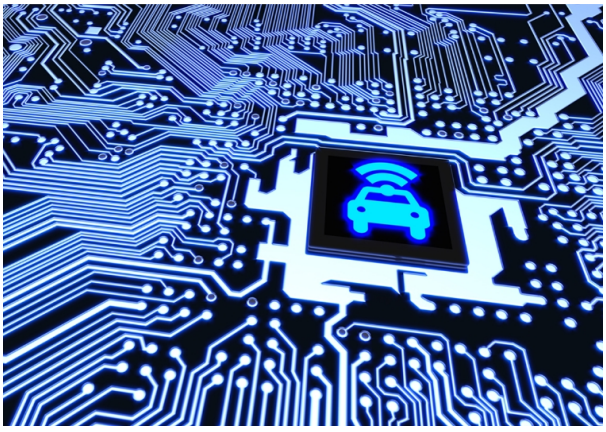
La cybersécurité pour l'automobile



Les nouveaux véhicules sont de plus en plus constitués d'un réseau de composants informatiques qui communiquent en interne, à l'aide d'interfaces câblées et sans fil (CAN, LIN ou Auto Ethernet), et en externe, avec des services télématiques, des systèmes de recharge de véhicules électriques et des systèmes de conduite intelligents.

Les fournisseurs automobiles de niveau 1 sont responsables du développement de la plupart des composants critiques pour la cybersécurité intégrés dans une voiture. Les équipementiers exigent des garanties quant à la mise en place de protections et de contre-mesures adéquates pour assurer la résilience des produits face à des attaquants potentiels.

L'écosystème des normes et réglementations automobiles relatives à la cybersécurité des véhicules et de leurs composants est encore en cours de développement. Le WP.29 de la CEE-ONU est la seule réglementation obligatoire en vigueur, tandis que les équipementiers disposent d'une myriade de normes sectorielles et de bonnes pratiques pour définir les exigences de cybersécurité imposées par les constructeurs de niveau 1.

Afin de démontrer la résistance des composants aux attaques de pointe, les équipementiers et les fabricants de niveau 1 peuvent se tourner vers des laboratoires de sécurité spécialisés pour évaluer leurs produits.

Évaluations de la cybersécurité pour les composants automobiles

Les laboratoires informatiques d'Applus+ ont une solide expérience en matière d'évaluation de la sécurité des composants intégrés au niveau du matériel, des logiciels, des communications et de la cryptographie. Nous disposons d'une expertise avec la pile OSI complète, du démarrage du système aux communications intersystèmes. Cette vue

d'ensemble nous permet d'évaluer des systèmes complexes avec un niveau d'assurance élevé.

Analyse des menaces et évaluation des risques (TARA)

- Examen de la gestion et des activités de cybersécurité globales, par projet et continues pour les phases de conception, de développement et de post-développement du cycle de vie du produit, afin d'atteindre le niveau souhaité de garanties de sécurité.
- Les projets TARA peuvent être réalisés conformément à des normes automobiles spécifiques, telles que ISO/SAE DIS 21434, ou à des cadres moins sectoriels, tels que ISO/IEC 62443, même avec des systèmes TARA personnalisés (tels que des exigences internes).

Évaluations de la sécurité adaptées aux besoins du client

- Nous pouvons adapter l'effort d'évaluation en fonction du niveau d'assurance souhaité (assurance de base, modérée et complète).
- Les cibles d'évaluation vont des composants individuels (SoC, HSM, PCB) aux dispositifs (ECU, TCU, OBC) en passant par les systèmes et les réseaux (3GPP, Bluetooth, CAN, 100-BaseT1).
- Examen de la conception, examen du code source (SCR) et analyse de la vulnérabilité (VA).
- Essais de pénétration complets pour évaluer la résistance aux attaques et la résilience de l'appareil.
- Évaluations personnalisées pour les exigences de conformité OEM/Tier.

Formation à la sécurité et meilleures pratiques (conception et code)

Formations et cours ouverts sur la cybersécurité destinés à des rôles tels que les ingénieurs système, les responsables de la cybersécurité ou les architectes logiciels. Quelques exemples de nos formations :

- Les principes de codage sécurisés les plus récents et la manière dont ils peuvent être appliqués aux opérations quotidiennes.
- Solutions automobiles du point de vue d'un attaquant et comment les dispositifs peuvent être attaqués, en aidant à identifier les moyens d'appliquer ces connaissances à votre produit et de le rendre plus robuste.

Pourquoi choisir Applus+ comme partenaire de cybersécurité ?

- Laboratoire d'évaluation de la sécurité à haut niveau d'assurance avec une expérience dans plusieurs secteurs : automobile, paiements, télécommunications, industrie, téléphonie mobile...
- Techniques et équipements d'attaque de pointe pour évaluer les composants et les dispositifs intégrés dans un véhicule, couvrant les attaques physiques, les attaques logicielles et les attaques réseau et sans fil.
- Expertise pour soutenir la validation d'un cycle de vie sécurisé pendant le développement du produit.
- Empreinte de cybersécurité en Europe (3 laboratoires en Espagne), en Amérique du Nord (1 laboratoire au Canada et 1 laboratoire aux États-Unis) et en Asie (1 laboratoire à Shanghai, en Chine).
- Capacité à couvrir plusieurs normes et réglementations liées à la cybersécurité dans le secteur automobile.

Note : Étant donné que Applus+ Laboratories est accrédité en tant que laboratoire tiers par plusieurs programmes d'évaluation et de certification, et afin de garantir son impartialité, les ingénieurs d'Applus+ ne sont jamais impliqués dans le développement réel des produits ou la mise en œuvre des solutions.