Votre voiture risque-t-elle d'être hackée ? Si elle se trouve dans cette liste, c'est probable

Nous nous méfions de nos ordinateurs mais nos voitures sont tout autant dangereuses entre les mains de hackers.

Avec Gérôme Billois

Un rapport de deux chercheurs en sécurité informatique Chris Valasek et Charlie Millerpointent la vulnérabilité de certains véhicules face aux hackers. Chaque voiture a été étudiée selon trois critères : la surface d'attaque, soit le degré communication avec l'extérieur, l'architecture réseau c'est-à-dire la sécurité des circuits du véhicule, et enfin, le nombre d'éléments pilotables informatiquement. La voiture la plus susceptible d'être hackée sera celle qui possède de nombreux éléments qui communiquent avec l'extérieur, un seul circuit réunissant tous les systèmes et une quantité importante d'éléments pilotables informatiquement.

(Cliquer sur l'image pour l'agrandir)

Atlantico : Les voitures sont de plus en plus modernes et donc contiennent de plus en plus d'éléments électroniques et connectés tels que le port bluetooth ou le wifi. Selon les experts Charlie Miller et Chris Valasek à l'origine d'un rapport, des pirates utilisent ces éléments pour hacker le véhicule. Quelles sont les voitures les plus sûres en termes de sécurité ? Quelles sont les voitures qui comportent le plus de risques ? Pourquoi ? Y a-t-il des marques qui se démarquent ?

Gérôme Billois : Les travaux de recherche concernant la vulnérabilité des attaques commencent actuellement. Les deux chercheurs ont révélé une analyse théorique, ils n'ont pas attaqué les voitures mais ont réfléchi, selon la conception de la voiture, à sa potentialité d'attaque. **Ils ont ainsi pu dresser une liste de 20 voitures suivant la facilité à être hackées ou non selon trois critèresLe premier est la surface d'attaque : est-ce que la voiture communique beaucoup avec l'extérieur** ? Y a-t-il du bluetooth, du wifi ? Peut-on démarrer la voiture à distance ? Quels sont les moyens de communication avec l'extérieur ? Plus la voiture a de moyens de communiquer avec l'extérieur, plus elle est vulnérable. **Le deuxième critère est l'architecture réseau.** Une voiture a un réseau informatique où les données sont échangées entre les différents systèmes. Quand on appuie sur l'accélérateur, l'information passe par le réseau pour atteindre le moteur. Il existe différentes possibilités de conception du réseau. Le constructeur peut opter pour un seul réseau qui contient tous les systèmes (freins, accélérateur, direction, fonctionnement électrique du véhicule...) ou pour trois réseaux qui divisent le données entre celles qui sont dites critiques (accélérateur, freins, direction), celles qui sont dédiées au fonctionnement de la voiture (vitres, commandes des portes, fonction d'usage de la voiture) et celles dites de loisirs (température, affichage du GPS). Si le constructeur découpe le réseau en trois la voiture sera plus sûre que celle qui ne possède qu'un seul réseau. Le troisième et dernier critère est la quantité d'éléments qui sont pilotables informatiquement. Toutes les voitures n'ont pas les mêmes fonctions, avec

certaines d'entre elles on peut changer les roues de direction, activer le frein à main...

Les pires voitures en terme de sécurité sont donc celles qui sont très connectées avec l'extérieur et qui ne possèdent qu'un seul réseau. **Les voitures les plus sûres sont celles qui possèdent un bon cloisonnement entre les réseaux, ainsi, même si les pirates parviennent à y accéder, ils ne pourront pas faire grand chose.**

Quelles fonctions ou options favorisent les risques de piratage ?

Les fonctions qui favorisent les risques sont celles qui incluent des réseaux sans fil. Les plus connues sont le bluetooth et le wifi. Attention également aux réseaux spécifiques comme le réseau des télécommandes, les réseaux 3G et 4G ainsi que les réseaux d'activation à distance.

Comment s'y prennent les hackers ? Est-ce à la portée de tous ?

Aujourd'hui tous les cas démontrés d'attaque ont été réalisés en branchant un boitier à l'intérieur du véhicule, plus précisément sur la prise de diagnostique appelée OBD 2, une fois le boitier connecté, on peut commencer à essayer le réseau de la voiture. Ce n'est techniquement pas à la portée de tout le monde mais c'est de plus en plus simple. **Le boitier coûte environ 100 euros, avec un ordinateur du commerce on peut le contrôler, il suffit ensuite de chercher des informations sur internet et hacker la voiture.**

Quelles peuvent être les conséquences ? Le hacker peut-il prendre le contrôle de notre véhicule ?

L'année dernière les chercheurs ont attaqué deux voitures de Ford et Toyota. Ils ont montré la capacité à prendre le contrôle du véhicule, on peut changer les indications du tableau de bord, freiner, accélérer... Les modifications se font aussi bien sur des éléments essentiels comme le freinage, l'accélération ou la direction, que sur les fonctions facultatives ; le contrôle des vitres électriques, l'affichage du compteur...

Comment s'en protéger ?

Aujourd'hui le grand public peut difficilement s'en protéger. Chaque propriétaire de voiture doit faire attention à ne pas laisser son véhicule facilement accessible à n'importe qui, qui pourrait brancher le boitier. Si le propriétaire du véhicule en a vraiment peur, il peut vérifier que rien n'est branché à la prise diagnostique qui se trouve souvent sous le volant. C'est plutôt aux constructeurs de régler ce problème de sécurité.

Est-ce un problème dont ont conscience les fabricants ?

C'est un problème dont ils ont conscience. Des équipes sont chargées de concevoir des systèmes de sécurité efficaces. C'est un sujet qu'ils suivent de près. D'autant plus que le nombre de voitures connectées augmentera avec le temps. La voiture de demain sera connectée aux autres véhicules, à la route même, dont elle retirera des informations.