Publicado en el 24/01/2017

Francisco Sancho, de Intel Security, cree que hay que repensar el coche autónomo

El camino por recorrer hasta la implantación completa de los coches autónomos es largo. A los aspectos relacionados con la seguridad física, hay que añadir la ciberseguridad para impedir que, por ejemplo, alguien acceda al control de tu vehículo y haga un uso inadecuado de él. Intel Security desempeña un papel importante en este nuevo paradigma

Francisco Sancho ha desarrollado su carrera profesional en algunas de las compañías más importantes del sector IT. Desde el año 2011, es Product Partner Manager Consumer and Mobile de Intel Security España, una de las empresas referentes del mercado de la seguridad en el mundo.

Año 2020. Si se cumplen las previsiones, los primeros coches autónomos de fabricantes como Ford, estarán circulando por las calles. El conductor disfrutará de un trayecto sin preocupaciones mientras el propio coche le lleva a su destino. Sin embargo, el cuento de hadas se puede ir al traste si alguien accede al sistema de información, alterando, por ejemplo, el sistema de frenos.

La ciberseguridad es el otro campo en el que no sólo están trabajando los fabricantes de automóviles, sino las más importantes compañías de tecnología, que han sabido ver la gran oportunidad que representa el futuro de la automoción. En el caso de Intel Security, han creado incluso una división independiente para investigar y ofrecer los mejores parámetros de seguridad en la llegada e implantación de los coches autónomos. El tiempo corre, y aún hay bastante por hacer.

En Hipertextual hemos hablado con Francisco Sancho, Product Partner Manager Consumer and Mobile de Intel Security España, sobre los aspectos más importantes relacionados con los vehículos autónomos y conectados.

El mundo habla del 5G, el Internet de las Cosas y los vehículos conectados. Son las principales tendencias de futuro que la industria y los medios de comunicación observan y debaten. Pero la materialización de todas esas tendencias, además de nuevas infraestructuras materiales, requieren grandes esfuerzos en otros campos. ¿Estamos actualmente preparados para afrontar, a nivel de seguridad, la materialización de dichas tendencias?

De los tres puntos que comentas, para nosotros hay dos muy novedosos: el Internet de las cosas y los vehículos conectados. El 5G lo vemos como una evolución de la conectividad, capaz de dar más servicios y para los que estamos mejor preparados en caso de tener que resolver los posibles problemas que surjan.

"Estamos trabajando con los principales fabricantes de automóviles para ofrecerles la seguridad que

necesitan los vehículos conectados."

En cuanto al Internet de las Cosas vemos unas problemáticas muy particulares. Primero, la proliferación de sistemas operativos o softwares en diferentes dispositivos. En el mundo móvil hay una consolidación muy clara de iOS, Android y Windows. Sin embargo, en el mundo Internet de las Cosas va a existir una mayor proliferación de nuevos sistemas operativos, mayores limitaciones para poder desplegar seguridad en los dispositivos y, sobre todo, una gran proliferación de dispositivos de bajo coste que llevan asociados niveles de seguridad muy básicos.

Desde Intel Security estamos desarrollando una tecnología propia para proteger los hogares desde una perspectiva consciente de la proliferación de dispositivos con problemas de seguridad. Sabemos que no podemos proteger esos dispositivos, pero sí la conexión a Internet para proteger todo el perímetro del hogar.

En el mundo de los vehículos conectados, la situación exige rediseñar su arquitectura. Venimos de una época en la que, por ejemplo, en los talleres sólo era necesario conectar una máquina para conocer el estado del coche. En el futuro será más complicado y por ello será necesario crear una infraestructura que aporte seguridad. Además, habrá que aislar los componentes vitales del resto del vehículo. Nosotros ya estamos trabajando con varios fabricantes para ayudarles a conseguir esa seguridad.

"Para que los vehículos autónomos sean seguros, necesitamos añadir nuevas capas de cifrado y autentificación biométrica."

Aunque ya existen vehículos como el Tesla Model S, que funcionan conectados a Internet y de forma semi-autónoma, los vehículos autónomos y conectados están dando sus primeros pasos. ¿Cuáles son los mayores riesgos, a nivel de seguridad, a los que se enfrentan los vehículos conectados y, en un futuro, autónomos?

Los principales riesgos a los que nos enfrentamos son ataques a lo que llamamos sistema Core (frenos, motor…), robo de información personal o secuestro o bloqueo del vehículo. En todos estos casos, el intruso podría pedirnos dinero a cambio de recuperar el control.

En el caso de la conducción autónoma, el problema está en proteger la comunicación de vehículo a vehículo o de vehículo a diferentes dispositivos. Para que nadie sea capaz de llevar a cabo un ataque.

Todo esto exige rediseñar el modelo de los vehículos, añadir más funciones de encriptación e implantar Big Data. En Intel llevamos tiempo observando un incremento en la demanda de los sistemas de todo lo que es inteligencia en la nube, y es necesario ser capaces de procesar esa información. Al final todos estos vehículos van a generar y captar mucha información y van a tener que manejarla y

tomar decisiones en tiempo real y, para ello, el manejo del Big Data es crucial.

También estamos trabajando con varias compañías en la conducción autónoma. Dentro de Intel, independientemente de Intel Security, todo lo que son las cámaras o Real Sense, han sido diseñadas para incorporar esas funcionalidades de seguridad.

"No podemos continuar con la dinámica que se está llevando ahora mismo, con cada fabricante creando sus propios estándares y dónde todo funciona bien si estás dentro de su ecosistema."

Con cierta periodicidad se publican noticias sobre hackeos a servicios usados por personas de todo el mundo (Yahoo! es uno de los más recientes). En todos ellos, la información hackeada es sensible (cuentas bancarias, contraseñas, imágenes, etc.). Pero, en el caso de los vehículos conectados y autónomos, un hackeo como el que sufren bancos o servicios online puede traducirse en accidentes de tráfico y, por consiguiente, en muertes. ¿Cómo está trabajando Intel Security y el resto de compañías del sector para evitar ese tipo de hackeos procedentes de una persona con acceso a internet?

En Intel tenemos tecnologías implementadas para ser capaces de hacer identificaciones tanto del software como del hardware. Incluso somos capaces de crear un modo de arranque seguro en caso de que el vehículo esté hackeado. También buscamos que tanto el hardware como el software ajeno a la configuración original, sea capaz de interactuar con nuestro vehículo si no cumple los requisitos de seguridad exigidos.

En caso de que eso ocurra, tenemos la opción de situar esos nuevos componentes en una zona segura, por si existe un problema, ser capaz de aislarlo y que no entre en conflicto con el core del vehículo. Ahí estamos poniendo el foco.

¿Cómo se conectarán los vehículos entre sí? ¿El punto de unión será el sistema operativo, tipo Android Auto o Apple Car Play?
Es complicado porque para ello, en primer lugar, es necesario establecer una definición clara de estándares. No se puede llevar la dinámica que se está llevando ahora mismo, con cada fabricante creando sus propios estándares y dónde todo funciona bien si estás dentro de su ecosistema. Este es el caso de los sistemas operativos iOS o Android. Tiene que existir una unificación.

Las estrategias de conexión se centran en conectar vehículos entre sí, con sistemas de GPS y de navegación o con información de posicionamiento en la nube, y con lo que podemos conocer datos de otros vehículos.

Al estar conectado a Internet o a cualquier dispositivo, acceder a un vehículo estacionado puede llegar a ser más sencillo. ¿Cómo se pueden evitar los robos de los vehículos conectados?

Hay diferentes estrategias. Por ejemplo, con las Unidades de Control Electrónico (ECUS) para evitar que los hackers puedan tomar el control. Sistemas de diagnóstico a bordo para comprobar el estado de los componentes y para que el hacker no pueda entrar en los OBDs.

También es importante trabajar en sistemas avanzados de asistencia a los conductores para evitar que los hackers puedan entrar, tecnología anti malware y aislar los componentes externos.

Por último, es necesario implementar el cifrado y evitar la suplantación de personalidad en las aplicaciones móviles de acceso remoto al vehículo. Para ello, se pueden utilizar sistemas de identificación como la huella digital o la identificación biométrica. Para ello, los desarrolladores deben crear aplicaciones para smartphones sin problemas de seguridad.

¿Tienen cabida los dispositivos de autenticación biométrica como vía de autenticación en los vehículos electrónicos? ¿Podemos esperar su implementación en los próximos años?
Sí. Yo pongo el ejemplo de mi coche. Lanzo la aplicación móvil y la autentificación es el email y la contraseña. ¿Es suficiente? Para mí no. En Intel Security hemos desarrollado una tecnología que nos permite hacer un reconocimiento facial para acceder al dispositivo. No está conectado a la aplicación, pero protege el acceso al teléfono. Esto para mí sí tiene sentido.

Durante los últimos meses, varios grupos de hackers lograron engañar el sistema de detección de obstáculos del Tesla Model S. Afortunadamente, se hizo de forma experimental y no causó ningún incidente. En la vida real, este tipo de sucesos pueden desencadenar accidentes. ¿Cómo se pueden proteger los sistemas de detección de obstáculos y auto pilotaje de esta clase de interferencias —pese a no estar conectados directamente a Internet—?
Lo necesario es desarrollar los sistemas avanzados de ayuda a la conducción y pensar en las medidas anti-intrusión en lo relacionado a la comunicación del vehículo a la nube. Añadir nuevas capas de cifrado y autentificación, repudio, todo lo que sea identificación del vehículo.

Sin ser coches autónomos, llevamos años viendo ejemplos de hackeo de vehículos en los que no se era consciente de que se producía un intercambio de información, y no cumplían las medidas de seguridad. La clave para mi es segurizar todas las comunicaciones de vehículos.

También hay un problema en la parte de cifrado porque son los propios dispositivos los que van a descargar todas esas tareas desde las unidades centrales y se van a encargar de hacer toda la parte de cifrados.

"Hemos hecho un estudio que revela que en 2022, el 78% de los vehículos tendrán capacidades de conducción autónoma".

El smartphone, en múltiples ocasiones, se utiliza como puente en los vehículos conectados. No

obstante, la seguridad del teléfono móvil no puede ser asegurada por el fabricante del vehículo. De esta forma, si un teléfono está "infectado" por cualquier tipo de malware, puede "contagiar" al vehículo conectado. ¿Cómo se pueden evitar estas situaciones?

Teniendo una aplicación de protección en el móvil. Para cualquier tipo de acción. El primer campo en el que actuamos con nuestras medidas de seguridad es el de la banca online, con una aplicación con un módulo en libre de malware y que ve si es seguro acceder o no al site del banco. En este caso, muchos fabricantes nos decían que no podían pedir a sus usuarios que se descargasen nuestra aplicación, pero sí incluir esas funciones en la suya propia.

Lo mismo lo estamos haciendo para vehículos autónomos. Incluir un módulo que analice en primer lugar el dispositivo, y si no se reúnen los requisitos de seguridad exigidos, no permitir el acceso.

En los últimos meses estamos viendo cómo los fabricantes de vehículos están poniendo el foco en el aumento de prestaciones para el usuario y no tanto en la seguridad. Nosotros les decimos a los usuarios: "tranquilo, tu vehículo está conectado y está protegido".

¿Qué pasaría cuando el vehículo vaya por un tramo sin mucha cobertura, por ejemplo, entre montañas o un túnel muy largo? ¿Lo solucionaría el 5G?
Efectivamente, con 5G vamos a tener en general mejor cobertura, pero existen varios problemas como, por ejemplo: si perdemos la conectividad, ¿podemos contar con la información guardada en el vehículo? ¿si el coche está conduciendo de manera autónoma, podemos exigir al conductor que tome los mandos? Es necesario buscar nuevos canales de comunicación para obtener la información, como por ejemplo a través de canales de radio, aunque sea con una señal peor.

¿Podríamos afirmar que, en el futuro, conducir un vehículo conectado y ceder el control al mismo, será un ejercicio seguro?
No hace falta mirar mucho hacia atrás en la historia para ver el ejemplo del primer vehículo de Henry Ford. Casi todo el mundo pensaba que sería un desastre, que no tenía sentido un invento así teniendo los caballos. Veían riesgos como que podía morir gente o ser atropellados. Para evitarlo, se implantaron medidas de seguridad como los semáforos o códigos de circulación.

A día de hoy, con el coche autónomo, nos pasa algo parecido. Por eso es necesario poner una serie de reglas y crear una infraestructura fiable. Y esto, es un trabajo que puede durar años.

¿Cuándo podemos esperar que el vehículo conectado y autónomo sean el estándar en la sociedad?
Bueno, en Intel manejamos un dato de Gartner que dice que, en los próximos cuatro años, el 75% de los vehículos estará conectado a Internet. Es el primer paso. También hay que tener en cuenta los tiempos de renovación de flotas de los vehículos actuales. Qué vida útil tiene un coche, ¿10 años? En ese sentido, el proceso será lento.

En cuanto a la generalización, yo pongo el ejemplo del aire acondicionado. Hace 20 años era un extra

y ahora está incluido en prácticamente todos los coches. Los vehículos conectados es un extra a día de hoy, pero la tendencia apunta a que será una necesidad, una comodidad.

En relación a cuándo será el coche totalmente autónomo, en Intel Security hemos hecho un estudio que revela que en 2022 el 78% de los vehículos tendrán capacidades de conducción autónoma. Hay que distinguir porque hay diferentes escalas, entre ayudas a la conducción o conducción 100% autónoma. Esto va muy ligado a las infraestructuras de comunicaciones y Data Centers.

¿Quién será el responsable en accidentes con coches autónomos?
En este sentido, existe un problema legal. La legislación no está preparada para este caso. Y las compañías aseguradoras, tampoco. ¿Una aseguradora cobrará más si tengo un coche autónomo? ¿Cómo se hace un atestado en el que ha participado un coche autónomo? ¿Vamos a poder hacer un análisis de la información de cada vehículo implicado en un accidente? ¿Hay una responsabilidad subsidiaria de los fabricantes por si ha habido algún fallo?

El presente comunicado fue publicado primero en HiperTextual.com

Datos de contacto:

Nota de prensa publicada en:

Categorías: Automovilismo Sociedad Ciberseguridad Industria Automotriz