Communiqué de presse

Des solutions de sécurité IT performantes protègent la communication V2X contre les cyberattaques

L'avenir est à la conduite connectée. Mais les échanges de données entre les véhicules et l'infrastructure de transport ne deviendront réellement bénéfiques que lorsqu'ils seront protégés de manière fiable contre tout accès non autorisé. Spécialiste de la cybersécurité, ESCRYPT présente sa solution de sécurisation de la communication V2X.

Les avantages que procurera la communication V2X sont indéniables : renforcement de la sécurité de conduite, amélioration de la sécurité routière, commande intelligente du trafic. Elle permettra d'éviter des accidents et de réduire les temps de parcours et facilitera considérablement la recherche d'un emplacement de stationnement. Mais elle présuppose que la communication en temps réel entre les véhicules (V2V) ou entre le véhicule et l'infrastructure de transport (V2I) soit protégée de manière fiable contre toute utilisation abusive, manipulation et espionnage des données. La seule idée que des hackers puissent attaquer l'infrastructure et les systèmes de régulation du trafic, créer des profils de mouvement ou accéder à la communication du réseau de bord de certains véhicules via V2X serait de nature à donner un coup de frein fatal à la mobilité connectée.

Security Credentials Management : l'infrastructure de sécurité qui se cache derrière V2X

C'est pourquoi V2X a besoin de sa propre infrastructure de sécurité de soutien, afin de garantir des échanges mutuels réellement sécurisés de messages authentifiés. C'est dans ce but qu'ESCRYPT a développé des outils logiciels spécifiques et des produits de sécurité qui permettent la mise en place d'un Security Credentials Management System (SCMS) pour garantir une communication V2X sûre. Le SCMS sécurise la communication des véhicules entre eux et avec l'équipement routier de deux façons différentes : au moyen de signatures numériques, qui protègent les messages contre toute manipulation et tout accès non autorisé, et via des certificats qui identifient l'expéditeur comme étant digne de confiance.

Les échanges de données V2X doivent globalement être sécurisés à deux niveaux : d'une part dans les systèmes embarqués eux-mêmes, dans les calculateurs des véhicules et dans la commande électronique des installations de transport, et d'autre part via un backend

qui gère de manière sûre et efficace le nombre considérable de certificats requis pour sécuriser la communication V2X.

Solution globale complémentaire :
la gestion des certificats assure l'authentification et l'anonymat
En tant qu'expert et leader en matière de sécurité automobile et IoT, ESCRYPT propose des solutions complémentaires allant au-delà de ces deux niveaux. Le kit de développement logiciel CycurV2X permet par exemple aux constructeurs automobiles, équipementiers de rang 1 et fabricants d'installations de transport de mettre en œuvre des protocoles de sécurité V2X dans leurs systèmes automobiles embarqués. CycurV2X constitue une solution de sécurité V2X robuste, qui isole les interfaces sécurité-infrastructure via une simple API. L'avantage spécifique de ce système est que la sécurité V2X peut être étendue en continu à tout moment, de l'introduction prudente jusqu'au fonctionnement en temps réel avec des fonctions de sécurité IT complètes.

Dans cette solution complète, la sécurité et la protection des données sont indissociables. Les messages V2X sont en permanence authentifiés de manière fiable, afin de garantir que seuls des véhicules et des installations de transport autorisés communiquent. La sphère privée des utilisateurs de véhicules est par ailleurs protégée : les mouvements des usagers de la route ne peuvent pas être suivis dans la mesure où CycurV2X détient en permanence un lot de certificats valables simultanément et remplace successivement le certificatif actif par un nouveau durant le trajet, à intervalles de quelques minutes.

ESCRYPT propose par ailleurs CycurV2X-SCMS**,** les composants backend nécessaires à la sécurité pour l'infrastructure à clé publique. CycurV2X-SCMS comporte une plateforme complète conforme aux normes qui permet de fournir et de bloquer des certificats pour les véhicules et les installations de transport. Ces deux solutions sont conformes à la fois aux normes nord-américaines et européennes. En termes de performances et d'évolutivité, elles sont par ailleurs d'ores et déjà conçues pour gérer les échanges permanents de messages authentifiés entre des millions de véhicules et d'installations de transport.

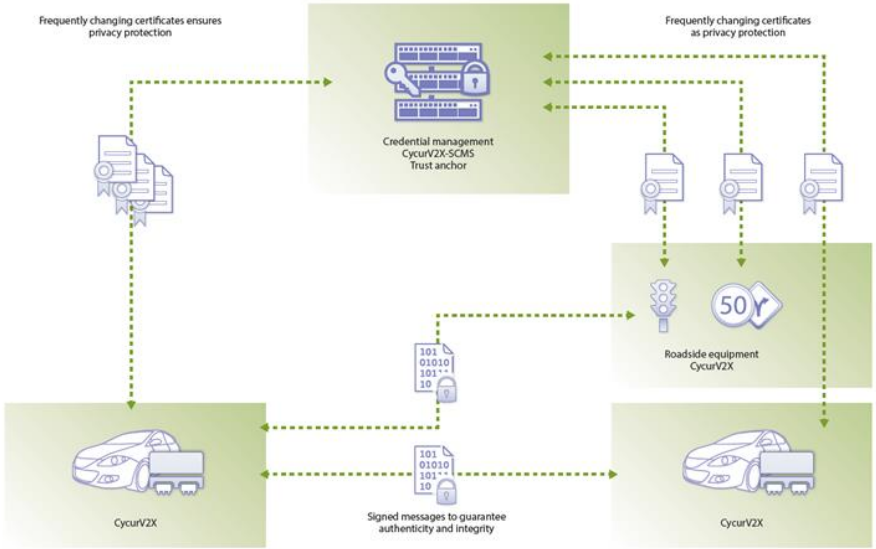
Lorsqu'il sera finalisé, le système de sécurité V2X sera de loin la plus grande infrastructure à clé publique du monde. Parallèlement, il devra offrir une certaine liberté de manœuvre à différents acteurs. Aussi le concept de sécurité des solutions ESCRYPT repose-t-il sur une architecture distribuée avec séparation des rôles. Les constructeurs automobiles et gestionnaires de systèmes de transport intelligents (ITS) peuvent ainsi travailler dans un

système indépendamment les uns des autres, sur la base d'une unique ancre de confiance. Les véhicules et installations de transport peuvent échanger des messages authentifiés en toute sécurité, même s'ils sont gérés par des organisations différentes entre lesquelles il n'existe pas de connexion officielle. Parallèlement, la protection des données et l'anonymat des usagers de la route demeurent garantis à tout moment.

Des solutions éprouvées dans le cadre de projets pilotes ITS

Les solutions V2X démontrent déjà leur aptitude à fournir une infrastructure de sécurité V2X qui fonctionne dans le cadre de plusieurs projets pilotes ITS. En Amérique du Nord, ESCRYPT soutient par exemple différents projets de référence sur l'interconnexion des véhicules aux côtés du Ministère américain des Transports et de l'initiative « Crash Avoidance Metrics Partnership » (CAMP) dont l'objectif est d'éviter les accidents. En en Europe, l'Office fédéral allemand pour la sécurité en matière de technologies de l'information (BSI) a chargé ESCRYPT de fournir au projet « Cooperative ITS Corridor » l'infrastructure à clé publique requise pour sécuriser la communication V2X.
La conduite connectée est un modèle qui ne relève plus désormais de la fiction. Grâce aux solutions de sécurité IT connectées et intelligentes, elle est en passe de devenir une réalité au quotidien.

La communication V2X sécurisée comment ça marche ?



ESCRYPT GmbH – Embedded Security

ESCRYPT - Embedded Security est le premier fournisseur mondial de systèmes de sécurité embarquée. Présent en Allemagne, au Royaume-Uni, en Suède, aux Etats-Unis, au Canada, en Chine, en Corée et au Japon, ESCRYPT s'appuie sur ses spécialistes en sécurité dont la mission est d'aider les clients sur les sujets de sécurité actuels, tels que les communications M2M sécurisées, la sécurité informatique dans l'Internet des objets, la protection des modèles de e-business et la sécurité automobile. Ils développent des produits et des solutions hautement sécurisés, appréciés dans le monde entier et qui répondent aux besoins spécifiques des systèmes embarqués et des infrastructures informatiques correspondantes. Ces produits ont été testés et éprouvés à plusieurs millions de reprises dans des véhicules automobiles produits en série.
Pour plus d'informations : www.escrypt.com