LES ENJEUX DE LA CYBER SÉCURITÉ DANS LE DOMAINE DES VÉHICULES CONNECTÉS

IMPROVING AND MANAGING CYBERSECURITY INTO CONNECTED VEHICLES

Florian STOSSE,
Franck SADMI, Lucas DUBOC
Bureau Veritas
60 Avenue du Gal de Gaulle
92800 Puteaux

Antoine OLIVIER,
Jean-Christophe TOUVET
Devoteam
73 Rue Anatole France
92300 Levallois-Perret

Résumé

De récentes attaques informatiques médiatisées ont mis en évidence un manque de préparation et d'anticipation du cyber risque dans le domaine automobile. Les nouvelles fonctionnalités des véhicules, marquées par une forte connectivité, impliquent une ouverture sur leur environnement et sont sources de risques d'intrusion. Même si des efforts de standardisation sont en cours, et que la recherche se poursuit au niveau académique, il manque encore des référentiels permettant d'évaluer les efforts déjà entrepris et de réduire les risques à un niveau acceptable. Bureau Veritas et Devoteam se sont associés afin de répondre à ce besoin.

Summary

Recent news-breaking cyberattacks demonstrated a lack of readiness and foresight of the cybersecurity threat in the automotive industry. New embedded functionalities and features of modern connected cars imply new potential attacks and a new battleground. In spite of the current ongoing efforts to bring automotive standards on par with this new threat, and while academics are actively seeking for new solutions, we are still lacking practical guidelines to evaluate and assess the effectiveness of current countermeasures. Bureau Veritas and Devoteam teamed up to tackle this need.

1. Introduction : les problèmes de l'émergence des véhicules connectés

Depuis une dizaine d'années, nous pouvons tous constater que la révolution numérique s'accélère et ne se cantonne plus à nos ordinateurs. L'arrivée de smartphones a offert des possibilités de nomadisme jusque-là insoupçonnées, et l'internet des objets, bien qu'encore balbutiant, promet d'accroître encore plus les capacités numériques des foyers, des villes et des infrastructures. Cette révolution s'accompagne d'ailleurs, comme toute révolution, de nouvelles appellations censées la représenter. Ainsi, les villes deviennent « smart », la gestion de l'énergie devient « smart », les objets deviennent « smart »…

Il n'était qu'une question de temps avant que la voiture, symbole fort de liberté et de différenciation sociale, ne devienne à son tour « smart ». La transition, débutée en 2007 par Ford avec son système Sync puis très vite suivie par tous les autres constructeurs, a permis d'intégrer un ensemble de fonctionnalités inenvisageables ne serait-ce qu'au début des années 2000. Sur la période 2000-2016, la plupart des véhicules ont intégré des systèmes de navigation par satellite, des systèmes de divertissement pour les passagers (i.e. lecteurs DVD pour les places arrière), le Bluetooth ou encore la radio numérique, tandis que les modèles haut de gamme actuels offrent en standard des hotspot Wi-Fi et des connexions au réseau cellulaire.

L'intégration de capacités communicantes au sein des véhicules et des infrastructures (V2V et V2I), ainsi que l'arrivée prochaine des capacités de conduite autonome, qui sont des enjeux majeurs pour les industriels, ouvrent de nombreuses portes aux potentielles agressions extérieures, du même ordre que celles qui affectent aujourd'hui les ordinateurs ou les smartphones. Le développement des composants automobiles doit donc intégrer dès à présent une dimension « cyber sécurité », afin de permettre aux industriels du secteur d'identifier correctement les menaces et de mettre en place des mesures de sécurité adaptées à cette nouvelle problématique.

De récents exemples très médiatisés impliquant de grands constructeurs illustrent bien ce risque qui pèse non seulement sur la sécurité des usagers mais aussi sur l'image de marque et les finances des constructeurs :

- Une faille affectant un industriel américain a récemment connu un retentissement médiatique certain, puisque, au-delà des aspects techniques de l'exploit, elle permettait à l'attaquant de prendre le contrôle total du véhicule à distance, à l'arrêt ou en mouvement. C'est actuellement le pire scénario envisageable, puisque tous les risques identifiables peuvent se réaliser : vol, espionnage économique et industriel, destruction du bien ou encore dommages corporels…

- Un grand constructeur allemand a également eu quelques déboires avec son système d'« infotainment » communicant, puisque celui-ci était vulnérable aux attaques de type Man-in-the-Middle et permettait aux attaquants de déverrouiller le véhicule. Cette faille, bien que corrigée par une mise à jour plus d'un an après sa découverte, a affecté 2.2 millions de véhicules.

- Un constructeur japonais a très récemment (février 2016) vu la dernière-née de sa gamme électrique faire la une de la presse spécialisée après les révélations de Troy Hunt, un chercheur en sécurité informatique, concernant la vulnérabilité de certaines APIs permettant de contrôler les fonctionnalités de la voiture via son smartphone. Même si

les fonctions accessibles via ces APIs sont assez limitées (contrôle de la climatisation et de la température, etc.), il était possible d'accéder à un nombre conséquent de voitures à travers le monde, puisque les requêtes s'appuyaient sur le VIN (Vehicle Identification Number) et que la liste de ces derniers est facilement énumérable. En outre, les requêtes faites aux serveurs du constructeur n'étaient pas chiffrées, et dévoilaient notamment l'identifiant de l'utilisateur associé à la voiture, qui est lui-même dérivé du nom du propriétaire. [1]

Ces exemples ne sont que les prémisses d'une question qui deviendra vite centrale pour les constructeurs automobiles. En effet, le public est de plus en plus demandeur de ces évolutions technologiques [2], mais ne semble pas prêt à en assumer les risques, ce qui va induire un véritable besoin d'intégration de la sécurité informatique dans les véhicules dès la conception.

Enfin, l'émergence des véhicules autonomes (Figure 1 : US National Highway Traffic Safety Authority (NHTSA) Levels of Vehicle Autonomy.) va poser des questions sur la responsabilité légale de la voiture, et donc de son constructeur, en cas d'accident. Cette responsabilité ne pourra être assurée et garantie qu'au moyen de mécanismes de sécurité forts intégrés dans les véhicules.

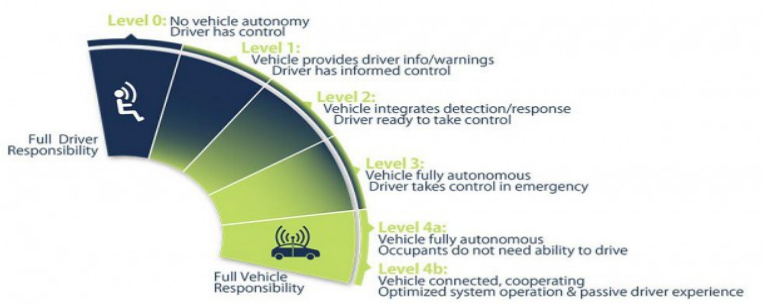


Figure 1 : US National Highway Traffic Safety Authority (NHTSA) Levels of Vehicle Autonomy.

2. État de l'art

2.1 Attaques connues et dangers associés

Le premier risque venant à l'esprit est une prise de contrôle pirate d'un véhicule afin de le rendre inopérant, voire de provoquer un accident. Néanmoins, il serait réducteur de considérer cette prise de contrôle sans s'intéresser aux motivations animant les pirates. Au fur et à mesure de discussions avec des parties prenantes et des experts de ce domaine, nous pouvons faire émerger de nombreux autres scénarios (Tableau 1 : Exemples de scénarios), qui doivent être pris en compte dès maintenant.

Leur impact varie en fonction de la simplicité de mise en œuvre, des conséquences sur les différents acteurs (véhicule, occupants, constructeurs, infrastructure, …) et du nombre de véhicules potentiellement impactés.

Scénario	Motivations spécifiques (non exhaustives)	Conséquences (non exhaustives)
Intrusion par l'accès Internet de divertissement ou de maintenance (Bluetooth, GSM, Wi-Fi) et prise de contrôle des organes de commande (moteur, freins, direction…)	Volonté de nuire à l'image du constructeur, terrorisme	Accident (forte probabilité)
Diffusion de logiciels malveillants (bombe logicielle ou autre) dès la mise en production ou via le système de mise à jour (maintenance par le garagiste)	Idem	Immobilisation du véhicule, accident…
Envoi de messages routiers falsifiés vers les systèmes dits « intelligents » d'assistance à la conduite	Idem	Gêne à la circulation, accident possible
Prise de contrôle à distance ou espionnage du système de navigation (via Google send-to-car etc.)	Banditisme (diriger le véhicule vers un guet-apens, le localiser…)	Vol du véhicule, atteinte à la sécurité des passagers
Voitures partagées : récupération de données personnelles d'autres utilisateurs via une faille dans les solutions d'accès à distance de la voiture (GSM, Bluetooth, Wifi, …)	Espionnage	Atteinte à la vie privée
Prise de contrôle des systèmes antivol et de démarrage du véhicule via la prise de diagnostic ou par exploitation d'une faille dans le système « sans clé » (clonage, faiblesse cryptographique…)	Banditisme	Vol du véhicule
Accès aux paramètres du véhicule via la prise de diagnostic ou l'accès Internet de maintenance (GSM, OBD, USB port, Bluetooth, Wifi, …)	Modification des paramètres (amélioration des performances du moteur, changement des valeurs du compteur kilométrique, etc)	Financières (limitées), perte d'image, escroquerie
Intrusion dans les organes de contrôle du véhicule via l'insertion d'un périphérique USB exploitant une faille du système de divertissement	Idem intrusion via la prise de diagnostic	Idem intrusion via la prise de diagnostic

Tableau 1 : Exemples de scénarios

Ces scénarios doivent également nous amener à réfléchir sur les acteurs des piratages. A l'heure actuelle, les piratages publiés et expliqués sont techniques et exploitent des failles de l'architecture ou de l'implémentation des systèmes de bord. Les développeurs, administrateurs des sites de fabrication et garagistes sont également des vecteurs de menace.

Face à ces menaces, des solutions apparaissent afin de durcir le cœur informatique des équipements automobiles. C'est le cas avec QNX Neutrino, un système d'exploitation complet, robuste et sécurisé appartenant à Blackberry. Il évolue à très bas niveau pour répondre aux besoins des systèmes temps réel embarqués. La force de QNX Neutrino réside dans le fait que chaque pilote, application, appel système et protocole fonctionne indépendamment des autres (sandboxing) ce qui garantit un système stable même si un processus échoue. Nous imaginons aisément que Tesla, Google ou Apple développent des systèmes similaires.

Si elles apportent un début de solution nécessaire, ces réponses ne sont pas suffisantes. La compromission de la Jeep Cherokee en 2015 par deux chercheurs américains est l'exemple le plus marquant de ces derniers mois. Ce véhicule était équipé de BlackBerry QNX, qui est resté intègre et n'a pas été piraté [3]. Les attaquants ont exploité des failles sur les fonctionnalités ajoutées au-dessus de ce système par le constructeur.

Lors de ce piratage, les chercheurs ont réussi à prendre le contrôle sur plusieurs éléments critiques du véhicule, à distance et sans aucune intervention physique sur la voiture. Ils ont également précisé qu'il aurait été possible de transformer le véhicule en ver informatique, c'est-à-dire de s'en servir comme relais pour chercher et infecter tous les autres véhicules vulnérables. Suite à ces révélations, Jeep a rappelé 1,4 millions de véhicules vulnérables [4]. Le tableau ci-dessous (Tableau 2 : Les différentes étapes du piratage de la Jeep) reprend les étapes pour la prise de contrôle du véhicule.

Étape	Composant	Faille
1. Identifier la cible	Réseau GSM Sprint	Possibilité de scanner les plages IP de Sprint à la recherche d'un port spécifiquement ouvert sur les véhicules (port 6667)
2. Envoi de commandes au Head Unit	Puce OMAP	Port 6667 ouvert (bus de communication inter-processus) et joignable
3. Contrôle du système UConnect	Head Unit	Une méthode execute() est disponible pour exécuter du code arbitraire : Possibilité de contrôler la climatisation, l'affichage, …
4. flash du firmware d'une puce accédant au CAN	Puce V850	Possibilité de modifier un exécutable appelé par défaut
5. Effectuer des actions physiques	CAN	Utilisation de la chaîne pour envoyer des messages CAN

Tableau 2 : Les différentes étapes du piratage de la Jeep

La même équipe s'est ensuite procurée une « valise » de garagiste et a réussi à flasher, c'est-à-dire à changer le firmware des ECU. L'équipe précise aussi que le fait que la direction soit contrôlable par des messages envoyés sur le CAN n'était pas possible sur des versions précédentes, ce qui laisse entendre que des nouvelles fonctionnalités sont aussi sources de failles. Ce point pose aussi la question de la robustesse de la validation pour s'assurer de la non régression.

En parallèle, il n'est pas nécessaire d'avoir des connaissances avancées pour s'initier à ce genre d'attaques. Il est possible de suivre et de contrôler les paramètres de certains véhicules commerciaux équipés d'un boîtier vulnérable [5].

Depuis plusieurs années maintenant, les véhicules haut de gamme peuvent être démarrés en quelques secondes via des boîtiers vendus au marché noir[6]. Ces équipements ne nécessitent aucune connaissance particulière et, même si leur impact est limité au fait que l'on ne peut démarrer qu'une seule voiture à la fois, ils démontrent bien l'existence de failles sérieuses au démarrage du véhicule.

La plupart des failles techniques présentées ici sont assez basiques et auraient pu être détectées et corrigées si une analyse structurée, sinon exhaustive, avait été menée. Pour ce faire, il faut prendre en compte le nombre d'intervenants lors de la réalisation d'un véhicule. Les constructeurs écrivent leurs propres programmes, mais ils achètent également des composants qui contiennent leur propre firmware, et incluent des briques logicielles tierces (typiquement BlackBerry QNX), quand ce n'est pas un programme développé en partenariat avec un concurrent.

2.2 Prise en compte de la cyber sécurité dans les normes automobiles

Face à ces différentes attaques, il semble clair que la sécurité doit être prise en compte et intégrée à chaque étape du développement du véhicule, ainsi que sur tout son cycle de vie. La norme ISO26262, qui adresse la sécurité fonctionnelle des véhicules (et non la cybersécurité), se démocratise rapidement chez les constructeurs automobiles et semble la mieux positionnée pour intégrer de façon incrémentale différentes exigences concernant la cyber sécurité (le working group n°8 (ISO/TC 22/SC 32/WG 8) y travaille activement).

La SAE International (ex-Society of Automotive Engineers) a de son côté décidé de prendre les devants et de publier son propre standard, le J3061, qui s'appuie sur la structure actuelle de l'ISO 26262 pour proposer des mesures applicables aux véhicules en cours de développement. Ce standard propose deux façons différentes d'intégrer la cyber sécurité dans les phases de développement :

- en combinant complètement les processus de safety et de security,
- en parallélisant ces deux processus, tout en créant des points de jonction à différentes étapes du cycle en V.

Ces approches permettent d'intégrer la sécurité dans la plupart des cycles de développement actuellement en place au sein de l'industrie, que ce soit chez les constructeurs, mais également chez les partenaires et les équipementiers.

Il est cependant important de noter que ces efforts d'intégration de la cyber sécurité au sein des normes internationales sont encore très récents et vont demander un certain temps de maturation. La nécessité d'aller vite dans le déploiement de solutions de sécurité, imposée par un parc automobile hétérogène et déjà communicant (et donc potentiellement vulnérable), a conduit les industriels et les chercheurs à lancer des initiatives à la marge du processus de normalisation, comme par exemple ACES [7] ou le projet de recherche européen EVITA [8].

2.3 Autres domaines

Pour la sécurité des systèmes d'informations, l'industrie s'appuie principalement sur les normes ISO2700X, qui sont indépendantes des technologies utilisées. Elles définissent un ensemble de principes, fonctionnalités, contraintes et de contrôles nécessaires pour assurer la sécurité du système. A ces normes sont attachées des certifications, qui concernent :

- les systèmes informatiques, avec un périmètre défini : IS27001, SOC 2, ISAE Type 2, …
- les personnes : ISO27001 Lead Implementer, CISSP, …
- les personnes testant ces systèmes : SANS, Certified Ethical Hacker, …

Ces référentiels sont organisés en chapitres couvrant aussi bien les réseaux que la journalisation, les systèmes, la sécurité physique ou encore la continuité d'activité en cas de défaillance.
Pour résumer, il y a une vraie approche globale de la sécurité, qui tente d'appréhender les concepts techniques aussi bien que les processus, que ce soit en interne ou avec les fournisseurs. Malgré la maturité de ces référentiels, il n'en reste pas moins que les exigences identifiées sont génériques et ne sont pas adaptées aux spécificités du domaine automobile.

De la même manière, l'IEC 62443, « INDUSTRIAL NETWORK AND SYSTEM SECURITY ", qui adresse les problématiques de cyber sécurité des systèmes industriels, n'est pas complètement terminée (à ce jour) et a une approche générique pour les grands systèmes industriels.

Finalement, dans les domaines ferroviaires ou aéronautiques où la sécurité fonctionnelle est maîtrisée depuis plusieurs années, la cybersécurité est gérée de manière indépendante avec des règles qui dépendent largement de l'implication de l'industriel. Effectivement les référentiels applicables dans ces domaines (DO-178, DO-254, ARP-4754 et ARP 4761 pour l'aéronautique et EN 5012x pour le ferroviaire) ne spécifient rien sur la cyber sécurité.

3. Solutions

3.1 PDCA

L'approche Plan-Do-Check-Act, ou Planifier-Développer-Contrôler-Ajuster (PDCA) est un cycle permettant la résolution de problèmes et la gestion du changement de manière continue et efficace. Elle permet de s'assurer que les nouveautés sont correctement testées avant d'être implémentées en offrant une structure au changement. Cette méthodologie est notamment préconisée par la norme ISO27001:2005, référence en matière de sécurisation des systèmes d'information. Nous allons étudier son application à la sécurisation des véhicules connectés.

3.1.1 PLAN

Le véhicule est sujet à des cybers attaques à cause de la présence de vulnérabilités dans son architecture ou de faiblesses dans les implémentations. L'objet de cette phase est d'identifier les risques potentiels, de décider lesquels adresser et comment, puis de définir un objectif de risque résiduel après changements.
Nous pourrons pour cela utiliser, entre autres, la modélisation présentée en 4.1 et une liste des vulnérabilités les plus communes.

Concrètement, en reprenant le scénario déroulé dans l'exemple de la Jeep précédemment, nous obtenons le tableau simplifié (Tableau 3 : Tableaux des vulnérabilités réelles) suivant :

Exemple de vulnérabilités	Exemple de solution
Possibilité d'identifier l'adresse IP des voitures	Sécuriser le réseau
Dépassement de mémoire possible sur une puce	Corriger le code du firmware
Les ECUs ne prennent pas en compte le contexte	Détecter les messages anormaux sur le CAN

Tableau 3 : Tableaux des vulnérabilités réelles

3.1.2 DO

Les mesures décidées à l'étape précédente doivent maintenant être implémentées. Ces mesures peuvent avoir pour but de réduire le risque, de l'éviter ou de l'externaliser. Par exemple, on peut :

- modifier la table de routage pour rendre impossible l'identification de l'adresse IP des véhicules,
- corriger le dépassement mémoire,
- implémenter un système de détection de messages de coupure du moteur alors que la voiture se déplace.

3.1.3 CHECK

Il convient maintenant de vérifier l'efficacité de mesures décidées et implémentées. Des tests d'intrusion ciblés menés par un « white hat »[1] permettront de contrôler l'efficacité des mesures mises en place, tout en détectant d'éventuels effets de bord. La mise à jour de la modélisation listera tous les scénarios impactés par la modification. Il faut tous les tester afin de vérifier que cela correspond bien aux objectifs de risques résiduels définis dans la phase « Plan ».

Dans notre scénario, cela revient à rejouer le scénario du piratage à l'identique, puis sur chaque composant modifié individuellement. Il est également possible d'inclure des variations du scénario afin de détecter des effets de bord.

Nous pouvons également envoyer des messages anormaux aux ECU pour voir si une alerte est remontée.

3.1.4 ACT

Cette partie prépare le redémarrage du cycle PDCA. Si les tests d'intrusion montrent que la correction n'efface pas le risque, ou que le système de détection de messages anormaux aux ECU ne remonte pas d'alerte, il va falloir décider quoi faire et planifier de nouvelles modifications.

3.2 Rapprochement avec l'ISO 26262

L'ISO 26262 est la norme internationale de sécurité fonctionnelle pour les véhicules routiers à 4 roues de moins de 3,5T pour la version en cours de 2011. Une mise à jour de la norme est en cours d'élaboration pour prendre en compte les 2 roues et les camions (prévue pour 2016).
Cette norme couvre l'ensemble des composants du véhicule avec une approche fonctionnelle, système, logicielle et matérielle. Elle contient des exigences sur toutes les phases de vie du système allant du concept à l'exploitation en passant par le développement et la fabrication (et aussi démantèlement). Cette norme contient 10 volumes.

La démarche générale préconisée en termes de sécurité fonctionnelle est présentée ci-dessous :

- Gestion de la sécurité fonctionnelle,
- Analyse de sécurité avec une approche fonctionnelle,
- Réalisation de concepts de sécurité pour les fonctions véhicule puis sur les éléments les réalisant,
- Spécification des exigences de sécurité pour le développement puis vérification et validation de l'ensemble,
- Recommandations particulières sur la production et l'exploitation du véhicule.

Cette norme permet donc d'appréhender l'ensemble des phases de vie des différents types de composants du véhicule. D'un point de vue réglementaire, la mise en œuvre de cette norme n'est pas encore obligatoire. Cela étant, les constructeurs imposent le respect de cette norme dans leur cahier des charges. Les exigences de cyber sécurité peuvent s'inscrire dans ce processus de développement ayant déjà fait ses preuves.

L'approche PDCA exposée ci-dessus (Cf. « §3.1 PDCA») peut s'intégrer dans l'organisation ISO 26262 comme suit :

- Concernant l'activité « Plan », de manière analogue à la sécurité fonctionnelle, les dangers (Cf. « §2 État de l'art ») de type cyber sécurité peuvent être identifiés lors de l'activité « Hazard analysis and risk assessment » (Partie 3.7 de la norme) pour identifier les risques. En fonction de cette liste, une différentiation peut être menée pour gérer les exigences cybersécurité et sécurité fonctionnelle.

- Pour l'activité « Do », l'ISO 26262 préconise une analyse de risques pour chaque niveau du cycle de vie de la sécurité fonctionnelle, i.e. de la fonction (Partie 3 « Concept Phase ») aux composants élémentaires (Partie 5 « Product development at hardware level » et Partie 6 « Product development at the software level ») en passant par le système (Partie 4 « Product development at the system level »). Lors de ces analyses de risques avec pour objectif la sécurité fonctionnelle, des analyses cyber sécurité peuvent être réalisées pour mettre en évidence des contre-mesures à implémenter.

- Pour l'activité « Check », les activités ISO 26262 liées aux tests et à la validation peuvent permettre de couvrir les Penetration Tests ou Pen-tests. Avec l'approche top-down de la norme, cette activité de Pen-tests peut être décomposée au niveau véhicule, ECU et réseaux.

- Pour la partie « Act », elle est directement intégrée dans le processus de sécurité fonctionnelle qui implique une vérification systématique des résultats et l'adoption de mesures adaptées en cas de non atteinte de l'objectif.

Concernant les spécificités du véhicule sur la fabrication et l'exploitation (Partie 7 « Production and operation »), des analyses spécifiques cybersécurité peuvent être réalisées pour diminuer l'exposition du véhicule ou alors contraindre son utilisation avec

[1] Professionnel de la sécurité testant la sécurité des systèmes à des fins légitimes de sécurisation, par opposition aux « black hat », des attaquants aux intentions illégitimes.

des moyens sécuritaires. Effectivement ces phases spécifiques ont la particularité d'exposer le véhicule au monde extérieur non maitrisé, ni sécurisé (garagistes, concessionnaires et utilisateurs).

Le rapprochement sécurité fonctionnelle et cyber sécurité sur un support ISO 26262 est donc possible. Il est souvent question d'incompatibilités entre certaines exigences cyber sécurité et sécurité fonctionnelle. Par ce rapprochement en termes d'organisation et d'activités menées en parallèle, des solutions optimales pourront être trouvées au plus tôt.

4. Technique(s) de modélisation

4.1 Méthode / innovation

Un véhicule est un système extrêmement complexe, comprenant des centaines, voire des milliers, d'éléments hardware ou software susceptibles de contenir une ou plusieurs vulnérabilités.
Des milliers de modèles de véhicules différents existent, chacun contenant différentes options ajoutant ou retirant des sous-systèmes.

Face à cette complexité, nous proposons une modélisation par graphe, afin de représenter de manière la plus exhaustive possible tous les scénarios d'attaque, que ce soit au niveau :

- Des acteurs : développeurs chez le constructeur, pirate externe, utilisateur via la compromission de son smartphone, …
- Des composants : ECU, Head Unit, puce GSM, clé sans contact, …
- Des conséquences : accident, vol du véhicule, perte d'image pour la marque, …
- Des vulnérabilités : port ouvert, débordement mémoire, signal RFID reproductible, …

Il s'agit ensuite d'exploiter cette masse de données pour déterminer, pour un véhicule donné avec des options spécifiques, les scénarios les plus sensibles, ou encore tous les scénarios menant à une conséquence donnée (vol du véhicule), mais également tous les scénarios affectant un composant précis.

La montée en puissance du *Big Data* et de l'*internet des objets* et des outils associés ces dernières années rend cette modélisation possible et exploitable à très court terme.

Une modélisation par graphe comporte deux éléments principaux : des nœuds et des arcs. Chaque nœud comporte des attributs, qui peuvent être différents. Ces nœuds sont reliés entre eux par des arcs, et il en existe potentiellement plusieurs entre deux nœuds donnés. Ces arcs peuvent également porter des attributs, qui peuvent à leur tour être évalués.

La modélisation (Figure 2 : Exemple de représentation graphique possible avec une base de données orientée graphes) est basée sur ces éléments avec des nœuds représentant les acteurs (ou sources de menaces), les composants et les conséquences (ou évènements redoutés). Les arcs portent les vulnérabilités et la potentialité associée. La potentialité est la probabilité la plus élevée de passage d'un nœud à l'autre.

Chaque nœud est relié au suivant par des arcs qui représentent les vulnérabilités affectant le composant cible et qui sont exploitables par une des sources de menaces situées en amont. Les arcs portent une description de la vulnérabilité et une probabilité que celle-ci puisse être exploitée. La probabilité est calculée conformément aux standards de sécurité informatique, comme CVSS [9], en tenant compte notamment de la difficulté d'exploitation de la vulnérabilité.

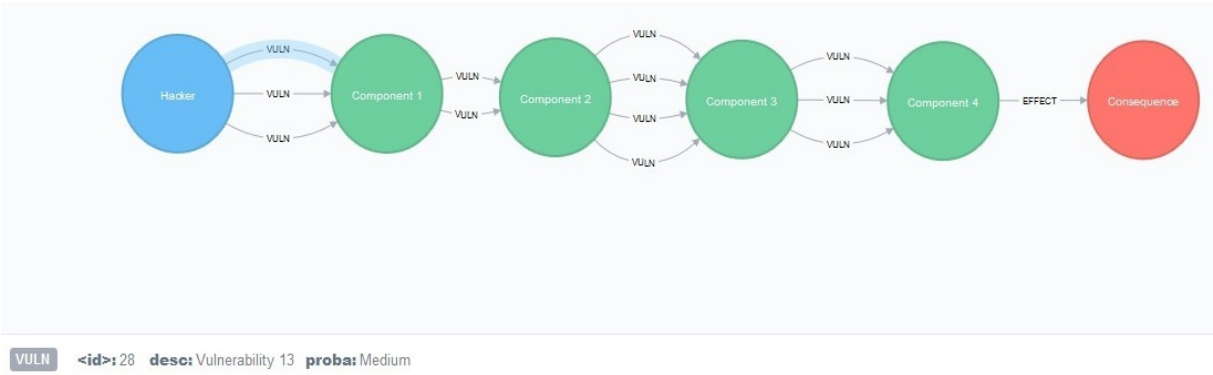
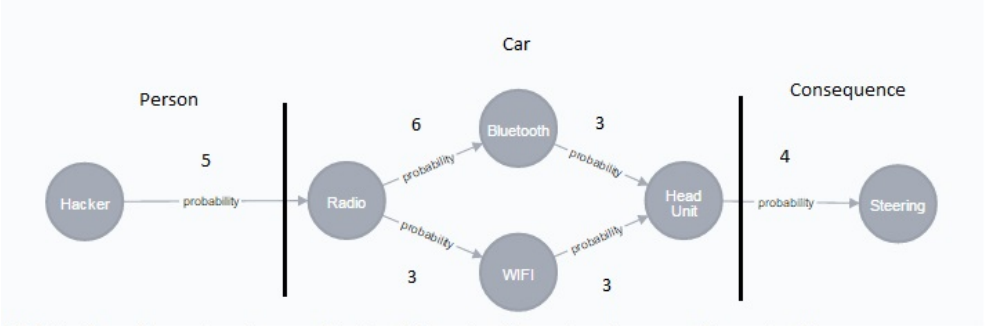


Figure 2 : Exemple de représentation graphique possible avec une base de données orientée graphes

Les potentialités seront calculées de la manière suivante :

- potentialité entre deux nœuds = max(potentialités(vulnérabilités)),
- potentialité totale = min(potentialités entre chaque noeud).

Ci-dessous (Figure 3 : Exemple de modélisation d'une attaque permettant la prise de contrôle de la direction via le Wi-Fi ou le Bluetooth) est présenté un exemple de modélisation ainsi qu'une requête pour calculer la potentialité :




```
MATCH (from:Location { name:'Hacker' }), (to:Location { name: 'Steering'}),
path = (from)-[:probability*]->(to)
RETURN path AS shortestPath,
    reduce(probability = 0, r in relationships(path) | probability+r.probability) AS totalprobability
    ORDER BY totalprobability ASC
    LIMIT 1
```

Figure 3 : Exemple de modélisation d'une attaque permettant la prise de contrôle de la direction via le Wi-Fi ou le Bluetooth

Le croisement entre la potentialité du scénario et le niveau d'impact de l'évènement redouté donne classiquement un niveau de risque, qui permettra par exemple de prioriser les mesures de remédiation.

4.2 Gains attendus pour la modélisation

Le principal gain escompté est une capacité accrue d'automatisation, nécessaire en considérant les dizaines de millions de combinaisons possibles et la transformation de l'industrie automobile. Cette automatisation concerne une quantification du risque.

Cela consiste en :

- Un ajustement automatique des scénarios après avoir associé les valeurs spécifiques à un constructeur/contexte.
- Un ajustement automatique après avoir implémenté des contre-mesures sur un ou plusieurs composants. Si ce composant était impliqué dans plusieurs scénarios, la répercussion sera visible pour tous.
- Un calcul automatique des nouveaux chemins à plus haut risque.
- Un calcul automatique des nouveaux composants à plus haut risque.
- Une vérification des effets de l'ajout d'une contre-mesure, y compris les effets de bord si cette contre-mesure consiste en l'ajout d'un composant (ajout d'un pare-feu par exemple).
- Un ajustement automatique en cas de découverte d'une nouvelle faille sur un composant.

Parallèlement à cette automatisation, un gain est attendu au niveau de la sensibilisation des différents acteurs, car il sera possible de leur présenter une vue adaptée à leur contexte. Dans une industrie où les cycles de changement sont longs, une bonne compréhension des problématiques par les différents acteurs est nécessaire le plus tôt possible. Ce gain s'obtient par une visualisation :

- Dynamique, avec l'affichage d'informations nous concernant directement (épuration des résultats).
- Adaptée au spectateur : PDG, équipe marketing, ingénieur.
- Adaptée au risque que l'on souhaite appréhender/traiter.

Enfin, cette modélisation se veut évolutive, de manière à pouvoir :

- Ajouter des informations sur les nœuds et les arcs, puis modifier les requêtes pour exploiter ces nouvelles informations.
- Gérer un nombre de plus en plus important de données. Là où Excel se retrouve rapidement limité par la puissance de la machine ou de ses mécanismes internes, une solution Big Data peut traiter un nombre potentiellement infini de données.
- Garantir la cohérence, par exemple lors de l'ajout d'une brique logicielle entière (intégration de BlackBerry QNX typiquement).

5. Conclusion

Cet article présente une approche pour aborder un secteur d'activités dynamique et en pleine évolution technologique. Les véhicules proposent de plus en plus de fonctionnalités à fortes interactions avec le monde extérieur, avec une autonomie de plus en plus forte, impliquant un risque cybersécuritaire omniprésent.

Les réglementations actuelles n'ont pas d'obligations sur ce sujet, et les normes existantes appliquées n'adressent pas cette problématique spécifique. En conséquence, il est de la responsabilité de chaque constructeur d'implémenter un niveau de sécurité satisfaisant afin d'assurer non seulement l'intégrité du véhicule et de ses occupants, mais également la confidentialité de ce qui s'y passe et la disponibilité des fonctionnalités.

Le constructeur doit en outre prendre en compte les développements réalisés par ses équipementiers.
Ce chantier a été initié, mais les nombreux piratages récents montrent qu'il reste une grande marge de progression. La sécurité est un processus qui a besoin de maturité et doit considérer l'écosystème du véhicule comme un tout.

Bureau Veritas et Devoteam proposent une méthode pour s'assurer du niveau de sécurité d'un véhicule face à ces nouvelles menaces. Cette méthode est spécifiée dans un guide de bonnes pratiques qui permet d'évaluer un système avec le point de vue constructeur ou d'un équipementier. Ce guide permet d'avoir un référentiel commun d'objectifs.

Ce guide reprend les bonnes pratiques en cyber sécurité à mener sur un véhicule. Il est basé sur ce qui se fait dans d'autres domaines, telle que l'approche PDCA et s'inspire de ce qui se fait déjà dans l'automobile avec la norme ISO26262 afin de simplifier son adoption. L'approche est globale et préconise des mesures à fois organisationnelles et techniques.

Il est aussi basé sur des exigences telles que la vérification de la robustesse d'un système vis-à-vis des attaques les plus fréquentes. Pour cette vérification, nous avons pris le parti d'analyses s'appuyant sur de la modélisation pour faciliter l'évaluation. Les objectifs du guide peuvent s'intégrer dans la démarche ISO 26262 qui est actuellement utilisée par les constructeurs et équipementiers automobiles en sécurité fonctionnelle.

La méthode préconisée permettra de rendre plus sécuritaires les véhicules et offrira aux acteurs automobiles une garantie supplémentaire sur la qualité de leur produit.

6. Abréviations & glossaire

Terme	Définition
API	Application Programming Interface : interface logicielle d'un programme permettant aux développeurs de s'interfacer avec celui-ci.
CAN	Controller Area Network : bus de communication dédié aux véhicules, permettant aux ECUs et périphériques embarqués de communiquer entre eux.
ECU	Electronic Controller Unit : système embarqué au sein d'un véhicule, contrôlant une fonctionnalité
GSM	Global System for Mobile communications : norme numérique de communication pour les téléphones mobiles.
Man-In-The-Middle (MITM)	Type d'attaque où l'attaquant s'intercale sur le canal de communication entre sa cible et le serveur qu'elle cherche à contacter. Cela lui permet d'écouter et d'enregistrer le trafic (recherche de mots de passes, d'informations confidentielles, etc) et de potentiellement le modifier à la volée.
OBD	On Board Diagnostic : prise permettant de dialoguer avec les ECUs du véhicule. Réservé majoritairement aux garagistes pour les opérations de maintenance.
OMAP	Open Multimedia Applications Platform : puce processeur dédié aux applications mobiles. (solutions développées par Texas Instruments)
RFID	Radio Frequency IDentification
USB	Universal Serial Bus : port série couramment implémenté sur les ordinateurs et au sein des véhicules.
V2I	Vehicle to Infrastructure : désigne la communication entre un véhicule et l'infrastructure routière existantes (capteurs sur les feux de signalisation, …)
V2V	Vehicle to Vehicle : désigne la communication directe entre deux véhicules.
VIN	Vehicle Identification Number

7. Bibliographie

[1] T. Hunt, «Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs,» 24 Février 2016. [En ligne]. Available: https://www.troyhunt.com/controlling-vehicle-features-of-nissan/.

[2] R. Viereckl, D. Ahlemann et A. Koster, «Connected Car Study 2015: Racing ahead with autonomous cars and digital innovation,» 16 Septembre 2015. [En ligne]. Available: http://www.strategyand.pwc.com/reports/connected-car-2015-study.

[3] C. Miller et C. Valasek, «Remote Exploitation of an Unaltered Passenger Vehicle,» 2015.

[4] A. Greenberg, «After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix,» 24 Juillet 2015. [En ligne]. Available: https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

[5] J. C. Norte, «Hacking industrial vehicles from the internet,» 6 Mars 2016. [En ligne]. Available: http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html. [Accès le 30 Avril 2016].

[6] France 2 - Auto Plus, «Démarrage de véhicule sans clefs,» Youtube, 2011. [En ligne]. Available: https://www.youtube.com/watch?v=rmTSSKQfy1U.

[7] SwRI, «Automotive Consortium for Embedded Security,» 2013. [En ligne]. Available: http://www.swri.org/4org/d10/comm/aces/.

[8] «E-safety Vehicle Intrusion Protected Applications,» 2012. [En ligne]. Available: http://www.evita-project.org/.

[9] FIRST, «Common Vulnerability Scoring System,» [En ligne]. Available: https://www.first.org/cvss.