ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

UIT-T X.1382 (03/2023)

SÉRIE X: Réseaux de données, communication entre systèmes ouverts et sécurité

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

---

Lignes directrices relatives au partage des informations sur les menaces de sécurité pour les véhicules connectés

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.1449
Protocoles de sécurité (2)	X.1450–X.1459
Sécurité du web (2)	X.1470-X1489
ÉCHANGE 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
Cyberdéfense	X.1590-X.1599
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
Protection des données	X.1770-X.1789
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.1382

Lignes directrices relatives au partage des informations sur les menaces de sécurité pour les véhicules connectés

Résumé

Le développement rapide des véhicules connectés s'accompagne de problèmes de sécurité des réseaux de plus en plus importants. Les informations sur les menaces de sécurité des véhicules connectés, qui jouent un rôle essentiel dans la sécurisation de ces derniers, sont toutes les informations qui peuvent aider un organisme à identifier un véhicule connecté, à l'évaluer, à le surveiller et à lui répondre. Les organismes qui partagent des informations sur les menaces pour les véhicules connectés peuvent améliorer leurs propres dispositifs de sécurité et ceux d'autres organismes.

La Recommandation UIT-T X.1382 fournit des orientations concernant les principes, les règles, la méthodologie et les procédures relatifs au partage d'informations concernant la sécurité des véhicules connectés. Elle contient également une brève description des différents domaines de compétence, des rôles et de l'efficacité des divers organismes lorsqu'ils participent au cycle de vie du partage d'informations sur les menaces de sécurité.

La présente Recommandation est destinée à aider les organismes à rester en contact avec les spécialistes du partage d'informations en lien avec les véhicules connectés et à fournir des informations sur les menaces propres à appuyer les pratiques liées à la protection de la sécurité des véhicules connectés. De manière générale, elle vise à améliorer le partage d'informations sur les menaces de sécurité et à atténuer les incidences potentielles des attaques de cybersécurité sur les véhicules connectés.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1382	03-03-2023	17	11.1002/1000/15104

Mots clés

Véhicules connectés, partage d'informations sur les menaces.

* 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.

À 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 ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise 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 les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1382

Lignes directrices relatives au partage des informations sur les menaces de sécurité pour les véhicules connectés

1 Domaine d'application

La présente Recommandation vise à fournir des lignes directrices relatives au partage des informations sur les menaces pour les écosystèmes des véhicules connectés, notamment en ce qui concerne le rôle des organismes et leurs partenariats, la portée du partage d'information, ainsi que les procédures et les orientations relatives au partage des informations sur les menaces pour les véhicules connectés.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation ou autre référence étant sujette 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.

[UIT-T X.1371] Recommandation UIT-T X.1371 (2020), *Menaces pour la sécurité des véhicules connectés*.

[NIST SP 800-150] *Guide to Cyber Threat Information Sharing*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 alerte [NIST SP 800-150]: brève notification technique, généralement lisible par l'homme, concernant les vulnérabilités, les exploits et autres problèmes de sécurité existants. Également appelée avis, bulletin ou note de vulnérabilité.

3.1.2 informations sur les menaces de sécurité [NIST SP 800-150]: informations relatives à une menace qui pourraient aider un organisme à se protéger contre celle-ci ou à détecter les activités d'un acteur.

3.1.3 menace [b-ISO/CEI 27000]: cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 tactiques d'un acteur: description des objectifs techniques d'un acteur pour effectuer une action.

3.2.2 techniques d'un acteur: description de la manière dont un acteur atteint les objectifs techniques en effectuant une action.

3.2.3 procédures suivies par l'acteur: description de la mise en œuvre d'une technique donnée par un acteur.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ACL liste de contrôle d'accès (*access control list*)

APP application

CERT équipe d'intervention en cas d'urgence informatique (*computer emergency response team*)

CSIRT équipe de réponse aux incidents de sécurité informatique (*computer security incident response team*)

ECU unité de commande électronique (*electronic control unit*)

GSMA Association GSM (*GSM association*)

ISAC Centre de partage et d'analyse des informations (*information sharing and analysis center*)

MEC informatique en périphérie à accès multiples (*multi-access edge computing*)

T-BOX boîtier télématique (*telematics box*)

TSP fournisseur de services télématiques (*telematics service provider*)

TTP tactiques, techniques et procédures (*tactics, techniques and procedures*)

V2X de véhicule à tout autre élément (*vehicle-to-everything*)

5 Conventions

Dans la présente Recommandation:

L'expression "il est recommandé" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

6 Aperçu

Les principaux éléments du partage d'informations sur les menaces pour les véhicules connectés comprennent les informations sur les types de menaces, les principes de partage, les rôles, les règles, les communautés et les procédures. En général, différents organismes relatifs aux véhicules connectés génèrent différents types d'informations sur les menaces de sécurité. Différents types d'agents jouent différents rôles dans les activités de partage d'informations sur les menaces pour les véhicules connectés. Les activités de partage de ces informations entre les organismes doivent suivre certains principes, règles et procédures, car les informations sur les menaces ont différents effets. Différents organismes peuvent former une communauté de partage, avec un mode et une plate-forme de partage donnés.

6.1 Types d'informations sur les menaces pour les véhicules connectés

Selon le document [NIST SP 800-150], les informations sur les menaces pour les véhicules connectés peuvent être classées en différentes catégories, notamment les indicateurs; les tactiques, techniques et procédures (TTP); les alertes de sécurité; et les rapports relatifs aux renseignements sur les menaces:

a) Les indicateurs sont des signes observables indiquant qu'une attaque est imminente ou en cours. Ils peuvent être utilisés pour détecter les menaces potentielles et les contrer. Parmi les indicateurs des véhicules connectés, on trouve des organisations d'auteurs présumés d'attaques visant les communications de véhicule à tout autre élément (V2X).

b) Les TTP décrivent le comportement d'un acteur. Elles pourraient décrire la tendance d'un acteur à utiliser une variante de logiciel malveillant, un ordre d'opérations, un outil d'attaque, un mécanisme de distribution ou un système d'exploitation spécifique. Il existe différentes menaces, notamment des menaces concernant les serveurs dorsaux et le serveur, et des menaces concernant les canaux de communication des véhicules. Les TTP peuvent inclure

des actions visant à manipuler la connectivité des fonctions du véhicule ou à contourner le système de surveillance, qui sont différentes des menaces traditionnelles relatives aux réseaux.

c) Les alertes de sécurité sont des notifications techniques concernant des vulnérabilités, des exploits, des logiciels malveillants et d'autres problèmes de sécurité. Ces alertes proviennent généralement de sources dignes de confiance, telles que les équipes d'intervention en cas d'urgence informatique (CERT) ou les équipes de réponse aux incidents de sécurité informatique (CSIRT). Elles sont émises lorsque les véhicules connectés concernés sont nombreux ou lorsque les menaces pourraient causer des dommages importants.

d) Les rapports relatifs aux renseignements sur les menaces fournissent une analyse approfondie des menaces, y compris les participants à l'événement, le système cible, le type d'attaque ainsi que d'autres informations, et fournissent des avis sur les actions à mener pour atténuer les menaces. Ces rapports peuvent également présenter les tendances futures des menaces. Ils jouent un rôle important dans la prévention de nouvelles attaques visant les véhicules connectés.

6.2 Avantages et défis liés au partage d'informations sur les menaces pour les véhicules connectés

Grâce au partage d'informations sur les menaces pour les véhicules connectés, les organismes liés à l'industrie des véhicules connectés peuvent améliorer leur dispositif de sécurité en tirant parti des connaissances, de l'expérience et des capacités de leurs partenaires de manière proactive. Les avantages du partage d'informations sur les menaces pour les véhicules connectés sont notamment les suivants:

a) Amélioration de la capacité de défense des organismes liés aux véhicules connectés. Les véhicules connectés sont associés à de nouvelles menaces, mais le partage d'informations peut aider les organismes à améliorer leurs capacités de défense contre ces dernières. Les nouvelles vulnérabilités sont souvent utilisées comme outil principal pour les attaques. Le partage d'informations sur les menaces peut permettre de faire face aux attaques visant les nouvelles vulnérabilités sans retard et d'améliorer la capacité de défense contre les attaques. Alors que les véhicules connectés sont exposés à de nombreuses nouvelles attaques, le partage d'informations sur les menaces permet d'y faire face et d'améliorer les capacités de défense.

b) Maintien d'un écosystème des véhicules connectés sain. Le partage d'informations sur les menaces contribue à promouvoir la sécurité de l'environnement économique des véhicules connectés et à établir la sécurité écologique de tous ces véhicules. La sécurité de la chaîne de production des véhicules connectés comprend la sécurité des fournisseurs de services, des fournisseurs de services télématiques (TSP), des constructeurs de véhicules, des opérateurs de télécommunication, des fournisseurs d'équipements pour véhicules et terminaux portatifs, des fournisseurs d'équipements pour terminaux intelligents mobiles, etc.

Bien que le partage d'informations sur les menaces présente des avantages, certains défis subsistent, notamment les suivants:

a) Établissement d'un système normalisé de partage des informations sur les menaces pour les véhicules connectés. Pour maintenir un écosystème des véhicules connectés sain, il est nécessaire d'établir un système normalisé raisonnable pour le partage d'informations. À l'heure actuelle, il n'existe pas de système normalisé international unifié pour le partage d'informations sur les menaces pour les véhicules connectés. Sans l'établissement d'un tel système, le partage d'informations sera entravé, ce qui aura à terme des répercussions sur son développement.

NOTE – Certaines lignes directrices telles que [UIT-T X.1371] et les lignes directrices GSMA IoT relatives à la sécurité [b-GSMA CLP.11] peuvent traiter des questions de sécurité pouvant être considérées comme les meilleures pratiques possibles en termes de partage d'informations.

b) Définition de la portée des informations sur les menaces. La chaîne industrielle des véhicules connectés est composée de différents maillons, et chacun d'entre eux est confronté à différents types de menaces. Il est nécessaire de définir le partage d'informations sur les menaces au sein de chaque maillon et le mode de partage d'informations entre les maillons.

c) Protection des informations sensibles et classées: le partage d'informations sur les menaces pour les véhicules connectés expose à un risque de divulgation d'informations sensibles. Les technologies de chiffrement peuvent être compromises ou ne sont pas suffisamment appliquées. 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. Les informations sensibles à protéger comprennent: les logiciels soumis à des droits d'auteur ou exclusifs du véhicule; les données personnelles du propriétaire, notamment concernant son identité, son compte de paiement, son carnet d'adresses, sa localisation et l'identifiant électronique du véhicule; les clés cryptographiques, etc. En outre, les organismes non autorisés n'ont pas le droit d'accéder aux informations classées. Pour les organismes, obtenir et conserver les habilitations nécessaires à l'accès permanent aux sources d'informations classées est coûteux et chronophage.

7 Principes de partage d'informations sur les menaces pour les véhicules connectés

Pour garantir l'efficacité, l'exactitude et la sécurité du processus de partage et de transmission des informations sur les menaces, les organismes et les entreprises doivent suivre certains principes.

7.1 Intérêt mutuel

Le partage d'informations sur les menaces de sécurité vise essentiellement à améliorer la capacité de protection de la sécurité des réseaux des véhicules connectés grâce à des efforts de collaboration. Il est recommandé aux parties participant au partage d'informations sur les menaces pour la sécurité des véhicules connectés de prendre conscience de leurs droits, devoirs et responsabilités mutuels dans le cadre des activités de partage d'informations. Les organismes reçoivent des informations sur les menaces qui pèsent sur eux, mais il leur est également recommandé de contribuer activement aux efforts, afin de parvenir à des avantages mutuels et à des situations avantageuses pour tous.

7.2 Catégorisation et classification

Les différents organismes jouent des rôles différents dans le processus de partage d'informations sur les menaces de sécurité. La signification et l'importance de certaines informations sur les menaces semblent varier selon les organismes. Il est recommandé aux organismes de catégoriser et de classer les informations sur les menaces pour les véhicules connectés, ainsi que d'en définir la portée effective. Il leur est recommandé d'établir différents niveaux au sein du système de gestion en fonction de leurs étiquettes de catégorisation, de classification et de portée. Il est recommandé d'utiliser un chiffrement approprié pour préserver la confidentialité et l'intégrité des informations sensibles et/ou protéger leur authenticité.

7.3 Sécurité des données

Des problèmes tels que l'utilisation illégale, le vol et la falsification de données relatives aux informations sur les menaces, ainsi que l'accès non autorisé par des utilisateurs, nuisent considérablement à l'échange de renseignements entre les parties et diminuent la sécurité et l'efficacité des activités de partage de renseignements. C'est pourquoi le partage d'informations sur les menaces est également axé sur le contrôle du risque lié au partage. Les contre-mesures, notamment le

chiffrement, la désensibilisation des données partagées, l'identification et la destruction, etc., sont efficaces pour protéger les données relatives aux informations sur les menaces pour la sécurité des véhicules connectés.

8 Organismes, rôles et partenariat

8.1 Organismes et leurs rôles

8.1.1 Constructeurs automobiles

Les constructeurs automobiles jouent un rôle de premier plan dans les activités de partage d'informations sur les menaces pour les véhicules connectés, car ils interagissent directement avec les utilisateurs et sont responsables de la sécurité de leurs véhicules.

Grâce à la collecte de données provenant de leurs propres systèmes de production, des composants embarqués et de l'infrastructure des véhicules connectés, les constructeurs automobiles recueillent, intègrent, produisent et analysent des informations relatives aux menaces de sécurité liées aux véhicules connectés, et prennent des mesures pour atténuer ces menaces.

8.1.2 Fournisseurs

Les fournisseurs mettent à disposition du matériel ou des logiciels embarqués pour les véhicules connectés, y compris des puces pour véhicules, des équipements pour le boîtier télématique (T-BOX) et des passerelles internes/externes. Les fournisseurs recueillent et reçoivent des informations sur les menaces de sécurité liées à leurs produits, et aident l'équipe de coordination, les constructeurs automobiles et les autres parties concernées à atténuer les menaces et/ou à prévenir et limiter les incidents de sécurité liés à leurs produits.

8.1.3 Fournisseurs de produits et de services tiers

Les fournisseurs de produits et de services tiers désignent principalement les organismes qui fournissent des produits et services indépendants liés aux véhicules connectés, autres que les constructeurs automobiles et leurs équipementiers. Il s'agit notamment des fournisseurs TSP, des fournisseurs de services d'informatique en nuage, des vendeurs de matériel, des fabricants de terminaux mobiles, des fournisseurs de services d'assurance automobile, et des autres opérateurs de plates-formes de services tiers.

Les fournisseurs de produits et de services tiers recueillent/produisent/partagent des informations sur les menaces pour la sécurité de leurs produits ou plates-formes de services, telles que des informations sur les menaces liées à la défaillance des véhicules connectés, le comportement des utilisateurs non autorisés et les attaques à distance, et aident les parties concernées, notamment les équipes de coordination dédiées aux véhicules connectés et les constructeurs automobiles, à atténuer les menaces et/ou à traiter les incidents de sécurité liés aux véhicules connectés. Les fournisseurs de services d'informatique en nuage sont également responsables du partage d'informations, y compris en cas de mauvaise configuration ou d'erreur, d'utilisation abusive des ports de commande, de mauvaise gestion des justificatifs d'identité, de fuite de données en nuage, etc.

8.1.4 Équipes de coordination

Les équipes de coordination dédiées aux véhicules connectés fonctionnent généralement comme des entités indépendantes qui se concentrent sur la coordination des informations relatives aux menaces de sécurité et sur la réponse aux incidents, telles que les CERT, les CSIRT et le Centre Auto-ISAC.

Ces équipes aident les parties concernées à coordonner le partage d'informations sur les menaces de sécurité entre les organismes, et fournissent des services de notification et d'alerte avancée aux parties concernées.

8.1.5 Opérateurs de télécommunication

Les opérateurs de télécommunication fournissent des services de télécommunication de base pour les véhicules connectés.

Ils assurent la sécurité des infrastructures de réseaux de télécommunication, tels que les réseaux centraux, les stations de base, les plates-formes MEC, etc.

NOTE – On peut se reporter aux lignes directrices GSMA à l'intention des opérateurs de réseau [b-GSMA CLP.14] pour trouver des exemples d'opérateurs de télécommunications dans le contexte des véhicules connectés.

8.1.6 Fournisseurs de cybersécurité

Les fournisseurs de cybersécurité sont des entreprises ou des organismes dans le domaine des réseaux qui jouent un rôle dans des entreprises et des organismes du secteur automobile fournissant des produits ou des services de cybersécurité.

Grâce à des sources telles que les dispositifs de sécurité, les logiciels de terminaux et l'Internet, les fournisseurs de cybersécurité aident les organismes concernés à collecter, intégrer et analyser les informations relatives aux menaces de sécurité pour les véhicules connectés, et fournissent un appui en matière de sécurité ainsi que des services de sécurité afin de prévenir et limiter les incidents de sécurité.

8.2 Portée du partage entre les organismes

Il est recommandé aux organismes de définir la portée des activités de partage d'informations, notamment en identifiant les types d'informations sur les menaces qui peuvent être partagées, les circonstances dans lesquelles les activités de partage d'informations sur les menaces sont autorisées, et les priorités en matière de partage d'informations sur les menaces pour les véhicules connectés.

L'étendue des activités de partage d'informations variera en fonction des ressources et des capacités d'un organisme. La portée du partage d'informations sur les menaces pour les véhicules connectés varie selon les types d'organismes. Par exemple, elle n'est pas la même pour les fournisseurs de cybersécurité, les constructeurs automobiles, les fournisseurs d'équipements V2X, les fournisseurs d'équipements de communication, les opérateurs de télécommunication, etc. Il est recommandé aux producteurs d'informations sur les menaces pour les véhicules connectés qui disposent de ressources limitées de se concentrer sur un ensemble plus restreint d'activités relatives à la production/la collecte d'informations sur les menaces, afin de fournir des informations présentant une plus grande valeur pour l'organisme et les partenaires avec lesquels il les partage. Un organisme disposant de ressources importantes et de capacités évoluée pourra choisir une portée initiale plus large qui permet un plus large éventail d'activités de partage des informations sur les menaces. Un organisme disposant de ressources plus importantes et de capacités avancées peut opter pour une portée initiale plus large qui lui permet de mener un ensemble plus vaste d'activités de partage afin d'atteindre ses buts et ses objectifs.

Le Tableau 1 présente les organismes qui peuvent être concernés par chaque type de menace défini dans la norme [UIT-T X.1371].

Tableau 1 – Types de menaces visant les véhicules connectés et organismes concernés

Type de menace	Organismes partageant des informations sur les menaces					
	Constructeurs automobiles	**Fournisseurs**	**Fournisseurs de produits et de services tiers**	**Équipes de coordination**	**Opérateurs de télécommunication**	**Fournisseurs de cybersécurité**
Menaces concernant les serveurs dorsaux	✓		✓	✓		✓
Menaces pour les véhicules liées à leurs canaux de communication	✓	✓	✓	✓	✓	✓
Menaces pour les véhicules liées à leurs procédures de mise à jour	✓		✓	✓		✓
Menaces pour les véhicules liées à des actions humaines non intentionnelles	✓	✓	✓			
Menaces pour les véhicules liées à leur connectivité et leurs connexions externes	✓	✓	✓	✓	✓	✓
Cibles ou motivations potentielles d'une attaque	✓	✓	✓	✓		✓
Vulnérabilités potentielles	✓	✓	✓	✓	✓	✓

8.3 Règles de partage des informations entre les organismes

Sur la base des caractéristiques et de la classification des informations sur les menaces pour les véhicules connectés, les règles de partage des informations sur les menaces entre les organismes peuvent être décrites comme suit:

a) Il est recommandé aux organismes de partager des informations sur les menaces pour les véhicules connectés.

b) Les informations sur les menaces pour les véhicules connectés sont souvent partagées au niveau des plates-formes de gestion des véhicules connectés, des fournisseurs de services de transports partagés, des entreprises de fabrication de véhicules, des fournisseurs d'équipements V2X, des fournisseurs d'équipements de communication et des opérateurs de télécommunication.

c) De nombreux organismes, tels que les constructeurs automobiles et les fournisseurs de cybersécurité, jouent à la fois le rôle de producteurs et de consommateurs d'informations sur les menaces.

d) Il est recommandé que les producteurs d'informations sur les menaces soient des professionnels.

e) Il est recommandé d'appliquer des exigences relatives à la gestion, telles que le filtrage des informations sur les menaces et la vérification des abonnements.

8.4 Mise en place d'une communauté de partage

Il est recommandé d'établir une communauté pour partager et analyser les informations sur les menaces pour les véhicules connectés. Les modèles de partage des informations sur les menaces sont le modèle d'homologue à homologue, le modèle source/abonné et le modèle en étoile [b-OASIS TAXII]. Grâce à une communauté de partage, les organismes peuvent recevoir en temps réel des données sur les menaces et les vulnérabilités liées aux réseaux pour les véhicules connectés. Prenons l'exemple du Centre Auto-ISAC, qui a été créé par des entreprises du secteur de l'automobile en 2015. Il se concentre sur la mise en place d'une communauté de partage d'informations rassemblant un nombre croissant de véhicules intelligents. Le portail du Centre Auto-ISAC permet à ses membres de soumettre et de recevoir des informations de manière anonyme, et aide les membres à faire face aux menaces relatives au réseau de manière plus efficace. Le Centre encourage activement la coopération et le partage d'informations entre les fournisseurs, les revendeurs de véhicules et les constructeurs automobiles dans le domaine de la sécurité des réseaux de véhicule. L'Appendice I présente les activités de partage d'informations sur les menaces menées par le Centre Auto-ISAC.

Une communauté de partage peut mettre en place plusieurs sous-communautés de partage, et les organismes peuvent choisir d'intégrer une ou plusieurs sous-communautés liées aux véhicules connectés. Il est recommandé que la communauté de partage soit une communauté ouverte, permettant à différents organismes de se joindre à elle et d'en sortir librement grâce à une coopération volontaire. Lorsqu'un organisme choisit de rejoindre une sous-communauté, il lui est recommandé de choisir une communauté disposant de ressources d'informations sur les menaces pour les véhicules connectés complétant les siennes. Chaque organisme publie volontairement des informations sur les menaces pour les véhicules connectés auprès de la communauté de partage et est chargé de s'assurer que les informations sur les menaces fournies à la communauté sont appropriées pour le partage.

9 Procédures et orientations relatives au partage d'informations sur les menaces pour les véhicules connectés

9.1 Introduction

La Recommandation [UIT-T X.1371] définit et décrit les menaces pour les véhicules connectés. Les organismes peuvent détecter, analyser et traiter les menaces de sécurité au moyen de ressources internes, et peuvent également partager des informations sur les menaces en établissant un cadre de partage interorganismes. Dans le cadre d'une procédure de partage interorganismes, les organismes peuvent:

a) obtenir et utiliser des informations sur des menaces externes pour prévenir et atténuer les menaces pour les véhicules connectés;

b) produire et fournir des informations sur les menaces pour les véhicules connectés en coopération avec d'autres organismes, afin de renforcer la sécurité de l'écosystème des véhicules.

Conformément à la disposition de la chaîne de transmission des informations, les organismes peuvent être classés en deux catégories avec, d'une part, les consommateurs et, d'autre part, les producteurs. D'habitude, de nombreux organismes, comme les constructeurs automobiles et les fabricants de produits de cybersécurité, sont à la fois des producteurs et des consommateurs d'informations sur les menaces.

9.2 Procédures relatives aux activités de partage d'informations sur les menaces

Les consommateurs sont les victimes potentielles des menaces qui pèsent sur les véhicules connectés. En obtenant et en utilisant des informations sur les menaces, les consommateurs peuvent repérer

rapidement les actifs touchés et prendre les mesures nécessaires pour atténuer les menaces. Parmi tous les organismes concernés, les constructeurs automobiles sont les principaux consommateurs d'informations sur les menaces. Les procédures applicables aux consommateurs s'articulent autour de cinq phases:

a) Préparation: mettre au point des mécanismes appropriés pour se préparer à participer aux activités de partage d'informations sur les menaces.

b) Réception: recevoir des informations sur les menaces externes.

c) Analyse: effectuer une analyse des informations sur les menaces reçues.

d) Atténuation: prendre des mesures pour atténuer les menaces compte tenu des résultats de l'analyse.

e) Prévention: prendre des mesures pour éviter que des menaces ne se présentent à l'avenir.

Les producteurs sont des entités ayant des capacités techniques et analytiques, ainsi que l'intention de partager dans un écosystème de véhicule. En règle générale, les producteurs doivent également consommer des informations sur les menaces pour la sécurité, car la production/collecte d'informations sur les menaces nécessite une multitude de sources, parmi lesquelles figurent les informations sur les menaces reçues. Les procédures applicables aux producteurs s'articulent autour de trois phases:

a) Préparation: mettre au point des mécanismes appropriés pour se préparer à participer aux activités de partage d'informations sur les menaces.

b) Analyse: effectuer une analyse en vue de produire des informations de qualité sur les menaces.

c) Partage: partager les informations sur les menaces produites avec les parties intéressées.

9.3 Orientations à suivre durant les phases de la procédure

9.3.1 Orientations à l'intention des organismes en tant que consommateurs

9.3.1.1 Orientations relatives à la phase de préparation

Il est recommandé aux organismes d'élaborer leur politique relative aux informations sur les menaces pour la sécurité des véhicules connectés, notamment en fixant des objectifs, en définissant le champ d'application et en établissant le processus de prise de décisions. Pour ce faire, il convient de procéder comme suit:

a) Fixer des objectifs: les organismes doivent prendre note du fait qu'ils font face à des menaces de sécurité. Compte tenu de l'analyse des menaces pour la sécurité des organismes, il est recommandé à ces derniers de déterminer leurs objectifs en matière de sécurité pour renforcer leurs capacités de protection de la sécurité.

b) Définir le champ d'application: compte tenu des objectifs en matière de sécurité, des capacités techniques et du budget financier des organismes, ainsi que des incidences que pourraient avoir différentes menaces pour l'organisme, il est recommandé de définir la portée des informations sur les menaces dont l'organisme a besoin et de déterminer le rang de priorité.

c) Établir le processus de prise de décisions: il est recommandé de déterminer le temps nécessaire à la prise de décisions selon le type d'informations sur les menaces dont l'organisme a besoin et le rang de priorité, de façon à éviter qu'un processus de décisions chronophage ait des répercussions sur l'élimination en temps voulu des informations sur les menaces.

9.3.1.2 Orientations relatives à la phase de réception

Il convient de procéder comme suit:

a) Il est recommandé aux organismes de stocker correctement les informations sur les menaces pour la sécurité qui ont été partagées.

b) Il est recommandé aux organismes de prendre des mesures pour garantir la sécurité du stockage des informations sur les menaces.

c) Il est recommandé aux organismes d'effacer des informations sur les menaces obsolètes ou inutiles.

9.3.1.3 Orientations relatives à la phase d'analyse

Il convient de procéder comme suit:

a) Il est recommandé aux organismes d'évaluer la valeur des informations sur les menaces. On trouvera dans l'Appendice II une méthode de référence pour évaluer la valeur des informations sur les menaces. Une évaluation automatique est recommandée.

b) Il est recommandé aux organismes de procéder à des vérifications et d'effectuer des analyses pour évaluer les dommages qui pourraient être causés à leurs produits et services.

c) Il est recommandé aux organismes d'analyser le contexte en vue d'identifier les informations relatives aux auteurs des attaques, aux TTP et aux cibles, par exemple.

d) Il est recommandé aux organismes d'identifier les actifs touchés, comme les serveurs, le(s) domaine(s), l'/les unité(s) de commande électronique(s) (ECU), le(s) système(s), etc.

e) Il est recommandé aux organismes de filtrer, de procéder à des vérifications et d'effectuer des analyses dans un environnement sécurisé afin d'éviter toute incidence sur les systèmes essentiels des organismes.

9.3.1.4 Orientations relatives à la phase d'atténuation

Il convient de procéder comme suit:

a) Il est recommandé aux organismes de développer des solutions de traitement et de mettre en œuvre leurs processus de traitement compte tenu des informations sur les menaces et des résultats des analyses. Les solutions comprennent la déconnexion, l'installation de programmes de correction, la mise à jour logicielle et la modification de la configuration, pour ne citer que ces exemples.

b) Il est recommandé aux organismes qui ne disposent pas des capacités de traitement nécessaires de prendre contact avec les équipes de coordination pour les véhicules connectés et de demander une assistance.

c) En ce qui concerne les indicateurs, il est recommandé aux organismes de déployer les indicateurs reçus dans les dispositifs de cybersécurité.

d) En ce qui concerne les menaces de sécurité apportées par des utilisateurs légitimes, par exemple moyennant la modification de la configuration ou la diffusion de programmes malveillants, il est recommandé aux organismes d'analyser sans délai la situation et de renforcer la gestion. Les organismes peuvent réparer et gérer les vulnérabilités exploitables, les défauts ou la mauvaise configuration du réseau en utilisant les informations sur les menaces, y compris les mesures d'élimination.

9.3.1.5 Orientations relatives à la phase de prévention

Il est recommandé aux organismes de continuer de surveiller leurs produits et services.

9.3.2 Orientations à l'intention des organismes en tant que producteurs

9.3.2.1 Orientations relatives à la phase de préparation

Il est recommandé aux organismes d'élaborer leur politique, notamment en fixant des objectifs, en définissant le champ d'application et en établissant le processus de prise de décisions. Il convient de procéder comme suit:

a) Il est recommandé aux organismes d'établir un processus de gestion des interventions pour éviter la fuite de données importantes.

b) Il est recommandé aux organismes de déployer des ressources et des outils essentiels pour produire des indicateurs et d'autres données sur les menaces.

c) Il est recommandé aux organismes d'identifier, d'évaluer et de classer les données sur les menaces pour le réseau qui sont hétérogènes et qui proviennent de sources multiples, de façon à veiller à ce que toutes les informations relatives aux menaces soient décrites en tout point et entièrement mises à jour, à tout moment.

d) Il est recommandé aux organismes de mettre sur pied ou d'intégrer une communauté de partage, d'obtenir des données en achetant/recevant des renseignements non publics et en collectant des renseignements publics, d'analyser ces données en fonction de certains scénarios d'application et de certaines exigences opérationnelles, et de produire ensuite les renseignements sur les menaces correspondants. Dans le cadre du partage, une communauté de partage intègre les informations sur les menaces partagées par tous les membres selon les besoins actuels, en vue de produire des renseignements sur les menaces plus ciblés, plus complets et précis, et les partage sous la forme de renseignements à code source ouvert ou de renseignements payants, en fonction du type et de la valeur des renseignements.

e) Il est recommandé aux organismes de définir la portée des activités de partage d'informations, notamment en définissant les informations sur les menaces à partager et en décidant du format d'échange.

9.3.2.2 Orientations relatives à la phase d'analyse

Il convient de procéder comme suit:

a) Il est recommandé aux organismes de filtrer les journaux d'alerte de manière automatique ou manuelle, afin de supprimer les alertes inutiles, voire les fausses alertes.

b) Il est recommandé aux organismes d'évaluer la valeur des informations partagées et de définir le mandat de l'organisme de partage.

c) Il est recommandé aux organismes de définir l'observabilité de divers scénarios relatifs aux menaces pour les réseaux ainsi que des métadonnées correspondantes, et d'analyser et de traiter par la suite les résultats de la comparaison de ces indicateurs relatifs aux caractéristiques des menaces.

9.3.2.3 Orientations relatives à la phase de partage

Il convient de procéder comme suit:

a) Il est recommandé aux organismes de mettre en œuvre le partage d'informations sur les menaces selon le champ d'application défini.

b) Il est recommandé aux organismes de fournir des informations sur les menaces pour la sécurité dans un format normalisé.

c) Il est recommandé aux organismes de fournir davantage d'informations contextualisées.

d) Il est recommandé aux organismes de formuler le modèle et les mécanismes de partage, et de résoudre les questions ayant trait à la validité du partage et de l'échange de renseignements et à l'équité des transactions.

e) À la lumière des besoins en matière de développement du secteur, il est recommandé de créer une plate-forme d'échange et de partage d'informations sur les menaces pour les véhicules connectés afin de procéder au partage d'informations.

f) Il est recommandé aux organismes de mettre au point un mécanisme de contrôle pour le partage des données d'informations sur les menaces, y compris pour ce qui est de la désensibilisation, de l'authentification et de la destruction des données partagées.

g) Compte tenu de la capacité de produire des informations sur les menaces pour les véhicules connectés, il est recommandé aux organismes de partager des informations sur les menaces avec des organismes jouissant d'une bonne réputation.

Appendice I

Bonnes pratiques définies par le Centre Auto-ISAC concernant les activités de partage d'informations sur les menaces

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

Le Centre d'échange et d'analyse des informations sur le secteur automobile [b-AUTO-ISAC] a publié, en 2019, un guide de bonnes pratiques, intitulé "Collaboration and engagement with appropriate third parties" *(Collaboration avec les tierces parties compétentes et mobilisation de celles-ci)*, version 1.3. Dans ce guide de bonnes pratiques, le Centre Auto-ISAC fournit des bonnes pratiques en matière de partage d'informations, notamment en ce qui concerne les tierces parties compétentes, le niveau d'ouverture, les contenus qu'il est utile de partager et les processus de partage d'informations, etc.

Pour renforcer la cybersécurité des véhicules, ces organismes ont la possibilité de collaborer avec diverses tierces parties à l'échelle de l'écosystème des véhicules connectés et de les mobiliser. Au rang des tierces parties compétentes figurent des partenaires et des organismes du secteur privé, des gouvernements, des établissements universitaires, des instituts de recherche et des médias.

Les organismes peuvent déterminer le niveau approprié d'ouverture en fonction de leurs objectifs individuels en matière de cybersécurité des véhicules et du paysage des risques qui leur est propre. Le niveau d'ouverture peut être classifié comme suit: limité, modéré et élevé.

Les principaux processus pour partager des informations avec diverses parties prenantes sont les suivants:

a) Identifier des contenus qu'il est utile de partager.

b) Mobiliser les parties prenantes internes compétentes.

c) Créer des processus pour recevoir des informations partagées et prendre des mesures en conséquence.

d) Créer des processus pour diffuser des informations auprès de tierces parties externes.

e) Acquérir les outils et les technologies appropriés.

Appendice II

Méthode pour évaluer la valeur des informations sur les menaces

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

Lors de l'évaluation de la valeur de chaque information sur les menaces, les organismes peuvent se baser sur cinq facteurs, tel qu'indiqué ci-dessous:

a) Réputation des sources de menace: la réputation des sources de menaces diffère selon le cas. En effet, les sources dont la réputation est élevée peuvent fournir des informations sur les menaces qui ont plus de valeur.

b) Diffusion des informations en temps voulu: les informations sur les menaces sont sensibles au temps. Des informations plus précoces peuvent aider les organismes à protéger leurs actifs et à prévenir les attaques à leur encontre.

c) Complétude de la description: en général, les informations sur les menaces qui contiennent des descriptions plus détaillées et des informations contextualisées ont plus de valeur.

d) Pertinence et incidence pour l'organisme: certaines informations sur les menaces visent un secteur précis, des produits spécifiques, voire des entreprises en particulier. Les informations sur les menaces relatives à un organisme donné doivent faire l'objet d'une attention particulière.

e) Efficacité des informations sur les menaces: la multiplicité des ressources entraîne la duplication et les collisions d'informations sur les menaces, raison pour laquelle la fusion des menaces similaires et la détermination de l'authenticité des informations peuvent améliorer l'efficacité des informations sur les menaces au sein d'un organisme.

Bibliographie

[b-AUTO-ISAC] *Collaboration and Engagement with Appropriate Third Parties Best Practice Guide*, Version 1.3, 2019.

[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-GSMA CLP.11] GSMA CLP.11 (2020), *IoT Security Guidelines Overview Document, Version 2.2.*

[b-GSMA CLP.14] GSMA CLP.14 (2020), *IoT Security Guidelines for Network Operators, Version 2.2*.

[b-OASIS TAXII] *OASIS Committee Specification*, TAXII™ Version 2.1.

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, 2023