Grâce à un simulateur, les ingénieurs de Kereval testent la performance des logiciels embarqués, mais aussi leur compatibilité avec les standards et les risques d'intrusion dans les réseaux de communication.
Klervi L'Hostis

DOSSIER : LA VOITURE CONNECTÉE

METTEZ VOTRE CYBERCEINTURE !

Communications internes et externes, connectivité, on ne peut plus se passer de la cybersécurité à bord des voitures.

En 2015, aux États-Unis, des chercheurs en informatique ont pris le contrôle du tableau de bord d'une Jeep Cherokee de Fiat Chrysler, à distance. Après avoir mis en route la climatisation, les essuie-glaces et l'autoradio, ils ont purement et simplement coupé le moteur. Très médiatisée, cette expérience réalisée en complicité avec le conducteur (un journaliste de Wired), a montré à quel point la cybersécurité automobile devait être mieux prise en compte.

Des failles faciles à combler

« *La plupart des failles de sécurité dans les véhicules sont assez classiques et faciles à combler via des mises à jour. Si elles existent, c'est parce que les constructeurs et les équipementiers n'ont pas toujours intégré cette réflexion dans leur démarche, ils ont privilégié l'aspect fonctionnel de leurs solutions logicielles. Aujourd'hui, c'est en train de changer. Ils participent à des projets de recherche européens sur ce thème* », explique Yacine Tamoudi, ingénieur sécurité de Kereval. Depuis quatorze ans, cette entreprise située à Thorigné-Fouillard (Ille-et-Vilaine) est un laboratoire d'ingénierie et de tests logiciels dans différents secteurs : les box d'accès à Internet, les applications mobiles, les logiciels de santé dans les centres médicaux... Et depuis 2006, elle s'intéresse aussi aux systèmes embarqués dans les véhicules et plus récemment aux véhicules connectés, déjà nombreux sur le marché.

« *Nous testons la performance des programmes, la compatibilité avec les standards, les risques d'intrusion dans l'architecture des réseaux...* »

Pour analyser la vulnérabilité informatique d'une voiture, les experts de Kereval se mettent dans la peau d'un hacker : « *Il va d'abord essayer d'atteindre le système* », décrit Yacine Tamoudi. Et les portes d'entrée sont nombreuses, notamment à distance : le Wi-Fi, le Bluetooth, la 3G ou le navigateur Web du tableau de bord du véhicule. Un CD avec un programme informatique dédié peut également faire l'affaire une fois inséré dans le lecteur. Dès que l'on branche un smartphone à un port USB de la voiture, une nouvelle porte peut s'ouvrir... « *Une fois que le hacker est dans le système, il n'aura pas forcément accès au fonctionnement de la voiture, tout dépend de l'architecture du réseau, des connexions entre les briques logicielles.* » Et là, on trouve de tout chez les constructeurs. Certains ont développé des réseaux très complexes qui séparent bien ceux qui commandent la mécanique du véhicule (freins, moteur, essuie-glaces...) de ceux qui gèrent les loisirs (radio, navigateur Web...). Chez d'autres, les architectures sont beaucoup plus permissives. Les composants logiciels peuvent aussi être à l'origine de problèmes.

Des nœuds de spaghettis

Certains codes sources ont été décrits comme « de véritables nœuds de spaghettis », résume Yacine Tamoudi. « *Ils sont difficilement testables et pas toujours compatibles les uns avec les autres. On ne peut même pas prédire leur comportement si un mauvais message circule.* »

« *Pour éviter les risques, il faudrait développer et établir une architecture logicielle standardisée pour l'électronique des véhicules.* » C'est justement le but du projet Autosar, un partenariat de développement mondial de l'industrie automobile créé en 2003. « *Il était prévu qu'une certification des briques logicielles soit obligatoire pour les constructeurs et équipementiers avant la commercialisation d'un véhicule connecté. Finalement, ce n'est pas encore le cas, mais nous avons profité de cette occasion pour approfondir nos compétences dans le domaine.* »

Même si la route est encore longue, l'importance de la cybersécurité dans la voiture est de plus en plus considérée à sa juste valeur. Un nouvel appel à projets(1), lancé en avril par la Région Bretagne, vise d'ailleurs le développement de briques technologiques destinées à la robustesse des dispositifs embarqués dans tous les moyens de transports.

Connectées mais anonymes !

Tandis que Kereval s'intéresse aux réseaux de communication à l'intérieur des voitures, la start-up YoGoKo et des chercheurs de Télécom Bretagne se concentrent sur les échanges d'informations à l'extérieur de l'habitacle. « *Les voitures de demain communiqueront ensemble et avec l'infrastructure routière, pour anticiper des événements comme les embouteillages, les accidents, le brouillard...* », rappelle Jean-Marie Bonnin, professeur au département Réseaux, sécurité et multimédia de Télécom Bretagne. « Si on laisse les informations circuler librement sans prendre de précaution, les parcours des usagers sont traçables », ce qui soulève la question de la protection de la vie privée. « *Nous poursuivons plusieurs objectifs contradictoires : les messages doivent être signés pour les protéger et garantir leur légitimité, mais anonymes pour des questions de protection de la vie privée. En même temps, en cas d'usage abusif ou pour des questions de traçabilité des échanges, les autorités doivent pouvoir remonter à l'identité de la source.* » La solution envisagée dans les standards consiste à changer régulièrement l'identité visible de l'émetteur en utilisant des certificats pseudonymes. Il est ainsi possible de signer les messages sans dévoiler son identité.

Rens. : Jean-Marie Bonnin tél. 06 60 76 79 76 jm.bonnin@telecom-bretagne.eu

KLERVI L'HOSTIS

(1) www.bretagne.bzh/jcms/prod_323159/fr/appel-a-projets-experimentation-cyber.

Contacts
Yacine Tamoudi
tél. 02 23 20 36 64
yacine.tamoudi@kereval.com