Sécurité des véhicules autonomes

Depuis peu, vous pouvez déjà apercevoir sur les routes des véhicules autonomes. Les avantages de ce type de véhicules sont nombreux. On citera les principaux, la diminution du nombre d'accidents, (grâce à un meilleur temps de réaction notamment), la réduction des embouteillages, la réduction de la pollution grâce à une conduite plus intelligente ou encore à la facilitation de la mobilité des personnes. Une des principales interrogations que lèvent les véhicules autonomes se pose : comment ce nouveau type de véhicule va réussir à protéger ses passagers ainsi que lui-même.

Pour commencer, rappelons ce qu'est un véhicule autonome. Un véhicule autonome est un véhicule qui est capable d'effectuer les mêmes actions qu'un véhicule ordinaire, mais sans intervention humaine. Il doit être capable d'aller d'un point A à un point B sans que personne n'ait besoin d'effectuer la moindre action. Cela implique que nos véhicules de tous les jours deviennent autonomes, dotés d'intelligence artificielle. En effet, les véhicules devront respecter le code la route pour éviter tout risque de créer des accidents.

SAE International définit 6 niveaux d'autonomie, allant du niveau 0 au niveau 5. Le niveau 5 définit un véhicule totalement autonome. (Actuellement, nos véhicules sont des véhicules de niveau 2 voire 3).

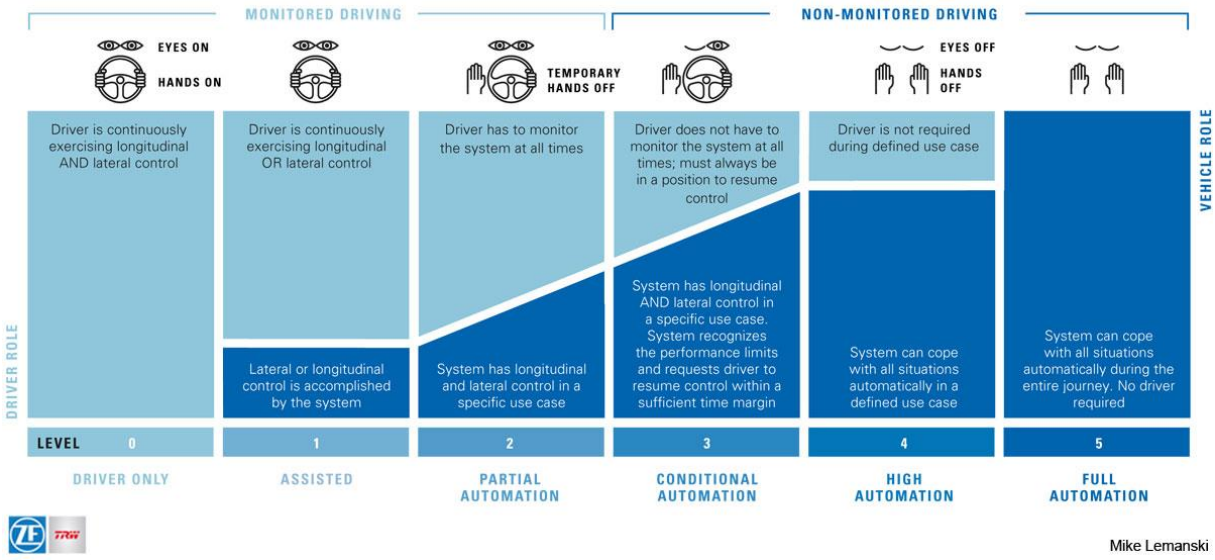

Figure 1 : Schéma SAE International sur les niveaux d'autonomie

Ces niveaux sont basés sur de l'informatisation du véhicule. Sur un véhicule de niveau 5, les décisions ne seront plus prises par un être humain, ce seront des éléments informatiques qui vont décider des actions que devra effectuer le véhicule. Par conséquent, plus il y aura d'informatique dans le véhicule, plus le véhicule deviendra vulnérable à des menaces.

Un véhicule autonome a besoin de cinq éléments sans lequel il ne peut pas fonctionner. Ces éléments sont :

- ➔ Sa perception :
- ➔ Son algorithme de décisions :
- ➔ Ses trois actionneurs (frein, accélérateur et colonne de direction) :

Ce sont ces éléments qui vont être ciblés majoritairement par les attaques.

Plusieurs cas sont déjà révélateurs, comme la Jeep en 2015, ou plus récemment BMW en 2018.

En effet, en 2015, Chris Valasek and Charlie Miller, deux chercheurs en cyber-sécurité ont réussi une performance novatrice dans le domaine : pirater à distance une voiture connectée. Pour ce faire, ils ont ciblé deux éléments du véhicule. Le premier, le multimédia, est considéré comme une porte d'entrée très prisée des pirates. Le multimédia du véhicule se devra d'être connecté et donc ouvert sur l'extérieur. En exploitant une faiblesse dans la sécurité du WIFI du véhicule, les deux pirates ont réussi à s'introduire dans le véhicule.
Une fois introduits dans le véhicule, les deux hackers ont dû trouver un moyen d'agir sur les actionneurs. Pour cela, ils se sont intéressés au bus CAN présent dans le véhicule. Le bus CAN (Controller Area Network) est un bus système série très répandu dans l'automobile ; il permet notamment la communication entre plusieurs éléments du véhicule. C'est là que le deuxième équipement ciblé par Chris Valasek and Charlie Miller entre en jeu. En effet, les actionneurs n'étant pas directement reliés au multimédia (on devinera aisément pourquoi), les deux chercheurs ont dû trouver un moyen de communiquer avec les actionneurs. Après s'être aperçu que le controller V850 pouvait recevoir des trames CAN, les deux chercheurs ont changé le firmware afin de pouvoir cette fois envoyer des trames CAN ; ils ont donc pu atteindre les actionneurs.

Comme rappelé au début de ce document, les véhicules autonomes sont vulnérables à plusieurs types de menaces. Des menaces que l'on connait déjà dans le monde I.T. classique, mais également des menaces nouvelles qui apparaissent grâce à l'émergence des véhicules autonomes. En effet, le vol de données, l'intrusion sur le réseau du véhicule, les dénis de service, etc. sont des menaces que les personnes du monde de la cyber s'emploient à défendre depuis plusieurs années. Cependant, les attaques évoluent au même titre que la technologie, également. Un ransomware par exemple, serait bien plus dommageable et dangereux au vu du nombre de véhicules dans les années futures, de même que des attaques de type Botnet pourraient donner lieu à des attaques simultanées qui serait totalement différentes de ce qu'on connait aujourd'hui.

Pour illustrer ce propos, prenons cet exemple. Les ransomwares actuels demandent généralement des rançons exorbitantes car peu de personnes paient (34% de personnes en 2017). Dans le cas des véhicules autonomes, on dénombrera plusieurs millions de véhicules, le nombre de victimes augmentant, il sera plus facile et plus avantageux de demander une rançon plus faible (ex : 5€ pour débloquer le véhicule).

En conclusion, avec l'arrivée des voitures autonomes, arrivent de nouvelles menaces. Certaines sont des menaces que l'on connait déjà tandis que d'autres sont nouvelles. Il sera donc intéressant de voir comment vont évoluer ces nouveaux systèmes ainsi que les mécanismes de détection et de protection déjà beaucoup utilisés dans l'IT classique d'aujourd'hui.

Bibliographie

https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/
https://www.thesandreckoner.co.uk/self-driving-cars-coming-sooner-think/
https://www.altospam.com/actualite/2017/10/ransomwares-chiffres-statistiques/
https://fr.wikipedia.org/wiki/Bus_de_donn%C3%A9es_CAN

Autobiographie

Je m'appelle Martin Boyer. J'ai passé un BAC scientifique avant de rejoindre l'I.U.T d'Orléans en 2013. En 2015, après l'obtention de mon D.U.T, j'ai décidé de me spécialiser dans la sécurité informatique, domaine que j'avais peu couvert lors de ma précédente formation. J'ai donc décidé de rejoindre l'INSA Centre Val de Loire à Bourges en 2015. C'est d'ailleurs lors de cette formation que j'ai eu l'opportunité de devenir Vice-Président du club Informatique et Sécurité Informatique.

A l'issue de cette formation, j'ai réalisé un stage à l'IRT SystemX qui a clos ma formation. J'ai ensuite été embauché dans cette IRT au sein de l'équipe CTI (Cybersécurité du Transport Intelligent). J'interviens sur les scénarios d'attaques et la détection de ces dernières.

A côté, j'interviens sur des sujets de sensibilisation sur la sécurité informatique et je suis passionné par les nouvelles technologies. J'aime également effectuer de la veille technologique.