Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1371

(05/2020)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés (2) – Sécurité des systèmes de transport intelligents

Menaces pour la sécurité des véhicules connectés

Recommandation UIT-T X.1371

Union internationale des télécommunications

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	**X.1370–X.1389**
Sécurité de la technologie des registres distribués	X.1400–X.1429
Sécurité de la technologie des registres distribués	X.1430–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1371

Menaces pour la sécurité des véhicules connectés

Résumé

La Recommandation X.1371 décrit les menaces pour la sécurité des véhicules connectés et l'écosystème des véhicules.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1371	2020-05-29	17	11.1002/1000/14090

Mots clés

Menace pour la sécurité, véhicule connecté.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

© UIT 2020

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	1
	3.1 Termes définis ailleurs	1
	3.2 Termes définis dans la présente Recommandation	1
4	Abréviations et acronymes	1
5	Conventions	2
6	Modèle de véhicule connecté (écosystème du véhicule)	3
7	Menaces pour les véhicules connectés ou l'écosystème des véhicules et informations possibles concernant les menaces	4
	7.1 Menaces pour les véhicules connectés ou l'écosystème des véhicules	4
	7.2 Informations potentielles concernant les menaces	8
Appendice I – Exemples de vulnérabilités ou de méthodes d'attaque relatives aux menaces		11
Bibliographie		17

Recommandation UIT-T X.1371

Menaces pour la sécurité des véhicules connectés

1 Domaine d'application

La présente Recommandation décrit les menaces qui pèsent sur la sécurité des véhicules connectés. On pourrait faire mention de cette Recommandation dans les Recommandations futures de l'UIT-T, pour veiller à ce qu'elles prennent systématiquement en considération les aspects sécurité des systèmes de transport intelligents (ITS).

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut d'une Recommandation.

Néant.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 disponibilité [b-UIT-T X.800]: Propriété d'être accessible et utilisable sur demande par une entité autorisée.

3.1.2 confidentialité [b-UIT-T X.800]: Propriété d'une information qui en interdit l'accès à des personnes, des entités ou des processus non autorisés.

3.1.3 intégrité [b-ISO/CEI 27000]: Propriété d'exactitude et d'exhaustivité.

3.1.4 menace [b-ISO/CEI 27000]: Source potentielle d'évènements indésirables qui peuvent nuire à un système ou à un organisme.

3.2 Termes définis dans la présente Recommandation

Néant.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

3G troisième génération

4G quatrième génération

5G cinquième génération

ADAS système évolué d'aide à la conduite (*Advanced Driver Assistance System*)

CAM message de sensibilisation fondé sur la coopération (*Cooperative Awareness Message*)

CAN gestionnaire de réseau de communication (*Controller Area Network*)

C-V2X systèmes cellulaires de véhicule à X (*Cellular-based Vehicle-to-X*)

DENM message de notification environnementale décentralisé (*Decentralized Environmental Notification Message*)

DRM gestion des droits numériques (*Digital Right Management*)

DSRC communications spécialisées à courte distance (*Dedicated Short-Range Communication*)

ECU unité de commande électronique (*Electronic Control Unit*)

GNSS système mondial de navigation par satellite (*Global Navigation Satellite System*)

ID identifiant (*Identifier*)

IT technologies de l'information (*Information Technology*)

ITS système de transport intelligent (*Intelligent Transport System*)

IVN réseau embarqué (*In-Vehicle Network*)

JTAG groupe d'action de test mixte (*Joint Test Action Group*)

LIN réseau local d'interconnexion (*Local Interconnect Network*)

MOST transport dans des systèmes orientés média (*Media Oriented Systems Transport*)

OBD diagnostic embarqué (*On-Board Diagnostics*)

ODR enregistreur de données de fonctionnement (*Operating Data Recorder*)

OEM fabricant d'équipements d'origine (*Original Equipment Manufacturer*)

OTA transmission sans fil (*Over-The-Air*)

RF fréquence radioélectrique (*Radio Frequency*)

RSU unité de bord de route (*Roadside Unit*)

SD numérique sécurisé (*Secure Digital*)

SQL langage de requête structuré (*Structured Query Language*)

TIC technologies de l'information et de la communication

USB bus série universel (*Universal Serial Bus*)

V2D de véhicule à dispositif nomade (*Vehicle-to-Nomadic Device*)

V2I de véhicule à infrastructure (*Vehicle-to-Infrastructure*)

V2P de véhicule à piéton (*Vehicle-to-Pedestrian*)

V2V de véhicule à véhicule (*Vehicle-to-Vehicle*)

V2X de véhicule à X (*Vehicle-to-X)*

VIN identifiant du véhicule (*Vehicle Identification Number*)

WiFi fidélité sans fil (*Wireless Fidelity*)

5 Conventions

Néant.

6 Modèle de véhicule connecté (écosystème du véhicule)

La Figure 1 illustre le concept de véhicule connecté et de l'écosystème qui lui est associé. Ce modèle est une représentation conceptuelle de l'écosystème du véhicule, et est indépendant des mises en œuvre physiques ou des technologies particulières, étant donné que celles-ci sont appelées à évoluer au fil du temps. Ce modèle peut ne pas recouvrir toutes les technologies ou tous les systèmes utilisés dans l'écosystème d'un véhicule, mais peut servir de base à l'identification des menaces pour la sécurité.

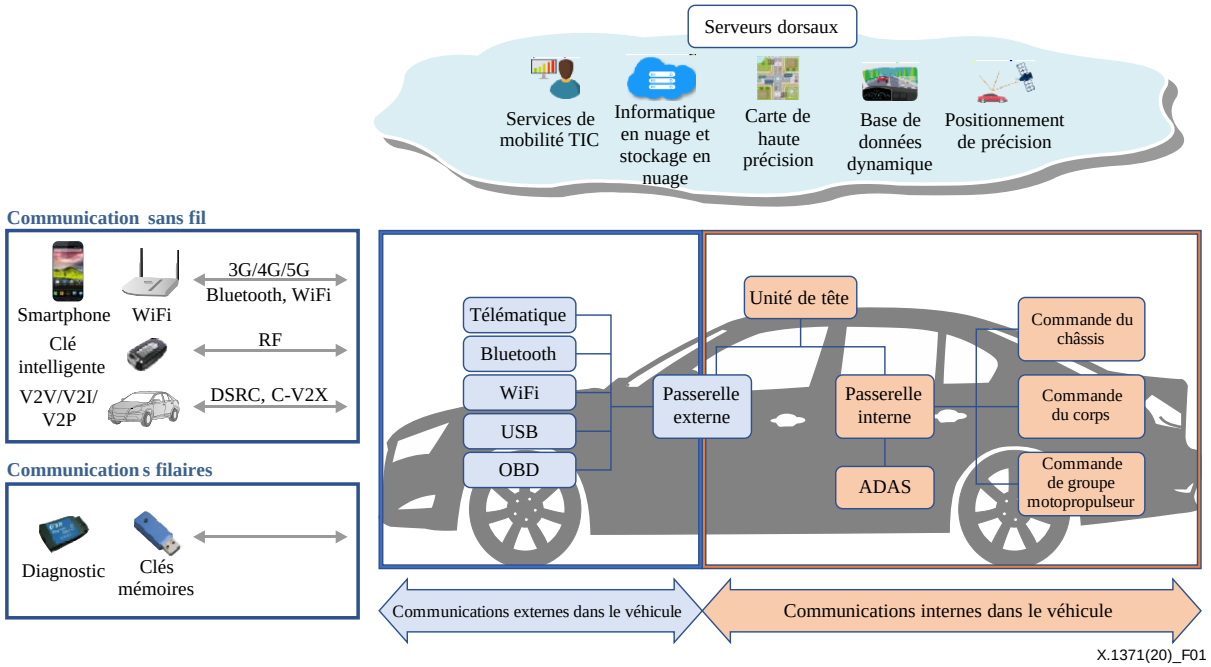

Figure 1 – Concept de véhicule connecté (écosystème du véhicule)

À l'heure actuelle, les technologies de communication jouent un rôle important dans les véhicules. Les communications dans un véhicule peuvent être classées en communications externes ou internes à un véhicule. Le réseau interne d'un véhicule, appelé réseau embarqué (IVN), comprend des composants de véhicule tels que des capteurs et des unités de commande électronique (ECU). Ces capteurs et ces unités ECU sont utilisés dans plusieurs domaines, tels que la commande du châssis, la commande du corps et la commande de groupe motopropulseur du véhicule. De plus, ces composants sont utilisés dans un système évolué d'aide à la conduite (ADAS), qui est destiné à aider le conducteur pendant la conduite d'un véhicule et offre par exemple des fonctionnalités d'aide au maintien dans la voie de circulation et de régulation de la vitesse. L'unité de tête est un composant des systèmes d'infoloisirs à bord des véhicules, qui permet à l'usager de commander les informations et les supports de divertissement – audio et vidéo par exemple – du véhicule.

On appelle communications V2X – à savoir les communications "entre un véhicule et tous les éléments", les communications externes d'un véhicule, "tous les éléments" désignant tout ce qui se rapporte à la sécurité et à l'efficacité du fonctionnement du véhicule. En particulier, les communications V2X sont utilisées comme terme générique pour désigner des modes de communication tels que les communications entre véhicules (V2V), de véhicule à infrastructure (V2I), de véhicule à dispositif nomade (V2D) et de véhicule à piéton (V2P). Les technologies V2X comprennent les communications spécialisées à courte portée (DSRC) et les communications cellulaires V2X (C-V2X). L'infrastructure comprend des unités de bord de route (RSU) et des installations dorsales, par exemple des systèmes de gestion et de surveillance du trafic. Les unités RSU peuvent être connectées aux installations dorsales par des réseaux filaires ou hertziens. La Figure 1 illustre différentes fonctions proposées dans les serveurs dorsaux, à savoir les services de

mobilité issus des technologies de l'information et de la communication (TIC), le stockage dans le nuage, les cartes haute définition, une base de données dynamique pour l'environnement voisin et le positionnement de précision du véhicule.

Les passerelles externes et internes indiquées sur la Figure 1 jouent un rôle pour remédier à la complexité des communications à bord de véhicules. La passerelle interne gère les données dans le domaine des technologies embarquées dans le véhicule. La passerelle externe est responsable des communications entre le véhicule et des dispositifs externes, par exemple un smartphone et d'autres véhicules par l'intermédiaire des technologies de communication V2X. Les communications externes peuvent être classées en communications filaires et en communications hertziennes. Les communications filaires peuvent utiliser le port II de diagnostic embarqué (OBD II) pour communiquer avec les dispositifs de diagnostic et les mises à jour de logiciels ou de micrologiciels du véhicule. Le canal de communication hertzien comprend des techniques de communication cellulaire, ainsi que les techniques WiFi et Bluetooth pour connecter un véhicule à des dispositifs mobiles, par exemple un smartphone.

7 Menaces pour les véhicules connectés ou l'écosystème des véhicules et informations possibles concernant les menaces

7.1 Menaces pour les véhicules connectés ou l'écosystème des véhicules

7.1.1 Menaces concernant les serveurs dorsaux

Ces dernières années, la connectivité des véhicules s'est considérablement diversifiée et la connectivité avec différents serveurs (appelés "serveurs dorsaux") situés à l'extrémité arrière des véhicules, en particulier, est devenue absolument indispensable. Les serveurs dorsaux comprennent ceux qui sont fournis par les fabricants d'équipements d'origine (OEM), par les fournisseurs et par les services TIC pour prendre en charge l'écosystème des véhicules depuis le système dorsal distant.

7.1.1.1 Serveurs dorsaux utilisés pour attaquer un véhicule ou extraire des données

Dans un écosystème de véhicule, le serveur dorsal recueille principalement des données auprès du véhicule, les stocke puis envoie les informations au véhicule. Le serveur dorsal devra faire face aux menaces ci-après pour éviter d'être compromis par une entité non autorisée:

– Abus de pouvoir de la part d'un initié: L'abus de droits d'administrateur de la part d'un initié au niveau du serveur dorsal peut faire apparaître des fuites de données en provenance du serveur, envoyer des informations erronées au véhicule, etc.

– Accès non autorisé depuis l'extérieur vers un serveur dorsal: S'il subsiste une vulnérabilité par des portes dérobées ou une vulnérabilité connue dans le serveur dorsal, elle peut être exploitée de l'extérieur pour attaquer le serveur dorsal au moyen de méthodes d'attaque telles que l'injection de codes en langage de requête structuré (SQL) et l'injection d'un logiciel malveillant. Si l'auteur d'une attaque obtient les droits d'administrateur du serveur, il convient également de considérer le préjudice comme analogue à celui qui a été décrit précédemment.

– Accès physique sans autorisation: L'accès physique au serveur dorsal peut s'effectuer de diverses manières, par exemple au moyen d'une clé flash drive de bus série universel (USB) ou en pénétrant à l'intérieur du bâtiment d'un serveur au moyen de l'identité usurpée d'un membre du personnel. En pareil cas, le préjudice et les perturbations occasionnés pour les données associées au véhicule et les installations de traitement des informations correspondantes sont encore plus importants.

7.1.1.2 Perturbation des services d'un serveur dorsal

Les attaques visant le serveur dorsal peuvent entraîner un dysfonctionnement du serveur et l'empêcher d'interagir avec les véhicules et de fournir les services dont ils ont besoin, ce qui peut avoir des effets

très préjudiciables sur la disponibilité des services associés au véhicule, par exemple la gestion de certification pour le véhicule et l'infrastructure.

7.1.1.3 Perte ou altération des données stockées sur des serveurs dorsaux

Un serveur dorsal altéré par suite d'un abus de privilèges de la part d'un initié, d'un accès non autorisé depuis l'extérieur, ou d'un accès physique non autorisé, comme indiqué au § 7.1.1.1, peut entraîner la perte ou la fuite de données du serveur dorsal et être exposé à d'autres menaces, par exemple:

– Perte d'informations dans le nuage: Des données sensibles, telles que l'identifiant du véhicule (VIN) ou les données personnelles du conducteur, peuvent faire l'objet de fuites et d'altérations lorsque les données sont stockées dans les systèmes des prestataires de services tiers de stockage dans le nuage.

– Atteinte à la sécurité de l'information due au partage involontaire de données: Si un serveur est situé dans un périmètre non sécurisé en raison d'une mauvaise configuration de la part d'un administrateur, les données risquent d'être partagées ou divulguées par inadvertance.

7.1.2 Menaces pour les véhicules liées à leurs canaux de communication

Les communications dans les véhicules comprennent les communications externes, telles que les communications V2V, V2I, V2D et V2P, et les communications à l'intérieur de véhicules, telles que les communications de gestionnaire de réseau de communication (CAN), de réseau local d'interconnexion (LIN), de transport dans des systèmes orientés média (MOST) et FlexRay. Les canaux utilisés pour ces communications peuvent être la cible d'attaques telles que la simulation, l'interception, ou la manipulation de messages, notamment.

7.1.2.1 Simulation de messages

Il peut y avoir simulation de messages par usurpation d'identité. Dans le cas des messages utilisés dans des communications V2X et le système mondial de navigation par satellite (GNSS), un véhicule peut recevoir des messages non valables en raison d'une attaque par usurpation d'identité. En outre, s'il y a de nombreux véhicule sur une route donnée, une attaque Sybil peut être lancée afin de simuler d'autres véhicules.

NOTE – Il peut y avoir une attaque Sybil lorsque, par exemple, un véhicule fait croire qu'il y a plusieurs véhicules en utilisant plusieurs identifiants de véhicule.

7.1.2.2 Manipulations, suppressions ou autres modifications non autorisées du code ou des données du véhicule

En présence d'une vulnérabilité ou d'une faille dans le véhicule, l'accès illicite à distance ou une attaque par intrusion de logiciels malveillants sont possibles par le biais des canaux de communication du véhicule. En conséquence, le canal de communication peut engendrer la mise à exécution d'un grand nombre de menaces pour la sécurité, à savoir:

– l'injection de code, par exemple un code binaire qui a été altéré peut être injecté dans le flux de communication;

– la manipulation des données ou du code du véhicule;

– l'écrasement des données ou du code du véhicule;

– l'effacement ou la suppression des données ou du code du véhicule.

7.1.2.3 Utilisation de messages non fiables ou non sécurisés et attaques par détournement ou répétition de session

Des messages provenant d'une source non fiable ou non sécurisée peuvent être reçus par le biais des canaux de communication. Des attaques par hôte interposé et un détournement de session sont possibles via les canaux de communication. Ainsi, une attaque contre une passerelle de communication dans le véhicule permet à l'auteur d'une attaque d'installer une version antérieure du

logiciel d'une unité ECU, ou du micrologiciel de la passerelle, en utilisant des vulnérabilités connues du logiciel, au moyen d'une attaque par répétition de session, au cours de laquelle des transferts de données valables sont effectués à plusieurs reprises à des fins malveillantes.

7.1.2.4 Divulgation d'informations

Des informations peuvent être facilement divulguées, par exemple en interceptant les communications ou en permettant l'accès non autorisé à des fichiers ou des dossiers sensibles. Autrement dit, les informations échangées sur le canal de communication peuvent être interceptées à des fins malveillantes, subir des rayonnements brouilleurs ou faire l'objet d'une surveillance des communications. À cette fin, l'auteur de l'attaque peut obtenir des droits d'accès non autorisé à des fichiers.

7.1.2.5 Attaques par déni de service

L'auteur d'une attaque peut perpétrer une attaque par déni de service via un canal de communication, en envoyant une grande quantité de données parasites au système d'information du véhicule, ce qui a pour effet de perturber l'essentiel des fonctions du véhicule. De plus, en cas de circulation en peloton ou de communication de véhicule à véhicule, l'auteur de l'attaque pourrait empêcher l'envoi des données nécessaires aux autres véhicules du groupe, afin que ceux-ci perdent tout contrôle en raison de l'absence de données en provenance des autres véhicules du groupe. C'est ce qu'on appelle une "attaque par trou noir".

7.1.2.6 Accès privilégié par un utilisateur sans privilèges

Au moyen d'un accès illicite par le biais de canaux de communication, un utilisateur sans privilèges peut obtenir un accès privilégié, par exemple un accès racine au système. On parle d'"escalade au niveau des privilèges non autorisés": une fois que cette escalade aboutit, l'auteur d'une attaque peut faire ce qu'un utilisateur normal ne peut faire.

7.1.2.7 Virus introduits dans des supports de communication

Une fois que des vulnérabilités ont été détectées dans le système du véhicule, il est possible d'injecter des virus ou des logiciels malveillants dans le système du véhicule par le biais des canaux de communication. Les virus peuvent devenir un administrateur doté d'un accès privilégié et perpétrer toute attaque dans le véhicule. Par exemple, si le virus déchiffre des fichiers et des informations sans autorisation dans le système du véhicule visé – on parle de "rançongiciel" –, le système du véhicule ne se sera plus fonctionnel.

7.1.2.8 Messages comportant des contenus malveillants

Des messages reçus par le véhicule (par exemple des messages de diagnostic ainsi que des messages provenant d'autres véhicules), ou transmis à l'intérieur du véhicule, peuvent contenir des contenus malveillants. Dans le cas de réseaux IVN, l'auteur d'une attaque peut modifier le logiciel des unités ECU en injectant des virus (voir le § 7.1.2.7) et rejoindre le réseau du véhicule en tant que membre par usurpation d'identité.

Des messages V2X malveillants, par exemple des messages de sensibilisation fondés sur la coopération (CAM), et des messages de notification environnementale décentralisés (DENM) peuvent être reçus par les véhicules se trouvant à proximité. Étant donné que les communications V2X reposent sur la radiodiffusion, un grand nombre de messages V2X malveillants peuvent avoir une incidence préjudiciable sur l'ensemble des réseaux du véhicule, y compris les réseaux IVN dans le véhicule proprement dit.

Des messages de diagnostic malveillant peuvent également être reçus. L'auteur d'une attaque peut enregistrer un message de diagnostic et l'utiliser en vue d'une attaque par répétition. En outre, même le message de commande du véhicule peut être reçu via une attaque par répétition.

Les messages propres au fournisseur sont en principe envoyés par un fabricant OEM ou un fournisseur de composants, de systèmes ou de fonctions. Cependant, les messages propres au fournisseur qui ont un caractère malveillant et visent à perturber le système du véhicule. peuvent également être reçus par les auteurs d'une attaque.

7.1.3 Menaces pour les véhicules liées à leurs procédures de mise à jour

La mise à jour des systèmes du véhicule peut se faire de deux manières, à savoir par voie filaire sur un port OBD et des dispositifs portables, par exemple une carte numérique sécurisée (SD), ou à l'aide d'un flash drive USB par voie hertzienne (OTA). Le logiciel à mettre à jour peut être un micrologiciel ou les données de configuration du véhicule. La plupart des problèmes électroniques et des défauts logiciels peuvent être mis à jour et résolus par voie électronique sans accès physique, par exemple au moyen d'un testeur OBD. En outre, les mises à jour OTA (sans fil) permettent de raccourcir le cycle de mise à jour, de façon à limiter le plus possible l'exposition à des attaques en ce qui concerne les vulnérabilités connues du logiciel.

7.1.3.1 Utilisation abusive ou altération des procédures de mise à jour

Que la mise à jour utilisée soit effectuée localement ou physiquement ou par voie hertzienne, la procédure de mise à jour peut s'accompagner de menaces qui consistent à créer de toutes pièces des programmes de mise à jour du système ou à utiliser des microgiciels compromis.

Le logiciel peut être manipulé avant le processus de mise à jour, bien que ce processus reste intact. Le fournisseur de logiciel créé ou prépare son logiciel aux fins de la mise à jour et celui-ci est fourni aux systèmes visés nécessitant la mise à jour. En conséquence, il existe un risque grave de manipulation et de corruption du logiciel avant sa mise en service.

En particulier, les données de chiffrement, telles que les clés et les certificats utilisés dans la procédure de mise à jour logicielle, peuvent être compromises et rendre non valables les mises à jour du logiciel.

7.1.3.2 Refus d'une mise à jour légitime

Une attaque par déni de service contre un serveur ou un réseau de mise à jour pour empêcher le déploiement de mises à jour critiques du logiciel ou le déverrouillage de fonctionnalités propres au client est possible dans la procédure de mise à jour du logiciel. Il est également possible de refuser des mises à jour légitimes.

7.1.4 Menaces pour les véhicules liées à des actions humaines non intentionnelles

Des actions humaines peuvent donner lieu par inadvertance à des menaces non reconnues. Ces menaces comprennent, par défaut, la modification non autorisée, ou par inadvertance, du logiciel. Au nombre des erreurs fortuites figurent les violations de la configuration, les erreurs de programmation et la corruption de données dues à des erreurs commises par l'utilisateur ou l'opérateur.

7.1.4.1 Mauvaise configuration de l'équipement ou des systèmes par un acteur légitime

Un utilisateur légitime peut prendre des mesures qui entraînent involontairement des cyberattaques. Ainsi, le paramétrage du système du véhicule peut être modifié de façon anormale par un utilisateur légitime lors de l'installation, de la réparation ou de l'utilisation non intentionnelle. Des erreurs peuvent également être commises lors de la gestion ou de l'utilisation de systèmes ou dispositifs comprenant des mises à jour logicielles.

7.1.4.2 Cyberattaque facilitée de façon involontaire par un acteur légitime

Un utilisateur légitime (par exemple le propriétaire, un opérateur ou un ingénieur chargé de la maintenance) peut être une victime innocente et être amené par la ruse et à son insu à charger un code malveillant (logiciel malveillant) ou à permettre une attaque. De plus, bien souvent, l'utilisateur légitime ne se conforme pas à des procédures de sécurité définies.

7.1.5 Menaces pour les véhicules liées à leur connectivité et leurs connexions externes

Pour fournir divers services pratiques, les véhicules peuvent être équipés de composants permettant de communiquer avec les serveurs dorsaux et peuvent communiquer avec tout ce qui est rendu possible par les usagers de la route sur une connexion hertzienne. Outre les fonctionnalités pratiques, il existe des avantages sur le plan de la sécurité tels que la fonctionnalité que constitue le système automatique d'appel d'urgence ainsi que les fonctionnalités assurées par les communications V2X. Toutefois, plus les véhicules assurant une connexion avec des entités externes pour améliorer la connectivité sont nombreux, plus il y a de risques de menaces et de vulnérabilités, étant donné que les interfaces additionnelles élargissent la surface vulnérable du système.

7.1.5.1 Manipulation de la connectivité des fonctions du véhicule

La manipulation de la connectivité des fonctions du véhicule permet une cyberattaque. Cette menace peut apparaître dans les éléments suivants du véhicule, et se manifester de la façon suivante:

– manipulation des fonctions conçues pour commander à distance des systèmes tels qu'une clef à distance, un dispositif d'immobilisation et une pile de chargement;

– manipulation de la télématique embarquée dans le véhicule: par exemple déverrouillage à distance des portes de chargement;

– manipulation via une interface d'un système ou de capteurs sans fil de courte portée.

7.1.5.2 Logiciels tiers embarqués

Un système d'infoloisirs de véhicules modernes connectés au réseau IVN peut permettre l'installation d'applications de tiers. Les applications de tiers peuvent être corrompues ou leur sécurité logicielle est déficiente, de sorte qu'elles peuvent être utilisées pour attaquer des systèmes du véhicule.

7.1.5.3 Dispositifs connectés à des interfaces externes

Les fonctions de connectivité sont associées à des interfaces externes et les dispositifs connectés à ces interfaces peuvent être utilisés comme moyen pour attaquer les systèmes du véhicule dont les interfaces ci-après sont vulnérables:

– interfaces externes telles que les ports USB: pour perpétrer une attaque par injection de code;

– support infecté par un virus: le virus peut attaquer le système embarqué dans le véhicule via le support infecté;

– accès diagnostique: les fonctions de diagnostic auxquelles ont accès les dongles Bluetooth dans les ports OBD sont utilisées pour visualiser le statut des véhicules et manipuler les paramètres de ces derniers qui figurent dans le logiciel du véhicule.

7.2 Informations potentielles concernant les menaces

7.2.1 Cibles ou motivations potentielles d'une attaque

Les véhicules peuvent devenir la cible de cyberattaques potentielles lorsqu'ils sont connectés par voie électronique à de nombreux systèmes ou services de l'écosystème du véhicule. En outre, les auteurs d'attaques cherchent souvent à retirer des avantages financiers en faisant connaître leurs techniques d'attaque au monde entier, et plus particulièrement aux fournisseurs OEM. Les attaques peuvent avoir les conséquences décrites aux § 7.2.1.1 à 7.2.1.7 sur les systèmes de véhicules.

7.2.1.1 Extraction des données ou du code du véhicule

Les données sensibles ou les données de justificatif d'identité peuvent devenir une cible pour l'extraction, dans la mesure où elles peuvent contenir les informations ci-après qui peuvent être utilisées afin de retirer un gain financier:

– logiciels soumis à des droits d'auteur ou exclusifs du véhicule;

– données personnelles du propriétaire, notamment concernant son identité, son compte de paiement, son carnet d'adresses, sa localisation, l'identifiant électronique du véhicule, etc.;
– clés cryptographiques, etc.

7.2.1.2 Manipulation des données ou du code du véhicule

En manipulant les données ou le code du véhicule, les auteurs d'une attaque pourraient usurper l'identité de quelqu'un ou répudier le comportement du propriétaire légitime. Les méthodes de manipulation ci-après peuvent être identifiées:

– modifications illicites/non autorisées de l'identifiant électronique d'un véhicule;
– usurpation d'identité: un utilisateur souhaite afficher une autre identité lorsqu'il communique avec les systèmes de péage et les systèmes dorsaux du constructeur;
– mesures visant à contourner les systèmes de surveillance, par exemple, piratage, altération ou blocage de messages, tels que les données de suivi de l'enregistreur de données de fonctionnement (ODR) ou le nombre de passages;
– manipulation de données visant à falsifier les données relatives à la conduite du véhicule, par exemple le kilométrage, la vitesse de conduite, l'itinéraire et le temps de référence du véhicule;
– modifications non autorisées des données de diagnostic du système;
– fraude concernant la version du microgiciel: la version la plus récente du microgiciel bénéficiant de correctifs pour lutter contre certaines failles peut être remplacée par l'ancienne version n'ayant pas fait l'objet de correctifs.

7.2.1.3 Effacement des données ou du code

Les journaux d'événements du système peuvent faire l'objet d'une suppression ou d'une manipulation non autorisée. Du fait de cette falsification, il est souvent impossible d'analyser des données ou il est difficile de rechercher la cause de l'attaque.

7.2.1.4 Introduction d'un logiciel malveillant

La première étape, pour l'auteur d'une attaque, consiste à utiliser de nombreuses méthodes d'attaque pour introduire un logiciel malveillant dans le système d'un véhicule. Il existe diverses interfaces d'attaque pour introduire un logiciel malveillant, par exemple le recours à des interfaces externes et à des modules physiques infectés.

7.2.1.5 Introduction de nouveaux logiciels ou écrasement de logiciels existants

L'introduction d'un nouveau logiciel ou l'écrasement d'un logiciel qui est malveillant sur un logiciel existant risque d'avoir de graves conséquences, sur le plan de la cybersécurité, sur les logiciels du système de commande du véhicule ou du système d'information.

7.2.1.6 Perturbation des systèmes ou de l'exploitation

Une attaque par déni de service contre le système du véhicule peut être déclenchée sur le réseau interne en "inondant" de messages un bus CAN ou en provoquant des pannes sur une unité UCE en envoyant un grand nombre de message.

7.2.1.7 Manipulation des paramètres du véhicule

La manipulation des paramètres du véhicule peut avoir des incidences importantes sur le système du véhicule, par exemple l'accès non autorisé visant à falsifier:

– les paramètres de configuration des fonctions principales d'un véhicule, telles que les données de freinage ou le seuil de déploiement de l'airbag;
– les paramètres de charge, tels que la tension de charge, la puissance de charge, la température de la batterie, etc.

7.2.2 Vulnérabilités potentielles

7.2.2.1 Technologies de chiffrement vulnérables

Les technologies de chiffrement peuvent être compromises ou ne sont pas suffisamment appliquées. Il est possible d'exploiter des clés ou des certificats de chiffrement comprenant des justificatifs d'identité, tels qu'un mot de passe. Ainsi, si des clés de chiffrement faibles sont utilisées ou si les clés de chiffrement n'ont pas été mises à jour depuis longtemps, le système de chiffrement peut être interrompu par des attaques en force. Une utilisation insuffisante des techniques de chiffrement peut également entraîner une fuite des clés de chiffrement ou des justificatifs chiffrés. En outre, l'utilisation de technologies de chiffrement déjà défectueuses et obsolètes peut accroître le risque de fuite d'informations.

7.2.2.2 Pièces ou fournitures de véhicules compromises

Le matériel ou les logiciels utilisés dans l'écosystème d'un véhicule peuvent être modifiés de façon à ne pas répondre aux critères de conception permettant de parer à une attaque. Des pièces ou des fournitures d'un véhicule pourraient être compromises pour permettre l'attaque d'un véhicule.

7.2.2.3 Vulnérabilités dans la conception des logiciels ou du matériel

La présence de bugs logiciels peut être la cause de vulnérabilités potentiellement exploitables. Ceci est particulièrement vrai si le logiciel n'a pas été testé pour vérifier si un mauvais code ou des bugs connus sont présents et pour réduire le risque de leur présence.

L'utilisation des restes de la phase de développement (par exemple, ports de débogage, ports du groupe d'action de test mixte (JTAG), microprocesseurs, certificats de développement et mots de passe des développeurs) peut permettre à l'auteur d'une attaque d'accéder aux unités UCE ou d'obtenir des privilèges plus élevés.

7.2.2.4 Vulnérabilités dans la conception des réseaux

Si l'accès au réseau est autorisé alors que des ports de communication superflus sont laissés ouverts, le nombre d'attaques telles que l'accès non autorisé risque d'augmenter.

En outre, l'utilisation de passerelles non protégées, ou de points d'accès (tels que les passerelles camion-remorque), pour contourner les protections et accéder à d'autres segments du réseau, peut donner lieu à des actes malveillants, comme l'envoi de messages arbitraires du bus CAN.

7.2.2.5 Perte physique de données

Des données sensibles utilisées dans les écosystèmes du véhicule peuvent être perdues ou compromises en raison de dommages matériels subis en cas d'accident de la circulation ou de vol. Des données peuvent également être perdues en raison de la gestion des droits numériques (DRM) et les données de l'utilisateur peuvent par exemple être effacées.

De plus, l'intégrité de données sensibles peut être perdue en raison de l'usure des composants informatiques (IT), ce qui peut entraîner des problèmes en cascade (par exemple en cas de modification des clefs).

7.2.2.6 Transfert involontaire de données

Des données privées ou sensibles peuvent être divulguées lorsque la voiture change de main (par exemple, en cas de vente ou d'utilisation comme véhicule de location par une personne différente).

7.2.2.7 Manipulation physique des systèmes

La manipulation physique de systèmes, par exemple du matériel OEM, peut donner lieu à des attaques. Ainsi, une attaque par hôte interposé est possible si du matériel non autorisé est ajouté dans le véhicule.

Appendice I

Exemples de vulnérabilités ou de méthodes d'attaque relatives aux menaces

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

On trouvera dans le présent Appendice des exemples de vulnérabilités ou de méthodes d'attaque relatives aux menaces qui sont reproduits dans le Tableau 1 de la publication [b-UNECE GRVA].

NOTE – Les numéros de paragraphe indiqués dans la première colonne à gauche du Tableau I.1 sont ceux utilisés dans la publication [b-UNECE GRVA].

Tableau I.1 – Liste d'exemples de vulnérabilités ou de méthodes d'attaque liées aux menaces

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			**Exemple de vulnérabilité ou de méthode d'attaque**	
4.3.1 Menaces concernant les serveurs dorsaux	1	Serveurs dorsaux utilisés pour attaquer un véhicule ou extraire des données	1.1	Abus de privilèges de la part du personnel (attaque d'initié)
			1.2	Accès Internet non autorisé au serveur (activé par exemple par des portes dérobées, des vulnérabilités logicielles système non corrigées, des attaques SQL ou d'autres moyens)
			1.3	Accès physique non autorisé au serveur (en utilisant, par exemple, des clefs USB ou d'autres supports connectés au serveur)
	2	Services d'un serveur dorsal perturbé, affectant le fonctionnement d'un véhicule	2.1	Attaque d'un serveur dorsal bloquant son fonctionnement, par exemple en l'empêchant d'interagir avec les véhicules et de fournir les services dont ils ont besoin
	3	Données stockées sur des serveurs dorsaux perdues ou compromises ("atteinte à la sécurité des données")	3.1	Abus de privilèges de la part du personnel (attaque d'initié)
			3.2	Perte d'informations dans le "nuage". Des données sensibles peuvent être perdues en raison d'attaques ou d'accidents lorsque les données sont stockées par des prestataires de services tiers de stockage dans le nuage
			3.3	Accès Internet non autorisé au serveur (activé par exemple par des portes dérobées, des vulnérabilités logicielles système non corrigées, des attaques SQL ou d'autres moyens)
			3.4	Accès physique non autorisé au serveur (en utilisant, par exemple, des clefs USB ou d'autres supports connectés au serveur)
			3.5	Atteinte à la sécurité de l'information due au partage involontaire de données (par exemple, erreurs administratives, stockage des données sur des serveurs situés dans des garages)
4.3.2 Menaces pour les véhicules liées à leurs canaux de communication	4	Simulation de messages ou de données reçus par le véhicule	4.1	Simulation de messages par usurpation d'identité (802.11p V2X en cas de circulation en peloton, messages GNSS, etc.)
			4.2	Attaque Sybil (visant à simuler d'autres véhicules pour faire croire qu'il y en a beaucoup sur la route)

Tableau I.1 – Liste d'exemples de vulnérabilités ou de méthodes d'attaque liées aux menaces

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			Exemple de vulnérabilité ou de méthode d'attaque	
	5	Canaux de communication utilisés pour effectuer des manipulations, suppressions ou autres modifications non autorisées du code ou des données du véhicule	5.1	Les canaux de communication permettent l'injection de code, par exemple un code binaire altéré peut être injecté dans le flux de communication
			5.2	Les canaux de communication permettent de manipuler les données ou le code du véhicule
			5.3	Les canaux de communication permettent d'écraser les données ou le code du véhicule
			5.4	Les canaux de communication permettent d'effacer les données ou le code du véhicule
			5.5	Les canaux de communication permettent l'introduction de données ou de code dans le véhicule (écriture de données ou de code)
	6	Canaux de communication permettant l'acceptation de messages non fiables, ou vulnérables au piratage ou aux attaques par rejeu	6.1	Acceptation d'informations provenant d'une source non fiable
			6.2	Attaque par hôte interposé/détournement de session
			6.3	Attaque par répétition, par exemple une attaque contre une passerelle de communication permettant à l'attaquant d'installer une version antérieure du logiciel d'une unité de commande électronique (UCE) ou du microprogramme de la passerelle
	7	Les informations peuvent être facilement divulguées. Par exemple, en interceptant les communications ou en permettant l'accès non autorisé à des fichiers ou dossiers sensibles	7.1	Interception de l'information/rayonnements brouilleurs/surveillance des communications
			7.2	Obtention d'un accès non autorisé à des fichiers ou des données
	8	Attaques par déni de service sur les canaux de communication pour perturber les fonctions du véhicule	8.1	Envoi d'un grand nombre de données parasites au système d'information du véhicule, de façon qu'il soit incapable de fournir des services de manière normale
			8.2	Attaque par trou noir, visant à perturber la communication entre les véhicules en bloquant les messages entre ceux-ci
	9	Un utilisateur sans privilèges peut obtenir un accès privilégié aux systèmes du véhicule	9.1	Un utilisateur sans privilèges peut obtenir un accès privilégié, par exemple un accès racine
	10	Des virus introduits dans les moyens de communication peuvent infecter les systèmes du véhicule	10.1	Un virus introduit dans les moyens de communication infecte les systèmes du véhicule
	11	Des messages reçus par le véhicule (par exemple, messages X2V ou de diagnostic), ou transmis à l'intérieur de celui-ci,	11.1	Messages internes malveillants (par exemple, bus CAN)
			11.2	Messages V2X malveillants, par exemple, messages d'infrastructure à véhicule ou de véhicule à véhicule (CAM, DENM, etc.)
			11.3	Messages de diagnostic malveillants

Tableau I.1 – Liste d'exemples de vulnérabilités ou de méthodes d'attaque liées aux menaces

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			Exemple de vulnérabilité ou de méthode d'attaque	
		contiennent des contenus malveillants	11.4	Messages propriétaires malveillants (par exemple, ceux normalement envoyés par les fabricants d'équipement d'origine OEM ou les fournisseurs de composants/systèmes/fonctions)
4.3.3 Menaces pour les véhicules liées à leurs procédures de mise à jour	12	Utilisation abusive ou compromission des procédures de mise à jour	12.1	Compromission des procédures de mise à jour logicielle sans fil, y compris la fabrication du programme ou du microprogramme de mise à jour du système
			12.2	Compromission des procédures de mise à jour logicielle locales/physiques, y compris la fabrication du programme ou du microprogramme de mise à jour du système
			12.3	Le logiciel est manipulé avant le processus de mise à jour (et est donc corrompu), bien que le processus de mise à jour soit intact
			12.4	Compromission des clés de chiffrement du fournisseur du logiciel pour permettre une mise à jour non valide
	13	Possibilité d'empêcher des mises à jour légitimes	13.1	Attaque par déni de service contre le serveur ou le réseau de mise à jour pour empêcher le déploiement de mises à jour logicielles critiques et/ou le déverrouillage de fonctionnalités spécifiques au client
4.3.4 Menaces pour les véhicules liées à des actions humaines non intentionnelles	14	Mauvaise configuration de l'équipement ou des systèmes par un acteur légitime, par exemple le propriétaire ou la communauté de maintenance	14.1	Mauvaise configuration de l'équipement par la communauté de maintenance ou le propriétaire lors de l'installation, la réparation ou l'utilisation, avec des conséquences imprévues
			14.2	Utilisation ou administration erronée de dispositifs et de systèmes (y compris les mises à jour sans fil)
	15	Des acteurs légitimes peuvent prendre des mesures susceptibles de faciliter involontairement une cyberattaque	15.1	Victime innocente (par exemple, propriétaire, opérateur ou ingénieur de maintenance) amenée par la ruse et à son insu à charger un logiciel malveillant ou à permettre une attaque
			15.2	Les procédures de sécurité définies ne sont pas suivies
4.3.5 Menaces pour les véhicules liées à leur connectivité et leurs connexions externes	16	La manipulation de la connectivité des fonctions du véhicule permet une cyberattaque, les moyens utilisés comprenant: la télématique, les systèmes permettant des opérations à distance et les systèmes utilisant des communications sans fil à courte portée	16.1	Manipulation des fonctions conçues pour commander à distance des systèmes, tels qu'une clef à distance, un dispositif d'immobilisation et une pile de chargement
			16.2	Manipulation de la télématique du véhicule (par exemple, manipulation de la mesure de la température de biens sensibles, déverrouillage à distance des portes de chargement)
			16.3	Interférence avec des systèmes ou capteurs sans fil à courte portée
	17	Utilisation de logiciels tiers embarqués, comme les applications de divertissement, pour attaquer les systèmes du véhicule	17.1	Utilisation d'applications corrompues, ou dont la sécurité logicielle est déficiente, pour attaquer des systèmes du véhicule

Tableau I.1 – Liste d'exemples de vulnérabilités ou de méthodes d'attaque liées aux menaces

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			Exemple de vulnérabilité ou de méthode d'attaque	
	18	Utilisation de dispositifs connectés à des interfaces externes, par exemple des ports USB ou le port OBD, pour attaquer les systèmes du véhicule	18.1	Interfaces externes telles que les ports USB ou autres utilisées comme point d'attaque, par exemple par injection de code
			18.2	Support infecté par un virus connecté à un système du véhicule
			18.3	Accès diagnostique (par exemple, dongles dans le port OBD) utilisé pour faciliter une attaque, comme la manipulation (directe ou indirecte) des paramètres du véhicule
4.3.6 Cibles ou motivations potentielles d'une attaque	19	Extraction des données ou du code du véhicule	19.1	Extraction de logiciels soumis à des droits d'auteur ou exclusifs des systèmes du véhicule (piratage de produits)
			19.2	Accès non autorisé aux données personnelles du propriétaire, notamment concernant son identité, son compte de paiement, son carnet d'adresses, sa localisation, l'identifiant électronique du véhicule, etc.
			19.3	Extraction de clés de chiffrement
	20	Manipulation des données ou du code du véhicule	20.1	Modifications illicites/non autorisées de l'identifiant électronique du véhicule
			20.2	Usurpation d'identité. Par exemple, si un utilisateur souhaite afficher une autre identité lorsqu'il communique avec les systèmes de péage, le système dorsal du constructeur
			20.3	Mesure visant à contourner les systèmes de surveillance (par exemple, piratage/altération/blocage de messages tels que les données de suivi ODR ou le nombre de passages)
			20.4	Manipulation des données visant à falsifier les données de conduite du véhicule (kilométrage, vitesse de conduite, itinéraire, etc.)
			20.5	Modifications non autorisées des données de diagnostic du système
	21	Effacement des données ou du code	21.1	Effacement/manipulation non autorisé(e) des journaux d'événements du système
	22	Introduction de logiciels malveillants	22.1	Introduire un logiciel malveillant ou une activité logicielle malveillante
	23	Introduction de nouveaux logiciels ou écrasement de logiciels existants	23.1	Fabrication du logiciel du système de commande ou d'information du véhicule
	24	Perturbation des systèmes ou des opérations	24.1	Déni de service pouvant, par exemple, être déclenché sur le réseau interne en inondant un bus CAN, ou en provoquant des pannes sur une UCE en envoyant un grand nombre de messages
	25	Manipulation des paramètres du véhicule	25.1	Accès non autorisé visant à falsifier les paramètres de configuration des fonctions critiques du véhicule, telles que les données de freinage, le seuil de déploiement de l'airbag, etc.

Tableau I.1 – Liste d'exemples de vulnérabilités ou de méthodes d'attaque liées aux menaces

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			Exemple de vulnérabilité ou de méthode d'attaque	
			25.2	Accès non autorisé visant à falsifier les paramètres de charge, tels que la tension de charge, la puissance de charge, la température de la batterie, etc.
4.3.7 Vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites	26	Les technologies de chiffrement peuvent être compromises ou ne sont pas suffisamment appliquées	26.1	L'utilisation de courtes clés de chiffrement ayant une longue période de validité permet à l'attaquant de casser le cryptage
			26.2	Recours insuffisant aux algorithmes de chiffrement pour protéger les systèmes sensibles
			26.3	Utilisation d'algorithmes de chiffrement obsolètes ou sur le point de l'être
	27	Des pièces ou des fournitures pourraient être compromises pour permettre l'attaque des véhicules	27.1	Matériel ou logiciel modifié pour permettre une attaque ou ne répondant pas aux critères de conception permettant de bloquer une attaque
	28	La conception des logiciels ou du matériel est à l'origine de vulnérabilités	28.1	Bugs logiciels. La présence de bugs logiciels peut être la cause de vulnérabilités potentiellement exploitables. Ceci est particulièrement vrai si le logiciel n'a pas été testé pour vérifier l'absence de mauvais code ou de bugs connus et pour réduire le risque de leur présence
			28.2	L'utilisation des restes de la phase de développement (ports de débogage, ports JTAG, microprocesseurs, certificats de développement, mots de passe des développeurs, etc.) peut permettre l'accès aux UCE ou permettre à des attaquants d'obtenir des privilèges plus élevés
	29	La conception des réseaux introduit des vulnérabilités	29.1	Ports Internet superflus laissés ouverts, permettant l'accès aux systèmes réseau
			29.2	Contourner la séparation réseau pour en prendre le contrôle. Par exemple, en utilisant des passerelles non protégées, ou des points d'accès (tels que les passerelles camion-remorque), pour contourner les protections et accéder à d'autres segments du réseau pour commettre des actes malveillants, comme l'envoi de messages arbitraires du bus CAN
	30	La perte physique de données est possible	30.1	Dommages causés par un tiers. Des données sensibles peuvent être perdues ou compromises en raison de dommages matériels subis en cas d'accident de la circulation ou de vol
			30.2	Perte due à des conflits de gestion des droits numériques (DRM). Les données de l'utilisateur peuvent être effacées en raison de problèmes de DRM
			30.3	Des données sensibles (ou leur intégrité) peuvent être perdues en raison de l'usure des composants informatiques, ce qui peut entraîner des problèmes en cascade (en cas de modification des clefs, par exemple)

Tableau I.1 – Liste d'exemples de vulnérabilités ou de méthodes d'attaque liées aux menaces

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			Exemple de vulnérabilité ou de méthode d'attaque	
	31	Le transfert involontaire de données est possible	31.1	Atteinte à la sécurité de l'information. Des données privées ou sensibles peuvent être divulguées lorsque la voiture change de main (par exemple, en cas de vente ou d'utilisation comme véhicule de location par de nouveaux clients)
	32	La manipulation physique des systèmes peut permettre une attaque	32.1	Manipulation du matériel OEM, par exemple ajout de matériel non autorisé à un véhicule pour permettre une attaque par hôte interposé

Bibliographie

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[b-ISO/CEI 27000] ISO/CEI 27000 (2018), *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-UNECE GRVA] UNECE GRVA-01-17 (2017), *Projet de recommandation sur la cybersécurité du Groupe spécial de la cybersécurité et des questions de sûreté des transmissions sans fil – Commission économique pour l'Europe (CEE-ONU) GT.29 GRVA*. Disponible à l'adresse [consultée le 07-08-2020]: https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2020