hackercar.com

Los ciberataques a los que tendrán que enfrentarse los coches autónomos - HackerCar

Silvia Gálvez

8-10 minutos

Los coches ya están **sufriendo ciberataques**. La causa de ello son las distintas tecnologías de conectividad que equipan. Con ellas, el conductor y los pasajeros pueden disfrutar de nuevas funcionalidades de confort y seguridad, pero también los exponen a ciberataques en caso de que el fabricante no haya instalado **las medidas de ciberseguridad necesarias** para evitar que un

cracker haga de las suyas.

Esas posibles vulnerabilidades aumentan a medida que el vehículo en cuestión esté equipado con más tecnología. Y el paradigma de un coche conectado es aquel que puede conducir por sí mismo: el coche autónomo.

¿Qué riesgos específicos tienen los vehículos sin conductor? Una investigación -disponible en este enlace– ha señalado **todas las amenazas a las que los fabricantes deberán hacer frente para evitar crackeos** en sus modelos autónomos. El estudio, realizado por Jonathan Petit -de OnBoard Security- y Steven E. Shladover – de la Universidad de California-, señala **todas las posibles tecnologías por las que podría entrar un ciberataque en un vehículo sin conductor**. Además, los autores indican qué probabilidad de suceder tiene cada riesgo -alto, medio o bajo- y proponen posibles soluciones que deberían implementar los fabricantes para ponérselo más difícil a los ciberdelincuentes.

Estos son los riesgos de ciberseguridad que, según ellos, deberían atajar los fabricantes de coches autónomos.

Alteración de las marcas y señales viales

Para poder circular sin necesidad de que haya nadie a los mandos, los vehículos sin conductor deben ser **capaces de reconocer e interpretar las señales de tráfico que se encuentran a su paso**, así como las líneas dibujadas sobre el asfalto.

El estudio advierte que, **si esas indicaciones son manipuladas, pondrían en un aprieto a los coches autónomos**. Los posibles peligros serían que alguien elimine, modifique o haga ilegible la señal -riesgo alto de que suceda-, o que alguien incluya una señal diferente -riesgo bajo-. Este tipo de alteraciones ya han sucedido, incluso algunos investigadores han comprobado sus efectos sobre coches autónomos.

Como posibles **soluciones a estas amenazas**, el estudio sugiere que el vehículo cuente con una base de datos de señales de tráfico o que el conductor esté alerta.

Visión artificial

Este tipo de sistemas procesan imágenes de vídeo del exterior del vehículo para detectar objetos -carreteras, obstáculos, señales de tráfico, etc-.

Pero los investigadores afirman que **se puede cegar a las cámaras -riesgo alto- o engañarlas para que capten imágenes falsas -riesgo bajo-**. Esos supuestos afectarían a la capacidad de este sistema de analizar la información externa.

Algunas ideas para contrarrestar estos problemas son instalar múltiples cámaras en diferentes ángulos o contar con otro receptor de información que supla a las cámaras en caso de ataque.

GPS

Aparte del ya habitual sistema de posicionamiento con el que cuentan los navegadores integrados en los coches, los vehículos autónomos incluirán otros GPS para controlar la circulación sin conductor.

Sin embargo, **esta tecnología se enfrenta a dos amenazas que tienen un alto riesgo de suceder**: el spoofing y el jamming, que son dos formas de manipular la señal del GPS, pudiendo anular la auténtica e incluso sustituirla por otra falsa en el caso del spoofing.

Para evitar ambos ciberataques, Petit y Shladover recomiendan trabajar en los sistemas de autentificación e incorporar sistemas de navegación que estimen la trayectoria del vehículo en base a sensores odométricos.

Sensores odométricos

Sin embargo, ni siquiera esos sensores son seguros por sí mismos. En esta categoría entran sensores inerciales, como acelerómetros o giroscopios. **Estos mecanismos podrían fallar** en caso de un ataque magnético -alta probabilidad de que suceda- o térmico -probabilidad media-.

¿La solución? Equipar otros sistemas que den información al coche por otras fuentes. Y es que atacar al GPS mediante spoofing y a la vez causar un ataque magnético para inutilizar los sensores odométricos es bastante improbable.

Dispositivos externos

En esta categoría entran **todos aquellos dispositivos que un usuario puede conectar** al sistema de infoentretenimiento del coche a través de Bluetooth, Wifi o el CANbus. O sea, teléfonos móviles, tablets, pen drives…

El peligro con estos elementos radica en que, **si están infectados por un** malware**, este podría traspasarse al vehículo**. La investigación calcula que esto tiene una probabilidad media de suceder.

Algunas medidas de prevención que propone el estudio incluyen la instalación de antivirus o de sistemas de detección, y separar los ordenadores que controlan el sistema multimedia de aquellos relacionados con funciones de seguridad del coche para que un virus que infecte a los primeros no se transfiera a los segundos.

Sensores acústicos

Estos sistemas están entrenados para **reconocer un determinado tipo de estímulo sonoro**. Por ejemplo, un sensor de sonido de choque detecta una colisión más rápido que un sensor de airbag, por lo que desplegaría los airbag con más rapidez. Este componente también considera sistemas ultrasónicos, como el sonar ultrasónico.

¿Cómo podría engañarlos un cracker? Pues reproduciendo sonidos falsos -riesgo alto- o causando interferencias mediante ultrasonidos -riesgo medio-.

Las formas de **mitigar estas vulnerabilidades** propuestas por el estudio son instalando analizadores de espectro de ondas y contar con otros receptores que cotejen la información recibida.

Radar

Los vehículos autónomos usan los **radares para detectar objetos que estén alrededor** y poder esquivarlos. Estos sistemas funcionan mediante el envío de ondas de radio que rebotan contra los objetos que haya en su camino. Al regresar esa onda rebotada, el coche puede sacar información de la forma y colocación del objeto.

La investigación refleja que **hay varias formas de despistar a los radares** para que reciban una señal falsa u oculten la señal que emitiría un objeto. Algunas son sencillas -mediante un ataque de jamming- y otras son complejas -superficies hechas con materiales que absorben la señal del radar para que no rebote.

Para evitar estos riesgos, **lo mejor es que el vehículo no dependa solo del radar** y cuente con otros sistemas de información que los suplan en caso de un ataque de estas características.

Lidar

Similar a los radares en cuanto a funcionamiento, pero envían luz infrarroja en vez de ondas de microondas.

Los riesgos son muy similares a los que tendría un

radar y, por tanto, su forma de evitarlos también.

Sensores del vehículo

Los vehículos cuentan con **gran número de sensore**s. Cada uno de ellos da una información importante para que el coche se comporte de forma adecuada al circular. Por ejemplo, los hay que informan de la velocidad de rotación de una rueda o de la presión de los neumáticos.

Los riesgos relacionados con estos sensores serían **que alguien pudiera interceptar su señal**, con lo que un ciberdelincuente podría, por un lado, acceder a información interna del coche -esos sensores están conectados con el CANbus- y, por otro, ofrecer al vehículo falsas lecturas -algo que ya comentamos aquí-.

Para evitarlo, Petit y Shladover recomiendan aplicar medidas de seguridad internas que no detallan.

¿Están bien protegidos? Para saberlo, el test EUROCYBCAR

Los fabricantes de vehículos pero también de componentes pueden someter a sus productos al Test EUROCYBCAR: **el primer test en todo el mundo que mide y certifica el nivel de ciberseguridad de coches, autobuses, camiones, furgonetas…** y cuyas pruebas se realizan en el CYBERCARLAB, ubicado en el Parque Tecnológico BIC ÁRABA de Vitoria-Gasteiz.

Un test fundamental de cara a lograr algo que será

obligatorio en Europa a partir de julio de 2022 para los vehículos de nueva homologación: que sean ciberseguros y que lo demuestren con un certificado. Para conseguir dicho certificado de ciberseguridad, los fabricantes deberán demostrar que sus modelos están **protegidos contra 70 vulnerabilidades diferentes**.

Ese listado de riesgos a evitar incluye **posibles ciberataques durante el desarrollo, la producción y la posproducción del vehículo**, por lo que aquellos modelos que logren el certificado de ciberseguridad serán ciberseguros a lo largo de todo su ciclo de vida… pero para que un coche sea ciberseguro en su conjunto, también deben serlo cada uno de los componentes que lo forman.