Coche conectado, ¿coche "hackeado"?

Por José Antonio Sorroa González-Cavada

EN 2020, **EL 75% DE LOS COCHES VENDIDOS** ESTARÁN CONECTADOS A INTERNET. Y NO SÓLO EL COCHE EXCLUSIVAMENTE, EN 2020 HABRÁ MÁS DE 50.000 MILLONES DE DISPOSITIVOS CONECTADOS A LA RED –HOY EN DÍA LA CIFRA ES, APROXIMADAMENTE, DE 16.000 MILLONES–. COMO ES BIEN SABIDO, EN INFORMÁTICA TODO LO QUE SE CONECTA A INTERNET ES **SUSCEPTIBLE DE SER "HACKEADO"**, INCLUIDOS LOS COCHES...

El 14% de los coches vendidos en la actualidad en el mundo tienen algún tipo de conectividad con el exterior, y esta cifra llegará al 75% en sólo cuatro años. Esto supone que, si las normativas lo permiten, los conductores podrán controlar remotamente sus vehículos, comprobando si está cerrado, su nivel de combustible y un sinfín de nuevas funcionalidades que pueden ser controladas desde el "sillón de casa", usando cualquier dispositivo móvil, ya sean ordenadores, *smartphones o tablets*.

Qué es el coche conectado

Mucho se habla del coche conectado, pero realmente ¿qué es? La conectividad en el vehículo está relacionada principalmente con estos factores: la seguridad integral y los sistemas de ayuda al conductor; el denominado *"infotaintment"* (infoentretenimiento), asociado al uso de Internet y de aplicaciones de a bordo. Por último, el coche autónomo supone una fase más avanzada, en la que aún hay muchos hándicaps por solucionar.

Los ADAS, o sistemas de ayuda a la conducción, destacan por su integración en el coche conectado: novedosos sistemas anticolisión, asistentes de aparcamiento, reconocimiento de señales de tráfico, etc. Ahora viajar en coche es más cómodo y seguro, gracias a estos sistemas, pues permiten una conducción más automática y reducen el error humano, presente en más del 92% de los accidentes.

En cualquier caso, la conectividad persigue un objetivo claro: reducir el número de accidentes gracias a coches más seguros, cómodos y eficientes.

> EL OBJETIVO DE LA CONECTIVIDAD ES REDUCIR EL NÚMERO DE ACCIDENTES CON COCHES MÁS SEGUROS, CÓMODOS Y EFICIENTES

Informados y entretenidos "a bordo"

En una década el coche conectado ofrecerá la misma experiencia de conexión a servicios de Internet que los dispositivos móviles. ¿A quién no le gustaría disfrutar en el coche de servicios de navegación *on line*, información de tráfico en tiempo real, reproducción de música en *streaming*, leer mensajes, enviar o recibir llamadas o interaccionar en las redes sociales... y, lo que es más importante, sin desviar la atención de la carretera?

Algunos fabricantes de automóviles ven en la conectividad una gran oportunidad para ofrecer servicios de valor añadido y soluciones propias que exigen aceptar su catálogo de aplicaciones.

Algunos sistemas de conectividad de fabricantes de vehículos	
Audi	Audi Connect
BMW	ConnectedDrive
Chevrolet	Mylink
Citroën	Connect Box
Ford	SYNC
Mercedes	ME Connect
Opel	OnStar
Renault	RLink2
Skoda	SmartLink
Volkswagen	Connect

Pero cada vez más hay sistemas que facilitan la integración de aplicaciones del *smartphone* del usuario o de los actuales relojes inteligentes a través del sistema de *infotainment* o infoentretenimiento del coche. Se pueden controlar por voz, con el volante multifunción o los mandos del coche para reducir las distracciones del conductor. Y es en este apartado donde entran en juego sistemas de empresas tecnológicas como MirrorLink, Android Auto de Google o CarPlay de Apple.

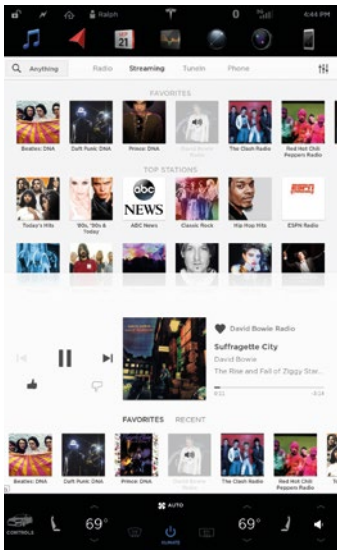
Coche autónomo

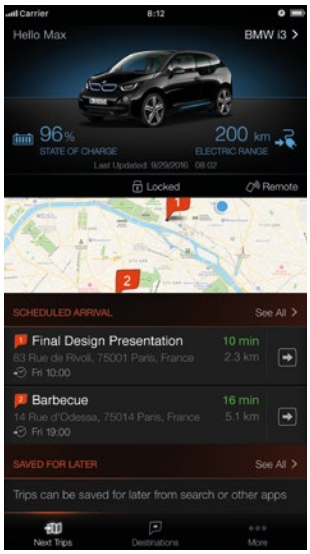
Para que el coche autónomo sea una realidad previamente tiene que desarrollarse la conectividad entre coches y entre vehículo e infraestructura. Este último apartado es el menos evolucionado por los déficits que presenta el entorno. Bosch ha empezado a producir en serie en 2016 nuevos sistemas de asistencia que cubren el aparcamiento remoto, los atascos de tráfico, maniobras de esquiva y giros con tráfico contrario y prevén tener listo un piloto automático para circular automatizadamente por autopista en 2020. Como ejemplos de lo que ya está ocurriendo, este mismo año un camión fabricado por Daimler se ha convertido en el primer vehículo autónomo con licencia para circular sin conductor por las carreteras de Estados Unidos y Volvo ha anunciado que en 2017 entregará una flota de 100 vehículos autónomos a sus clientes para que rueden en sus trayectos cotidianos por algunas carreteras de Suecia. Google también tiene su coche autónomo.
Así pues la conectividad *online* permitirá que los conductores tengan acceso a información sobre atascos, hielo en la calzada o accidentes, así como información para encontrar plazas libres de aparcamiento y lugares de recarga –que se podrá reservar y pagar inmediatamente– para vehículos eléctricos.

¿Coche 'hackeado'?

Cuanta más tecnología de conectividad tenga un coche, más fácil será encontrar puntos vulnerables y poder controlarlo, de alguna manera. Por ejemplo, cuando no había cierre centralizado en los coches, la única forma de acceder a ellos era forzar la cerradura. Ahora, con los accesos sin llave o *keyless*, es más fácil robar el código de acceso para

Cuanta más tecnología de conectividad tenga un coche, más fácil será encontrar sus puntos vulnerables





sustraer el coche. Pero eso son trucos de ladrones profesionales.
La revista "Wired Magazine" ha contado con la ayuda de dos hackers que llevan tiempo investigando sobre las posibilidades que ofrece el automóvil en control remoto: Charlie Miller (ingeniero de seguridad en Twitter) y Chris Valasek (director de investigación de seguridad en el automóvil de Ioactive). El coche elegido ha sido un Jeep Cherokee de última generación, y lo que han hecho ha sido publicado recientemente. Mientras un piloto de prueba conducía el vehículo, los hackers conseguían encender el aire acondicionado, después mandarle una foto y hacer que ésta se muestre en la pantalla del coche; luego activan el sistema de audio a todo volumen, conectan los limpiaparabrisas, etc. Lo peor de todo es que después le apagan el motor e incluso hacen una demostración de lo que pueden hacer con los frenos, en un aparcamiento, eso sí. Encontraron, asimismo, notables brechas de seguridad en el Toyota Prius y el Ford Escape. Tras varios meses de investigación, Miller y Valasek explicaban, entre otras cosas, que fueron capaces de frenar a distancia un Toyota Prius que circulaba a 128 kilómetros por hora, y que también manipularon su volante y frenaron su motor. En el caso del Ford Escape, pudieron desactivar sus frenos cuando éste circulaba muy despacio. Descubrieron otra brecha de seguridad, que afectaba a miles de coches correspondientes a modelos del mismo fabricante, Fiat Chrysler Automobiles, llegados al mercado entre finales de 2013 y 2015. La brecha se localiza en el *chip* que estos automóviles incorporan para permitir su conexión inalámbrica y móvil a Internet. Y, precisamente, a través de Internet es cómo estos dos expertos en ciberataques fueron capaces de rastrear a estos vehículos e intervenir en algunas de sus funciones de forma remota y no autorizada.
No obstante, nos consta el esfuerzo que los fabricantes y sus proveedores están haciendo para proteger sus vehículos, aunque "los malos" siempre estarán ahí...

En definitiva, nos encontramos ante un nuevo mundo de posibilidades, en el que habrá de ser estudiado en detalle su seguridad ■

Seguro Ciber para PYMES y Autónomos, de MAPFRE

La nueva realidad digital y de transformación tecnológica está afectando especialmente a la esfera empresarial. La mayor dependencia de los sistemas informáticos en las empresas, en aras a optimizar su funcionamiento y conectividad, provoca la aparición de ciberriesgos, ciberataques y ciberdelincuentes. Para combatirlos las empresas necesitan protegerse, no solo con prevención, sino también con soluciones aseguradoras.

MAPFRE ha desarrollado un nuevo producto muy completo, que lanzará en 2017 y que, entre otras garantías, contempla la cobertura de daños ocasionados a terceros o a empleados, consecuencia de la publicación, violación, robo o deterioro de los datos contenidos en los sistemas informáticos de la empresa asegurada. Igualmente incluye coberturas por daños propios, que pueda sufrir el asegurado, derivados de un ciberataque y que le puedan paralizar su actividad, indemnizando dicha pérdida y restaurando el software dañado y los sistemas de control de acceso.

PARA SABER MÁS

Área de Informática
ingenieria@cesvimap.com

https://www.youtube.com/watch?v=MK0SrxBC1xs

www.revistacesvimap.com

@revistacesvimap