SIEMENS
Ingenuity for life

Siemens Digital Industries Software

La cyber-sécurité appliquée à l'automobile moderne au travers d'une communication sécurisée, d'une authentification robuste et d'un pare-feu flexible

Résumé

Les menaces continues liées à la sécurité ciblant les voitures connectées ont exposé les vulnérabilités critiques des systèmes. Pour atténuer ces risques, les organismes de réglementation définissent à présent des exigences de cyber-sécurité en rédigeant une nouvelle législation et en tenant les constructeurs automobiles et leur chaîne d'approvisionnement responsables des manquements à la sécurité.

Pour répondre comme il convient aux problèmes de sécurité actuels et futurs, ce livre blanc examine une approche à plusieurs niveaux en matière de sécurité des véhicules connectés, et explique comment cette architecture sécurisée peut protéger les points d'entrée des véhicules ainsi que les réseaux embarqués contre les menaces. Plusieurs stratégies de sécurité telles que les pare-feu intégrés, l'authentification, les communications sécurisées, le chiffrement et les certificats numériques seront abordés.

Dr Ahmed Majeed Khan
Chef de produit senior
Siemens Digital Industries Software

Alan Grau
VP des solutions IoT / embarquées
Sectigo

Sommaire

Introduction 3

L'augmentation spectaculaire des menaces liées à la cyber-sécurité 4
Les nouvelles lois visant spécifiquement les constructeurs automobiles 4

La sécurité du réseau automobile 5
Les quatre surfaces d'attaque des voitures connectées 5
Surfaces d'attaque et architecture d'un véhicule 6
Définition de la sécurité 6

La démarche à adopter aujourd'hui : L'approche de sécurité à plusieurs niveaux 7

Les pare-feu intégrés 7
Les pare-feu intégrés pour les calculateurs 8
Que doit faire votre pare-feu ? 8

Cas d'utilisation 9

Communication sécurisée 9

Authentification 10

Conclusion 11

Références 11

Introduction

L'industrie automobile est influencée par un groupe de mégatendances appelées "Automatisation, connectivité, électrification et partage" ou plus communément "ACES" pour "Automation, Connectivity, Electrification and Sharing".

Les tendances ACES représentent une nouvelle opportunité pour l'industrie, car elles relèvent un tout nouvel ensemble de défis. L'un de ces défis consiste à savoir comment faire face à l'augmentation de l'utilisation des logiciels dans l'automobile d'aujourd'hui. En réalité, il y a plus de lignes de code dans les voitures connectées que dans d'autres machines sophistiquées de notre époque telles que le F-35 Joint Strike Fighter de l'U.S. Air Force, le Boeing 787 Dreamliner ou la navette spatiale américaine[1]. Le matériel informatique utilisé aujourd'hui est plus puissant et, par conséquent, des millions de lignes de code peuvent être exécutées lors de l'exécution d'innombrables fonctions complexes. Les voitures connectées intègrent ainsi une multitude de systèmes. Elles communiqueront bientôt vers l'extérieur au moyen de la communication de véhicule à véhicule (V2V) et de la communication de véhicule à infrastructure (V2I), ainsi qu'en interne entre les sous-systèmes et les réseaux du véhicule. La sécurité est primordiale. Tous les systèmes embarqués doivent être sécurisés pour que rien n'affecte le véhicule lorsqu'il est en mouvement (ou à l'arrêt).

L'augmentation spectaculaire des menaces de cyber-sécurité

Le graphique ci-dessous (schéma 1) montre l'augmentation continue des attaques de cyber-sécurité ciblant les automobiles entre 2010 et 2019. Le graphique, extrait du rapport *"2020 Automotive Cybersecurity Report"* élaboré par Upstream Security, montre que les attaques ont été multipliées par six au cours de cette période de neuf ans[2]. Les chiffres ont doublé en 2019 par rapport à 2018. De plus, le graphique décrit une croissance annuelle de 94 % des cyberattaques depuis 2016[3].

On estime que 57 % des réclamations en responsabilité dans le secteur automobile seront payées par l'écosystème automobile[4]. Il ne fait aucun doute que les nouveaux modèles économiques devront évoluer à mesure que la complexité, la fiabilité, le risque et la responsabilité deviendront les moteurs principaux.

Les nouvelles lois visant spécifiquement les constructeurs automobiles

Le succès accru et la prolifération incontestée des cyberattaques automobiles ont mis en lumière l'urgence de développer des solutions de sécurité. On observe actuellement un niveau sans précédent d'initiative commerciale partout dans le monde, qui inclut l'action des législateurs élaborant de nouveaux règlements pour empêcher les cyberattaques.

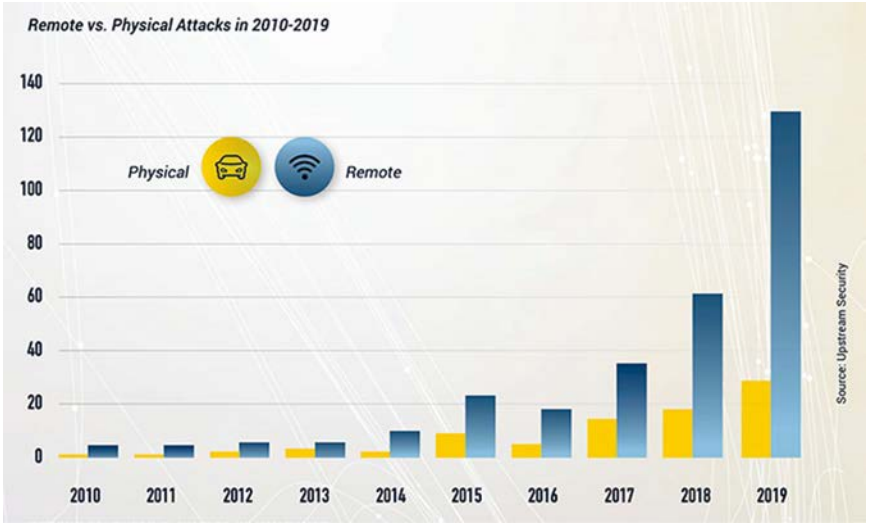


Schéma 1 : Ces neuf dernières années, les incidents de cyber-sécurité automobile opérés à distance ont considérablement augmenté. Alors que de plus en plus de véhicules connectés sont commercialisés, le potentiel de préjudice augmente de façon exponentielle. Source : La sécurité en amont.

Le projet de loi américain sur la sécurité et la protection des renseignements personnels dans les véhicules (U.S. Security and Privacy in Your Car Act[5] ou Spy Car Act) de 2017 définit les exigences concernant la protection contre les accès non autorisés aux données et leur signalement. Le projet de loi ordonne à l'agence fédérale américaine chargée de la sécurité routière (National Highway Traffic Safety Administration ou NHTSA) de publier des directives en matière de cyber-sécurité des véhicules qui exigent que les véhicules automobiles destinés à être vendus aux États-Unis intègrent une protection contre les accès non autorisés aux commandes électroniques et aux données de conduite.

De même, en 2017 également, la chambre des représentants des États-Unis a adopté le projet de loi H.R. 3388[6], « The SELF DRIVE Act », une législation unique visant à assurer le développement, le test et le déploiement sûrs et innovants des véhicules autonomes. Ce projet de loi parvient à un équilibre en assurant la sécurité des consommateurs tout en encourageant l'innovation.

La Chine a établi un conseil pour la cyber-sécurité automobile afin d'assurer l'exploitation sécuritaire des voitures intelligentes, connectées et électriques. Le conseil facilitera les efforts déployés par les chercheurs et les fabricants pour mener des recherches et élaborer des normes, des politiques, des lois et des règlements pour la cyber-sécurité dans l'industrie automobile.

La discussion portant sur le propriétaire des données est également un sujet d'actualité pour les sociétés informatiques ces dix dernières années. Le débat ne porte pas seulement sur le propriétaire des données, mais aussi sur le responsable de leur protection. Ce débat concerne également l'industrie des véhicules connectés. Des règlements sur les données commencent à voir le jour. Les règlements sur les données personnelles tels que le RGPD de l'UE[7], la loi canadienne sur la protection des renseignements personnels et les documents électroniques (LPRPDE)[8] et l'appel de la Commission des transports et du tourisme du Parlement européen à la publication d'un règlement européen sur l'accès aux données embarquées[9] en sont quelques exemples.

La sécurité du réseau automobile

Le programme de recherche en cyber-sécurité automobile de la NHTSA adopte une approche d'analyse des menaces en matière de cyber-sécurité, classant les menaces dans six catégories différentes.

Les six catégories de menaces sont les suivantes :

- **Mystification** : situation dans laquelle une personne, un programme ou un appareil se fait passer pour quelqu'un ou quelque chose d'autre en manipulant les données afin d'obtenir un avantage illégitime.
- **Falsification** : altération volontaire des données de manière à nuire au consommateur. Dans le contexte des voitures connectées, la falsification renvoie aux modifications apportées aux données de configuration, aux logiciels ou au matériel utilisés dans les systèmes de commande des véhicules.
- **Non-répudiation** : situation dans laquelle l'auteur d'une déclaration ne peut pas contester sa paternité ni sa validité. En d'autres termes, l'auteur ou la déclaration ne peut pas prétendre ensuite qu'il ou elle n'a pas fait la déclaration. Par exemple, lorsque l'authenticité d'une signature est contestée, elle est "répudiée".
- **Divulgation d'informations** : peut faire référence à de nombreux types de sabotages liés à la fuite de données.
- **Déni de service (DoS)** : renvoie à une cyberattaque au cours de laquelle une machine est inondée de demandes excessives par un pirate à tel point qu'elle devient indisponible pour les utilisateurs légitimes. Le déni de service est généralement accompli en inondant la ressource ciblée de demandes superflues dans le but de surcharger ses systèmes et d'empêcher le traitement des demandes légitimes.
- **Élévation de privilèges** : situation dans laquelle un pirate informatique utilise de manière abusive une machine et réalise des activités non autorisées en obtenant un accès illégitime aux ressources. Les pirates informatiques dont l'attaque d'élévation de privilèges aboutit, étendent leur accès aux ressources et données des systèmes, ce qui leur permet de faire plus de dégâts.

Maintenant que nous comprenons les bases de ces menaces, nous pouvons désormais examiner les surfaces d'attaque potentielles des voitures connectées. Pour qu'une cyberattaque aboutisse, le pirate informatique doit tout d'abord trouver un moyen d'accéder à la voiture. Il doit ensuite accéder à un calculateur du véhicule en exploitant une vulnérabilité ou des contrôles de cyber-sécurité insuffisants. Enfin, il doit exploiter une fonction de contrôle du calculateur compromis.

Pour mieux comprendre ce que cela signifie, la voiture connectée comporte quatre surfaces d'attaque principales qui peuvent être exploitées.

Les quatre surfaces d'attaque des voitures connectées

La première surface d'attaque est la surface **physique directe**. Cela comprend l'accès au port de diagnostic embarqué (OBD), au port de chargement ou aux connecteurs de faisceaux. Une voiture devient vulnérable lorsqu'un pirate informatique obtient un accès physique direct. Ce scénario se produit lorsqu'une voiture est chez un concessionnaire ou dans un atelier de réparation pour un entretien ou une réparation, ou lorsqu'un autre intervenant a obtenu un accès au véhicule. Un pirate informatique doué travaillant comme voiturier, par exemple, pourrait exécuter une attaque physique directe.

La deuxième surface d'attaque est la surface **physique indirecte**. Ici, un support quelconque est nécessaire pour exécuter l'attaque. Le support pourrait être une clé USB ou un CD qui compromet le micro-logiciel de la voiture. L'utilisation de cartes SD et de mises à jour du micro-logiciel dans les voitures modernes offre toutes sortes de possibilités d'attaque.

La troisième possibilité d'attaque est réalisée au moyen d'une communication **sans fil**. Le Bluetooth et le réseau mobile sont des options de choix pour une attaque sans fil. La connectivité accrue des voitures modernes a considérablement augmenté le risque d'attaques de ce genre.

La dernière surface d'attaque est le **sabotage de capteurs**. À ce jour, aucune attaque connue contre les capteurs d'une voiture connectée n'a été recensée. Cependant, les chercheurs ont démontré que ces types d'attaques sont possibles, bien qu'elles soient irréalisables dans un environnement de laboratoire. Les voitures connectées et autonomes font souvent appel à la technologie des capteurs de télédétection par laser (LiDAR). Ces systèmes peuvent être aveuglés ou trompés par de fausses informations qui pourraient causer de graves préjudices au conducteur du véhicule et à ses occupants. Le GPS est une autre technologie dont les vulnérabilités pourraient être exploitées.

Surfaces d'attaque et architecture d'un véhicule

Le schéma 2 représente les surfaces d'attaque correspondant à l'architecture d'un véhicule. Ce schéma de base met l'accent sur la connectivité embarquée, notamment l'utilisation de passerelles automobiles et de multiples bus de communication. Il montre différents aspects dont l'infodivertissement, la sécurité active (comprenant les caméras et le radar) et l'habitacle. Les calculateurs du châssis et du groupe motopropulseur utilisent un bus CAN qui peut être facilement exploité. Le schéma représente également différents types de bus utilisés pour la communication de données avec la passerelle centrale. Le calculateur de la passerelle centrale est vulnérable aux attaques, car il est directement exposé au monde extérieur.

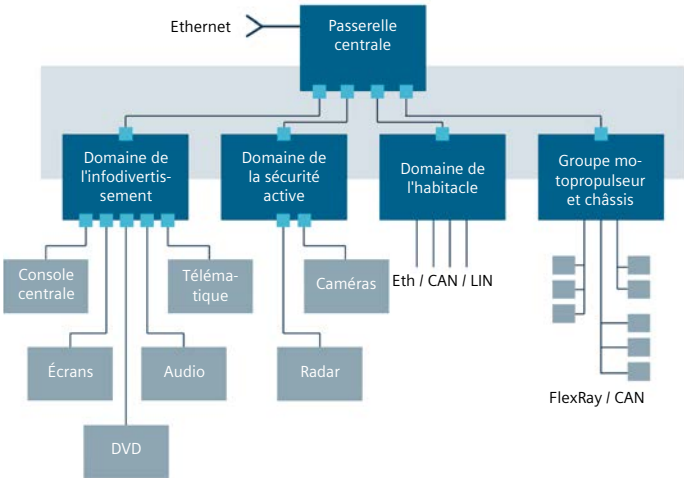


Schéma 2 : Surfaces d'attaque et unités fonctionnelles correspondantes. Source : Université de Californie à San Diego, "Comprehensive Experimental Analyses of Automotive Attack Surfaces" (Analyses expérimentales complètes des surfaces d'attaque des véhicules).

Le schéma 3 montre comment les surfaces d'attaque peuvent être mises en correspondance avec les unités fonctionnelles du véhicule, telles que la communication V2V, la télématique et le diagnostic embarqué (OBD). Aujourd'hui, les propriétaires mettent de plus en plus souvent à jour leurs véhicules via les technologies SOTA (Software Over The Air). Les mises à jour SOTA nécessitent un accès continu, et c'est à ce moment-là que le véhicule est le plus vulnérable. Le port de diagnostic OBD-II est également vulnérable aux cyberattaques. Plusieurs protocoles sont utilisés lors de cette procédure, notamment J1850, CAN ISO 15765, etc. De même, de nombreux systèmes et calculateurs des véhicules sont connectés via un bus CAN, et cette configuration s'est également avérée vulnérable aux attaques.

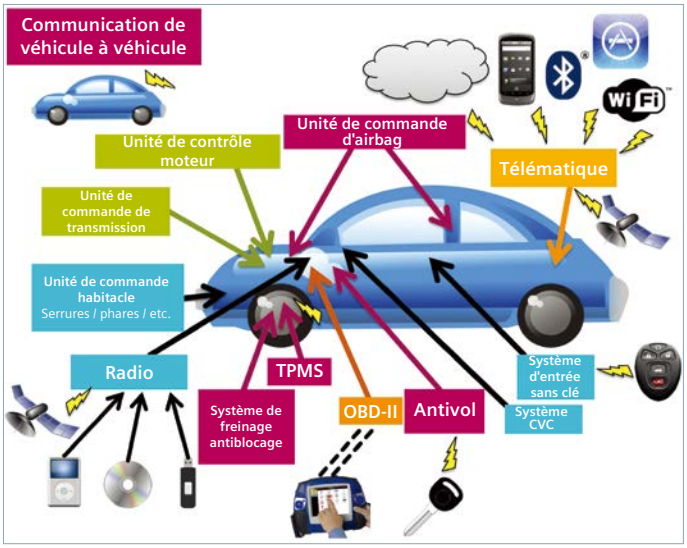


Schéma 3 : Surfaces d'attaque dans l'architecture d'une voiture connectée. Source : Université de Californie à San Diego, "Comprehensive Experimental Analyses of Automotive Attack Surfaces" (Analyses expérimentales complètes des surfaces d'attaque des véhicules).

Si l'on examine les schémas 2 et 3, il est évident que les voitures connectées modernes comportent de multiples points d'entrée. Ces points d'entrée sont considérés par les pirates informatiques à la fois comme un défi et comme une opportunité. Pour éviter tout type de cyberattaque, il est impératif que tous les points d'entrée maintiennent un niveau de sécurité approprié. Pour bien comprendre les mesures nécessaires pour protéger un véhicule, il serait préférable de définir la "sécurité".

Définition de la sécurité

La sécurité s'articule autour de trois aspects. Le premier aspect comprend l'authentification et le contrôle d'accès. L'authentification permet d'autoriser une personne ou un système à effectuer des actions à l'intérieur d'un véhicule. Le contrôle d'accès indique les actions que la personne ou le système est autorisé à réaliser une fois à l'intérieur.

Le deuxième aspect de la sécurité est la protection contre les attaques extérieures. Il peut s'agir d'assurer une protection contre les accès illégitimes ou une protection contre les fuites de données, de garantir la sécurité des communications et, pour finir, d'éviter l'installation de logiciels malveillants ou de chevaux de Troie de toutes sortes sur les véhicules.

Enfin, le dernier aspect de la définition de la sécurité, qui revêt une importance capitale, est la détection et le signalement des incidents de sécurité.

La démarche à adopter aujourd'hui : l'approche de sécurité à plusieurs niveaux

La compréhension des surfaces d'attaque et de la signification de la sécurité pour l'industrie des véhicules connectés implique la proposition d'une approche de sécurité à plusieurs niveaux qui prend ces principes en compte.

Pour qu'une approche de sécurité à plusieurs niveaux fonctionne, les équipementiers automobiles doivent sécuriser toutes les communications, externes comme internes.

Lors de l'examen d'une approche de sécurité à plusieurs niveaux, de nombreux facteurs doivent être pris en compte, car ces solutions de sécurité sont intégrées à la voiture connectée. Un pare-feu intégré, ou un système de détection d'intrusion destiné à empêcher le véhicule d'accepter le trafic, les données ou les signaux non autorisés envoyés par une adresse IP malveillante, doit faire partie de l'équation. Bien entendu, l'authentification est également un élément essentiel. L'utilisation d'un système d'exploitation sécurisé, d'un système multi-cœur et d'une prise en charge d'hyperviseurs doit également être envisagée.

Ce livre blanc analyse quelques-uns des composants les plus critiques nécessaires pour protéger une voiture connectée : les pare-feu intégrés, la communication sécurisée et l'authentification.

Les pare-feu intégrés

L'intégration d'un pare-feu dans un véhicule est un processus hautement spécialisé. Il faut comprendre qu'il ne s'agit pas d'un pare-feu de réseau classique fonctionnant sur un routeur ou une passerelle ou tout autre appareil d'entreprise. Il s'agit d'une solution hautement spécialisée, exclusivement conçue pour l'environnement automobile.

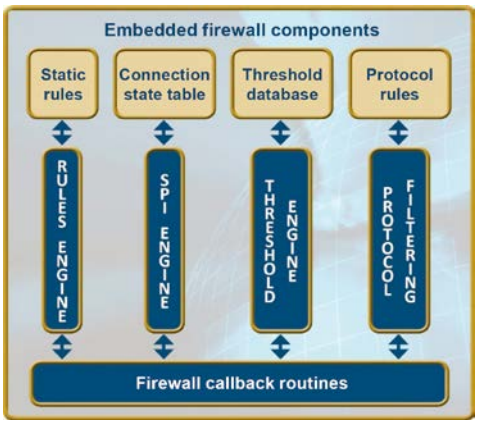
Pour commencer l'intégration du pare-feu, il faut disposer d'un kit de développement logiciel (SDK). Le kit SDK peut être directement intégré à la pile de communication, que ce soit le protocole TCP/IP, le réseau CAN ou une autre solution connectée. Le pare-feu doit respecter des exigences spécifiques. Il doit disposer d'une flexibilité intégrée pour pouvoir être exécuté sur un calculateur. Il doit fonctionner avec un système d'exploitation en temps réel (RTOS) voire dans l'environnement AUTOSAR. Certains environnements disposent de ressources limitées, et leur configuration s'accompagne de son propre lot de défis. Pour fonctionner, le pare-feu intégré doit être une solution modulaire hautement configurable, compatible avec les nombreux calculateurs automobiles utilisés de nos jours.

Lors de l'intégration du pare-feu, il est recommandé de prendre du recul et de tenir compte des exigences à respecter. De nombreuses cyberattaques commencent par l'envoi de paquets à la voiture connectée, à la recherche de points faibles. Si le pare-feu peut rapidement détecter cette activité et s'assurer que la réception ou la transmission de certains paquets n'est pas autorisée, une attaque potentielle sera déjouée avant même qu'elle ne soit menée. Il est important de contrôler les ports et protocoles utilisés pour recevoir des messages pour le véhicule. Si l'on peut contrôler les adresses IP qui envoient des données au véhicule, on peut protéger le véhicule et signaler toute activité suspecte.

Pourquoi est-ce important ? Lorsque l'on étudie certaines des premières cyberattaques, l'attaque de Miller Vilsack sur la Jeep Cherokee par exemple, on s'aperçoit que les pirates informatiques n'ont pas commencé par envoyer quelques paquets à la voiture, terminé leur attaque puis sont passés à autre chose. Dans le cas de la Jeep Cherokee, comme dans de nombreuses cyberattaques, l'attaque a commencé par l'envoi de centaines voire de milliers de messages différents au véhicule pour détecter d'éventuelles faiblesses. Quels messages le pirate informatique envoie-t-il au véhicule ? Quelle réponse le pirate informatique reçoit-il du véhicule ? Le véhicule peut-il "percevoir" quand il est sondé et répondre en temps voulu et de manière appropriée ?

Les pare-feu intégrés pour les calculateurs

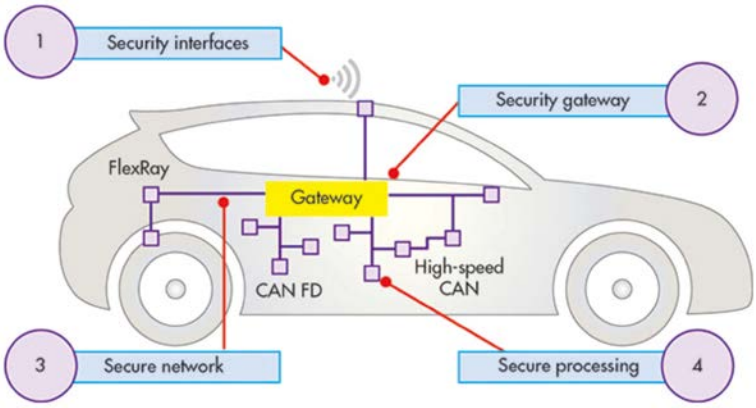
L'ajout d'un pare-feu à une passerelle centrale nécessite un code source portable qui peut être intégré au calculateur. Le pare-feu doit être configurable. Par exemple, dans le cas de l'attaque de Miller Vilsack, si un pare-feu avait été installé, le trafic suspect des adresses IP aurait été signalé en appelant les domaines suspects envoyant les messages. Les règles de filtrage intégrées au pare-feu pour bloquer des adresses IP spécifiques auraient reconnu l'activité indésirable et réagi rapidement : un moyen sûr d'empêcher une attaque.



Il est extrêmement important que le pare-feu prenne en charge différents types de capacités de filtrage.
Le pare-feu idéal doit prendre en charge le filtrage du bus CAN et le filtrage basé sur les règles.
Le blocage des messages par ports, protocole, adresses IP, etc., est un moyen sûr d'empêcher une attaque de se produire. Le pare-feu doit pouvoir effectuer un filtrage basé sur un seuil, un filtrage statique ou basé sur des règles et une inspection de paquets. Ce ne sont là que quelques-uns des modules qui doivent être intégrés au pare-feu.
L'enregistrement et l'établissement de rapports sur les attaques permettent la détection d'intrusion, une technologie permettant de savoir quand un événement inhabituel se produit. Le signalement de ces événements à une sorte de centre des opérations du véhicule permet aux équipes chargées des opérations de sécurité d'agir sur la base de ces informations et de mettre fin à l'attaque avant que les pirates informatiques ne l'aient achevée.

Que doit faire votre pare-feu ?

Un pare-feu intégré peut fonctionner dans différents modes. Un pare-feu fonctionnant en mode actif bloque toute activité extérieure enfreignant les règles du pare-feu. Un pare-feu fonctionnant en mode passif recherche les activités suspectes ou anormales et transmet les données correspondantes à un centre des opérations. Il peut également exister des scénarios dans lesquels un pare-feu doit prendre en charge un fonctionnement en mode apprentissage où le pare-feu apprend des modèles de trafic types et peut ensuite fonctionner en mode actif, reconnaissant et bloquant le trafic qui ne correspond pas au modèle pertinent.



Un pare-feu intégré peut être déployé de multiples façons. Il est notamment possible de le déployer sur un **calculateur de passerelle externe**. Ce type de passerelle gère la communication avec toutes les entités extérieures. Point focal de communication, cette passerelle devient la cible d'attaques. Le pare-feu installé sur un calculateur de passerelle externe applique des règles de filtrage pour toute communication entrante dans le véhicule. Son rôle est de détecter et de bloquer les attaques avant qu'elles n'atteignent les calculateurs ciblés.

Il est également possible de déployer le pare-feu sur un **calculateur de passerelle interne**. Si la voiture comprend plusieurs réseaux, un calculateur de passerelle interne permet la communication entre les différents réseaux. Dans ce cas, un pare-feu permet d'isoler les fonctions essentielles de sécurité, c'est-à-dire que le système interne le plus important est protégé de tout trafic réseau potentiellement malveillant.

Enfin, un pare-feu peut être déployé sur un **calculateur terminal**, le calculateur de commande réel qui gère les fonctions essentielles du véhicule. Les calculateurs de commande sont des dispositifs tels que les systèmes de freinage antiblocage, les airbags, les systèmes de commande de direction, etc. Dans la plupart des situations, il est recommandé de déployer un pare-feu sur plusieurs calculateurs terminaux. Après tout, la sécurité est un système de défense en profondeur constitué de plusieurs niveaux de protection. Si un aspect de la solution de sécurité est défaillant, vous devez disposer d'autres niveaux de sécurité en renfort.

Cas d'utilisation

Un fournisseur mondial de calculateurs automobiles va commercialiser une nouvelle plateforme sécurisée
Leader mondial des solutions de cyber-sécurité, Sectigo s'est associé à l'entité qui produit les logiciels automobiles embarqués de Siemens Digital Industries Software pour développer une solution de pare-feu intégrée pour un grand fournisseur mondial de calculateurs automobiles. Les deux partenaires ont été chargés d'élaborer une solution de pare-feu pour s'adapter à la nouvelle génération de véhicules caractérisée par de hauts niveaux de connectivité. Dans les versions précédentes, le client devait se fier à un calculateur de passerelle automobile interne pour gérer la communication externe. Cependant, cela s'est révélé problématique, car la passerelle devenait la cible de cyberattaques. Une nouvelle approche était nécessaire concernant la sécurité du réseau.

Sectigo a lancé un pare-feu destiné à être intégré dans une passerelle de calculateur externe. Pour accélérer l'adoption, et améliorer d'autant plus les fonctionnalités de sécurité, Siemens a intégré le pare-feu Sectigo à sa plateforme AUTOSAR très connue, Capital VSTAR. Les fonctionnalités de sécurité comprennent le contrôle des paquets transmis aux réseaux internes et le blocage du trafic en fonction de règles de filtrage préconfigurées et d'un comportement d'exécution. De plus, le pare-feu intégré de Sectigo donne la possibilité de signaler toute activité suspecte à un système de gestion.

L'année dernière, des clients ont testé le pare-feu dans le cadre d'essais concluants. La plateforme Sectigo compatible AUTOSAR devrait être entièrement déployée d'ici 2021.

SECTIGO

Communication sécurisée

À l'instar des pare-feu intégrés, la communication sécurisée compte de nombreux cas d'utilisation. Les scénarios comprennent la communication entre la voiture et les systèmes externes, la communication V2V et la communication à l'intérieur de la voiture. Plus fréquente aujourd'hui, la communication V2V représente une forme essentielle de communication qui doit être protégée. Et là encore, s'agissant de la communication sécurisée à l'intérieur de la voiture, tous les calculateurs doivent être protégés.

La communication sécurisée vise à s'assurer que chaque fois qu'une session de communication débute, l'origine de cette communication est connue. Pour garantir une communication sécurisée, il est recommandé d'avoir recours au chiffrement. Une communication chiffrée utilise des protocoles IP comme TLS, DTLS et SSH. En cas d'exécution sur un bus CAN, il est possible d'utiliser CANcrypt. Il est essentiel de s'assurer que toutes les données sont chiffrées en utilisant une cryptographie forte pour repousser les cyberattaques.

Authentification

L'authentification est utilisée lors de l'établissement d'une session de communication pour vérifier que l'appareil ou le processus avec lequel vous communiquez est réellement celui qu'il prétend être. Pour la communication entre machines, on a souvent recours à une authentification par certificat. Parmi les aspects importants de l'authentification, on peut citer le rôle de l'infrastructure à clés publiques (ICP) et la gestion et la délivrance des certificats numériques. Chaque calculateur doit pouvoir être identifié. Ainsi, les certificats basés sur une ICP sont idéals, car ils assurent une authentification forte et peuvent être utilisés pour la communication entre machines. Un autre aspect de la sécurité basée sur une ICP est la signature de code qui permet un démarrage sécurisé et la mise à jour sécurisée des calculateurs.

Les certificats basés sur une ICP jouent un rôle central. Tout au long de ce livre blanc, nous avons considéré les communications V2V et V2I comme des enjeux essentiels dans le domaine des voitures connectées. Avec les communications V2I, la délivrance automatisée et ultra rapide de certificats est indispensable. Et il est essentiel de disposer d'un moyen d'héberger et de gérer l'ensemble du processus de façon sécurisée. Où l'autorité de certification est-elle hébergée ? Comment le certificat est-il délivré ? S'agit-il d'un processus automatisé ? Est-ce sécurisé ? Comment les clés privées sont-elles protégées ? Toutes ces questions sont d'une importance capitale et doivent être prises en compte.

Lorsqu'on examine un équipementier automobile et sa solution de cyber-sécurité, il est fréquent que le fabricant possède sa propre stratégie interne pour les voitures connectées. Il a parfaitement le droit de posséder son propre écosystème de sécurité breveté. Mais lorsqu'on considère les communications V2I ou V2V, quand les véhicules de plusieurs équipementiers partagent la même route, les constructeurs automobiles doivent élaborer un écosystème partagé avec les mêmes exigences de sécurité, capacités de gestion et autres capacités liées à la sécurité pour assurer l'interopérabilité entre tous les véhicules sur la route.

Conclusion

L'intégration de la sécurité dans les voitures connectées nécessite l'adoption d'une approche à multiples facettes (schéma 4). Cette décision ne peut être prise après coup. Pour protéger ces véhicules, il convient de disposer de plusieurs niveaux de sécurité et de tenir compte de toutes les surfaces d'attaque. Il est raisonnable de supposer qu'une voiture connectée sera la cible d'une cyberattaque à un moment ou à un autre. Les pirates informatiques qui tentent de pénétrer dans un dispositif embarqué au moyen d'attaques à distance sondent le dispositif pour détecter les ports ouverts afin d'identifier d'éventuelles faiblesses. Le blocage de tous les ports et protocoles non utilisés limite la surface d'attaque. L'enregistrement des paquets qui violent les règles de filtrage configurées permet de détecter les comportements suspects. Et rappelez-vous, la plupart des cyberattaques ne sont détectées que lorsqu'il est trop tard. Une détection précoce est donc indispensable.

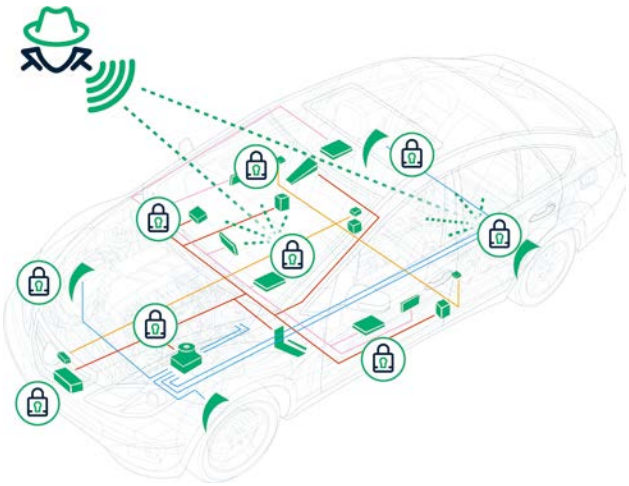


Schéma 4 : Protection de calculateurs contre une cyberattaque au moyen d'un pare-feu intégré et d'une authentification par certificat. Source : Sectigo.

Lorsque deux appareils communiquent au sein d'un réseau automobile, la communication doit être sécurisée pour interdire l'accès aux tiers malveillants. Il est important de vérifier un programme ou un appareil d'une manière suffisamment rigoureuse et de façon intrinsèque. L'authentification doit garantir la sécurité du système en résistant à toute attaque que le système pourrait subir en vérifiant les identités de toutes les connexions entrantes.

À mesure que les voitures connectées évoluent, il est recommandé de procéder à la configuration de la cyber-sécurité à distance avec un système de gestion de la sécurité d'entreprise. Cette intégration offre une gestion centralisée des politiques de sécurité, une connaissance de la situation et une surveillance des données des appareils, ainsi qu'une gestion des événements et une analyse des fichiers journaux à des fins d'analyse des données.

Enfin, il revient à la communauté automobile de prouver qu'elle est digne de confiance pour que les consommateurs fassent confiance aux voitures connectées. La sécurité ne doit pas devenir un avantage concurrentiel distinctif. Ce doit être une ressource commune partagée. Comme le souligne ce livre blanc, le pare-feu intégré, la communication sécurisée et les techniques d'authentification forte sont des éléments essentiels qui constituent une approche de sécurité à plusieurs niveaux.

Références :

1. Robert N. Charette. "This car runs on code", IEEE Spectrum, février 2009.
2. 2020 Automotive Cybersecurity Report by Upstream Security, décembre 2019.
3. "Automotive cybersecurity incidents doubled in 2019, up 605% since 2016", Help Net Security, janvier 2020.
4. "The chaotic middle: the autonomous vehicle and disruption in automobile insurance", KPMG, juin 2017, PDF.
5. Projet de loi S. 2182 - Spy Car Act of 2017, Sénat des États-Unis www.congress.gov/bill/116th-congress/senate-bill/2182/text.
6. Projet de loi H.R 3888 - The Self Drive Act of 2017, Chambre des représentants des États-Unis www.congress.gov/bill/115th-congress/house-bill/3388/text.
7. Règlement général sur la protection des données (RGPD) - Union européenne. https://gdpr.eu.
8. La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) - Canada. www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda.
9. "Parliament calls for EU regulation for access to car data." FIA Region 1, février 2018, www.fiaregion1.com/parliament-calls-eu-regulation-access-car-data.

Siemens Digital Industries Software

Siège social
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

Amériques
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

Europe
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD, Royaume-Uni
+44 (0) 1276 413200

Asie-Pacifique
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

siemens.com/software

81953-C6-FR 3/21 in-C

À propos de Siemens Digital Industries Software

Siemens Digital Industries Software facilite la transformation numérique des entreprises intéressées par des solutions d'avenir en matière de conception, d'ingénierie et de fabrication. Xcelerator™, le portefeuille complet et intégré de logiciels et de services de Siemens Digital Industries Software, aide les entreprises de toutes tailles à créer et à exploiter un jumeau numérique complet qui offre aux entreprises de nouvelles perspectives, opportunités et niveaux d'automatisation pour stimuler l'innovation. Pour d'autres informations sur les produits et les services de Siemens Digital Industries Software, visitez siemens.com/software, ou suivez-nous sur LinkedIn, Twitter, Facebook ou Instagram. Siemens Digital Industries Software – Where today meets tomorrow.

À propos des auteurs

Le **Dr Ahmed Majeed Khan** est un ingénieur en chef, qui a l'habitude de travailler avec des groupes inter fonctionnels pour repousser les limites des technologies mises en œuvre dans divers domaines du secteur automobile et de l'électronique grand public.
Ayant travaillé dans la Silicon Valley, il maîtrise le développement « onshore » et « off-shore » de produits innovants et disruptifs, et a dirigé des équipes partout dans le monde pour produire plusieurs solutions système de haute qualité et très largement diffusées. Il occupe actuellement le poste de directeur principal de l'ingénierie chez Siemens Digital Industries Software, où il a contribué à la création d'un portfolio de produits pour l'automobile, leader sur le marché. Le Dr Khan a également le rôle d'interlocuteur pour Siemens auprès du consortium international des logiciels automobiles, AUTOSAR.
Il a obtenu un doctorat en gestion de l'ingénierie à l'Université George-Washington et une maîtrise en génie électrique à l'Université d'État du Michigan, et possède plus de dix ans d'expérience dans les systèmes intégrés.

Alan Grau possède plus de 30 ans d'expérience dans le domaine des télécommunications et sur le marché des logiciels embarqués. Il est vice-président des solutions IoT / embarquées chez Sectigo (anciennement Comodo CA), la plus grande autorité de certification commerciale du monde et un fournisseur de solutions ICP spécialisées et automatisées. Alan a rejoint Sectigo en mai 2019, dans le cadre de l'acquisition d'Icon Labs, un important fournisseur de logiciels de sécurité pour l'IoT et les dispositifs embarqués, dont il est le cofondateur et l'ancien CTO, et est également l'architecte du pare-feu primé Floodgate d'Icon Labs. Conférencier bien connu de l'industrie, il est également blogueur et détient de nombreux brevets dans le domaine des télécommunications et de la sécurité. Avant de fonder Icon Labs, il a travaillé pour AT&T Bell Labs et Motorola. Alan a obtenu une maîtrise en informatique à l'université Northwestern.