Unión Internacional de Telecomunicaciones

UIT-T X.1371

(05/2020)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios seguros (2) – Seguridad de los sistemas de transporte inteligentes (STI)

Amenazas a la seguridad de los vehículos conectados

Recomendación UIT-T X.1371

UIT-T

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (STI)	**X.1370–X.1389**
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE 5G	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1371

Amenazas a la seguridad de los vehículos conectados

Resumen

En la Recomendación UIT-T X.1371 se describen amenazas a la seguridad de los vehículos conectados y al ecosistema del vehículo.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1371	29-05-2020	17	11.1002/1000/14090

Palabras clave

Vehículo conectado, amenaza a la seguridad.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1371

Amenazas a la seguridad de los vehículos conectados

1 Alcance

En esta Recomendación se describen amenazas a la seguridad de los vehículos conectados. En futuras Recomendaciones del UIT-T se podría hacer referencia a la presente Recomendación, a fin de garantizar que los aspectos relacionados con la seguridad de los sistemas de transporte inteligentes (STI) se tengan en cuenta de forma coherente.

2 Referencias

Las siguientes Recomendaciones UIT-T y otras referencias contienen disposiciones que, mediante referencia en este texto, constituyen disposiciones de la presente Recomendación. En el momento de la publicación, las ediciones indicadas eran válidas. Todas las Recomendaciones y demás referencias están sujetas a revisión; por lo tanto, se insta a los usuarios de esta Recomendación a que estudien la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias enumeradas a continuación. Se publica periódicamente una lista de las Recomendaciones del UIT-T en vigor. La referencia a un documento en la presente Recomendación no le confiere, como documento autónomo, la categoría de Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 disponibilidad [b-UIT-T X.800]: la propiedad de ser accesible y utilizable a petición de una entidad autorizada.

3.1.2 confidencialidad [b-UIT-T X.800]: propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

3.1.3 integridad [b-ISO/CEI 27000]: cualidad de preciso y completo.

3.1.4 amenaza [b-ISO/CEI 27000]: posible causa de un incidente no deseado, que puede dañar un sistema o perjudicar a una organización.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las abreviaturas y los acrónimos siguientes:

3G Tercera generación

4G Cuarta generación

5G Quinta generación

ADAS Sistema avanzado de asistencia al conductor (*advanced driver assistance system*)

CAN Red de controlador de zona (*controller area network*)

CAM Mensaje de sensibilización cooperativa (*cooperative awareness message*)

C-V2X Vehículo a X de tipo celular (*cellular-based vehicle-to-X*)

DENM Mensaje descentralizado de notificación medioambiental (*decentralized environmental notification message*)

DRM Gestión de derechos digitales (*digital rights management*)

DSRC Comunicación de corto alcance especializada (*dedicated short-range communication*)

ECU Unidad de control electrónico (*electronic control unit*)

GNSS Sistema mundial de navegación por satélite (*global navigation satellite system*)

ID Identificador

IVN Red intravehicular (*in-vehicle network*)

JTAG Grupo de acción de prueba conjunta (*joint test action group*)

LIN Red de interconexión local (*local interconnect network*)

MOST Transporte de sistemas orientados a los medios (*media oriented systems transport*)

OBD Diagnóstico a bordo (*on-board diagnostic*)

ODR Registrador de datos de funcionamiento (*operating data recorder*)

OEM Fabricante de equipo original (*original equipment manufacturer*)

OTA Por aire (*over-the-air*)

RF Radiofrecuencia

RSU Unidad al borde de la carretera (*roadside unit*)

SD *Secure Digital*

SQL Lenguaje de consulta estructurado (*structured query language*)

STI Sistema de transporte inteligente

TI Tecnología de la información

TIC Tecnología de la información y la comunicación

USB Bus serial universal (*universal serial bus*)

V2D Dispositivo de vehículo a nómada (*vehicle-to-nomadic device*)

V2I Vehículo a infraestructura (*vehicle-to-infrastructure*)

V2P Vehículo a peatón (*vehicle-to-pedestrian*)

V2V Vehículo a vehículo (*vehicle-to-vehicle*)

V2X Vehículo a X (*vehicle-to-X*)

VIN Número de identificación del vehículo (*vehicle identification number*)

Wi-Fi Fidelidad inalámbrica (*wireless fidelity*)

5 Convenios

Ninguno.

6 Modelo de vehículo conectado (ecosistema del vehículo)

En la Figura 1 se muestra el concepto de un vehículo conectado y su ecosistema. Este modelo es una representación conceptual del ecosistema del vehículo, y es independiente de implementaciones físicas o tecnologías concretas reconociéndose que éstas cambian con el paso del tiempo. Puede que el modelo no capte todas las tecnologías o los sistemas utilizados en un ecosistema de vehículo, pero puede utilizarse como base para determinar cuáles son las amenazas para la seguridad.

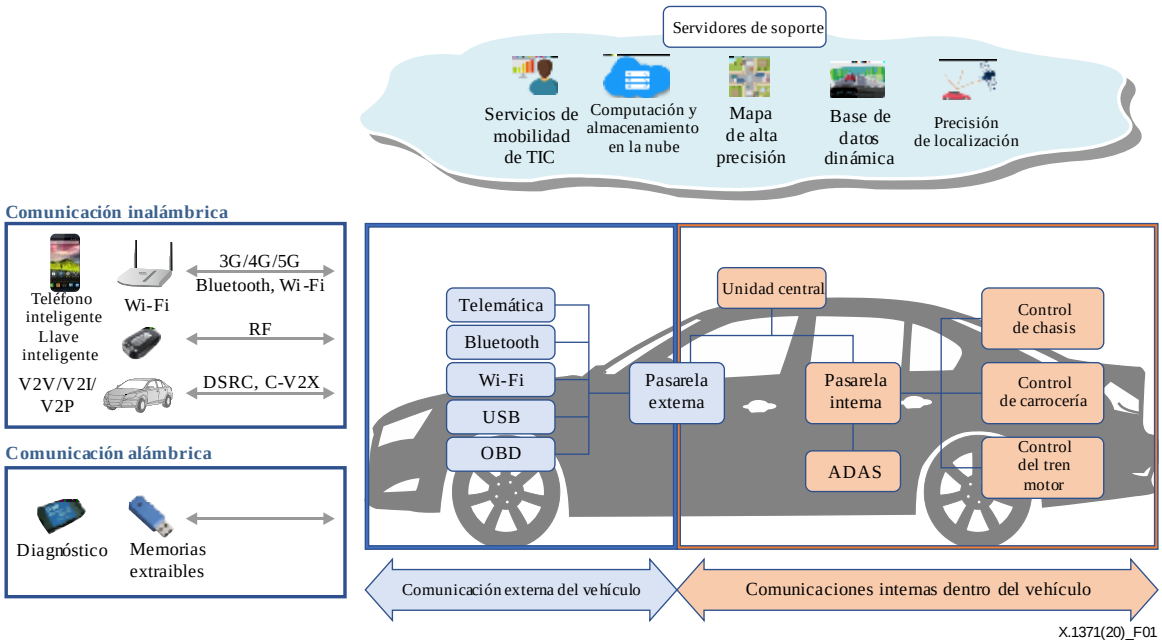

Figura 1 – Un concepto de vehículo conectado (ecosistema del vehículo)

Hoy en día, la tecnología de la comunicación desempeña un papel importante en los vehículos. Las comunicaciones de los vehículos se pueden clasificar en externas al vehículo e internas del vehículo. La red interna de un vehículo, conocida como red intravehicular (IVN), incluye componentes del vehículo tales como sensores y unidades de control electrónico (ECU). Estos sensores y ECU se utilizan en varios campos como el control de chasis, el control de carrocería y el control del tren motor del vehículo. Además, estos componentes se utilizan en un sistema avanzado de asistencia al conductor (ADAS), que presta asistencia al conductor mientras conduce, por ejemplo, para mantenerse en el carril de conducción y controlar la velocidad de crucero. La unidad central es un componente del infoesparcimiento a bordo del automóvil, que proporciona al usuario el control sobre los medios de información y esparcimiento del vehículo, por ejemplo, de audio y vídeo.

Las comunicaciones externas de un vehículo se denominan V2X, que significa "vehículo a cualquier cosa", siendo "cualquier cosa" todo aquello que revista importancia para el funcionamiento seguro y eficaz del vehículo. En particular, V2X se utiliza como término genérico para modos de comunicación tales como de vehículo a vehículo (V2V), de vehículo a infraestructura (V2I), de vehículo a dispositivo nómada (V2D) y de vehículo a peatón (V2P). La tecnología V2X incluye las comunicaciones de corto alcance especializadas (DSRC) y las V2X de tipo celular (C-V2X). La infraestructura consiste en unidades al borde de la carretera (RSU) e instalaciones de soporte, tales como sistemas de gestión y seguimiento del tráfico. Las RSU pueden estar conectadas a instalaciones de soporte mediante redes alámbricas o inalámbricas. En la Figura 1 se muestran varias funciones de los servidores de soporte, incluidos dispositivos de movilidad de tecnologías de la información y la comunicación (TIC), almacenamientos en la nube, mapas de alta definición, una base de datos dinámica para el entorno cercano y la localización precisa del vehículo.

En la Figura 1, las pasarelas interna y externa cumplen un papel en lo que respecta a la complejidad de la comunicación del vehículo. La pasarela interna gestiona los datos en el dominio interno del vehículo. La pasarela externa se encarga de las comunicaciones entre el vehículo y dispositivos externos, tales como teléfonos inteligentes y otros vehículos, mediante tecnología de comunicación V2X. La comunicación externa puede clasificarse en alámbrica e inalámbrica. La comunicación alámbrica puede utilizar un puerto de diagnóstico a bordo II (OBD II) para la comunicación con los dispositivos de diagnóstico y las actualizaciones del *software* o del *firmware* del vehículo. El canal de comunicaciones inalámbricas incluye la tecnología de telefonía móvil, Wi-Fi y Bluetooth para conectar un vehículo a dispositivos móviles tales como teléfonos inteligentes.

7 Amenazas a los vehículos conectados o al ecosistema del vehículo y posible información relacionada con las amenazas

7.1 Amenazas a los vehículos conectados o al ecosistema del vehículo

7.1.1 Amenazas relativas a los servidores de soporte

En los últimos años, la diversificación de la conectividad en vehículos ha aumentado notablemente y, en particular, se ha hecho muy necesaria la conectividad con varios servidores (llamados "servidores de soporte") situados en la parte posterior de los vehículos. Los servidores de soporte incluyen los proporcionados por los fabricantes de los equipos originales (OEM), los proveedores y los servicios de TIC para dar apoyo al ecosistema del vehículo desde el soporte a distancia.

7.1.1.1 Servidores de soporte utilizados como medio para atacar un vehículo o extraer datos

En el ecosistema de un vehículo, el servidor de soporte recoge principalmente datos del vehículo, los almacena y envía información al vehículo. Para evitar que el servidor de soporte se vea amenazado por una entidad no autorizada, deben abordarse las siguientes amenazas al mismo.

– Abuso de autoridad desde el interior: el abuso interno de los privilegios administrativos sobre el servidor de soporte puede revelar una filtración de datos desde el servidor, enviar falsa información al vehículo, etc.

– Acceso no autorizado desde el exterior a un servidor de soporte: si se mantiene una puerta de atrás o vulnerabilidad conocida en el servidor de soporte, puede explotarse desde el exterior para atacar al servidor de soporte mediante métodos de ataque como la infiltración de lenguaje de interrelación de bases de datos (SQL) y la implantación de programas maliciosos (*malware*). Si el atacante obtiene los privilegios administrativos del servidor, también deberían considerarse los mismos perjuicios que en el caso anterior.

– Acceso físico no autorizado: existen distintas maneras de acceder físicamente al servidor de soporte, por ejemplo, utilizando una memoria de tipo bus universal en serie (USB) o entrando en el edificio donde se encuentra el servidor utilizando un identificador (ID) profesional ficticio. En este caso, el daño y la interferencia con los datos relacionados con el vehículo y sus instalaciones de procesamiento de la información son aún mayores.

7.1.1.2 Perturbación de los servicios del servidor de soporte

Los ataques contra el servidor de soporte pueden ocasionar su mal funcionamiento y alterar su interacción con los vehículos y la prestación de servicios de los que dependen los vehículos. Además, pueden afectar seriamente a la disponibilidad de servicios relacionados con el vehículo como, por ejemplo, la gestión de las certificaciones para el vehículo y la infraestructura.

7.1.1.3 Pérdida o puesta en peligro de los datos del servidor de soporte

Los datos almacenados en un servidor de soporte pueden perderse o filtrarse si este se ve comprometido, ya sea a causa de un abuso de autoridad desde el interior, un acceso no autorizado desde el exterior o un acceso físico no autorizado, según se especifica en la cláusula 7.1.1.1. Además, se plantean las siguientes amenazas adicionales:

– Pérdida de información en la nube: la información sensible, como el número de identificación del vehículo (VIN) o la información personal del conductor, puede filtrarse y quedar comprometida, si está almacenada en sistemas de terceros proveedores de servicios de nube.

– Filtrado de información por un intercambio de datos no intencional: si un servidor está ubicado en un perímetro inseguro debido a una mala configuración por parte de un administrador, los datos pueden compartirse o filtrarse de manera no intencional.

7.1.2 Amenazas a los canales de comunicación de los vehículos

La comunicación del vehículo incluye comunicaciones externas, tales como las comunicaciones V2V, V2I, V2D y V2P, y comunicaciones dentro del vehículo, como las de la red de controlador de zona (CAN), la red de interconexión local (LIN), el transporte de sistemas orientados a los medios (MOST), y FlexRay. Los canales utilizados para estas comunicaciones pueden ser objeto de ataques tales como la usurpación de identidad, la escucha clandestina, la manipulación de mensajes, etc.

7.1.2.1 Mensajes de usurpación

Un emisor puede enviar un mensaje falso, usurpando la identidad de otro. En el caso de los mensajes utilizados en comunicaciones V2X y en el sistema mundial de navegación por satélite (GNSS), un vehículo puede recibir mensajes inválidos, debido a un ataque de usurpación de identidad. Además, si hay muchos vehículos en una determinada carretera, puede realizarse un ataque Sybil a fin de hacer suplantaciones de identidad en otros vehículos.

NOTA – Un ataque Sybil se produce, por ejemplo, cuando un vehículo simula múltiples vehículos utilizando múltiples identidades de vehículo.

7.1.2.2 Manipulación, supresión u otras modificaciones de códigos o datos almacenados en el vehículo

Si existe una vulnerabilidad o debilidad en el vehículo, pueden lanzarse ataques de acceso ilegal a distancia o intrusión de programas maliciosos a través de los canales de comunicación del vehículo. Como consecuencia, el canal de comunicación puede hacer posibles las siguientes amenazas a la seguridad:

– inyección de códigos, por ejemplo, un código binario de *software* que ha sido manipulado podría inocularse en la corriente de comunicación;

– manipulación de datos o códigos almacenados en el vehículo;

– sustitución de datos o códigos almacenados en el vehículo;

– borrado o supresión de datos o códigos almacenados en el vehículo.

7.1.2.3 Uso de mensajes sospechosos o no fiables y ataques por apropiación de la sesión o repetición

Pueden recibirse a través de los canales de comunicaciones mensajes de fuentes no fiables o sospechosas. Los ataques de intermediario (*Man-in-the-middle attack*) y la apropiación de sesión son posibles a través de los canales de comunicaciones. Por ejemplo, un ataque contra una pasarela de comunicación en el vehículo permite a un atacante degradar el *software* de una ECU o el *software* del fabricante (*firmware*) de la pasarela utilizando vulnerabilidades conocidas del *software* por medio de un ataque de repetición en el que se realizan repetidamente transferencias de datos válidas con fines maliciosos.

7.1.2.4 Divulgación de información

La información puede divulgarse directamente a través de la escucha ilegal de las comunicaciones o permitiendo el acceso no autorizado a archivos o carpetas confidenciales. Esto es, la información intercambiada a través del canal de comunicación puede ser escuchada ilegalmente a través de una interceptación maliciosa, la radiación interferente y el seguimiento de las comunicaciones. Con este fin, el atacante puede obtener derechos de acceso no autorizados a los archivos.

7.1.2.5 Ataques de denegación de servicio

Un atacante puede lanzar un ataque de denegación de servicio a través de un canal de comunicación enviando un gran volumen de datos basura al sistema de información del vehículo, de manera que se vean muy perturbadas las funciones del vehículo. Por otra parte, en casos de agrupación (*platooning*) de vehículos o de comunicaciones de vehículo a vehículo, el atacante podría impedir el envío de los datos necesarios a los demás vehículos del grupo, de tal manera que los otros vehículos pierdan el control debido a que carecen de datos de los demás vehículos. Esto se llama un "ataque de agujero negro" (*black hole attack*).

7.1.2.6 Acceso privilegiado por parte de un usuario sin privilegios

Mediante accesos ilegales a través de los canales de comunicación, un usuario sin privilegios puede obtener un acceso privilegiado, como por ejemplo el acceso al sistema como usuario de alto nivel (acceso a la raíz). Esto se llama un "aumento de privilegios no autorizado" (*unauthorized privilege escalation*) y, una vez llevado a cabo de forma satisfactoria, un atacante puede hacer cosas que están fuera del alcance de los usuarios normales.

7.1.2.7 Virus inoculados en los medios de comunicación

Una vez descubiertas las vulnerabilidades en el sistema del vehículo, es posible inocular virus o programas malintencionados en el sistema del vehículo a través de los canales de comunicación. Los virus pueden convertirse en administradores con acceso privilegiado y lanzar cualquier ataque que deseen en el vehículo. Por ejemplo, si el virus encripta cualquier archivo e información sin autorización en el sistema del vehículo objeto del ataque, lo que se conoce como "ransomware", entonces el sistema del vehículo perderá su función.

7.1.2.8 Mensajes con contenido malicioso

Los mensajes recibidos por el vehículo (por ejemplo, los mensajes de diagnóstico o los mensajes de otros vehículos), o transmitidos en su interior, pueden incluir contenidos maliciosos. En el caso de las IVN, un atacante puede modificar el *software* de las ECU mediante la inoculación de virus (véase la cláusula 7.1.2.7), y unirse a la red del vehículo como miembro utilizando la usurpación de identidad.

Los vehículos próximos pueden recibir mensajes V2X maliciosos, tales como mensajes de sensibilización cooperativa (CAM) y mensajes descentralizados de notificación medioambiental (DENM). La comunicación V2X se basa en la radiodifusión, por lo que son muchos los mensajes V2X maliciosos que pueden tener una influencia perjudicial sobre las redes vehiculares en su conjunto, incluidas las IVN en el propio vehículo.

También pueden recibirse mensajes de diagnóstico maliciosos. Un atacante puede registrar un mensaje de diagnóstico y utilizarlo para un ataque por repetición (*replay attack*). Además, incluso el mensaje de control del vehículo puede recibirse a través de un ataque de repetición.

Los mensajes propietarios suelen ser enviados por un OEM o un proveedor de componentes, sistemas o funciones. Sin embargo, también pueden recibirse de atacantes mensajes propietarios maliciosos, cuyo objetivo es perturbar el sistema del vehículo.

7.1.3 Amenazas a los vehículos a través de sus procedimientos de actualización

Existen dos maneras de actualizar los sistemas de los vehículos, a saber, la actualización mediante cable a través de un puerto OBD y dispositivos portátiles, como una tarjeta Secure Digital (SD) o una memoria USB, y la actualización inalámbrica por el aire (OTA). El *software* que hay que actualizar puede ser el del fabricante (*firmware*) o los datos de configuración del vehículo. La mayoría de los problemas electrónicos y los defectos de *software* pueden actualizarse y resolverse electrónicamente sin necesidad de acceso físico, por ejemplo, a través del probador OBD. Además, las actualizaciones OTA (inalámbricas) ayudan a acortar el ciclo de actualización para reducir al mínimo la exposición a los ataques a vulnerabilidades conocidas del *software*.

7.1.3.1 Uso indebido o puesta en peligro de los procedimientos de actualización

Con independencia de que la actualización se lleve a cabo de forma local o física, o mediante OTA, el procedimiento de actualización puede incluir amenazas que utilizan programas de actualización del sistema de fabricación o *software* comprometido del fabricante.

El *software* puede manipularse antes del proceso de actualización, aunque el proceso de actualización quede intacto. El proveedor de *software* crea o prepara el *software* para la actualización y lo entrega a los sistemas destinatarios que lo necesitan. Por tanto, puede existir una seria amenaza de manipulación y corrupción del *software* antes de su puesta en servicio.

Especialmente, los materiales criptográficos, tales como claves y certificados, utilizados en el proceso de actualización del *software* pueden quedar comprometidos y, en consecuencia, causar actualizaciones del *software* que no son válidas.

7.1.3.2 Denegación de actualización legítima

Durante el proceso de actualización del software, pueden producirse ataques de denegación de servicio contra un servidor o una red de actualización, para evitar la distribución de actualizaciones de *software* esenciales o desbloquear características específicas del cliente. También es posible denegar actualizaciones legítimas.

7.1.4 Amenazas a vehículos relativas a acciones humanas no intencionadas

Las acciones humanas pueden entrañar involuntariamente amenazas desconocidas. Estas amenazas incluyen, por defecto, la modificación no autorizada o inadvertida del *software*. Los errores incidentales pueden incluir violaciones de la configuración, errores de programación y corrupción de datos debido a errores cometidos por el usuario o el operador.

7.1.4.1 Mala configuración de equipos o sistemas por un actor legítimo

Un usuario legítimo puede tomar medidas que induzcan ciberataques de manera involuntaria. Un usuario legítimo puede modificar de forma involuntaria y anómala la configuración del sistema del vehículo durante su instalación, reparación o utilización. También se pueden producir errores al gestionar o utilizar sistemas o dispositivos que incluyen actualizaciones de *software*.

7.1.4.2 Facilitación involuntaria de un ciberataque por parte de un actor legítimo

Un usuario legítimo (por ejemplo, el propietario, el operador o el ingeniero de mantenimiento) puede ser una víctima inocente y verse inducido a realizar una acción para descargar de manera no intencional códigos maliciosos (*malware*) o para permitir un ataque. Además, el usuario legítimo a menudo no sigue procedimientos de seguridad definidos.

7.1.5 Amenazas a los vehículos en relación con su conectividad y sus conexiones externas

Para un gran número de servicios útiles, los vehículos pueden estar equipados con componentes para comunicar con servidores fuera del terminal, y pueden comunicarse con cualquier cosa habilitada por los usuarios de las carreteras a través de una conexión inalámbrica. Además de los servicios útiles, hay beneficios para la seguridad como son la funcionalidad de llamada de emergencia automática y

las que se apoyan en la comunicación V2X. Sin embargo, cuantos más vehículos se conectan a entidades exteriores para mejorar la conectividad, aparecen más amenazas y vulnerabilidades, ya que se amplían las superficies de ataque a través de interfaces adicionales.

7.1.5.1 Manipulación de la conectividad de las funciones del vehículo

La manipulación de la conectividad de las funciones del vehículo hace posible un ciberataque. Esta amenaza puede considerarse en los siguientes elementos del vehículo:

– manipulación de funciones destinadas a explotar sistemas a distancia: llave a distancia, inmovilizador y pila de carga;

– manipulación de la telemática del vehículo: por ejemplo, desbloqueo a distancia de la carga;

– manipulación a través de una interfaz con un sistema inalámbrico a corta distancia o sensores.

7.1.5.2 *Software* de terceros instalado

Un sistema de infoesparcimiento de un vehículo moderno conectado a la IVN puede permitir la instalación de aplicaciones de terceros. Es posible que las aplicaciones de terceros estén corruptas o cuenten con una seguridad de *software* insuficiente, y utilizarse como vectores para atacar los sistemas del vehículo.

7.1.5.3 Dispositivos conectados a interfaces externas

Las funciones de conectividad aportan interfaces externas y los dispositivos conectados a ellas pueden utilizarse como medio para atacar los sistemas del vehículo con las siguientes interfaces vulnerables:

– interfaces externas tales como el puerto USB: para atacar por medio de la inoculación de códigos;

– medios infectados por virus: el virus puede atacar el sistema interno del vehículo a través del medio infectado;

– acceso de diagnóstico: las funciones de diagnóstico a las que se accede a través de los adaptadores Bluetooth en puertos del OBD se utilizan para conocer la situación del vehículo y ajustar los parámetros incluidos en el *software* del vehículo.

7.2 Posible información relacionada con las amenazas

7.2.1 Posibles objetivos de, o motivos para, un ataque

Los vehículos pueden convertirse en el blanco de posibles ciberataques, en los casos en que están conectando electrónicamente a muchos sistemas o servicios del ecosistema del vehículo. Además, los atacantes a menudo buscan beneficios financieros dando a conocer sus habilidades de ataque no sólo al mundo en general, sino también a los OEM. Los ataques pueden afectar a los sistemas de los vehículos tal como se describe en las cláusulas 7.2.1.1 a 7.2.1.7.

7.2.1.1 Extracción de datos o códigos del vehículo

Los datos sensibles o las credenciales figuran entre los objetivos de las actividades de extracción, dado que pueden contener la siguiente información útil para obtener un beneficio financiero:

– derechos de autor o *software* patentado del vehículo;

– información privada del propietario, como datos personales, información de la cuenta de pago, información del libro de direcciones, información de localización y el ID electrónico del vehículo;

– las claves criptográficas, etc.

7.2.1.2 Manipulación de los datos o códigos del vehículo

Mediante la manipulación de los datos o códigos del vehículo, los atacantes pueden suplantar o repudiar el comportamiento del propietario legítimo. Pueden identificarse los siguientes métodos de manipulación:

– cambios ilegales/no autorizados al ID electrónico de un vehículo;
– fraude de identidad: si un usuario desea mostrar otra identidad al comunicarse con los sistemas de peaje y los sistemas de soporte del fabricante;
– medidas para eludir los sistemas de supervisión: piratería, manipulación o bloqueo de mensajes, tales como datos del registrador de datos de funcionamiento (ODR) o número de ejecuciones;
– manipulación de datos para falsificar los datos de conducción del vehículo, por ejemplo, el kilometraje, la velocidad de conducción, las direcciones de conducción y el tiempo de referencia del vehículo, etc.;
– cambios no autorizados a los datos de diagnóstico del vehículo;
– versión fraudulenta del *software* del fabricante (*firmware*): la última versión del *firmware*, que incluye un parche para compensar alguna vulnerabilidad, puede verse remplazada por la versión antigua que carece del correspondiente parche.

7.2.1.3 Borrado de datos o códigos

Puede producirse el borrado o manipulación sin autorización del registro de eventos del sistema. Esta falsificación hace a menudo imposible analizar los datos o dificulta la búsqueda de la causa del ataque.

7.2.1.4 Introducción de *malware*

Utilizando numerosos métodos de ataque, la introducción de *malware* en el sistema de un vehículo es el primer paso en la actividad de un atacante. Existen varias interfaces de ataque para introducir *malware*, por ejemplo, utilizando interfaces externas y módulos físicos infectados.

7.2.1.5 Introducción de nuevo *software* o sobreescritura del *software* existente

La introducción de *software* nuevo o la sobreescritura del existente con *software* malicioso puede afectar gravemente a la ciberseguridad del sistema de control del vehículo o del sistema de información.

7.2.1.6 Perturbación de los sistemas o de las operaciones

Puede lanzarse un ataque de denegación de servicio contra el sistema del vehículo en la red interna inundándola de mensajes en un bus de CAN o provocando fallos en una ECU mediante una alta densidad de mensajes.

7.2.1.7 Manipulación de los parámetros del vehículo

La manipulación de los parámetros del vehículo puede tener una fuerte influencia sobre el sistema del vehículo, véase el acceso no autorizado para falsificar:

– los parámetros de configuración de las funciones clave de un vehículo, por ejemplo, los datos de frenado o el umbral para el despliegue del airbag;
– los parámetros de carga, tales como el voltaje de carga, la potencia de carga, la temperatura de la batería, etc.

7.2.2 Posibles vulnerabilidades

7.2.2.1 Tecnologías criptográficas vulnerables

Las tecnologías criptográficas pueden quedar comprometidas o aplicarse de manera insuficiente. Es posible explotar las claves o certificados criptográficos que incluyen credenciales, como una contraseña. Por ejemplo, si se utilizan claves criptográficas débiles o las claves criptográficas no se actualizan desde hace tiempo, es posible quebrar el sistema criptográfico mediante ataques de fuerza bruta. El uso insuficiente de tecnologías criptográficas puede dar lugar a una filtración de claves criptográficas o credenciales. Además, puede acrecentarse el riesgo de filtración de información con el uso de tecnologías criptográficas ya quebradas u obsoletas.

7.2.2.2 Piezas o suministros del vehículo expuestos

El *hardware* o el *software* utilizado en el ecosistema de un vehículo pueden manipularse de tal manera que este último no cumpla los criterios de diseño que permiten defenderse de un ataque. En posible dejar expuestos piezas o suministros de un vehículo para que éste pueda ser objeto de ataques.

7.2.2.3 Vulnerabilidades de concepción del *software* o de los equipos

La presencia de errores de programación puede servir de base para vulnerabilidades potencialmente explotables. Esto resulta especialmente cierto si no se ha probado el *software* para verificar si contiene códigos incorrectos o errores de programación reconocidos y reducir el riesgo de que incluya códigos incorrectos o errores de programación.

La utilización de restos del desarrollo (por ejemplo, puertos de depuración de errores, puertos acordes a la norma del grupo de acción de prueba conjunta (JTAG), microprocesadores, certificados de desarrollo y contraseñas de programador) también puede dar acceso a las ECU o permitir a los atacantes obtener privilegios más elevados.

7.2.2.4 Vulnerabilidades en el diseño de la red

Si se permite el acceso a la red al tiempo que se dejan puertos de comunicación innecesariamente abiertos, es probable que aumenten ataques tales como los de acceso no autorizado.

Además, el uso de pasarelas o de puntos de acceso (como las pasarelas camión-remolque) desprotegidos para eludir las protecciones y obtener acceso a otros segmentos de la red puede dar lugar a actos maliciosos, tales como el envío de mensajes de bus CAN arbitrarios.

7.2.2.5 Pérdida física de datos

Los datos sensibles utilizados en el ecosistema del vehículo pueden perderse o quedar comprometidos debido a daños físicos causados por accidentes de tráfico o robos. También puede darse la pérdida de datos de gestión de derechos digitales (DRM), como la supresión de datos del usuario.

Además, puede perderse la integridad de datos sensibles debido al desgaste normal de los componentes de las tecnologías de la información (TI), lo que puede ocasionar problemas en cascada (por ejemplo, en el caso de alteración de la clave).

7.2.2.6 Transferencia de datos no intencional

Datos privados o sensibles pueden filtrarse cuando cambian los usuarios del vehículo (por ejemplo, cuando el vehículo se vende o es utilizado por otra persona como vehículo de alquiler).

7.2.2.7 Manipulación física de los sistemas

La manipulación física de sistemas como el equipo del OEM puede dar lugar a ataques. Por ejemplo, si se añaden equipos no autorizados al vehículo es posible un ataque de intermediario.

Apéndice I

Ejemplos de vulnerabilidad o métodos de ataque relacionados con las amenazas

(Este apéndice no forma parte integrante de la presente Recomendación.)

En este Apéndice se facilitan ejemplos de vulnerabilidad o métodos de ataque relacionados con las amenazas que figuran en el Cuadro 1 de [b-UNECE GRVA].

NOTA – Los números de apartado indicados en la columna de la izquierda del Cuadro I.1 son los utilizados en [b-UNECE GRVA].

Cuadro I.1 – Lista de ejemplos de vulnerabilidad o métodos de ataque relacionados con las amenazas

Descripciones de alto nivel y de nivel inferior de la vulnerabilidad/amenaza			**Ejemplo de vulnerabilidad o métodos de ataque**	
4.3.1 Amenazas en relación con los servidores de soporte	1	Servidores de soporte utilizados como medio para atacar un vehículo o extraer datos	1.1	Abuso de privilegios por parte del personal (ataque desde el interior)
			1.2	Acceso no autorizado de Internet al servidor (permitido, por ejemplo, por puertas traseras, vulnerabilidades del *software* de sistema sin parches, ataques SQL u otros medios)
			1.3	Acceso físico no autorizado al servidor (realizado mediante, por ejemplo, llaves USB u otros medios que se conectan al servidor)
	2	Perturbación de los servicios del servidor de soporte, afectando al funcionamiento de un vehículo	2.1	El ataque al servidor de soporte detiene su funcionamiento, por ejemplo, le impide interactuar con los vehículos y proporcionar los servicios de los que éstos dependen
	3	Pérdida o puesta en peligro de los datos almacenados en los servidores de soporte ("ruptura de datos")	3.1	Abuso de privilegios por parte del personal (ataque desde el interior)
			3.2	Pérdida de información en la nube. Pueden perderse datos sensibles debido a ataques o accidentes cuando los datos son almacenados por un tercer proveedor de servicios de nube
			3.3	Acceso no autorizado de Internet al servidor (permitido, por ejemplo, por puertas traseras, vulnerabilidades del *software* de sistema sin parches, ataques SQL u otros medios)
			3.4	Acceso físico no autorizado al servidor (realizado mediante, por ejemplo, llaves USB u otros medios que se conectan al servidor)
			3.5	Comunicación involuntaria de información por el intercambio no intencional de datos (por ejemplo, errores administrativos, almacenamiento de datos en servidores situados en garajes)

Cuadro I.1 – Lista de ejemplos de vulnerabilidad o métodos de ataque relacionados con las amenazas

Descripciones de alto nivel y de nivel inferior de la vulnerabilidad/amenaza			Ejemplo de vulnerabilidad o métodos de ataque	
4.3.2 Amenazas a los vehículos en relación con sus canales de comunicación	4	Pirateo de mensajes o datos recibidos por el vehículo	4.1	Pirateo de mensajes mediante usurpación de identidad (por ejemplo, 802.11p V2X durante la agrupación, mensajes del GNSS, etc.)
			4.2	Ataque Sybil (a fin de piratear otros vehículos, como si hubiera muchos vehículos en la carretera)
	5	Canales de comunicación utilizados para proceder a la manipulación no autorizada, la supresión u otras modificaciones en los códigos/datos mantenidos en el vehículo	5.1	Los canales de comunicación permiten la inyección de códigos, por ejemplo, puede inyectarse *software* binario manipulado en la corriente de comunicación
			5.2	Los canales de comunicación permiten la manipulación de códigos/datos mantenidos en el vehículo
			5.3	Los canales de comunicación permiten sobrescribir códigos/datos mantenidos en el vehículo
			5.4	Los canales de comunicación permiten el borrado de los códigos/datos mantenidos en el vehículo
			5.5	Los canales de comunicación permiten la introducción de códigos/datos en el vehículo (*write data code*)
	6	Los canales de comunicación permiten aceptar mensajes sospechosos/no fiables o son vulnerables al pirateo de sesión/ataques por repetición	6.1	Aceptar información de una fuente sospechosa/no fiable
			6.2	Ataque de intermediario/pirateo de sesión
			6.3	Ataque por repetición, por ejemplo, un ataque contra una pasarela de comunicación permite al atacante degradar el *software* de un ECU o el *software* del fabricante de la pasarela
	7	Es posible descubrir directamente la información. Por ejemplo, mediante escuchas de las comunicaciones o permitiendo el acceso no autorizado a archivos o carpetas sensibles	7.1	Intercepción de información/interferencia de radiaciones/seguimiento de las comunicaciones
			7.2	Obtener acceso no autorizado a archivos o datos
	8	Ataques de denegación de servicio a través de los canales de comunicación para perturbar las funciones del vehículo	8.1	Enviar un gran número de datos basura al sistema de información del vehículo, de manera que no pueda prestar servicios de manera normal
			8.2	Ataque de agujero negro a fin de perturbar las comunicaciones entre vehículos, el atacante es capaz de bloquear mensajes entre los vehículos

Cuadro I.1 – Lista de ejemplos de vulnerabilidad o métodos de ataque relacionados con las amenazas

Descripciones de alto nivel y de nivel inferior de la vulnerabilidad/amenaza			Ejemplo de vulnerabilidad o métodos de ataque	
	9	Un usuario sin privilegios es capaz de obtener acceso privilegiado a los sistemas del vehículo	9.1	Un usuario sin privilegios es capaz de obtener acceso privilegiado, por ejemplo, acceso a nivel de raíz
	10	Los virus integrados en los medios de comunicación pueden infectar los sistemas de los vehículos	10.1	Virus integrados en los medios de comunicación infectan los sistemas de los vehículos
	11	Los mensajes recibidos por el vehículo (por ejemplo, mensajes X2V o de diagnóstico) o transmitidos en él incluyen contenido malicioso	11.1	Mensajes internos (por ejemplo, CAN) maliciosos
			11.2	Mensajes V2X maliciosos, por ejemplo, mensajes de infraestructura a vehículo o de vehículo a vehículo (por ejemplo, CAM, DENM)
			11.3	Mensajes de diagnóstico maliciosos
			11.4	Mensajes propietarios maliciosos (por ejemplo, los enviados normalmente por el OEM o el proveedor de componentes/sistemas/funciones)
4.3.3 Amenazas a los vehículos en relación con sus procedimientos de actualización	12	Uso indebido o puesta en peligro de los procedimientos de actualización	12.1	Puesta en peligro de los procedimientos de actualización del *software* inalámbricos. Esto incluye la fabricación de programas de actualización del sistema y de *software* del fabricante
			12.2	Puesta en peligro de los procedimientos de actualización del *software* locales/físicos
			12.3	El *software* es objeto de manipulación antes del proceso de actualización (y está por tanto corrompido), aunque el proceso de actualización permanezca intacto
			12.4	Puesta en peligro de las claves criptográficas del proveedor de *software* para permitir actualizaciones no válidas
	13	Es posible denegar actualizaciones legítimas	13.1	Ataque de denegación de servicio contra el servidor o la red de actualización para evitar la distribución de actualizaciones de *software* esencial y/o desbloquear características específicas del cliente
4.3.4 Amenazas a los vehículos en relación con acciones humanas no intencionales	14	Mala configuración de equipos o sistemas por un actor legítimo, por ejemplo, el propietario o la comunidad de mantenimiento	14.1	Mala configuración del equipo por parte de la comunidad de mantenimiento o el propietario durante la instalación/reparación/utilización provocando consecuencias no deseadas
			14.2	Utilización o administración erróneas de los dispositivos y sistemas (incluidas las actualizaciones OTA)

Cuadro I.1 – Lista de ejemplos de vulnerabilidad o métodos de ataque relacionados con las amenazas

Descripciones de alto nivel y de nivel inferior de la vulnerabilidad/amenaza			Ejemplo de vulnerabilidad o métodos de ataque	
	15	Actores legítimos pueden tomar medidas que facilitarían involuntariamente un ciberataque	15.1	Se engaña a la víctima inocente (por ejemplo, el propietario, el operador o el ingeniero de mantenimiento) para que realice una acción a fin de cargar sin intención un *software* malicioso o de permitir un ataque
			15.2	No se siguen los procedimientos de seguridad definidos
4.3.5 Amenazas a los vehículos en relación con su conectividad y sus conexiones externas	16	La manipulación de la conectividad de las funciones del vehículo hace posible un ciberataque, esto puede incluir la telemática; sistemas que permiten operaciones a distancia; y sistemas que utilizan comunicaciones inalámbricas de corto alcance	16.1	Manipulación de funciones destinada a explotar sistemas a distancia, como la clave a distancia, el inmovilizador y la pila de carga
			16.2	Manipulación de la telemática del vehículo (por ejemplo, manipular la medición de temperatura de bienes sensibles, desbloquear a distancia las puertas de carga)
			16.3	Interferencia con sistemas o sensores inalámbricos de corto alcance
	17	Alojamiento de *software* de terceros, por ejemplo, aplicaciones de entretenimiento utilizadas para atacar los sistemas del vehículo	17.1	Aplicaciones corruptas, o las que disponen de poca seguridad del *software*, utilizadas para atacar los sistemas del vehículo
	18	Dispositivos conectados a interfaces externas, por ejemplo, puertos USB o puerto OBD, utilizados como medio para atacar a los sistemas del vehículo	18.1	Interfaces externas tales como puertos USB o de otro tipo utilizados como punto de ataque, por ejemplo, mediante la inoculación de códigos
			18.2	Medios infectados por un virus y conectados a un sistema del vehículo
			18.3	Se utiliza el acceso de diagnóstico (por ejemplo, adaptadores en el puerto OBD) para facilitar un ataque, por ejemplo, manipulando (directa o indirectamente) los parámetros del vehículo
4.3.6 Posibles objetivos de, o motivos para, un ataque	19	Extracción de datos/códigos del vehículo	19.1	Extracción de los derechos de autor o del *software* patentado de los sistemas del vehículo (pirateo de producto)
			19.2	Acceso no autorizado a la información privada del propietario como la identidad personal, la información de la cuenta de pago, la información del libro de direcciones, la información de localización y el identificador electrónico del vehículo, etc.
			19.3	Extracción de claves criptográficas
	20	Manipulación de los datos/códigos del vehículo	20.1	Cambios ilegales/no autorizados al identificador electrónico de un vehículo

Cuadro I.1 – Lista de ejemplos de vulnerabilidad o métodos de ataque relacionados con las amenazas

Descripciones de alto nivel y de nivel inferior de la vulnerabilidad/amenaza			Ejemplo de vulnerabilidad o métodos de ataque	
			20.2	Fraude de identidad. Por ejemplo, si un usuario desea mostrar otra identidad al comunicarse con los sistemas de peaje y los sistemas de soporte del fabricante
			20.3	Medidas para eludir los sistemas de supervisión (por ejemplo, la piratería/manipulación/bloqueo de mensajes tales como los datos del registrador de datos ODR o el número de ejecuciones)
			20.4	Manipulación de datos para falsificar los datos de conducción del vehículo (por ejemplo, kilometraje, dirección de conducción, instrucciones de conducción, etc.)
			20.5	Cambios no autorizados de los datos de diagnóstico del sistema
	21	Borrado de datos/códigos	21.1	Borrado o manipulación sin autorización del registro de eventos del sistema
	22	Introducción de *malware*	22.2	Introducir *software* malicioso o actividad de *software* malicioso
	23	Introducción de nuevo *software* o sobreescritura del *software* existente	23.1	Fabricación de *software* del sistema de control o del sistema de información del vehículo
	24	Perturbación de los sistemas o de las operaciones	24.1	Denegación de servicio, por ejemplo, puede ponerse en marcha en la red interna inundándola de mensajes en un bus de CAN o provocando fallos en una ECU mediante una alta densidad de envío de mensajes
	25	Manipulación de los parámetros del vehículo	25.1	Acceso no autorizado para falsificar los parámetros de configuración de las funciones clave de un vehículo, por ejemplo, los datos de frenado o el umbral para el despliegue del airbag, etc.
			25.2	Acceso no autorizado para falsificar los parámetros de carga, tales como el voltaje de carga, la potencia de carga, la temperatura de la batería, etc.
4.3.7 Vulnerabilidades potenciales que podrían ser explotadas si no están suficientemente protegidas o fortalecidas	26	Pueden ponerse en peligro o se aplican insuficientemente las tecnologías criptográficas	26.1	La combinación de claves de encriptado cortas y largos periodos de validez permiten al atacante romper las claves
			26.2	Utilización insuficiente de algoritmos criptográficos para proteger sistemas sensibles
			26.3	Utilizar o aprestarse a utilizar algoritmos criptográficos obsoletos
	27	Las partes o los suministros podrían quedar comprometidos a fin de permitir que se ataque a los vehículos	27.1	Equipos o *software*, diseñados para permitir un ataque o que no cumplen los criterios para detener un ataque

Cuadro I.1 – Lista de ejemplos de vulnerabilidad o métodos de ataque relacionados con las amenazas

Descripciones de alto nivel y de nivel inferior de la vulnerabilidad/amenaza			Ejemplo de vulnerabilidad o métodos de ataque	
	28	La concepción del *software* o de los equipos permite vulnerabilidades	28.1	Errores de programación. La presencia de errores de programación puede servir de base para vulnerabilidades potencialmente explotables. Esto resulta especialmente cierto si no se ha probado el *software* para verificar que no estén presentes códigos incorrectos/errores de programación reconocidos y reducir el riesgo de la presencia de códigos incorrectos/errores de programación
			28.2	La utilización de restos del desarrollo (por ejemplo, puertos de depuración de errores, puertos JTAG, microprocesadores, certificados de desarrollo, contraseñas de programador, etc.) también puede dar acceso a las ECU o permitir a los atacantes obtener privilegios más elevados
	29	El diseño de la red introduce vulnerabilidades	29.1	Puertos de comunicación que se dejan abiertos sin necesidad, dando acceso a los sistemas de la red
			29.2	Evitar la separación de redes para obtener el control. Un ejemplo concreto es el uso de pasarelas o de puntos de acceso (como las pasarelas camión-remolque) desprotegidos para eludir las protecciones y obtener acceso a otros segmentos de la red para realizar actos maliciosos tales como el envío de mensajes de bus CAN arbitrarios
	30	Puede producirse la pérdida física de los datos	30.1	Daños causados por un tercero. Los datos sensibles pueden perderse o quedar comprometidos debido a daños físicos en casos de accidentes de tráfico o robo
			30.2	Pérdida de datos por conflictos de gestión de los derechos digitales (DRM). Los datos del usuario pueden borrarse por problemas de DRM
			30.3	Pueden perderse datos sensibles (o la integridad de los mismos) debido al desgaste normal de los componentes de TI, pudiendo ocasionar problemas en cascada (en caso de alteración de la clave, por ejemplo)
	31	Puede producirse la transferencia de datos no intencional	31.1	Datos privados o sensibles pueden filtrarse cuando cambian los usuarios del vehículo (por ejemplo, cuando el vehículo se vende o es utilizado por otras personas como vehículo de alquiler)
	32	La manipulación física de los sistemas puede hacer posible un ataque	32.1	La manipulación del equipo del OEM, por ejemplo, añadiendo equipos no autorizados al vehículo, hacen que sea posible un ataque de intermediario

Bibliografía

[b-UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

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

[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*. Disponible [consultado el 07-08-2020] en: https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2020