Publicado en Madrid el 15/12/2023

S2 Grupo: "hay que implementar la ciberseguridad en los coches conectados desde la primera fase de su diseño"

Según el último informe de S2 Grupo sobre coches conectados, todavía no existen vehículos con un nivel de ciberseguridad "fiable", porque aún no hay sistema que esté implementado dentro de estos con la capacidad de mitigar incidentes de ciberseguridad. Esto supone un problema en el estado de la ciberseguridad en el vehículo eléctrico y conectado, que requiere del diseño de soluciones específicas para la monitorización de la ciberseguridad de los vehículos eléctricos conectados

El aumento de la conectividad y la automatización de los vehículos inteligentes los expone a amenazas cibernéticas cruciales. Por ello, "es necesaria la implementación de la ciberseguridad desde la primera fase de su diseño para ciberprotegerlos", según el informe "Ciberseguridad en el vehículo eléctrico conectado" que ha realizado S2 Grupo, compañía de referencia en Europa y Latinoamérica en ciberseguridad, ciberinteligencia y en operaciones de sistemas de misión crítica.

Según ha indicado la compañía, estos vehículos están expuestos a distintas amenazas porque, entre otros motivos, tanto ellos como sus puntos de recarga requieren de un buen número de conexiones remotas a efectos de garantizar el mantenimiento, la geolocalización, la gestión de pagos y usuarios, la gestión de incidencias o las actualizaciones de firmware, y cuentan también con interfaces que pueden ser explotadas, en algunos casos, desde fuera.

"No nos estamos planteando qué pasaría si los sistemas que utilizan estos vehículos fueran vulnerados y esto es esencial en estos momentos. Hasta ahora, la seguridad en los vehículos ha estado centrada en evitar peligros físicos y, sin embargo, debido a la creciente conectividad de los vehículos, especialmente para monitorizar el estado de estos, junto con la irrupción de las comunicaciones inalámbricas, ya no es necesario el acceso físico para comprometer el sistema", ha explicado José Rosell, socio-director de S2 Grupo.

"Por ejemplo, si se inyecta un mensaje malintencionado para provocar una operación no deseada, bastaría con que el sistema embarcado interprete dicho mensaje como auténtico para que se llevase a cabo la operación. Estos ataques podrían conllevar la pérdida de integridad del vehículo, suponiendo daños financieros y en la reputación de la marca que lo ha fabricado, pero, además, podrían causar peligros en la seguridad del pasajero", ha continuado Rosell.

Peligros que llegan desde fuera del vehículo conectado

Según se detalla en el informe, las ciberamenazas en este campo pueden dirigirse directamente a los vehículos inteligentes o a otros elementos con los que se relaciona, como pueden ser los semáforos, cargadores, señales o servidores remotos a los que están conectados. Algunos de los ciberataques ya experimentados en el sector han sido contra los cargadores que dejaron de funcionar, robo del coche abriendo sus puertas en remoto y arrancando el motor, o ataques mediante bluejacking (a través del

bluetooth). Junto a esto, podría darse el secuestro de coches o incidentes de software que, por ejemplo, afecten a los ajustes de velocidad.

"Actualmente, no existe un vehículo con una ciberseguridad fiable porque no existe un sistema implementado dentro del interior de estos con la capacidad de mitigar incidentes de ciberseguridad. Aún no se han desarrollado los mecanismos necesarios para cada uno de sus componentes y esto supone un gran problema en el estado de la ciberseguridad en el vehículo eléctrico y conectado. Es necesario trabajar en el diseño de soluciones específicas para la monitorización de ciberseguridad en el ámbito del vehículo eléctrico conectado", ha asegurado José Rosell.

S2 Grupo: Proyecto Estratégico para la Recuperación y Transformación Económica (PERTE) en el sector del vehículo eléctrico y conectado

Ante este contexto, y como parte de la fuerte apuesta de S2 Grupo por la inversión en I+D+i, la compañía está trabajando en la monitorización de ciberseguridad y detección de anomalías en el ámbito del vehículo eléctrico y conectado.

Uno de los focos de atención principales es la detección temprana de cualquier intento de ataque y en especial a las amenazas persistentes avanzadas (APT). Estas pueden emplear una nueva generación de software malicioso y sofisticado con metas concretas y dirigidas, que tienen un nivel de eficacia muy elevado y son sigilosas durante su ejecución. Así, son capaces de ocultarse ante las posibles medidas de seguridad tradicionales.

S2 Grupo está participando en un Proyecto Estratégico para la Recuperación y Transformación Económica (PERTE) en el sector del vehículo eléctrico y conectado, financiado por los fondos Next Generation de la Unión Europea. El propósito es el desarrollo de una nueva solución tecnológica para la detección, protección y respuesta ante cualquier ciberamenaza que afecte a estos vehículos.

La solución propuesta está basada en una herramienta nacional que utiliza tecnología de monitorización y detección de incidentes de ciberseguridad y que ha sido desarrollada por S2 Grupo para entornos IT y entornos OT, y que forma parte del ecosistema de herramientas del CCN-CERT, al mismo tiempo que es la tecnología empleada en los sistemas de alerta temprana del CCN-CERT (SAT-INET, SAT-SARA y SAT-ICS) y en el SOC de la AGE.

La solución deberá poder integrarse físicamente en un vehículo, tanto por dimensiones como por capacidades técnicas, teniendo en cuenta las posibles limitaciones de recursos.

Además, cuenta con capacidades para interpretar y diseccionar las capas de los protocolos más importantes en el vehículo, y para inspeccionar el tráfico de red de los diferentes vectores de entrada inalámbricos del vehículo. Junto a esto, contará con la capacidad de poder alertar tanto a un SOC como al mismo conductor en caso de producirse una alerta que pudiera ser crítica. Estas alertas y casos de uso deberán de generarse a partir de la evaluación de riesgos del vehículo conectado.

Todos estos desarrollos se están probando en un laboratorio específico que recrea la infraestructura del vehículo eléctrico conectado y, entre otros elementos, cuenta con un vehículo de estas características y un punto de recarga, así como las herramientas de hardware y software necesarias para el despliegue de la solución, diagnóstico del estado del vehículo o la interacción con el entorno.

S2 Grupo está avanzando en el desarrollo de una tecnología disruptiva y, hoy en día no asentada, para aportar al vehículo eléctrico conectado y a sus infraestructuras de recarga de la ciberseguridad que necesitan para poder utilizarse.

Datos de contacto:
Luis Núñez Canal
S2 Grupo
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Ciberseguridad Movilidad y Transporte Industria Automotriz Innovación Tecnológica