COMMENT J'AI HACKÉ VOTRE VOITURE

GODEFROY GALAS
ingénieur-élève
du corps des Mines

J'ai réalisé en 2018 dans le cadre de mon cursus à Télécom Paris, sous la supervision de Pascal Urien, un projet de fin d'études qui s'attachait à la conception de scénarios d'attaque visant à altérer, en situation réelle, le fonctionnement d'une automobile moderne vendue en Europe.

Les attaques menées avec succès comptent, entre autres, la manipulation des compteurs du tableau de bord, l'activation de la caméra de recul en marche avant, l'ouverture et la fermeture sur commande des portes et du coffre, le blocage des freins avec l'activation forcée de l'ABS ou encore la mise hors service du moteur à combustion.

Votre voiture parle trop

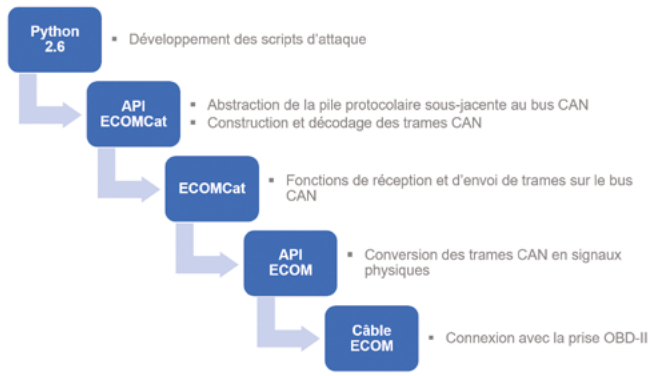
Ces différentes attaques reposent sur l'insécurité globale du bus CAN (*Controller Area Network*) qui permet aux différents composants électroniques du véhicule – nommés ECU (*Electronic Control Units*) – de s'échanger, en temps réel, des données de capteurs (température du moteur, pression des pneus) ou des ordres de commande (« abaisser la vitre », « activer les freins »). Ce bus présente deux caractéristiques majeures constituant des vulnérabilités exploitables *via* un vecteur d'attaque physique : le fonctionnement en mode *broadcast* et l'absence de chiffrement des messages.

L'accès au bus CAN peut se faire *via* la prise OBD-II qui est obligatoire dans tous les véhicules récents vendus aux États-Unis et en Europe. Cette prise permet, en utilisant des équipements peu onéreux et en appliquant une méthode de *reverse engineering*, d'écouter et de manipuler les données circulant sur le bus en se faisant passer pour un ECU légitime du véhicule. L'accroissement de la connectivité des véhicules permettrait à un attaquant potentiel de les exécuter également sur des véhicules connectés voire autonomes, en rebondissant sur le bus CAN à distance.

Comment un hacker parle à votre voiture

Pour communiquer avec le bus CAN, ce projet a adapté un programme C dénommé ECOMCat et développé par deux chercheurs en sécurité automobile, Chris Valasek et Charlie Miller. La figure ci-dessus présente l'ensemble des outils et programmes installés sur la machine Windows 7 d'attaque.

Cet équipement a permis d'enregistrer en temps réel dans un fichier, avec horodatage, chaque message circulant sur le bus CAN au cours du déplacement du véhicule. Les fichiers obtenus, comptant de l'ordre de 50 000 trames par minute, ont été analysés grâce à des scripts Python afin de lister l'ensemble des types de messages existants (repérés par un identifiant) et de déterminer, par différenciation, la structure de chacun. En associant ces analyses avec des expérimentations d'injection de trames et de manipulation des composants du véhicule, il est possible d'identifier le rôle, la structure et la fréquence de diffusion des différents types de messages circulant sur le bus, ouvrant ainsi la voie vers la conception des scénarios d'attaque précités.



Des véhicules autonomes vulnérables

Dès cette année, la loi d'orientation des mobilités a autorisé la circulation de navettes autonomes potentiellement vulnérables sur l'ensemble du réseau routier français. Dans ce contexte, l'action publique devra s'attacher, d'une part, à intégrer dans la réglementation technique les nouveaux enjeux de cybersécurité induits par la connectivité des véhicules autonomes et, d'autre part, à soutenir financièrement des programmes de R & D incitant les différents constructeurs d'automobiles à développer des architectures électroniques conformes aux nouveaux impératifs de sécurité. Une telle action doit être menée en associant étroitement les acteurs industriels concernés, à l'échelle nationale ou européenne.

Ressources

Des vidéos illustratives sont visualisables à l'adresse suivante : https://nextcloud.ggalas.net/index.php/s/6meXqJrJanL2nfk

VALASEK (Chris), MILLER (Charlie), « *Adventures in Automotive Networks and Control Units* », 2013.