Universidad Católica
"Nuestra Señora de la Asunción"

Teoría y Aplicación de la Informatica 2

Alumno:

Matías Bavera

Car Hacking

---

1. Introducción

El mundo actual es un mundo en constante evolución y desarrollo sobre todo en el ámbito de la tecnología, en especial a todo lo que se pueda referir a dispositivos móviles que se ha hecho muy de moda.

Vivimos en una época donde el avance tecnológico es inminente, en la actualidad se van agregando o sustituyendo a las actividades cotidianas del hombre, ya sea por mayor confort, mas facilidad o efectividad, como por ejemplo la automatización de algunas tareas del hogar como el control de luces, robots encerador de pisos, el amazon eco (alexa, el cual es un asistente de Amazon) y en

nuestro caso particular las computadoras integradas a los vehículos las cuales no solo sirven mejorar el confort sino la eficiencia del vehículo en sí.

Debido a que últimamente estamos rodeados de tecnología, y la misma puede ser modificada por un grupo específico de personas, ya sea de forma dañina o no, tendemos a poseer entorno vulnerable, pudiendo afectar a todo lo mencionado anteriormente y más, centrándonos en el hacking de vehículos lo cual a parte de ser una vulnerabilidad a nuestra información, también puede poner en peligro nuestra integridad física.

1.1. Definiciones, Siglas, Abreviaciones

1.1.1. Definiciones

Software: Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación. (IEEE 729).

Firewall: Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Hacking: Hacking es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.[7]

Cracking: En el caso de seguridad informática es el permanente intento de violación de seguridad de los sistemas informáticos, con fines justificados o no.[7]

Sistema Operativo: Un sistema operativo (SO o, frecuentemente, OS —del inglés Operating System—) es un programa o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes (aunque puede que parte de él se ejecute en espacio de usuario).

Uconnect: Es un sistema de comunicación inalámbrica y activada por voz que funciona con un teléfono celular con tecnología Bluetooth, disponible sólo para ciertos vehículos Chrylser, Dodge y Jeep .[6]

Arduino: es una plataforma de hardware libre, basada en una placa con un microcontrolador y un entorno de desarrollo, diseñada para facilitar el uso

de la electrónica en proyectos multidisciplinares.El hardware consiste en una placa con un microcontrolador Atmel AVR y puertos de entrada/salida.4 Los microcontroladores más usados son el Atmega168, Atmega328, Atmega1280, y Atmega8 por su sencillez y bajo coste que permiten el desarrollo de múltiples diseños.[33]

Open source: Se llama hardware libre, hardware de código abierto, electrónica libre o máquinas libres a aquellos dispositivos de hardware cuyas especificaciones y diagramas esquemáticos son de acceso público, ya sea bajo algún tipo de pago, o de forma gratuita. La filosofía del software libre es aplicable a la del hardware libre, y por eso forma parte de la cultura libre. [35]

1.1.2. Siglas

C.A.N. Bus: CAN es la abreviatura de Controller Area Network. Es un protocolo de comunicaciones desarrollado por la firma alemana Robert Bosch GmbH, basado en una topología bus para la transmisión de mensajes en entornos distribuidos, que se utiliza en la fabricación y en la industria del automóvil. Un vehículo está lleno de pequeños sistemas embebidos y unidades de control (ECU). Todos ellos se comunican utilizando el protocolo CAN.[34]

E.C.U.:(Engine Control Unit) La unidad de control del motor (ECU) es el cerebro en el vehículo. Hay muchas unidades de control en un vehículo, y agrupaciones de estas unidades se denominan módulos. Por ejemplo, la ECU con el apoyo de la Unidad de Control de Transmisión (TCU) y los dos se llama el módulo de control del tren motriz (PCM). Unidades de control relacionadas con el usuario normalmente se agrupan en el módulo de control de la carrocería (BCM).[40]

M.O.S.T. Bus: (Media Oriented Systems Transport) Transporte de Sistemas Orientados a Media, es un estándar de bus de datos que se destina a la interconexión de componentes multimedia en automóviles y otros vehículos. Fue creado en 1997, y su diferenciación principal con respecto a otros estándares de buses en automóviles es que se basa en un bus de fibra óptica. Esta característica permite al MOST una tráfico de datos superior que el del resto de buses del automóvil.[37]

L.I.N Bus: (Local Interconnect Network) es un sistema usado en las actuales redes de transmisión de datos de automoción. El bus LIN es un sistema pequeño y lento que se utiliza como una sub-red barata de un bus CAN para integrar los dispositivos o actuadores inteligentes en los coches de hoy. LIN se puede utilizar recientemente también sobre la batería del vehículo con un transmisor-receptor especial de DC-LIN.[36]

T.P.M.S.: son las siglas de Tire-Pressure Monitoring System o “sistema de

monitorización de la presión de los neumáticos". El TPMS es uno de esos elementos de seguridad activa que siendo sencillos nos ahorran problemas ya que nos recuerdan la importancia de la presión del neumático. En sí, la función del sistema es esta: avisar al conductor de una pérdida de presión de inflado en los neumáticos.

V2V:(Vehicle to Vehicle) abreviatura de un vehículo a otro, es una tecnología de automóvil diseñado para permitir a los automóviles para comunicarse entre sí. Los sistemas utilizarán una región de la banda de 5.9 GHz, la frecuencia sin licencia también utilizada por WiFi.[41]

RJ:(Registered Jack) traducido como "clavija registrada" o "enchufe registrado", son un grupo de estándares para interfaz física, tanto para la construcción de conectores como para el diseño del cableado, para la conexión de equipos de telecomunicaciones o de datos (redes de computadoras).Son usados como estándares a nivel internacional y vienen integrados predeterminadamente en las computadoras.

OEM: Se denomina fabricante de equipos originales (en inglés: Original Equipment Manufacturer, siglas: OEM, literalmente fabricante de equipamiento original) a la empresa que manufactura productos que luego son comprados por otra y vendidos al por menor bajo la marca de la empresa compradora (a veces conocida como empresa reenvasadora). Las siglas OEM comúnmente hacen referencia a la empresa fabricante del producto original.[39]

2. Sección Técnica

2.1. Herramientas, Costo Accesibilidad

La herramienta es básicamente un Arduino que ejecuta el software y hace el trabajo principal, tiene una palanca o perilla de cambios de nivel para dejar pasar 12V a 5V al Arduino, un lector de tarjetas SD, una pequeña pantalla LCD y los conectores necesarios. La herramienta se puede controlar a través de Bluetooth inalámbrico, que permite el control del mismo desde un smartphone. Esta Herramienta de ECUS se anunció en la conferencia de hackers DefCon 21.[32]

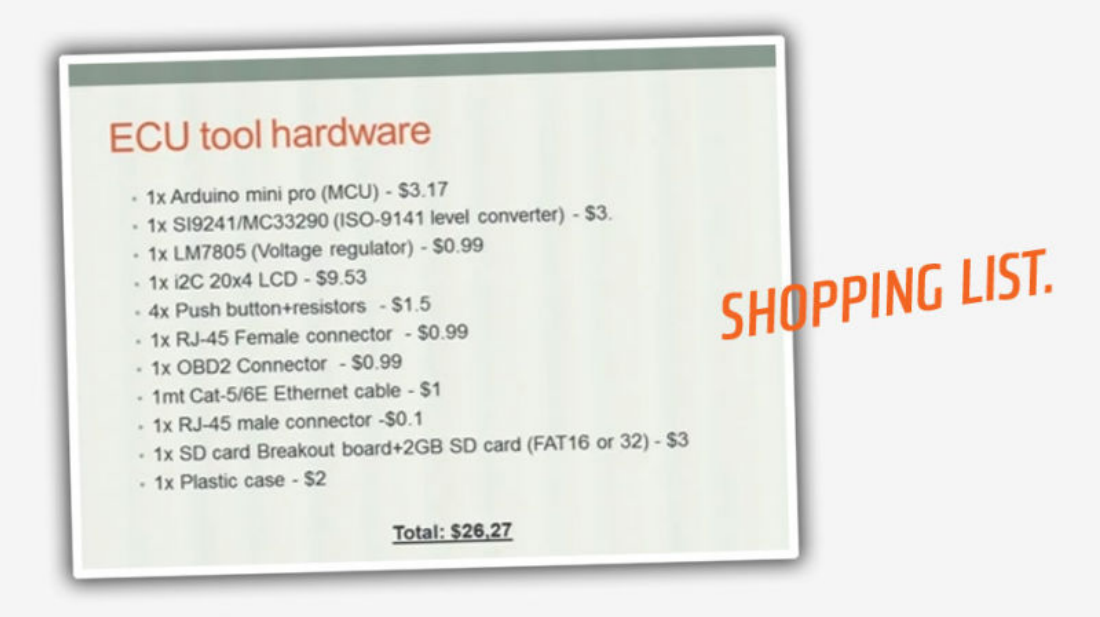

Figura 1: Materiales para elaborar la herramienta con la cual hackear el vehículo.[32]

2.2. Vías de acceso

En esta sección hablaremos de la superficie de ataque que son todas las posibles maneras de atacar un objetivo, este podría ser un componente o todo el vehículo. En esta etapa no consideramos dañar o modificar algún componente , sólo nos enfocaremos a todos los puntos de entrada a él, que podríamos tener.

Debemos encontrar las debilidades, evaluar el perímetro y documentar el entorno. Para un vehículo, debemos tener en cuenta todas las formas de datos que se pueden obtener del vehículo es decir, las maneras en que el vehículo se comunica con el mundo exterior.

2.2.1. De donde se pueden producir los ataques:

1. Desde el exterior del vehículo:

   a) ¿Qué señales se reciben? ¿Ondas de radio? Mandos? Sensores de distancia?

   b) El acceso al teclado físico?

   c) Sensores táctiles o de movimiento?

   d) Si es eléctrico, ¿cómo se carga?

2. Desde el interior del vehículo:

   a) Opciones de entrada de audio: CD? ¿USB? ¿Bluetooth?

   b) Puertos de diagnóstico? [17]

2.2.2. Receptores(Por donde atacar):

En esta sección se especificaran los recepetores finales. Cuales son, su categorización y por ende si es o no posible poder establecer una conexion con el de acuerdo a lo que podamos acceder y establecer una comunicación.

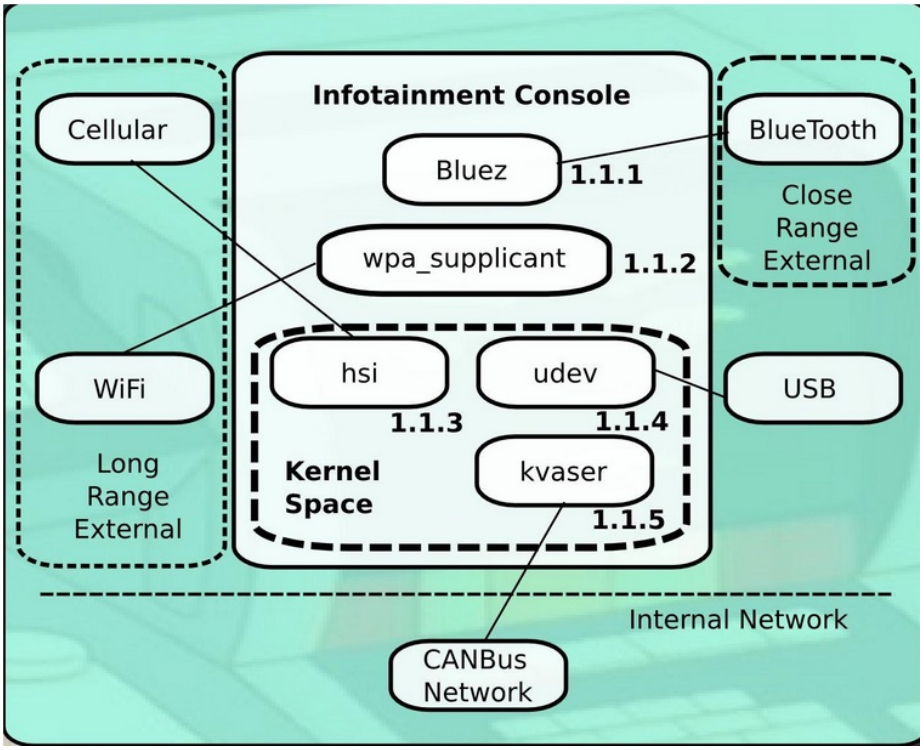

Figura 2: [17]

La parte superior del diagrama es la de menor confianza y la parte inferior es la más confiable. Mientras mas barreras de confianza de un canal de comunicación atraviesa, más arriesgado que se convierte.

Ahora estamos llegando al nivel en el que podemos ver a la comunicación que tiene lugar en el interior del vehículo. Nos estamos centrando en la información y entretenimiento, ya que es uno de los receptores más complicados y se conecta directamente a la red CANBus. Aquí agrupamos los canales de comunicación en las cuadrados con líneas de puntos para representar los límites de confianza. Hay un nuevo límite de confianza dentro de la consola de información y entretenimiento con la etiqueta "Kernel Space."

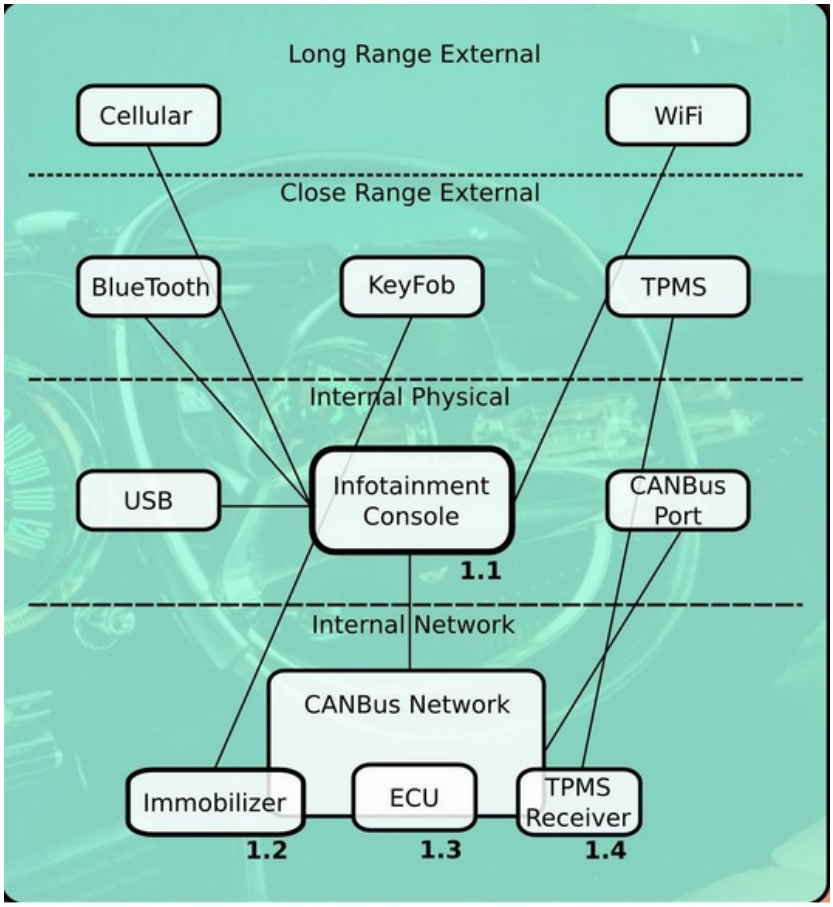

Figura 3: [17]

Estos mecanismos se comunican directamente con el kernel y suponen un riesgo más alto que los mecanismos que se comunican con las aplicaciones del sistema.

2.2.3. Información del sistema:

Sistema de información y entretenimiento es el nombre dado a menudo a esa interfaz de pantalla táctil en la consola central del vehículo. Estos a menudo poseen un sistema operativo como Windows CE o Linux. Estas unidades apoyan una variedad de características y tienen diferentes niveles de integración con el vehículo. Hay entradas normalmente físicas: auxiliar Jack CD-ROM de DVD con pantalla táctil Puerto USB, botones, etc, y las entradas inalámbricas: Conexión Móvil Bluetooth WiFi GPS XM control remoto de sus partes.

2.2.4. Determinar la arquitectura del objetivo :

El primer elemento que debemos de conocer es, ¿cuál es el sistema en funcionamiento? El método más sencillo es la búsqueda de la marca de la pantalla(o radio)[17].

2.3. Métodos de ataque

Una vez conocido el sistema operativo, la arquitectura y el método de actualización, el siguiente paso es ver si se puede utilizar esta información para modificar el sistema. Algunos cambios son "protegidos"por haber sido firmados. Estos pueden ser difíciles de actualizar. A menudo no hay protección o si la hay, es una simple comprobación hash MD5. La mejor manera de encontrar estos es modificar el software de actualización existente y desencadenar una actualización[17].

2.3.1. Aplicaciones y Plugins

Algunos sistemas permiten aplicaciones de terceros en el dispositivo. Esto a menudo se maneja a través de una tienda de aplicaciones o una interfaz de distribuidor-personalizado. Apunta a la modificación de un plugin existente o crear el tuyo propio. A menudo hay un método para que los desarrolladores puedran probar las aplicaciones carga lateral(sideload apps). Esto puede ser una gran manera de ejecutar código para desbloquear aún más el sistema.

Si usted está buscando vulnerabilidades existentes en la unidad de información y entretenimiento, a continuación, el siguiente objetivo es recojer todos los binarios fuera del sistema para que pueda analizarlos en busca de vulnerabilidades.[17]

2.3.2. Ataques Ethernet

Redes Ethernet en los vehículos, son relativamente nuevos, no están estandarizados ni es requerido. El cable de red mínimo es de cuatro cables: TX +, TX-,

RX +, RX-. Estos cables no son los que se usan para conectar su ordenador, pero se utilizan en entornos industriales. Los puertos Ethernet para vehículos a menudo tienen conectores como conector RJFRB. Es posible elaborar un conector personalizado con el conector RJ45 para su computadora para rastrear e inyectar paquetes. La buena noticia es que no se necesita ningún equipo especial de instalación; se puede utilizar un ordenador portátil y cualquier sniffer de red que usted prefiera. Las redes en vehículos tienen una puerta de enlace CAN Ethernet, a menudo encapsulado en UDP. Si se ve mucho ruido UDP, estos son los datos de la CAN más probables. Puede utilizar todos los ataques normales y métodos de inyección en estos paquetes CAN.[17]

2.3.3. Atacar Mandos e inmovilizadores

Los sistemas de entrada remota sin llave normalmente funcionan a 315 MHz para América del Norte y 433,92 MHz para Europa y Asia. Los sistemas más antiguos usaban infrarrojos. Estos por lo general tienen un código variable. Aquí está la configuración Gqrx para monitorear una pulsación de tecla de desbloqueo de un llavero de Honda:

Las teclas tienen generalmente un transpondedor en ellos. Estos transpondedores se comunican con el inmovilizador con RFID. El inmovilizador cambia el código variable al tiempo, esto permite al atacante ver la secuencia de teclas correcta. Los inmovilizadores a veces tienen la llave todavía en memoria por unos minutos después de que se ha eliminado la clave. Esto puede proporcionar una ventana de oportunidad para arrancar el coche sin la llave. Ataques de repetición. Inmovilizadores más antiguos utilizaron un código estático en lugar de un código variable. [17]

Volcado de memoria del transpondedor: A menudo es posible volcar la memoria del transpondedor y obtener la clave secreta. Se debe obtener el Mando de Identificación del UHF y tratar de reunir la cadena de claves mediante la reproducción y la grabación.

Atascar la cerradura del vehículo: Un atacante puede simular el "bloqueo"presionando el botón que impediría el coche de bloquearse y permitir así a una persona con malas intenciones robar el contenido del vehículo.

2.3.4. Entrada sin llave y Start (PKES)

Estos sistemas son muy similares a un sistema inmovilizador transpondedor tradicional, excepto la llave de control puede permanecer en el bolsillo del propietario. Esto se logra a través de múltiples antenas en el vehículo que ubican la llave de control. Estos mandos lían un chip RFID LF y una señal de UHF para desbloquear comienzo. Las señales UHF serán ignoradas si el LF RFID no está lo suficientemente cerca. La RFID recibe un desafío criptográfico

y el microcontrolador resuelve este desafío y responde sobre la señal de UHF.[17]

2.3.5. Atacando la ECU y otros Sistemas Embebidos

La unidad de control del motor (ECU) es un objetivo común de la ingeniería inversa. Probablemente el truco más popular para hackear una ECU es modificar el mapa de combustible. Esto es básicamente un gráfico que muestra la cantidad de combustible a inyectar en una RPM y posición del acelerador. Uno podría modificar este mapa para alterar el equilibrio de la eficiencia y el rendimiento de combustible.[17]

2.4. Algunas formas y aplicaciones de hack

Dependiendo del modelo del vehículo, habría que acceder al maletero, capó o en la parte inferior del mismo. Se conecta al CAN bus del automóvil y en pocos minutos se entrar en contacto con la sistema del mismo, algo que suena muy peligroso y preocupante.

2.4.1. Las llaves

Las llaves de los automóviles son uno de los objetos que, con el tiempo, han dejado de ser fragmentos de metal con incrustaciones especiales para convertirse en chips electrónicos con códigos que, en efecto, pueden ser descifrados por ingenieros o matemáticos. Existe un artículo de un profesor de la Universidad de Birmingham, Reino Unido, sobre el algoritmo que gestiona los códigos que las llaves les envían a los vehiculos de lujo. Esto debido a que, según el fabricante alemán Volkswagen, el artículo revelaba los códigos secretos que usan vehículos de esa y otras marcas –como Porsche, Audi y Lamborghini- para arrancar el motor. El procedimiento que analizaron los profesores se llama chip slicing y consiste en desmantelar dicho objeto electrónico, analizarlo con un microscopio e interferir el algoritmo que hay en sus pequeños transistores. El proceso cuesta más de 50.000 dólares. Un auto de estos(lujosos) vale unos 250.000 dólares. [20]

2.4.2. El tablero

En el tablero del vehículo se pueden modificar los índices de combustible o velocidad entre otras cosas. Un estudio de las universidades de Wisconsin y San Diego, en Estados Unidos, probó que se puede hackear un vehículo a través de la red: "Descubrimos que el ataque inalámbrico es factible a través de una amplia gama de vectores de ataque, incluyendo herramientas mecánicas, reproductores de CD, Bluetooth y señales de celular.[A]demás de esto, el estudio encontró que "los canales de comunicaciones inalámbricas permiten el control del vehículo a larga distancia, hacer un seguimiento de la ubicación y filtrar el audio en la cabina". Todo esto a través de una intervención de esas redes. Es posible intervenir la radio, tocar la bocina, activar y desactivar limpiaparabrisas,

controlar el aire acondicionado y alterar tablero de instrumentos (para falsificar el nivel de combustible y las lecturas del velocímetro). [20]

2.4.3. El motor

Uno investigadores utilizaron cables para conectar sus dispositivos a las unidades de control electrónico de los vehículos (conocidos en inglés como ECUs) a través del puerto de diagnóstico a bordo (conocidos como OBDs, también utilizados por los mecánicos para identificar fallas). Incorporado en la mayoría de los vehículos modernos, el ECU es parte de la red de ordenadores que controla la mayoría de los aspectos funcionales del auto, incluyendo aceleración, frenado, dirección y bocina. Los científicos pudieron diseñar un software que envía instrucciones a la computadora de la red del vehículo y reemplaza los comandos de los controladores reales de la unidad. [20]

3. Vehículos mas vulnerables

TABLE TITLE

CAR	ATTACK SURFACE	NETWORK ARCHITECTURE	CYBER PHYSICAL
2014 Jeep Cherokee	++	++	++
2015 Cadillac Escalade	++	+	+
2014 Ford Fusion	++	-	++
2014 Dodge Ram 3500	++	++	--
2014 BMW X3	++	--	++
2014 Chrysler 300	++	-	++
2014 Range Rover Evoque	++	-	++
2014 Toyota Prius	+	+	++
2010 Toyota Prius	+	+	++
2014 Infiniti Q50	++	+	+
2014 Audi A8	++	--	+
2010 Infiniti G37	-	++	+
2014 BMW 3 Series	++	--	+
2014 BMW i12	++	--	+
2014 Dodge Viper	++	-	--
2014 Honda Accord LX	-	+	+
2010 Range Rover Sport	-	--	-
2006 Range Rover Sport	-	--	-
2006 Toyota Prius	-	--	--
2006 Ford Fusion	--	--	--

A '+' sign means a car is 'more hackable', and a '-'sign represents a 'less hackable' vehicle.

A car's wireless **'attack surface'** includes the range of features that could be hacked, including Bluetooth, Wi-Fi, mobile network connections, key fobs, and tyre pressure monitoring systems.

The **network architecture** includes how much access these features give to the vehicle's critical systems, such as the horn, the steering and brakes.

Cyber physical relates to capabilities such as automated braking and parking sensors that could be controlled using wireless commands.

Figura 4: [25]

4. Ataques más conocidos

Estos son los ataques que causaron mas conmoción y pusieron en relieve la inseguridad de los sistemas que incorporan algunos de los vehículos más avanzados del momento.

4.1. Ownstar

Es un tipo de ataque en el cual un atacante puede abrir y arrancar coches sin problema. Eso es lo que ha conseguido el investigador Sammy Kamkar con su dispositivo OwnStar, un nombre que tiene un punto claro de burla, ya que es capaz de vulnerar la seguridad del sistema OnStar que incorpora General Motors en sus coches.

Entre las posibilidades que dicho dispositivo confiere al atacante la posibilidad de abrir el vehículo, arrancarlo y realizar un seguimiento del mismo, ya que intercepta la señal de la aplicación móvil OnStar y se aprovecha de ella[16].

4.2. Jeep Cherokee de 2014

En la conferencia Black Hat en Las Vegas, Charlie Miller y Chris Valasek mostraron un ataque en un Jeep Cherokee que permite manipular a control remoto del motor, los frenos del vehículo, y sistemas menores de millas de distancia, simplemente por saber la dirección IP pública del vehículo. Los detalles completos de hack siguen siendo privados, pero se basa en la UConnect de red celular; desde el año 2009, los vehículos de Chrysler han incluido hardware para conectarse a esta red para llegar a la Internet. Los dos investigadores han demostrado que un hacker astuto puede utilizar el sistema UConnect conseguir el acceso inalámbrico a los principales componentes de los controles de un automóvil, y potencialmente bloquearlo de forma remota. La falla ha existido en el sistema desde el 2013.

Miller dice que el hack funciona en los últimos motores Fiat Chrysler - tales como Ram, Durango, y los modelos de Jeep. La pareja reveló las fallas a los fabricantes para que un parche pudiera ser preparado y distribuido antes de su platica en Black Hat. La solución supone previene que los malhechores accedan a sistemas críticos a través de la red celular, un mecanismo de protección que habrías esperado desde el primer día [13].

4.3. Corvette

Un grupo de investigadores de la Universidad de California en San Diego descubrió un tipo de hack de forma inalámbrica a través de un dispositivo comercial pequeño: Un dispositivo de 2 pulgadas que está diseñado para ser conectado a

los tableros de vehículos y camiones utilizados por las empresas de seguros y de las flotas de transporte por carretera para supervisar vehículos, su ubicación, velocidad y eficiencia de los mismos. Mediante el envío de mensajes SMS cuidadosamente elaborados para uno de esos dispositivos baratos conectados al tablero de un Corvette, los investigadores fueron capaces de transmitir órdenes al bus CAN -red interna del vehículo que controla sus componentes físicos de conducción,- controla también la inflexión en los limpiaparabrisas y el parabrisas del Corvette incluso la activación o desactivación de sus frenos.

El dispositivo que los investigadores de UCSD utilizaron para esos ataques fue el llamado dongle OBD2 construido por una empresa de dispositivos móviles con sede en Francia[12].

5. Reacción de fabricantes ante reporte de hacks

5.1. Fiat

En un principio Chrysler se negó a aceptar que había un problema generalizado sobre el cual se les había dado aviso. Su respuesta no es citada por la BBC fue que la explotación de la falla requiere conocimiento técnico único y amplio, el acceso físico prolongado a un vehículo sujeto y largos períodos de tiempo para escribir código.Çhrysler también dijo que la manipulación de su software çonstituye una acción penal".

Luego de un tiempo Chrysler reconoció el problema ante CNNMoney. La automotriz dijo que dejó abierto un canal de comunicación no usado que, sin saberlo, permitía el acceso externo a los controles del vehículo. Y ahora ofrece una actualización de software que deben instalar los clientes. Sin embargo, Chrysler no dijo que se tratara de una llamada a revisión o recall, ni que los conductores corrieran riesgo [23].

Entonces Fiat Chrysler anunció el retiro de aproximadamente 1.4 millones de vehículos y camionetas en Estados Unidos. Esto pocos días después de que dos hackers detallaran por internet cómo pudieron tomar control de los todoterreno Jeep Cherokee. El fabricante de autos actualizará el software para proteger a los vehículos de ser controlados remotamente. Asimismo, agregó en un comunicado que los hackers cometen un crimen al manipular el vehículo sin autorización. El retiro afecta a vehículos con pantallas táctiles de 8.4 pulgadas, incluidas las pickups o cabinas Ram modelos 2013 a 2015, así como los autos deportivos Dodge Viper. También incluye los todoterreno Dodge Durango, Jeep Grand Cherokee y Cherokee modelos 2014 y 2015, los Chrysler 200 y 300 2015, y el Dodge Challenger. Fiat Chrysler también ha tomado medidas de seguridad en su propia red de vehículos para evitar a los hackers.

La situación también atrajo atención de la Administración Nacional de Segu-

ridad del Tráfico en Carreteras de Estados Unidos, que abrió una investigación para revisar la efectividad del retiro de Fiat Chrysler [14].

5.2. Bmw

Un experto informó los defectos que descubrió a los principales fabricantes de automóviles, pero BMW ya era consciente de ellos durante meses antes de que el investigador lo presente a la prensa el cual todavía no se había reparado. Según Han Sahin, cofundador firma Securiy, informó de la vulnerabilidad a la BMW el 22 de abril de 2015. El BMW CISO confirmó la recepción del informe de fallo al día siguiente, pero el ataque Ownstar todavía funciona con la aplicación Remota para iOS [30].

5.3. Tesla

Tesla Motors Inc. ha anunciado recientemente que se había distribuido una actualización de software para corregir las vulnerabilidades de seguridad en el sedán de Tesla Model S. Según la compañía, un atacante mediante la explotación de la falla podría tomar el control del vehículo Tesla. Tesla admitió la existencia de la falla e informó a la prensa que ya ha emitido un parche de software. En un comunicado oficial, Tesla aclaró que los hackers no pueden apagar sus vehículos de forma remota, pero sí desde el interior del vehículo[30].

Actualmente Tesla ofrece una interesante suma de dinero en concepto de premio a los hackers que puedan hackear su nuevos sistemas encontrando las fallas de los mismos para poder optimizar la seguridad del vehículo.

5.4. Parches

Los propietarios de automóviles pueden introducir su número de identificación del vehículo en el sitio web de UConnect para averiguar si necesitan descargar una actualización. Si necesita una actualización, los propietarios de automóviles pueden descargar la actualización a una unidad USB e instalarlo en el vehículo, "FCA(Fiat Chrysler Automobiles) se pondrá en contacto con los clientes potencialmente afectados por estos detalles (problemas de seguridad) proporcionado la actualización de software a la red de concesionarios de la FCA de Estados Unidos para la instalación inmediata por parte del cliente", dijo el comunicado.

En el caso de las otras empresas las cuales sus vehículos tienen problemas de seguridad deben ser llevados a las empresas autorizadas de cada marca para la instalación de la actualización la cual es a nivel software y sirve para "tapar el agujero" de seguridad con el cual pudieron ingresar al mecanismo vehículo. [22]

6. Sistemas de protección - Antivirus

6.1. Intel

Para ayudar a mitigar los riesgos de seguridad cibernética asociados con los automóviles conectados, fomentando al mismo tiempo la progresión y la innovación tecnológica, Intel Corporation anunció hoy la creación de la Junta de Revisión de Seguridad Automotriz (ASRB). La junta abarcará expertos en las industrias de seguridad de todo el mundo con las áreas de especialización en sistemas ciber-físicos. Los investigadores ASRB realizarán pruebas de seguridad en curso y las auditorías destinadas a codificar las mejores prácticas y recomendaciones de diseño de soluciones y productos de seguridad cibernética avanzada en beneficio de la industria del automóvil y los controladores. Intel también publicó la primera versión de su ciberseguridad automoción mejores prácticas de papel blanco, que la compañía seguirá actualizando en base a hallazgos ASRB [24] .

6.2. ARGUS

Argus es un pionero de la seguridad cibernética de la automoción, ayudando a los fabricantes de automóviles, protegen vehículos conectados y vehículos comerciales de car-hacking. Proporciona una solución a la seguridad cibernética para automóviles y plataformas de conectividad del mercado de accesorios. Argus combina métodos de seguridad innovadoras y provee know-how comprobado sobre redes de computadoras con un profundo conocimiento de las mejores prácticas de automoción.

Argus ofrece innovadores sistemas de prevención de intrusiones (IPS) para fabricantes de equipos originales y del mercado de accesorios (aftermarket) de navegación inteligente. The Argus IPS protege los componentes críticos de un vehículo de ser hackeado, y genera informes y alertas para el control remoto de la salud(cyber health) del vehículo. Argus incorpora ambos métodos de seguridad innovadoras y prácticas de redes informáticas probadas en soluciones integrales para la industria del automóvil para evitar los ataques cibernéticos. [31]

6.3. Mcafee

Mcafee la cual es una empresa muy importante en el mundo de la seguridad informática se esta preparando fuertemente para combatir las debilidades de seguridad, mediante el diseño de la seguridad en sus productos para el automóvil desde el principio. En particular, esto incluirá tres niveles de seguridad: módulos de hardware, servicios de hardware y servicios de seguridad de software. Seguridad del hardware puede proporcionar a los vehículos el rendimiento criptográfico necesario, lo que les permite hablar de forma segura entre sí sin riesgo

de que instrucciones maliciosas se inyecten en las comunicaciones. La seguridad del software también puede proporcionar la exploración activa de actividad maliciosa.

Mcafee estará trabajando muy de cerca con la ASRB y con la industria automotriz para asegurar los vehículos autónomos y nuestra futura flota de transporte[4].

6.4. Mas Protección en el futuro?

Los expertos no tienen la confianza de que podamos proteger las calles de nueva generación y vehículos de hackers.

Las calles mismas pronto podrán conectarse a Internet en las redes llamadas V2I (de vehículo a infraestructura), que conllevan importantes beneficios de transporte y seguridad, pero también ofrecen más objetivos para los hackers. ¿Pueden las redes protegerse de los ataques que podrían rastrear vehículos o robar información personal? La seguridad es el reto más importante para la tecnología V2I emergentes, de acuerdo con una Oficina de Responsabilidad Gubernamental (GAO) de la encuesta de expertos gubernamentales, académicos y especialistas de la industria. Menos de la mitad de los expertos encuestados dijo que sería posible desarrollar un sistema seguro.

En un futuro no muy lejano, el vehículo va a comunicarse con semáforos través de una conexión inalámbrica para advertir que no permita pasar luces rojas. Las carreteras les dirán cuando el tiempo ha hecho la conducción insegura, y las intersecciones le dirán la velocidad más amigable con el medio ambiente con la cual manejar(ECO-DRIVE).

El Departamento de Transporte está investigando cómo mantener estas nuevas redes seguras, y hasta ahora, no tienen la respuesta[5].

7. Riesgo

Nuestros vehículos se están transformando rápidamente en ordenadores de 2000 kilogramos con ruedas y una de las armas más peligrosas que un hacker puede atacar.

Hasta ahora, los ataques realizados a vehículos fueron con fines investigativos y de alertar sobre la fallas de seguridad que tienen los diferentes vehículos, es decir, las personas que realizaron estas demostraciones o hackeos no tenían fines perversos. Sería muy preocupante que esta información caiga en manos incorrectas debido a que como hemos visto se pueden realizar varios tipos de hack alterando el funcionamiento del vehículo(entre los mas llamativos tenemos la desactivación de los frenos lo cual en situaciones, puede atentar contra la vida de una persona).

8. Leyes

8.1. Aplicadas al tema especifico

Dos senadores estadounidenses Edward Markey de Massachusetts y Richard Blumenthal de Connecticut presentaron una ley para fijar estándares nacionales en materia de seguridad y privacidad para los automóviles, así como un sistema de calificación que te diga qué tan protegido está un auto contra los ciberataques. La llamaron Security and Privacy in Your Car Act o Ley para la seguridad y privacidad en tu automóvil.

8.2. Leyes en Paraguay

La Ley 4439 representa una modificación del Código Penal, fue sancionada en el Congreso Nacional el 8 de septiembre de 2011, promulgada por el Poder Ejecutivo el 3 de octubre de 2011 y publicada el 5 de octubre de 2011 en la Gaceta Oficial Nro. 192.

Si bien la ley solo cuenta con dos artículos, el primero de ellos modifica tres artículos del Código Penal e introduce seis nuevos artículos al mismo cuerpo legal. Todos ellos se encuentran en la Parte Especial del Código Penal.

8.2.1. Artículos y apartados

1. **Sabotaje de sistemas informáticos (art. 175 CP)**

   El art. 175 Sabotaje de computadoras pasa a denominarse Sabotaje de sistemas informáticos. También se amplía el alcance del tipo, al eliminar el requerimiento de que los datos sean de importancia vital e incluyéndose a los particulares como posible objeto del ataque.

   art. 175 (303b StGB) y carece de un fundamento político-criminal, pues desde la vigencia del Código Penal (28-nov.1998), nadie ha advertido que debido al requerimiento importancia vital alguna conducta no pueda ser castigada, al menos por otros artículos. Por ejemplo, el art. 174 Alteración de datos o algún delito común como el Daño o el Hurto. Estos últimos, siempre y cuando nos refiramos a los soportes de los datos, como podrían ser el disco duro o un DVD, pues solo ellos serían considerados cosas a los fines de nuestro Código Penal.

2. **Interceptación de datos (art. 146c CP)**

   Será castigado con pena privativa de libertad de hasta dos años o con multa, cuando el hecho no es castigado con una pena mayor por otro precepto, quien empleando medios técnicos acceda o facilite indebidamente el acceso a datos que no están destinados a él (202a), que provienen de una

transmisión no pública o de la emisión electromagnética de un sistema de procesamiento de datos.

Es decir, lo que se debe castigar es la obtención con medios técnicos de datos no autorizados, cuando estos provengan de: a) una transmisión no pública de datos, o b) de la emisión electromagnética de un sistema de procesamiento de datos.

3. **Preparación de acceso indebido e interceptación de datos. (146d CP)**

   En el caso del 146d, se trata adelantar la punición de actos preparatorios correspondientes a los dos artículos anteriores. En tal sentido, se castigará tanto la producción, la difusión o hacer accesible a terceros claves de acceso u otros códigos de seguridad, así como programas de computación destinados a la realización de las conductas señaladas en los arts. 146b y 146c.

   Merece especial atención la cuestión de los programas informáticos que sirven para eludir las medidas de seguridad. Esto debido a que en muchas empresas se suelen utilizar ese tipo de programas para probar justamente si su sistema es seguro o no.

4. **Acceso indebido a sistemas informáticos (174b)**

   Otro artículo incorporado es el art. 174b Acceso indebido a sistemas informáticos, su ubicación sistemática hechos punibles contra otros derechos patrimoniales no parece condecirse con las conductas castigadas, pues estas parecen estar protegiendo el derecho a la intimidad. Es más, lo que se pretende castigar ya está cubierto por el art. 146b Acceso indebido a datos. Asimismo, el art. 174b introduce el elemento "sistemas informáticos", lo que dentro de nuestro CN se torna confuso. Según la definición dada por ese inciso, una computadora podría considerarse un sistema informático. [2]

9. Fabricación de vehículos Y Recomendaciones a Usuarios

9.1. Fabricación de vehículos

En la actualidad se pueden identificar tres áreas para los fabricantes de automóviles para centrarse en la hora de crear características del vehículo de modo a aumentar la seguridad de los mismos y disminuir riesgos de ataque.

1. **Diseño Vehículos Seguros:** Seguridad comienza con el coche. El proceso de diseño debe centrarse en la seguridad, lo que significa delineando

y comprobación de los riesgos y amenazas para cada componente, subsistema, y la red la cual el vehículo estará expuesto una vez que sale de la línea de producción de la marca de vehículos.

2. **Crear redes seguras:** Comunicaciones debe ser encriptado; esto significa que todas las organizaciones que proporcionan servicios que conectan las carreteras, los coches, y los dispositivos necesitan para proteger sus redes y monitorear las transacciones para detectar actividades sospechosas.

3. **Fortalecer el vehículo:** Estos coches conectados deben tener la seguridad fortalecida en todos los niveles:

   - El cifrado de datos en reposo y datos en movimiento.
   - La implementación de controles de seguridad en la nube adecuadas.
   - Mecanismos de control de acceso
   - Fijación del sistema operativo.
   - Las pruebas de penetración de las aplicaciones.

   Los investigadores deben animar a la industria del automóvil a considerar seriamente la seguridad como un requisito obligatorio para la seguridad de los propietarios de automóviles; más importante es que los propietarios de automóviles en el futuro próximo deben elegir los mismos en basea las características de seguridad implementadas por los fabricantes. [30]

9.2. Recomendaciones a Usuarios

Entonces, digamos que usted tiene un vehículo inteligente con conexión a Internet, de asistencia al conductor y más. ¿Qué se puede hacer para asegurarse de que su vehículo es seguro? Bueno, hay un par de cosas a tener en cuenta:

Mantenga su software actualizado. Lo mejor que puede hacer por cualquier dispositivo es el propietario - ya sea un coche inteligente o un teléfono inteligente - es mantener su software actualizado. Las actualizaciones de software pueden venir en una variedad de formas. Algunos vendrán forma inalámbrica, mientras que otros pueden requerir que usted inserte un pen USB en un puerto especial. Revise su controlador de manual o pregunte a su distribuidor para más detalles. Este al tanto de las noticias. En este momento, los ataques cibernéticos en los vehículos son poco comunes, y los investigadores de ciberseguridad están buscando activamente, y ayudando a mediar, potenciales amenazas. Si usted oye hablar de una vulnerabilidad en las noticias, consulte al fabricante del vehículo para una actualización, y reparar su vehículo. [4]

10. Vehículos open source

Al enfocarnos en el car hacking, no podemos dejar de lado una rama tan importante como los vehículos open-source. La idea se central al igual como en la informática, el código abierto hace más libre al consumidor, no solo se puede tener en cuenta la construcción de vehículos nuevo sino que las posibilidades de personalización son tan amplias como lo sea nuestra imaginación. Algunos fabricantes, compañías del sector de la automoción y makers tienen a nuestra disposición una plataforma que cualquiera de nosotros puede modificar o mejorar y así construir el vehículo que mejor satisfaga nuestras necesidades.

Entre ellos tenemos varios proyectos importantes que han sido desarrollados a lo largo de los años.

10.1. Ford - OpenXC

La experiencia de Ford con el diseño de código abierto viene de un punto de partida diferente de un experimento académico (StreetScooter) o un inicio disruptivo (Local Motors). Es uno de los más grandes y sin duda uno de los más antiguos OEM, pero ha estado mirando para usar el poder de la nube por un buen tiempo. Venkatesh Prasad es el centro en este esfuerzo. Prasad que tiene una formación ecléctrica para la industria automotriz, (llegando a Ford de CalTech y el Laboratorio de Propulsión a Chorro de la NASA a través de Silicon Valley) dijo que la iniciativa surge de un deseo de colaboración.Ëstábamos buscando que grado de dificultad tendría conseguir datos de los coches que la gente creativa en el exterior [de Ford] querían ; dijo. C̈omenzamos a sacar a luz la información que en algún momento saldría a luz de todos modos (es decir, la velocidad o dirección del vehículo, ángulo de la rueda) en una base de sólo lectura .

El resultado es una plataforma de software y hardware llamado OpenXC. El hardware es un dongle OBD2 que conecta con el coche con una plataforma de software que facilita a los usuarios trabajar con los datos procedentes de la CAN. N̈uestro principio rector es el hardware y el software de código abierto, de sólo lectura para que las cosas que están reguladas, (seguridad, emisiones) no sean alteradas; dijo. [28]

10.2. OSVehicle - TABBY

Un proyecto muy renombrado de fuentes abiertas (Open Source), denominado OSVehicle (OSV), que desarrolla este concepto para que sea accesible a todos nosotros y que incluso pueda ser industrializado. OSV (Open Source Vehicle) es una plataforma para construir nuestro propio coche eléctrico o híbrido y no solo podemos construir coche nuevo sino que las posibilidades de personalización son bastante amplias.

TABBY es un framework Open Source para Vehículos, es un proyecto para armar un vehículo usando solamente elementos de software/hardware open

source, es decir, puedes descargar los planos e instrucciones y modificarlos y todo lo que ya conocemos en el mundo GNU/Linux. Por el momento solo cuenta con los elementos necesarios para poder andar legalmente en Europa pero se espera poder lograr cubrir más terreno en el futuro[19].

El primer chasis universal se ha llamado Tabby y es el núcleo central del proyecto OSV. Ideado para ser totalmente versátil y flexible, puede ser ensamblado de muchas formas posibles, dando lugar a vehículos de 4, 3, 2 ruedas, coches urbanos, carritos de golf, vehículos de reparto, todoterrenos, y lo que podamos necesitar. Nuestro vehículo puede ser más largo o más corto, tener 2 o 4 asientos, o podemos dotarlo de más capacidad de carga[8].

10.3. Otros proyectos conocidos

- OScar.
- EDAG LCOS.
- Riversimple Urban Car.
- c,mm,n.
- OSCav.
- Open Source Velomobile Development Project.
- Open Source Green Vehicle (OSGV).
- Freedom EV de EVProduction Club.
- Trev (Two-seater Renewable Energy Vehicle).

[9]

11. Conclusión

A medida que la tecnología avanza, se van computarizando y automatizando más los procesos, ya sea por confort o facilidades brindadas, en nuestro caso de los automóviles, estamos abriendo una brecha grande de posibilidades, refiriéndonos a las vías de acceso a la información de sistema de automovil.

Los vehículos modernos cada vez son más computadora-dependendientes, la computadoras a bordo van regulando las funcionalidades de los mismos para un comportamiento en teoría óptimo, lo cual es muy bueno para la optimización de los recursos pero más peligroso a la hora de un ataque debido a que se puede deshabilitar esa acción, como ejemplo tenemos el bastante conocido caso del jeep cherokee 2014, el cual unos hackers para demostración de vulnerabilidad del mismo desactivaron los frenos de manera remota.

El hacking de vehículos no solo se refiere a dañar un sistema, sino que también a la personalización de un sistema de acuerdo a lo posible, como la modificación de la interfaz de las pantallas touchscreen o alguna otra actividad que se pueda realizar con la misma(en los vehículos no open-source).En los proyectos de vehículos open-source también se pueden realizar modificaciones o personalizaciones de acuerdo a gusto pero teniendo una gama más grande de facilidades, bases e información que proveen los opensoruce . El hackeo de los autos no es un tema que haya sido globalmente discutido, eso es porque no ha habido ningún incidente criminal al respecto, pero poco a poco va a ir creciendo el interés tanto de las personas afectadas como las empresas que puedan tener relaciones con el tema.

Referencias

[1] Santi Araujo. Hackear un coche via bluetooth: dispositivo desarrollado por espanoles, 2014.

[2] ABC Color. Ley contra los delitos informaticos. breve resena - articulos - abc color, 2015.

[3] creoentuproyecto. El fabricante de coches open source, 2014.

[4] Gary Davis. How the cars of the future will be secured, 2015.

[5] The Daily Dot. Experts have no confidence that we can protect next-gen streets and cars from hackers, 2015.

[6] Driveuconnect. Uconnect access for chrysler, dodge, fiat , jeep and ram, 2015.

[7] Duiops. Hacking cracking y otras definiciones, 2015.

[8] ecointeligencia ponte al día en diseño sostenible. Construye tu propio coche eléctrico en menos de una hora, 2014.

[9] Faircompanies. Coches open source 10 coches libres de código abierto, 2015.

[10] Sean Gallagher. Highway to hack why we're just at the beginning of the auto-hacking era, 2015.

[11] Jonathan Gitlin. Welcome to the era of open source cars, 2015.

[12] Andy Greenberg. Hackers cut a corvette's brakes via a common car gadget, 2015.

[13] Andy Greenberg. Hackers remotely kill a jeep on the highway with me in it, 2015.

[14] Fiat hackers. Fiat chrysler retira 1.4 millones de vehiculos tras reporte de hackers, 2015.

[15] Intel. Intel's automotive security review board (asrb) benefits industry, 2015.

[16] Contacto Interactivo. Los autos de gm tambien se pueden hackear, 2015.

[17] Car Hacker's manual. *Craig Smith*. Theia Labs, 2014.

[18] Microsiervos. Por qué el software de los coches debería ser código abierto microsiervos, 2015.

[19] Nacho Morato and rarr. Tabby construye tu coche diy open source - ikkaro, 2014.

[20] BBC Mundo. Todo lo que se puede hackear en un auto - bbc mundo, 2015.

[21] Ian Murphy. Are car manufacturers being disingenuous - enterprise times, 2015.

[22] Alyssa Newcomb. Car hacking what every driver needs to know, 2015.

[23] Finanzas Newsletter and Life Style. Estos autos pueden ser hackeados de manera remota, 2015.

[24] Intel Newsroom. Intel commits to mitigating automotive cybersecurity risks, 2015.

[25] Mail Online. The 20 most hackable cars revealed: Report lists vehicles most at risk, 2014.

[26] Opengarages. Opengarages, 2015.

[27] OSVehicle openSource Vehicle. Osvehicle - open source vehicle, 2015.

[28] Openxcplatform. Overview - openxc, 2015.

[29] Charlie Osborne. Intel launches automotive security board to tackle connected car security risks, zdnet, 2015.

[30] InfoSec Resources. The nightmare of car hacking - infosec resources, 2015.

[31] Argus Cyber Security. Argus solutions, argus cyber security, 2015.

[32] Jason Torchinsky. Hackers can take over your car with this simple $26 device, 2015.

[33] wikipedia. Arduino, 2015.

[34] wikipedia. Bus can, 2015.

[35] wikipedia. Hardware libre, 2015.

[36] wikipedia. Local interconnect network, 2015.

[37] wikipedia. Media oriented systems transport, 2015.

[38] wikipedia. Media oriented systems transport, 2015.

[39] wikipedia. Original equipment manufacturer, 2015.

[40] wikipedia. Unidad de control de motor, 2015.

[41] Wikipedia. Vehicular communication systems, 2015.