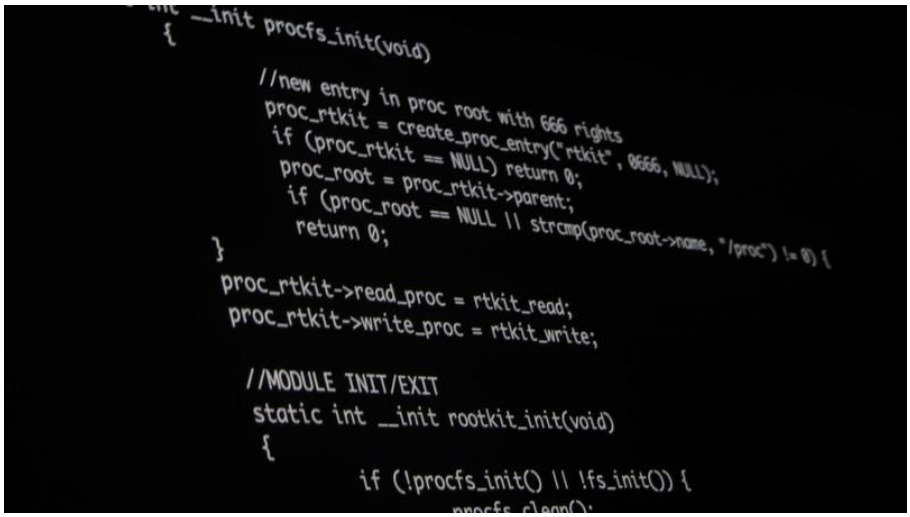
Les américains s’inquiètent de la cyber-sécurité automobile



Les américains s’inquiètent de la cyber-sécurité automobile

Après l'attentat de Nice, les questions de cyber-sécurité sont devenues une urgence pour les américains, qui imaginent le scénario catastrophe d'un pirate informatique prenant le contrôle d'un véhicule.

L'attentat terroriste de Nice a ravivé dans le secteur automobile américain les craintes d'un scénario catastrophe où un pirate informatique prend à distance le contrôle d'une voiture pour l'utiliser comme projectile. Cette éventualité, digne d'un scénario hollywoodien, est alimentée par la circulation croissante de voitures semi-autonomes et connectées, équipées de systèmes multimédias embarqués censés les rendre plus sûres et fiables.

Paradoxalement, ces mêmes technologies de pointe en font des cibles privilégiées pour les hackers, selon les sociétés de sécurité informatique américaines Mission Secure Inc (MSi) et Perrone Robotics Inc. Car, selon celles-ci, les pirates informatiques pénètrent via les connexions sans fil, bluetooth et wifi, nécessaires à leur fonctionnement. «La technologie crée beaucoup d'opportunités nouvelles et excitantes pour les consommateurs mais (génère) aussi des défis», opine Mary Barra, la PDG de General Motors (GM). «L'un de ces défis est la problématique sur la cyber-sécurité», a-t-elle insisté vendredi devant un parterre composé de ses pairs, d'officiels et d'experts de l'automobile réunis à Detroit pour évoquer les cyber-attaques.

Le 14 juillet, Mohamed Lahouaiej-Bouhlel, un Tunisien, a foncé au volant d'un camion dans la foule à Nice tuant 84 personnes et blessant plus de 330 personnes.

«Nous connaissons ces terroristes (…) il ne faut pas beaucoup d'imagination pour penser qu'ils vont se servir d'une voiture autonome et la faire foncer dans une foule.»
John Carlin, un ministre-adjoint américain de la Justice.

«Nous connaissons ces terroristes. Ils n'en ont peut-être pas encore les capacités mais s'ils parviennent à convaincre les gens de foncer dans une foule avec un camion, il ne faut pas beaucoup d'imagination pour penser qu'ils vont se servir d'une voiture autonome et la faire foncer dans une foule», redoute John Carlin, un ministre-adjoint américain de la Justice. «Les méchants emploient de plus en plus de moyens sophistiqués», souscrit David Johnson, un des responsables du FBI chargé des cybercrimes et des menaces sur internet.

A l'été 2015, deux chercheurs américains en informatique ont démontré qu'il était facile de prendre le contrôle d'une voiture «connectée». Charlie Miller et Chris Valase étaient parvenus à pirater à distance la Jeep Cherokee d'un journaliste du site spécialisé Wired. Ils avaient ainsi pu allumer la radio, fait fonctionner les essuie-glaces et, surtout, couper le moteur. Ils étaient aussi parvenus à désactiver les freins. Les «menaces évoluent», avance Titus Melnyk chargé de la sécurité chez Fiat Chrysler Automobiles (FCA), qui vient de lancer un programme visant à encourager les hackers à informer le groupe des failles liées à la cyber-sécurité de ses voitures. Le constructeur des Jeep promet une prime pouvant aller jusqu'à 1.500 dollars par alerte. «On ne sait jamais. Cela peut être la base d'une attaque», défend M. Melnyk insistant sur le fait que ce programme est «très sérieux».

En 2015, le constructeur de véhicules électriques de luxe Tesla – dont les deux modèles commercialisés (Model S et Model X) sont équipés d'un système d'aide à la conduite leur permettant d'effectuer seuls certaines manoeuvres comme le freinage en urgence – avait été l'un des premiers à lancer un tel plan. Tesla, qui a construit sa réputation sur l'innovation, n'avait pas le choix: deux chercheurs avaient révélé qu'ils pouvaient couper à distance le moteur d'une berline Model S en piratant le système multimédia. GM, qui dit recevoir et résoudre plusieurs alertes liées à de possibles cyber-attaques par jour, gère un programme sur les vulnérabilités de ses voitures sur le site hackerone.com.

Les nouvelles technologies embarquées exposent également les conducteurs à un vol potentiel de leurs données personnelles quand ils connectent leur téléphone intelligent.

Article original de lefigaro.fr

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Les américains s’inquiètent de la cyber-sécurité automobile