EN QUOI AUGMENTED SECURITY PEUT SERVIR LE MONDE DE L'AUTOMOBILE

L'industrie automobile est une grosse consommatrice de logiciels que ce soit des logiciels de gestion de clientèle, gestion des stocks, conception de pièces etc. Kompass en affiche 107 différents.

Quant à la cybercriminalité de l'automobile, tout le monde s'y met depuis Kaspersky jusqu'aux plus grands comme Apple, Oracle, EMC Symantec, SAP, CapGemini depuis longtemps. Il n'y a qu'à lire les nombreux communiqués de presse qui sortent actuellement. La Guerre en Ukraine y serait-elle pour quelque chose ? Ci-dessous des extraits d'un article de Wikipedia qui est édifiant :

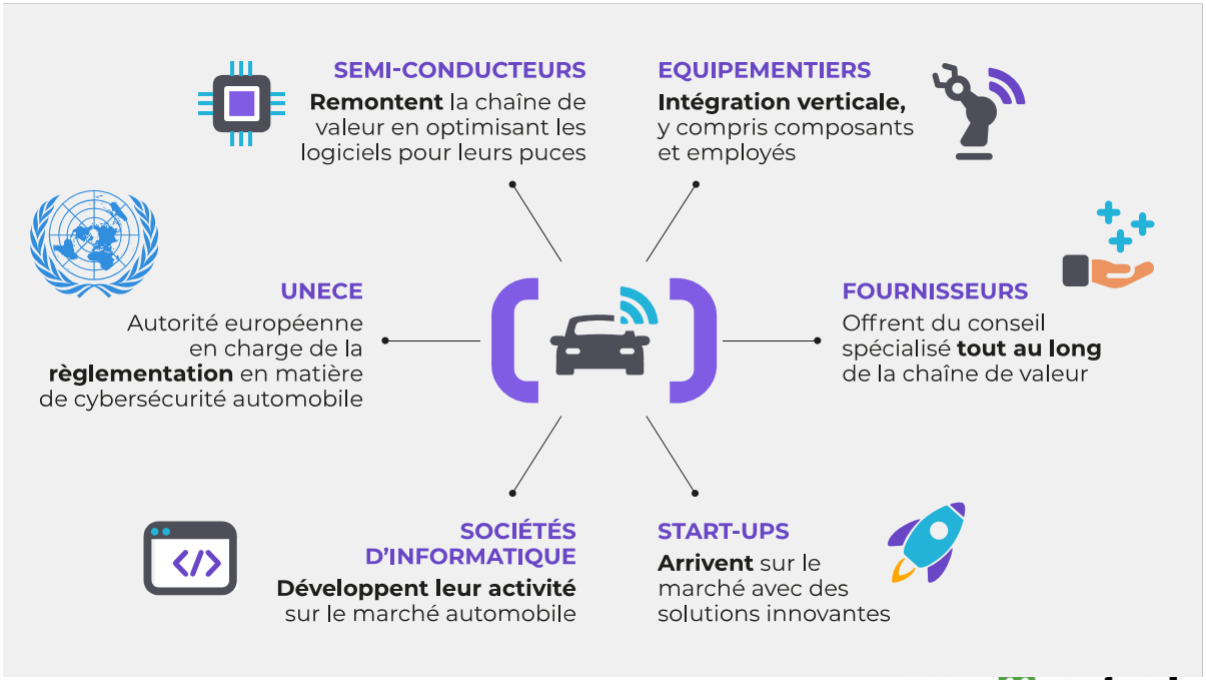
*« La **sécurité informatique des véhicules** est un enjeu majeur des véhicules automobiles modernes. Cet enjeu est pris en compte dès la conception des systèmes embarqués.*

Le véhicule connecté est contrôlé par des calculateurs embarqués et interconnectés (ECU). À travers ces calculateurs, le véhicule moderne offre des fonctionnalités nouvelles qui améliorent la qualité de conduite et renforcent la sécurité du passager. Cependant, les constructeurs sont confrontés à des problématiques de sécurité informatique induits par des dispositifs tels que prise ODB, Bluetooth, Wi-Fi, 3G/4G, RFID, clé USB, CD, très courants sur les véhicules modernes. Chacun de ces dispositifs risquerait d'ere une porte ouverte pour des hackeurs souhaitant accéder aux différents calculateurs de bord.

*En 2015, les chercheurs américains Chris Valasek **(en)** et Charlie Miller exploitent la vulnérabilité du système multimédia et prennent le contrôle des fonctions de sécurité et de confort (freins, volant, alimentation électrique du moteur, essuie-glaces) et de divertissement (volume sonore de l'autoradio). Cette démonstration effectuée à partir d'un ordinateur externe distant met en valeur les faiblesses de sécurité des applications embarquées sur les véhicules. Ces dispositifs sont chargés d'échanger des informations entre le véhicule et/ou le conducteur et le système informatique du constructeur ainsi que du processus d'authentification et le chiffrement des codes embarqués.*

Pour anticiper et éviter ces cyberattaques, l'industrie des véhicules connectés et/ou autonomes et les équipementiers s'associent de plus en plus avec des spécialistes de la sécurité pour trouver des solutions ou contre-mesures. Les enjeux économiques, technologiques et sociétaux sont à la mesure de ce défi.

Source L'automobile, le dernier défi de la cybersécurité ?



Tous mettent en avant des architectures propriétaires qui sécurisent les communications et les process entre le véhicule (depuis la voiture en passant par les camions, les bus et bien évidemment les véhicules militaires) vers le cloud et/ou leurs systèmes propriétaires de communication.

Pour simplifier il existe trois normes de cybersécurité

- WP29 U
- UN 155 «Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system » *C'est la norme utilisée par l'UTAC.*
- ENISA 2019

Ces normes participent à sécuriser les véhicules depuis leur construction jusqu'à leur utilisation.
A la fois sécuriser le comportement mais aussi la construction.

Mais, ces nouvelles normes que ces partenaires mettent en place ne concernent pas la confirmation par le conducteur que son véhicule est connecté à internet.

Également, sauf l'une d'entre elles, ces normes ne sont pas approuvées par l'UTAC[1] qui est le laboratoire quasiment officiel de l'automobile. C'est l'autorité reconnue qui valide toutes les procédures automobiles ainsi que les véhicules. Autrement dit c'est bien que le monde automobile sécurise l'environnement moteur/véhicule/communication mais ces volontés sécuritaires ne semblent pas tenir compte de l'importance d'impliquer l'usager, quel qu'il soit.

Pourtant, l'application de ces normes de cybersécurité ne peuvent se faire sans l'accord du dernier maillon : le conducteur au sens large. Cela risque de créer une incompréhension de leur part : « *une fois de plus on nous cache quelque chose »* sauf que là ce n'est pas la pollution, c'est le contrôle même du véhicule. Et sauf que dans certains cela fait 10 ans que cela existe, sans l'annoncer.

Pensons positivement : on prive ce dernier maillon, le conducteur, d'une information forte : il est protégé contre des agressions extérieures.

D'autant plus que les lois européennes demandent que les interactions répondent à la norme DSP2 « dans le domaine des dispositifs de sécurité, l'élément le plus sensible de la DSP2 est la généralisation de l'authentification multi-facteurs (MFA) pour certaines opérations, dont le paiement en ligne.

Il semble normal, alors, au vu du prix de ces véhicules que la norme DSP2 s'y applique.

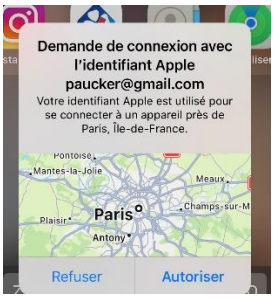
Au fond que fait cette norme ? Elle oblige à demander un deuxième accord de validation à un acheteur (dans notre cas un conducteur). Des CGV électroniques en quelque sorte. Autrement dit, il est normal de protéger un véhicule, encore faut-il que le conducteur le sache et en soit d'accord.
Sinon, des risques de scandales à la VWgate apparaîtront quand des journalistes se saisiront de l'opacité mise en place à nouveau par les constructeurs ou des organismes consommateurs s'en rendront compte.

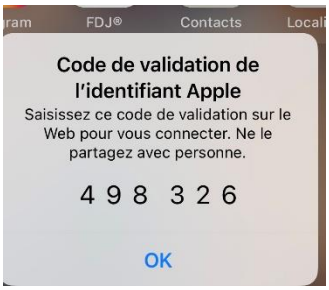
[1] UTAC = **Union technique de l'automobile du motocycle et du cycle**, est un organisme privé, contrôlé et financé majoritairement par l'industrie automobile française

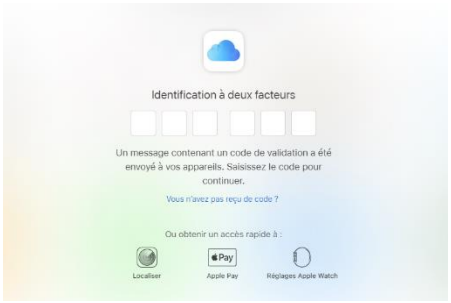
Comment fonctionnent les doubles signatures, pour la plupart

En ce qui concerne cet acte de validation, juridique de double signature ou d'authentification forte, il existe des protections mises en place par le marché.

Par exemple Chez Apple vous recevez un premier message pour vérifier que c'est bien vous qui demandez la connexion suivi d'un code que vous devez recopier sur la transaction en cours d'achat ou simple ouverture d'un logiciel (photoshop par exemple). C'est un peu lourd.







Aujourd'hui la très grande majorité de tels systèmes fonctionnent avec l'envoi d'un code par SMS.

UN SMS est piratable et la seule protection restant la durée de validité du dit SMS qui est en moyenne inférieure à 10 minutes. Ce qui explique le nombre de transactions qui échouent. Il faut jongler entre deux fenêtres d'un même terminal ou jongler avec deux écrans distincts PC et smartphone. Puis ce code doit être retranscris sur la transaction elle-même, sans erreur alors que le nombre de caractères tend à s'allonger.

En général les systèmes existants :

- Fonctionnent sur le cloud donc pas de maitrise locale
- Sources américaines. Aucun contrôle et aucune certitude que le système est réellement opaque

En conclusion, la double signature ou signature renforcée dans la plupart des cas reste piratable aujourd'hui et c'est un processus assez complexe car il nécessite de reporter sans faire d'erreurs des codes tous uniques et difficiles à mémoriser.

En quoi sommes nous uniques

Le brevet d'Augmented Security facilite l'accord sur le déclanchement des protections de cybersécurité en inversant la demande de preuve.
Procédure actuelle : le constructeur envoi à chaque démarrage par SMS un code différent à chaque fois que le conducteur doit ressaisir sur un clavier

Procédure Augmented Security : il suffit que le conducteur tape le mot de passe qu'il aura chois, donc facile à mémoriser et implanté dans l'espace sécurisé par Augmented Security.
Ce code sera toujours le même à chaque demande puisque la sécurisation passe par l'environnement logiciel et non pas par un code piratable, envoyé par un SMSM non sécure.

Un exemple :la procédure Augmented Security peut se traduire par un message affiché sur l'un des écrans du véhicule « *Etes vous d'accord pour être connecté à notre cybersécurité* » suivi d'un espace où le conducteur tapera pour accord son code de 4 à 6 chiffres connu de lui seul, sur un clavier virtuel qui s'affichera. Evidemment, cela peut aussi servir à démarrer le véhicule.

Gain de temps mais aussi simplification des procédures pour les conducteurs. L'expérience a prouvé que plus la procédure est complexe plus les chances qu'elles soient contournées sont grandes.

En conclusion, Augmented Security propose une interface brevetée entre le véhicule et le constructeur qui déclenchera les activités de cybersécurité avec l'accord du conducteur.
Augmented Security rempli cette fonction d'une manière rapide et très simple. A notre connaissance il n'y a pas de procédures équivalentes :

- Brevet Européen
- Nous sommes propriétaire de 100% de notre code, de nos sources.
- Solution horizontale, cross-plateformes
- Intégration à des solutions constructeurs.
- Double signatures 100% sécurisées, ce qui n'est pas le cas de nombreuses procédures actuelles utilisant les SMS qui sont « hackables ».
- Sécurisation forte des terminaux utilisés mais aussi des serveurs créant un continuum sur toute la chaîne depuis l'émetteur jusqu'au récepteur.
-

En conclusion Augmented Sécurité offre une véritable Authentification Forte, qui donnera aux conducteurs le contrôle des communications de leurs véhicules, une fonction qui va être amenée à se développer.