
10.1042228459	39.9551

الشكل 3.I – السلسلة الزمنية العادية للموضع

إذا كان جهاز استشعار النظام العالمي للملاحة الساتلية (GNSS) في حالة انتحال، ستختلف معلومات الموضع والفاصل الزمني اختلافاً واضحاً عن البيانات السابقة. انظر الشكل 4.I.

الفاصل الزمني (بالثواني)	خط العرض (º)
10.4741553595	39.9503
10.2682504585	39.9595
10.2750387130	39.9597
10.4752930715	39.9568
10.6371744699	39.9520
5.4110037357	45.1525
5.5768263688	39.9597
10.4367481108	39.9508
10.0731090275	39.9550
10.5550728359	39.9529
10.5853553005	39.9518
10.1983262711	39.9554

الشكل 4.I – السلسلة الزمنية لسوء سلوك الموضع

ويوضح الجدول 3.I بيانات السلاسل الزمنية الشائعة في المركبة.

الجدول 3.I – بيانات السلاسل الزمنية لجهاز الاستشعار المؤتمت

العقدة	البيانات
خدمة الطرف الخلفي	خط العرض، الفاصل الزمني

4.I حالة كشف المعلومات الاستخباراتية الترابطية

هناك حالتان كشف للمعلومات الاستخباراتية الترابطية للفقرة 4.1.2.8، لذلك ترد حالتان من حالات الاستخدام، واحدة لكل منهما.

1.4.I حالة كشف المعلومات الاستخباراتية الترابطية المباشرة

يُعد كشف سوء السلوك بناءً على المعلومات الاستخباراتية الترابطية المباشرة أسهل طريقة في مركبة موصولة. وتشير جميع أشكال المعلومات الاستخباراتية الترابطية المباشرة إلى سوء السلوك بشكل مباشر، من قبيل عنوان بروتوكول الإنترنت (IP) واسم الميدان ومحدد موقع الموارد المُوحّد (URL) وبحوث الأمن السيبراني الداخلي وتقرير نقاط الضعف الخارجي. وتتضمن أي من هذه البيانات سمة مطلقة لكشف سوء السلوك.

ويوضح الجدول 4.I المعلومات الاستخباراتية الترابطية المباشرة الشائعة في أنظمة النقل الذكية.

الجدول 4.I – بيانات كشف المعلومات الاستخباراتية الترابطية المباشرة

العقدة	البيانات
نظام المعلومات والترفيه داخل المركبة	عنوان IP URL اسم الميدان
قاعدة البيانات الاستخباراتية	تقرير نقاط الضعف الخارجي بحوث الأمن السيبراني الداخلي

2.4.I حالة كشف المعلومات الاستخباراتية الترابطية غير المباشرة

يتعذر استخدام المعلومات الاستخباراتية الترابطية غير المباشرة لكشف سوء السلوك بشكل مستقل، ولكن يمكن دمجها مع مصادر استخباراتية أخرى. وفي بعض الظروف، لا يمكن استغلال نقطة ضعف واحدة، ولكن يمكن للمهاجم استخدام العديد من نقاط الضعف لبناء سلسلة استغلال لتحقيق الاستغلال. فعلى سبيل المثال، لا يقوم كل بائع بإصلاح نقاط الضعف ليحول دون استغلالها. وعندما يتلقى محرك الكشف تقريراً تقنياً جديداً عن سَلسَلة المرجعين [b-CVE-2017-11906] و[b-CVE-2017-11907] يمكنه الوصول إلى تنفيذ شفرة عشوائية؛ وتُلتقط نسخة المتصفح في نظام المعلومات والترفيه داخل المركبة لاستخدامها مع البيانات الذكية لكشف سوء السلوك.

ويوضح الجدول I.5 المعلومات الاستخباراتية الترابطية غير المباشرة الشائعة في أنظمة النقل الذكية.

الجدول 5.I – بيانات كشف المعلومات الاستخباراتية الترابطية غير المباشرة

العقدة	البيانات
قاعدة البيانات الاستخباراتية	نظام المعلومات والترفيه داخل المركبة تقرير تقني خارجي

بيبليوغرافيا

[b-ISO/TR 17427-4] ISO/TR 17427-4:2015, *Intelligent transport systems – Cooperative ITS – Part 4: Minimum system requirements and behaviour for core systems*.

[b-CVE-2017-11906] Common Vulnerabilities and Exposures, CVE-2017-11906 (2017). *Internet Explorer information disclosure vulnerability*. Bedford, MA: Mitre Corporation. Available [viewed 2021-02-21] at: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11906

[b-CVE-2017-11907] Common Vulnerabilities and Exposures, CVE-2017-11907 (2017). *Scripting engine memory corruption vulnerability*. Bedford, MA: Mitre Corporation. Available [viewed 2021-02-21] at: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11907

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