ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

60/2017 01 de junio de 2017

*Fernando Ruiz Domínguez**

La implantación del automóvil inteligente: ¿un riesgo calculado para la seguridad global?

La implantación del automóvil inteligente: ¿un riesgo calculado para la seguridad global?

Resumen:

El elevado número de vehículos inteligentes existentes en el mundo y los riesgos que estos tienen de sufrir ciberataques se multiplica día a día. Aunque la seguridad total no existe, no podemos ser ajenos a la problemática que estos suponen en cualquiera de sus niveles de automatización.

Así, una visión global del tema nos puede servir para posicionarnos en un entorno evolutivo e inexorable.

Abstract:

The high number of smart vehicles in the world and the risks they have to undergo cyber-attacks multiplies day by day. Although total security does not exist, we cannot be oblivious to the problems they pose at any level of automation.

Thus a global vision of the subject can serve us to position ourselves in an evolutionary and relentless environment.

Palabras clave:

Vehículo inteligente, vehículo conectado, vehículo autónomo, ciberataques.

Keywords:

Smart vehicle, connected vehicle, self-drive vehicle, cyberattacks.

Introducción

El cambio de la no automatización en la conducción de vehículos modernos, en los que el conductor tiene el completo y único control del mismo, a la total automatización de la auto-conducción[1] —para básicamente evitar accidentes[2] y facilitar la movilidad[3]— es un tema muy avanzado tecnológicamente —puesto que incluso se usan sistemas aeroespaciales[4]—, al que esencialmente le queda una regulación legal completa[5] y el salto a la masificación global[6].

Así, a su vez, los vehículos inteligentes o conectados son una realidad y estos se pueden definir como unos sistemas que proporcionan especiales funciones conectadas[7] para mejorar no solo la experiencia de conducción sino la seguridad de los mismos.

Por otra parte, y si bien las tecnologías presentes que incluyen estos vehículos modernos anteriormente citados sirven para mejorar sensiblemente la seguridad de pasajeros y viandantes, también hay que tener en cuenta que los vehículos incorporan o incorporarán las otras tecnologías en desarrollo que con el mismo fin o el de la seguridad de otros conductores, pasajeros e infraestructuras viarias se están desarrollando[8].

---

[1] El estándar SAE J3016 define 5 niveles que van desde la no automatización a la total automatización, Disponible en https://www.sae.org/misc/pdfs/automated_driving.pdf

[2] Ejemplo disponible en https://www.youtube.com/watch?v=-NDsHR8Mj_s

[3] Según el Laboratorio de Informática e Inteligencia Artificial (CSAIL) del MIT, con 3.000 taxis autónomos se podría cubrir el 98 % de la demanda de taxis en Nueva York.

[4] Por ejemplo, la Alianza Nissan-Renault llegó a un reciente acuerdo con la NASA para utilizar su sistema SAM.

[5] Entre otras cuestiones, la de dilucidar los problemas éticos que generan la programación de los algoritmos que usan estos vehículos a la hora de evitar accidentes, como por ejemplo el llamado dilema del tranvía.

[6] TESLA anunció el 19 de octubre de 2016 que los vehículos encargados a partir de esa fecha incluirían el *hardware* necesario para la conducción autónoma. Disponible en https://www.tesla.com/en_GB/blog/all-tesla-cars-being-produced-now-have-full-self-driving-hardware?redirect=no

[7] Básicamente son las siguientes: Telemática, utilizada por ejemplo para la gestión de una flota de vehículos o la geolocalización de estos; Información y entretenimiento que ofrece una oferta multimedia integrada con servicios, como el acceso a una tienda de aplicaciones, etc. y puede acceder a la información de la conducción (velocidad), así como controlar funciones no esenciales (radio, sistema de aire acondicionado); Y la comunicación intra-vehicular, donde las conexiones de info-entretenimiento pueden ser compartidas con dispositivos de usuario, a través de un punto de conexión dentro del vehículo.

[8] Tecnologías de vehículos conectados, como las de Vehículo a Vehículo (V2V); Vehículo a Infraestructuras (V2I); o Vehículo a Todo (V2X); en las que se envían datos entre vehículos, infraestructuras viarias y dispositivos de comunicación personal para mejorar la seguridad, alertando a conductores y viandantes, de accidentes potenciales; o tecnologías relativas al vehículo autónomo.

Por todo ello y tratado desde un punto de vista de aproximación global, genérica y somera a este tema, se pueden mencionar a continuación las siguientes cuestiones teniendo además en cuenta que el coche conectado «es la clave para que llegue el autónomo»[9] y que ya hay una pregunta que flota en el ambiente: ¿Hasta cuándo los ciberatacantes van a estar solo centrados en los ordenadores personales y los teléfonos inteligentes?

Vulnerabilidades y amenazas

Brechas de seguridad

Considerando que el envejecimiento del parque automovilístico a nivel mundial sufrió con la última crisis económica —llegando a superar actualmente, en casos como España, los diez años de antigüedad de los vehículos[10]— y el hecho de que los fabricados con anterioridad al año 2000 sean menos vulnerables[11] a los ciberataques (por su menor conectividad a redes externas), ello no es óbice para que dado el elevado número que suponen los nuevos[12], se pueda decir en términos generales que los automóviles fabricados a partir de 2009 y ya masivamente desde 2015, tienen cada vez más sistemas integrados de control electrónico IoT (Internet de las Cosas) o M2M (Comunicación entre Máquinas) que los hacen más accesibles a los ciberatacantes.

Además, hay que tener en cuenta que las conexiones mediante cableado entre las diferentes unidades de control integradas[13] en un vehículo se han visto reducidas significativamente mediante el sistema de bus central y a que los diferentes fabricantes de automóviles utilizan distintos sistemas para el control del área de red[14], los cuales

[9] Frase pronunciada por Luca de Meo, presidente de SEAT, en el *Automobile* de Barcelona 2017 (un evento donde las marcas de automóviles presentan al público su tecnología).

[10] En concreto 10,8 años en 2017, según la consultora GIPA.

[11] Hay estudios, como los del departamento de seguridad informática de la Universidad de Birmingham que demuestran en el año 2016 que, por ejemplo, se puede clonar con facilidad la señal que emiten los mandos de apertura a distancia de los vehículos del grupo automovilístico Audi, Volkswagen, Seat y Skoda, vendidos desde el año 1995. Esto mismo sucede con otras marcas de vehículos. Disponible en https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_garcia.pdf

[12] Según la consultora tecnológica *Gartner* en 2020 el 75 % de los vehículos estará conectado de una u otra forma a Internet.

[13] Las que controlan la dirección, el motor, los frenos, la telemática, etc.

[14] *FlexRay, Local Interconnect Network (LIN), Ethernet*, etc., si bien el más utilizado es el *CAN* desarrollado por la firma alemana Robert Bosch GmbH (curiosamente con un bajo ancho de banda y el más débil frente

tienen velocidades de transmisión de datos que van desde los pocos centenares de *bytes por segundo,* a superar ampliamente la unidad de millar de estos.

Todo ello sin perder de vista que, a día de hoy, ya hay vehículos que superan los cien millones de líneas de código, y a cuya décima parte ni se acercan las que tiene un moderno avión de pasajeros.

De esta manera, los ciberataques a un automóvil inteligente o conectado se pueden realizar de forma directa:

- Accediendo a los puertos USB (para conexión de dispositivos electrónicos del usuario); conectándose al puerto de diagnosis del ordenador de a bordo[15] (OBD al que acceden habitualmente en todos los talleres mecánicos cada vez que se acude a ellos por revisiones o averías del vehículo y que curiosamente además es legalmente obligatorio contar con el mismo por su relación con las pruebas de emisiones de gases contaminantes[16]); o a través del reproductor de CD-ROM (dispositivo cada vez más obsoleto) o puertos para dispositivos USB[17] (sus sustitutos).

Por otra parte, los ciberataques se pueden producir también de forma inalámbrica a corta distancia[18] y a larga distancia[19].

- En el primer caso, se utilizan como puntos de acceso: El control remoto de las llaves para acceder al vehículo; el sistema de monitorización de la presión individual de los neumáticos; los sistemas de asistencia avanzada al conductor; el sistema de conexión de dispositivos con *bluetooh* (como los *smartphones*); o el sistema de conexión a la red inalámbrica *wi-fi*[20].

---

a ciberataques).

[15] En algunos casos (por ejemplo, los que cuentan con un dispositivo *dongle* – un tipo de *hardware* auxiliar- que permite a su vez la conexión *bluetooth o wi-fi*) también se puede acceder a los OBD por vía remota.

[16] El *On-board Diagnostics* (OBD) es obligatorio en EE.UU. desde 1996 y en la U.E. desde 2004 (el OBD-II se encuentra disponible en la UE desde 2001).

[17] Los Universal Serial Bus (USB) son unos puertos para conexión de dispositivos de almacenamiento masivo de texto, audio, vídeo o imágenes, los cuales utilizan genéricamente el nombre de dispositivos USB.

[18] Entre 5 y 300 metros.

[19] A más de 1000 metros.

[20] Existen múltiples sistemas de conexión telemática en el mercado del automóvil y vinculadas a diferentes fabricantes, tales como: On Star; Sync; Safety Connect; etc.

- En el segundo caso, mediante las comunicaciones de radio AM/FM; las de teléfono móvil; o por vía satélite.

En definitiva, el acceso al puerto de diagnosis del ordenador de a bordo (OBD) supone un riesgo limitado ya que se requiere el contacto directo con el mismo y, por lo tanto, en caso de ataques múltiples, la necesidad de hacerlo uno a uno por parte de los ciberatacantes.

Sin embargo, el acceso mediante medios inalámbricos supone la posibilidad de poder atacar a múltiples objetivos al mismo tiempo, lo cual, si tenemos en cuenta que uno de ellos es a través de las conexiones telefónicas, esto complica el asunto exponencialmente, puesto que además habría que añadir el factor de que las mismas se pueden llevar a cabo desde cualquier parte del planeta.

Al menos desde el año 2011, se han llevado a cabo diversos trabajos de investigación[21] que confirman la seriedad de la amenaza que pueden suponer este tipo de ataques que comprometen la seguridad y la privacidad de las personas. Algunos de ellos culminaron con conocidos resultados públicos, principalmente en 2015[22] [23] y de entre los cuales —como en este último caso y sin duda por la gran repercusión mediática— los hay que llevaron a la revisión de algún modelo de vehículo por parte del fabricante.

Aunque si bien el tipo de ataques pueden suponer: fraudes, apropiaciones de las propiedad empresarial o intelectual, filtraciones de datos, daños colaterales por manipulaciones indebidas con otros fines, denegaciones de servicio, propagación de *software* malicioso, etc., lo cierto es que los mismos, en términos generales, tienen dos grandes grupos de amenazas como son el acceso no autorizado a los datos[24] y los ataques maliciosos mediante el control de los vehículos[25].

---

[21] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage (University of California, San Diego), Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno (University of Washington), Comprehensive Experimental Analyses of Automotive Attack Surfaces, 2011, Disponible en http://www.autosec.org/pubs/cars-usenixsec2011.pdf

[22] CBSnews.com, *Car hacked on 60 Minutes*, 06-02-2015, http://www.cbsnews.com/news/car-hacked-on-60-minutes/

[23] Wired.com, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, 21-07-2015, Disponible en https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[24] Robo, sabotaje, vigilancias ilegales, etc.

[25] Daños, atentados terroristas, etc.

Finalmente en este apartado hay que mencionar que algunos de los ciberataques que se podrían efectuar a distancia y que ofrecen mayor peligro se pueden materializar a través de los tele-servicios[26], aplicaciones para teléfonos móviles[27] [28], los servicios a distancia[29] o las páginas de internet para la administración a distancia de los vehículos[30] [31].

Pero, cuando parecía que esto era todo, la cuestión se podría complicar aún más con la comercialización masiva[32] de ingenios tecnológicos por empresas ajenas al fabricante del automóvil, los cuales han sido diseñados para facilitar la conectividad de los vehículos fabricados a partir de 2002[33] y que no tuvieran la misma funcionalidad instalada de serie a bordo. Dichos dispositivos conectados al puerto OBD del vehículo, mediante una instalación que los deja totalmente ocultos a la vista, permiten al usuario un acceso remoto a su vehículo —por ejemplo mediante un teléfono inteligente—, que va desde la geolocalización al control parental, pasando por la emisión de alertas, estadísticas, etc.[34]

Acceso no autorizado a datos

En este supuesto las implicaciones se refieren no solo al acceso o robo de información personalmente identificable —como pueden ser las cuentas de correo electrónico, los números o información de las tarjetas de crédito, etc.— sino también a los datos de

[26] Ataque del tipo *Man in the Middle* mediante la suplantación del código que se instala en el vehículo (por ejemplo, a la hora de efectuar una actualización de *software*).

[27] Las *In Car Smartphones Apps* permiten que los ciberatacantes creen aplicaciones para suplantar a las aplicaciones autorizadas por los fabricantes de vehículos o las oficiales.

[28] La creación de *hotspots* de *wi-fi* gratuito permite la descarga de *malware, camuflado como una Aplicación legítima,* con el que se puede robar fácilmente un vehículo inteligente tras haber obtenido el nombre de usuario y contraseña. Disponible en https://www.youtube.com/watch?v=5jQAX4540hA

[29] Son los que convierten a los teléfonos inteligentes en un mando a distancia con el que se puede efectuar diferentes acciones con el vehículo como arrancarlo, poner en funcionamiento la climatización, etc. Ejemplo: http://www.volvocars.com/es/servicios-cliente/extras/volvo-on-call

[30] Mediante la sustracción previa de las contraseñas, se podría acceder a estos servicios.

[31] En julio de 2016 se detectaron, por ejemplo, dos vulnerabilidades en la página *BMW ConnectedDrive*. Disponible en https://www.vulnerability-lab.com/get_content.php?id=1736

[32] De momento en Francia se han instalado más de 7.000 unidades del modelo MIDAS Connect y en España el mismo se comercializa desde diciembre de 2016.

[33] Compatibilidad con el 85 % de los modelos de vehículos para el modelo MIDAS Connect.

[34] Por ejemplo, las del modelo MIDAS Connect, Disponible en http://www.midas.es/midas-connect

control electrónico o de conducción. Es decir, ello incluye no solo la información facilitada voluntariamente por los usuarios —sobre, por ejemplo, la localización del vehículo, la velocidad, el conductor, el propietario o los pasajeros—, sino también los datos de conducción recopilados por los sistemas electrónicos del vehículo mientras estos son almacenados a bordo o son transferidos desde el vehículo a otro lugar (para su uso o almacenamiento).

Además, recientes ciberataques genéricos a escala mundial[35] no solo refuerzan esta posibilidad sobre los vehículos inteligentes, sino que dan buena cuenta de las dimensiones que podría tener el asunto.

Ataques maliciosos mediante el control del vehículo

Llegados a este punto, a nadie se le escapa que el riesgo de ciberataques a los vehículos inteligentes puede generar daños personales y materiales, por lo que las implicaciones pueden ir más allá de los que puedan producir los ataques individuales —máxime dado el nivel de sofisticación[36] y formación requerido— ya que inevitablemente la autoría potencial se centraría mayoritariamente en los grupos del crimen organizado y del terrorismo —aunque sin olvidarnos de las posibilidades que ofrece de cara a una ciberguerra[37]— puesto que todos los implicados mencionados, por regla general, poseen más recursos y motivación para su ejecución.

Por otra parte, la singularidad de la dualidad de uso de los modelos de automóviles voladores[38], cada vez más avanzados y presentes en la actualidad y en nuestro futuro inmediato, nos hace plantearnos la cuestión del riesgo que entrañaría el uso en su

[35] Por ejemplo, en mayo de 2017 en el que mediante un *exploit – software* enmascarado que corrompe el sistema informático- los *hackers* utilizaron la técnica del *ransomware* – rescate para desencriptar los archivos – para atacar masivamente a grandes empresas a nivel mundial.

[36] No siempre es así, dado que hay casos como el de un joven de 14 años que con equipamiento técnico por valor de tan solo 15 dólares fue capaz de abrir un vehículo e incluso entre otras cuestiones, arrancar de forma remota su motor durante el *SAE Battelle CyberAuto Challenge* de 2015, Disponible en http://www.sae.org/events/pdf/cyberauto/2015_cyberauto_brochure.pdf

[37] YouTube, *Hacking a Car with an Ex-NSA Hacker: CYBERWAR*. Disponible en https://www.youtube.com/watch?v=MeXfCNwMG64

[38] Por ejemplo el de la empresa eslovaca Aeromobil, Disponible en https://www.aeromobil.com/official-news/

fabricación del mismo tipo de sistemas informáticos vulnerables que, como se verá, utilizan los más conocidos fabricantes de automóviles puros.

No hay que olvidarnos de que algunos de estos automóviles voladores son capaces de hacerlo: a más de cien kilómetros por hora, a alturas de hasta unos 3.000 metros[39] y con autonomías de más de 500 kilómetros, lo cual supone, en el caso que nos ocupa, un riesgo añadido al de un vehículo exclusivamente terrestre, al poderlo estrellar, por ejemplo, contra un objetivo protegido perimetralmente mediante elementos físicos de contención.

De la misma manera y dados los múltiples ataques terroristas con camiones lanzados sin control por diferentes suicidas contra una masa humana, no podemos olvidar que el riesgo de ataques mediante los vehículos inteligentes o conectados que se analizan no se reduce al sector del automóvil de pasajeros, sino que también nos encontramos con este tipo de tecnologías en autobuses[40] y camiones [41][42] de diferentes marcas y fabricantes a nivel global.

Posibles consecuencias económicas y políticas

Igualmente hay que tener en cuenta al ya de por sí complejo mundo de los seguros y reaseguros y las implicaciones crematísticas que pueden acarrear los ciberataques masivos a la hora de que una compañía o varias hagan frente a las demandas particulares para obtener estos las correspondientes indemnizaciones; y el no olvidarnos del posible daño colateral que puede suponer que se ponga en cuestión mediática la seguridad y fiabilidad de un determinado producto.

[39] Porque sus cabinas no están presurizadas.

[40] Por ejemplo, los de la marca Navya que circulan por París desde octubre de 2015 o en Las Vegas desde enero de 2017. Disponible en http://navya.tech/

[41] MIT Technology review, *Mining 24 Hours a Day with Robots*, 28-12-2016, Disponible en https://www.technologyreview.com/s/603170/mining-24-hours-a-day-with-robots/

[42] Aunque se trata de un mero ejemplo de una versión cinematográfica de un libro basado en hechos reales de hace décadas y evidentemente la manipulación de los elementos de control del camión que se muestra en la misma está realizado mediante la incorporación de otros elementos técnicos accionados a su vez por radiofrecuencia que actúan sobre la dirección y los frenos, ello nos puede servir para hacernos una idea del potencial y usos que en la actualidad puede tener este tipo de ataques trasladados a los vehículos inteligentes y a unos camiones que ni siquiera necesitaría del terrorista suicida pues este ya no iría a bordo. *Killer Elite*, 2011, minuto 52 al 53, Disponible en https://www.youtube.com/watch?v=MYNknmvDtyA

Así, y aunque es cierto que la seguridad total no existe, no lo es menos que una llamada general a revisión de un determinado modelo de vehículo puede suponer como mínimo la paralización de múltiples ventas previstas para dicho fabricante; o un descalabro político, si no se ha previsto, por ejemplo, la diversificación de proveedores de vehículos inteligentes a la hora de dotar con una flota de ellos a los servicios de emergencias o fuerzas y cuerpos de seguridad.

Tampoco se puede perder de vista el volumen de vehículos que representa actualmente este asunto sobre el mercado de este sector empresarial a la hora de comprender no solo el potencial de las amenazas, sino también el de las consecuencias ya que, según los analistas del mismo, durante 2017 se alcanzará la cifra del 60 % de dichos vehículos sobre el volumen total de vehículos a nivel mundial y en casos como EE.UU. y Europa occidental ello supondrá hasta el 80 %[43].

Dificultades internas y desde el inicio

Sin duda alguna, la falta de comunicación, transparencia, y colaboración en materia de ciberseguridad de vehículos entre los participantes de toda la cadena de suministros que los mismos necesitan para su diseño, producción, etc. genera los grandes problemas y retos a los que dicha industria de automoción se tiene que enfrentar.

En concreto donde se ven claramente estas dificultades es en relación a la vulnerabilidad que suponen las redes de comunicación donde los códigos del *software* de todos los proveedores de la cadena productiva tienen que interactuar.

Por otra parte, el eterno dilema de la relación entre los beneficios para el comprador/usuario del vehículo y los costes de producción para la red empresarial, genera otro problema que se antoja insalvable sin un posicionamiento legal de los actores gubernamentales a nivel global y que consiste básicamente en determinar también aquí y para estas nuevas amenazas, el marco mínimo de seguridad de los productos introducidos en el mercado, para que el fabricante pueda determinar si

[43] ABI Research.com, *By 2017 60 % of New Cars Shipping Globally Will Feature Connected Car Solutions*, 03-07-2012, Disponible en https://www.abiresearch.com/press/by-2017-60-of-new-cars-shipping-globally-will-feat/

empresarialmente resulta interesante repercutir todo, parte o nada, de los costes en ciberseguridad, sobre el precio final que deben abonar los compradores de los mismos.

Además, si ya de por sí empezar a trabajar en el asunto viene lastrado por todas estas dificultades, hay que añadir que: encontrar a técnicos especialistas en ciberseguridad no es tarea fácil, puesto que su número es reducido; que evidentemente estos deberían estar especializados en la industria del automóvil; y que además deberían de resistir (principalmente a base de buenos incentivos laborales) la tentativa de ser fichados por otras grandes empresas tecnológicas ajenas a la industria de la automoción. Es decir, todo un reto que seguramente necesite un cambio de enfoque y una búsqueda de apoyos superiores.

Incluso una vez iniciada la fase de desarrollo tecnológico de un nuevo producto hay que tener en cuenta que actualmente y en este sector, el mismo no verá la cadena de producción hasta pasados normalmente unos cinco años. Por lo tanto, en su momento, el vehículo recién puesto en la calle estará dotado de una tecnología en materia de ciberseguridad posiblemente ya obsoleta o con un dilatado tiempo de estudio por parte de los ciberatacantes, que la hagan vulnerable si la misma no se puede actualizar de manera eficaz en el momento de ser vendido el vehículo.

Por si no fuera suficiente, firmas tecnológicas como Apple o Google[44] están interesadas en el mercado de los vehículos autónomos y por ello se encuentran desarrollando sus propios productos[45], pero sin olvidar que el gran negocio se encuentre probablemente en el *Big Data*[46].

[44] Con los problemas añadidos que suponen la centralización de servicios, las cuentas de correo electrónico asociadas e incluso el almacenamiento de las grabaciones de voz recopilados de los clientes (https://support.google.com/websearch/answer/6030020?hl=es) , por lo que las posibilidades de ciberataques se elevan sustancialmente hasta límites insospechados.

[45] Más centradas en el *software* que en el propio *hardware*.

[46] Mediante el ofrecimiento a los usuarios de estos vehículos, de paquetes de servicios y aplicaciones para teléfonos inteligentes.

Investigaciones y medidas adoptadas: ¿todo sigue igual?

Teniendo en cuenta, y según lo visto, que las actualizaciones de *software* y de *firmware* son una de las formas más importantes para prevenir o mitigar los efectos de los ciberataques, pero que estas desgraciadamente no se producen salvo por un reducido número de fabricantes y de forma limitada[47]; que la separación total entre los sistemas electrónicos de seguridad crítica y no crítica es imposible o carente de practicidad[48]; que también se sabe que existen medios para lograr una cierta protección de las unidades de control electrónico, de las redes de conexión a bordo o de las redes de comunicación externas, de los vehículos[49]; etc.; resulta de interés ver por comparación qué es lo que últimamente están haciendo algunos de los bloques más influyentes al respecto, dado que en algún momento habrá que decidir algo de cara al futuro.

Estados Unidos

Aunque desde septiembre de 2016 se aboga por una estricta política de seguridad[50] con respecto al diseño y venta de los vehículos altamente autónomos[51] —que obliga a los fabricantes a incluir en los mismos, por ejemplo, un sistema de grabación de datos de conducción que se pueda compartir[52] o medidas para evitar los ciberataques—, esto no resuelve la compleja cuestión pues la normativa es específica para ellos y no incluye al

[47] De ellos, solo Tesla puede actualizar todos los sistemas críticos y no críticos y además haciéndolo de forma remota para todos sus vehículos, aunque eso no evita que sus vehículos puedan sufrir un ciberataque. De hecho, el informe de tres expertos informáticos chinos de la empresa *Keen Security Lab,* del grupo Tencent, puso en evidencia dicho extremo en septiembre de 2016 al hacerse con el control de un Tesla modelo S. Disponible en http://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

[48] Por ejemplo, la desconexión automática del sistema de reproducción de vídeo cuando el vehículo se encuentra en marcha (para que el conductor no se distraiga) supone que el sistema de infoentretenimiento tenga información de que el vehículo está siendo conducido en ese momento (de los sistemas de dirección, freno, gestión del motor, etc.).

[49] *Firewalls* (cortafuegos); Gateway (para facilitar la separación de los sistemas de seguridad crítica y no crítica); Mensajes de autentificación y encriptación (para proteger no solo las señales recibidas sino las transmitidas entre los diferentes sistemas conectados); Sistemas de prevención y detección de la intrusión; Módulos de seguridad *(hardware*); Micro núcleo (pequeño *software* para enviar información fiable entre unidades de control electrónico); etc.

[50] DOT, NHTSA, Federal Automated Vehicles Policy. Accelerating the Next Revolution In Roadway Safety, septiembre 2016, Disponible en https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf

[51] Autonomía de nivel 3 o superior, según estándar SAE J3016.

[52] Una especie de “caja negra”.

resto de los vehículos inteligentes o conectados, pese a que estos cuentan con sistemas que permiten cierto grado de conducción automatizada.

Ley MAP-21

Se trata de una ley promulgada en 2012, dirigida a la NHTSA[53] y en la que en definitiva se busca dejar clara la necesidad de llegar a unos estándares de seguridad en relación a los sistemas electrónicos en los vehículos de pasajeros y en especial en lo que se refiere a las necesidades de seguridad de los componentes electrónicos para evitar el acceso no autorizado.

Ley FAST (*Fixing America's Surface Transportation Act*).

Promulgada en 2015 exige al DOT[54] el remitir un informe al Congreso sobre las operaciones del Consejo de Electrónica[55], algunas de las cuales se establecieron en la Ley MAP-21 para proporcionar un foro para la investigación, la regulación y que las Agencias de Seguridad coordinen y compartan información internamente sobre la electrónica de vehículos avanzada y las nuevas tecnologías.

Proyecto de Ley de Seguridad y Privacidad en el automóvil *(Security and Privacy in Your Car Act[56]).*

El 21 de julio de 2015 fue remitida a la Comisión de Comercio, Ciencia y Transporte del Senado[57]. La intención es que con ella la NHTSA lleve a cabo una regulación sobre asuntos referidos a la ciberseguridad de los vehículos y en especial en lo que se refiere a aquellos fabricados para la venta en EE.UU. El objetivo es proteger a los ciudadanos del acceso no autorizado a sus vehículos.

Lo significativo de todo ello es que los fabricantes tendrán que dotar al vehículo con sistemas que sean capaces de detectar, informar y detener tentativas para interceptar los datos de conducción o el control no autorizado del mismo.

[53] *National Highway Traffic Safety* Administration (Administración Nacional de Seguridad del Tráfico en las Carreteras).
[54] *Department of Transportation* (Departamento de Transporte).
[55] Abreviatura del *Council for Vehicle Electronics, Vehicle Software and Emerging Technologies*.
[56] Conocida como la *SPY Car Act*.
[57] Congress.gov, Disponible en https://www.congress.gov/bill/114th-congress/senate-bill/1806/all-info

Proyecto de Ley de Estudio de Seguridad y Privacidad en el automóvil *(Security and Privacy in Your Car Study Act).*

Remitido a la Subcomisión de Negocios, Manufacturas y Comercio, del Senado el 11 de junio de 2015[58] este Proyecto de Ley busca que la NHTSA dirija un estudio para determinar y recomendar los estándares de seguridad para la regulación de la ciberseguridad de los vehículos de motor fabricados o importados, para su venta en EE.UU.

Básicamente se busca: identificar las medidas de aislamiento necesarias para separar los sistemas de *software* crítico que puedan afectar al control de los movimientos del vehículo, de los otros sistemas de *software*; así como de las medidas necesarias para detectar y evitar o minimizar los códigos anómalos en los sistemas de *software* del vehículo que están asociados a comportamientos maliciosos; o incluso todo lo referente a la seguridad vinculada a la recogida de datos sobre la conducción del vehículo, el conductor y los pasajeros.

Automotive ISAC

En otro orden de cosas, centrado en los aspectos más prácticos de este tema y sirviendo desde finales de 2015 para la recopilación de inteligencia, análisis y discusión entre sus miembros que anónimamente compartan información sobre amenazas y vulnerabilidades, se encuentra el *Automotive ISAC*[59], dirigido por dos asociaciones industriales[60].

A largo plazo se desconoce el papel que pueda desempeñar la misma pero, debido a que lo cierto es que, a día de hoy, dada la heterogeneidad de las arquitecturas técnicas de los diferentes modelos de vehículos existentes en el mercado y a que los distintos fabricantes son potencialmente competidores en el mismo, nada hace suponer que se logren grandes metas en ese sentido si no se introducen otras variables en la ecuación.

[58] Congress.gov, Disponible en https://www.congress.gov/bill/114th-congress/house-bill/3994

[59] *Information Sharing and Analysis Center*.

[60] *Alliance for Automobile Manufacturers y Association of Global Automakers.*

SAE International[61]

También es importante reseñar que desde 2012 dos equipos de trabajo dirigidos por representantes de los fabricantes de vehículos de EE.UU. estuvieron trabajando en materia de ciberseguridad y específicamente en los riesgos que se plantean en el desarrollo de un nuevo vehículo. El resultado, en enero de 2016, fue la SAE J3061[62], una guía de principios básicos para incorporar protecciones de ciberseguridad en el desarrollo de vehículos.

La complejidad y peligrosidad del tema

Finalmente, en este apartado hay que mencionar que, si ya de por sí el tema es complejo, en EE. UU. nos encontramos con la presencia de múltiples agencias de seguridad que tienen competencias de una u otra manera en el asunto, lo que añade la dificultad no solo del reparto de tareas sino del trabajo conjunto y coordinado. Así, desde el FBI, el DHS, etc. tendrían que trabajar con la NHTSA, lo cual a día de hoy sigue sin definirse por completo.

Tampoco nos podemos olvidar del hecho que el FBI ya alertó en 2014[63] sobre la posibilidad de ataques terroristas mediante vehículos inteligentes o en 2016 sobre el incremento de sus vulnerabilidades ante ciberataques[64]; y que, por ejemplo, una empresa tecnológica puntera como IBM trabaja en el desarrollo de antivirus específicos para estos vehículos conectados, basados en la tecnología *QRadar* empleada en el estratégico sector bancario.

Unión Europea

Por su parte y no menos complejo en la Unión Europea, el planteamiento pasa por poner de acuerdo a todos sus Estados miembros, lo que generalmente conlleva mucho tiempo y esfuerzos, pero sin que por ello se hayan dejado de lado las correspondientes

---

[61] Society of Automotive Engineers. Una organización que desarrolla estándares para la industria de este tipo.

[62] Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.

[63] FBI, Directorate of Intelligence/Strategic Issues Group, *Strategic Perspective: Executive Analytic Report, Autonomous Cars Present Game Changing Opportunities and Threats For Law Enforcement,* 20-05-2014.

[64] FBI, *Motor vehicles increasingly vulnerable to remote exploits*, 2016, disponible https://www.ic3.gov/media/2016/160317.aspx

regulaciones normativas —como la Declaración de Ámsterdam firmada el 14-04-2016 por los 28 ministros de transporte de la UE— y los programas de investigación pertinentes, cuyos resultados podrán servir de base para la adopción de las oportunas decisiones futuras, como un reglamento común en materia de movilidad inteligente que evite que cada Estado vaya regulando por su cuenta y luego haya que armonizar todas esas normativas con el resto de ellos.

De esta manera se pueden mencionar las siguientes líneas de trabajo:

Proyecto EVITA *(E-safety Vehicle Intrusion-protected Applications).*

El mismo se llevó a cabo desde julio de 2008 a diciembre de 2011, con un presupuesto de 5,8 millones de euros y centrado en tratar de proporcionar una base futura para el despliegue seguro de las ayudas electrónicas de seguridad basadas en la comunicación vehículo a vehículo y vehículo a infraestructura.

En este sentido, el resultado alcanzado fue el desarrollo de un prototipo de investigación que no puede ser integrado directamente en los vehículos de producción[65], destacando además que los participantes en este proyecto no solo fueron empresas europeas sino también las filiales europeas de una empresa matriz japonesa[66], lo que igualmente deja constancia de que el mercado asiático también está interesado en este tema y no solo los dos grandes bloques que, como mero ejemplo, se ponen en contraste en este trabajo.

Proyecto PRESERVE *(Preparing Secure Vehicle-to-X Communication Systems).*

Básicamente este proyecto europeo iniciado en enero de 2011; finalizado en junio de 2015; y con un presupuesto de 5,4 millones de euros; contribuye a la seguridad y privacidad de los futuros sistemas de comunicación vehículo a vehículo y vehículo a infraestructura, al abordar problemas críticos como el rendimiento, la escalabilidad y el despliegue de los sistemas de seguridad V2X.

El resultado final y conclusiones del proyecto supusieron el acuerdo sobre que los vehículos inteligentes y los autónomos crearán nuevos retos y ataques, y esto requerirá que las actividades de investigación no deban detenerse y el buen diálogo e intercambio de información entre el mundo académico, la industria y los actores políticos deberá

[65] EU, CORDIS, EVITA, Disponible en http://cordis.europa.eu/docs/projects/cnect/5/224275/080/deliverables/001-EVITAD442.pdf
[66] Fujitsu.

continuar en el futuro. Además, y dado que se trata de un desafío mundial, el tema en su conjunto también debe tratarse de una manera mundial y armonizada.

Nuevo estándar ISO[67] en ciberseguridad para vehículos.

Se trata de un proyecto similar al de *SAE International* anteriormente visto e impulsado principalmente por fabricantes alemanes de vehículos[68] que voluntariamente se centran en el desarrollo de un estándar de seguridad —también voluntario— para el diseño y desarrollo industrial en el sector de la automoción.

Se pretende que sea muy flexible en cuanto a las obligaciones de los adheridos y que, por tanto, no implique el uso obligatorio de determinadas tecnologías para alcanzar los objetivos.

Por otra parte, y debido a la similitud del proyecto con el de *SAE International,* ambas organizaciones acordaron a finales de 2015 unificar esfuerzos y poner los trabajos en común, aunque para ver grandes resultados posiblemente haya que esperar más años.

Normativa EU y ciberseguridad de los vehículos inteligentes.

A todo lo visto hasta el momento hay que añadir una fecha de especial trascendencia y marcada por la votación favorable del Parlamento Europeo, el 25-04-2015, a la iniciativa estratégica de la Comisión Europea sobre el mercado único digital. De esta manera el mismo decidió que todos los vehículos fabricados en Europa a partir de abril de 2018 estarán equipados con la tecnología *eCall*[69], la cual en caso de accidente grave permite la llamada automática a los servicios de emergencia.

Es decir, surge la recurrente paradoja de que, por una parte, se pretende salvar vidas humanas con la introducción de un adelanto técnico pero, por otra, el mismo es susceptible de ser utilizado para quitarlas con la misma o mayor efectividad, en este caso si se produce un ciberataque.

[67] *International Organization for Standardization.*

[68] *United States Government Accountability Office, Vehicle Cybersecurity*, marzo 2016, página 30.

[69] European Commission, *eCall: Time saved = lives saved*, Disponible en https://ec.europa.eu/digital-single-market/ecall-time-saved-lives-saved

Además, y vinculado directamente a esta última decisión, tenemos la reciente normativa de la UE que afecta, sin lugar a dudas, a los vehículos en cuestión, por cuanto los mismos suponen un punto de captación, almacenamiento, tratamiento, etc., de datos de todo tipo:

- El Reglamento General de Protección de Datos[70] de la UE 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016 se refiere a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y ha supuesto la derogación de la Directiva 95/46 /CE;
- La Directiva sobre seguridad de las redes y la información (NIS)[71] de la UE 2016/1148 del Parlamento Europeo y del Consejo, se refiere por su parte a las medidas para un alto nivel común de seguridad de los sistemas de red y de información en toda la Unión.

Por su parte ENISA se ha volcado en el asunto de la ciberseguridad de los vehículos inteligentes y así ha transmitido recientemente su preocupación a la UE evaluando múltiples escenarios[72].

Logotipo de la agencia ENISA de la UE

[70] Disponible en http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

[71] Disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG

[72] ENISA, *Cyber Security and Resilience of smart cars, Good practices and recommendations*, diciembre 2016, ISBN: 978-92-9204-184-7.

El caso normativo de España

En nuestro país destaca más el interés gubernamental por regular la cuestión del vehículo autónomo y así se publicó la normativa que establece desde el 16-11-2015, el marco para la realización de pruebas con vehículos de conducción automatizada en vías abiertas a la circulación.

Además, la Dirección General de Tráfico, mediante el proyecto de Movilidad Autónoma y Conectada, trabaja en un primer reglamento con la intención de regular los vehículos autónomos en 2017, pero como ello lleva implícito la modificación de la ley de seguro obligatorio y la de seguridad vial, posiblemente la cuestión se demore algo más.

Que de la misma manera, a nivel comercial se apuesta fuerte por este tipo de tecnología, dado por ejemplo el interés de la marca TESLA en el país y su política de rápida expansión mediante su creciente red de supercargadores[73].

Es decir, se constata un desembarco progresivo de la tecnología del vehículo autónomo, lo cual lleva aparejado todo lo que se viene analizando hasta el momento, por ser este tipo de vehículo el peldaño más alto dentro de los vehículos inteligentes o conectados.

Medidas futuras

Aunque la División de Investigación de Seguridad de Sistemas Electrónicos[74] de la NHTSA de EE. UU. está estudiando la necesidad de incorporar estándares gubernamentales o regulación relativa a la ciberseguridad de los vehículos, sin embargo, dicha agencia no tomara una decisión definitiva hasta al menos 2018, y no parece que por parte de la UE lo mismo vaya a suceder antes.

Por otra parte, diferentes asociaciones o grupos de fabricantes de vehículos, o de sus componentes, siguen trabajando en la línea de una estandarización de protocolos de seguridad[75] con la que se intenta hacer frente a este reto tecnológico.

[73] TESLA, 2017, Disponible en https://www.tesla.com/en_GB/findus/list/superchargers/Spain?redirect=no

[74] Creada en 2012 lo que de por sí muestra: La creciente preocupación del tema de la ciberseguridad de los vehículos inteligentes (vehículos conectados); la fiabilidad electrónica de los mismos; así como los retos que en especial presentan los vehículos autónomos, etc.

[75] Por ejemplo, AUTOSAR (*Automotive Open System Architecture*); el IEEE (Instituto de Ingeniería Eléctrica y Electrónica); etc.

Además, el hecho de que la amenaza de un ciberataque sea algo que puede y suele evolucionar constantemente plantea igualmente la cuestión de que las medidas de seguridad a considerar deban ser flexibles y adaptativas, y que inevitablemente deban pasar por un filtro de los actores gubernamentales, pero sin que ello suponga que las partes interesadas de la industria de la automoción no puedan incluir paulatinamente y de forma mucho más rápida y eficaz, las soluciones técnicas complementarias o de nueva factura que se requieran para hacer frente a dicho peligro.

[i]

*Fernando Ruiz Domínguez**
Subinspector de la Policía Nacional