État de l'art associé au projet tuteuré

Voitures autonomes et cyber-sécurité :
Un défi majeur pour la pérennité de cette technologie

Quels sont les enjeux de la cyber-sécurité pour les voitures autonomes ?

Puech Camille, c_puech@etud.insa-toulouse.fr

Taillardat Elie, taillard@etud.insa-toulouse.fr

Olsen Anja, olsen@etud.insa-toulouse.fr

Année d'étude : 4 AE-SE

Tuteur : Tounsi Patrick

Résumé du projet

Sommaire

1. Introduction

Le domaine de l'automobile a aujourd'hui dépassé le monde de la mécanique. Les voitures possèdent désormais un grand nombre de composants électroniques communicants. Les voitures modernes peuvent contenir jusqu'à 50 unités de contrôle électroniques (ECU) reliées entre elles [1]. La sécurité générale du véhicule s'appuie sur ces ECUs. Une fois que des composants électroniques sont rajoutés à un système, la question de robustesse et de sûreté du code se pose. Quand de plus l'intégrité d'êtres humains est en jeu, il est d'autant plus important de s'interroger.

L'automatisation des véhicules a été une des applications majeures dans le domaine des systèmes de transport intelligents (ITS – *Intelligent Transportation Systems*) depuis les années 1980. Pourtant, ce ne sont que ces dernières années où cette idée se rapproche vraiment de sa réalisation. De nombreux essais concernant cette technologie ont vu la lumière du jour, notamment par la légalisation des véhicules autonomes en Californie [2]. Il y a actuellement 50 sociétés qui sont en train de mener des tests de 300 voitures autonomes sur les routes californiennes. Les essais sont suivis attentivement par des sociétés comme General Motors, Google, Tesla, Waymo et Uber qui développent tous des séries de véhicules autonomes dans l'espoir de pouvoir se passer de conducteur humain.

Les voitures autonomes éliminent la problématique du conducteur préoccupé, fatigué ou ivre et peuvent potentiellement réduire les 1,3 millions d'accidents mortels qui ont lieu dans le monde chaque année [3]. Les défenseurs des voitures autonomes affirment que ces voitures vont révolutionner le secteur du transport, faire gagner du temps et augmenter la mobilité d'un grand nombre de personnes tels que les personnes âgées et handicapées [4].

Cependant, le sujet du véhicule autonome révèle une problématique non négligeable sur la sécurité informatique. Ils fonctionnent sur le concept des véhicules « connectés », appelés « cooperative ITS » en anglais [5]. Cela est soit basé sur la communication entre véhicules (V2V) soit sur la communication entre les véhicules et l'infrastructure (V2I/I2V). Ces connections font partis des facteurs qui permettent les cyber-attaques.

Dans le présent rapport, nous allons développer l'importance de la sécurité informatique dans les véhicules autonomes, la sécurité des données liées à l'utilisateur. Nous allons aussi mettre en évidence les vulnérabilités connues sur les voitures autonomes et les projets mis en place les sécuriser au travers des différentes entreprises qui sont entrées en concurrence dans le domaine.

2. À quels types de cyber-menaces les voitures autonomes font-elles face ?

2.1. Hack des logiciels de commande embarqués

La technologie des voitures autonomes peut être un outil très commode, utilisé avec bienveillance. Pourtant, elle représente aussi un réel danger pour la société et l'ordre public si elle est utilisée avec malveillance.

2.1.1. La voiture autonome : un outil pour les terroristes

Pour donner un exemple, Mikko Hypponen, analyste de sécurité finlandais, proclame qu'il existe des preuves concrètes qui montrent que Daesh développent des voitures autonomes pour remplacer les kamikazes [6]. Dans une vidéo faite par le groupe terroriste lui-même et diffusée par Sky News [7], on peut également voir des terroristes en train de faire des modifications sur une voiture pour la rendre autonome ou pilotable à distance. Pour passer inaperçu, ils mettent un mannequin dans le siège du conducteur. Le mannequin reproduit alors la chaleur émise par un être humain pour tromper un éventuel capteur infra-rouge.

On comprend donc que les terroristes ont bien réfléchi aux mesures de sécurité qui pourraient potentiellement être mises en place pour détecter des voitures sans conducteur, et donc une certaine anticipation des différents plans d'action envisageables. Ils montrent aussi tous les explosifs qu'ils peuvent mettre dans la voiture. Le projet est prévu pour faire des attaques terroristes dans des grandes villes européennes pour toucher une large foule publique. Cela réduit le besoin de kamikazes volontaires. À l'heure actuelle, le seul groupe terroriste que l'on connaisse qui développe des voitures est le groupe Daesh.

Les voitures autonomes permettraient en outre à un terroriste de tirer par exemple sur une foule sans devoir se préoccuper de conduire, ce qui faciliterait alors l'attaque terroriste.

2.1.2. Les dangers d'une voiture autonome soumise au contrôle d'un hackeur

Un autre danger est la possibilité pour les hackeurs d'entrer dans le système de navigation du véhicule et de faire sortir la voiture de la voie, tourner, et par conséquent de faire des armes mortelles de ces véhicules, que ce soit avec ou sans conducteur. Les voitures d'aujourd'hui étant suffisamment connectées pour être piratées, elles présentent un danger pour l'ordre public. Les voitures autonomes sont bien évidemment d'autant plus connectées que les voitures normales, et sont donc encore plus susceptibles.

Il y a quelques années, l'idée qu'un hackeur soit capable d'arrêter une voiture était considérée paranoïde et technophobe. Aujourd'hui, il existe plusieurs exemples de voitures qui ont été « hackées » par des chercheurs en sécurité, tels que la Jeep qui a été piratée par les deux ingénieurs Charlie Miller et Chris Valasek en 2015 [8]. Les deux chercheurs ont contacté le

magazine technologique américain « Wired » pour faire une démonstration des pouvoirs d'un hackeurs sur une voiture. Ce n'était pas la première fois que ces deux chercheurs ont compromis une voiture. Ils ont aussi fait une démonstration en 2013 sur un Ford Escape et un Toyota Prius [9], la différence étant qu'en 2013, il fallait une connexion physique avec la voiture. Les chercheurs étaient alors dans la voiture, et ont pu par exemple désactiver les freins, fausser les valeurs du compteur de vitesse ou encore klaxonner.

En 2015, ils ont ensuite réussi à pirater une voiture de la marque Jeep à une distance de 16 kilomètres sans aucune connexion physique avec la voiture. Ils ont pu contrôler la climatisation, le volant, les freins et même stopper le moteur. Ils ont pu observer les coordonnées du GPS, mesurer la vitesse de la voiture à distance et changer sa trajectoire. On reviendra sur ce qui a permis de faire cette attaque dans la prochaine partie de ce rapport, à savoir : *« Quels aspects technologiques vulnérables permettent de telles attaques »*. On retient donc qu'il existe un véritable risque pour qu'une voiture comprenant de nombreux systèmes informatiques soit piratée. Ces deux chercheurs ont partagé leurs résultats avec Chrysler, le fabricant de la voiture, mais il est très probable qu'il existe d'autres hackeurs qui essaient de trouver des vulnérabilités dans les systèmes des voitures, toutefois sans partager leurs résultats.

Ces exemples ont forcé les fabricateurs de voitures à prendre conscience des vulnérabilités informatiques de ces dernières [10], autonomes ou pas. Pourtant, les fabricants ont tendance à refuser d'admettre le danger que représente ces failles. La société Chrysler n'a donné aucune reconnaissance aux deux chercheurs qui ont découvert les défaillances, et ont juste déployé une mise à jour pour la voiture en question [8].

2.2. Sécurité des données personnelles de l'utilisateur

2.2.1. Les données potentiellement accessibles dans une voiture connectée

Les deux chercheurs Miller et Valasek ont montré que les vulnérabilités dans les voitures connectées connues à ce jour représentent un véritable risque d'accident pour le conducteur et pour l'environnement. Leurs résultats font aussi remonter le problème de sécurité des données personnelles de l'utilisateur. La problématique concerne le piratage éventuel d'une voiture, mais également le cas où le fournisseur de la voiture se sert des données récupérées.

Dorothy J. Clancy, chercheuse à l'Université Santa Clara School of Law, dit dans son article de recherche [11] que la sécurité des données personnelles dans les véhicules autonomes ne serait pas un problème tant que des personnes ne sont pas impliquées. Cependant, comme il y aura forcément des personnes dans au moins certaines des voitures, la question se pose pour le transport individuel sur des chemin publiques.

Les voitures connectées possèdent potentiellement des données sur l'utilisateur telles que la vitesse à laquelle la voiture roule, les destinations fréquentées, l'adresse de l'utilisateur, la musique préférée de l'utilisateur, et bien plus. Si on considère que le téléphone portable de l'utilisateur est connecté à la voiture, ce qui est très souvent le cas, et si on considère également

que la voiture est piratée par quelqu'un qui maîtrise le hacking, on peut imaginer le hackeur ayant accès à presque la totalité des données personnelles de la victime. Les données peuvent servir pour des objectifs de marketing ciblé par exemple, quand une société est capable d'analyser où la personne vit, travaille, fait ses courses et où elle mange par exemple. [12][13]

2.2.2. Le cas de Cambridge Analytica

Aujourd'hui, il y a une quantité énorme de données qui circule sur Internet. Cela n'est pas uniquement une mauvaise chose, mais fait partie du progrès technologique. Ce progrès a de nombreux avantages pour la technologie de bien-être, notamment dans le secteur des objets connectés. En même temps, cette quantité importante de données peut également être utilisée avec « malveillance ». Plusieurs exemples ont pu récemment illustrer ces propos, notamment avec le cas Facebook et Cambridge Analytica.

Cambridge Analytica a développé une application pour téléphone portable en 2015 qui s'appelle *This Is Your Digital Life* et qui a été téléchargée par plus de 270 000 personnes [14]. Cette application permet à l'utilisateur de répondre à plusieurs questions. Néanmoins, ce que les utilisateurs de cette appli ignoraient, c'est que toutes leurs données Facebook ont été partagées avec Cambridge Analytica. Les données étant alors des données de type nom, âge, liste d'amis, mais aussi tous les pages « likées », date d'anniversaire et nom de la ville dans laquelle la personne vit, et parfois même dans certains cas des messages privés. De plus, cette récupération de données s'étendait également aux « amis » de la personne en question. Ce qui augmente le nombre de personnes concernées de 270 000 à potentiellement 87 millions. Facebook proclame que le nombre le plus réaliste est environ 40 millions – mais ce chiffre reste beaucoup trop élevé. La question est alors ce qu'a pu faire Cambridge Analytica de toutes ces données : ils ont traité les données collectées afin de pouvoir faire « de l'analyse psycographique » pour « mieux connaître le groupe cible ». Ils proclament avoir contribué au Brexit et également à la victoire de Donald Trump aux élections présidentielles aux Etats-Unis, et même éventuellement à l'issue des élections au Kenya, tout en ayant ciblé les campagnes politiques [15][16].

Le PDG de Cambridge Analytica, Alexander Nix, a en 2016 prétendu que sa société détenait entre 4 et 5 milles données sur chaque adulte aux Etats-Unis, et qu'ils sont donc capables de « modéliser » chacun d'entre eux, soit environ 230 millions personnes [17].

La collecte des données peut alors avoir un impact sur des principes fondamentaux de notre société tels que la démocratie. Il suffit d'avoir avoir une vingtaine de « likes » sur Facebook pour pouvoir déterminer pour quel parti politique une personne vote. C'est donc alors un problème majeur dont il faut tenir compte.

Ceci étant dit, la majorité de la population est au courant que par exemple Facebook a des quantités énormes d'informations sur nous, sans toutefois être inquiétée. Pour certains, Facebook est un outil incontournable du quotidien. Une partie importante des échanges d'informations sur nos activités quotidiennes se font sur Facebook. Comme ce ne sont pas des

données que l'on considère très personnelles, on ne fait pas trop attention. Pourtant, ces données peuvent avoir une grande utilité pour les grands pouvoirs dans notre société.

Le règlement européen 2016/679 du 27 avril 2016, aussi dit « règlement général sur la protection des données » ou RGPD (GDPR en anglais) précise que la protection des données personnelles nécessite de prendre des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » (article 32) [18].

Après le scandale de Cambridge Analytica, le PDG de Facebook, Mark Zuckerberg a dû s'expliquer auprès d'un tribunal. Sous les yeux, il avait des notes écrites. Ces notes étant pris en photo par des journalistes, on a pu voir la phrase suivant écrite : « *Don't say we already do what GDPR requires* » [19]. Facebook a donc indirectement avoué de ne pas respecter le règlement européen qui va être directement applicable dans l'ensemble des 28 États membres de l'Union européenne à compter du 25 mai 2018.

En résumé, les données de caractère personnel se sont montrées très utiles pour des objectifs psycho-sociaux, et cela s'applique aussi aux données concernant les voitures, telles que les endroits fréquentés par l'utilisateur, sa station radio préférée, si la personne roule vite ou lentement, etc. On peut aussi envisager que des données comme celles-là soient utilisées pour d'autres motifs. Par exemple, certains disent que l'on pourrait utiliser des méthodes d'analyse de données pour déterminer le prix d'une assurance pour une personne particulière ou pour savoir si une personne pourra se voir accorder un emprunt ou pas.

1.2.3 L'importance de la protection des données biométriques

Avec l'avancement de la technologie, des données biométriques sont utilisées pour par exemple déverrouiller des téléphones, des voitures ou bien autre chose. Une donnée biométrique est une caractéristique physique ou biologique permettant d'identifier une personne (ADN, contour de la main, empreintes numériques). C'est par exemple envisageable d'utiliser la reconnaissance vocale pour piloter une voiture. Dans l'avenir, l'utilisation des données biométriques sera de plus en plus présente. L'avantage d'un mot de passe est que l'on peut le changer en cas de problème. Cela est moins évident avec une donnée biométrique. D'où l'importance énorme de protéger telles données contre des vols. Il existe aujourd'hui des lois aux Etats-Unis, où les essais des voitures autonomes sont mis en œuvre, prenant certains de ces dangers en compte. Cependant, comme c'est un domaine en plein essor, tous les aspects ne sont pas entièrement analysés, maîtrisés, traités [13].

3. Quels aspects technologiques vulnérables permettent de telles attaques ?

Ce n'est pas forcément évident de pointer précisément les problèmes de sécurité dans les voitures autonomes, mais nous allons nous appuyer sur les rapports de recherche écrits par des chercheurs reconnus dans ce domaine.

3.1. Les vulnérabilités découvertes dans le Jeep Cherokee de 2014

Valasek et Miller ont après leur piratage du Jeep en 2015, sorti un document de recherche sur les vulnérabilités trouvées [20]. Cela nous donne une idée sur les points faibles des voitures actuelles. Les deux chercheurs ont dit que le piratage était possible grâce au fait que Chrysler, le fabricant de Jeep, essaie de « transformer la voiture moderne en smartphone », comme la plupart des fabricants [8].

3.1.1. L'architecture du système : des bus CAN

Les chercheurs ont trouvé le choix d'architecture dans le 2014 Jeep Cherokee intéressant, surtout à cause du fait que la radio soit connectée aux deux bus CAN qui sont implémentés dans le véhicule. Les deux bus CAN étant : le CAN-C, celui de haute vitesse qui relie le moteur, les freins, les airbags etc., et le CAN-IHS, pour les tâches moins critiques telles que la climatisation.

Un bus CAN (Controller Area Network) est un système d'émission (broadcast) de message qui fixe la fréquence maximum d'émission à 1 mégabit par seconde. Contrairement à d'autres types de réseaux tels que l'USB ou l'Ethernet, le CAN n'envoie pas des grands paquets d'un nœud A à un nœud B sous la supervision d'un maître de bus. Dans un réseau CAN, plusieurs messages courts comme la température ou les tr/min sont « broadcastés » au réseau entier, ce qui assure la régularité d'information dans chaque nœud du système. [21]

En compromettant la radio, ils ont soupçonné une faille à exploiter et ainsi se voir capable d'envoyer des messages aux ECUs (Electronic Control Unit) sur les deux bus. Plus tard dans leurs recherches, ils ont trouvé que le fait de compromettre la radio ne donne pas directement accès aux bus CAN, et il a fallu aller plus loin. Par contre, ils ont découvert qu'il n'y a aucune restriction sur le réseau CAN. Ils proposent de séparer le CAN-C de l'unité radio pour mieux sécuriser. Cela veut dire que si l'on est capable d'envoyer des messages depuis la radio, on peut contrôler la voiture à distance en envoyant des messages à tous les ECUs dans le réseau. Un tableau dans le rapport de Miller et Valasek nous montre tous les unités accessibles depuis le réseau CAN-C auquel est connectée la radio. On y trouve par exemple le module ABS (Anti-Lock Brakes), le module ACC (Adaptive Cruise Control), le module EPB (Electronic Parking Brake), le module PAM (Park Assist), le module SCM (Steering Control) et encore bien d'autres.

3.1.2. Le système de la radio

La radio dans le Jeep reçoit beaucoup de signaux différents : bien évidemment les signaux audios, mais aussi des signaux comportant des informations telles que des données GPS, du radio AM/FM, et des signaux satellites. La plupart du temps, ces signaux ne sont pas vraiment décryptés par le système, et ne représentent donc pas de vulnérabilités exploitables. Une exception trouvée par les chercheurs Miller et Valasec [20] est le cas du système radio qui envoie des données *avec* les signaux FM. Typiquement pour afficher le nom de la chanson sur l'écran ou afficher le nom de la station radio. Dans ce cas, les données doivent être traitées, et cela représente un point faible qui peut être exploité par des hackeurs à distance.

3.1.3. Les fonctionnalités cyber-physiques

Le 2014 Jeep Cherokee possède plusieurs systèmes de conduite assistée, tels que le module ACC (Adaptive Cruise Control) et le module PAM (Park Assist). De telles fonctionnalités ont déjà été exploitées dans des attaques pour contrôler des aspects physiques de voitures [1][20]. Pendant que ces fonctionnalités augmentent le niveau de sécurité du conducteur et de l'environnement, elles présentent aussi une opportunité pour un hackeur de prendre le contrôle du véhicule.

3.1.4. Les connexions cellulaires

Certains automobiles sont capables de créer un point Wi-Fi à partir de la connexion à Internet si cette dernière est cellulaire. Cette connexion est vulnérable aux attaques, et des techniques de piratage de telles connexions sont connues depuis plusieurs années [22]. Plusieurs automobiles ont aussi des radios cellulaires qui permettent au véhicule de se connecter à un réseau cellulaire. La connexion cellulaire Uconnect dans le 2014 Jeep Cherokee est possible à cause d'un seul élément vulnérable qui permet à n'importe qui, si il connaît l'adresse IP de la voiture, de se connecter. Le système utilisé est Uconnect 8.1AN/RA4 fabriqué par Harman Kardon. Ce système est aussi présent dans des véhicules de Chrysler, Dodge, Jeep, Ram, Ferraris et potentiellement d'autres encore. Le système Uconnect fonctionne sur le système d'exploitation QNX sur un STM32 ARM processeur. Ce système d'exploitation peut être installé à partir d'une machine virtuelle sur un ordinateur qui pourra s'en servir pour commander la voiture à distance sur le réseau CAN comme décrit précédemment [20].

3.2. D'autres vulnérabilités connues

Dans le rapport « Cyber Threats Facing Autonomous and Connected Vehicles » de 2017 [23] écrit par des chercheurs de l'Université de Huddersfield en Grande-Bretage, les auteurs ont exposé quelques grandes lignes de vulnérabilités connues dans le domaine de la voiture autonome. Ils ont souligné quelques absences dans la recherche actuelle qui peuvent potentiellement causer des problèmes de sécurité.

En effet, ils écrivent qu'il y a eu à plusieurs reprises des exemples démontrant que l'environnement de la voiture peut être utilisé pour compromettre le bon fonctionnement de

celle-ci, et que des techniques d'atténuation de risque tels que des caméras ou des capteurs supplémentaires sont souvent utilisés. Par contre, la recherche ne montre pas encore quelle solution est la meilleure ; est-ce qu'il faut opter pour plusieurs caméras de la même technologie, ou alors pour plusieurs capteurs de technologies différentes ?

Ils écrivent de même que depuis le cas du 2014 Jeep Cherokee, il y a eu plusieurs autres cas compromettant les ECU à travers les entrées des capteurs ou d'autres ECUs. Dans le cas général, le bus CAN nécessite une connexion physique avec le véhicule. C'est donc une faille normalement inaccessible pour le hackeur. Le 2014 Jeep Cherokee était donc mal conçu dans la perspective de sécurité.

De plus, il n'est pas du tout clair à l'heure actuelle quelles données seront générées et sauvegardées dans le véhicule. Le propriétaire de ces données est de même mal identifié, tout comme la manière de les protéger, et quelles lois peuvent agir sur ce domaine.

Un autre point à mettre en évidence sur les véhicules autonomes aujourd'hui est qu'il n'y a presque pas eu de recherches sur la manière dont réagissent les voitures à une cyber-attaque : pourront-elles rentrer dans un « mode sécurité » ? En outre, si la voiture détecte qu'elle est compromise, doit-elle passee la commande au conducteur ?

Le niveau de connectivité des véhicules automatisés augmente, et la dépendance sur l'intégration des fonctionnalités technologiques fait de même. L'utilisateur souhaite avoir accès à un navigateur web, une boîte mail, et une connexion Bluetooth. La voiture est donc susceptible à des attaques de type phishing ou Denial of Service (DoS) ou Distributed Denial of Service (DDoS). Il n'est pas connu à l'heure actuelle si les mesures de sécurité dans une voiture autonome sont suffisants contre ce type d'attaque, qui permettent aujourd'hui de compromettre des ordinateurs partout dans le monde.

Les auteurs du rapport écrivent qu'aujourd'hui, les fabricants utilisent des technologies (hardware et software) qui ont des vulnérabilités de sécurité inhérentes. Ceci est dû à l'objectif trop orienté « fonctionnalité » plutôt que « sécurité » dans la chaîne de production. À causes des contraintes de temps et des clauses contractuelles, les fournisseurs favorisent la productivité plutôt que la qualité.

Un dernier point sur lequel il serait important d'insister, est que toutes les vulnérabilités identifiées par des spécialistes en sécurité tels que Valasec et Miller, sont justement trouvées par des experts. Comme les voitures autonomes deviennent de plus en plus courantes et connectées, il y aura certainement des attaques par des personnes ayant la même expertise. On ne sait donc pas quelle forme les attaques auront, et il sera donc difficile de les anticiper.

4. Quels moyens les entreprises mettent-elles en œuvre pour faire face à ces failles technologiques ?

La sécurité 'software' ou cyber-sécurité est l'enjeu majeur des entreprises qui veulent commercialiser leur modèle de voiture autonome dans les années à venir. Ce défi de grande ampleur est commun à l'ensemble de ce secteur technologique. Ainsi, le futur de la voiture « driverless » est totalement dépendant de la résolution de tous les problèmes de sécurité potentiels liés au hack des logiciels embarqués et à la prise de contrôle à distance du véhicule.

3.1 Plusieurs solutions technologiques entreprises

3.1.1. Intégrer la sécurité dans la conception même du véhicule

Une des solutions pour protéger les voitures autonomes de ces menaces grandissantes serait d'intégrer la totalité du modèle de sécurité lors de la conception initiale de la voiture. En effet, cela permettrait d'éviter tout conflit, erreur ou mauvaise configuration entre chaque composant individuel présents dans la voiture. Les différentes communications (type Wifi, Bluetooth, Radio Fréquence, etc.) entre ces équipements, et qui sont les points d'entrée des hackeurs comme nous avons pu le voir précédemment, seraient alors moindres l'ensemble du système est uniforme et designé comme une seule entité [24].

Dans le cas contraire, les tests doivent être encore plus pertinents ; on parle alors de tests de pénétration ou réelles attaques perpétrées sur le système réel, mais contrôlées. Les tests et essais sont donc très nombreux, variés, et poussés afin de palier à tout potentiel bug, faille dans le code qui permettrait l'entrée malveillante d'un pirate informatique [25].

Enfin, des changements fondamentaux dans l'architecture du système intégrant la sécurité seront nécessaires. C'est le cas avec le « codesigning », qui permettra aux logiciels et fonctionnalités embarquées de n'exécuter que le code signé et auquel on a accordé un certificat de confiance unique. Pour le moment, uniquement Tesla a annoncé publiquement son utilisation dans la conception de son modèle de voiture autonome [26].

3.1.2. Des softwares développés pour déceler de potentielles failles

BlackBerry, ancien géant dans les téléphones mobiles, pivote et concentre maintenant ses efforts et ses moyens dans le développement de softwares destinés à la cyber-sécurité pour protéger les voitures autonomes.

La compagnie canadienne a récemment lancé un nouveau software, nommé Jarvis, capable d'identifier des vulnérabilités dans les programmes utilisés dans les véhicules autonomes. Cet outil sera dans un premier temps destiné au secteur automobile, pour prévenir des cyber-attaques de la part de hackers malveillants, mais il aura par la suite une potentielle utilisation dans les secteurs industriels et de la santé.

John Chen, PDG de BlackBerry, a en outre déclaré lors du lancement de ce nouveau software : « Les véhicules autonomes demandent l'un des softwares les plus complexes jamais développé », ce qui appui l'importante complexité tournant autour de la sécurité des voitures autonomes.

3.2. S'appuyer sur la communication et l'expertise de hackeurs

3.2.1. Changer l'approche de la voiture autonome

Un des points primordiaux sera de partager au public et aux consommateurs une vision des véhicules autonomes très différente de celle que l'on peut avoir aujourd'hui, et d'effacer les craintes suscitées à leur encontre. En effet, « les voitures autonomes seraient moins vulnérables aux attaques que des voitures conduites par des humains », selon Craig Smith, chercheur en matière de sécurité et hackeur de voiture autonome [27].

Jonathan Brossard, hackeur « white hat » et directeur de Toucan Systems, pense personnellement que la pauvreté en termes de sécurité des réseaux de communication entraînera quoi qu'il arrive des failles dans tout système. Cependant, les développeurs de ces voitures autonomes sont les plus puissants du monde technologique, comme Google qui possède selon lui la meilleure équipe de sécurité informatique du monde [28].

3.2.2. Se servir des hackeurs comme « outil » d'amélioration

Les entreprises engagées dans la course aux premières voitures autonomes qui seront proposées sur le marché vont devoir faire appel à l'expertise de professionnels dans le domaine : les hackeurs eux-mêmes.

Craig Smith, cité quelques lignes plus haut, gère aussi l'évènement « Car Hacking Village », la plus grande convention de « hacking » du monde, à Las Vegas. On peut y voir les différents hacks qui ont pu avoir lieu sur des voitures autonomes, notamment la Jeep Cherokee contrôlée à distance. La perception des hackeurs par les producteurs automobiles est dans un premier temps très négative, les pirates informatiques étant considérés comme des criminels essayant de détruire le produit sur lequel ils ont déployé tant de moyen. Mais cette attitude a récemment changé, avec une vision des hackeurs comme potentiels alliés, ou du moins partenaires indirects permettant d'avancer dans la guerre contre le cybercrime. Il est en effet préférable que des hackeurs « white hat » décèlent ces bugs, plutôt que des hackeurs « black hat » ayant de mauvaises intentions [27].

Un autre exemple serait celui de Charlie Miller and Chris Valasek, qui avaient piraté à distance la Jeep via sa connexion internet, et qui sont devenus deux chercheurs travaillant pour Uber sur leur prototype de voiture autonome, afin d'aider la startup à sécuriser leur modèle

contre tout type d'attaque qu'ils ont prouvé possible auparavant. Miller a par ailleurs récemment quitté Uber, car il souhaitait qu'il existe une communication plus ouverte et libre dans les échanges à l'intérieur et entre les industries... [26]

3.3. Faire coopérer les entreprises dans ce domaine

3.3.1. Un apport mutuel nécessaire entre les équipes de développement

Le plus grand challenge pour ces entreprises sera inévitablement de travailler de manière plus fréquente « main dans la main » pour pallier aux problèmes communs qu'engendrent cette technologie. Cependant la très forte rivalité existante dans ce secteur à tous les niveaux entraîne une réticence des entreprises à partager leurs différentes avancées dans la gestion des cyber menaces [24][26].

3.3.2. Des modèles structurés et unifiés sur lesquels s'appuyer

La communication est de plus un élément majeur pour appréhender les problèmes liés à la cyber-sécurité, que ce soit entre les gouvernements ou société spécialisées et les entreprises, ou entre les entreprises elle-même et les consommateurs.

Le gouvernement britannique a de ce fait mis en place tout un document listant de nombreuses directives concernant ce secteur : « Principles of cyber security for connected and automated vehicles, *Overview of the principles for obtaining good cyber security within the automotive sector* ». Elle privilégie la coopération des entreprises afin de créer des structures logicielles solides de véhicule dont la sécurité ne sera pas menacée par les « hackers » [29].

De même, la « Société des Ingénieurs de l'Automobile » aux États-Unis a introduit son propre set de lignes directrices pour démontrer de quelle manière la cyber-sécurité peut être appréhendée dans la conception d'une voiture autonome [24].

4. Conclusion

Par conséquent, comme nous avons pu l'observer au travers de cette recherche bibliographique, les voitures autonomes sont vulnérables aux cyber-attaques. Cela pose des problèmes au niveau de la sécurité physique des passagers et de l'environnement. C'est donc une problématique très importante pour toutes les entreprises qui souhaitent se lancer dans le marché des voitures autonomes.

Il y a également une problématique de sécurité de données personnelles qui se relève pertinente dans le domaine. Les énormes quantités de données qui circulent peuvent servir à faire du marketing ciblé ou même pour influencer la population concernant des choix politiques importants, ce qui concerne donc des fonctionnalités fondamentales de notre société.

Les voitures autonomes sont cependant bel et bien le futur de l'automobile en perspective, et il faut donc que la cyber-sécurité soit un domaine de priorité pour ce progrès technologique. Le véhicule autonome a de nombreux avantages, même si la cyber-sécurité est aujourd'hui un enjeu majeur pour cette technologie.

5. Bibliographie :

[1] C. Miller et C. Valasek, « Adventures in Automotive Networks and Control Units ». 2013.

[2] A. J. Hawkins, « California green lights fully driverless cars for testing on public roads », *The Verge*, 26-févr-2018. [En ligne]. Disponible sur: https://www.theverge.com/2018/2/26/17054000/self-driving-car-california-dmv-regulations. [Consulté le: 20-mai-2018].

[3] K. Naughton, « Just How Safe Is Driverless Car Technology, Really? », *Bloomberg.com*, 27-mars-2018.

[4] S. Edelstein, « Toyota announces artificial intelligence research collaboration with MIT and Stanford », *Digital Trends*, 04-sept-2015. [En ligne]. Disponible sur: https://www.digitaltrends.com/cars/toyota-to-collaborate-with-mit-and-stanford-on-artificial-intelligence-research/. [Consulté le: 20-mai-2018].

[5] J. Petit et S. E. Shladover, « Potential Cyberattacks on Automated Vehicles », *IEEE Trans. Intell. Transp. Syst.*, juin 2014.

[6] S. Edelstein, « ISIS progressing with work on driverless car bombs, security analyst says », *Digital Trends*, 16-mars-2016. [En ligne]. Disponible sur: https://www.digitaltrends.com/cars/isis-autonomous-car-bombs/. [Consulté le: 20-mai-2018].

[7] R. Glon, « ISIS is testing a deadly remote-controlled car bomb that fools infrared sensors », *Digital Trends*, 13-janv-2016. [En ligne]. Disponible sur: https://www.digitaltrends.com/cars/isis-remote-contrlled-car-bomb-news-demonstration/. [Consulté le: 20-mai-2018].

[8] A. Greenberg, « Hackers Remotely Kill a Jeep on the Highway—With Me in It », *WIRED*. [En ligne]. Disponible sur: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Consulté le: 20-mai-2018].

[9] A. Greenberg, « Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video) ». [En ligne]. Disponible sur: https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#f04e8aa228c7. [Consulté le: 20-mai-2018].

[10] Alexander Kalogianni, « Hackers wirelessly disable a Jeep Cherokee from 10 miles away with Uconnect », *Digital Trends*, 21-juill-2015. [En ligne]. Disponible sur: https://www.digitaltrends.com/cars/uconnect-hackers-jeep-cherokee/. [Consulté le: 20-mai-2018].

[11] D. J. Glancy, « Privacy in Autonomous Vehicules », *52 St. Clara Rev 1171*, nov. 2012.

[12] J. M. Such, « Privacy and Autonomous Systems », *Proc. Twenty-Sixth Int. Jt. Conf. Artif. Intell. IJCAI-17*, 2017.

[13] N. R. Fulbright, « The Privacy Implications of Autonomous Vehicles », *Data Protection Report*, 17-juill-2017. [En ligne]. Disponible sur: https://www.dataprotectionreport.com/2017/07/the-privacy-implications-of-autonomous-vehicles/. [Consulté le: 20-mai-2018].

[14] B. Chapell, « How To Check If Your Facebook Data Was Used By Cambridge Analytica », *NPR.org*, 10-avr-2018. [En ligne]. Disponible sur:

https://www.npr.org/sections/thetwo-way/2018/04/10/601163176/how-to-check-if-your-facebook-data-was-used-by-cambridge-analytica. [Consulté le: 21-mai-2018].

[15] L. L. Randeberg, B. E. Thon, M. Goodwin, et H. C. Pretorius, *Hva vet internett EGENTLIG om deg? (What does the internet REALLY know about you?)*. Oslo: Tekna, 2018.

[16] C. Cadwalladr et E. Graham-Harrison, « How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool », *The Guardian*, 17-mars-2018.

[17] T. Cheshire, « Behind the scenes at Donald Trump's UK digital war room », *Sky News*, oct. 2016.

[18] CNIL, « Sécurité : Introduction ». [En ligne]. Disponible sur: https://www.cnil.fr/fr/securite-introduction. [Consulté le: 21-mai-2018].

[19] N. Statt, « Read Mark Zuckerberg's notes from today's Facebook privacy Senate hearing », *The Verge*, 10-avr-2018. [En ligne]. Disponible sur: https://www.theverge.com/2018/4/10/17222546/facebook-mark-zuckerberg-senate-hearing-notes-cambridge-analytica-privacy. [Consulté le: 21-mai-2018].

[20] C. Miller et C. Valasek, « Remote Exploitation of an Unaltered Passenger Vehicle ». 10-août-2015.

[21] S. Corrigan, « Introduction to the Controller Area Network (CAN) ». Texas Instruments, mai-2016.

[22] INTEGRITY, « From 0-day to exploit - Buffer overflow in Belkin N750 (CVE-2014-1635) | INTEGRITY Labs », *INTEGRITY*, 06-nov-2015. [En ligne]. Disponible sur: https://labs.integrity.pt/articles/from-0-day-to-exploit-buffer-overflow-in-belkin-n750-cve-2014-1635/. [Consulté le: 21-mai-2018].

[23] S. Parkinson, P. Ward, K. Wilson, et J. Miller, « Cyber Threats Facing Autonomous and Connected Vehicules: Future Challenges », 2017.

[24] M. Cheah et S. A. Shaikh, « Here's how we can stop driverless cars from being hacked », *The Conversation*. [En ligne]. Disponible sur: http://theconversation.com/heres-how-we-can-stop-driverless-cars-from-being-hacked-82799. [Consulté le: 21-mai-2018].

[25] IT Governance, « Penetration testing from IT Governance ». [En ligne]. Disponible sur: https://www.itgovernance.co.uk/penetration-testing. [Consulté le: 21-mai-2018].

[26] A. Greenberg, « Charlie Miller on Why Self-Driving Cars Are So Hard to Secure From Hackers | WIRED », *WIRED*, avr. 2017.

[27] A. Hern, « Assume self-driving cars are a hacker's dream? Think again », *The Guardian*, 30-août-2017.

[28] G. James et Greenfield, « Can driverless cars be made safe from hackers? | Technology | The Guardian », *The Guardian*.

[29] « Principles of cyber security for connected and automated vehicles », *GOV.UK*. [En ligne]. Disponible sur: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles. [Consulté le: 21-mai-2018].