VÉHICULES AUTOMATISÉS

La cybersécurité et les véhicules automatisés

brainonboard.ca/fr

TIRF

lAu cours de la dernière décennie, d'importants progrès ont été réalisés au chapitre de la technologie et des mécanismes de sécurité des véhicules, bien que les types de technologies utilisés dans les véhicules d'aujourd'hui, à l'instar de nombreux autres appareils électroniques, présentent de nombreuses vulnérabilités en matière de cybersécurité. La conception de véhicules automatiques (VA) soulève de défis en matière de sécurité des données, puisque ces véhicules possèdent sans doute une technologie de véhicules connectés (VC) pour permettre les communications externes d'un véhicule à l'autre, et entre les véhicules et l'environnement. Cette connectivité pourrait créer de nouvelles possibilités, pour les pirates informatiques, d'accéder aux véhicules à distance et de commettre des cyberattentats. C'est donc important de prévoir des mécanismes judicieux pour atténuer ces menaces et maintenir la confiance et la perception du public à l'égard de la sécurité. Ainsi, la question de la cybersécurité doit être abordée efficacement avant le déploiement à grande échelle de ces technologies sur les voies publiques.

Cette fiche de renseignements se penche sur d'importantes questions liées à la cybersécurité de la technologie des véhicules automatisés et des véhicules connectés. Elle présente un aperçu des risques et vulnérabilités potentiels en matière de cybersécurité et décrit les façons dont les gouvernements et l'industrie peuvent travailler en collaboration pour veiller à l'atteinte des niveaux maximaux de cybersécurité afin de pouvoir déployer en toute sécurité ces véhicules sur les voies publiques.

Questions et réponses

Quelle est la différence entre la technologie des véhicules automatisés (VA) et celle des véhicules connectés (VC)?

Les technologies des VA misent sur des capteurs, des analyses informatiques et des systèmes technologiques pour exécuter certaines fonctions sans intervention humaine. Celle des VC fait appel à des réseaux sans fil pour permettre les communications d'un véhicule à l'autre, et entre les véhicules et l'environnement, mais sans l'automatisation des tâches de conduite. Bien que les VA

Votre cerveau est la caractéristique de sécurité la plus importante de votre véhicule.

n'aient pas besoin de la technologie des VC pour fonctionner, celle-ci peut faciliter certaines fonctions automatisées et est fort susceptible d'être intégrée aux véhicules offrant une automatisation conditionnelle (niveau 3) ou supérieure.[1] Par exemple, la connectivité peut permettre aux automobilistes d'accéder aux plus récentes cartes géographiques ou aux véhicules de recevoir des mises à jour opérationnelles. La technologie de VC contribue aussi à la sécurité des VA, puisque les données recueillies par les capteurs pourraient être transmises à d'autres VA à proximité pour les informer d'un problème imminent sur la route.[2]

Les VA seront-ils vulnérables aux cyberattentats?

Probablement. Les véhicules dotés d'une automatisation conditionnelle (niveau 3) ou supérieure détiendront probablement un certain degré de connectivité et devront donc accéder aux réseaux de données.[3] Bien que la connectivité permette l'utilisation des fonctionnalités désirées, elle a aussi pour effet d'accroître le nombre de points d'accès physiques pour les pirates informatiques, ce qui s'apparente aux risques associés à d'autres appareils reliés à des réseaux externes (ex. : téléphones, tablettes électroniques ou appareils ménagers intelligents). Le risque d'attentats malicieux est encore plus élevé, puisque ces véhicules seront en mesure d'accomplir des tâches de conduite sans intervention humaine. Si un pirate informatique prend en charge certaines fonctions critiques, des problèmes opérationnels pourraient survenir et mettre en danger la sécurité des occupants du véhicule et d'autres usagers de la route.[4] Selon un sondage national sur les véhicules automatisés, les vulnérabilités perçues de ces derniers en matière de cybersécurité inquiètent les gens. En effet, seulement 21 % des automobilistes sont d'accord avec l'affirmation voulant que la technologie des VA soit protégée contre les cyberattentats. Un sondage réalisé par Transports Canada a révélé des résultats comparables et aussi démontré que les craintes suscitées par la cybersécurité des VA étaient proportionnelles aux niveaux de confort des automobilistes à l'égard des véhicules automatisés.[5]

Quelles sont certaines des façons dont les VA pourraient être piratés?

Comme la technologie des VA prévoira éventuellement un certain degré de connectivité, les véhicules pourraient être vulnérables à des attentats à distance si les pirates informatiques étaient en mesure d'accéder aux réseaux de données. En théorie, ceux-ci pourraient ainsi mettre la main sur de vastes quantités de données, tels que des renseignements personnels et financiers. Ils pourraient aussi obtenir des données sur les trajets, comme les destinations fréquentes, la durée des parcours et le nombre de trajets par jour.

Ils pourraient aussi, théoriquement, troubler certaines composantes des véhicules, comme les capteurs, le radar et la navigation GPS. Il s'agit, dans ces cas, d'attentats « par brouillage » ou « par mystification ». Un attentat par brouillage survient quand les signaux émis par une composante du véhicule sont interrompus et que celui-ci ne peut ni recevoir l'information ni la transmettre. Pour sa part, un attentat par mystification survient lorsque de faux renseignements sont injectés dans le système, outrepassant le fonctionnement d'une composante du véhicule. Par exemple, les pirates informatiques pourraient brouiller les signaux GPS requis pour la navigation sécuritaire du véhicule ou injecter de faux renseignements dans le système pour faire dévier le véhicule de sa trajectoire ou l'orienter vers une nouvelle destination.[6] Les pirates informatiques pourraient aussi être en mesure d'accéder au réseau interne du véhicule[7] , qui est

Les pirates informatiques pourraient troubler certaines composantes des véhicules, comme les capteurs, le radar et la navigation GPS. Il s'agit dans ces cas d'attentats « par brouillage » ou « par mystification ».

Le téléchargement d'applications non conçues par le fabricant du véhicule pourrait aussi créer certaines vulnérabilités graves.

responsable de nombreuses fonctions essentielles à sa maîtrise (ex . : freins, direction et accélération). Après s'être infiltrés dans le réseau interne, les pirates informatiques pourraient théoriquement contrôler toutes les fonctions du véhicule.[8]

Bien que les attentats à distance soient une importante source de préoccupations en raison des possibilités de connectivité externes, les pirates informatiques pourraient aussi commettre un attentat en accédant directement au véhicule. Si un appareil infecté était branché à un port (USB, par exemple), les pirates pourraient y injecter de faux messages, contournant ainsi les fonctions automatisées et ordonnant le véhicule d'exécuter des manœuvres dangereuses.[9]

Le gouvernement fédéral, les fabricants de véhicules et d'autres parties prenantes de l'industrie considèrent la cybersécurité comme étant la principale priorité pour assurer la sécurité de la technologie des véhicules automatisés. Transports Canada a élaboré des lignes directrices, en collaboration avec des parties prenantes nationales, pour renforcer la cyberrésilience des véhicules.[10] Lire la suite ci-dessous pour plus de renseignements sur la façon dont les parties prenantes protègent les VA contre les cyberattentats.

Pourrais-je, à mon insu, télécharger un virus dans mon VA?

Peut-être. La technologie des VA exige la fréquente mise à jour des logiciels, qui fournissent des correctifs réguliers, des améliorations en matière de programmation, de nouvelles fonctionnalités et des correctifs pour les bogues. Bien que les VA soient sans doute appelés à recevoir ces mises à jour chez le concessionnaire, certains fabricants pourraient permettre à certaines d'entre elles d'être téléchargées à distance.[11] HCela dit, si la base de données du fabricant était ciblée par des pirates informatiques, ceux-ci pourraient injecter des programmes infectés dans les mises à jour régulières du système, contaminant ainsi la flotte entière.

Le téléchargement d'applications non conçues par le fabricant du véhicule pourrait aussi créer certaines vulnérabilités graves, car celles-ci pourraient offrir aux pirates informatiques une autre voie d'accès aux véhicules. Par conséquent, les fabricants de véhicules devront concilier le désire des consommateurs d'obtenir une personnalisation accrue avec la sécurité des applications issues de tiers. Par exemple, l'utilisation d'appli mobiles reliées aux réseaux sociaux et l'intégration de systèmes de paiements pourraient accroître les cybermenaces pour ces véhicules.[12]

Who would be responsible for damages in the event of a cyberattack?

Même si la technologie serait sans doute en mesure de déceler un attentat, il y aurait peu de preuves permettant d'identifier et de poursuivre le pirate informatique. De plus, on ignore si les propriétaires des véhicules seraient responsables des dommages découlant de l'attentat (ex. : réparation, extraction du maliciel ou dommages potentiels à d'autres véhicules).[13]

Quelles sont certaines des motivations des pirates informatiques?

Théoriquement, un pirate informatique pourrait exécuter un cyberattentat pour transformer en arme un véhicule ou une gamme de véhicules. Il pourrait lui être possible de créer une situation chaotique ou des embouteillages à grande échelle en mettant les véhicules hors service au sein d'un rayon donné. Les pirates informatiques motivés par le vol pourraient s'emparer de véhicules personnels ou commerciaux contre rançon. Heureusement, les recherches et attentats sur la technologie des VA sont actuellement effectués par des pirates en « chapeau blanc », soit des chercheurs qui y procèdent pour détecter les vulnérabilités et assurer la sécurité des véhicules.[14]

Quelles mesures sont-elles prises pour protéger les VA contre les cyberattentats?

Des mesures de cybersécurité avancées doivent être conçues conjointement avec les nouvelles technologies automatisées. L'approche « défense en profondeur »[15] l'une des principales dans ce domaine, pourrait offrir des mécanismes de défense à plusieurs niveaux. Ainsi, si l'un d'entre eux ne parvenait pas à déjouer un attentat, le niveau suivant interviendrait. Cela dit, le développement des protocoles de cybersécurité devra reposer sur une approche détaillée et systémique en vertu de laquelle toutes les parties prenantes collaboreraient pour concevoir des normes et des pratiques optimales visant à assurer la cybersécurité de tous les VA. Collectivement, tous les paliers de gouvernement, ainsi que les parties prenantes de l'industrie de l'automobile, ont un rôle à jouer pour optimiser les avantages en matière de sécurité de cette technologie, tout en minimisant les risques de perturbations technologiques et de conséquences négatives. Sécurité publique Canada a élaboré une stratégie nationale de cybersécurité[16], qui offre une vision et une orientation générales pour la sécurité au Canada. Tablant sur cette stratégie, Transports Canada a, en mai 2020, publié de Lignes directrices sur la cybersécurité des véhicules au des véhicules.[17] Celles-ci renferment un ensemble de principes directeurs neutres sur le plan technologique pour aider l'industrie à intégrer aux véhicules des pratiques optimales en matière de cybersécurité, et ce, pour la durée de vie entière de ces derniers. Cette approche cadre avec celle du gouvernement américain, qui a aussi élaboré des lignes directrices non obligatoires sur la cybersécurité et des pratiques optimales pour l'industrie de l'automobile.[18]

Conclusion

Au fil de l'évolution de la technologie des VA, les niveaux croissants d'automatisation donneront naissance à de nouvelles vulnérabilités en matière de cybersécurité. Les défis à ce chapitre exigeront la collaboration des gouvernements et des parties prenantes de l'industrie pour élaborer une stratégie détaillée. Celle-ci devra prévoir des normes neutres sur le plan technologique précises et des exigences réglementaires applicables à tout l'écosystème de fournisseurs responsables des divers aspects de la technologie. La stratégie de cybersécurité devra aussi être uniforme dans tous les territoires de sorte que l'industrie puise viser l'obtention d'une accréditation universelle. Par conséquent, il est essentiel que la stratégie de cybersécurité suive le rythme des progrès technologiques afin de favoriser la mise en œuvre sécuritaire de cette technologie sur nos routes.

Références

Chong, J. (2016). Véhicules autonomes et connectés : état d'avancement de la technologie et principaux enjeux stratégiques pour les pouvoirs publics au Canada. Bibliothèque du Parlement, Publication no 2016-98-F

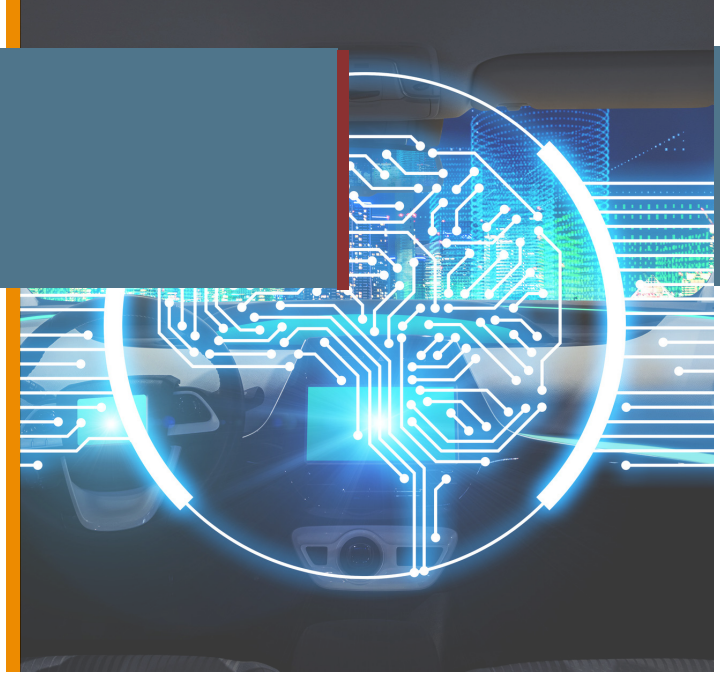
Cutean, A. (2017). Véhicules autonomes et l'avenir de l'emploi au Canada. Conseil des technologies de l'information et des communications (CITC). Ottawa, Canada.

Deloitte (2019). Cybersécurité pour les véhicules connectés et autonomes. Tiré de **https://www2.deloitte.com/ca/fr/pages/risk/articles/cybersecurite-vehicules-connectes-autonomes.html**

Deloitte (2017). Securing the future of mobility. Tiré de : **https://www2.deloitte.com/content/dam/Deloitte/be/Documents/strategy/Securing%20The%20Future%20Of%20Mobility.pdf**

Georgia Institute of Technology (2019). "Hackers could use connected cars to gridlock whole cities." ScienceDaily. Retrieved from: **www.sciencedaily.com/releases/2019/07/190729111337.htm>**.

Kakareka, A. (2013). What Is Vulnerability Assessment?. In Managing Information Security (pp. 201-221). Syngress.



Meryem, S., & Mazri, T. (2019, October). Security study and challenges of connected autonomous vehicles. In Proceedings of the 4th International Conference on Smart City Applications (pp. 1-4).

Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015, 91.

National Highway Traffic Safety Administration (2016, October). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333). Washington, DC: Author.

National Highway Traffic Safety Administration (2013). Preliminary statement of policy concerning automated vehicles. U.S. Department of Transportation.

Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE transactions on intelligent transportation systems*, 18(11), 2898-2915.

Sécurité publique Canada (2018). Stratégie nationale de cybersécurité. Cat. no : PS4-239/2018F ISBN : 978-0-660- 26553-7

RAND Corporation (2017). When Autonomous Vehicles Are Hacked, Who Is Liable? Retrieved from: **https://www.rand.org/pubs/research_reports/RR2654.html**

Robertson, R. D., Meister, S. R., & Vanlaar, W. G. (2016). Automated vehicles: driver knowledge, attitudes and practices. Ottawa, ON.

Transport Canada (2020) Canada's Vehicle Cyber Security Guidance. Retrieved from: **https://tc.canada.ca/sites/default/files/2020-05/cyber_guidance_en.pdf**

Transport Canada (2021) Public opinion research study: Consumer awareness of, and confidence in, automated vehicles (AVs) and advanced driver assistance systems (ADAS). #POR 046-20. Ottawa, ON.

Weimerskirch, A. (2016). Cybersecurity of Connected and Automated Vehicles. ATZelektronik worldwide, 11(3), 26-31.

Woo, S., Jo, H. J., & Lee, D. H. (2014). A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Transactions on intelligent transportation systems*, 16(2), 993-1006.

[1, 3] NHTSA 2013
[2] Chong 2016
[4, 9] Parkinson et al. 2017
[5] Robertson et al. 2016 ; Transport Canada 2021
[6] Meryem & Mazri 2019
[7] Woo et al. 2014; R
[8] Miller and Valasek (2015) ont commis, à des fins de recherche, un attentat à distance en accédant à la connexion Wi-Fi pour infecter le système multimédia d'un véhicule. En fin de compte, ils ont pu accéder au réseau interne principal du véhicule et transmettre des commandes à chaque composante de ce dernier, ce qui leur a permis de contrôler des fonctions telle que la direction, le moteur, la transmission, les freins, les essuie-glace, l'air climatisé et le verrouillage des portes (pour plus de renseignements, consultez (for more information, visit: **https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/)**.
[10, 17] Transport Canada 2020
[11] Weimerskirch 2016
[12] Cutean 2017; Deloitte 2017
[13] Parkinson et al. 2017; RAND Corporation 2017
[14] Georgia Institute of Technology 2019
[15] Kakareka 2013; Deloitte 2019
[16] Public Safety Canada 2018
[18] NHTSA 2016

Vous désirez en savoir plus?

Visitez **brainonboard.ca/fr** pour vous familiariser davantage avec les véhicules automatisés.

Fondation de recherche sur les blessures de la route

La vision de la Fondation de recherche sur les blessures de la route (FRBR) est de s'assurer que les gens qui utilisent les routes rentrent chez eux en toute sécurité chaque jour en éliminant les décès sur la route, les blessures graves et leurs coûts sociaux. La mission de la FRBR est d'être une source de connaissances pour des usagers de la route plus sécuritaires et un chef de file mondial en matière de recherche, de développement de programmes et de politiques, d'évaluation et de transfert de connaissances. La FRBR est un organisme de bienfaisance canadien enregistré qui dépend de bourses, de contrats et de dons afin d'offrir des services au public. Pour plus d'information, visitez **www.tirf.ca**.

Fondation de recherche sur les blessures de la route (FRBR)
171, rue Nepean, bureau 200, Ottawa, ON K2P 0B4
Courriel : tirf@tirf.ca ISBN : 978-1-989766-84-2

Remerciements

La production de cette feuillet d'information a été rendue possible grâce au parrainage de Desjardins et au savoir technique de Greg Overwater et Andrew McKinnon, Constructeurs mondiaux d'automobiles du Canada.

Desjardins

Constructeurs mondiaux d'automobiles du Canada

Votre cerveau est la caractéristique de sécurité la plus importante de votre véhicule.