# Véhicules connectés & cyber-risques : sécuriser les fonctionnalités intelligentes

*Par Jeff Davis, Senior Director, IVY Ecosystems Business Development, BlackBerry*

L'automobile a beaucoup évolué depuis le modèle T créé par Henry Ford, voiture qui a contribué à démocratiser l'automobile. Au début du 20ème siècle, elle était la solution parfaite qui permettait de répondre aux besoins croissants de déplacements des personnes sur de longues distances. Aujourd'hui, la technologie et les besoins ont changé notre façon de voyager.

La technologie réécrit sans cesse les règles du transport. Qu'il s'agisse du développement de véhicules électriques (VE) pour réduire les émissions ou de nouvelles fonctionnalités intelligentes pour les rendre les routes plus sûres, les constructeurs et les développeurs continuent de repousser les limites de l'innovation automobile. Plus que jamais, la nécessité des VE devrait être solidement ancrée dans nos esprits, comme en témoigne le dernier rapport sur le changement climatique de l'ONU. Le réchauffement climatique a été causé sans équivoque par l'activité humaine et les émissions de gaz à effet de serre. L'innovation et la technologie des véhicules électriques seront essentielles dans la lutte universelle contre le changement climatique.

Les gaz d'échappement ne représentent qu'une partie du carbone émis par les véhicules, mais les réduire constitue en une première étape pour assurer un avenir sans carbone. À mesure que la production d'énergie deviendra plus verte, le besoin de centrales électriques brûlant des combustibles fossiles éliminera le carbone produit par la production et le transfert d'énergie. Mais ne vous méprenez pas, une flotte de véhicules entièrement électriques est seulement un premier pas – et non pas un bond, dans un avenir très compliqué. Les structures d'emploi actuelles, le droit du travail, le développement des infrastructures et la répartition des pouvoirs sont autant de défis pour les constructeurs automobiles, les législateurs, les régulateurs et les propriétaires d'infrastructures. Le nombre croissant de VE est un tout petit pas si l'on considère les 1,2 milliard d'automobiles sur la route – et les 2 milliards prévus d'ici à 2035, à remplacer dans le monde.

Pour compliquer un peu plus les choses, examinons une des problèmes auxquels est confrontée la technologie de l'électrification : les logiciels. Un moteur à combustion interne actuel comprend, à sa sortie des chaînes de montage, pas moins de 100 millions de lignes de code. Avec la transition aux véhicules électriques et l'utilisation de l'informatique de pointe sur les véhicules, ce chiffre peut augmenter de manière significative.

Au-delà des systèmes de sécurité qui sont renforcés et améliorés chaque année, les voitures électriques disposent de systèmes capables d'évaluer et d'améliorer la production d'énergie, l'utilisation de la batterie et les fonctionnalités relatives à la charge. Le défi logiciel et technologique ainsi posé est atteignable grâce à systèmes embarqués très innovants. Pensez une seconde à ce que tout cela signifie pour le véhicule : le cœur de l'automobile, les fonctions de sécurité, la source d'alimentation, tout est géré ou régulé par logiciel. Tous les aspects de l'automobile sont donc susceptibles de présenter des vulnérabilités en matière de

cybersécurité. La voiture, qui est plus connectée et plus dépendante de la technologie que jamais, est alors une de cible de choix pour les cyber-prédateurs.

Au-delà de la voiture elle-même, celle-ci doit se connecter au réseau électrique pour obtenir être chargée. Pensez aux connexions de ce réseau, pensez aux dommages qui pourraient être causés à une économie, à un pays, à un peuple si vous deviez les priver de leurs sources d'énergie. Par conséquent, l'un des plus grands défis pour assurer notre avenir plus vert et connecté sera la cybersécurité.

**Les écueils de la cybercommunication**

Plus il y a de logiciels dans une voiture, plus la surface de cyberattaque est importante. Les véhicules connectés, qui peuvent contenir plus de 100 composants développés indépendamment, sont difficiles à sécuriser alors que plusieurs fournisseurs interviennent dans leur assemblage. D'ailleurs, la chaîne logistique automobile complexe rend l'application des critères communs de cybersécurité onéreuse.

Du simple vol de données au détournement de systèmes avancés, les véhicules peuvent être compromis via un simple smartphone. Le détournement de n'importe quelle partie d'un véhicule peut avoir des conséquences graves aussi bien pour les passagers que pour les piétons.

Sécuriser les véhicules contre les cyber-menaces devient de plus en plus complexe avec l'ajout des connexions, des composants électroniques et des systèmes pilotés par logiciel. Dans ce contexte, il n'est pas concevable de livrer des logiciels pour véhicules criblés de vulnérabilités, nécessitant en permanence des mises à jour et des outils de sécurité. Tant que des protocoles de cybersécurité efficaces n'auront pas été intégrés dans la fabrication des véhicules et de leurs composants, les automobiles modernes resteront effectivement des réseaux non sécurisés.

**Passer la seconde pour rester en tête**

Les fonctionnalités intelligentes représentent un changement de paradigme dans les transports. Toutefois, ce ne sont pas les fonctionnalités proprement dites qui leur donnent de la valeur, mais leur connectivité. De plus, les téraoctets de données générés quotidiennement peuvent être analysés et utilisés à plus grande échelle pour rendre les villes intelligentes plus sûres et plus efficaces.

Cependant, les risques de cybersécurité, qui ne peuvent être négligés, représentent un inconvénient principal. Un véhicule moyen a aujourd'hui plus de lignes de code que la plupart des avions de chasse. Les voitures sont connectées, fonctionnent à partir du cloud et sont segmentées en architectures spécifiques.

Nous ne pouvons pas prédire tous les modes d'attaque des cybercriminels, mais nous savons que la confidentialité des données sera visée. Les décideurs politiques doivent veiller à ce que

le système régissant la prochaine génération de transports protège la vie des personnes qu'il sert et leur vie privée. L'ONU a créé des directives de cybersécurité pour les constructeurs automobiles, en établissant les bases d'une sécurité accrue des véhicules que tous les pays devraient suivre.

**La solution : renforcer la sécurité grâce au Machine Learning**

Les données et leur contexte sont essentiels pour sécuriser efficacement les véhicules connectés. Heureusement, de nombreuses données sont générées par les flottes connectées ainsi que par les systèmes d'annuaires et de ressources humaines distribués qui indiquent les activités des utilisateurs autorisées et celles qui ne le sont pas. Ces données peuvent fournir des indices contextuels pour réduire les menaces.

Le Machine Learning (ML) excelle dans cet environnement. En comprenant largement l'activité qui entoure les actifs sous leur contrôle, les solutions axées sur le ML permettent aux analystes de découvrir la relation entre les événements dans le temps, et les relations entre les hôtes, les utilisateurs et des réseaux disparates. L'application correcte du ML peut fournir des informations contextuelles permettant de réduire les risques et les coûts potentiels liés à une faille de sécurité.

Les professionnels du secteur de la mobilité doivent comprendre les capacités et les limites du Machine Learning, et être en mesure de déterminer ce qu'est une solution de véhicule intelligent sécurisée appropriée.

Avec l'augmentation du nombre d'attaques par ransomware dans le monde, la cybersécurité fait l'objet d'une attention accrue, notamment dans le domaine de la sécurité nationale. Cependant, il est tout aussi important d'examiner la sécurité en profondeur lorsqu'il s'agit de véhicules connectés. Les véhicules sont intelligents, mais n'en restent pas moins machines, et les interférences avec le fonctionnement d'une voiture pourraient être catastrophiques. Ce n'est que lorsque la sécurité aura été traitée efficacement que les véhicules intelligents et connectés pourront circuler sans risque.