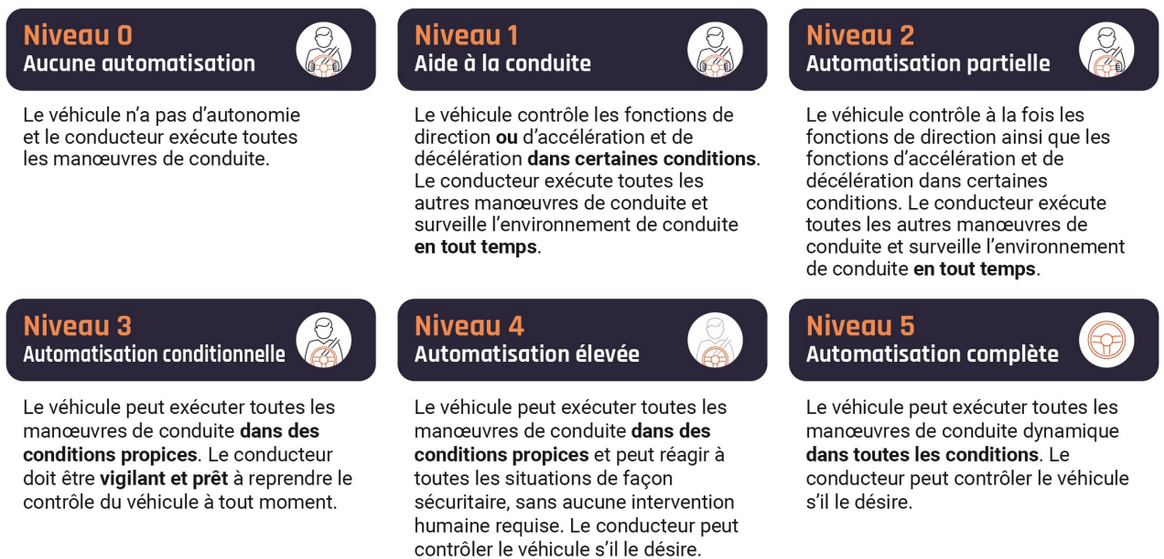
La cybersécurité des véhicules connectés et automatisés pour votre organisation

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

OCTOBRE 2022 | ITSAP.00.142

Les véhicules entièrement automatisés sont appelés à prendre de l'ampleur dans les années à venir. Entre-temps, il existe actuellement sur nos routes de nombreux véhicules partiellement automatisés et un nombre encore plus important de véhicules connectés. Les conducteurs peuvent transformer leurs déplacements en connectant leurs véhicules à des réseaux sans fil et en utilisant leurs appareils pour produire et transmettre de l'information en temps réel. Bien qu'ils offrent toute une gamme de fonctionnalités pratiques, les véhicules connectés, et dans certains cas les véhicules automatisés, peuvent exposer l'information sensible à des risques. Il est donc essentiel de comprendre les risques associés à ces véhicules et de prendre les mesures nécessaires afin de les atténuer.

Niveaux d'automatisation de la conduite



Qu'est-ce qu'un véhicule connecté et qu'est-ce qu'un véhicule automatisé?

Les véhicules connectés sont munis de différentes technologies utiles, comme les réseaux cellulaires. Cette connexion donne accès à de nombreuses fonctionnalités, par exemple le guidage de navigation, pour communiquer avec l'environnement de conduite. Ces fonctionnalités peuvent se connecter à des appareils mobiles et à des appareils de l'Internet des objets (IdO) en vue de tirer profit des applications et des services, et peuvent également se connecter à d'autres véhicules. Voici des exemples de capacités dont sont dotés les véhicules connectés :

- **Bluetooth et Wi-Fi :** Les passagers peuvent écouter de la musique, faire des appels téléphoniques ou envoyer des messages vocaux au moyen d'applications système ou de la connexion d'un téléphone intelligent. Certains véhicules permettent même de télécharger les mises à jour logicielles sur des réseaux Wi-Fi.
- **Services de localisation ou GPS :** Le suivi de l'emplacement, l'assistance routière et les services d'urgence contribuent à la sûreté et à la sécurité d'un véhicule connecté. Lors de vos déplacements, les données de localisation vous permettent de recevoir de l'information telle que des itinéraires, des restaurants, des lieux d'hébergement et plus encore.

Très prochainement, les conducteurs pourraient avoir accès à encore plus d'information sur les infrastructures et les dangers routiers environnants grâce aux technologies de communication entre véhicules (V2V) et véhicule-infrastructure (V2I).

Il existe plusieurs niveaux d'automatisation pour les véhicules, y compris les véhicules partiellement automatisés qui offrent certaines fonctionnalités d'aide à la conduite, de même que les véhicules entièrement automatisés qui ne demandent aucune intervention du conducteur et qui peuvent donc fonctionner de manière autonome. Il convient toutefois de noter que les véhicules connectés et automatisés (niveaux 3 à 5) ne sont pas encore en vente au Canada. Les chercheurs et les concepteurs sont en train de mettre à l'essai ces véhicules afin de promouvoir leur sécurité.

Les véhicules automatisés utilisent diverses technologies pour évaluer l'environnement de conduite et réaliser des tâches précises (p. ex. la direction, le freinage, l'accélération et la décélération), comme des ordinateurs, des logiciels et l'intelligence artificielle (IA). Ils emploient une gamme de capteurs pour réaliser leurs tâches :

- Les **capteurs de rendement des systèmes du véhicule** servent à optimiser le rendement sur route d'un véhicule automatisé et comprennent les capteurs de direction et de freinage. Les capteurs environnementaux, comme les capteurs de température extérieure et de pluie, ajustent le rendement du véhicule en fonction des conditions météorologiques et environnementales.
- Les **capteurs de sécurité des passagers** comprennent le capteur du poids de l'occupant, les caméras externes, les capteurs de collision ainsi que les caméras internes qui surveillent le mouvement oculaire du conducteur et la position de sa tête pour déterminer son niveau de vigilance.
- Les **capteurs de distance et de localisation** comprennent les capteurs de localisation basés sur la technologie GPS ainsi que les technologies de télémétrie qui déterminent la distance entre les objets en mesurant la réflexion des ondes radioélectriques (RADAR), des lumières laser (LiDAR) ou des ondes sonores (capteurs de stationnement ultrasoniques).

Les technologies automatisées offrent de nombreux avantages, comme les systèmes d'aide à la conduite qui peuvent réduire les incidents de la route et anticiper les situations dangereuses. Elles sont aussi particulièrement pratiques pour les personnes à mobilité réduite.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

La cybersécurité des véhicules connectés et automatisés pour votre organisation

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

OCTOBRE 2022 | ITSAP.00.142

Comment mon organisation peut-elle atténuer les risques?

Lorsque vous utilisez les fonctionnalités des véhicules connectés ou automatisés, vous exposez vos renseignements personnels et organisationnels à des risques. Les appareils connectés à votre véhicule, les connexions Wi-Fi et Bluetooth, ainsi que les applications ou les logiciels installés sur votre véhicule ou sur votre appareil peuvent tous constituer des vulnérabilités que les auteurs de menace peuvent exploiter dans le but de pirater votre appareil ou votre véhicule.

- **Exploitation des vulnérabilités logicielles et des réseaux Wi-Fi:** Les véhicules connectés et automatisés sont vulnérables aux cyberattaques ciblant les logiciels intégrés et les réseaux mobiles ou Wi-Fi. Les auteurs de menace exploitent les systèmes d'infodivertissement, les micrologiciels et les applications tierces pour mener diverses attaques. À titre d'exemple, une attaque par déni de service distribué (DDos pour Distributed Denial of Service) peut perturber les communications d'un véhicule en l'inondant de données et en interrompant ainsi ses fonctionnalités.
- **Usurpation et brouillage:** Les auteurs de menace peuvent manipuler plusieurs types de capteurs pour créer des données erronées qu'un véhicule automatisé traitera en tant que données légitimes. Au moyen d'un dispositif électronique, ils peuvent envoyer des signaux qui créent de faux obstacles (comme des voitures, des murs ou des piétons) ou transmettre de faux signaux au récepteur GPS et ainsi orienter le conducteur dans la mauvaise direction ou induire le véhicule en erreur en lui affirmant qu'il est à un autre endroit. Le brouillage des signaux entrave les communications d'un véhicule en bloquant complètement les signaux entrants, comme les signaux entre une télécommande et un véhicule. Un auteur malveillant pourrait donc avoir recours à cette technique pour tenter de voler un véhicule.

Les organisations peuvent réduire les risques liés aux véhicules connectés et automatisés en assurant une meilleure protection des données des parcs de véhicules et des appareils. Voici quelques stratégies d'atténuation:

- **Faire preuve de vigilance à bord d'un véhicule automatisé:** Les conducteurs doivent être prêts à interrompre le fonctionnement des systèmes automatisés lorsqu'une situation potentiellement dangereuse se manifeste. Ils doivent respecter les exigences relatives à la surveillance et à la vigilance requises pour chaque niveau d'automatisation de la conduite. Il pourrait s'avérer nécessaire de signaler les activités suspectes ou anormales au fabricant du véhicule ou aux autorités appropriées.
- **Mener des évaluations des vulnérabilités:** Votre organisation doit s'efforcer de détecter, de surveiller et d'analyser les menaces visant ses parcs de véhicules connectés et automatisés. Les vérifications courantes et un plan de gestion des vulnérabilités aident à protéger les actifs contre les défauts de programmation et un environnement de menace en constante évolution.
- **Prioriser la sécurité:** Assurez-vous que les logiciels et micrologiciels de vos véhicules et appareils connectés sont à jour par l'entremise des fabricants de véhicules. Mettez en œuvre des méthodes d'authentification et de contrôle d'accès pour définir les employés qui sont autorisés à accéder aux véhicules connectés ou automatisés et à les utiliser. Dans la mesure du possible, chiffrez les données recueillies par les véhicules pour protéger votre organisation et vos clients. Séparez vos véhicules connectés ou automatisés des réseaux qui contiennent de l'information sensible ou des systèmes, afin de réduire au minimum les dommages en cas de cyberattaque.
- **Désactiver la fonction Bluetooth et protéger les renseignements personnels:** La désactivation de la fonction Bluetooth sur votre véhicule et sur votre appareil connecté est une mesure importante afin de garantir que seuls les appareils de confiance sont connectés. Vous pouvez également choisir de désactiver les fonctions de connexion automatique et, si possible, de faire en sorte que le véhicule demande au conducteur ou au passager d'autoriser ou d'interdire l'accès aux contacts ou à d'autres données conservées sur les appareils mobiles avant la connexion. Lorsque vous vendez ou échangez votre véhicule, prenez les mesures nécessaires afin de retirer vos renseignements personnels. Pour vous préparer en vue du transfert de la propriété de votre véhicule connecté ou automatisé, vous pouvez entre autres annuler les abonnements, vous déconnecter des applications mobiles de même que retirer les contacts et l'information de navigation routière du véhicule.

Pour en savoir plus

Consultez le site Web du Centre canadien pour la cybersécurité (cyber.gc.ca) pour en apprendre davantage sur la cybersécurité et les services offerts par l'organisme.

Vous y trouverez le catalogue des publications, y compris les suivantes :

- Intelligence artificielle (ITSAP.00.040)
- Utiliser la technologie Bluetooth (ITSAP.00.011)
- Sécurité de l'Internet des objets (IdO) (ITSAP.00.012)
- Application des mises à jour sur les dispositifs (ITSAP.10.096)
- Pratiques exemplaires en matière de cybersécurité à intégrer dans votre organisation (ITSAP.10.102)
- Protéger son organisation contre les attaques par déni de service (ITSAP.80.100)

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada