الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1371

(2020/05)

السلسلة X: شبكات البيانات والاتصالات،
بين الأنظمة المفتوحة ومسائل الأمن

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

التهديدات الأمنية التي تتعرض لها المركبات الموصولة

التوصية ITU-T X.1371

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات، بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب	X.1140–X.1149
بروتوكولات الأمن (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230-X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1360–X.1369
أمن أنظمة النقل الذكية (ITS)	**X.1370–X.1389**
أمن سجل الحسابات الموزع	X.1400–X.1429
أمن سجل الحسابات الموزع	X.1430–X.1449
البروتوكول الأمني (2)	X.1450–X.1459
تبادل معلومات الأمن السيبراني	
نظرة عامة على 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
المولد الكمومي للأعداد العشوائية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية (QKDN)	X.1710–X.1711
التصميم الأمني للشبكات QKDN	X.1712–X.1719
التقنيات الأمنية للشبكات QKDN	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
أمن الجيل الخامس	X.1800–X.1819

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

التوصية ITU-T X.1371

التهديدات الأمنية التي تتعرض لها المركبات الموصولة

ملخص

تصف التوصية X.1371 التهديدات الأمنية التي تتعرض لها المركبات الموصولة والنظام الإيكولوجي للمركبات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1371	2020-05-29	17	11.1002/1000/14090

مصطلحات أساسية

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

جدول المحتويات

الصفحة

التوصية ITU-T X.1371

التهديدات الأمنية التي تتعرض لها المركبات الموصولة

1 مجال التطبيق

تصف هذه التوصية التهديدات الأمنية التي تتعرض لها المركبات الموصولة. ويمكن الإشارة إلى هذه التوصية في التوصيات التي يضعها قطاع تقييس الاتصالات في المستقبل للتأكد من أنها تأخذ في الاعتبار باستمرار الجوانب الأمنية لأنظمة النقل الذكية (ITS).

2 المراجع

تضم توصيات قطاع تقييس الاتصالات المذكورة أدناه وغيرها من المراجع أحكاماً تؤلف، من خلال الإشارات الواردة إليها في هذا النص، أحكاماً لهذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجعة، 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. ولا تضفي الإشارة إلى وثيقة ما في هذه التوصية على تلك الوثيقة في حد ذاتها صفة التوصية.

لا شيء.

3 تعاريف

1.3 مصطلحات معرّفة في مكان آخر

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 التيسر (availability) [b-ITU-T X.800]: خاصية إمكانية النفاذ وإمكانية الاستعمال بناءً على طلب من كيان مرخص له.

2.1.3 الخصوصية (confidentiality) [b-ITU-T X.800]: خاصية عدم إتاحة المعلومات أو الكشف عنها لأشخاص غير مرخص لهم أو لكيانات أو عمليات غير مرخص لها.

3.1.3 السلامة (integrity) [b-ISO/IEC 27000]: خاصية الدقة والاكتمال.

4.1.3 التهديد (threat) [b-ISO/IEC 27000]: السبب المحتمل لحادث غير مرغوب فيه، والذي يمكن أن يؤدي إلى ضرر بالنظام أو المنظمة.

2.3 المصطلحات المعرّفة في هذه التوصية

لا توجد.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

3G الجيل الثالث *(Third Generation)*

4G الجيل الرابع *(Fourth Generation)*

5G الجيل الخامس *(Fifth Generation)*

ADAS نظام متقدم لمساعدة السائق *(Advanced Driver Assistance System)*

CAN شبكة منطقة التحكم *(Controller Area Network)*

CAM رسالة توعية تعاونية *(Cooperative Awareness Message)*

C-V2X اتصالات خلوية من مركبة إلى كل شيء *(Cellular-based Vehicle-to-X)*

DENM رسالة إخطار بيئية لامركزية *(Decentralized Environmental Notification Message)*

DRM إدارة الحقوق الرقمية *(Digital Right Management)*

DSRC اتصالات مكرسة قصيرة المدى *(Dedicated Short-Range Communication)*

ECU وحدة التحكم الإلكتروني *(Electronic Control Unit)*

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

ICT تكنولوجيا المعلومات والاتصالات *(Information and Communication Technology)*

ID معرّف الهوية *(Identifier)*

IT تكنولوجيا المعلومات *(Information Technology)*

ITS أنظمة النقل الذكية *(Intelligent Transport Systems)*

IVN شبكة داخل المركبة *(In-Vehicle Network)*

JTAG فريق عمل الاختبار المشترك *(Joint Test Action Group)*

LIN شبكة توصيل بيني محلية *(Local Interconnect Network)*

MOST نقل الأنظمة المتمحورة حول الوسائط *(Media Oriented Systems Transport)*

OBD التشخيص على متن المركبة *(On-Board Diagnostics)*

ODR جهاز تسجيل بيانات التشغيل *(Operating Data Recorder)*

OEM مصنّع المعدات الأصلي *(Original Equipment Manufacturer)*

OTA عبر الأثير *(Over-The-Air)*

RF تردد راديوي *(Radio Frequency)*

RSU وحدة على جانب الطريق *(Roadside Unit)*

SD رقمي آمن *(Secure Digital)*

SQL لغة الاستعلام البنيوية *(Structured Query Language)*

USB ناقل عمومي بالتسلسل *(Universal Serial Bus)*

V2D من مركبة إلى جهاز جوال *(Vehicle-to-nomadic Device)*

V2I من مركبة إلى بنية تحتية *(Vehicle-to-Infrastructure)*

V2P من مركبة إلى المشاة *(Vehicle-to-Pedestrian)*

V2V من مركبة إلى مركبة *(Vehicle-to-Vehicle)*

V2X من مركبة إلى كل شيء *(Vehicle-to-X)*

VIN رقم تعرف هوية المركبة *(Vehicle Identification Number)*

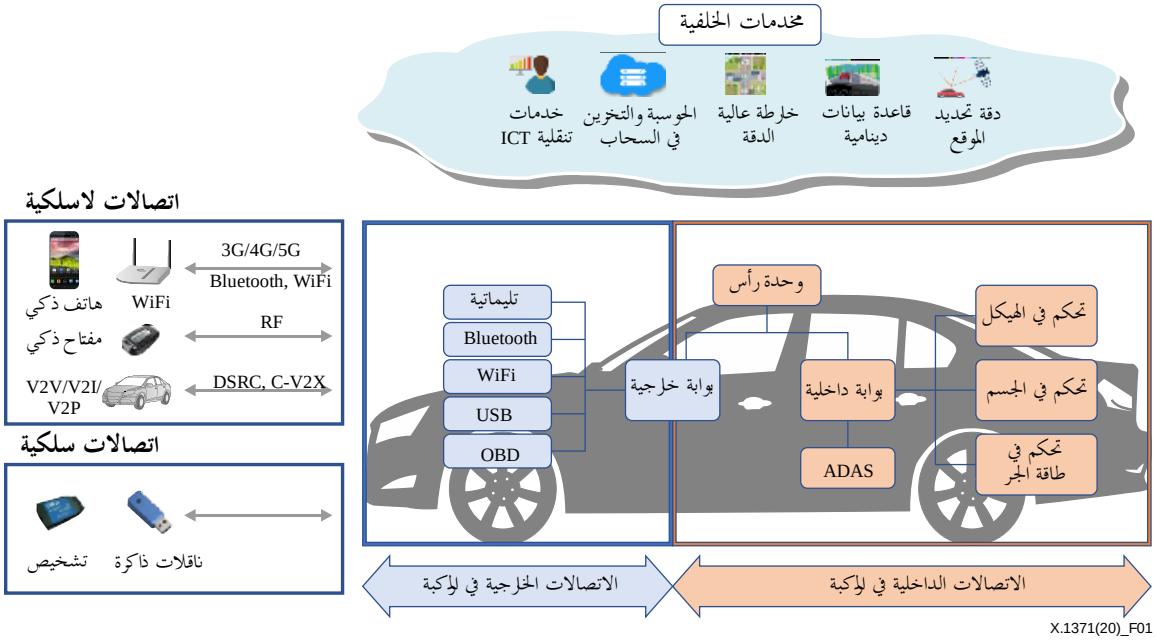
Wi-Fi أمانة لا سلكية *(Wireless Fidelity)*

5 اصطلاحات

لا شيء.

6 نموذج مركبة موصولة (النظام الإيكولوجي للمركبة)

يوضح الشكل 1 مفهوم المركبة الموصولة ونظامها الإيكولوجي. وهذا النموذج هو تمثيل مفاهيمي للنظام الإيكولوجي للمركبة، وهو غير مرتبط بأي عمليات تنفيذ مادية أو تقنيات محددة، علماً بأن هذه العمليات أو التقنيات تتغير بمرور الزمن. وقد لا يصور النموذج جميع التقنيات أو الأنظمة المستخدمة في نظام إيكولوجي للمركبة ولكن يمكن استخدامه كأساس لاستبانة التهديدات الأمنية.



الشكل 1 – مفهوم لمركبة موصولة (نظام إيكولوجي لمركبة)

في الوقت الحاضر، تنهض تكنولوجيا الاتصالات بدور هام في المركبات. ويمكن تصنيف اتصالات المركبات إلى اتصالات خارج المركبة وداخلها. وتتضمن الشبكة الداخلية للمركبة، والمعروفة باسم الشبكة داخل المركبة (IVN)، مكونات المركبة مثل المحاسيس ووحدات التحكم الإلكتروني (ECU). وتستخدم هذه المحاسيس ووحدات التحكم الإلكتروني في العديد من المجالات مثل التحكم في الهيكل، والتحكم في الجسم، والتحكم في قوة الجر للمركبة. وعلاوة على ذلك، تستخدم هذه المكونات في نظام متقدم لمساعدة القيادة (ADAS)، يدعم السائق أثناء القيادة مثل الحفاظ على مسلك القيادة ووظائف التحكم في التطواف. وتعتبر وحدة الرأس مكونة من مكونات المعلومات والترفيه في السيارة، وهي تتيح للمستخدم التحكم في معلومات المركبة ووسائط الترفيه، مثل الصوت والفيديو.

وتعرف الاتصالات الخارجية للمركبة بالمختصر V2X، الذي يعني "من المركبة إلى كل شيء" حيث "كل شيء" هو أي شيء متعلق بالتشغيل الآمن والفعال للمركبة. وعلى وجه الخصوص، يستخدم المختصر V2X كمصطلح عام لأنماط الاتصال مثل مركبة إلى مركبة (V2V) ومن مركبة إلى بنية تحتية (V2I) ومن مركبة إلى جهاز جوال (V2D) ومن مركبة إلى المشاة (V2P). وتتضمن تقنية V2X الاتصالات المخصصة قصيرة المدى (DSRC) والاتصالات V2X الخلوية (C-V2X). وتتكون البنية التحتية من وحدات على جانب الطريق (RSU) ومرافق خلفية، مثل أنظمة إدارة حركة المرور والمراقبة. ويمكن توصيل وحدات RSU بالمرافق الخلفية من خلال شبكات سلكية أو لاسلكية. يوضح الشكل 1 مختلف الوظائف في المخدمات الخلفية. وهي تشمل خدمات تنقلية تكنولوجيا المعلومات والاتصالات، ومستودعات سحابية، وخارطة عالية الدقة وقاعدة بيانات دينامية للبيئة المجاورة وجهاز تحديد موقع المركبة بدقة.

وتنهض البوابات الخارجية والداخلية، في الشكل 1، بدور في معالجة تعقيد اتصالات المركبات. وتقوم البوابة الداخلية بمعالجة البيانات في المجال داخل المركبة. والبوابة الخارجية هي المسؤولة عن التواصل بين المركبة والأجهزة الخارجية مثل الهواتف الذكية والمركبات الأخرى من خلال تكنولوجيا الاتصالات V2X. ويمكن تصنيف الاتصالات الخارجية إلى اتصالات سلكية ولاسلكية. ويمكن أن يستخدم الاتصال السلكي منفذ التشخيص II على متن المركبة (OBD II) للتواصل مع الأجهزة التشخيصية أو تحديثات البرمجيات والمعدات الثابتة في المركبة. وتتضمن قناة الاتصالات اللاسلكية تقنية الاتصالات الخلوية وشبكات Wi-Fi وBluetooth لتوصيل المركبة بأجهزة متنقلة مثل الهواتف الذكية.

7 تهديدات المركبة الموصولة أو النظام الإيكولوجي للمركبة والمعلومات المحتملة المتعلقة بالتهديدات

1.7 التهديدات التي تتعرض لها المركبات الموصولة أو النظام الإيكولوجي للمركبات

1.1.7 التهديدات المتعلقة بالمخدمات الخلفية

في السنوات الأخيرة، زاد تنوع التوصيلية في المركبات بشكل ملحوظ، وعلى وجه الخصوص، اشتد الطلب على التوصيلية مع مختلف المخدمات (وتسمى "المخدمات الخلفية") الموجودة في النهاية الخلفية للمركبات. وتشمل المخدمات الخلفية تلك التي توفرها الشركات المصنّعة للتجهيزات الأصلية (OEM)، والمورّدون، وخدمات تكنولوجيا المعلومات والاتصالات (ICT) لدعم النظام الإيكولوجي للمركبة من الواجهة الخلفية البعيدة.

1.1.1.7 المخدمات الخلفية المستخدمة كوسيلة لمهاجمة مركبة أو استخراج البيانات

في النظام الإيكولوجي للمركبة، يقوم المخدم الخلفي بجمع البيانات من المركبة بشكل أساسي، ويقوم بتخزينها، ويرسل المعلومات إلى المركبة. وينبغي التصدي للتهديدات التالية للمخدم الخلفي لوقايته من تلاعب كيان غير مصرح له:

- إساءة استخدام السلطة من جانب طرف داخلي: قد تؤدي إساءة استخدام الامتيازات الإدارية من طرف داخلي في المخدم الخلفي إلى الكشف عن تسرب البيانات من المخدم أو إرسال معلومات خاطئة إلى المركبة، وما إلى ذلك.
- نفاذ غير مرخص به من الخارج إلى المخدم الخلفي: إذا بقي هناك باب خلفي أو نقطة ضعف معروفة في المخدم الخلفي، فقد تستغل من الخارج لمهاجمة المخدم الخلفي بأساليب الهجوم مثل دس لغة الاستعلام البنيوية (SQL) والبرمجيات الخبيثة. وإذا حصل المهاجم على الامتيازات الإدارية للمخدم، فينبغي النظر في نفس الضرر على النحو الموصوف في المدخل السابق.
- نفاذ مادي غير مرخص به: هناك عدة أساليب للنفاذ مادياً إلى المخدم الخلفي من قبيل استخدام ناقل عمومي بالتسلسل (USB) أو الدخول إلى مبنى المخدم بانتحال هوية موظف (ID). وفي هذه الحالة، يكون مقدار التلف والتدخل في البيانات المتعلقة بالمركبة ومرافق معالجة المعلومات الخاصة بها أكبر.

2.1.1.7 تعطيل خدمة المخدم الخلفي

يمكن أن تتسبب الهجمات على المخدم الخلفي في تعطيل المخدم وتفاعله مع المركبات وتوفير الخدمات التي تعتمد عليها المركبات. وقد تتسبب الهجمات في أثر ضار شديد على تيسر الخدمات المتعلقة بالمركبة مثل إدارة الشهادات للمركبة والبنية التحتية.

3.1.1.7 فقدان البيانات الموجودة في المخدمات الخلفية أو العبث بها

قد تُفقد أو تتسرب البيانات الموجودة على المخدم الخلفي إذا تم العبث به من خلال إساءة استخدام السلطة من جانب طرف داخلي أو النفاذ غير المرخص به من الخارج أو النفاذ المادي غير المرخص به، على النحو المحدد في البند 1.1.1.7. وعلاوةً على ذلك، هناك تهديدات إضافية على النحو التالي:

- فقدان المعلومات في السحابة: قد تتسرب معلومات حساسة مثل رقم تعريف المركبة (VIN) أو المعلومات الشخصية للسائق وتتعرض للعبث إذا تم تخزينها في أنظمة مزودي خدمات السحابة التابعة لطرف ثالث.
- انتهاك المعلومات بتقاسم البيانات غير المقصود: إذا كان المخدم موجوداً في محيط غير آمن جراء سوء التشكيل من جانب المدير، فقد تتعرض البيانات للتقاسم أو التسرب عن غير قصد.

2.1.7 التهديدات التي تتعرض لها المركبات فيما يتعلق بقنوات الاتصال الخاصة بها

تتضمن اتصالات المركبات الاتصالات الخارجية مثل الاتصالات من مركبة إلى مركبة (V2V) ومن مركبة إلى بنية تحتية (V2I) ومن مركبة إلى جهاز جوال (V2D) ومن مركبة إلى المشاة (V2P) والاتصالات داخل المركبة مثل شبكة منطقة التحكم (CAN) وشبكة التوصيل البيني المحلية (LIN) ونقل الأنظمة المتمحورة حول الوسائط (MOST) وشبكة الاتصالات FlexRay. وقد تكون القنوات المستخدمة في هذه الاتصالات أهدافاً لهجمات من قبيل الانتحال أو التنصت أو التلاعب بالرسائل وما إلى ذلك.

1.2.1.7 رسائل الانتحال

قد يحدث العبث بالرسائل عن طريق الانتحال. وفي حالة الرسائل المستخدمة في الاتصالات من المركبة إلى كل شيء (V2X) والنظام العالمي للملاحة الساتلية (GNSS)، يمكن لمركبة أن تتلقى رسائل غير صالحة جراء هجوم انتحال الهوية. وبالإضافة إلى ذلك، إذا كان هناك العديد من المركبات على طريق معين، يمكن تنفيذ هجوم Sybil بغية خداع المركبات الأخرى.

ملاحظة – يحدث هجوم Sybil مثال ذلك عندما تحاكي مركبة ما مركبات متعددة باستخدام معرفات هوية مركبات متعددة.

2.2.1.7 التلاعب أو الحذف غير المرخص به أو أي تعديلات أخرى في الشفرة أو في البيانات المحمولة في المركبة

إذا كان هناك ثغرة أو موطن ضعف في المركبة، فقد يحدث نفاذ غير قانوني عن بُعد و/أو هجوم برمجية خبيثة عبر قنوات اتصال المركبة. ونتيجةً لذلك، قد تعمل قناة الاتصال على تمكين العديد من التهديدات الأمنية على النحو التالي:

- دس شفرة، حيث يمكن مثلاً التلاعب بشفرة ثنائية برمجية مع تدفق الاتصالات؛
- التلاعب في البيانات أو الشفرة الموجودة في المركبة؛
- استبدال البيانات أو الشفرة الموجودة في المركبة؛
- محو أو حذف البيانات أو الشفرة الموجودة في المركبة.

3.2.1.7 استخدام رسائل غير موثوق بها أو لا يمكن الاعتماد عليها وهجمات اختطاف أو استعادة الجلسة

يمكن تلقي رسائل من مصدر غير موثوق أو لا يمكن الاعتماد عليه عبر قنوات الاتصال. وهجوم الاعتراض واختطاف الجلسة أمر ممكن عبر قنوات الاتصال. مثال ذلك، يمكّن الهجوم على بوابة الاتصالات في المركبة المهاجم من تخفيض كفاءة برمجية وحدة التحكم الإلكتروني (ECU) أو البرمجية الثابتة للبوابة باستخدام نقاط الضعف المعروفة للبرمجية من خلال هجوم استعادة التشغيل حيث يجري تكرار نقل بيانات صالحة لأغراض خبيثة.

4.2.1.7 الكشف عن المعلومات

يمكن الكشف عن المعلومات بسهولة من خلال التنصت على الاتصالات أو من خلال تمكين النفاذ غير المرخص به إلى الملفات الحساسة. أي أن المعلومات المتبادلة عبر قناة الاتصال يمكن التنصت عليها من خلال الاعتراض الخبيث والإشعاع المتداخل ومراقبة الاتصالات. ولهذه الغاية، يستطيع للمهاجم الحصول على حقوق نفاذ غير مرخص بها إلى الملفات.

5.2.1.7 هجمات رفض الخدمة

يمكن للمهاجم القيام بهجوم رفض الخدمة عبر قناة اتصال من خلال إرسال قدر كبير من بيانات القمامة إلى نظام معلومات المركبة مما يؤدي إلى تعطيل وظائف المركبة إلى حد كبير. ومن ناحية أخرى، وفي حالات الاتصالات ضمن الفصيل أو الاتصالات من مركبة إلى أخرى، يمكن للمهاجم منع إرسال أي بيانات ضرورية إلى مركبات أخرى في المجموعة بحيث تفقد المركبات الأخرى التحكم بسبب عدم وجود بيانات من المركبات الأخرى. وهذا ما يُعرف باسم "هجوم الحفرة السوداء".

6.2.1.7 نفاذ امتياز لمستخدم ليس له امتياز

يستطيع مستخدم ليس له امتياز الحصول، بشكلٍ غير قانوني عبر قنوات الاتصال، على نفاذ امتياز، من قبيل النفاذ إلى جذر النظام. وهذا ما يسمى "تصعيد الامتياز غير المرخص به" وعند نجاح هذا التصعيد، يستطيع المهاجم أن يقوم بأشياء لا يستطيع المستخدمون العاديون القيام بها.

7.2.1.7 الفيروسات المضمنة في وسائط الاتصال

بعد اكتشاف مواطن الضعف في نظام المركبات، يمكن دس الفيروسات أو البرمجيات الخبيثة في نظام المركبات عبر قنوات الاتصال. ويمكن أن تأخذ الفيروسات مكان مدير يتمتع بامتياز النفاذ ويمكنها القيام بأي هجمات مقصودة في المركبة. مثال ذلك، إذا قام فيروس بتجفير أي ملفات أو معلومات دون ترخيص في نظام المركبات المستهدف، وهو ما يسمى "برمجية الفدية"، عندئذٍ يفقد نظام المركبة وظيفته.

8.2.1.7 رسائل خبيثة المحتوى

قد تكون الرسائل التي تتلقاها المركبة (من قبيل الرسائل التشخيصية أو الرسائل من المركبات الأخرى)، أو المرسلة داخلها، خبيثة المحتوى. في حالة الشبكات داخل المركبة، يمكن للمهاجم تعديل برنامج وحدات التحكم الإلكترونية (ECU) من خلال دس الفيروسات (انظر البند 7.2.1.7)، والانضمام إلى شبكة المركبات كعضو عن طريق الانتحال.

ويمكن للمركبات المجاورة أن تتلقى رسائل خبيثة من مركبة إلى كل شيء (V2X) مثل رسائل التوعية التعاونية (CAM) ورسائل الإخطار البيئية اللامركزية (DENM). وتعتمد الاتصالات V2X على البث، وبالتالي، قد تتسبب الكثير من رسائل V2X الخبيثة في أثر ضار على شبكات المركبات بأكملها، بما في ذلك الشبكات داخل المركبة نفسها.

ويمكن أيضاً تلقي رسائل تشخيص خبيثة. ويمكن للمهاجم أن يسجل رسالة تشخيصية ويستخدمها لهجوم استعادة تشغيل. بل يمكن، علاوة على ذلك، تلقي رسالة التحكم بالمركبة عبر هجوم استعادة تشغيل.

وترسل الرسائل المسجلة الملكية من مصنّع المعدات الأصلي (OEM) أو مورّد المكونة أو النظام أو الوظيفة. ولكن من الممكن أيضاً تلقي رسائل خبيثة من المهاجمين لتعطيل نظام المركبات.

3.1.7 التهديدات التي تتعرض لها المركبات فيما يتعلق بإجراءات التحديث الخاصة بها

هناك طريقتان لتحديث أنظمة المركبات، وهما التحديث السلكي عبر منفذ التشخيص على متن المركبة (OBD) أو الأجهزة المحمولة مثل بطاقة رقمية آمنة (SD) أو محرك ناقل ذاكرة USB والتحديث اللاسلكي عبر الأثير. وقد تكون البرمجية المراد تحديثها برمجية ثابتة أو بيانات تشكيل خاصة بالمركبة. ويمكن تحديث غالبية المشكلات الإلكترونية وعيوب البرمجيات وحلها إلكترونياً دون نفاذ مادي، وذلك عن طريق اختبار OBD مثلاً. وعلاوة على ذلك، فإن التحديثات (اللاسلكية) على الأثير تساعد في تقصير دورة التحديث لتقليل التعرض للهجمات بالنسبة لمواطن الضعف الأمنية المعروفة للبرمجية.

1.3.1.7 سوء استخدام إجراءات التحديث أو العبث بها

بغض النظر عما إذا كان يتم إجراء التحديث المستخدم بطريقة محلية أو مادية أو عبر الأثير، قد ينطوي إجراء التحديث على تهديدات باستخدام البرامج الحاسوبية التحديث النظام أو البرمجية الثابتة التي تعرضت للعبث.

ويمكن التلاعب بالبرمجية قبل عملية التحديث، على الرغم من أن عملية التحديث سليمة. إذ يقوم مزودو البرمجيات باستحداث أو إعداد البرمجيات للتحديث وتسليمها إلى الأنظمة المستهدفة التي تتطلب ذلك. ولذلك، قد يكون هناك تهديد خطير بالتلاعب بالبرمجية وإفسادها قبل استخدامها.

وبشكلٍ خاص، قدد تتعرض للخطر مواد التجفير، مثل المفاتيح والشهادات المستخدمة في إجراء تحديث البرمجية وبالتالي تسبب تحديثات برمجية غير صالحة.

2.3.1.7 رفض التحديث المشروع

إن هجوم رفض الخدمة على مخدم تحديث أو شبكة لمنع بدء تحديثات البرمجيات الهامة أو الإفراج عن الميزات الخاصة بالعملاء ممكن في إجراء تحديث البرمجيات. ومن الممكن أيضاً رفض تحديثات مشروعة.

4.1.7 التهديدات التي تتعرض لها المركبات فيما يتعلق بإجراءات بشرية غير مقصودة

يمكن أن تؤدي إجراءات بشرية دون قصد إلى تهديدات دون أن تلاحظ. وتتضمن هذه التهديدات، بالتغيب، التعديل غير المرخص به أو غير المقصود للبرمجية. وتتضمن الأخطاء العرضية مخالفات التشكيل وأخطاء البرمجة وفساد البيانات بسبب أخطاء من جانب المستخدم أو المشغل.

1.4.1.7 سوء تشكيل للمعدات أو الأنظمة من جانب طرف مشروع

يمكن لمستخدم مشروع اتخاذ إجراءات تحفز هجمات سيبرانية دون قصد. أي قد يتغير إعداد نظام المركبة بشكلٍ غير طبيعي من قبل مستخدم مشروع أثناء التثبيت أو الإصلاح أو الاستخدام غير المقصود. وقد تكون هناك أيضاً أخطاء في إدارة أو استخدام الأنظمة أو الأجهزة التي تتضمن تحديثات البرمجيات.

2.4.1.7 التيسير غير المقصود من جانب طرف مشروع لهجوم سيبراني

قد يكون المستخدم المشروع (المالك أو المشغل أو مهندس الصيانة) ضحية بريئة وأن يُخدع لاتخاذ إجراء لتحميل شفرة (برمجية) خبيثة أو تمكين هجوم ما عن غير قصد. وعلاوة على ذلك، لا يتبع المستخدم المشروع في كثير من الأحيان الإجراءات الأمنية المحددة.

5.1.7 التهديدات للمركبات فيما يتعلق بتوصيليتها الخارجية وتوصيلاتها

بالنسبة لطائفة متنوعة من الخدمات المريحة، يمكن تجهيز المركبات بمكونات للتواصل مع المخدمات الخلفية ويمكنها التواصل مع كل شيء خاضع للتمكين من جانب مستخدمي الطرق عبر اتصال لاسلكي. وإلى جانب ميزات الراحة، هناك مزايا السلامة مثل وظيفة نداءات الطوارئ التلقائية وتلك التي تدعمها الاتصالات من المركبة إلى كل شيء (V2X). ومع ذلك، كلما تزايد تواصل المركبات مع كيانات خارجية لتعزيز التوصيلية، تزايدت التهديدات ومواطن الضعف نظراً لتوسع أسطح الهجمات جراء الواجهات الإضافية.

1.5.1.7 التلاعب في توصيلية وظائف المركبات

من شأن التلاعب في توصيلية وظائف المركبات أن يمكن الهجوم السيبراني. ويمكن التصدي لهذا التهديد في عناصر المركبات التالية:

- التلاعب بالوظائف المصممة لتشغيل الأنظمة عن بُعد: المفتاح النائي، وجهاز إيقاف الحركة، وبطارية الشحن؛
- التلاعب في تليماتية المركبات: من قبيل فتح الشاحنة عن بعد؛
- التلاعب من خلال واجهة مع نظام لاسلكي أو محاسيس قصيرة المدى.

2.5.1.7 برمجية طرف ثالث مستضافة

قد يسمح نظام المعلومات والترفيه في المركبات الحديثة الموصولة بالشبكة داخل المركبة بتثبيت تطبيقات لطرف ثالث. وقد تكون تطبيقات الطرف الثالث فاسدة أو ذات برمجية ضعيفة الأمان وتستخدم كوسيلة لمهاجمة أنظمة المركبات.

3.5.1.7 الأجهزة الموصولة بالواجهات الخارجية

من شأن وظائف التوصيلية أن تجلب واجهات خارجية، ويمكن استخدام الأجهزة الموصولة بها كوسيلة لمهاجمة أنظمة المركبات ذات الواجهات المستضعفة التالية:

- واجهات خارجية مثل منفذ USB: للهجوم من خلال دس الشفرة
- الوسائط المصابة بالفيروس: يمكن للفيروس مهاجمة النظام داخل المركبة عبر الوسائط المصابة
- النفاذ التشخيصي: تستخدم وظائف التشخيص التي يمكن النفاذ إليها بواسطة Bluetooth في منافذ التشخيص على متن المركبة (OBD) لاستعراض حالة المركبات والتلاعب بمعلمات المركبة المضمنة في برمجية المركبة.

2.7 المعلومات المحتملة المتعلقة بالتهديدات

1.2.7 الأهداف، أو الدوافع المحتملة، للهجوم

قد تصبح المركبات هدفاً للهجمات السيبرانية المحتملة عندما تكون موصولة إلكترونياً بالعديد من الأنظمة أو الخدمات في النظام الإيكولوجي للمركبات. وعلاوة على ذلك، يسعى المهاجمون غالباً إلى الحصول على فوائد مالية من خلال جعل مهاراتهم الهجومية معروفة ليس للعالم فحسب، بل وأيضاً لبائعي المعدات الأصلية (OEM). وقد تؤثر الهجمات على أنظمة المركبات على النحو المبين في الفقرات من 1.1.2.7 إلى 7.1.2.7.

1.1.2.7 استخراج بيانات أو شفرة المركبة

البيانات الحساسة أو بيانات الاعتماد هي أهداف للاستخراج لأنها قد تحتوي على المعلومات المفيدة التالية لتحقيق مكاسب مالية.

- حقوق النشر أو البرمجيات المسجلة الملكية للمركبة؛
- المعلومات الخاصة التابعة للمالك، مثل الهوية الشخصية ومعلومات حساب الدفع، ومعلومات دفتر العناوين، ومعلومات الموقع، والمعرف الإلكتروني للمركبة؛
- مفاتيح التجفير وما إلى ذلك.

2.1.2.7 التلاعب ببيانات أو شفرة المركبة

من خلال التلاعب ببيانات أو شفرة المركبة يمكن للمهاجمين انتحال سلوك المالك الشرعي أو التنصل منه. ويمكن استبانة طرائق التلاعب التالية:

- تغييرات غير قانونية/غير مرخص بها في المعرف الإلكتروني للمركبة؛
- تزوير الهوية: عندما يقدم المستخدم هوية أخرى عند الاتصال بأنظمة تحصيل الرسوم وأنظمة الواجهة الخلفية للمصنعين؛
- التحايل على أنظمة المراقبة: القرصنة أو العبث أو حظر الرسائل مثل بيانات تتبع مسجل بيانات التشغيل (ODR) أو عدد مرات التشغيل؛
- تزوير بيانات قيادة المركبة: مثال ذلك، عدد الكيلومترات وسرعة القيادة واتجاهات القيادة والوقت المرجعي للمركبة؛
- تغييرات غير مرخص بها في بيانات تشخيص النظام؛
- تزوير إصدار البرمجيات الثابتة: يمكن استبدال أحدث البرمجيات الثابتة التي تنطوي على تصحيح لمواجهة بعض الثغرات بالإصدار القديم بدون تصحيح.

3.1.2.7 محو البيانات أو الشفرة

قد تحدث عمليات حذف أو معاملة غير مرخص بها لسجلات أحداث النظام. وغالباً ما يجعل هذا التزييف تحليل البيانات أمراً مستحيلاً أو يجعل من العسير البحث عن سبب الهجوم.

4.1.2.7 إدخال البرمجيات الخبيثة

في إطار العديد من أساليب الهجوم، يعد إدخال البرمجيات الخبيثة في نظام المركبات الخطوة الأولى لنشاط المهاجم. وهناك واجهات هجوم متعددة لإدخال البرمجيات الخبيثة، مثل استخدام الواجهات الخارجية والنمائط المادية المصابة.

5.1.2.7 إدخال برمجية جديدة أو استبدال برمجية قائمة

إدخال برمجية جديدة أو استبدال برمجية قائمة ببرمجية خبيثة، قد يكون له آثار خطيرة على الأمن السيبراني بالنسبة لنظام التحكم في المركبة أو نظام المعلومات.

6.1.2.7 تعطيل الأنظمة أو العمليات

قد ينطلق هجوم رفض الخدمة على نظام المركبات في الشبكة الداخلية عن طريق إغراق الرسائل في ناقلة شبكة منطقة التحكم (CAN) أو عن طريق إثارة الأعطال في وحدة التحكم الإلكترونية (ECU) عبر معدل مرتفع من الرسائل.

7.1.2.7 التلاعب في المعلمات المركبة

قد يكون للتلاعب بمعلمات المركبات أثر قوي على نظام المركبات مثل النفاذ غير المرخص لتزييف:

- معلمات التشكيل للوظائف الرئيسية في المركبة، من قبيل بيانات الكوابح أو عتبة نشر الوسادة الهوائية؛
- معلمات شحن البطارية، مثل فلطية الشحن، وقوة الشحن، ودرجة حرارة البطارية، وما إلى ذلك.

2.2.7 مواطن الضعف المحتملة

1.2.2.7 تقنيات التجفير الضعيفة

يمكن استضعاف تقنيات التجفير أو عدم تطبيقها بشكلٍ كاف. ويمكن استغلال مفاتيح التجفير أو الشهادات بما في ذلك بيانات الاعتماد مثل كلمة السر. مثال ذلك، في حال استخدام مفاتيح تجفير ضعيفة أو عدم تحديث مفاتيح التجفير لفترة طويلة، فقد يتعطل نظام التجفير جراء هجمات قاسية. وقد يؤدي الاستخدام غير الكافي لتقنيات التجفير إلى تسرب مفاتيح التجفير أو بيانات الاعتماد. وعلاوةً على ذلك، قد يزداد خطر تسرب المعلومات عن طريق استخدام تقنيات التجفير المعطلة والمتقادمة أصلاً.

2.2.2.7 أجزاء المركبة أو اللوازم المتأثرة

يمكن هندسة المعدات أو البرمجيات المستخدمة في النظام الإيكولوجي للمركبة بحيث لا تلبي معايير التصميم للدفاع عن أي هجوم. وقد تتعرض الأجزاء أو اللوازم الموجودة في مركبة للخطر بحيث تتعرض المركبات للهجوم.

3.2.2.7 مواطن الضعف في تطوير البرمجيات أو المعدات

قد يكون وجود أخطاء البرمجيات أساساً لثغرات أمنية قابلة للاستغلال. ويصح ذلك بشكلٍ خاص إذا لم يتم اختبار البرمجية للتحقق مما إذا كانت الشفرة السيئة أو الأخطاء المعروفة موجودة والتقليل من خطر وجود الشفرة السيئة أو الأخطاء غير المعروفة.

ومن شأن استخدام البقايا من التطوير (من قبيل منافذ التصحيح ومنافذ فريق عمل الاختبار المشترك (JTAG) والمعالِجات الدقيقة وشهادات التطوير وكلمات سر المطورين) أن يتيح أيضاً النفاذ إلى وحدات التحكم الإلكتروني (ECU) أو تمكين المهاجمين من اكتساب امتيازات أعلى.

4.2.2.7 مواطن الضعف في تصميم الشبكة

إذا أمكن النفاذ إلى الشبكة وفي الوقت ذاته بقيت منافذ الاتصالات غير الضرورية مفتوحة، فمن المحتمل أن تزداد الهجمات من قبيل النفاذ غير المرخص به.

وعلاوةً على ذلك، من شأن استخدام البوابات غير المحمية أو نقاط النفاذ (مثل بوابات الشاحنات–المقطورات) للتحايل على الحماية والنفاذ إلى قطاعات الشبكة الأخرى، أن يؤدي إلى ممارسة أعمال خبيثة من قبيل إرسال رسائل تعسفية عبر ناقلة شبكة منطقة التحكم (CAN).

5.2.2.7 الفقدان المادي للبيانات

من الممكن أن تفقد البيانات الحساسة المستخدمة في الأنظمة الإيكولوجية للمركبة أو أن تتعرض للخطر بسبب الأضرار المادية الناجمة عن حوادث المرور أو السرقة. وقد يحدث فقدان البيانات من إدارة الحقوق الرقمية (DRM) مثل حذف بيانات المستخدم.

وعلاوة على ذلك، قد تفقد سلامة البيانات الحساسة بسبب تقادم مكونات تكنولوجيا المعلومات، مما يتسبب في حدوث مشكلات متتالية محتملة (في حالة تغيير المفتاح، مثلاً).

6.2.2.7 النقل غير المقصود للبيانات

قد تتسرب البيانات الخاصة أو الحساسة عند تغيير مستخدمي المركبة (مثال ذلك، عند بيع المركبة أو استخدامها كمركبة استئجار من قبل شخص مختلف).

7.2.2.7 التلاعب المادي بالأنظمة

من المحتمل أن يؤدي التلاعب المادي بالأنظمة مثل معدات المصنّع الأصلي (OEM) إلى هجمات. مثال ذلك، يمكن تنفيذ هجوم الاعتراض إذا أضيفت إلى المركبة معدات غير مرخص بها.

التذييل I

أمثلة على الاستضعاف أو طريقة الهجوم المتعلقة بالتهديدات

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

يقدم هذا التذييل أمثلة على الاستضعاف أو طرائق الهجوم المرتبطة بالتهديدات المبينة في الجدول 1 من المعيار [b-UNECE GRVA].

ملاحظة – أرقام البنود في العمود أقصى اليسار بالجدول 1.I، هي تلك المستخدمة في [b-UNECE GRVA]

الجدول 1.I – قائمة بأمثلة طريقة الضعف أو الهجوم المتعلقة بالتهديدات

وصف الاستضعاف/التهديد في المستوى الأعلى والمستوى الأدنى			**مثال للاستضعاف أو طريقة الهجوم**	
1.3.4 تهديدات بشأن المخدمات الخلفية	1	تستخدم المخدمات الخلفية كوسيلة لمهاجمة مركبة أو استخراج البيانات	1.1	إساءة استخدام الامتيازات من قبل الموظفين (هجوم من الداخل)
			2.1	النفاذ غير المرخص به عبر الإنترنت إلى المخدم (مثلاً، من خلال أبواب خلفية أو ثغرات أمنية في برمجيات النظام غير المصححة أو هجمات لغة الاستعلام البنيوية (SQL) أو وسائل أخرى)
			3.1	نفاذ مادي غير مرخص به إلى المخدم (بواسطة USB مثلاً أو وسائط أخرى موصولة بالمخدم)
	2	تعطيل الخدمات من مخدم الخلفية، مما يؤثر على تشغيل المركبة	1.2	يعمل الهجوم على المخدم الخلفي على إيقاف تشغيله، حيث يمنعه من التفاعل مع المركبات وتوفير الخدمات التي تعتمد عليها
	3	البيانات المحفوظة في المخدمات الخلفية المفقودة أو المعرضة للخطر ("انتهاك البيانات")	1.3	إساءة استخدام الامتيازات من قبل الموظفين (هجوم من الداخل)
			2.3	فقدان المعلومات في السحابة. قد تُفقد البيانات الحساسة جراء الهجمات أو الحوادث عندما يتم تخزين البيانات من جانب مقدمي الخدمات السحابية التابعين لأطراف ثالثة
			3.3	النفاذ غير المرخص به عبر الإنترنت إلى المخدم (مثلاً، من خلال أبواب خلفية أو ثغرات أمنية في برمجيات النظام غير المصححة أو هجمات لغة الاستعلام البنيوية (SQL) أو وسائل أخرى)
			4.3	نفاذ مادي غير مرخص به إلى المخدم (بواسطة USB مثلاً أو وسائط أخرى موصولة بالمخدم)
			5.3	انتهاك المعلومات من خلال التقاسم غير المقصود للبيانات (مثل أخطاء الإدارة وتخزين البيانات في مخدمات الكراج)

الجدول 1.I – قائمة بأمثلة طريقة الضعف أو الهجوم المتعلقة بالتهديدات

وصف الاستضعاف/التهديد في المستوى الأعلى والمستوى الأدنى			مثال للاستضعاف أو طريقة الهجوم	
2.3.4 التهديدات للمركبات فيما يتعلق بقنوات الاتصال الخاصة بها	4	تزييف الرسائل أو البيانات التي تتلقاها المركبة	1.4	تزييف الرسائل بالانتحال (مثل التواصل V2X بمعيار 802.11p أثناء التوزع إلى فصائل ورسائل النظام GNSS وما إلى ذلك)
			2.4	هجوم Sybil (من أجل محاكاة المركبات الأخرى كما لو كان هناك العديد من المركبات على الطريق)
	5	تستخدم قنوات الاتصال بغية التلاعب أو الحذف غير المرخص به أو أي تعديلات أخرى على الشفرة/البيانات المحفوظة في المركبة	1.5	تسمح قنوات الاتصال بدس الشفرة، حيث يمكن دس ثنائية برمجية متلاعب بها في تدفق الاتصالات
			2.5	تسمح قنوات الاتصال بالتلاعب بالبيانات/الشفرة المحفوظة في المركبة
			3.5	تسمح قنوات الاتصال باستبدال البيانات/الشفرة المحفوظة في المركبة
			4.5	تسمح قنوات الاتصال بمحو البيانات/الشفرة المحفوظة في المركبة
			5.5	تسمح قنوات الاتصال بإدخال البيانات/الشفرة إلى المركبة (كتابة شفرة البيانات)
	6	تسمح قنوات الاتصال بقبول الرسائل غير الموثوق بها/غير المعتمد عليها أو التي تتأثر بهجمات اختطاف/استعادة الجلسة	1.6	قبول المعلومات من مصدر غير موثوق أو لا يعتمد عليه
			2.6	هجوم الاعتراض/اختطاف الجلسة
			3.6	هجوم إعادة التشغيل، من قبيل هجوم على بوابة اتصال يسمح للمهاجم بتخفيض كفاءة برمجية وحدة التحكم الإلكتروني (ECU) أو البرمجية الثابتة للبوابة
	7	يمكن الكشف بسهولة عن المعلومات. بالتنصت على الاتصالات أو بالسماح بالنفاذ غير المرخص به إلى الملفات الحساسة	1.7	اعتراض المعلومات/تداخل الإشعاعات/مراقبة الاتصالات
			2.7	النفاذ غير المرخص به إلى الملفات أو البيانات
	8	هجمات إنكار الخدمة عبر قنوات الاتصال لتعطيل وظائف المركبة	1.8	إرسال عدد كبير من بيانات القمامة إلى نظام معلومات المركبة، بحيث يتعذر عليه تقديم الخدمات بالأسلوب المعتاد
			2.8	هجوم "الحفرة السوداء"، حيث يتمكن المهاجم من حظر الرسائل لتعطيل التواصل بين المركبات
	9	يستطيع المستخدم دون امتياز الحصول على نفاذ امتياز إلى أنظمة المركبات	1.9	يستطيع المستخدم دون امتياز الحصول على نفاذ امتياز، بالنفاذ إلى الجذر مثلاً
	10	الفيروسات المضمنة في وسائط الاتصال قادرة على إصابة أنظمة المركبات	1.10	فيروس مضمن في وسائط الاتصال يصيب أنظمة المركبات
	11	تحتوي الرسائل التي تتلقاها المركبة (مثل X2V أو الرسائل التشخيصية)، أو المرسلة داخلها، على محتوى خبيث	1.11	الرسائل الداخلية الخبيثة (مثل CAN)
			2.11	رسائل V2X الخبيثة، من بنية تحتية إلى مركبة ومن مركبة إلى أخرى (مثل CAM وDENM)
			3.11	رسائل التشخيص الخبيثة
			4.11	الرسائل الخبيثة المسجلة الملكية (تلك التي ترسل عادةً من الشركة المصنّعة للمعدات الأصلية أو مورّد المكونة/النظام/الوظيفة)

الجدول 1.I – قائمة بأمثلة طريقة الضعف أو الهجوم المتعلقة بالتهديدات

وصف الاستضعاف/التهديد في المستوى الأعلى والمستوى الأدنى			مثال للاستضعاف أو طريقة الهجوم	
3.3.4 تهديدات للمركبات فيما يتعلق بإجراءات التحديث الخاصة بها	12	سوء استخدام أو تعطيل إجراءات التحديث	1.12	تعطيل إجراءات تحديث البرمجيات على الأثير. ويشمل ذلك برمجية تحديث نظام المصنّع أو البرمجية الثابتة
			2.12	تعطيل إجراءات تحديث البرمجيات المحلية/المادية. ويشمل ذلك برمجية تحديث نظام المصنّع أو البرمجية الثابتة
			3.12	التلاعب بالبرمجية قبل عملية التحديث (وبذلك تصبح فاسدة)، على الرغم من أن عملية التحديث سليمة
			4.12	تعطيل مفاتيح التجفير لدى مزود البرمجية لتمكين تحديث باطل
	13	من الممكن رفض التحديثات المشروعة	1.13	هجوم رفض الخدمة ضد مخدم التحديث أو الشبكة لمنع نشر تحديثات البرمجيات الهامة و/أو إطلاق الميزات الخاصة بالعميل
4.3.4 التهديدات للمركبات فيما يتعلق بالأعمال البشرية غير المقصودة	14	سوء تشكيل المعدات أو الأنظمة من قبل طرف مشروع، المالك أو فريق الصيانة	1.14	سوء تشكيل المعدات من قبل فريق الصيانة أو المالك أثناء التثبيت/الإصلاح/الاستخدام مما يتسبب في عواقب غير مقصودة
			2.14	الاستخدام الخاطئ للأجهزة والأنظمة أو إدارتها (بما في ذلك تحديثات OTA)
	15	الأطراف المشروعة قد تتخذ إجراءات من شأنها تسهيل هجوم سيبراني عن غير قصد	1.15	ضحية بريئة (مثل المالك أو المشغل أو مهندس الصيانة) يغرر بها لاتخاذ إجراء لتحميل برمجيات خبيثة أو تمكين هجوم عن غير قصد
			2.15	لا تتبع الإجراءات الأمنية المحددة
5.3.4 التهديدات للمركبات فيما يتعلق بتوصيليتها واتصالاتها الخارجية	16	التلاعب في توصيلية وظائف المركبة يتيح الهجوم السيبراني، ويمكن أن يشمل ذلك التيليماتية؛ والأنظمة التي تسمح بالعمليات عن بعد؛ والأنظمة التي تستخدم الاتصالات اللاسلكية قصيرة المدى	1.16	التلاعب بالوظائف المصممة لتشغيل الأنظمة عن بُعد، مثل المفتاح النائي، وجهاز إيقاف الحركة، وبطارية الشحن
			2.16	التلاعب في تليماتية المركبة (مثل التلاعب بقياس درجة حرارة البضائع الحساسة، وفتح أبواب الشاحنة عن بُعد)
			3.16	التداخل مع أنظمة لاسلكية أو محاسيس قصيرة المدى
	17	برمجية الطرف الثالث المستضاف، مثل تطبيقات الترفيه، تستخدم كوسيلة لمهاجمة أنظمة المركبات	1.17	تستخدم التطبيقات الفاسدة، أو تلك التي تتسم بقدر ضعيف من أمان البرمجية، كوسيلة لمهاجمة أنظمة المركبات
	18	الأجهزة الموصولة بالواجهات الخارجية، مثل منافذ USB، ومنفذ OBD، تستخدم كوسيلة لمهاجمة أنظمة المركبات	1.18	واجهات خارجية مثل USB أو منافذ أخرى تستخدم كنقطة هجوم، من خلال دس شفرة مثلاً
			2.18	الوسائط المصابة بفيروس موصول بنظام مركبة
			3.18	يستخدم النفاذ التشخيصي (مثل المضافات في منفذ التشخيص على متن المركبة OBD) لتسهيل الهجوم، مثل التلاعب بمعلمات المركبة (بشكلٍ مباشر أو غير مباشر)
6.3.4 الأهداف المحتملة لهجوم ما أو الدوافع له	19	استخراج بيانات المركبة/الشفرة	1.19	استخراج حقوق النشر أو البرمجيات المسجلة الملكية من أنظمة المركبات (قرصنة المنتج)
			2.19	نفاذ غير مرخص به إلى معلومات خصوصية المالك مثل الهوية الشخصية ومعلومات حساب الدفع ومعلومات دفتر العناوين ومعلومات الموقع ومعرف هوية المركبة الإلكتروني وما إلى ذلك.
			3.19	استخراج مفاتيح التجفير

الجدول 1.I – قائمة بأمثلة طريقة الضعف أو الهجوم المتعلقة بالتهديدات

وصف الاستضعاف/التهديد في المستوى الأعلى والمستوى الأدنى			مثال للاستضعاف أو طريقة الهجوم	
	20	التلاعب في بيانات/شفرة المركبة	1.20	تغييرات غير قانونية/غير مرخص بها في الهوية الإلكترونية للمركبة
			2.20	تزوير الهوية. مثال ذلك، إذا كان المستخدم يريد عرض هوية أخرى عند الاتصال بأنظمة تحصيل الرسوم، خلفية الجهة المصنعة
			3.20	التحايل على أنظمة المراقبة (مثل القرصنة/العبث/حظر الرسائل، بيانات تتبع جهاز تسجيل بيانات التشغيل (ODR) أو عدد مرات التشغيل)
			4.20	التلاعب بالبيانات لتزوير بيانات قيادة المركبة (مثل عدد الكيلومترات وسرعة القيادة واتجاهات القيادة، وما إلى ذلك)
			5.20	تغييرات غير مرخص بها في بيانات تشخيص النظام
	21	محو البيانات/الشفرة	1.21	الحذف/التلاعب غير المرخص به لسجلات أحداث النظام
	22	إدخال برمجيات خبيثة	2.22	إدخال برمجيات خبيثة أو نشاط برمجيات خبيثة
	23	إدخال برمجية جديدة أو استبدال برمجية موجودة	1.23	تصنيع برمجيات نظام التحكم في المركبة أو نظام معلومات المركبة
	24	تعطيل الأنظمة أو العمليات	1.24	رفض الخدمة، حيث يمكن إطلاق ذلك الشبكة الداخلية بإغراق ناقلة شبكة منطقة التحكم (CAN)، أو بإثارة أعطال في وحدة التحكم الإلكترونية عبر معدل رسائل مرتفع
	25	التلاعب في معلمات المركبة	1.25	نفاذ غير مرخص به لتزوير معلمات التشكيل في الوظائف الرئيسية للمركبة، مثل بيانات المكابح، وعتبة نشر الوسادة الهوائية، وما إلى ذلك
			2.25	نفاذ غير مرخص به من تزييف معلمات الشحن، مثل فلطية الشحن، وقوة الشحن، ودرجة حرارة البطارية، وما إلى ذلك
7.3.4 مواطن الضعف المحتملة التي يمكن استغلالها إن لم تكن محمية أو صلبة بما فيه الكفاية	26	يمكن تعطيل تقنيات التجفير أو عدم تطبيقها بشكلٍ كاف	1.26	الجمع بين مفاتيح التجفير القصيرة وفترة الصلاحية الطويلة يمكن المهاجم من فك التجفير
			2.26	عدم كفاية استخدام خوارزميات التجفير لحماية الأنظمة الحساسة
			3.26	استخدام خوارزميات التجفير تقادمت أو موشكة على التقادم
	27	أجزاء أو لوازم يمكن أن تتعرض للخطر وتعرض المركبات للهجوم	1.27	الأجهزة أو البرمجيات، مصممة هندسياً لتمكين الهجوم أو تفشل في تلبية معايير التصميم لوقف الهجوم
	28	تطوير البرمجيات أو الأجهزة يسمح بمواطن ضعف	1.28	أخطاء البرمجيات. قد يكون وجود أخطاء البرمجيات أساساً لمواطن ضعف قابلة للاستغلال. ويصح هذا بشكل خاص إذا لم تختبر البرمجية للتحقق من أن الشفرة السيئة /الأخطاء المعروفة غير موجودة وتقلل من خطر وجود الشفرات السيئة/الأخطاء غير المعروفة.
			2.28	استخدام البقايا من التطوير (مثل منافذ التصحيح، ومنافذ فريق عمل الاختبار المشترك (JTAG)، والمعالِجات الدقيقة، وشهادات التطوير، وكلمات سر المطورين، وغيرها) يمكن أن يسمح بالنفاذ إلى وحدات التحكم الإلكترونية (ECU) أو السماح للمهاجمين باكتساب امتيازات أعلى
	29	تصميم الشبكات ينطوي على مواطن ضعف	1.29	بقاء منافذ الإنترنت الزائدة مفتوحة، مما يوفر النفاذ إلى أنظمة الشبكة

الجدول 1.I – قائمة بأمثلة طريقة الضعف أو الهجوم المتعلقة بالتهديدات

وصف الاستضعاف/التهديد في المستوى الأعلى والمستوى الأدنى			مثال للاستضعاف أو طريقة الهجوم	
			2.29	التحايل على فاصل الشبكة للتمكن من التحكم. ثمة مثال محدد هو استخدام البوابات غير المحمية أو نقاط النفاذ (مثل بوابات الشاحنات– المقطورات)، للتحايل على عوامل الحماية والنفاذ إلى قطاعات الشبكة الأخرى للقيام بأعمال خبيثة، مثل إرسال رسائل تعسفية عبر ناقلة شبكة منطقة التحكم (CAN)
	30	احتمال حدوث فقدان مادي للبيانات	1.30	الأضرار الناجمة عن طرف ثالث. قد تفقد البيانات الحساسة أو تتعرض للخطر بسبب الأضرار المادية في حالات حوادث المرور أو السرقة
			2.30	الفقدان جراء تعارض إدارة الحقوق الرقمية (DRM). قد تحذف بيانات المستخدم بسبب مسائل DRM
			3.30	قد تُفقد (سلامة) البيانات الحساسة بسبب تآكل مكونات تكنولوجيا المعلومات، مما يسبب سلسلة من المشاكل المحتملة (في حالة تغيير المفتاح، مثلاً)
	31	احتمال حدوث نقل غير مقصود للبيانات	1.31	انتهاك المعلومات. قد تسرب البيانات الخاصة أو الحساسة عند تغيير مستخدم المركبة (عندما تباع أو تُستأجر من جانب مستخدمين جدد)
	32	التلاعب المادي بالأنظمة قد يمكن الهجوم	1.32	التلاعب بأجهزة مصنّع المعدات الأصلي (OEM)، مثال ذلك إضافة أجهزة غير مرخص بها إلى المركبة لتمكين هجوم "الاعتراض"

بيبليوغرافيا

[b-ITU-T X.800] التوصية ITU-T X.800 (1991)، *معمارية الأمن في التوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف.*

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

[b-UNECE GRVA-01-17] Draft recommendation on cyber security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA.

[b-UNECE GRVA] UNECE GRVA-01-17 (2017), *Draft Recommendation on cyber security of the Task Force on Cyber Security and Over-the-air Issues of UNECE WP.29 GRVA*. Available [viewed 2020-08-07] at: https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.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، 2020