Communiqué de presse

ETAS S.A.S.
32, avenue Michelet
BP 170-93404 Saint-Ouen
Cedex

Lutter contre les cyberattaques sur les véhicules avec la nouvelle solution Escrypt

Mieux détecter et repousser les cyberattaques sur des véhicules individuels et des flottes entières : tel est le défi que relève la nouvelle solution Escrypt destinée aux constructeurs automobiles. Selon les prévisions, d'ici 5 ans plus de 380 millions de véhicules seront connectés. Pionnier en matière de sécurité automobile, ESCRYPT met à profit sa longue expertise pour préparer les véhicules aux profondes transformations qui accompagnent le monde connecté.

L'ouverture des systèmes, la conduite automatisée… quels risques ?
Les systèmes de véhicule qui étaient jusqu'à présent fermés s'ouvrent désormais très rapidement au monde extérieur. Or les interfaces avec les smartphones et la possibilité d'une communication car-to-x font surgir de nouveaux risques à bord des véhicules. Un hacker peut par exemple prendre le contrôle de l'autoradio d'un véhicule et mettre soudain le volume à fond ou encore dérober des données personnelles contenues dans un smartphone connecté, sans parler des attaques menées contre les calculateurs pilotant le comportement du véhicule, ni des manipulations contraires à la loi au niveau du système d'entraînement.

Parallèlement, de plus en plus de responsabilités sont transférées du conducteur aux calculateurs et à leurs logiciels : la conduite automatisée devient une réalité.

Ce nouveau monde ultra connecté nécessite des stratégies sécuritaires globales dans lesquelles la sécurité fonctionnelle est indissociable de la sécurité automobile et ce, sur tout le cycle de vie des véhicules. Cela commence au lancement du développement, se poursuit en production avec une paramétrisation sécurisée des calculateurs, garantissant un fonctionnement sûr du véhicule à tout moment, et ne se termine qu'avec l'effacement des clés cryptographiques et l'invalidation de l'identité du véhicule avant la mise au rebut du véhicule.

ETAS S.A.S.
32, avenue Michelet
BP 170-93404 Saint-Ouen
Cedex

IDPS : une approche globale de la sécurité

Disponible depuis 2017, la solution IDPS (Intrusion Detection and Prevention Solution) développée par Escrypt et proposée en France par Etas, permet de détecter, analyser et repousser les cyberattaques. IDPS documente les tentatives d'intrusion et peut transmettre automatiquement les données pour analyse à un système backend de cybersécurité. Des équipes d'experts y utilisent les données pour effectuer des analyses criminalistiques des incidents, afin de pouvoir définir et mettre en œuvre des contre-mesures adaptées (comme par exemple des mises à jour de sécurité transmises over-the-air).

Grâce à cette détection et à cette défense contre les attaques, la sécurité automobile devient un processus continu allant de la prévention (via un pare-feu par exemple) à l'analyse des attaques et à un déploiement constant de contre-mesures adaptées, en passant par le suivi et le reporting des attaques.

Au lieu de se contenter de mesures de défense statiques dans les différents véhicules, IDPS prend ainsi en compte des données actualisées en permanence et issues de l'ensemble de la flotte, permettant ainsi de fournir rapidement des réponses adaptées aux nouveaux risques et stratégies d'attaque qui évoluent en permanence.

L'expertise ESCRYPT : une technologie fiable

ESCRYPT travaille depuis plus de 12 ans sur ces concepts de protection globaux. IDPS représente une nouvelle pièce importante du puzzle que constituent ces concepts complets et met l'accent avec cette solution sur la sécurité de fonctionnement des véhicules connectés.

Les contrôles d'intégrité des logiciels de calculateurs, la communication authentifiée à bord des véhicules et la sécurisation de différents domaines du véhicule via des pare-feu font déjà partie de la gamme de solutions proposées par ESCRYPT. Avec IDPS, ESCRYPT s'attaque à des risques qui n'existent pas encore ou sont encore inconnus au moment du développement et de la production du véhicule concerné.

Détection et prévention des intrusions pour les véhicules

Grâce à l'analyse des données, les constructeurs disposent d'un aperçu complet et actualisé en permanence des stratégies mises en place par les hackers et des points d'entrée choisis pour leurs attaques. Ils peuvent également déterminer si les attaques se multiplient. L'une des étapes de la stratégie de défense porte sur l'analyse de cette vaste base de données d'événements. Cette solution logicielle automatisée, et basée sur des

ETAS S.A.S.
32, avenue Michelet
BP 170-93404 Saint-Ouen
Cedex

méthodes de big data, analyse les modèles d'attaque et effectue un tri préliminaire sur la base duquel les experts en sécurité et en criminalistique des données du centre de cyberdéfense décident des contre-mesures à mettre en place. Il peut s'agir d'ajustements ciblés des pare-feu, de mises à jour de l'ensemble de règles de CycurIDS, ou, en étroite concertation avec les fabricants des calculateurs concernés, de mesures visant à remédier aux vulnérabilités de leurs logiciels (étape 5).

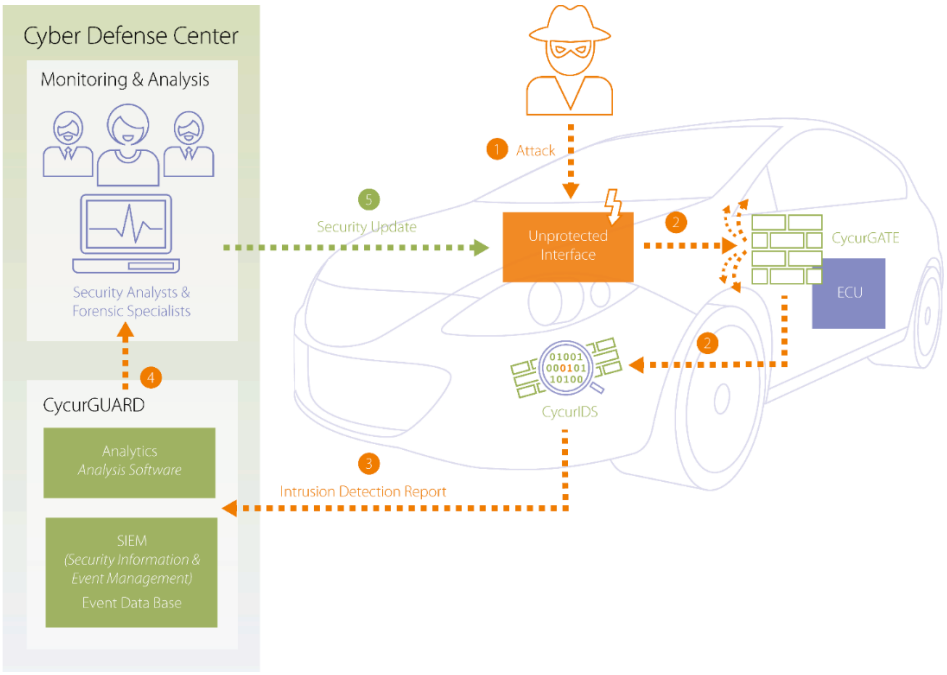
Les mesures peuvent ensuite être transmises over-the-air à tous les véhicules connectés d'une flotte, la transmission intervenant bien entendu exclusivement via des liaisons de communication sécurisées par voie cryptographique. Les mises à jour elles-mêmes sont par ailleurs protégées contre toute modification non autorisée à l'aide de signatures numériques. La solution complète de gestion des clés (CycurKEYS) utilisée dans de tels cas figure également dans la gamme de solutions proposées par ESCRYPT.

IDPS dote ainsi la voiture connectée d'une défense immunitaire qui se renforce au fil des attaques et dont l'intelligence croît en permanence grâce à l'enrichissement constant de la base de données.

La sécurité intelligente s'appuie sur une vaste base de données mise à jour en continu
Avec sa stratégie de défense en cinq étapes, IDPS constitue une solution pérenne et évolutive. Mais elle offre en outre d'autres atouts : à chaque véhicule qui vient rejoindre le réseau, les capacités d'analyse de la détection d'intrusion augmentent, et donc aussi les possibilités de défense. Chaque attaque invisible jusqu'à présent, et bloquée le cas échéant par des pare-feu, aide à adapter les mesures de sécurité aux risques actuels. Au lieu de demeurer dans les mémoires de données jusqu'au prochain passage à l'atelier, les rapports d'anomalie enregistrés et transmis sans délai au centre backend de cybersécurité contribuent immédiatement au renforcement de la protection.

Au lieu de rester sur la défensive avec une protection passive, les clients peuvent grâce à IDPS adapter à tout moment les systèmes de défense aux nouvelles stratégies d'attaque et aux nouveaux cyber-risques. Fort de sa longue expérience acquise dans le cadre de nombreux projets de série, ESCRYPT peut aisément intégrer ses solutions de sécurité globales dans le développement et la vérification du matériel et des logiciels de calculateurs. IDPS et les mises à jour over-the-air sont ainsi incorporés dans les modèles de série par des moyens sûrs et établis. Les traces de tentatives d'intrusion numérique ne demeurent de ce fait plus invisibles, mais sont bien au contraire utilisées pour améliorer les mesures de défense.

ETAS S.A.S.
32, avenue Michelet
BP 170-93404 Saint-Ouen
Cedex



Vue d'ensemble de l'IPDS - Intrusion Detection and Prevention

ESCRYPT GmbH – Sécurité embarquée

ESCRYPT – Sécurité embarquée est le premier fournisseur au monde de solutions de sécurité dans le domaine des systèmes embarqués. Répartis entre cinq sites allemands et des filiales implantées en Grande-Bretagne, en Suède, aux Etats-Unis, au Canada, en Inde, en Chine, en Corée et au Japon, ses experts se concentrent sur des sujets d'actualité en matière de sécurité des données tels que la sécurité de la communication M2M, la sécurité informatique au sein de l'Internet des objets, la sécurisation des modèles e-business et la sécurité automobile. Ils développent pour ce faire des produits et solutions ultra sécurisés et très prisés dans le monde entier. Ces produits et solutions répondent spécifiquement aux exigences des systèmes embarqués et de l'infrastructure informatique associée et ont déjà fait leurs preuves en plusieurs millions d'exemplaires dans le cadre de la production automobile en série.
En France, la marque ESCRYPT est commercialisée par la société ETAS SAS.

Des informations complémentaires sont disponibles : www.escrypt.com