Hacker les voitures connectées ? C'est en Open Source

C'est une bien belle queue de poisson que s'apprête à faire Eric Evenchick au secteur qui l'employait précédemment. Cet ex-employé de Tesla, le constructeur californien de voitures électriques, vient de placer en Open Source **un outil de diagnostics et le design d'une carte permettant de se raccorder au CAN** (Controller Area Network, un bus de communication très employé dans l'automobile) afin de détecter d'éventuelles vulnérabilités logicielles. Développée en Python, cette CANard – c'est son nom – doit aider l'industrie à prendre plus au sérieux le sujet de la sécurité des véhicules connectés, estime **Eric Evenchick**. De facto, la carte va permettre aux chercheurs en sécurité de tester plus simplement la robustesse des systèmes embarqués.

« *Cette boîte à outils permettra de travailler facilement avec CAN, de dialoguer avec les contrôleurs embarqués dans les voitures, de réaliser des diagnostics et de tester automatiquement la présence d'éventuelles vulnérabilités* », explique le chercheur dans la présentation de sa conférence lors de la conférence BlackHat Asie, qui se tient du 24 au 27 mars à Singapour. Et de promettre la mise au jour de vulnérabilités via l'outil.

Permis de hacker

Le matériel associé, une **interface entre bus CAN** (via un port nommé OBD2) **et USB**, permet de lancer les diagnostics **sur Mac OS, Windows ou Linux**, depuis une machine standard. Cette carte appelée CANtact sera vendue moins de 60 $. Et son design sera, lui aussi, ouvert. Ce qui place le piratage de voitures informatisées à la portée d'à peu près n'importe qui… De quoi donner quelques sueurs froides aux constructeurs, qui savent pertinemment que leurs systèmes embarqués n'ont pas été développés pour résister à des attaques réseau sophistiquées.

Au cours des derniers mois, plusieurs chercheurs en sécurité ont d'ailleurs démontré la porosité des systèmes embarqués dans les véhicules. Et ce, avec des technologies de plus en plus banalisées. Cette année, des chercheurs financés par la Darpa (une agence chargée des technologies émergentes au sein du département américain de la défense) ont pris le contrôle d'un véhicule depuis un simple PC portable. En 2013, déjà, Chris Valasek et Charlie Miller ont placé en Open Source des scripts Python testant la vulnérabilité des voitures aux attaques informatiques. Eric Evenchick va un pas plus loin dans la **démocratisation de ces techniques** en y ajoutant l'interface matérielle rendant les tests extrêmement simples à mettre en œuvre.

Face à la montée de ces menaces, les constructeurs ont plutôt adopté jusqu'alors la politique de l'autruche. Très peu d'industriels ont ainsi publié des procédures permettant aux chercheurs en sécurité de les alerter avant la divulgation des failles.

A lire aussi :

Voitures connectées : General Motors se dote d'un directeur cybersécurité
Sécurité des voitures connectées : l'inquiétude des experts grandit

Jérôme Boyer, Continental : « Pourquoi la voiture va embarquer Ethernet »

crédit photo © vichie81 – shutterstock