Sécurité des véhicules connectés et/ou autonomes

Ludovic Apvrille
Enseignant-chercheur à Telecom ParisTech. Ludovic.apvrille@telecom-paristech.fr

Letitia Li
Doctorante VEDECOM / Télécom ParisTech – letitia.li@vedecom.fr

L'antivirus de votre véhicule est-il bien à jour ? Son pare-feu est-il bien configuré ? Si cela est pour l'instant de l'ordre de la science fiction, l'on commence à voir apparaître des attaques sophistiquées sur les systèmes embarqués des véhicules. Cet article présente les architectures actuelles, les attaques qu'elles peuvent subir, et les solutions de sécurité actuelles. Il explique aussi en quoi ces solutions devront évoluer pour sécuriser aussi les véhicules communicants et/ou autonomes.

VÉHICULES CONNECTÉS / VÉHICULES AUTONOMES / ARCHITECTURES EMBARQUÉES SÉCURISÉE

Si les menaces d'attaques étaient avant réservées aux ordinateurs personnels et aux serveurs d'entreprise, elles concernent à présents de nombreux équipements connectés. Cela a principalement commencé avec la multiplication des malwares ciblant les smartphones – actuellement, plus de 2000 nouveaux logiciels malveillants (malwares) Android sont publiés chaque jour – et les systèmes industriels (Stuxnet en est un très bon exemple). L'avènement de l'« Internet of things » (IoT) ouvre de nouvelles cibles aux cyber criminels. Les véhicules sont en train de prendre aussi le virage de la connexion tous azimuts, en offrant de nombreux moyens d'échanges avec leur environnement : signalisation routière, péages, distraction pour les passagers (« infotainment »), mais aussi les plus classiques ports de diagnostic. Les véhicules autonomes offriront à l'avenir une connectivité encore plus élevée, et devront reconnaître leur environnement – qui pourrait être manipulé – pour déterminer leur trajectoire. Les véhicules pourraient d'autant plus servir de cible qu'ils présentent un intérêt important tant en termes de puissance de calcul (botnets), qu'en termes de valeur financière (ransomware). Et bien entendu, leur caractère critique pourrait en faire une cible privilégiée pour des actions terroristes, y compris de grande envergure par l'exploitation d'une faille commune à de multiples modèles de véhicules.

L'article dresse tout d'abord un panorama des systèmes embarqués automobiles, des attaques connues et des solutions de sécurités actuelles. Par la suite, l'article s'intéresse aux problématiques de sécurité propres aux véhicules autonomes.

1 Des véhicules de nos (arrières?) grands parents aux véhicules d'aujourd'hui et du futur

Les systèmes électroniques (puis informatiques), ne sont pas si récents que cela sur les automobiles. Les premiers systèmes nécessitant du courant électrique furent les avertisseurs sonores (les fameux « Klaxons ») au début du 20ème siècle, et la batterie associée qui fournissait la puissance nécessaire. Cela a permis de réduire les cris des automobilistes, notamment aux intersections. Ces batteries ont progressivement servi à alimenter d'autres équipements : phares, indicateurs (par exemple la vitesse), démarreurs, essuie-glaces, puis des équipements de confort (vitres électriques, climatisation), des équipements liés à la sécurité (l'ABS), et des équipements liés à la performance du véhicule (le contrôle électronique des moteurs), etc. Tous ces équipements ont engendré une multiplication du câblage, qui induit un coût plus important, un poids non négligeable, et une maintenance plus fréquente. Les systèmes modernes ont progressivement diminué le câblage par l'utilisation de bus de type CAN / FlexRay, voire Ethernet. La même tendance se retrouve d'ailleurs au niveau des systèmes avioniques.

Actuellement, les innovations disponibles dans les systèmes embarqués automobiles concernent principalement l'assistance à la conduite. Cela a commencé par le maintien de la vitesse d'un véhicule

(« cruise »). Les options en vogue actuellement vont plus loin : suivi d'une véhicule (« adaptative cruise »), alarme de franchissement de ligne, analyse des obstacles – y compris les piétons – avec décision de freinage d'urgence et réalisation du freinage en cas de collision imminente, assistance au parking.

Le futur appartient sans aucun doute aux véhicules autonomes, c'est à dire aux véhicules dans lesquels le conducteur peut laisser, sauf avis contraire du système, la conduite du véhicule à un ordinateur embarqué. Ce mouvement va probablement se faire progressivement, avec une autonomie limitée dans un premier temps à des espaces « faciles », comme par exemple la recherche d'un stationnement dans un parking souterrain, le suivi d'un véhicule dans un embouteillage (faible vitesse), ou la gestion du véhicule sur autoroute. Par la suite, les systèmes pourront évoluer dans des milieux plus complexes : routes, villes, etc.

Si ces systèmes autonomes pourront s'aider d'informations envoyées par des panneaux ou des autres véhicules communicants (cela s'appelle le V2X pour Vehicle-to-Something, ce qui englobe tous les communications d'un véhicule vers l'infrastructure appelée V2I, et le V2V qui concerne le Vehicle-to-Vehicle), ils devront aussi s'accommoder de systèmes non communicants : piétons ou véhicules plus anciens. Les communications inter-véhicules (V2V) ont pour objectif notamment une meilleure gestion du trafic routier - et donc une réduction de la consommation d'énergie -, et la réduction du nombre d'accidents. Le V2I et le V2V font partie de la thématique des routes dites intelligentes.

En France, le laboratoire VEDECOM [VEDECOM] étudie la problématique des véhicules autonomes. VEDECOM est issu d'un programme d'investissements d'avenir, et correspond à un partenariat public-privé dans lequel les plus grands constructeurs et équipements automobiles français sont présents. Pour l'instant, les véhicules autonomes restent cantonnés à des espaces privés ou d'expérimentation. C'est uniquement lors d'occasions spéciales que nous les rencontrons dans le domaine public. En effet, les législations ont encore à évoluer pour permettre l'évolution de ces véhicules sur la chaussée, notamment pour préciser les procédures en cas d'accident d'un véhicule autonome.

2 Architecture embarquée automobile

Présentons les architectures embarquées actuelles. Un véhicule classique est constitué d'environ 70 à 100 « ECU » (Electronic Control Units), jusqu'à 120 pour les véhicules les plus évolués. Ces unités sont parfois très modestes en termes de puissance de calcul et d'architecture logicielle / matérielle.

Il peut s'agir d'un composant simple comprenant typiquement un capteur – par exemple, un capteur de pression -, un microcontrôleur, une mémoire flash pour stocker le code logiciel, et un bus interne reliant ces différents composants. Cet ensemble de composant est appelé un domaine. Un domaine peut lui même contenir des sous-domaines, et faire partie de sur-domaines (organisation hiérarchique). Un « domaine » est connecté soit :

- à un autre domaine, qui peut-être un sur-domaine ou un sous-domaine ;
- au bus principal (un bus CAN, LIN, FlexRay, MOST, ou plus récemment Ethernet).

Un domaine complexe est constitué de processeurs plus puissants, parfois à plusieurs cœurs, de mémoire, et d'interfaces parfois multiples. Notons enfin qu'un domaine « simple » peut tout à fait être en charge d'une fonction extrêmement critique, comme la régulation de la mâchoire d'un frein à disque.

Pour concrétiser, citons quelques domaines et sous-domaines que l'on retrouve classiquement (cf. figure 1) :

- Des domaines (et sous-domaines) internes et liés à la gestion du moteur (PTC – PowerTrain), à la gestion du châssis et de la sûreté (CSC – Chassis and Safety), à la gestion des différents équipements électroniques de confort et d'information (BEM – Body Electronic), à l'interface avec le conducteur et les passagers (HU – Head Unit) et enfin à la communication (CU – Communication Unit).
- Deux domaines sont ouverts sur l'extérieur : le domaine HU permet à l'utilisateur d'interagir avec le système automobile, via un port USB, un téléphone connecté en Bluetooth, en insérant un CD dans l'autoradio... Le domaine CU concerne les communications du véhicule avec des équipements externes : l'interface vers la télécommande, la gestion du signal GPS, la communication avec des infrastructures routières, et enfin le port de debug (par exemple, de type ODB-II). Nous le verrons par la suite : ce sont surtout ces interfaces qui sont utilisées pour mener des attaques.

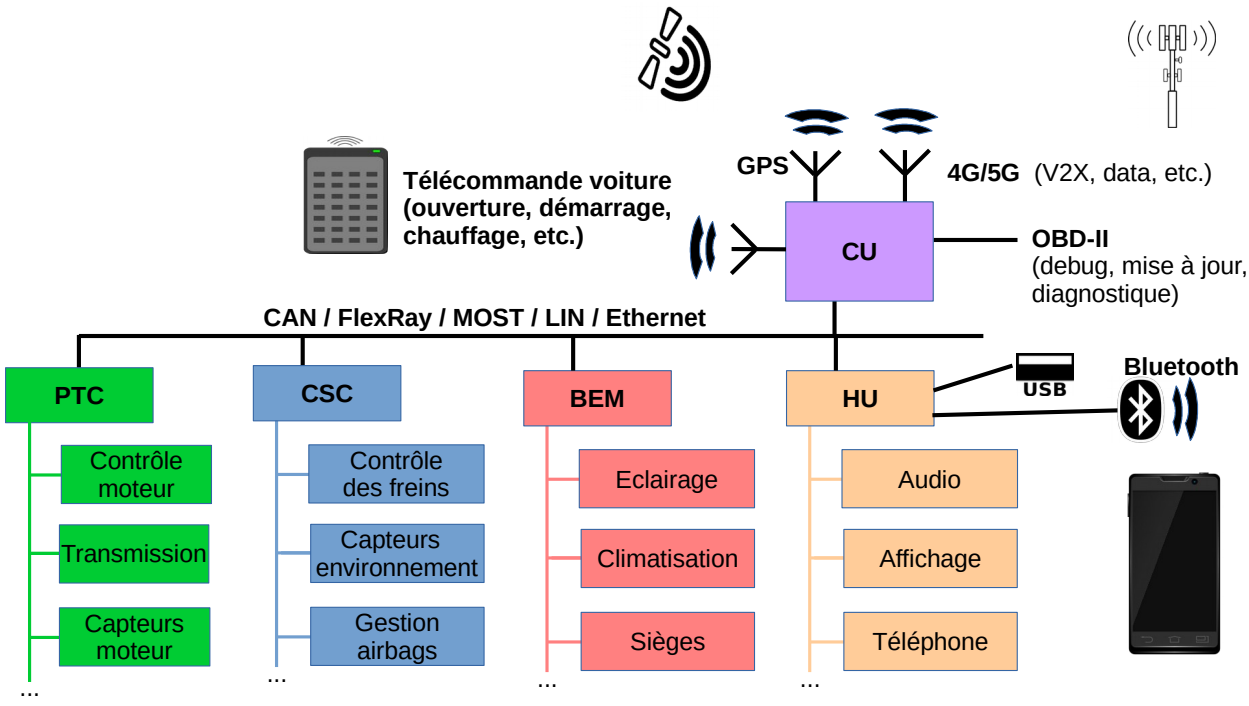

Fig. 1 : Architecture typique d'un système embarqué automobile. Les domaines sont interconnectés avec un bus principal.

3 Problèmes de sécurité des architectures actuelles

3.1 Attaques usuelles

Les attaques actuellement réalisées à grande échelle sur les systèmes automobiles ont deux motivations principales : l'activation d'options et le vol de véhicule.

L'activation d'options

L'activation d'options non payées nécessite que les composants de cette option soient physiquement présents dans le véhicule. Une « attaque » peut consister à reflasher le logiciel de gestion du moteur afin d'augmenter sa puissance. On peut trouver sur Internet des logiciels / firmwares tiers, ainsi que le moyen de les flasher au niveau des microcontrôleurs de gestion des fonctions automobiles. Par exemple, [INS 2016] explique comment activer des fonctions des plusieurs modèles BMW. Des entreprises qui ont « pignon sur rue » (ou sur le web, comme par exemple Bimcoding [BIMCODING 2016]) proposent aussi des services d'activation d'options non achetées sur le modèle initial. Elles sont capables de faire la mise à jour à distance, moyennant l'achat préalable d'un kit de connexion matériel. Ces entreprises et sites divers expliquent en général l'impact sur la garantie et les risques, selon l'option activée.

Le vol de véhicules

Le vol de véhicule peut être réalisé de plusieurs manières : attaques sur le système de verrouillage des portières, sur le système de démarrage... D'autant plus lorsque le démarrage et/ou le déverrouillage sont sans fil !

Les premiers systèmes sans fil utilisaient un code secret (« clé ») fixe que les attaquants n'avaient aucune peine à reproduire avec un enregistreur / émetteur radio. Les systèmes ont par conséquent été modifiés par les constructeurs pour changer régulièrement leur code (systèmes dits à « rolling code »). Ces systèmes restent toutefois sensibles à différentes attaques, nous en présenterons trois.

La première, la plus simple et plus fréquente consiste à brouiller les fréquences radio lorsque l'utilisateur verrouille sa voiture ; ceci aura pour effet d'empêcher le verrouillage et donc de laisser le véhicule ouvert. Mais cela repose sur le fait que l'utilisateur ne vérifie pas si les portières sont réellement fermées ou pas, et qu'aucun voyant externe (clignotement rapide des phares, son) ne signale le bon verrouillage.

Une deuxième attaque consiste à se placer au plus près du propriétaire de la clé – par exemple lorsqu'il fait ses courses dans un supermarché, en l'ayant repéré au préalable -, puis à activer un (puissant) répéteur radio : le signal de la clé peut alors être répété jusqu'au véhicule même si la personne se trouve loin. Une parade consiste à mesurer le temps de propagation du signal entre la clé et le véhicule pour calculer la distance entre la clé et le véhicule, mais cela nécessite du matériel plus coûteux car la différence de temps entre par exemple 10m de distance et 100m de distance pour une onde radio est de l'ordre de 300ns. Il est donc difficile de se prémunir de ce genre d'attaques, même si cette dernière reste complexe à mettre en œuvre.

Enfin, une troisième attaque repose sur l'utilisation d'un craqueur de « rolling codes » appelé *RollJam*, et publié à Defcon en 2015 [KAMKAR 2015]. L'attaque consiste à écouter le premier code, et le brouiller afin qu'il ne soit pas reçu par le véhicule. L'utilisateur appuie alors généralement à nouveau sur sa télécommande, ce qui a pour effet d'envoyer un second code. L'attaquant enregistre à nouveau ce deuxième code, le brouille puis renvoie le premier code vers le véhicule. Le deuxième code non utilisé reste valide, puisque seul le premier a été utilisé. Le matériel utilisé coûte dans les 30 US Dollars, et concerne de nombreuses marques de véhicules.

3.2 Proof of Concepts

Ces différentes « attaques » mettent en évidence la présence de vulnérabilités importantes à différents niveaux des architectures automobiles : capteurs, communications externes, communications internes (voir la Figure 2).

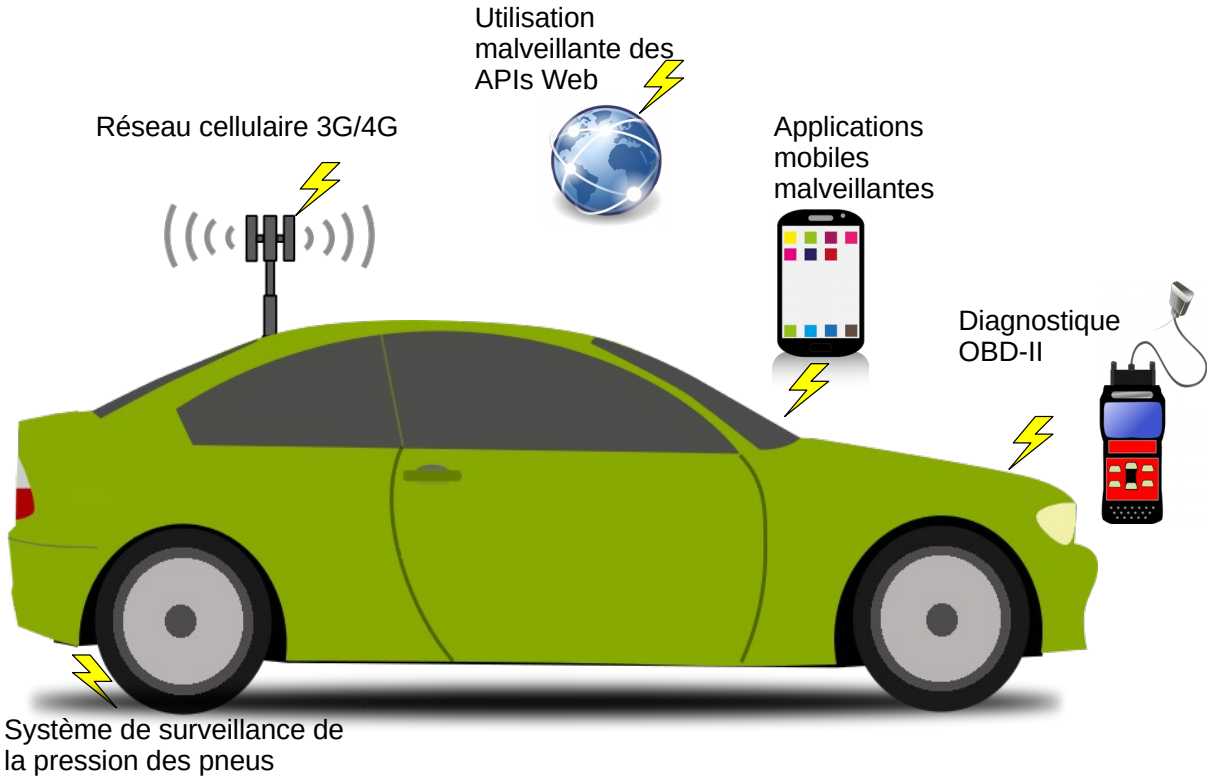

Fig. 2 : Attaques démontrées sur des véhicule actuels .

[ROUF 2010] a montré comment récupérer l'ID unique d'un capteur de pression de pneumatique, pour ensuite envoyer en RF des faux paquets – mais avec la bonne identification de capteurs – pour générer des alertes, menant ainsi un conducteur à freiner. Cette attaque permet aussi l'identification des véhicules par relevé RF.

L'on trouve de nombreuses attaques réalisées en se branchant sur le port de debug (OBD) du système embarqué. Par exemple, les auteurs de [KOSCHER 2010] ont réalisé une attaque via l'OBD qui a consisté à sniffer les paquets du bus CAN, puis à injecter des données par fuzzing. Ils sont arrivés par ce biais à modifier le code logiciel des ECUs, mais aussi à effacer toute trace d'attaque. Plus récemment, [WOO 2015] a montré que l'utilisation d'un smartphone connecté en bluetooth sur un « OBD-II scan tool » inséré ds le

véhicule permettait d'injecter à distance des paquets CAN malicieux. Les auteurs de [FOSTER 2015] ont aussi réalisé une attaque assez similaire : ils ont analysé un outil d'interfaçage avec le port OBD-II, le *Metromile TCU*, et ont constaté qu'ils comportent tous la même clé ssh (obtenue par dump de la flash). Ils ont ainsi pu envoyer, par SMS, un update aux TCU, ce qui leur a permis de lancer un shell distant, puis d'injecter des messages via ce shell. Ils ont notamment montré l'activation du freinage sur une Corvette. L'attaque mise en évidence par Miller et Valesek [MILLER 2015] repose aussi sur un accès distant via le réseau de Sprint et vise les unités de télémesure « Uconnect's Diagnostics Bus » qui est ouvert à tout équipement 3G du réseau Sprint. Les chercheurs ont montré la reprogrammation de l'unité afin d'injecter des messages CAN, et contrôler ainsi les ECUs. Cette attaque est assez exceptionnelle car elle permet d'attaquer tout véhicule ayant une unité connectée sur le réseau Sprint.

Parfois, les attaques distantes se font au travers d'applications utilisateur, y compris depuis des applications mobiles (les « companions apps ») dont l'objectif est la gestion d'options utilisateur (climatisation, etc.), et sans passer par un outil de télémesure particulier. Par exemple, l'application mobile de la NISSAN Leaf [HUNT 2016] possède un défaut sur le protocole d'authentification (utilisation seule du Vehicle Identification Number …) qui a permis d'accéder à l'activation de fonctions du véhicule, mais aussi à la récupération d'informations sur la conduite. Toutefois, l'interface WebAPI n'a pas permis d'accéder à des fonctions vitales du véhicule.

Enfin, les unités d'enregistrement de l'activité des véhicules mentionnés auparavant (usage, méthode de conduite, positionnements géographiques) permettent à des entreprises de tirer profit d'informations de conduite (assurances par exemple). Notons que des informations peuvent parfois être obtenues avec des dispositifs détachés du véhicule : lecteurs de plaques d'immatriculation, paiement par carte de crédit aux péages (ou télépéages).

4 Solutions pour la sécurisation des architectures embarquées

Tout d'abord, il faut savoir qu'il n'existe pas de standard définissant comment une architecture automobile doit être sécurisée : chacun fait ce qu'il veut dans son coin (bonjour la compatibilité!). Il y a tout de même certaines actions, initiées principalement par certains équipementiers et constructeurs automobiles allemands, qui ont défini des solutions d'architectures matérielles et logicielles pour sécuriser les systèmes automobiles : SEVECOM, SHE, et EVITA. SEVECOM est un projet collaboratif européen qui s'est intéressé à la sécurisation des communications entre véhicules. SHE s'est intéressé à l'ajout de modules matériels aux architectures embarquées automobiles pour accélérer des traitement cryptographiques. Enfin EVITA (E-safety Vehicle Intrusion Trusted Applications), qui est aussi un projet européen collaboratif terminé fin 2011, a défini une architecture automobile sécurisée dans son ensemble : accélérateurs matériels et protocoles de sécurité notamment. Les résultats d'EVITA ont été par la suite largement repris par plusieurs équipementiers, et plusieurs produits « compatibles EVITA » sont actuellement disponibles sur le marché (nous reviendrons là dessus par la suite).

4.1 L'approche EVITA

Avant de rentrer dans des considérations plus techniques, un premier point important pour la sécurisation d'un système automobile concerne le coût. Plus de 80 millions de véhicules sont produits par an par l'ensemble des constructeurs automobiles ; dont environ 2 millions en France (ce chiffre est en baisse en France d'année en année car les constructeurs français augmentent leur production à l'étranger). Si l'on accepte de donner 1 euro par ECU pour sa sécurité, soit 100 ECU par véhicule et 80 millions de véhicules : le coût représente 8 milliards d'euros par an, et ce n'est là que le coût de production (hors conception, maintenance, etc.). Bref, vous allez le voir, l'approche EVITA est sensiblement onéreuse … Le coût n'est pas forcément la seule difficulté pour intégrer la sécurité : la consommation d'énergie, les problématiques d'intégration avec des équipements non compatibles EVITA sont d'autres obstacles. Une difficulté importante est d'assurer la compatibilité entre la sécurité et la sûreté de fonctionnement. Par exemple, la sécurité ralentit forcément l'échanges de données : elle augmente donc la latence, y compris des messages critiques, comme par exemple, un ordre de freinage ...

EVITA ne s'intéresse pas aux attaques dites par les canaux cachés : analyse de la consommation d'énergie ou rayonnements électromagnétiques par exemple. EVITA considère un attaquant dit Dolev-Yao qui peut écouter le trafic et injecter des données sur les bus. Afin d'éviter que le bus « mémoire » d'un processeur puisse être espionné par cette technique, EVITA intègre sur la même puce le processeur et une mémoire embarquée. Par contre, toutes les données qui sortent de cette puce sont chiffrées, authentifiées et rendues intègres. Les échanges de données sont réalisés au travers de protocoles de sécurité qui ont été prouvés corrects mathématiquement, en prenant comme hypothèse que les algorithmes de sécurité eux-même (par exemple, AES) sur lesquels reposent les protocoles sont parfaits du point de vue sécurité. Les protocoles de

sécurité concernent aussi les communications avec le monde extérieur, comme par exemple la mise à jour à distance du firmware des ECUs ou le protocole de démarrage des ECUs qui assure la confiance dans le code démarré sur la plate-forme environnante. Enfin, les domaines sont isolés entre eux à l'aide d'un firewall dont la configuration est mise à jour dynamiquement, en fonction des conditions d'utilisation du véhicule. Le firewall peut aussi être utilisé pour faire de la détection d'intrusion, et remonter ainsi des alertes : un mode dégradé est suggéré lorsqu'une attaque est détectée.

Outre ce qui vient d'être décrit, EVITA met l'accent sur deux aspects des architectures embarqués :

- **L'ajout d'un module de sécurité** aux ECUs, appelé **HSM** – Hardware Security Module. En effet, l'architecture décrite ci-dessus oblige à l'exécution fréquente d'algorithmes cryptographiques, à utiliser des clés, à générer des nombre aléatoires, etc. Afin de réduire le coût des HSM, et selon la nature de l'ECU visé, trois accélérateurs ont été définis : une version légère, une version intermédiaire, et une version complète (voir la figure 3). La version légère vise les ECUs simples (un capteur avec un microcontrôleur basique). Dans tous les cas, EVITA recommande naturellement d'intégrer le HSM et le processeur / microcontrôleur sur la même puce.

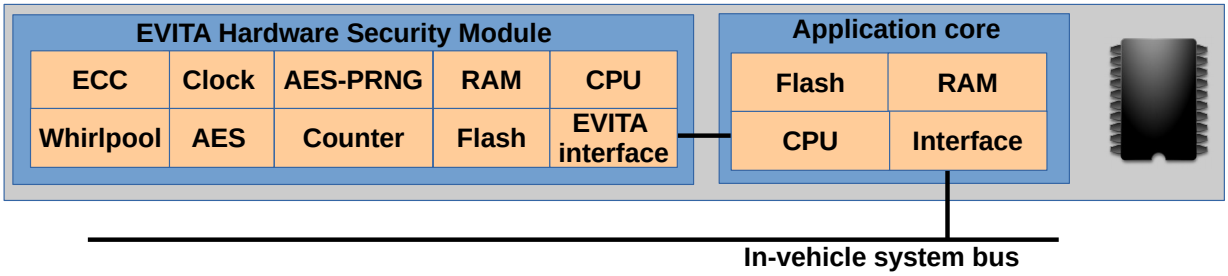

Fig. 3 : Spécification du module de sécurité EVITA complet (« Full HSM »). Le module HSM et le processeur d'applications sont implantés dans la même puce matérielle.

- **La distribution périodique de clés de sessions entre ECUs utilisées pour le chiffrement, l'authentification, et l'intégrité**. Ces clés de sessions sont utilisées au sein de groupes de communication qui sont mis à jour en fonction du véhicule. Par exemple, si la climatisation n'est pas en route, certains groupes de communication lui correspondant ne seront pas créés, et aucune clé ne sera générée pour ce groupe. Ces clés ont une durée de vie de deux heures : elles sont d'abord créées à la mise en route du service correspondant, puis renouvelées selon les besoins. Cette durée de deux heures est due au fait que les clés sont utilisées aussi pour les calculs de MAC (intégrité des messages). Or, le bus CAN ne supportant que des messages relativement courts, et chaque message comportant ainsi un MAC anormalement raccourci, une attaque brute-force pourrait permettre de créer une collision : cette durée de vie de deux heures a pour objectif de rendre extrêmement difficile une telle attaque. Notons que l'utilisation de bus plus récents – de type Ethernet - modifierait ce besoin en renouvellement de clés. Par contre, le bus Ethernet ne sait pas gérer de façon native différents types de trafic et ne peut donc pas forcément s'accommoder de trafic temps-réel. Il est toutefois fréquemment utilisé dans les systèmes avioniques, mais des calculs du scénario pire cas sont réalisés afin de s'assurer que le bus peut toujours acheminer le trafic en respectant ses spécifications temps-réel.

4.2 Les solutions commerciales

EVITA (et SHE) servant de facto de standard, différents équipementiers proposent des ECUs bâtis sur le modèle EVITA. A ma connaissance, ces produits reprennent avant tout la spécification des HSM tels que définis dans SHE ou EVITA.

Par exemple, la solution d'Infineon AURIX [AURIX 2016] supporte un HSM « EVITA medium » comprenant une accélération matérielle pour l'algorithme AES (EBC, CBC, etc.), permettant de stocker des clés cryptographiques, et intègrant un module pour la génération de nombres aléatoires. Cet HSM permet aussi éventuellement de supporter un processus de boot sécurisé. Le module matériel est de plus protégé par un firewall interne.

STMicroelectronics a aussi annoncé en 2015 la commercialisation future d'une solution matérielle reprenant la spécification HSM medium de EVITA [STM 2015]. Freescale, Bosch et d'autres fabricants d'ECUS ont aussi des solutions reprenant les spécifications de SHE/EVITA, alors que d'autres équipementiers s'intéressent aux couches logicielles d'interface avec les HSM (par exemple : Escrypt).

5 Et les véhicules autonomes ?

Un véhicule autonome est capable de se conduire lui-même sans intervention humaine. Un véhicule autonome comprend trois grandes fonctions (voir la figure 4) : la récupération d'information sur l'environnement (aussi appelée « perception »), la décision d'une trajectoire (« planning ») et enfin la réalisation de la trajectoire (l' « action »). En anglais, l'on parle de « sense, understand/decide, act ».

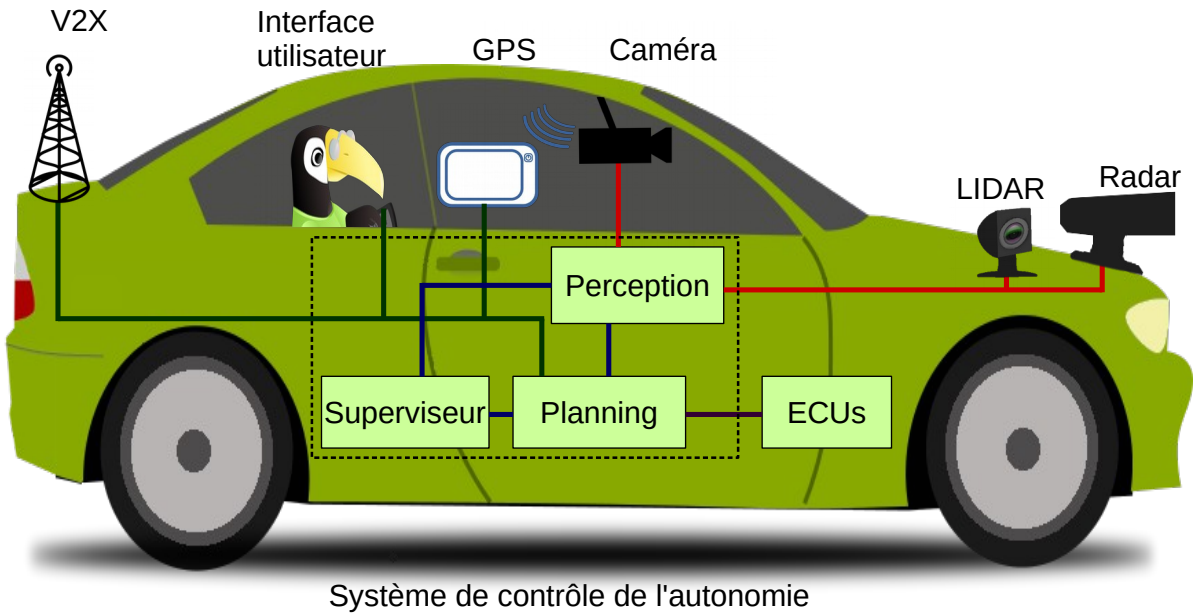

Fig. 4 : Architecture d'un véhicule autonome : capteurs et traitement.

En cas d'urgence, un conducteur doit pouvoir reprendre la main à tout moment : la voiture est alors une voiture classique. Mais, par le fait qu'elle comporte un mode « autonome », cela veut dire que les aspects conduites de la voiture sont intégralement robotisés. Dit différemment, l'ensemble des fonctions de la conduite (accélération, freinage, direction) sont accessibles de façon électronique/informatique.

Mise à part les fonction classiques, une voiture autonome offre deux surfaces d'attaques supplémentaires, qui peuvent avoir un impact sur la sûreté de fonctionnement :

- La manipulation de l'environnement peut conduire au choix d'une mauvaise trajectoire, ou plus généralement d'une mauvaise décision par le véhicule.
- La robotisation totale du véhicule peut permettre à un attaquant de potentiellement manipuler l'ensemble des fonctions de conduite du véhicule.

5.1 Manipulation de l'environnement

La manipulation de l'environnement peut viser un capteur en particulier, ou l'ensemble de la perception véhiculaire (voir la figure 5). Voici quelques exemples.

- L'attaque des communications V2I. L'interconnectivité forte des véhicules autonomes, notamment avec les systèmes d'information V2I (trafic, travaux) permettra un meilleur choix sur les routes empruntées. Ce système pourrait faire l'objet d'attaques, par exemple afin de forcer le guidage du véhicule vers un point précis - via la manipulation des informations trafic - afin de réaliser par exemple un « car hijacking » dans un lieu privilégié.
- L'attaque des dispositifs de vision (radars, lidars, caméras). Différentes techniques ont été publiées récemment, par exemple à BlackHat Europe 2015 [PETIT 2015]. Les attaques mentionnées concernent notamment le fait d'aveugler des caméras et d'ajouter des échos indésirables à des LIDARs.
- Le brouillage du signal GPS. Cela a en fait relativement peu d'importance puisque le véhicule est capable de se débrouiller sans signal GPS (par exemple, lors des traversées de tunnels), mais cela

pourrait amener le véhicule à adapter sa vitesse. Cette technique a été utilisée par des chercheurs de l'Université du Texas : en injectant un faux signal GPS [HUMP 2008], ils ont réussi à montrer le détournement d'un drone (2012) et d'un yacht (2013).

- L'ajout d'éléments à l'environnement difficilement détectables. Par exemple, le fait d'ajouter un piéton en carton sur l'autoroute pourrait mener à des freinages d'urgence en raison d'une mauvaise estimation de la dangerosité.

Contrer ces attaques repose sur la mise en place de capteurs qui prennent en compte leurs attaques, par exemple, des caméras qui résistent mieux à l'aveuglement, et aussi par la mise en place d'algorithmes de corrélations de données. Ces algorithmes de corrélation de données doivent comprendre aussi des mécanismes de détection de manipulation d'un capteur de données afin de l'invalider le temps nécessaire, et aussi d'avertir l'utilisateur. Une corrélation anormale et qui ne peut être corrigée sans tomber dans un nombre de données inférieur au strict minimal doit conduire à un arrêt d'urgence et/ou à la reprise de la conduite manuelle.

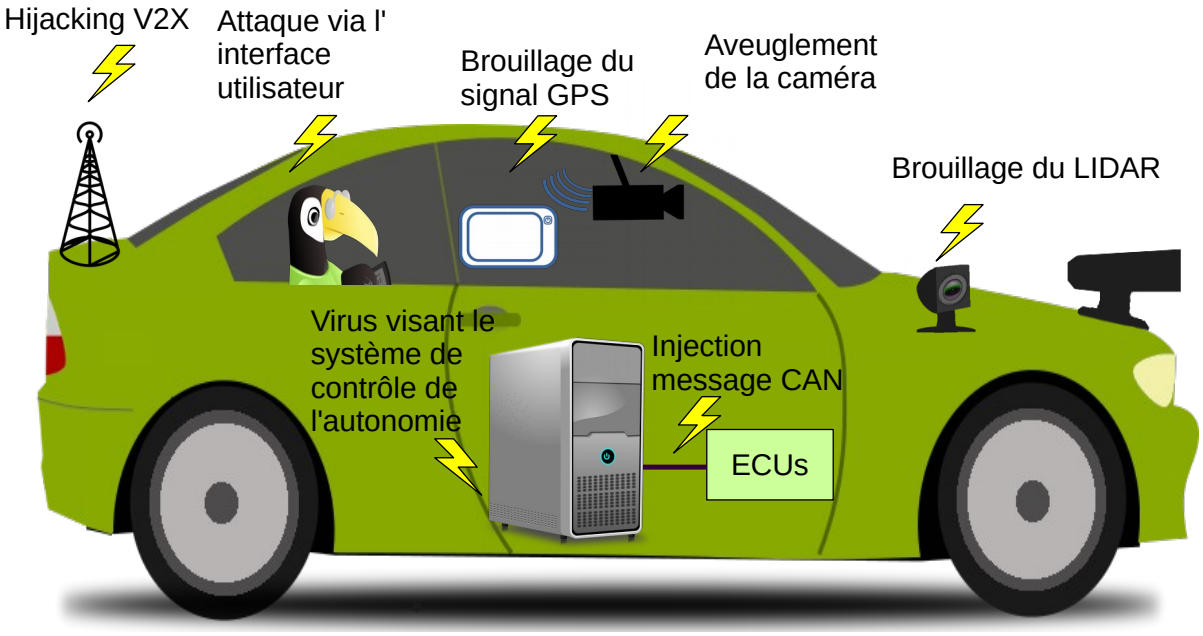

Fig. 4 : Attaques pressenties ou démontrées sur des véhicule autonomes.

5.2 Attaques sur la robotisation

Ces attaques ne sont pas forcément spécifiques aux véhicules autonomes, mais concernent bien entendu tous les véhicules dont des fonctions liées à la conduite sont accessibles électriquement. Des attaques listées dans la section 3 concernent des fonctions vitales, comme l'attaque permettant d'activer à distances des fonctions vitales (comme le freinage). Ce n'est pas tant le « à distance » qui est important, mais le fait que des fonctions vitales soient accessibles par l'informatique sur des véhicules robotisés.

Conclusion

Les attaques sur les systèmes automobiles existent déjà, mais elles ne sont pas a priori pratiquées par des organisation de cyber-criminalité, du moins à grande échelle. La robotisation croissante des véhicules, leur communication avec d'autres objets, ainsi que leur gain en autonomie va forcément augmenter leur surface d'attaque, et ainsi permettre l'apparition d'attaques que l'on retrouve dans d'autres domaines : ransomwares, botnets, et malwares divers.

Références

[AURIX 2016] AURIX™ Security Hardware, http://www.infineon.com/cms/en/product/microcontroller/32-bit-tricore-tm-microcontroller/aurix-tm-family/aurix-security-solutions/hardware/channel.html

[BIMCODING 2016] http://www.bimcoding.com/

[FOSTER 2015] Ian Foster et al, « Fast and Vulnerable: A Story of Telematic Failures », 9th USENIX Workshop on Offensive Technologies (WOOT 15).

[HUNT 2016] Troy Hunt, « Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs », https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

[HUMP 2008] Todd E Humphreys et al., « Assessing the spoofing threat: Development of a portable GPS civilian spoofer », Proceedings of the ION GNSS international technical meeting of the satellite division, Vol 55, p. 56, 2008.

[INS 2016] http://www.instructables.com/id/Hack-Your-Car/

[KAMKAR 2015] Samy Kamkar, "Drive It Like You Hacked It", Defcon 23 (2015), http://samy.pl/defcon2015/

[KOSCHER 2010] Karl Koscher et al, « Experimental Security Analysis of a Modern Automobile », Proceedings of the 2010 IEEE Symposium on Security and Privacy.

[MILLER 2015] Charlie Miller et al, « Remote exploitation of an unaltered passenger vehicle », Black Hat USA, 2015.

[PETIT 2016] Jonathan Petit et al, « Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR », BlackHat Europe, 2015.

[ROUF 2010] Ishtiaq Rouf et al, « Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study », USENIX Security'10.

[STM 2015] http://www.st.com/web/en/press/p3668

[SYSML-SEC] Site Internet de l'environnement SysML-Sec : http://sysml-sec.telecom-paristech.fr/

[VEDECOM] Institut du véhicule décarboné et communiquant et sa sa mobilité (VEDECOM) http://vedecom.fr

[WOO 2015] Samuel Woo et al, « A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN », IEEE Transactions on Intelligent Transportation Systems (Volume:16, Issue: 2).