VAS institute



Rapport nº 2022-R-08-FR

Cybersécurité de la conduite connectée

SERVICE PUBLIC FÉDÉRAL
MOBILITÉ ET TRANSPORTS

CYBERSÉCURITÉ DE LA CONDUITE CONNECTÉE

Rapport nº 2022 - R - 08 - FR

Auteurs : Dagmara Wrzesinska, John-John Deleuze

Révision : Lina Kolesnikova, Annelies Develtere

Éditeur responsable : Karin Genoe

Éditeur : Institut Vias

Date de publication : 4/01/2022

Dépôt légal : D/2022/0779/21

Veuillez référer au présent document de la manière suivante : Wrzesinska, D., & Deleuze, J.J (2022). Cybersécurité de la conduite connectée. Bruxelles : Institut Vias

Dit rapport is eveneens beschikbaar in het Nederlands onder de titel: Cyberveiligheid bij geconnecteerde voertuigen

This report includes a summary in English.

Remerciements

Cette étude a été financée par le Service Public Fédéral Mobilité et Transports.

Les auteurs et l'institut Vias souhaitent remercier les personnes et organisations suivantes pour leur contribution à cette étude :

l'Université Howest pour l'engagement enthousiaste dans le projet et l'invitation à participer au programme de stages de l'université, surtout **Preben Ver Eecke**, qui a aimablement soutenu et coordonné la collaboration.

Gauthier Willaerts, étudiant en informatique appliquée à l'université de Howest, pour une collaboration extraordinairement fluide et agréable, pour avoir complété l'équipe avec l'expertise cruciale pour le projet et pour une grande flexibilité pendant la période de confinement compliquée.

La responsabilité exclusive du contenu du rapport incombe à ses auteurs.

Table des matières

Summary 5
1. Contexte 6
2. Normalisation 7
2.1. Norme ISO/SAE 21434 8
2.2. CEE-ONU WP.29 8
2.3. Rapport entre la norme ISO et le règlement WP.29 9
3. Dépendances V2X 12
3.1. Technologie de communication V2X 12
3.2. Défis et exigences V2X 13
3.3. Solutions de sécurité V2X 14
4. Qui sont les hackers ? 16
4.1. White hats (chapeaux blancs) 16
4.2. Black hats (chapeaux noirs) 16
4.3. Grey hats (chapeaux gris) 16
5. Comment procèdent-ils ? 17
5.1. Taxonomie des menaces 17
5.2. Surfaces d'attaque 18
5.3. Vecteurs d'attaque 20
5.4. Dépendances et scénarios 21
5.5 Scénarios d'attaque appliqués 23
5.5.1Attaque « rolljam » 23
5.5.2Attaque d'infodivertissement 25
5.5.3Attaque OBD-II 26
5.5.4Attaque TPMS 28
6. Tentatives antérieures connues 31
7. Contre-mesures 34
8. Recommandations 36
9. Glossaire 39

Summary

The increasing connectivity of the vehicles results in a rise of automotive cyberattack and a growing number of threats across the entire automotive supply chain. With the increasing number of connected vehicles, increase of vulnerabilities is expected to follow. Cyber incidents with malicious intent in 2020 accounted for majority of the attacks (54,6%) and keep growing exponentially. The outbreak of COVID19 pandemic, imposed even more challenges and increased the exposure to safety breaches.

One of the most efficient way to ensure the cybersecurity of the vehicle over its entire life time – the *security by design* approach – is reflected in the growing number of standardization in the domain. Notably, ISO/SAE 21434 and the regulation of UNECE WP.29 on cybersecurity have been introduced to the market.

In this study, we lay the main focus on the threats related to Vehicle-to-Everything (V2X) communication, which supports the rise of connected and autonomous vehicles. It allows use cases such as vehicle platooning, cooperative collision avoidance and remote driving which results in an improved road safety and traffic flow thanks to real-time data exchange. To support such exchange, two main technologies are used: Dedicated Short Range Communication (DSRC), known as ITS-G5 in Europe, and hand Cellular V2X (C-V2X) using LTE, 4G and 5G in the near future. Different types of resulting challenges as well as possible countermeasures are discussed in this report.

We analyse 10 different types of possible cyberattacks, 12 attack surfaces and 5 attack vectors. Based on this framework, we constructed 4 attack scenarios that we applied on the vehicle from our own fleet. Two of them we were able to execute successfully.

Lastly, the 4-level countermeasure framework for ensuring cybersecurity is discussed as well as some possible technological solution that can reduce the risk of security. Additionally, we propose 5 major focus areas for the authorities to invest their efforts in the future.

1. Contexte

Les résultats de nos recherches préliminaires ont mis en évidence que la connectivité croissante de l'industrie automobile a induit une augmentation des cyberattaques automobiles et à cet égard, il est urgent que les fabricants d'équipement d'origine (OEM) fassent de la cybersécurité une priorité dans leur organisation afin de garantir la sécurité et la sûreté des usagers de la route. En 2020, les cyberincidents causés par des hackers dits « black hats » ont donc diminué d'environ 3 % par rapport à l'année précédente, mais la majorité des attaques ont toujours des intentions malveillantes (54,6 %). 2020 a imposé à l'industrie automobile de nombreux nouveaux défis qui ont également impacté sa cybersécurité :

- les OEM et les entreprises de niveau 1 ont vu leur chaîne d'approvisionnement perturbée en raison du confinement international et de la baisse de la demande de véhicules. C'en sont suivis l'interruption de sites de production, comme General Motors, Volkswagen ou BMW, et des pertes de revenus qui se chiffrent en milliards. Les OEM peuvent toutefois sortir plus forts de cette crise en revisitant leurs structures et leurs processus opérationnels, et peuvent se concentrer sur de nouvelles opportunités pour stimuler la demande avec la conduite électrique, connectée et partagée. Par ailleurs, en 2022, il sera obligatoire pour les véhicules circulant sur les routes de l'UE de disposer de systèmes avancés d'aide à la conduite (ADAS) soutenus par des technologies de communication V2X (Véhicule-à-Tout) qui augmentent considérablement le nombre de vulnérabilités et de points d'entrée, ce qui devrait aiguiser l'intérêt des hackers.

- De nombreux incidents de cybersécurité automobile surviennent en raison du manque de compétences en cybersécurité dont souffrent les OEM. Un effet dramatique de la Covid-19 est que les entreprises voient leur budget informatique impacté en raison de l'incertitude des revenus pour les années à venir. Selon une enquête de l'(ISC)², la crise sanitaire a creusé le déficit de compétences pour plusieurs raisons, notamment la baisse des budgets informatiques, et les travailleurs de la cybersécurité ont été affectés à d'autres rôles informatiques en raison de l'augmentation du télétravail et de la difficulté d'embaucher des personnes qualifiées. Par conséquent, l'écart se creuse, surtout à la lumière du nombre accru de cyberattaques. Pour combler ce manque, nous relevons une augmentation du nombre d'OEM qui lancent des programmes de primes aux bogues, comme Ford, GM, Tesla et Daimler. Il s'agit de programmes ou de concours lancés par une organisation pour déceler une faille dans sa cybersécurité en échange d'une récompense financière.

- Plus de 207 nouveaux cyberincidents automobiles ont été signalés en 2020, ce qui égalise le record, soit une augmentation de 34 % par rapport à 2019. Il est important de noter que tous les incidents ne sont pas déclarés publiquement et que de nombreuses activités de cyberpiratage illégales surviennent sur le dark web.

- Les attaques de serveurs ont augmenté de 73 % depuis 2019. Elles ont ciblé un serveur télématique, un serveur de données et un serveur web, elles se font à distance et à longue portée, et nécessitent des outils peu onéreux. L'attaque de serveurs est une pratique bien connue dans d'autres secteurs, mais ce type d'attaque cible de plus en plus le secteur automobile. Une telle attaque peut permettre au hacker d'avoir un accès non autorisé à plusieurs véhicules à la fois. C'est ce qui s'est produit en août 2020 quand un hacker a pu accéder à l'ensemble de la flotte de véhicules Tesla par le serveur de commande et de contrôle.

2. Normalisation

Une vingtaine de normes et réglementations applicables au domaine de la cybersécurité automobile ont été identifiées et sont répertoriées dans le tableau ci-dessous. Certaines d'entre elles ont été développées avant que l'industrie automobile ne soit ciblée par les cybermenaces d'aujourd'hui. Toutefois, du fait qu'elles ont été rédigées pour assurer le fonctionnement en toute sécurité des composants électroniques ou du protocole de communication, elles présentent toujours de l'intérêt pour produire des véhicules connectés sûrs et sécurisés.

Aujourd'hui, il est intéressant de se concentrer sur la norme ISO/SAE 21434 et la réglementation WP.29 de la CEE-ONU sur la cybersécurité. Elles seront, en effet, toutes deux publiées prochainement dans leur version définitive, avec leur application à court terme.

Standard code	Year	Full name	Link
IATF 16949	2016	Automotive Quality Management System	link
IEC 62443-2-1	2010	Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program	link
ISO 9001[1]	2015	Quality Management Systems — Requirements	link
ISO 14229-1:2020	2020	Road vehicles — Unified diagnostic services (UDS) — Part 1: Application layer	link
ISO 14230-2:2016	2016	Road vehicles — Diagnostic communication over K-Line (DoK-Line) — Part 2: Data link layer	link
ISO 15765-2	2016	Standard for Sending Data Packets Over a CAN-Bus -> Road Vehicles: Diagnostic Communication over Controller Area Network (DoCAN)	link
ISO 17458-1	2013	FlexRay Communications System	link
ISO 20078	2021	Extended vehicle (ExVe) web services	link
ISO 21434	2021	Road vehicles — Cybersecurity Engineering	link
ISO 26262- 3	2018	Road vehicles — Functional safety — Part 3: Concept phase -> Classification of hazardous events	link
ISO 26262-1:2018	2018	Road vehicles — Functional safety — Part 1: Vocabulary	link
ISO 29147	2018	Information technology — Security techniques — Vulnerability disclosure	link
ISO 31000:2019	2019	RISK MANAGEMENT: Assessment Techniques	link
ISO/IEC 27001	2018	INFORMATION SECURITY MANAGEMENT: Information technology — Security techniques — Information security management systems — Overview and vocabulary	link
ISO/IEC DIS 18045	2020	Information Security, Cybersecurity and Privacy Protection — Evaluation criteria for IT security — Methodology for IT security evaluation **(work in progress)**	link
ISO/IEC/IEEE 12207:2017	2017	Systems and Software Engineering — Software life cycle processes **(work in progress)**	link
ISO/IEC/IEEE 15288:2015	2015	Systems and Software Engineering — System life cycle processes **(work in progress)**	link

PAS 1885	2018	The Fundamental Principles of Automotive Cyber Security	link
PAS 11281	2018	Connected Automotive Ecosystems – Impact of Security on Safety – Code of practice	link
SAE J2602	2012	LIN Network for Vehicle Applications: Minimum Standard Level of Performance (seat belts, air conditioning, door locks etc.)	link
SAE J3061	2016	Cybersecurity Principles and Guidance for Cyber-Physical Vehicle Systems	link
SAE J3101	2020	Common Requirements for Security to be implemented in Hardware for Ground Vehicles	link
ISO/CD 24089	2020	Road vehicles – Software engineering	link

2.1. Norme ISO/SAE 21434

Le travail conjoint entre SAE et ISO devrait être une référence pour une chaîne d'approvisionnement cybersécurisée dans le secteur automobile. Soumise à consultation publique en 2020, cette norme est en cours d'examen par des comités techniques et la version définitive de la norme a été publiée mi-2021. La norme ISO/SAE 21434 vient s'ajouter à la norme ISO 26262 « *Véhicules routiers - Sécurité fonctionnelle* » en tant que norme liée à la sécurité dans le processus de développement automobile. De nombreuses entreprises, dont des OEM, des fournisseurs de matériel et des acteurs de la cybersécurité, travaillent sur cette norme dont les objectifs sont nombreux :

1	Créer une norme automobile mondiale avec une terminologie commune pour l'ingénierie de la cybersécurité
2	Définir les exigences minimales pour les processus et les activités en ingénierie de la cybersécurité
3	Promouvoir la coopération entre les différentes parties prenantes de la chaîne d'approvisionnement automobile
4	Considérer le véhicule sur l'ensemble de son cycle de vie : conception, fabrication, vente, maintenance après-vente, démantèlement

Son objectif principal est de veiller à la sécurité dès la conception. Elle vise à sécuriser le développement de véhicules sûrs, mais elle intègre également des objectifs de cybersécurité tout au long du cycle de vie du véhicule.

2.2. CEE-ONU WP.29

Le 25 juin 2020, le Forum mondial de l'harmonisation des Règlements concernant les véhicules WP.29, un groupe de travail de la Commission économique pour l'Europe des Nations Unies (CEE-ONU) a adopté la première réglementation en matière de cybersécurité automobile de l'histoire : Règlements CEE-ONU (UNR) n°155 et n°156.

- UNR 155 : ce règlement énonce les différentes exigences auxquelles les OEM doivent satisfaire pour l'approbation et la certification de leur système de gestion de la cybersécurité (CSMS). L'OEM et ses fournisseurs doivent fournir des preuves de l'analyse des cybermenaces et de la mise en œuvre de

contre-mesures afin d'obtenir l'approbation. Il vise à permettre plusieurs cyberactivités, de la gestion des risques aux tests de pénétration, en passant par la détection et la réponse aux incidents, la surveillance des menaces, etc., tout au long du cycle de vie du véhicule. Le règlement s'appuie sur la norme ISO 21434. Du fait que l'ensemble du cycle de vie est en jeu, il pourrait toutefois ne pas être suffisant de limiter la portée du cybersystème aux OEM.

- UNR 156 : approbation de la cybersécurité du type de véhicule en ce qui concerne la mise à jour logicielle et le système de gestion des mises à jour logicielles (SUMS). Elle vise à fournir des mises à jour logicielles sûres et sécurisées en instaurant une base légale pour les mises à jour dites « Over-the-Air » (OTA) de logiciels embarqués de véhicules. Ce règlement s'avère pertinent compte tenu de l'évolution constante du marché des options de mise à niveau logicielle des véhicules.

Ces deux règlements prescrivent les exigences et les mesures dans 4 disciplines distinctes :

- Gérer les cyberrisques liés aux véhicules ;
- Sécuriser les véhicules dès la conception pour atténuer les risques tout au long de la chaîne de valeur ;
- Détecter et répondre aux incidents de sécurité dans l'ensemble du parc automobile ;
- Fournir des mises à jour logicielles sûres et sécurisées en instaurant une base juridique pour ce que l'on appelle « OTA ».

Ces réglementations auront un impact sur l'industrie automobile à court terme, car les OEM devront se conformer aux réglementations pour leurs activités. Pour juillet 2022, les gammes de véhicules nouvellement produits doivent être conformes aux UNR 155 et 156 pour être vendues dans les États membres et à partir de juillet 2024, l'approbation de cybersécurité sera obligatoire pour les nouveaux véhicules produits. Ces échéances sont proches, les OEM doivent donc commencer à se préparer sans attendre pour être en phase avec le calendrier.

2.3. Rapport entre la norme ISO et le règlement WP.29

La dernière version du règlement n°155 de la CEE-ONU stipule clairement que la norme ISO/SAE 21434 soutient la mise en œuvre des exigences en matière de CSMS imposées aux organisations tout au long de la chaîne d'approvisionnement. De même, ISO élabore actuellement une norme ISO/CD 24089 « Véhicules routiers — Ingénierie de mise à jour du logiciel » pour soutenir l'UNR 156. Par conséquent, l'ISO/SAE 21434 et l'UNR 155 sont complémentaires et visent, tous deux, à sécuriser les véhicules connectés de façon similaire. On peut en distinguer plusieurs caractéristiques communes :

- **Technologiquement neutre** : les deux réglementations ne sont pas restrictives en décrivant des solutions techniques ou des processus spécifiques que les OEM doivent inclure dans leur CSMS. En effet, une description trop précise dans une réglementation sur la cybersécurité peut s'avérer dangereuse en raison de l'évolution constante du paysage de la cybersécurité et des nouvelles technologies. Les exigences décrivent donc des processus ou des fonctions dont devrait être doté un véhicule plutôt qu'une technologie spécifique.

- **Cycle de vie et chaîne d'approvisionnement sécurisée :** il est aisé de constater que la norme et la réglementation ont été élaborées en parallèle avec les personnes impliquées dans les deux, car elles partagent deux aspects importants. Tout d'abord, elles sont toutes deux révolutionnaires dans le domaine de la cybersécurité automobile, car elles obligent les OEM à mettre en œuvre des processus de cybersécurité tout au long du cycle de vie du véhicule, du développement à la postproduction. Ensuite, elles stipulent toutes deux que les OEM sont responsables de la sécurité et de la conception du produit, et doivent dès lors veiller à ce leur chaîne d'approvisionnement soit, elle aussi, sécurisée. Ils doivent spécifier et vérifier les exigences de sécurité et les processus des niveaux avant l'intégration des composants ou des logiciels.

- **Approche :** toutes deux ont une approche holistique de la cybersécurité automobile en décrivant les processus de pratiques de gouvernance aux niveaux organisationnel et opérationnel. Toutefois, l'UNR 155 envisage également une approche plus pratique de la cybersécurité en décrivant de façon détaillée des exemples pratiques de menaces et les mesures d'atténuation correspondantes dans son annexe 5.

- **Sécurité dès la conception :** ce concept est au cœur de la réglementation de la CEE-ONU et de la norme ISO. L'idée est de considérer la sécurité dès la première phase de la conception du produit afin que des mécanismes d'atténuation soient déjà intégrés et qu'il soit donc plus facile de mettre au jour de nouvelles menaces émergeant au cours du cycle de vie du produit. Ce processus est effectué à l'aide d'une analyse des risques de sécurité où les impacts sur la sécurité, les finances, les opérations et le respect de la vie privée sont évalués de façon itérative jusqu'à ce que le niveau de risque soit acceptable. Le fait qu'un produit soit conçu, mis en œuvre et testé pour être « sécurisé » (même si nous savons tous que la sécurité à 100 % n'existe pas) n'implique toutefois en aucun cas que le fonctionnement de ce produit est sécurisé. La combinaison de contrôles de sécurité liés aux produits et aux opérations est généralement une approche avantageuse.

- **CSMS :** ils nécessitent la mise en œuvre efficace d'un système de gestion de la cybersécurité au sein de l'organisation.

Aspect	Norme ISO/SAE 21434	CEE-ONU WP.29
Objectif	Établir des critères minimaux pour l'ingénierie automobile en matière de cybersécurité	Implémentation du CSMS et réception par type des véhicules
Utilisateur	OEM, niveau 1, niveau 2	OEM
Aspect juridique	Non juridiquement contraignant	Juridiquement contraignant
Date	Mi-2021 (publication)	Janvier 2021 (entrée en vigueur)
Lieu d'entrée en vigueur	Partout	54 pays membres
Type de véhicule	Tous types de véhicules routiers	Toutes les catégories de 4 roues
Phase du véhicule considérée	Cycle de vie complet (conception, ingénierie, production, exploitation, maintenance et démantèlement)	Développement, production et postproduction
Cartographie des cybermenaces	Non	Oui (annexe 5 de l'UNR 155)
Validité du CSMS	Une fois	Tous les trois ans

Comme l'ont déjà expérimenté les autres secteurs, la phase de livraison du produit dans le cycle de vie est un point de départ important et critique. Elle est assez facile à réaliser, car le nombre d'acteurs est restreint. Il peut toutefois s'avérer difficile de pousser la sécurité dans la phase opérationnelle du cycle de vie en raison du nombre plus élevé d'acteurs impliqués. Par conséquent, le développeur du produit (OEM) doit sécuriser l'offre de produits en fonction des normes convenues (développement logiciel sécurisé, etc.). Sauf si nous souhaitons implémenter plusieurs écosystèmes fermés (par ex. un par OEM), comme l'écosystème Apple, il conviendrait de se pencher davantage sur la phase opérationnelle du cycle de vie (appelée ici « postproduction »). Les OEM ne peuvent être entièrement responsables de ce qui se passe dans la phase opérationnelle de leur produit. Ils prodiguent simplement des conseils sur la meilleure façon de l'utiliser et ils procèdent à des contrôles de sécurité dans la mesure acceptée par un marché. En dehors des écosystèmes

fermés de type Apple, l'OEM n'est pas nécessairement concerné par le fonctionnement de ses produits et les activités opérationnelles y afférentes. À titre d'exemple, prenons les véhicules « militaires » : l'OEM n'est pas considéré comme le meilleur candidat pour faire fonctionner des équipements aussi délicats.

3. Dépendances V2X

On peut distinguer deux types de communication des véhicules : Communication embarquée (IV) et Véhicule-à-Tout (V2X). La communication V2X a suscité énormément d'intérêt ces dernières années, car elle permet de soutenir l'essor des véhicules connectés et autonomes, et s'appuie sur des technologies sans fil qui peuvent améliorer la sécurité routière, la fluidité du trafic par la communication de données en temps réel. Le déploiement V2X permet des cas d'utilisation intéressants, comme le pelotonnage de véhicules, l'évitement coopératif des collisions et la conduite à distance, ce qui améliore la sécurité routière et la fluidité du trafic grâce à l'échange de données en temps réel entre les véhicules, l'infrastructure routière, les piétons et le réseau. Dans le système de communication V2X, on distingue quatre types principaux en fonction de l'interlocuteur du véhicule pour l'échange des données :

-**Véhicule-à-véhicule (V2V)** : le partage de données entre véhicules permet de connaître la vitesse et la position des autres véhicules. Il contribue à rendre la conduite plus prévisible et plus sûre.

-**Véhicule-à-infrastructure (V2I)** : échange sans fil de données entre le véhicule et les infrastructures routières, comme des feux de signalisation, une signalisation intelligente ou une unité routière (RSU). Le but est d'obtenir des données sur le trafic et les conditions météorologiques pour, au final, réduire le nombre d'incidents routiers et les coûts qui y sont associés.

-**Véhicule-à-piéton (V2P)** : communication entre un véhicule et un piéton à des endroits clés, comme un passage pour piétons ou un carrefour. Le principal objectif de V2P est de protéger les usagers faibles des véhicules.

-**Véhicule-à-réseau (V2R)** : il permet la diffusion d'avis relatifs à des accidents de la route sur le trajet, un embouteillage ou des conditions météorologiques, ou l'utilisation d'un service embarqué, comme le streaming multimédia.

3.1. Technologie de communication V2X

Le système de communication V2X dépend fortement des capacités du système de communication sous-jacent reliant les véhicules les uns aux autres et à l'infrastructure de transport. Aujourd'hui, l'Europe et l'Amérique du Nord sont confrontées à des problèmes dans le déploiement de V2X en raison du manque de clarté réglementaire et du choix de la technologie de communication sur laquelle devraient se baser les OEM, les opérateurs de réseau mobile, les prestataires de services et les exploitants de propriétaires d'infrastructures. En général, les exigences du système de communication V2X sont une fiabilité élevée, une faible latence pour les cas d'utilisation liés à la sécurité et une bande passante et un débit de données plus élevés pour les cas d'utilisation liés à la conduite autonome.

Deux technologies principales sont utilisées dans la communication V2X. D'une part, la communication dédiée à courte portée (DSRC), connue sous le nom d'ITS-G5 en Europe et d'autre part, Cellular V2X (C-V2X) recourant à la LTE, à la 4G et à la 5G dans un proche avenir. Tous deux s'appuient sur le spectre radioélectrique de la bande de fréquences de 5,9 GHz qui a été désigné en 1999 pour une utilisation du V2V et du V2I. ITS-G5 a été initialement désigné comme la norme technologique pour les services ITS, mais il n'a pas été déployé de manière significative tandis que, selon le CTO de NXP semiconductors, après des années de développement, la technologie est prête et nous disposons de puces DSRC de qualité industrielle, très précises et robustes, conçues pour résister au piratage.

En mars 2019, une proposition de la Commission européenne visait à utiliser ITS-G5 comme communication à courte distance pour les services d'urgence et à utiliser la 3G et la 4G comme infrastructure ITS. Cependant, 21 des 28 États membres ont rejeté la proposition, marquant ainsi leur désaccord sur le choix de la technologie à courte portée. Le débat sur ces deux technologies se tient également sur les marchés américain et asiatique. Les performances de C-V2X ne pouvant s'améliorer qu'avec le temps, il est toutefois raisonnable de penser que C-V2X sera la technologie de référence pour la communication V2X à long terme, sans certitude, cependant. Différentes initiatives sont déployées en Europe pour évaluer les performances des deux technologies, comme le projet Smart Highway en Flandre.

Les principaux avantages de C-V2X sont les suivants : efficacité à haute vitesse et trafic dense, technologie peu onéreuse, autogestion, portée et fiabilité améliorées, sécurité intégrée des réseaux mobiles. Un autre point positif de cette technologie de communication est qu'elle peut tirer parti de l'infrastructure mobile existante et que moins de RSU doivent donc être installées, ce qui réduit le coût de l'infrastructure. Les technologies C-V2X et 5G aideront à compléter les technologies ADAS et à soutenir le déploiement de la conduite autonome.

Le tableau ci-dessous résume les différentes caractéristiques de chaque technologie. La difficulté qu'il convient de signaler est que chaque technologie trouve ses partisans et qu'il peut donc y avoir des conflits d'intérêts dans certains documents de recherche. En outre, les performances sont également sujettes à des changements en raison des améliorations technologiques.

	DSRC	**C-V2X**
Technologie de puce	ITS-G5	LTE/4G/5G (technologie de modem mobile)
Bande de fréquence	5,9 GHz	
Norme de message	IEEE 802.11p	3GPP
Sécurité	Signature numérique/cryptographie	
Portée	Courte - 300 m	Courte (directe) et longue (= réseau mobile/V2N)
Exigences d'infrastructure	Unité routière (RSU)	RSU + Tour mobile existante
Déploiement	Depuis 2017	Déploiement initial en 2021
Caractéristiques	Connectivité réseau rapide Faible latence (max. 150 ms) Sécurisation par rapport au hacking Débit de données (jusqu'à 27 Mo/s)	Latence ultra-faible (1-10 ms) Large bande passante/Flexibilité (fonctionnement sur 3 fréquences) Fiabilité élevée Rétrocompatibilité (4G<->5G)

3.2. Défis et exigences V2X

De nombreux pays promeuvent de plus en plus la connectivité entre les véhicules et les infrastructures de transport, et les véhicules compatibles V2X émergent comme le véhicule de nouvelle génération, basé initialement sur la DSRC qui n'offre qu'une connectivité intermittente. Aujourd'hui, la technologie C-V2X semble être la technologie de communication de référence pour l'avenir. Les voitures connectées échangent des données avec les infrastructures de transport, comme des RSU, afin d'améliorer la sécurité de la circulation et d'offrir une grande efficacité dans les services de mobilité. Toutefois, cette connectivité accrue crée de nouvelles passerelles de cyberattaque, de nouveaux risques de cyberattaque qui peuvent avoir des conséquences graves si les systèmes V2X ne sont pas suffisamment sécurisés.

La communication V2X doit satisfaire à plusieurs exigences fonctionnelles, comme un niveau acceptable de fiabilité, de latence de bout en bout, de bande passante, de débit et de portée. Le niveau acceptable de chaque fonctionnalité varie selon le cas d'utilisation considéré et est répertorié dans ce livre blanc de 5GAA.

La communication V2X doit être fiable et présenter les exigences de sécurité suivantes :

- **Authentification :** la fonction de sécurité principale est d'assurer l'authentification du message avant exécution.
- **Intégrité :** juste après l'étape d'authentification, les messages échangés entre un véhicule et une infrastructure routière doivent être protégés de toute modification non autorisée afin d'assurer la fiabilité, l'exactitude et la fiabilité des messages. Toute modification de message doit être détectée.
- **Non-répudiation :** l'identité, l'emplacement et l'heure de l'expéditeur peuvent être tracés. Cela peut se faire par le biais de la signature numérique.
- **Confidentialité :** sous réserve des exigences réglementaires régionales, la communication V2X doit prendre en charge l'anonymat, l'utilisation de pseudonymes et la confidentialité de l'équipement utilisateur. Toutefois, l'identité d'une personne malveillante peut être tracée.
- **Disponibilité :** elle garantit que les systèmes et l'information sont accessibles et utilisables par les personnes autorisées. Par exemple, dans un environnement V2I, les unités routières doivent toujours être disponibles pour assurer la fiabilité cible.

Tout d'abord, il est important de souligner que la planification du réseau et le déploiement des technologies C-V2X auront un impact considérable sur l'éventuelle exploitation des vulnérabilités et la nature des menaces. D'une part, le système 5G standardisé 3GPP fournit certains services de sécurité bien éprouvés sur le système 4G et d'autres services, comme le cryptage, l'authentification et le respect de la vie privée des utilisateurs, sont améliorés. D'autre part, la 5G est basée sur une structure plus complexe créant de nouvelles opportunités d'attaque et n'est pas intrinsèquement protégée contre les attaques DDos et le brouillage radio. Afin de disposer d'une technologie C-V2X sécurisée, il appartient à l'opérateur réseau de déployer un réseau sécurisé et de réduire la quantité d'attaques de surface pouvant mettre en danger les usagers de la route.

De nombreux types d'attaques peuvent menacer la communication C-V2X et sont présentés dans ce document, mais l'attaque Sybil[1] est probablement l'une des plus dangereuses, car elle peut compromettre l'intégrité des messages et la confidentialité de l'identité. Les principales attaques qui sont liées à V2X sont de nature distante et sont décrites dans la section 5.1 : faux messages, modification de messages, attaque Sybil, DoS, espionnage, attaque d'usurpation d'identité, attaque par rejeu, attaque trou noir, attaque trou gris, suivi de localisation.

3.3. Solutions de sécurité V2X

Aujourd'hui, en termes de sécurité V2X, plusieurs nouvelles technologies ont émergé pour augmenter le niveau de sécurité des réseaux de communication, avec une plus grande évolutivité et un contrôle bien plus précis. Certaines technologies présentent des capacités intéressantes pour sécuriser les communications dans le réseau de véhicules, mais certaines d'entre elles reposent sur une opération informatique complexe qui pourrait s'avérer peu pratique pour sécuriser une grande quantité de données en un bref laps de temps.

Isolement du V2X : cette mesure de sécurité ne précise pas de technologie particulière, mais concerne le rôle sécuritaire de l'architecture du module V2X. Des fonctions V2X peuvent être implémentées dans une ECU V2X dédiée ou dans une ECU existante. Il est recommandé de créer une ECU V2X dédiée, malgré les coûts supplémentaires que cela implique, car la sécurité peut être compromise en raison des vulnérabilités des autres ECU.

Infrastructure à clé publique pour véhicule (VPKI) : le problème des exigences de sécurité pour la communication V2X a été résolu à l'aide de certificats distribués et gérés par PKI. Ces certificats permettent que l'identité de l'expéditeur ne soit plus requise, mais que plusieurs pseudonymes soient, au lieu et place, attribués à un seul véhicule pour l'authentification des messages. Les pseudonymes du véhicule changent

[1] Le hacker subvertit le système de réputation d'un service de réseau en créant un grand nombre d'identités pseudonymes et les utilise pour avoir une influence disproportionnée.

fréquemment pour en éviter le traçage. La PKI assure des services de soutien, comme l'authentification, la fourniture et la révocation de pseudonymes, et est gérée par une autorité de certification.

Edge computing ou informatique en périphérie : un procédé dans lequel les données sont traitées à proximité de la source de données. L'edge computing offre une distribution correcte des ressources, un traitement plus rapide et une faible latence. Il peut assurer une bande passante élevée pour la disponibilité en répartissant les tâches de calcul.

Virtualisation de la fonction réseau : la NFV fait référence au processus de découplage des fonctions réseau du matériel intégré pour les faire fonctionner sur un logiciel, comme une machine virtuelle, ce qui peut fournir certaines fonctions de sécurité comme des pare-feu et des systèmes de détection d'intrusion, et des scanners de virus peuvent être instanciés et/ou migrés d'un nœud à l'autre à la demande pour aider à améliorer la sécurité globale de la communication V2X.

Blockchain ou chaîne de blocs : la technologie blockchain n'est pas encore utilisée pour sécuriser la transmission de données dans l'environnement V2X, mais elle présente un ensemble de fonctionnalités clés qui permettraient un niveau de sécurité et de confidentialité plus élevé. Elle est considérée comme un puissant outil de sécurisation des données, car elle repose sur de solides algorithmes de chiffrement et de déchiffrement, et empêche intrinsèquement la modification de toute donnée. La nature décentralisée de la blockchain garantit la confidentialité et l'intégrité des informations. Cette technologie introduit toutefois une charge non négligeable sur le réseau et va à l'encontre de l'exigence de faible latence de la plupart des cas d'utilisation V2X.

Software-Defined Networking : la gestion de réseau classique est complexe et sujette aux erreurs. Ces problèmes sont causés par le couplage fort de la transmission des données et de la logique de contrôle. En les découplant et en introduisant la programmabilité, il simplifie les tâches de gestion de réseau et offre davantage de flexibilité. Dans un environnement V2X, il peut être utilisé pour rediriger de façon dynamique et efficace les données vers différentes destinations.

Puissant chiffrement sans fil des données : les constructeurs veillent à ce que les informations échangées entre la voiture et l'infrastructure utilisent les derniers algorithmes de chiffrement afin qu'elles restent indéchiffrables pour les hackers.

4. Qui sont les hackers ?

Aujourd'hui, on peut distinguer différents types de hackers en fonction de leurs intentions et de l'aspect juridique de leur attaque. L'industrie automobile manque de personnes disposant de compétences en cybersécurité. Il est donc crucial pour elles de développer des activités de traçage et d'identification des hackers, et de tenter de les motiver à travailler pour les entreprises en trouvant et en corrigeant les vulnérabilités plutôt que de laisser ouverte la possibilité d'exploitations malveillantes. On peut distinguer trois types de hackers.I

4.1. White hats (chapeaux blancs)

Les « white hats », également connus sous le nom de « hackers éthiques », sont des personnes qui entrent par effraction dans un système de sécurité, toutefois sans intention malveillante, de l'intérieur (par ex. équipe de sécurité) ou de l'extérieur (par ex. chercheur indépendant) de l'organisation. L'aspect juridique de leur activité les rend différents des autres, car ils ont la permission des propriétaires de pirater leur système. Ils doivent toutefois veiller à ne pas enfreindre les lois régionales ou nationales.

Leurs principales activités sont les tests de pénétration et les évaluations des vulnérabilités : trouver les vulnérabilités, les contenus malveillants, les failles et les risques en testant un système informatique, un logiciel ou l'infrastructure informatique d'une organisation dans le but de prévenir toute attaque future. Les hackers « white hats » contribuent à améliorer la cybersécurité en décelant les menaces potentielles et sont donc bien perçus par l'industrie. L'un des moyens pour encourager les hackers « white hats » à s'impliquer est le *programme de primes aux bogues.*

4.2. Black hats (chapeaux noirs)

En revanche, les « black hats » utilisent leurs compétences de piratage illégalement avec une intention malveillante. Ils sont réputés pour des activités comme l'écriture de logiciels malveillants pour affaiblir et contourner un protocole de sécurité. Ils exploitent les vulnérabilités en sécurité et insèrent des logiciels rançonneurs et des logiciels espions. Leur motivation peut être pécuniaire en vendant les données personnelles des usagers de la route, en perturbant le service, et peut parfois entraîner la mort d'usagers de la route ou les blesser. Selon le dernier rapport sur la cybersécurité d'Upstream de 2020, 54,6 % des incidents ont été causés par des « black hats ».

4.3. Grey hats (chapeaux gris)

Ce troisième type de hackers se situe entre les « black hats » et les « white hats ». Ils pénètrent dans le système de sécurité et en recherchent les vulnérabilités sans l'autorisation du propriétaire, mais ils n'ont aucune intention malveillante comme les « black hats ». Leur motivation est souvent personnelle. Ils peuvent lancer une cyberattaque pour exposer à une entreprise ses vulnérabilités, sans toutefois causer de dommages, et facturer des frais pour y remédier, ou ils peuvent le faire pour accéder au produit payant d'un OEM.

5. Comment procèdent-ils ?

5.1. Taxonomie des menaces

Les cyberattaques peuvent être ventilées en deux grandes catégories : les cyberattaques à distance ou les cyberattaques physiques. Une attaque physique nécessite que le hacker soit physiquement connecté au véhicule tandis qu'une attaque à distance peut être effectuée à courte ou longue distance et dépendre de la connectivité du réseau. Une attaque physique nécessite la plupart du temps du matériel onéreux et n'est pas discrète du fait que le hacker doit avoir un accès physique au véhicule. En raison d'une connectivité accrue, les attaques d'accès à distance ont gagné en popularité, car elles sont moins onéreuses et plus difficiles à détecter et à contrer. Selon Upstream Security, entre 2010 et 2020, 79,6 % de toutes les attaques se sont faites à distance.

Il n'existe pas de taxonomie centrale pour les cyberattaques, mais l'annexe 5 du WP.29 UN R155 a identifié 69 méthodes d'attaque différentes, ventilées en 7 catégories de cybermenaces et de vulnérabilité. Du fait que les OEM devront montrer la façon dont ils atténuent les cybermenaces énumérées dans ce document en vue d'obtenir la conformité CSMS, les principaux types d'attaques peuvent être extraits et sont énumérés ci-dessous :

- Dans le cadre d'une **attaque frauduleuse**, l'intrus utilise une fausse identité ou envoie de fausses données. Il envoie des messages non autorisés contenant de fausses informations pour interrompre la communication du véhicule.
- Une **attaque par brouillage** consiste à interrompre, par un bruit de signal radio, la fréquence de la communication en vue d'obstruer ou d'entraver la communication V2X.
- Une **attaque masquée** est une intrusion qui utilise une fausse identité, comme une identité de réseau, pour avoir un accès non autorisé au véhicule sans authentification d'accès valide.
- Une **attaque par écoute**, également appelée « reniflage » ou « surveillance », est une incursion où les hackers tentent d'intercepter des informations qu'un véhicule envoie sur un réseau.
- Une **attaque trou noir** est une attaque courante où le hacker se trouve entre l'expéditeur et le destinataire, et arrête la transmission de messages. En créant un trou, le récepteur est plus en mesure d'intercepter des messages et peut en empêcher le fonctionnement en temps réel. Lors d'une *attaque trou gris*, le hacker ne transmet qu'une partie des messages, ce qui réduit ses chances de se faire attraper.
- Une **attaque par rejeu** est une sorte d'attaque trou noir, mais au lieu de faire passer les messages, le hacker les manipule afin d'attaquer le destinataire.
- Dans le cadre d'une **attaque par déni de service (DoS)**, un hacker inonde la cible de messages à haute priorité qui empêchent l'utilisateur légitime de recevoir ou de traiter tout autre message.
- Une **attaque par bus off** est un type d'attaque DoS où l'intrus envoie constamment des bits à la fois dans le champ ID et dans d'autres champs. Le compteur d'erreurs de transmission de l'ECU augmente alors jusqu'à ce que le bus CAN ne puisse pas transmettre ou recevoir de message.
- Lors d'une **attaque temporelle**, un hacker introduit un délai et l'indique à d'autres véhicules dans les environs, ce qui entraîne une mauvaise programmation des instructions et un faux embouteillage. Cette intrusion peut être catastrophique pour les réseaux de transport qui s'appuient sur des applications en temps réel.

- Une **attaque Sybil** se produit quand le hacker génère plusieurs identités et utilise chaque identité pour envoyer des messages différents à d'autres véhicules, aux piétons et aux infrastructures. L'objectif d'une attaque Sybil est d'induire en erreur d'autres véhicules, les piétons et les infrastructures afin qu'ils prennent de mauvaises décisions.

5.2. Surfaces d'attaque

Dans le cas de voitures connectées, l'accent est mis sur les attaques à distance. Dans ce contexte, les surfaces d'attaque font référence à des points d'entrée potentiellement vulnérables (pour des vecteurs d'attaque) où un utilisateur non autorisé peut tenter d'entrer, d'extraire ou de manipuler des données dans le véhicule pouvant être exploitées pour obtenir un accès non autorisé.

- **Télématique automobile :** les services télématiques permettent au véhicule de collecter et de transmettre des données opérationnelles aux systèmes télématiques de tête de réseau sous le contrôle d'un fournisseur de services télématiques (TSP), et de recevoir des données des systèmes du fabricant ou d'autres fournisseurs de services tiers. Les systèmes embarqués qui en sont responsables sont le système de diagnostic embarqué (dispositif OBD) et la passerelle télématique (TGU).

  La majorité des informations collectées et transmises par le véhicule dans le cadre d'opérations normales sont des informations de localisation, d'horodatages et de données décrivant l'état et la condition des composants critiques du véhicule. Ces données sont ensuite utilisées pour soutenir les calendriers de service en cours et les réclamations de garantie, et pour fournir des données de performances du monde réel pour une analyse ultérieure.

  Les données envoyées au véhicule comprennent des données de trafic en direct et de navigation, des alertes de service et même des mises à niveau logicielles « Over-the-Air ».

  Certains fabricants de services télématiques offrent au propriétaire du véhicule la possibilité d'interagir avec le véhicule à distance via une application téléphonique, pour lui permettre d'activer à distance la climatisation avant de prendre la route, de télécharger des cartes et des informations de navigation dans le système IVI, de localiser le véhicule par GPS, d'activer l'avertisseur sonore et les feux du véhicule ou même de déverrouiller à distance les portes du véhicule.

  Le système télématique embarqué est connecté à des sous-systèmes critiques du véhicule par l'intermédiaire du réseau central du véhicule et compte bon nombre de systèmes électroniques plus petits. La communication sans fil s'effectue sur des réseaux xG. Il est fourni à la fois par un modem mobile et une carte SIM, ou par un module machine-à-machine personnalisé avec le modem et l'électronique de la carte SIM intégrés dans un seul dispositif. Certaines des technologies de télécommunication sous-jacentes utilisées par les services télématiques, telles que xG, sont intrinsèquement non sécurisées en raison de leur prise en charge pour la transmission de données en texte en clair ou d'un cryptage faible et l'absence d'authentification mutuelle entre le dispositif mobile et la station de base mobile.

- **API SMS :** les SMS sont parfois utilisés comme canal de secours pour l'échange d'informations. Ils peuvent toutefois être déchiffrés et interceptés pour révéler des informations confidentielles. Les hackers peuvent également usurper les commandes SMS (remplacer ou modifier le numéro de mobile d'origine) en envoyant des commandes directes à l'appareil.

- **Interface web et API mobiles :** les hackers ouvrent des comptes sur une interface web à l'aide de paramètres comme des numéros SIM. En exploitant une application web, les hackers peuvent alors accéder à encore plus d'informations d'identification.

- **Applications mobiles :** les hackers s'attaquent aux vulnérabilités des applications mobiles qui donnent accès à des systèmes automatiques, comme la radio. Ils peuvent ensuite lire des fichiers sur des dispositifs multimédias.

- **Système de divertissement :** les hackers peuvent créer des fichiers multimédias qui peuvent changer de code sur le système. Cela ouvre des voies pour l'exploitation du système et même l'espionnage d'autres éléments des véhicules connectés.

- **Mises à niveau du micrologiciel :** lors des mises à niveau du micrologiciel, le système ne doit pas accepter de données externes. Dans le cas contraire, cela peut induire des attaques de porte dérobée reliant l'automobile au système du hacker.

- **Média sans fil :** les hackers peuvent s'attaquer aux vulnérabilités des canaux sans fil, comme le Bluetooth ou le wifi, pour contourner les privilèges d'administration.

- **Capteurs externes :** les hackers peuvent détourner des capteurs externes et forcer le véhicule à prendre des mesures non souhaitées.

- **Entrée à clé sans fil :** les hackers exploitent l'entrée à clé sans fil en utilisant un pont proxy entre la clé et le véhicule, ce qui leur permet de verrouiller ou d'ouvrir le véhicule à volonté.

- **Accès aux périphériques externes par le port OBD-II :** pourrait permettre aux hackers d'accéder aux systèmes internes du véhicule.

- **Attaques contre le service cloud du fournisseur automobile :** pourrait potentiellement permettre aux hackers d'attaquer de nombreuses voitures en une seule opération. Voir l'attaque sur le parc de véhicules Tesla en 2020.

- **Système de surveillance de pression des pneus :** les pneus peuvent contenir des capteurs de pression qui transmettent des données en temps réel à une ECU. Un hacker pourrait alors envoyer de faux messages de pneus dégonflés pour forcer le véhicule à s'arrêter pendant la conduite et il se peut qu'une voiture moderne empêche le moteur de démarrer avec des pneus dégonflés.

5.3. Vecteurs d'attaque

Les hackers peuvent exploiter les surfaces d'attaque en utilisant plusieurs vecteurs d'attaque, des méthodes pour exploiter ces points.

Serveurs : la plupart des incidents « black hats » concernent des serveurs back-end et couvrent un large éventail d'incidents concernant notamment des serveurs de commande et de contrôle télématiques, des services d'application de mobilité intelligente et des serveurs web enfreints comme le site web d'un OEM. Ils couvrent également les bases de données contenant des données sur les véhicules, les clients, les codes et les conducteurs. Les attaques de serveur impliquent souvent des vulnérabilités et des erreurs de configuration avec les TSP qui permettent au véhicule d'échanger des données avec des serveurs distants via un réseau mobile. Ces serveurs distants stockent les données collectées de véhicules et traitent des demandes de service à distance, comme le démarrage du moteur ou le verrouillage des portes, reçues d'une application sur smartphone. Les serveurs sont également le vecteur préféré des criminels qui utilisent des logiciels rançonneurs.

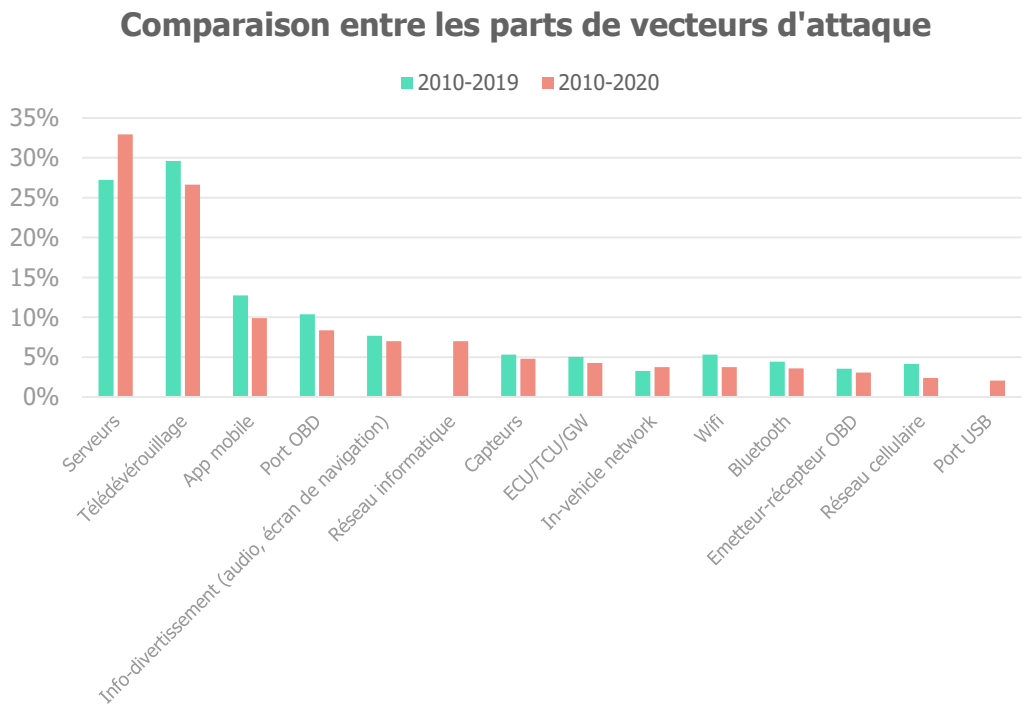
Entrée à distance sans clé : il existe quatre tendances pour ce type d'attaques de plus en plus fréquentes. L'une d'elles est un dispositif de programmation clé que les hackers utilisent pour tromper le connecteur de diagnostic et voler des voitures onéreuses. Ce vecteur est souvent relevé en Europe, en raison des lois sur la protection de la vie privée qui interdisent le chiffrement des données accessibles par le connecteur OBD. Le blocage sans clé est une autre technique qui consiste à bloquer le signal utilisé pour le verrouillage des portes de voiture. L'usurpation consiste à voler une clé cryptographique de véhicule. Enfin, les hacks de relais, où les criminels utilisent une boîte de relais pour capter le signal d'une télécommande à l'intérieur d'une maison et le transmettre pour ouvrir la porte d'un véhicule.

Port OBD : les systèmes OBD permettent au propriétaire du véhicule ou à un réparateur d'accéder à l'état des différents sous-systèmes du véhicule. Les attaques de port OBD nécessitent que le hacker ait un accès physique initial au véhicule même. Elles sont dès lors plus complexes. Toutefois, certains ports OBD peuvent être équipés d'un Bluetooth, d'un wifi d'un dongle/émetteur-récepteur mobile pour le diagnostic et la facilité d'accès, ou être placés préalablement par le hacker. Cela peut induire le vol de la voiture ou l'injection de messages de bus CAN malveillants pour manipuler le comportement du système de voiture, comme l'utilisation d'un brouilleur de signal pour empêcher les portes de voiture de se verrouiller. De nombreuses attaques provenant de l'accès au port OBD sont causées par un dispositif de dongle OBD directement fabriqué par le hacker.

Applications mobiles : les OEM développent souvent des applications mobiles qui permettent au propriétaire du véhicule de contrôler diverses caractéristiques de la voiture à distance à des fins d'accessibilité et de facilité d'utilisation. Tout d'abord, un hacker peut s'introduire dans l'application même, l'inverser pour en découvrir les vulnérabilités et l'utiliser pour accéder à une voiture. Naturellement, si un criminel s'empare du téléphone portable, il lui est encore plus facile de voler les données de la voiture ou du véhicule connecté. Ensuite, certaines applications ne sont pas ce qu'elles paraissent. Il peut en fait s'agir de fausses applications mobiles malveillantes créées de toute pièce pour sembler légitimes. Les hackers peuvent les utiliser pour récupérer les mots de passe des utilisateurs et prendre le contrôle de leurs comptes ainsi que des véhicules. Enfin, dans le cadre d'une attaque de l'homme du milieu, l'application mobile expose des données à caractère personnel et des contrôles de véhicule à des hackers. La connexion légitime d'un utilisateur (en l'occurrence le wifi) peut être utilisée à mauvais escient ou modifiée par un tiers.

Infodivertissement : le point d'entrée le plus courant pour accéder aux systèmes IVI se fait par lecture multimédia, des fichiers multimédias spécialement concoctés. Cela peut se faire par l'audio sur Bluetooth , wifi ou Android auto. Le port USB est également une possibilité si un adaptateur USB vers wifi est connecté par l'utilisateur ou via des moyens d'ingénierie sociale.

Le graphique ci-après représente la comparaison des parts de vecteurs d'attaque entre la période 2010-2019 et la période 2010-2020. Les serveurs, l'entrée sans clé et le mobile sont toujours les trois vecteurs d'attaque les plus fréquents.[2]



5.4. Dépendances et scénarios

Attaque « rolljam » :

Les clés de voiture utilisent la fréquence radio pour déverrouiller les portes du véhicule. Pour empêcher les hackers de capter le message de déverrouillage, les constructeurs automobiles utilisent un système appelé « codes roulants » où les clés suivent le code suivant dans une séquence qui correspond au code suivant de la voiture, de sorte qu'en théorie, les hackers ne puissent pas deviner le code suivant.

Quelle que soit la vulnérabilité à une attaque « rolljam », une telle attaque est censée être cachée sur ou à proximité d'un véhicule ou d'un garage cible. Le hacker est en attente d'une victime peu méfiante pour utiliser ses clés de voiture dans la portée radio. La victime remarquera seulement que sa télécommande n'a pas déverrouillé le véhicule à la première tentative. Sans se méfier, elle tente à nouveau de déverrouiller sa voiture. Cette fois, une pression réussie sur le bouton déverrouille les portes de la voiture. Le hacker peut alors revenir à tout moment pour récupérer ce qu'il convoite.

Dans la pratique, cela fonctionne en attendant que le propriétaire de la voiture appuie sur le bouton de déverrouillage. Le hacker envoie alors un signal de blocage qui empêche la voiture de recevoir le premier message de déverrouillage. C'est alors que le premier message de déverrouillage est enregistré. C'est possible du fait que la voiture lit une fréquence plus large que ce que la clé de voiture émet. Le signal de brouillage est plus fort que la clé.

Le propriétaire envoie alors le second signal de déverrouillage qui est également brouillé et enregistré. Le hacker envoie immédiatement le premier signal enregistré, faisant croire au propriétaire qu'il a déverrouillé le

[2] Basé sur le rapport d'Upstream Security « Global Automotive Cybersecurity Report 2021 »

véhicule avec le second signal. Le second signal est ainsi enregistré pour déverrouiller la voiture ultérieurement.

Impact : si le hacker réussit l'attaque « rolljam », en fonction du modèle de voiture, les portes pourraient être déverrouillées (au moins une fois) et laisser libre accès à l'intérieur de l'habitacle. Outre la question du vol d'objets, le hacker ne sera probablement pas en mesure de démarrer la voiture du fait que la clé est absente et que l'électronique est éteinte. Cela pourrait toutefois être le bon moment pour fixer ou brancher secrètement de l'électronique malveillante, comme un dongle OBD-II sans fil. Elle pourrait ensuite être utilisée pour contrôler la voiture dès qu'elle est mise sous tension par le conducteur.

Attaque par dongle OBD-II :

le port OBD2 est utilisé pour le diagnostic embarqué à l'aide du protocole CAN, une norme de bus de série de diffusion pour connecter les ECU, ce qui signifie qu'il n'y a pas d'ordinateur central. Quand une ECU envoie un message, une ECU sur deux sur le bus le reçoit et peut choisir d'y répondre ou de l'ignorer. Par exemple, le dispositif de commande du moteur envoie en continu un message CAN avec le régime moteur (en tr/min.). En principe, le port OBD-II est utilisé uniquement pour les diagnostics de lecture, mais avec certains équipements et composants électroniques spéciaux, il devrait être possible d'injecter des messages CAN dans le réseau pour cibler les ECU. Et pour étendre ce principe à une attaque sans fil, un dongle sans fil malveillant pourrait être secrètement branché au port OBD2.

Impact : le port OBD-II permet une connexion directe au réseau CAN. Cela permet d'interroger et de modifier presque tous les sous-systèmes du véhicule. Il peut être utilisé à mauvais escient en vue de compromettre la sécurité ou la sûreté du véhicule, notamment en programmant de nouvelles clés dans le module de sécurité du véhicule, en désactivant les systèmes d'alarme du véhicule, en téléchargeant des données d'étalonnage modifiées dans le module de commande du moteur (ECM) voire en désactivant les airbags et d'autres systèmes de sécurité.

Attaque TPMS :

le TPMS dans le pneu transmet des informations à l'ECU du véhicule par radio, tout en surveillant en permanence la pression du pneu pour permettre à l'ECU de déclencher un voyant d'avertissement sur le tableau de bord si la pression des pneus passe sous les spécifications. On sait que ces systèmes ont été déployés sans sécurité poussée. Une éventuelle attaque passive peut permettre aux hackers de suivre les mouvements et l'emplacement du véhicule à l'aide de stations de traçage mobiles ou routières, car les signaux TPMS peuvent être captés jusqu'à 40 mètres du véhicule. D'autre part, le manque de cryptage des signaux TPMS peut permettre une attaque active du fait que l'ECU du véhicule fait confiance à toute information fournie par les capteurs du véhicule. Il est donc possible d'injecter sans fil des signaux trompeurs, ce qui incite l'ECU à afficher de fausses mesures de pression des pneus. Dans certaines voitures modernes, il est même possible que la voiture s'arrête ou que le moteur refuse de démarrer.

Impact : la radio peut être analysée et exploitée à l'aide de radios définies par logiciel (SDR). Dans le cas du TPMS, il est possible d'effectuer une attaque active à l'aide d'une SDR et de forcer le véhicule à penser qu'un avertissement d'événement de basse pression TPMS est survenu alors que tous les pneus sont gonflés correctement. Cela pourrait présenter un risque important pour les occupants du véhicule si, par exemple, une personne importante se trouve à bord, et s'il est nécessaire de réduire à un minimum le nombre d'arrêts sur le trajet pour éviter d'être exposé à une attaque. En outre, dans le contexte des infrastructures de transport, si un système de la chaîne est compromis, cela met en danger d'autres véhicules ou systèmes.

Attaque d'infodivertissement :

l'infodivertissement permet aux utilisateurs d'accéder à la téléphonie, à l'audio, à la vidéo, à la navigation par satellite et aux informations de circulation en direct. Parfois, il fournit même une connectivité Internet et un accès aux services. Par conséquent, le système compte de nombreuses interfaces filaires et sans fil dont certaines sont accessibles aux occupants du véhicule tandis que d'autres sont exposées à distance. Il s'agit notamment de la radio, du Bluetooth, du wifi et d'autres services connectés. On peut tenter d'examiner ces interfaces et ports pour trouver des faiblesses qui pourraient permettre la manipulation des données voire l'escalade des privilèges au sein même du système. Puisque les systèmes d'infodivertissement diffèrent, une reconnaissance générale d'un système déterminé devrait d'abord être effectuée afin d'en évaluer les points faibles.

Impact : les composants individuels du système IVI peuvent être conçus et fabriqués par différentes entreprises tierces, dont chacune pourrait avoir des normes de qualité différentes en matière de développement d'un code sécurisé. Par conséquent, la probabilité que des vulnérabilités en matière de sécurité soient présentes dans le logiciel est élevée et représente un risque pour la sécurité du véhicule. En théorie, étant donné qu'il existe un chemin de réseau logique, partant sans fil de l'extérieur, vers le réseau CAN interne, toute vulnérabilité qui pourrait être exploitée pour prendre le contrôle du système IVI et envoyer des trames dans le réseau CAN interne pourrait avoir de lourdes conséquences. Il se peut également que l'utilisateur navigue sur des liens dangereux qui tentent d'infecter et d'exploiter le système. Enfin, si le hacker peut accéder au système IVI et le contrôler, il peut effectuer un mouvement latéral pour se connecter au smartphone d'un utilisateur qui est connecté au système IVI, ce qui fournit ensuite une voie d'attaque vers l'appareil mobile de l'utilisateur.

5.5 Scénarios d'attaque appliqués

Dans la section suivante, des scénarios d'attaque appliqués sont décrits par l'étudiant en stage de l'Université Howest qui a préparé et exécuté les attaques. Des séquences des attaques opérées peuvent être visionnées dans la vidéo.

5.5.1 Attaque « rolljam »

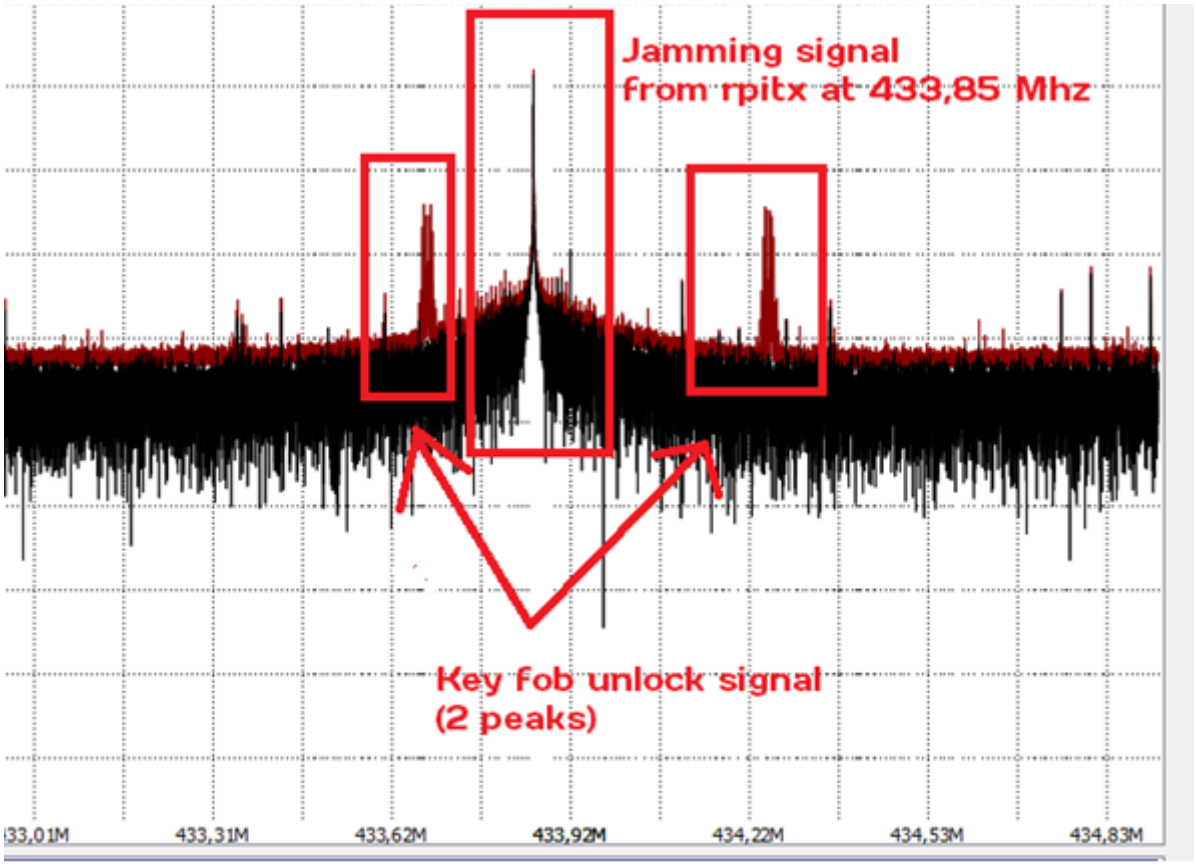
Pour l'attaque où je suis en mesure de déverrouiller la porte en captant un signal de déverrouillage inutilisé sur la fréquence radio, j'ai dû brouiller le signal tout en enregistrant et en lisant le signal de déverrouillage. Pour ce faire, j'ai utilisé un Raspberry Pi3 B+, un petit ordinateur monocarte réputé bon marché, de conception modulaire et ouverte, qui coûte environ 35 $. Je l'ai combiné au logiciel open source RpiTX pour les capacités de radiofréquence et à un câble fixé à l'une des broches pour faire office d'antenne.



Ensuite, pour lire et enregistrer le signal, j'ai utilisé un HackRF One, un émetteur-récepteur semi-duplex SDR à large bande de 330 $. Cela signifie qu'il peut envoyer et recevoir des signaux radio, mais pas les deux en même temps. Il faut donc recevoir puis envoyer le signal très vite. Voilà pourquoi on utilise le Raspberry Pi en combinaison avec le HackRF One. C'est aussi un puissant outil pour les professionnels de la sécurité, car il est capable de travailler sur une gamme de fréquences de 1 MHz à 6 GHz tandis que le matériel est également un projet open source.



Lors d'une attaque « rolljam », on tente essentiellement de contourner le système de codes roulants où la télécommande et la voiture avancent tous deux dans une séquence de codes utilisés pour vérifier l'authenticité. Nous allons tenter d'attaquer cette contre-mesure. La voiture qui reçoit les signaux de radiofréquence possède une fenêtre de réception, une plage de fréquences. Cela signifie que l'on peut bloquer sur une fréquence proche, mais pas au-dessus de la fréquence de la voiture. Si on devait bloquer directement au-dessus du signal de déverrouillage, on ne serait pas en mesure de l'enregistrer. Lors de mes tests, je devais tout d'abord trouver la bonne fréquence radio utilisée par la télécommande. En lisant et en utilisant des analyseurs de spectre, j'ai pu localiser la fréquence aux alentours des 434 MHz. J'ai toutefois été surpris de voir une chose à laquelle je ne m'attendais pas.



En utilisant la télécommande pour déverrouiller la porte, au lieu de voir un pic sur le spectrogramme, il y en avait deux ! J'étais alors pratiquement certain qu'il s'agissait d'un autre mécanisme et d'une autre contre-mesure, une longueur d'avance sur les hackers qui tentent des attaques « rolljam ». Je n'ai pas pu comprendre comment cela fonctionne exactement, mais je suppose qu'un certain algorithme ou une certaine fonction mathématique intervient dans le décodage du signal de la combinaison de pics. Presque toutes mes tentatives de brouillage ont alors été vaines. J'étais particulièrement surpris que mon attaque, sur une contre-mesure, était déjà devancée par une autre contre-mesure. Cela illustre parfaitement le jeu du chat et de la souris des hackers et des professionnels de la sécurité qui doivent toujours garder une longueur d'avance les uns sur les autres.

5.5.2 Attaque d'infodivertissement

Pour l'attaque suivante, j'ai effectué une attaque d'infodivertissement. On tente en l'occurrence de trouver des faiblesses dans le système d'infodivertissement. En général, ces systèmes fonctionnent à peu près comme des ordinateurs et des systèmes d'exploitation normaux, car ils fonctionnent essentiellement sous Linux ou Android.

Puisque l'accent est mis sur les attaques sans fil, j'ai immédiatement commencé par la phase de reconnaissance. Ici, on tente de recueillir le plus d'informations possible sur un système cible. J'ai cherché des interfaces ouvertes et j'ai pris les empreintes digitales de l'appareil pour comprendre le système d'exploitation qu'utilise le système d'infodivertissement.

Le système d'infodivertissement utilise le wifi pour communiquer avec le monde extérieur et d'autres appareils, ce qui signifie que l'on peut écouter et communiquer avec l'appareil en utilisant un autre appareil compatible wifi, comme un adaptateur wifi. J'ai également décidé d'utiliser un adaptateur compatible avec mode moniteur. Cela signifie qu'il accepte tous les paquets wifi transmis, car bien souvent, les adaptateurs normaux n'acceptent que les données qui leur sont destinées en ignorant les autres. En toute connaissance de cause, j'ai donc choisi l'adaptateur wifi TP-LINK TL-WN722N compatible avec moniteur, qui coûte environ 15 $.



Une autre surprise m'attendait : après avoir soigneusement pris les empreintes digitales du système, il s'est avéré que l'infodivertissement utilise Alpine Linux ! Une distribution Linux orientée sécurité. Et par défaut, Alpine Linux ne laisse aucune interface ouverte vers le monde extérieur, ce qui nous foudroie sur place pour les étapes ultérieures. Il n'accepte que les signaux qu'il s'attend à recevoir.

Il est à noter qu'il n'est pas impossible de le pirater, mais étant donné que les fabricants s'attendent à ce qu'il soit la cible des hackers, il doit évidemment être bien sécurisé. De plus, même si je pouvais compromettre le système, je devrais lancer d'autres attaques et veiller plutôt à entrer dans l'électronique sensible de la voiture. Voilà pourquoi j'ai décidé de mettre cette attaque de côté et de continuer avec les deux autres.

5.5.3 Attaque OBD-II

L'attaque OBD-II repose sur la connexion du hacker au port OBD. Et pour en faire une attaque sans fil, un dongle sans fil peut être attaché, qui peut communiquer directement avec le bus CAN tout en étant commandé à distance. Le dongle se place de diverses façons, par exemple par le conducteur pour passer en revue l'état de l'électronique de la voiture sur son smartphone, mais il pourrait également être combiné avec l'attaque « rolljam » pour déverrouiller la porte et placer l'appareil à l'insu du conducteur. Du fait que le port OBD est plutôt bien caché de la vue du conducteur, il est difficile de le remarquer.

J'ai utilisé l'outil macchina P1 pour mener cette attaque. Il s'agit d'un ordinateur Linux complet doté d'un connecteur OBD-II, capable de lire et d'écrire des messages CAN. De plus, il a un beagle de poche attaché pour permettre des capacités wifi. Il coûte 150 $.



Après avoir configuré la distribution Debian Linux du beagleboard, on peut s'y connecter. On peut ensuite placer l'outil dans le port OBD-II de la voiture et attendre que toutes les lumières bleues s'allument, ce qui signifie que la séquence de démarrage a bien été effectuée. On peut ouvrir un terminal SSH et écrire des commandes.

En général, la voiture aura deux interfaces CAN virtuelles, à savoir CAN0 et CAN1. Les deux utilisent un certain débit en BAUDS et comme chaque voiture est différente, il faut trouver la bonne. Après quelques essais et erreurs, j'ai pu découvrir (pour Volvo v40) que le débit en bauds de CAN0 est de 500 K et que celui de CAN1 est de 125 K. On définit le débit en bauds correct pour écouter et commencer à lire ce qui se passe à l'intérieur du bus CAN.

```
debian@beaglebone: ~
debian@beaglebone:~$ candump -cae can1,0:0,#FFFFFFFF
  can1  050   [8]  A8 00 00 00 00 53 50 88   '.....SP.'
  can1  2C0   [8]  A0 00 00 00 09 02 64 90   '......d.'
  can1  504   [8]  04 01 00 00 03 00 00 00   '........'
  can1  0F0   [8]  2F 00 00 35 0A 02 64 90   '/..5..d.'
  can1  505   [8]  05 01 00 00 03 00 00 00   '........'
  can1  050   [8]  A8 00 00 00 00 53 50 88   '.....SP.'
  can1  020   [8]  00 80 31 B0 2F 22 E2 C0   '..1./"..'
  can1  025   [8]  30 00 00 00 04 00 00 00   '0.......'
  can1  501   [8]  01 01 00 00 00 00 00 00   '........'
  can1  060   [8]  40 04 00 7F 00 00 00 00   '@.......'
  can1  080   [8]  81 D1 00 00 00 00 00 12   '........'
  can1  0F0   [8]  2F 00 00 35 0A 02 64 90   '/..5..d.'
  can1  07A   [8]  0C 00 00 60 00 80 80 00   '...`....'
  can1  050   [8]  A8 00 00 00 00 51 D0 88   '.....Q..'
  can1  0D5   [8]  60 00 00 01 02 03 00 00   '`.......'
  can1  010   [8]  00 00 00 00 08 00 04 00   '........'
  can1  0B0   [8]  00 00 00 00 00 00 00 00   '........'
  can1  2D4   [8]  00 00 00 00 00 00 00 00   '........'
  can1  020   [8]  00 00 31 B0 2F 22 E2 C0   '..1./"..'
  can1  0D0   [8]  00 00 00 00 00 00 00 00   '........'
  can1  104   [8]  04 00 40 00 00 00 00 01   '..@.....'
```

C'est alors que l'on est immédiatement inondé de milliers de messages CAN circulant dans le bus CAN, sans savoir ce que les données signifient pour beaucoup de ces messages. Cela veut dire que l'on doit passer beaucoup de temps à l'ingénierie inverse et au décodage du contenu en forçant une certaine action, comme l'ouverture de la porte, à la lecture et la sauvegarde des messages pour ensuite comparer et déterminer quel message signifie quoi.



Après beaucoup de temps passé par les messages poubelle du CAN, j'ai pu comprendre qu'en fait, il n'y a pas qu'un seul message responsable de quelque chose, mais grosso modo une séquence de messages. On peut ensuite prendre cette séquence et la renvoyer dans le bus CAN pour que d'autres composants électroniques la reprennent. De cette façon, j'ai pu usurper une séquence de déverrouillage des portes, ce qui a poussé tous les autres composants électroniques du véhicule à croire que la porte était bien ouverte, en l'affichant même sur le tableau de bord.

Cependant, j'ai également remarqué que ces messages utilisent un certain mécanisme à usage unique ou basé sur le temps pour empêcher que le message soit envoyé constamment. Cela signifie qu'une fois qu'une séquence est utilisée, elle ne fonctionne plus la plupart du temps. Voilà pourquoi il faut obtenir un nouveau signal de la voiture en forçant une action ou éventuellement une voiture simulée avec les mêmes paramètres. Non seulement on peut lire et suivre chaque mouvement et chaque changement de la voiture, mais maintenant, on peut aussi injecter des séquences de messages conçus pour pousser la voiture et son électronique critique à d'éventuelles commandes dangereuses ultérieures.

5.5.4 Attaque TPMS

La plupart des voitures modernes disposent d'un ensemble de capteurs à l'intérieur des pneus qui mesure la pression et envoie des informations au conducteur et à d'autres appareils électroniques. Puisque la roue est une pièce mobile, les capteurs doivent recourir à la radiofréquence pour transmettre des valeurs.

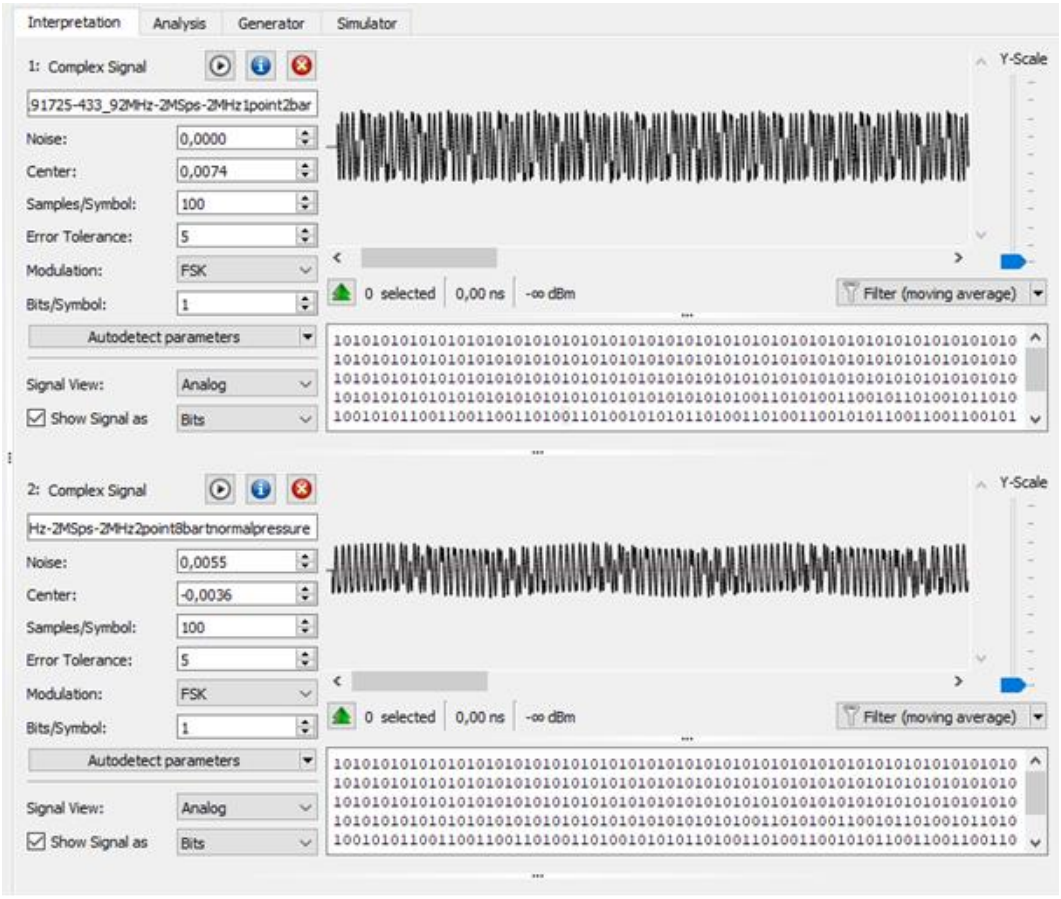
C'est là que l'attaque TPMS entre en jeu. On tente alors d'envoyer un faux signal contenant une valeur de pression fausse, inférieure à la pression autorisée pour conduire un véhicule en toute sécurité, afin de pousser la voiture à croire qu'un pneu s'est soudainement dégonflé, sans que ce soit le cas. Ici, j'ai utilisé le HackRF One, décrit précédemment, avec un système Jansite TPMS.



Pour commencer, il faut trouver la fréquence à laquelle ces appareils fonctionnent. En utilisant le HackRf One et un analyseur de spectre, j'attendrais qu'un signal soit transmis. Aussi étrange que cela puisse paraître, rien ne s'est passé dans un premier temps. On pourrait penser qu'il transmettrait périodiquement des valeurs, mais il s'avère que ce n'est pas une bonne idée du fait que la plupart du temps la voiture est immobile et qu'il est inutile de transmettre constamment des valeurs.

Les capteurs sont conçus pour n'envoyer un signal qu'en cas de changement de valeur. Puisque je ne veux pas dégonfler les pneus de la voiture, je les ai fixés à un vélo pour gonfler et dégonfler facilement le pneu et déclencher le signal à envoyer. Une fois de plus, la fréquence radio utilisée est en l'occurrence de 434 MHz.

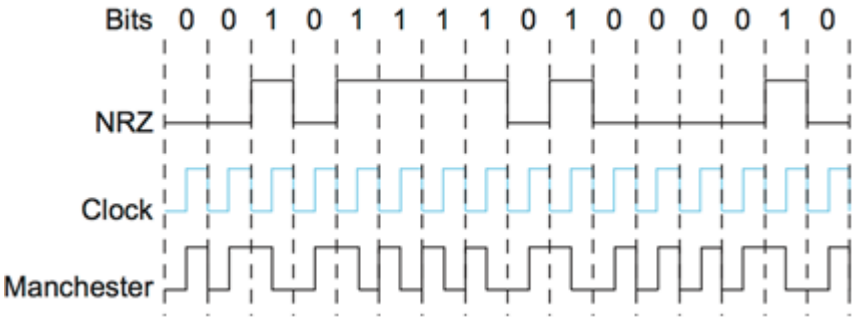
J'ai prélevé deux échantillons différents des capteurs qui se déclenchent, l'un à la pression normale, soit 2,8 bars, et l'autre à la pression « pneu dégonflé », soit 1,2 bar.



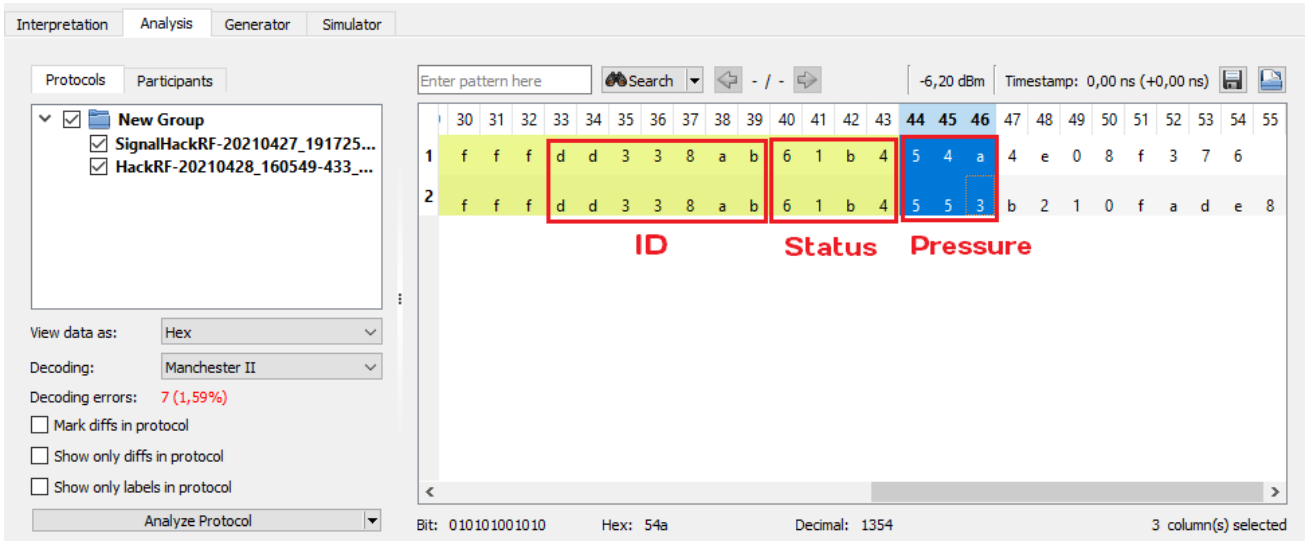
Puisque le signal utilise la radiofréquence, il faut tout d'abord convertir en binaire. On obtient quelque chose du genre :

10101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
10101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
10101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
10101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
01101001100101011001100110010110011001011001011010100101010101100101011010101001011010011010001101001000000000

Maintenant, il nous faut trouver le codage correct de ces données. En y regardant de plus près, on remarque qu'il y a souvent 2 fois 0 ou 2 fois 1, jamais 3 fois 0 ou 1. Cela indique très probablement un codage Manchester. Il est utilisé pour l'autosynchronisation de signaux sans composants CC.



Maintenant que l'on sait que l'on a affaire à un binaire Manchester, on peut décoder les valeurs en hexadécimal. Dans cette forme, on peut disséquer et tenter de comprendre à quoi pourrait ressembler l'en-tête. Pour faciliter l'ingénierie inverse, on peut enregistrer deux signaux avec un changement minimal, comme une baisse de seulement 0,1 bar, et comparer les signaux. L'ID du système TPMS restera le même (chaque TPMS a un ID unique différent pour empêcher la voiture voisine de recevoir vos valeurs). Ensuite, il faut les messages d'état et la lecture de la pression réelle. Des données utiles peuvent être extraites de ces messages pour être analysées et pour envoyer les faux signaux que nous avons créés pour tromper le système.



Le danger est en l'occurrence que l'on peut tracer un véhicule en fonction de son identifiant TPMS unique à partir d'une distance relativement moyenne sur les fréquences radio, lire l'état et la pression des pneus de la voiture. En parallèle, on peut également envoyer des signaux contenant une valeur de basse pression pour tromper la voiture et lui faire croire qu'elle a un pneu dégonflé, ce qui pourrait induire l'arrêt de la voiture voire l'impossibilité de démarrer le moteur.

6. Tentatives antérieures connues

L'analyse des tentatives d'attaques décrites ci-dessous a été effectuée sur la base des informations disponibles dans la presse ainsi que dans des publications professionnelles, des présentations lors d'événements officiels et des documents universitaires.

WHITE HAT					
Nom	**Année**	**Interaction utilisateur**	**Vecteur d'attaque**	**Point faible**	**Description**
Chevrolet Malibu	2011	Oui	Radio	Bluetooth	Après avoir eu accès à un périphérique « passerelle » (réseau CAN basse vitesse), le hacker a pu manipuler les freins en reprogrammant le périphérique dans un réseau CAN haute vitesse. Le téléphone synchrone était déjà utilisé.
Chevrolet Malibu (deuxième tentative)	2011	Non	Télématique	Connexion mobile	Les hackers ont composé le numéro de téléphone de l'unité et communiquent avec son modem sans interaction avec le conducteur. L'unité télématique était déjà sur un CAN haute vitesse. Ils ont donc eu accès aux freins.
Jeep Cherokee	2015	Non	Unité principale	Vulnérabilité accessible via Internet (mots de passe faibles du constructeur)	Étant en mesure d'exécuter leur code sur l'unité principale, les hackers ont reprogrammé un autre processeur qui avait accès au réseau CAN. Ils ont ainsi pu contrôler la direction, les freins et l'accélérateur. La connexion cellulaire d'Uconnect permet également à quiconque connaît l'adresse IP de la voiture d'y accéder de n'importe où.
Tesla S	2016	Oui	CID	Ancienne version de navigateur web	Il a fallu une proximité physique en obligeant l'utilisateur à visiter un site web malveillant ou quand il a rejoint un réseau wifi ouvert. Connaissant le point faible, les hackers ont reprogrammé le périphérique de la passerelle (connecté à CID via Ethernet) et ont pu envoyer des messages CAN et activer les freins.
Tesla S (deuxième tentative)	2016	Oui	CID	Ancienne version de navigateur web	Une fois que Tesla a amélioré le code sur le périphérique de la passerelle, les hackers étaient toujours en mesure de le contourner et de le reprogrammer.
BMW i3	2018	Non	Télématique	Connexion mobile	La télématique était séparée du CAN haute vitesse par un dispositif de passerelle et les hackers n'ont pas été en mesure de le contourner complètement. Ils ont toutefois pu envoyer des messages de diagnostic CAN via la passerelle à un CAN haute vitesse, ce qui leur a théoriquement

					permis de reprogrammer les ECU. Alors que l'utilisateur utilisait l'adaptateur OBD vers Ethernet ou Bluetooth, le signal sans fil de l'adaptateur en a permis le piratage. La voiture s'est alors connectée à la station de base mobile des hackers.
Ford Escape	2013	Hacker à l'intérieur du véhicule	N/A	N/A	N/A
Toyota Prius	2013	Hacker à l'intérieur du véhicule	N/A	N/A	N/A
Système sans clé pour Audi, BMW, DS3, Ford, Land Rover, Mercedes-Benz	2019	Données manquantes	Télécommande	N/A	Les chercheurs ont testé sept modèles de voiture différents, tous équipés d'une technologie d'entrée et de démarrage sans clé, et ont pu y entrer en quelques secondes.
Ford Focus	2020	Hacker à l'intérieur du véhicule	Unité principale	Wifi	À l'aide d'un connecteur OBD-II et d'un ordinateur portable, les chercheurs ont contrôlé les freins, modifié la vitesse de la voiture, accédé au système d'infodivertissement et bien plus encore.
Forward-looking Threat Research (FTR) & Politecnico di Milano	2017	Données manquantes	CAN	toute vulnérabilité exploitable à distance (par ex. infodivertissement)	Attaque qui désactive un dispositif (par ex. un airbag, des capteurs de stationnement, des systèmes de sécurité actifs) connecté au réseau de dispositifs de la voiture d'une manière invisible pour les mécanismes de sécurité de pointe. *Non rattachée à un fournisseur donné*
Flotte de véhicules Tesla	2020	Non	Télématique	Mécanisme côté serveur	Un chercheur a exploité une vulnérabilité dans le mécanisme côté serveur de Tesla et a pu accéder au serveur de « commande et contrôle ». Ce qui a permis de prendre le contrôle de n'importe quel véhicule de la flotte.

BLACK HAT					
Nom	**Année**	**Interaction utilisateur**	**Vecteur d'attaque**	**Point faible**	**Description**
Attaque de flotte (Philippines, Maroc, Inde, Afrique du Sud)	2019	Non	Application de traçage	Mots de passe faibles dans l'application de traçage de flotte	Sur certaines voitures, le logiciel (gestion de flotte) a la capacité de couper à distance les moteurs des véhicules à l'arrêt ou qui roulent à 20 km/h ou moins (le hacker ne l'a pas fait, il a seulement récupéré les données de l'application).
Camions NL & BE	2019	Données manquantes	Tachygraphes	N/A	Piratage des compteurs de temps et de vitesse des camions

7. Contre-mesures

L'architecture de sécurité des systèmes automobiles qui devient la norme depuis quelques années est une classification hiérarchique de 4 niveaux présentée sous le prisme de la sécurité. Pour chacun de ces niveaux de sécurité, des contre-mesures générales existantes sont déjà appliquées.

Sécurité de niveau 1 (matériel de communication externe)

communique avec le monde extérieur. Composé d'équipements embarqués pour communiquer avec des réseaux sans fil et des systèmes véhicule-à-véhicule/véhicule-à-infrastructure. Ce niveau comprend l'authentification et le contrôle d'accès sur les messages sans fil pour confirmer que le véhicule communique avec des systèmes externes autorisés et approuvés, tout en bloquant la communication avec d'autres systèmes externes. Les canaux de communication établis avec des systèmes externes devraient théoriquement être cryptés afin d'empêcher l'écoute ou l'injection de messages malveillants.

Sécurité du niveau 2 (passerelle automobile)

contrôle tous les systèmes de la voiture connectée. Constitué d'une passerelle automobile qui échange des messages entre le réseau embarqué et des dispositifs externes de niveau 1. À ce niveau, un filtrage est appliqué pour s'assurer que seuls les messages autorisés peuvent circuler entre les systèmes externes et le réseau embarqué. Il y a parfois une gestion des clés utilisées par les ECU pour le cryptage et l'authentification. Et détection d'anomalies de sécurité dans les messages échangés à l'intérieur du véhicule.

Sécurité de niveau 3 (réseaux embarqués)

est le réseau embarqué qui échange des messages entre les ECU. Elle peut être divisée en réseaux en fonction des applications et des rôles de l'ECU, comme une télématique pour la navigation du véhicule, la commande des freins et une unité pour le verrouillage des portes. Elle utilise le plus souvent le protocole CAN de communication embarqué.

Nous pouvons en l'occurrence trouver des contre-mesures qui comprennent la détection d'effraction en détectant quand des messages transmis entre les ECU ont été modifiés et en effectuant un cryptage pour empêcher l'écoute clandestine.

Sécurité de niveau 4 (matériel (ECU, etc.))

commande chaque composant individuel du véhicule, comme le moteur, les freins et le verrouillage des portes. Elle se compose d'ECU et d'autres composants qui exécutent une foule de fonctions. Ce niveau comprend l'utilisation de méthodes de conception et de programmation sécurisées pour éviter les erreurs humaines et les vulnérabilités dans les programmes qui fonctionne sur l'ECU, et un contrôle de démarrage du système sécurisé pour vérifier si le micrologiciel et le système d'exploitation n'ont pas été trafiqués lors du démarrage.

Outre les contre-mesures existantes, plusieurs autres solutions technologiques peuvent être appliquées en plus des contre-mesures existantes :

- **Segmentation du réseau** – un mécanisme de protection simple pour réduire la congestion du trafic sur les réseaux de la voiture, limiter les défaillances et améliorer la sécurité en général sépare les réseaux.
- **Systèmes de détection d'intrusion** - implémentés sur des systèmes critiques pour la sécurité qui nécessitent un traitement en temps réel.

- **Chiffrement de l'échange d'informations** – s'assurer que les informations échangées utilisent les derniers algorithmes de chiffrement afin qu'elles restent indéchiffrables pour les hackers.

- **Codes roulants basés sur le temps** – applicable en particulier à des systèmes comme le code roulant. Il permet de prévenir les attaques « rolljam » en introduisant un système de communication bidirectionnel basé sur le temps où la télécommande et la voiture restent synchronisées en échangeant des messages temporels. Puisque les hackers n'utiliseront pas immédiatement le signal capté et attendront le moment opportun, le message temporel dans le signal restera inchangé et la voiture aura un temps différent, se désynchronisant et refusant l'entrée.

- **Fermeture des ports et interfaces ouverts inutilement** - pour une communication fluide, ces ports doivent être ouverts, ce qui est normal. Cependant, quand les ports sont inutilement laissés ouverts, souvent oubliés ou laissés en raison d'un codage paresseux, cela devient dangereux. Il est également possible que les services utilisant le port soient mal configurés, non protégés ou vulnérables aux exploits.

8. Recommandations

Selon les spécialistes en cybersécurité de l'industrie automobile, à l'avenir, l'attention des hackers se portera de plus en plus vers les voitures et les attaques malveillantes intentionnelles augmenteront de façon exponentielle. Il ne s'agit plus de savoir *si*, mais *quand*, les menaces à la cybersécurité commenceront à avoir un impact sur notre vie quotidienne. La question que nous devrions nous poser en ce qui concerne la cybersécurité dans l'industrie automobile n'est pas *si nous arrivons trop tard*, mais plutôt *si nous pouvons être assez rapides* pour suivre le rythme effréné du développement technologique. En parallèle de l'augmentation du nombre de véhicules connectés, on s'attend à une augmentation des vulnérabilités. Nous proposons 5 domaines d'intervention majeurs sur lesquels les autorités doivent concentrer leurs efforts.

CYBERSÉCURITÉ DÈS LA CONCEPTION

La contre-mesure la plus importante est d'empêcher que des problèmes ne se posent : la sécurité dès la conception. Le véhicule doit être sécurisé tout au long de son cycle de vie, pendant les phases de développement, de production et de postproduction. Cela doit devenir une norme d'or non seulement pour le véhicule, mais aussi pour les produits et les réglages faisant appel aux technologies TIC. L'ensemble de la chaîne d'approvisionnement automobile contribue à la sécurité du véhicule, de sorte que des pratiques de sécurité rigoureuses doivent être appliquées à toutes ses étapes. Pour ce faire, toutes les entités doivent être à la fois incitatives et poussées vers les nouvelles meilleures pratiques.

Les solutions de cybersécurité à plusieurs niveaux devraient être une approche par défaut. Des audits indépendants pourraient également aider à veiller à ce que les solutions appliquées par les parties soient à jour et conformes aux réglementations les plus récentes. La réception par type des véhicules ne devrait être effectuée qu'au moyen d'une évaluation rigoureuse de la sécurité, selon une méthodologie indépendante des constructeurs mêmes.

Les entreprises et les institutions ne peuvent résolument plus saper la question de la cybersécurité. Selon une enquête récente menée par EY auprès de 1 300 professionnels dans le domaine de la cybersécurité, 65 % des entreprises considèrent que des mesures de cybersécurité ne doivent être mises en œuvre qu'après la survenue d'une attaque. Réagir aux menaces n'est plus une option. Il nous faut anticiper.

NORMES ET RÉGLEMENTATIONS

La publication des deux nouvelles prescriptions en matière de cybersécurité automobile prévues par les normes CSMS et SUMS du WP.29 des Nations-Unies et la norme ISO/SAE 21434 a constitué un pas important vers l'augmentation du nombre de véhicules automobiles. L'application de nouvelles normes et réglementations ne devrait pas être seulement suggérée, mais exigée par les institutions compétentes parmi les OEM, les fournisseurs de composants, les développeurs de logiciels et les fournisseurs de solutions de mobilité.

Les autorités devraient aider la CEE-ONU, l'ENISA, la Commission européenne et d'autres institutions compétentes à élaborer de nouvelles réglementations et normes à appliquer dans ce secteur. La cybersécurité étant un domaine relativement nouveau, les réglementations traditionnelles en matière de sécurité, qui s'appliquaient auparavant au secteur automobile, ne suffisent plus. Une plus grande normalisation est nécessaire, mais nous devons éviter de compliquer de façon excessive le processus compte tenu de la complexité de la chaîne d'approvisionnement automobile. Chaque couche de la chaîne d'approvisionnement automobile est confrontée à ses propres défis, qui requièrent des méthodes spécifiques à chaque couche et qui devraient être prises en compte dans la normalisation future. En outre, il convient d'éviter de centraliser l'écosystème de cybersécurité dans le cadre de normalisation afin de ne pas créer de points d'échec uniques.

SOCIÉTÉ CYBERSENSIBILISÉE

La grande majorité (environ 80 %) des attaques menées au cours des dix dernières années se sont faites à distance, donc bien plus difficiles à tracer, menaçant potentiellement plusieurs véhicules simultanément. Les attaques à distance peuvent causer des dommages bien plus graves et requièrent une attention particulière de la part des autorités, mais aussi des citoyens, car elles peuvent passer inaperçues.

Afin de sécuriser l'écosystème automobile, il nous faut encourager l'éducation dans le domaine de la cybersécurité et déployer tous les efforts nécessaires pour sensibiliser les citoyens à l'importance de sécuriser tous les appareils connectés. Pour l'instant, la négligence à cet égard constitue la plus grande menace. Les applications mobiles étaient le troisième vecteur d'attaque le plus fréquemment utilisé de 2010 à 2020, représentant près de 10 % de l'ensemble des incidents. De plus en plus de voitures sont connectées aux téléphones directement via les applications mobiles dédiées (par ex. l'app ConnectedDrive de BMW), ce qui présente un risque important en cas de compromission du téléphone mobile. Il est de la plus haute importance de veiller à ce que tous les dispositifs se connectant au véhicule soient à jour et correctement sécurisés à tout moment. Cela ne peut se faire à un niveau élevé. Voilà pourquoi il est crucial de veiller à une meilleure sensibilisation.

PRÉPARER LE MARCHÉ

Selon Forbes, pratiquement tous les constructeurs automobiles ont déjà été victimes d'une cyberattaque, ce qui indique que les cybermenaces font peu à peu partie du paysage tant au niveau de l'individu qu'au niveau du constructeur. Compte tenu du niveau élevé d'interconnexion de la chaîne d'approvisionnement automobile, toute interférence avec la sécurité dans cette chaîne d'approvisionnement présente un risque substantiel.

En outre, tant les OEM que les gouvernements ont été exposés à des cybermenaces (par ex. le département des transports du Texas a été attaqué par un logiciel rançonneur en mai 2020, mais le problème ne se limite pas aux États-Unis : des organisations gouvernementales du monde entier ont été ciblées, comme l'autorité nationale des autoroutes en Inde, le portail de services NTSA du Kenya et la flotte de transport militaire d'Allemagne). Les mesures de sécurisation de l'écosystème se font de plus en plus pressantes et nécessitent des actions immédiates, car de tels incidents auront des conséquences à grande échelle sur le développement futur de la cybercriminalité. Une attention de plus en plus grande est accordée aux incidents, ce qui entraînera probablement de nouvelles attaques plus graves, car l'exposition médiatique et le « *prestige* » qui en résulte inciteront les hackers « black hats ».

En supposant que les OEM continueront d'utiliser et de développer davantage les options de mise à niveau logicielle des véhicules, un marché massif émergera, tant sur le web légal que sur le dark web. Cela élargira davantage la portée de l'écosystème, déjà très complexe.

En matière de cybersécurité des véhicules connectés, il convient de prendre en compte l'ensemble de l'écosystème, à savoir les OEM et l'ensemble de la chaîne d'approvisionnement, la gestion du parc automobile, les services de covoiturage, les services de location de voitures, les services de concession et après-vente, les assurances ainsi que l'évolution rapide de la technologie, en particulier les applications dans les *villes intelligentes* qui, grâce à leur solution de gestion du trafic, etc., peuvent créer un vecteur d'attaque aux conséquences potentiellement très lourdes.

Du point de vue législatif, tous les aspects liés à la responsabilité, aux questions de garantie en cas d'attaque devraient être inclus dans la future législation afin d'éviter la création de zones grises et la diffusion de la responsabilité en cas de dommages.

VULNÉRABILITÉ ≠ RISQUE OPÉRATIONNEL

Bien qu'il ressorte de diverses études qu'un grand nombre de vulnérabilités peuvent être exploitées, il faut déployer d'énormes efforts pour envoyer des signaux corrects aux ECU concernés et provoquer de graves menaces pour la sécurité, mais cela reste possible. En raison d'un très grand nombre de surfaces et de vecteurs d'attaque, de la longue durée de vie du véhicule et de l'absence de cadre pour assurer sa protection tout au long de sa vie, ainsi que de l'exposition générale à la négligence en matière de sécurité (en particulier par les individus en ce qui concerne les dispositifs qui peuvent permettre la passerelle dans les systèmes du véhicule), des risques sont présents et ils ne peuvent être ignorés.

Par le passé, l'intérêt d'attaquer des entités appartenant à l'industrie automobile était moindre, mais compte tenu de l'exposition accrue des médias et des incitations financières, nous pouvons nous attendre à l'émergence de méthodes plus sophistiquées. Les vulnérabilités constamment découvertes par les « white hats » dans les programmes de primes aux bogues donnent une idée de l'étendue du problème. Les hackers « white hats » peuvent ne pas avoir d'intention malveillante, mais les vulnérabilités qu'ils mettent à jour sont toujours inquiétantes, car elles exposent des vecteurs d'attaque potentiels. Il convient de noter que dans la catégorie des « white hats », on trouve également des hackers « grey hats » qui ne piratent pas pour des raisons malveillantes, mais pour accéder à des services contournant le paywall, ce qui a un impact direct sur les revenus des OEM et des prestataires de services.

9. Glossaire

TPM	Trusted Platform Module (also known as ISO/IEC 11889): international standard for a secure cryptoprocessor, a dedicated microcontroller (chip) designed to secure hardware through integrated cryptographic keys.
TCP	Transmission Control Protocol: provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network.
UDP	User Datagram Protocol: a simple message-oriented transport layer protocol, which is suitable for purposes where error checking and correction are either not necessary or are performed in the application. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for packets delayed due to retransmission, which may not be an option in a real-time system.
ECU	Electronic Control Unit: any embedded system in automotive electronics that controls one or more of the electrical systems or subsystems in a vehicle.
CID	Central Information Display
Telematics	A method of monitoring a vehicle. By combining a GPS system with on-board diagnostics it's possible to record – and map – exactly where a car is and how fast it's traveling, and cross reference that with how a car is behaving internally.
Head unit	Automotive infotainment component providing a unified hardware interface for the system, including screens, buttons and system controls for numerous integrated information and entertainment functions.
Cellular connection	Connection established through a mobile network-communication network where the last link is wireless.
CAN bus	Controller Area Network- standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer (message-based protocol).
High speed CAN network	Implemented with two wires and allow communication at transfer rates up to 1 mbit/s.
Low speed CAN network	Implemented with two wires, can communicate with devices at rates up to 125 kbit/s, and offer transceivers with fault-tolerant capabilities.
Kernel	A computer program at the core of a computer's operating system with complete control over everything in the system.
802.1x	IEEE Standard for port-based Network Access Control (authentification)
OBD	On-Board Diagnostics
TCU	Transmission Control Unit
PII	Personally Identifiable Information
OTA	Over the Air Updates
RSU	Road Side Unit
LIN	Local Interconnect Network
MOST	Media Oriented Systems Transport -> high speed multimedia network
FlexRay	Automotive network communications protocol: designed to be faster and more reliable than CAN and TTP, but it is also more expensive
DSRC	Dedicated Short Range Communications
C-V2X	Cellular vehicle-to-everything
NFC	Near-field communication
IVI	In-Vehicle Infotainment
GNSS	Global Navigation Satellite System
TARA	Threat Assessment and Remediation Analysis
OEM	Original equipment manufacturer
TSP	Telematics Service Providers

VSOC	Vehicle Security Operation Center



Institut Vias

Chaussée de Haecht 1405
1130 Bruxelles

+32 2 244 15 11

info@vias.be

www.vias.be