UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Plan de Investigación de fin de carrera titulado:

ANÁLISIS DE VULNERABILIDADES A LA RED VEHICULAR GMLAN CAN BUS A TRAVÉS DE SU INTERFAZ DE COMUNICACIÓN OBD-II Y SU DISPOSITIVO TELEMÁTICO, CASO DE ESTUDIO GM MODELO TRACKER 2017.

Realizado por:

FRANCISCO XAVIER ESPINEL SIGCHA

Director del proyecto:

JOSÉ LUIS MEDINA

Como requisito para la obtención del título de:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN

DECLARACION JURAMENTADA

Yo, FRANCISCO XAVIER ESPINEL SIGCHA, con cédula de identidad #171398104-9, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional y que se ha elaborado consultando las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

FRANCISCO ESPINEL

C.C.: 171398104-9

DECLARATORIA

El presente trabajo de investigación titulado:

“ANÁLISIS DE VULNERABILIDADES A LA RED VEHICULAR GMLAN CAN BUS A TRAVÉS DE SU INTERFAZ DE COMUNICACIÓN OBD-II Y SU DISPOSITIVO TELEMÁTICO, CASO DE ESTUDIO GMC.”

Realizado por:

FRANCISCO XAVIER ESPINEL SIGCHA

como Requisito para la Obtención del Título de:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN

ha sido dirigido por el profesor

JOSE LUIS MEDINA

quien considera que constituye un trabajo original de su autor

DEDICATORIA

Durante mucho tiempo me pregunté, por qué mi padre no estaba en los momentos más felices o difíciles de mi vida, o simplemente donde se encontraba, quería sentir su compañía o su ayuda. Me doy cuenta que siempre estuviste presente, fuiste tú, abuelo.

Gracias por tus enseñanzas, por los mensajes de aliento, tus consejos, tu experiencia en la vida y tu excelente manera de instruirme para afrontar las verdades de esta vida.

En este reto universitario fuiste igualmente concluyente, no lo hubiera podido haber hecho sin tu ayuda.

Te doy mis más sinceras gracias, abuelo donde quiera que te encuentres.

AGRADECIMIENTO

Agradezco mucho la ayuda de mis maestros, mi tutor y a la universidad por los conocimientos instruidos hacia mi persona.

Mi madre y sin ser un hijo de sangre a mi padre, los cuales lucharon para el desarrollo y cada día me enseña algo nuevo, Gracias Padres.

Hay personas que aparecen en la vida para mejorar los días y crecer intelectual y sentimentalmente, gracias a mi novia por impulsarme a mejorar día a día.

Tabla de contenido

Organizations and people use different types of transport which have evolved to, have access to mobile networks, have an internal vehicular network such as GMLAN, which performs self-diagnoses to know the internal state of the vehicle. In those networks are latent threats, which user could be exposed. The following investigation starts in an exploration process that gives five vulnerabilities in a GM Tracker model 2017 vehicle. Four of these vulnerabilities are given through its OBD-II port, it can do to "frame sniffing" and "frame falsifying", so it could be possible to capture frames that send different devices connected to the vehicle, copy and send frames to " impersonate the identity "of ECUs or send erroneous frames in order to alter the operation of the vehicle. For the last vulnerability, the telematics device was used with its Bluetooth communication interface and did a "fuzz testing" and found a problem that the car started an immobilization and stop working. At the

Lista de Figuras

Lista de Tablas

Resumen

Hoy en día todas las organizaciones y personas utilizan medios de transporte vehiculares los cuales han evolucionado para tener acceso a, redes móviles, una red interna vehicular como es GMLAN, la cual realiza autodiagnósticos para conocer el estado interno del vehículo. Dentro de la red vehicular existen amenazas latentes, las cuales los usuarios se encuentran expuestos. En la siguiente investigación se da un proceso de exploración, mediante el uso de herramientas de diagnóstico vehicular para dar a conocer 5 vulnerabilidades en un vehículo GM Tracker modelo 2017. Cuatro de esta vulnerabilidades se dan a través de su puerto OBD-II, en la cuales se pueden constar un “frame sniffing” y “frame falsifying”, se logra capturar tramas que envían los distintos dispositivos conectados en vehículo, copiar y enviar tramas para suplantar ECUs o enviar tramas erróneas con el objetivo de alterar el funcionamiento del vehículo. Para la quinta vulnerabilidad se usa su dispositivo telemático con su interfaz de comunicación Bluetooth y mediante un “fuzz tester” se encuentra un problema de inmovilización vehicular. Se utilizan estas vulnerabilidades para indicar los riesgos que presentan en la red vehicular y se realiza recomendaciones para poder mitigar los riesgos mediante el uso de ISO 26612 e ISO 27002.

Abstract

Organizations and people use different types of transport which have evolved to, have access to mobile networks, have an internal vehicular network such as GMLAN, which performs self-diagnoses to know the internal state of the vehicle. In those networks are latent threats, which user could be exposed. The following investigation starts in an exploration process that gives five vulnerabilities in a GM Tracker model 2017 vehicle. Four of these vulnerabilities are given through its OBD-II port, it can do to "frame sniffing" and "frame falsifying", so it could be possible to capture frames that send different devices connected to the vehicle, copy and send frames to " impersonate the identity "of ECUs or send erroneous frames in order to alter the operation of the vehicle. For the last vulnerability, the telematics device was used with its Bluetooth communication interface and did a "fuzz testing" and found a problem that the car started an immobilization and stop working. At the end of the investigation it will use the 5 vulnerabilities to indicate the risks they presented in the vehicular network and did recommendations using ISO 26612 and ISO 27002.

Palabras Claves

GMLAN, CAN, Bluetooth, ECU telemático

CAPÍTULO I

INTRODUCCIÓN

La convergencia entre Tecnologías de la Información y Comunicación (TIC) y la industria automotriz se ha venido produciendo en la última década de forma progresiva. Lo que hasta hace poco eran dos mundos y dos industrias totalmente separadas empiezan a ir cada vez más de la mano. La mayor parte de la funcionalidad en un automóvil está controlada por la electrónica y el software y el automóvil se transformó desde un simple medio de transporte a un centro de información y entretenimiento móvil.

Es aquí donde nace el concepto de automóvil conectado, que hace referencia fundamentalmente al vehículo como un dispositivo más que se integra en las redes de comunicación, pero el concepto se extiende también al uso de las TIC dentro del vehículo y en el futuro lo hará a los vehículos de conducción autónoma. (Strandberg, Olovsson, & Jonsson, 2018)

Partiendo de un coche sin ningún tipo de comunicación hasta hace relativamente poco (última década), y que era uno de los pocos entornos que no estaban conectados a Internet en la vida diaria; las plataformas de conexión y la conectividad empiezan a verse con mayor frecuencia en más marcas y modelos, tendencia que se acelerará en los próximos años para acercarse a la casi totalidad de los vehículos, lo que hará crecer de forma exponencial las comunicaciones y el tráfico de datos que entra o sale de ellos.

La etapa actual del coche conectado trata de integrar los dispositivos móviles (teléfonos inteligentes o tabletas) y las aplicaciones existentes con la conectividad del vehículo. Los fabricantes de vehículos han adoptado este concepto para mejorar sus productos y brindar servicios con un valor agregado, ejemplos de esto es:

- Tráfico vehicular o geo-localización
- Gestión de mandos por voz
- Autodiagnóstico vehicular, conocer el estado del vehículo a tiempo real.
- Actualizaciones de noticias a través de un canal de comunicación inalámbrico.
- Interacción de dispositivos portátiles como teléfonos celulares, computadoras, tabletas, con el vehículo.
- Brindar conectividad inalámbrica dentro del vehículo usando redes móviles.

Conectividad, entretenimiento, navegación y autodiagnóstico son las bases de esta etapa, que el usuario valora cada vez más y que se han convertido en elementos fundamentales a la hora de elegir un coche.

El vehículo para realizar un autodiagnóstico vehicular, el cual detecta fallas y analiza el estado del mismo, debe tener una red interna vehicular como GMLAN, J1939, CAN y acceso a una red móvil la cual puede ser GSM, UMTS, LTE, Bluetooth mediante un dispositivo telemático. Es aquí donde se introduce una serie de riesgos propios de las redes o de los protocolos de comunicación lo cual se convierte en una problemática que merece ser abordada, estos riesgos de seguridad ya fueron explotados en países como Estados Unidos, Alemania, China. Para lograr un nivel adecuado de seguridad en el automóvil es un desafío, dado el entorno, los escenarios de uso y otros factores que puedan presentarse, las soluciones de seguridad deben adaptarse para admitir las características específicas del automóvil

conectado, la aplicación de una sola solución de seguridad para el sistema vehicular puede no ser suficiente. Se deben incorporar varios mecanismos de protección basados en diferentes enfoques para asegurar al vehículo y garantizar la seguridad de su conductor y pasajeros.

La presente investigación aborda la problemática mencionada, se sustenta en el capítulo uno mediante el planteamiento del problema, los síntomas, el pronóstico, los cuales son sustentado de forma teórica y científica de varias investigaciones que indican las problemáticas en CAN. Se marca una hipótesis para finalizar con los objetivos que se realizará en la presente investigación.

El capítulo dos aborda el método que varios autores utilizan para realizar un análisis a la red CAN y/o los dispositivos conectados, finalizando con una adopción de un método para realizar la investigación.

En el capítulo tres se realiza los ataques a la red GMLAN dando como resultados la alteración en el funcionamiento normal del vehículo GM modelo Tracker 2017, concluyendo que la GMLAN tiene vulnerabilidades.

Por último el capítulo cuatro se realiza un análisis de datos para obtener los riesgos asociados a estas estas vulnerabilidades y se concluye con recomendaciones de acuerdo a las normativas ISO 26262 y 27002

1.1. El problema de investigación

1.1.1. Planteamiento del Problema

Los automóviles conectados ya no son simples dispositivos mecánicos que se usan para transporte; ahora son supervisados y controlados de manera permanente por varias computadoras digitales coordinadas a través de redes vehiculares internas. Los consumidores demandan cada vez más una experiencia de una conexión continua y si bien esta transformación ha impulsado importantes avances en eficiencia y seguridad, también ha introducido una nueva gama de riesgos potenciales, acceso no autorizados al vehículo, alteraciones en el funcionamiento normal del vehículo, captura de credenciales en llaves de radio frecuencia, actualizaciones maliciosa. (Hashem Eiza & Ni, 2017).

La industria del automóvil siempre ha considerado la seguridad física como un problema crítico de ingeniería, de hecho, gran parte de estos nuevos software han introducido seguridades físicas, ejemplos de esto son los sistemas de frenos antibloqueo, airbags, etc. Pero el desarrollo de los protocolos de comunicación vehicular actuales no han anticipado en sus diseños la posibilidad de acceso a un intruso malicioso o evitar la manipulación de la información que viaja dentro de la red vehicular (Shay & Abbott-McCune, 2017).

El protocolo de comunicación más usado en la red vehicular es conocida como CAN (Control Access Network), el cual transmite diferentes mensajes relacionados al vehículo, estos mensajes son generados por las diferentes unidades de control vehicular conocidas como ECU (Electronic Control Unit), las cuales controlan o desempeñan diferentes funciones dentro de la red, aceleración del vehículo, frenado, posicionamiento vehicular, confort, aire acondicionado, entretenimiento y/o música, entre otras funcionalidades. Es aquí donde

empieza las primeras inquietudes, ¿La comunicación entre los ECUs son seguras?, ¿existe algún medio de autentificación entre los ECUs?, ¿existe algún método de cifrado para los mensajes de comunicación entre ECUs? Preguntas que necesitan ser respondidas con el fin de aportar un conocimiento sobre las amenazas, las falencias o la seguridad con la que cuenta el protocolo CAN.

De acuerdo al diseño de la red vehicular CAN, existe un puerto de acceso físico llamado diagnóstico a bordo o en inglés On Board Diagnostic (OBD). En diferentes países del mundo, en donde se ensamblan vehículos: Estados Unidos, Brasil, Argentina, México, es mandatorio contar con este puerto de diagnóstico, ya que las leyes en esos países lo exigen (Kulkarni, Rajani, & Varma, 2016). Este puerto se encuentra usualmente por debajo del tablero en todos los vehículos modernos, proporciona acceso directo a la red automotriz interna y por consiguiente el acceso a las diferentes unidades de control electrónico (ECUs). Este medio de acceso es un punto crítico en la red vehicular, al tener acceso a los diferentes ECUs puede realizar diferente tipos de daño en la red vehicular como, duplicar los mensajes de control de acceso vehicular, reescribir mensajes para controlar el encendido del vehículo entre otros (Zhang, Ge, & Li, 2016).

La red CAN, al poseer un acceso físico sin ningún control de seguridad, implica amenazas al vehículo y a la mensajería de la red, así como los ECUs estarían expuestos a alteraciones, manipulaciones o al conocimiento de su comportamiento para un ataque específico a la red.

Los ECUs al contener varios subsistemas, poseen interfaces de comunicaciones inalámbricas (Bluetooth, sensores de presión de neumáticos inalámbricos, Wi-Fi, modem de comunicación celular etc.), ejemplificados por ONSTAR de General Motors, que es un

dispositivo telemático, el cual proporciona diferentes datos del vehículo al usuario para obtener el posicionamiento, daños generales del carro, consulta de diagnóstico vehicular mediante una aplicación en su teléfono móvil; resultando otra amenaza a la seguridad vehicular. Si ONSTAR puede conectarse a redes externas como Wi-Fi, LTE, UMTS o Bluetooth, y estas redes heredan problemas conocidos, ¿Cuál sería el impacto en la red vehicular?, ¿se puede acceder a la red CAN, mediante la redes externas (Bluetooth, UMTS, LTE, etc.) utilizando a ONSTAR como medio para manipular los mensajes entre ECUs?

Las falencias de los ECUs telemáticos también se evidencias dentro de la compañía que los desarrolla, aunque no existan documentos públicos de los problemas, la empresa trata de minimizarlos, los trata como daños de bajo riesgo o no hace una investigación para conocer las falencias de seguridad de su sistema. En la documentación anexada se puede concluir, que el ECU telemático posee problemas de seguridad en los protocolos CAN, BLUETOOTH, dando como resultado inmovilizaciones vehiculares, filtración de posicionamiento vehicular, acceso no autorizado.

Por otro lado, los ataques para automóviles modernos están creciendo rápidamente a medida que las funciones de servicios y comunicaciones más sofisticadas se incorporan a los vehículos. En los últimos 3 años se suscitaron importantes ataques a diferentes marcas comerciales de vehículos los cuales se hicieron públicos en diferentes medios de comunicación, el más grave fue el control de un Jeep de forma remota en el cual se evidencia que es posible obtener el control total del vehículo sin que el conductor pueda neutralizar el ataque (Greenberg, WIRED, 2015).

Lo expuesto anteriormente indica que la red CAN pese a ser un protocolo de comunicación vehicular, no cuenta con las seguridades adecuadas para los usuarios y aún

sigue siendo vulnerable a diferentes tipos de ataques y el **desconocimiento** de estas brechas físicas y lógicas del protocolo, **propone** un problema que es pertinente de ser estudiado y resuelto. La propuesta de cambio que se plantea en el siguiente estudio dará a conocer las vulnerabilidades de GMLAN la cual está basada en CAN, mitigando los riegos y permitiendo reducir las brechas de desconocimiento.

1.1.1.1. Diagnóstico del Problema. Síntomas y Causas (Causa –efecto).

Existen varias dificultades que una red vehicular debe enfrentarse, a continuación se detallan una serie de eventos que se caracterizan como síntomas detectados en un mal funcionamiento.

- Acceso no autorizado al vehículo a través de la App en IOS de ONSTAR. Un analista de software logró capturar las tramas que utiliza la APP para realizar diferentes acciones como son, apertura de puertas, localización vehicular. Duplicó los mensajes de diagnóstico para poder enviar mensajes de apertura remota de los seguros, logrando tener acceso al vehículo. (Gallagher, 2015).
- Propietarios vehiculares con sistemas de llaves remotas, informaron que ladrones lograron robarse sus vehículos sin esfuerzo. Los ladrones capturaron la trama de radio frecuencia emitida por las llaves y suplantaron la identidad de sus llaves remotas (Greenberg, WIRED, 2016).

A más de los eventos descritos por los usuarios existe documentación de la empresa que desarrolla dispositivos telemáticos para GMLAN en la cual se detectan una serie de síntomas como se detalla a continuación

- Inmovilización vehicular por problemas en Bluetooth del equipo telemático. El dispositivo se encontraba en normal funcionamiento cuando se intentó emparejar un celular y se realizó un apagado del vehículo. Esta acción deja inmovilizado el coche y un con un daño al equipo telemático. (Anexo A).
- Mediante captura de tramas de Bluetooth, se constata que el dispositivo telemático envía errores en la capa L2CAP de Bluetooth. (Anexo B)
- Inmovilización vehicular por daños en diferentes modos de energía del sistema telemático. (Anexo C)
- Daños en el dispositivo telemáticos por pruebas de stress en campo. (Anexo D)
- Lectura de credenciales y datos en la red GMLAN CAN BUS. (Anexo E)

Por último existen estudios científicos publicados sobre problemas de seguridad y falencia de las redes vehiculares en especial el protocolo CAN, ya que es la base para todas las redes vehiculares,

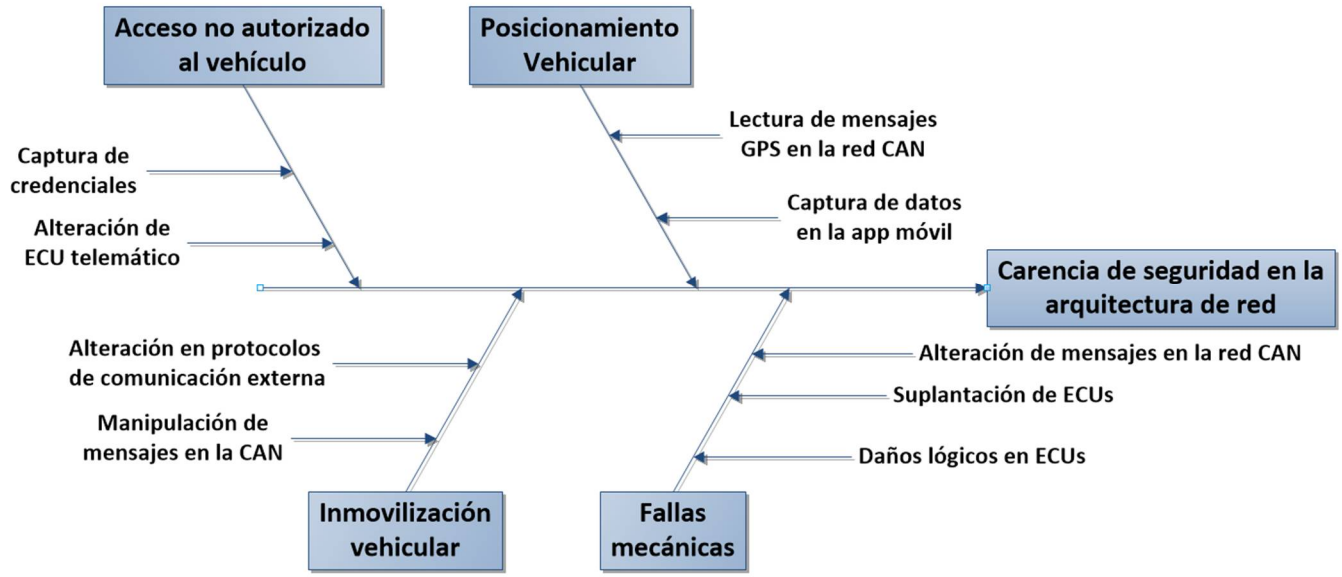
- Alteración de mensajes en la red CAN, debido a la introducción de errores en la trama de mensajería del BUS (Abbott-McCune & Shay, 2016).
- Suplantación de mensajes de diferentes ECUs en la red CAN, dando como resultado la alteración en funcionamiento de los vidrios eléctricos, calefacción y plumas (Koscher, Czeskis, Roesner, & Kohno, 2010)
- Personas no autorizadas obtuvieron datos del bus CAN como es el posicionamiento vehicular, aceleración, velocidad mediante un malware instalado (Woo, Jo, & Hoon, 2015).
- En la revista de “Driving with sharks”, se indica que OBD y los dispositivos telemáticos son puntos críticos en la seguridad vehicular, puesto que OBD es un

puerto físico de acceso libre y el dispositivo telemático cuenta con acceso a redes externas como redes móviles haciendo susceptible a vulnerabilidades que heredaría de la redes móviles (Hashem Eiza & Ni, 2017)

Para organizar, representar y ordenar los diferentes síntomas e inconvenientes que surgieron en el diagnóstico del problema, se debe tener en cuenta las causas y los efectos que generan y así lograr un conocimiento común de este problema complejo. Un diagrama causa-efecto es la forma de organizar las ideas y la documentación, en la figura 1 se puede visualizar el mapa de causa efecto en donde los síntomas obtenidos en la documentación nos indican:

- Inmovilización vehicular, causada por manipulación de mensajes CAN.
- Acceso no autorizado al vehículo, puerto de acceso OBD inseguro, captura de credenciales.
- Captura de posicionamiento vehicular
- Fallas mecánicas debido a las alteraciones de los ECUs en red vehicular

Figura 1. Mapa causa efecto de la red CAN, Fuente propia



Se establece que la red vehicular posee brechas que hace susceptible a daños lógicos, concluyendo que la causa del problema es la carencia de seguridad en la arquitectura, donde existe la posibilidad que un intruso tenga acceso físico o remoto y alterare su funcionamiento; en donde el dispositivo telemático es un punto crítico a ser analizado.

1.1.1.2. Pronóstico

El constante crecimiento tecnológico en el parque automotriz, producto de la adopción de nuevas tecnologías ofrece una mayor gama de acceso y beneficios a los usuarios finales, sin embargo el no tener un control de seguridad tecnológica adecuado se enfrentaría a graves problemas como daños físicos, robos de credenciales, conocimiento de posicionamiento vehicular a personas no autorizadas, daños lógicos en la red vehicular, lo que conllevaría a incrementar los delitos. Los usuarios tendrán más inseguridad en adquirir un vehículo de General Motors o un sistema telemático, porque estos sistemas estarían expuestos a alteraciones de su funcionamiento.

Si la empresa que desarrolla los dispositivos telemáticos no realiza estudios acerca de los problemas que poseen sus productos, quedaría en duda la continuidad del negocio, ya que una empresa que no conoce sus vulnerabilidades no puede brindar una seguridad adecuada a los futuros propietarios de un vehículo y continuarían con un desarrollo deficiente de los dispositivos para la red vehicular. Aún más, la confidencialidad de la información quedaría expuesta y esto conllevaría a problemas legales para la empresa.

1.1.1.3. Control del Pronóstico

La situación detallada, hace necesario un tratamiento urgente de la información y un estudio eficiente en la red vehicular GMLAN CAN BUS, del ECU telemático ONSTAR, el cual puede interactuar con redes externas (UMTS, Bluetooth, etc.) para establecer un sistema de comunicación efectiva.

Si se logra conocer los riesgos que posee GMLAN CAN BUS producto de un análisis de vulnerabilidades que se propone en la siguiente investigación, se los puede gestionar de manera ordenada, entregando el vehículo, el dispositivo telemático de una manera confiable para el usuario y las ventas de los mismos se incrementarán y por ende la imagen de la empresa mejorará. Reducción del impacto del daño, sin necesidad de realizar elevadas inversiones, ni contar con una gran estructura de personal.

1.1.2. Formulación del Problema.

La falta de conocimiento en la aplicación de pruebas de campo que permitan validar las vulnerabilidades en la red vehicular GMLAN CAN BUS y el dispositivo telemático, hacen

un producto totalmente susceptible a alteraciones en el funcionamiento, produciendo problemas para la compañía e inseguridad de información para el usuario final.

1.1.3. Sistematización del Problema.

- ¿Qué método se puede aplicar para conocer el estado de la red GMLAN CAN BUS?
- ¿Qué tipos de equipos se utilizarán para analizar la red GMLA CAN BUS?
- ¿Qué modelo de vehículo se utilizará para realizar el análisis?
- ¿Qué dispositivo telemático y cuál interfaz de comunicación se analizará para encontrar vulnerabilidades?
- ¿Qué tipos de ataques a la red externa se quiere mitigar?
- ¿Qué tipos de herramientas se debe usar para realizar ataques a la red vehicular?
- ¿Sería beneficiosa la implementación del modelo de seguridad a proponer para todos los ECUs en la red vehicular?
- ¿Qué escenarios aplican para las pruebas de vulnerabilidades de la red?

1.1.4. Objetivo General.

Analizar las vulnerabilidades a la red vehicular GMLAN CAN BUS a través de su interfaz de comunicación OBD-II y su dispositivo telemático ONSTAR, en los modelos de vehículos GM Tracker 2017, a fin de proponer controles de mitigación basadas en normas ISO 26612 e ISO 27002

1.1.5. Objetivos Específicos.

- Investigar la arquitectura de la red GMLAN CAN BUS, mediante un estudio de campo para conocer el estado actual de la misma.

- Analizar las diferentes técnicas de escaneo de vulnerabilidades aplicada a la red GMLAN CAN BUS a través de su puerto OBD-II, mediante equipos de diagnóstico vehicular con el fin de conocer el impacto en el funcionamiento vehicular.
- Realizar un análisis de vulnerabilidades al dispositivo telemático de ONSTAR y su interfaz de comunicación Bluetooth, mediante "fuzz testing", para analizar el comportamiento en la red GMLAN CAN BUS.
- Desarrollar recomendaciones de seguridad para disminuir los riesgos encontrados en el dispositivo telemático basado en las normas ISO 26612 e ISO 27002.

1.1.6. Justificaciones

En la actualidad la tendencia es conectar la mayor parte de aparatos de uso común a redes de acceso móviles, llámese Bluetooth, UMTS, Wi-Fi, etc. Las grandes empresas automotrices lo están realizando, conectando su parque automotriz con las redes móviles mediante dispositivos dedicados, enfocados en el entretenimiento, diagnóstico y comunicación de sus vehículos y así estas organizaciones se encuentran adoptando estándares y/o herramientas para asegurar la información en la red y con esto evitar ataques cibernéticos o por su nombre en inglés "cyberattack".

Los síntomas detallados previamente indican que esta investigación requiere ser realizada para solventar el desconocimiento de las amenazas a la red vehicular y así mejorar la calidad del producto de la empresa, el control de seguridad y la satisfacción del cliente final.

Justificación Teórica: el presente trabajo se justifica, mediante los diferentes artículos científicos y documentación privada de la empresa que desarrolla el dispositivo telemático

ONSTAR la cual fue detallada en el punto 1.1.1.1, en donde se evidencia la existencia de vulnerabilidades en la red vehicular. Como se indica en la investigación “A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN”, “muchos estudios se realizaron para indicar las vulnerabilidades de la red CAN, y se requiere de un mayor esfuerzo y conocimiento para encontrar más problemas y poder solventarlo” (Woo, Jo, & Hoon, 2015). De acuerdo a la publicación “DRIVING WITH SHARKS”, los ataques a los automóviles pueden poner en riesgo la vida humana y la solución es seguir investigando vulnerabilidades en dispositivos de conexión inalámbricas (Hashem Eiza & Ni, 2017).

Es por esto que GMLAN CAN BUS y su dispositivo telemático ONSTAR requiere de una indagación acerca del estado actual de sus vulnerabilidades siendo el segundo y el tercer objetivos específicos a ser cumplidos en la presente investigación; el cual generará reflexión y discusión.

Justificación Metodológica: La metodología a ser utilizada en este trabajo de investigación, se desprende de las investigaciones científicas realizada en, “In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions” (Liu, Zhang, & Sun, 2017), en la cual los autores realizan un estudio sobre la red CAN, las características específicas de cada dispositivos (ECUs) que están conectados dentro de la red, utilizando herramientas de diagnósticos y finalmente encontrando vulnerabilidades en los ECUs. Esto conlleva a una preocupación de seguridad sobre la posibilidad de que otros ECUs que no fueron parte del estudio tengan problemas; además los autores indican en sus recomendaciones que se debería realizar un análisis de vulnerabilidades a diferentes modelos de automóviles y así conocer los problemas en sus ECUs.

Algo importante en la investigación realizada por " (Koscher, Czeskis, Roesner, & Kohno, 2010)" señala que los dispositivos telemáticos son un punto de acceso vulnerable a la seguridad de la información ya que estos cuentan con acceso a redes inalámbricas y adquieren los problemas que cada tipo de red posee.

Para finalizar el estudio se apoyará en dos normas, la primera es ISO 26262:2011 la cual es una norma de seguridad automotriz define un marco, modelo de aplicación, actividades, métodos y resultados, ofreciendo a los fabricantes un mecanismo común para medir y documentar la seguridad de un sistema de automoción. Permite gestionar la seguridad funcional y regular el desarrollo de los automóviles a nivel de hardware, software y sistema durante todo el ciclo de vida. ISO 26262 contiene requisitos relacionados con la realización de un análisis de riesgos. Los requisitos de seguridad se especifican para evitar o prevenir los daños y reducción de riesgos. El trabajo de todas las empresas que se dedican al sector automotriz, debe estar basado en la norma dicha norma.

La última norma que se utilizará es ISO 27002:2013, ya que consiste en una guía de buenas prácticas para implantar controles que garantizarán la seguridad de la información gracias a sus recomendaciones. Por lo tanto las dos normativas se complementarían.

Justificación Práctica: El concepto de auto conectado se empezó a utilizarse en la última década cuando los dispositivos de control electrónico ECUs por siglas en inglés, lograron interactuar con redes de comunicación, UMTS, Bluetooth, Wi-Fi, etc. (Hashem Eiza & Ni, 2017) y con el desarrollo de herramientas de diagnóstico que son más fácil de usar para interpretar el comportamiento vehicular (Kulkarni, Rajani, & Varma, 2016).

Se encontraron falencias en la red vehicular utilizando distintas herramientas, como es el caso de "Techniques in hacking and simulating a modern automotive controller area

network", en este desarrollaron sus propias herramientas y software, tanto para simular una red vehicular como para realizar un ataque controlado al puerto OBD (Abbott-McCune & Shay, 2016). En la investigación "I Can Detect You: Using Intrusion Checkers to Resist Malicious Firmware Attacks" realiza ataques a la red CAN, utilizando herramientas de diagnóstico vehicular con el fin probar la solución que proponen al protocolo CAN para mitigar vulnerabilidades de seguridad (Shila, Geng, & Lovett, 2016) .Por último, la investigación llevada a cabo por (Woo, Jo, & Hoon, 2015), indica que se desarrolló un firmware y software para alterar el funcionamiento de la red CAN.

Justificación Legal: Esta investigación, se justifica de forma legal en base a lo que menciona la Constitución del Ecuador, en su Capítulo sexto. Derechos de libertad Art. 66.- Numeral 19.

> "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley." (pág. 49)

Y también en lo que menciona el Código Orgánico Integral Penal COIP, en su sección Tercera, Delitos contra la seguridad de los activos de los sistemas de información y comunicación. Artículo 230.- Interceptación ilegal de datos.

> Será sancionada con pena privativa de libertad de tres a cinco años: "1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible." (pág. 36)

Relevancia Social: Esta investigación abrirá nuevos caminos para que empresas con situaciones similares puedan tomar de referencia las vulnerabilidades que se encuentren en la red GMLAN CAN y así tomar las acciones pertinentes. Creará conciencia de seguridad a los usuarios de los dispositivos telemáticos y exigirá un mayor control de la información personal a las empresas que los proveen.

Creará nuevas oportunidades de estudios para solventar otras incógnitas como son ¿Existe vulnerabilidades en los ECUs que se conectan a la red móvil UMTS?, ¿puede un vehículo alterar su funcionamiento con un mensaje de texto o GPRS?

1.2. Marco Teórico

En los años 80 la industria automotriz tenía tres problemas:

El primero era la demanda de mayor comodidad en los automóviles particulares tales como ventanillas accionadas eléctricamente, asientos con calefacción, control de la temperatura del habitáculo, ajuste de asientos, espejos, equipos de audio, sistema de posicionamiento global controlado por satélite (GPS), etc.

El segundo era la seguridad en el vehículo: tales como mecanismos y dispositivos encargados de disminuir el riesgo a que se produzca un accidente y entre los cuales tenemos frenos, suspensión, luces y dirección, etc.

El tercer problema: consumo de combustible, rendimiento, y contaminación.

Los tres problemas eran enfrentados por medio de control electrónico, al principio con una única unidad electrónica de control (ECU), y luego con el agregado de otras. Entonces surge la necesidad de establecer una adecuada comunicación entre las distintas unidades electrónicas de control de dichos procesos.

1.2.1. Protocolo CAN y GMLAN

CAN o Controller Area Network (Control de Área de Red), nace para solventar la comunicación entre los ECUs, fue desarrollado por Bosch en 1985. Sin embargo, conforme los fabricantes comenzaron a utilizar más y más dispositivos electrónicos en los vehículos, el costo general del vehículo se incrementaba.

CAN tiene un concepto de comunicaciones de datos, que describe una relación entre un productor de mensajes y uno o más consumidores de estos. CAN es un protocolo orientado a mensajes, es decir la información que se va a intercambiar se descompone en mensajes, a los cuales se les asigna un identificador y se encapsulan en tramas para su transmisión. Cada mensaje tiene un identificador único dentro de la red, con el cual los nodos deciden aceptar o no dicho mensaje.

CAN está basado en las dos primeras capas del modelo referencial OSI (Open Systems Interconnection) como se indica en la figura 2 y 3. Las dos primeras capas son la capa física y la capa de enlace de datos. En la cual la capa de física se encarga de las conexiones físicas de la red, especifica los niveles o características eléctricas de las señales así como la codificación, decodificación, temporización y sincronización de los bits. Por último la capa de datos en la cual se controla el flujo de la información entre los nodos de la red, es decir se encarga de la transmisión de los bits *frames*, que los mensajes lleguen a su destino sin errores, controla las secuencias de transmisión, los acuses de recibido y si en determinado caso no se recibió bien un mensaje se encarga de retransmitirlo.

Figura 2. Modelo CAN vs modelo OSI, fuente: (Technosolutions, 2016)

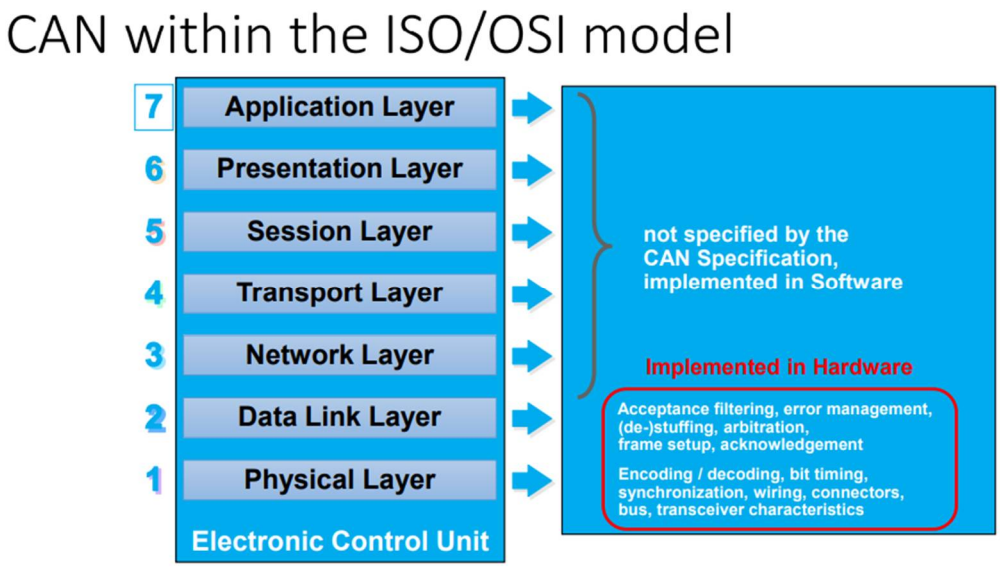
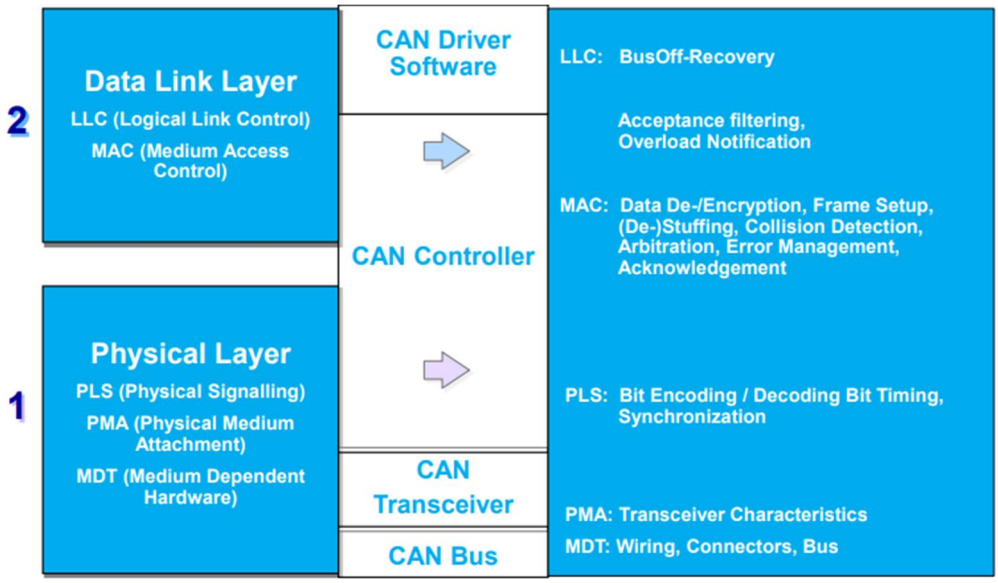


Figura 3. Capa 1 y 2, OSI vs CAN, fuente: (Technosolutions, 2016)



En noviembre de 1993 el protocolo CAN es estandarizado definido por las normas ISO (International Organization for Standardization):

- ISO/DIS 11898: Unidad de acceso al medio de alta velocidad. “HS BUS”

- ISO-CD 11519: Estándar para aplicaciones de baja velocidad, “LS BUS”
- J1939 de SAE: está dirigido a aplicaciones de camiones y autobuses.

En cada uno de estos estándares se encuentra, la capa de enlace y señalización física, unidad de acceso al medio, interfaz de velocidad y tolerancia de fallos, y el tiempo de comunicación. Dentro de sus principales características se encuentran:

- Prioridad de mensajes.
- Garantía de tiempos de latencia.
- Flexibilidad en la configuración.
- Recepción por multidifusión (multicast) con sincronización de tiempos.
- Detección y señalización de errores.
- Retransmisión automática de tramas erróneas
- Distinción entre errores temporales y fallas permanentes de los nodos de la red y desconexión autónoma de nodos defectuosos. (Pazul, 2018)

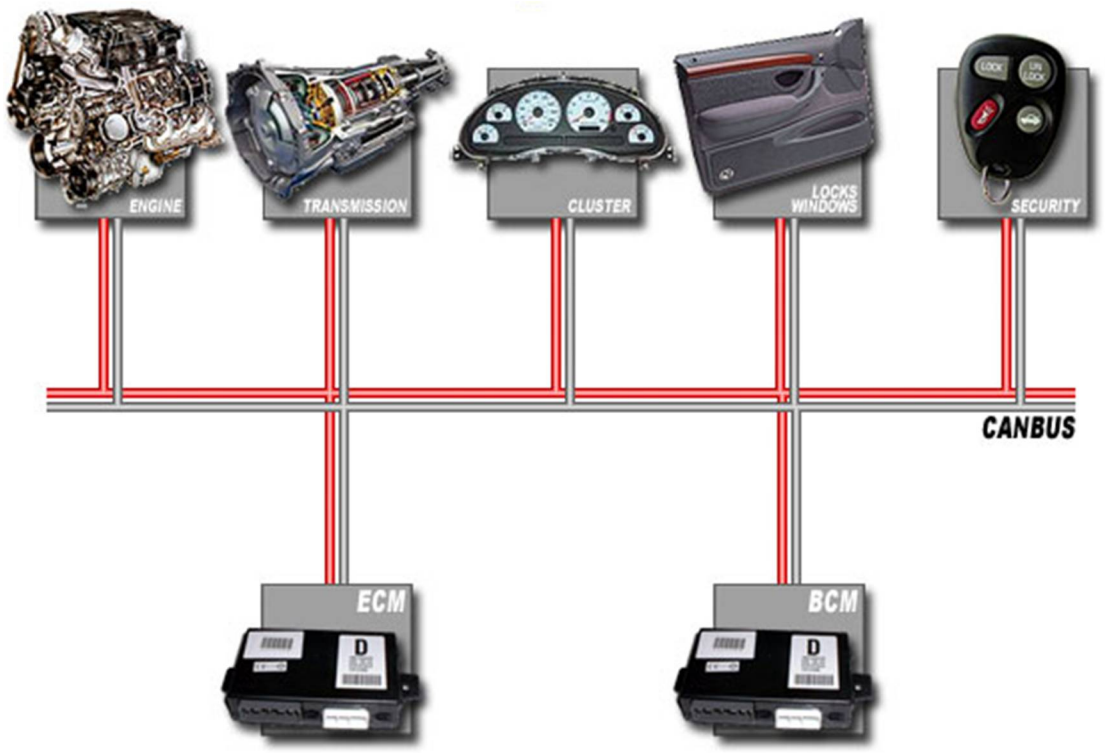
El desarrollador del software del sistema debe implementar el resto de las capas de la pila de protocolos OSI. Los protocolos de capa superior o sus siglas (HLP) se utilizan para:

1. Estandarizar los procedimientos de arranque, incluidas las tasas de bits usados,
2. Distribuir direcciones entre los nodos participantes o tipos de mensajes,
3. Determinar la estructura de los mensajes, y
4. Proporcionar rutinas de manejo de errores a nivel de sistema.

Esto de ninguna manera es una lista completa de las funciones que realizan los HLP, sin embargo, describe algunas de sus funciones básicas.

En la figura 4 se indica un ejemplo de una red CAN, en donde se encuentra conectado mediante un BUS de datos los diferentes nodos o partes un vehículo.

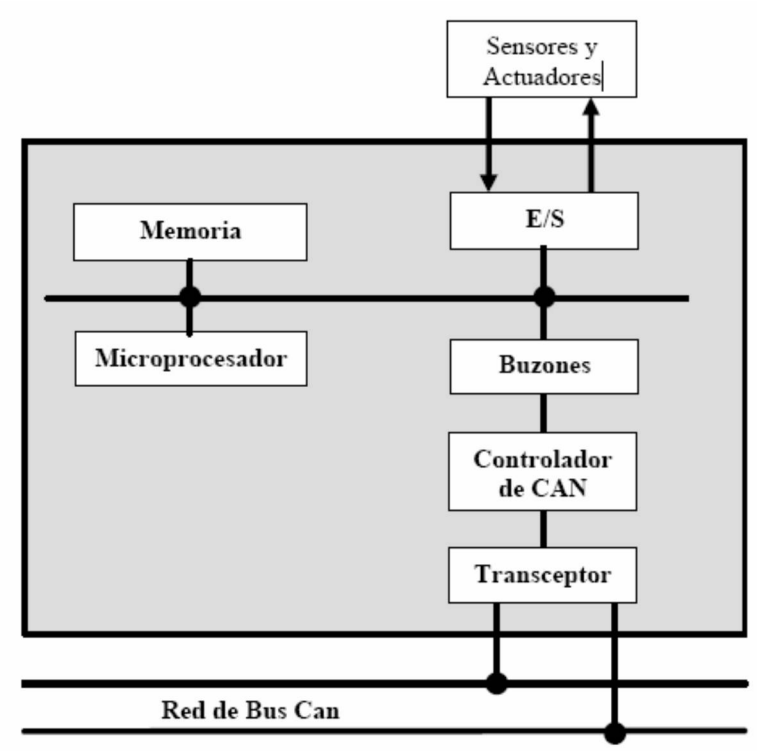
Figura 4. Ejemplo de una red CAN vehicular, fuente: (National Instrument, 2016)



Dentro de un nodo en la red CAN, se pueden distinguir una serie de módulos interconectados entre ellos: un bus de direcciones, datos y un control (paralelo) enlazando el controlador central, la memoria de los datos y el programa (donde está almacenado el software de aplicación y el controlador de red de alto nivel), los dispositivos de entrada y salida y, la interfaz de comunicación. Desde el punto de vista del micro-controlador, la interfaz de comunicación se puede ver como un conjunto de buzones, donde cada uno de estos sirve como registro lógico de interfaz entre el controlador local y los nodos o ECUs remotos. Si un nodo quiere comunicarse, tiene que dar de alta los correspondientes buzones de

recepción y transmisión antes de hacer ninguna operación. En la figura 5 se observa un ECU o nodo como diagrama de bloques de su funcionamiento descrito.

Figura 5. Diagrama Interno Nodo. Fuente: (MICROCHIP, 2012)



Teniendo en cuenta esta arquitectura, el funcionamiento sigue los siguientes pasos:

- Para inicializar, el programador especifica los parámetros de los registros de control de interfaz de comunicación, como las características del controlador de red o la velocidad de transmisión.
- A continuación, se actualizan todos los buzones. En cada buzón se especifica si es receptor o transmisor y, su estado inicial, inicializando su parte de datos del búfer.

- Posteriormente, para transmitir un mensaje es necesario poner los datos en el búfer de datos correspondiente al buzón de transmisión y activar el flanco de transmisión.

Por último, la interfaz de red intenta comunicar los datos a través de la red. El estado de la transferencia se puede comprobar en el estatus de estado de cada buzón.

En el BUS CAN es posible conectar hasta 22 nodos o ECUs, sin necesidad de alterar Hardware o Software, es por esto que el sistema se puede comparar a un “plug and play”. Entonces cada nodo se convierte en un elemento en el BUS de datos que es capaz de manipular la información, evaluar datos de sensores externos y tomar una decisión. A estos nodos se los conoce como Unidades de Control Electrónico con sus siglas en inglés ECU.

El protocolo CAN está basado en mensajes, no en direcciones. El nodo emisor transmite el mensaje a todos los nodos de la red sin especificar un destino y todos ellos escuchan el mensaje para luego filtrarlo según le interese o no.

Existen distintos tipos de tramas predefinidas por CAN para la gestión de la transferencia de mensajes:

- Trama de datos: Se utiliza normalmente para poner información en el bus y la pueden recibir algunos o todos los nodos.
- Trama de información remota: Puede ser utilizada por un nodo para solicitar la transmisión de una trama de datos con la información asociada a un identificador dado. El nodo que disponga de la información definida por el identificador la transmitirá en una trama de datos.
- Trama de error: Se generan cuando algún nodo detecta algún error definido.

- Trama de sobrecarga: Se generan cuando algún nodo necesita más tiempo para procesar los mensajes recibidos.
- Espaciado entre tramas: Las tramas de datos (y de interrogación remota) se separan entre sí por una secuencia predefinida que se denomina espaciado inter-trama.
- Bus en reposo: En los intervalos de inactividad se mantiene constantemente el nivel recesivo del bus.

En el BUS CAN los nodos transmiten la información espontáneamente con tramas de datos, bien sea por un proceso cíclico o activado ante eventos en el nodo. La trama de interrogación remota sólo se suele utilizar para detección de presencia de nodos o para puesta al día de información en un nodo recién incorporado a la red. Los mensajes pueden entrar en colisión en el bus, el de identificador de mayor prioridad sobrevivirá y los demás son retransmitidos lo antes posible. En la figura 6 se encuentra un ejemplo genérico de una trama de dato de CAN, la cual se detalla cada campo en la tabla 1.

Figura 6. Trama de datos en CAN, fuente: Propia

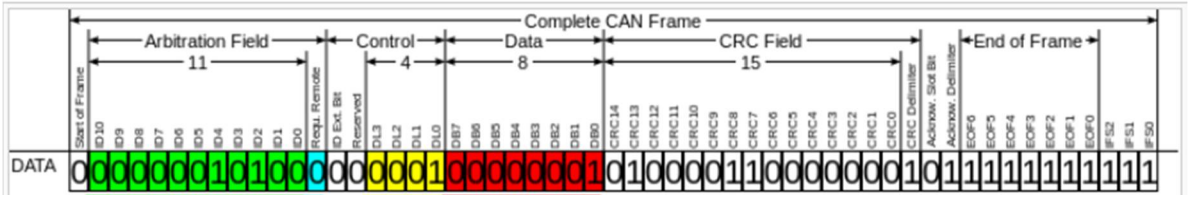


Tabla 1.Descripción trama de datos CAN, fuente: Propia

Campo	Tamaño (bits)	Descripción
Start-of-frame	1	Denotes the start of frame transmission
Identifier (green)	11	A (unique) identifier for the data which also represents the message priority
Remote transmission request (RTR)	1	Dominant (0) (see Remote Frame below)

Identifier extension bit (IDE)	1	Declaring if 11 bit message ID or 29 bit message ID is used. Dominant (0) indicate 11 bit message ID while Recessive (1) indicate 29 bit message.
Reserved bit (r0)	1	Reserved bit (it must be set to dominant (0), but accepted as either dominant or recessive)
Data length code (DLC) (yellow)	4	Number of bytes of data (0–8 bytes)
Data field (red)	0–64 (0-8 bytes)	Data to be transmitted (length in bytes dictated by DLC field)
CRC	15	Cyclic redundance check
CRC delimiter	1	Must be recessive (1)
ACK slot	1	Transmitter sends recessive (1) and any receiver can assert a dominant (0)
ACK delimiter	1	Must be recessive (1)
End-of-frame (EOF)	7	Must be recessive (1)

En 1999 General Motors empieza el uso del protocolo GMLAN (General Motor Local Area Netwtork), el cual tiene como protocolo base el mencionado CAN, cuenta con las mismas interfaces de acceso, los ECUs utilizan una misma base de datos para compartir mensajes e interactuar, componentes electrónicos similares y el desarrollo de controladores es administrado por la compañía VECTOR. Debe cumplirse dichas condiciones para el correcto funcionamiento de los ECUs en GMLAN.

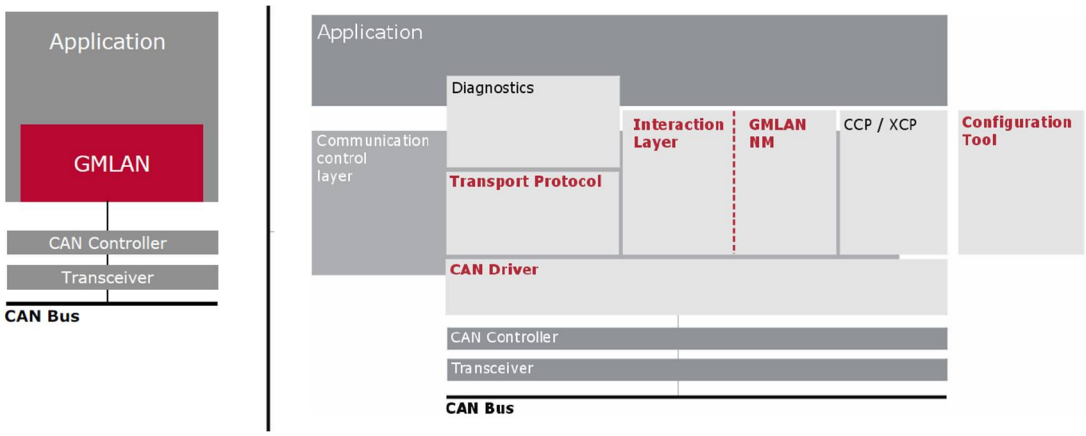
VECTOR se encarga de que el software sea compatible

- Con un micro controlador específico.
- Con un controlador CAN específico
- Con un compilador específico.

Entregando a los desarrolladores los controladores y librerías de GMLAN, para que ellos realicen la parte aplicativa de los ECUs a ser desarrollados, como se puede observar en

la figura 7 es un diagrama de bloques de como VECTOR maneja las librerías que entregan a los desarrolladores.

Figura 7. ECUs en un vehículo GM, fuente: (VECTOR, 2017)

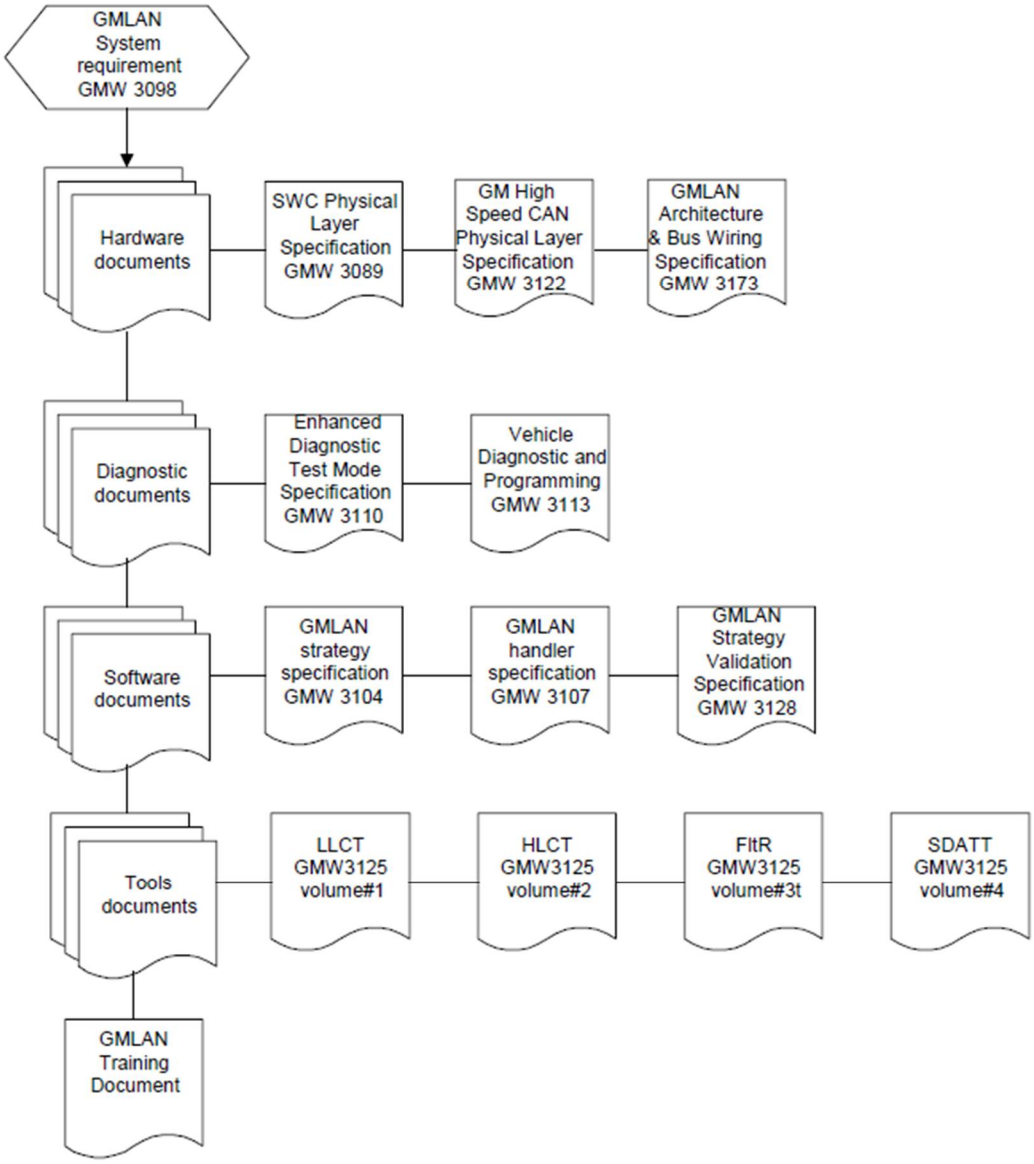


VECTOR al proveer el desarrollo de las capas 1 y 2 del modelo OSI, el desarrollador solo se encarga de realizar la parte aplicativa en la cual se encuentra GMLAN. GMLAN está basado en CAN, incluye dos buses CAN que se conectan entre sí a través de un nodo "gateway". Un bus CAN de doble cable de alta velocidad y el otro de un solo cable de baja velocidad. En GMLAN existe un nodo de puerta de enlace que permite la comunicación entre los nodos de alta velocidad y los nodos de baja velocidad, a este nodo se lo conoce como *Body Control Module* o por sus siglas BCM.

Para todo este tipo de comunicación e implementación GM y VECTOR realizaron diferentes normas, en la figura 8 se indica un resumen de sus normativas. La normativa en la cual se va a centrar esta investigación es la GMW3110 la cual establece la estrategia de diagnóstico en la red GMLAN. Se requiere que esta normativa sea implementada por cualquier nodo o ECU en cualquiera de las subredes de GMLAN. El objetivo principal de esta norma es que todos los ECUs mantengan una comunicación de diagnóstico entre ellos es

decir, se pueda conocer el status del carro y sus componentes a tiempo real para evitar posibles fallas y prevenir daños.

Figura 8. Normas de General Motor. Fuente: GMLAN General Specifications



La norma contempla diferentes tipos de mensajes entre los ECUs, a los cuales lo llamaron servicios de diagnóstico, en total son 20 servicios de diagnósticos que se enumerarán y se detallarán los que se utilizan en la presenta investigación:

1. Servicio $04, borrar de códigos de diagnóstico, DTC.
2. Servicio $10, inicio de sistemas de diagnóstico.
3. Servicio $12,leer de fallas
4. Servicio $1A, leer parámetros internos del dispositivo

El objetivo de este servicio es proporcionar la capacidad de leer el contenido de datos en los ECU haciendo referencia a un identificador de datos (DID) que contiene información estática, como datos de identificativos propias de cada ECU u otra información que no requiere actualizaciones en tiempo real. Para esto en la herramienta de diagnóstico vehicular se debe enviar un mensaje de que contenga el encabezado $1A XX YY, en donde XX significa el identificador de dos bytes y YY indica el ECU que se desea conocer la información. La respuesta que indicará el ECU será relaciona a los identificadores guardados en memoria ROM, como un ejemplo se requiere conocer el si la Radio está activa se enviará $1A 45 626

5. Servicio $20, regreso a comunicación normal
6. Servicio $22, leer señales
7. Servicio $23, leer memorias
8. Servicio $27, Seguridad
9. Servicio $28, deshabilitar la comunicación normal

El objetivo de este servicio es evitar que un dispositivo transmita o reciba todos los mensajes que no son el resultado directo de una solicitud de diagnóstico. El uso principal del servicio es configurar un evento de programación. Este es un servicio obligatorio que debe ser compatible con todos los ECUs. Para realizar esta solicitud se debe enviar la siguiente cabecera $28 XX YY ZZ, en donde XX indica a que ECU está dirigido el mensaje, YY el tiempo de duración, ZZ la longitud del mensaje.

10. Servicio $2C, envío de paquetes dinámicos
11. Servicio $2D, activar / desactivar funcionalidades del dispositivo
12. Servicio $34, solicitud de descarga
13. Servicio $36, transferencia de archivos
14. Servicio $3B, escribir parámetros internos
15. Servicio $3E, presencia de “*tester tool*”

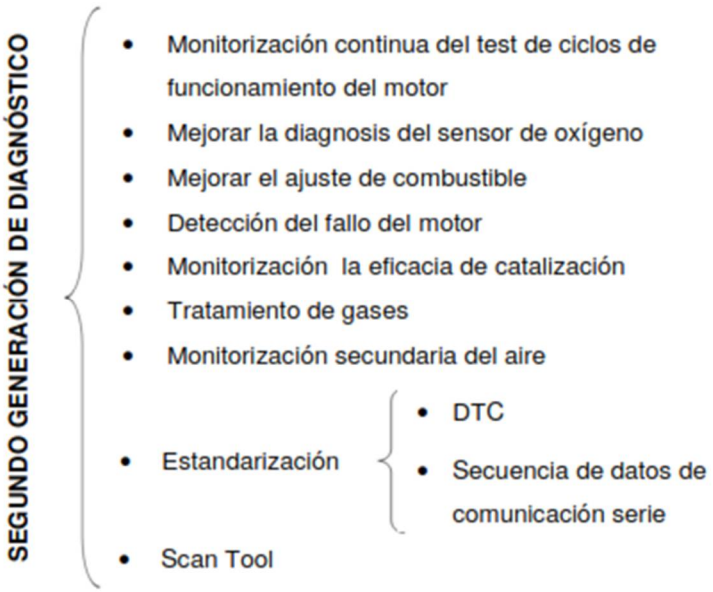
16. Servicio $A2, reporte el tipo de programación
17. Servicio $A5, diferentes tipos programación
18. Servicio $A9, códigos de fallas
19. Servicio $AA, señales continuas
20. Servicio $AE, control de interfaces del dispositivo I/O

1.2.2. Herramientas y Diagnóstico Vehicular

Durante los años 70 e inicios de los 80 ciertos fabricantes de automóviles, emprendieron el uso de ECUs orientado al **control y diagnóstico de errores**. Al principio fue solo para conocer y controlar la contaminación ambiental producida por el vehículo y adaptarlas a los estándares exigidos, pero con forme pasó del tiempo estos sistemas se volvieron cada vez más sofisticados, hasta los finales de los años 90, donde surgió el estándar OBD (Diagnóstico a Bordo).

OBD por definición es un sistema de diagnóstico integrado en la gestión de los sensores y actuadores del vehículo, por lo tanto es un programa instalado en las unidades de mando del motor, con un acceso físico (Caizatoa Chulca & Méndez Flores, 2014). Una de sus funciones es vigilar continuamente los componentes que intervienen en las emisiones de escape, al monitorear estas, también revisa sus componentes y funciones existente en el sistema del motor, los aspectos más importantes son de OBD son detallados en la Figura 9.

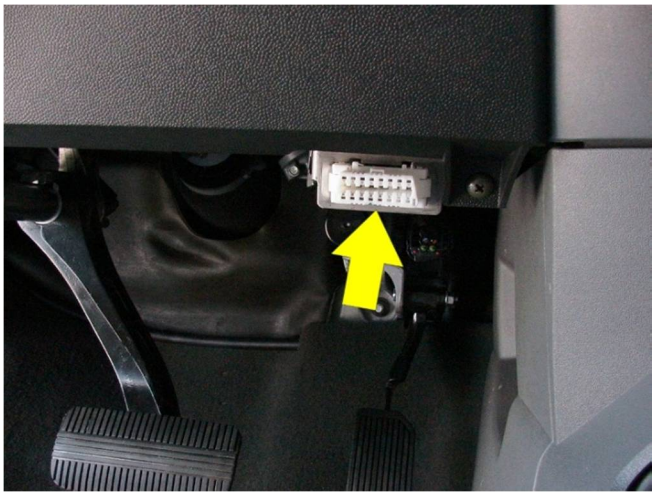
Figura 9. Aspectos importantes de OBD II, fuente: propia



La segunda versión de diagnóstico (OBD II) empieza a tomar fuerza a partir del año 1996, en esta segunda generación, se monitoriza y controla los sistemas y componentes en la red CAN. Lo más importante es que se estandariza la comunicación, logrando acceder a ciertos mensajes de los ECUS.

OBD-II tiene un interfaz hardware estándar de 16 pines (conector J1962 hembra). El conector cumple las especificaciones según la normativa ISO 15031-3:2004, que específica incluso donde debe estar situado el conector, aunque realmente se suele encontrar debajo del volante como se puede observar en la Figura 10 . La distribución de los pines se encuentra en la Figura 11.

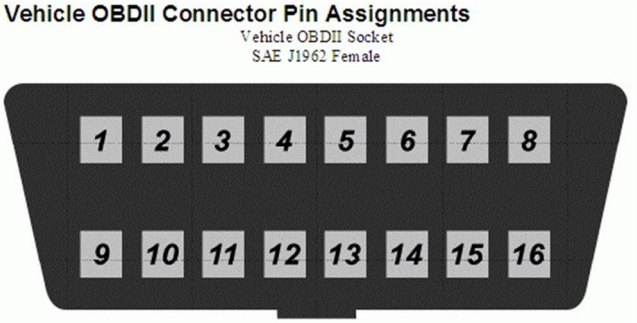
Figura 10. Puerto de acceso OBD II, Fuente: propia



El sistema OBD debe aportar un sistema de Códigos de Error de Diagnóstico o DTC (Diagnostic Trouble Codes) y tablas de errores en los manuales de reparación para ayudar a los técnicos (personal autorizado) a determinar las causas más probables de avería en el motor y problemas en las emisiones de gases. Los objetivos básicos de esta regulación son fundamentalmente dos:

- Reforzar el cumplimiento de las normativas de la regulación de la emisión de gases alertando al conductor cuando se presenta un fallo.
- Ayudar a los técnicos de reparación de automóviles en la identificación y reparación de fallos en el sistema de control de emisiones.

Figura 11.Conector OBD-II, fuente: Propia



Pin 1	GM LAN LS	Pin 9	GM LAN MS
Pin 2	J1850 Bus+	Pin 10	SAE J1850
Pin 3	Discretionary	Pin 11	Discretionary
Pin 4	Chasis Ground	Pin 12	Discretionary
Pin 5	Signal Ground	Pin 13	Discretionary
Pin 6	CAN HIGH (ISO 157645-4)	Pin 14	ISO 15765-4 CAN LOW
Pin 7	K-Line (ISO 9141-2)	Pin 15	ISO 9141-2
Pin 8	Discretionary	Pin 16	Battery Power

El OBD-II ofrece acceso a cinco protocolos diferentes, aunque la mayor parte de vehículos implementan solo uno de esos protocolos. Todos los pines de conexión de OBD-II usan el mismo conector, pero según el protocolo difieren en qué pines, excepto el pin 4 (Negativo batería) y el pin 16 (Positivo batería). OBD-II al ofrecer la conexión a los diferentes protocolos de comunicación, entre los cuales se encuentra los protocolos básicos de CAN y de GMLAN, es un acceso a la trama de mensajes que tiene el BUS y con herramientas adecuadas para la interpretación de los mensajes CAN, OBD se convierte un punto de acceso físico y ataque a la red CAN convirtiéndose en un nodo crítico para ser analizado. (Hoppe, Kiltz, & Dittmann, 2011)

Las herramientas que se utilizan para interpretar y acceder a las tramas GMLAN a través de su puerto OBD, se llaman herramientas de diagnóstico electrónico automotriz. Estas herramientas generalmente pueden ser usadas en una amplia variedad de carros y modelos. Estas herramientas leen problemas o códigos de error en la trama CAN de un vehículo para identificar módulos o ECUs con problemas para que luego sean revisadas por un mecánico.

Como un ejemplo de esto es la figura 12, la cual es una herramienta genérica para diferentes modelos de vehículos que inclusive puede llegar a cambiar el comportamiento de los ECUs pudiendo reprogramarlos. El costo de estas herramientas genéricas varía desde los $70 hasta los $3000, de igual manera poseen diferentes funcionalidades dependiendo del costo.

La mayoría de estas herramientas no pueden ser utilizadas en vehículos de modelos antiguos debido a temas de incompatibilidad, pero existen varias herramientas avanzadas de diagnóstico vehicular las cuales funcionan como un “sniffer” para el protocolo CAN, que cuentan con un propio software que traduce las tramas de datos binarios de CAN a mensajes ASCII para que el usuario interprete, generar nuevos mensajes, y cree aplicaciones muy similares al popular WireShark, pero para el protocolo CAN

Figura 12. Herramienta diagnóstica MaxiSys Mini MS90, Fuente: propia

1.2.3. Dispositivo Telemático

Con el acceso a Internet y los dispositivos de entretenimiento de audio/video, llegan nuevos ECUs a la red CAN del sistema automotriz, como son radios con acceso a redes móviles o dispositivos telemáticos, logrando crear el llamado INFOTAINMENT (información

y entrenamiento), con el cual el vehículo tiene acceso a redes móviles y envía información acerca de su estado. En la figura 13 se encuentra un diagrama indicando cómo se tiene acceso a la información del vehículo y la figura 14 en la las diferentes redes móviles que un vehículo puede tener.

Figura 13. Red CAN con acceso a redes móviles y dispositivos de diagnóstico, fuente (Woo, Jo, & Hoon, 2015)

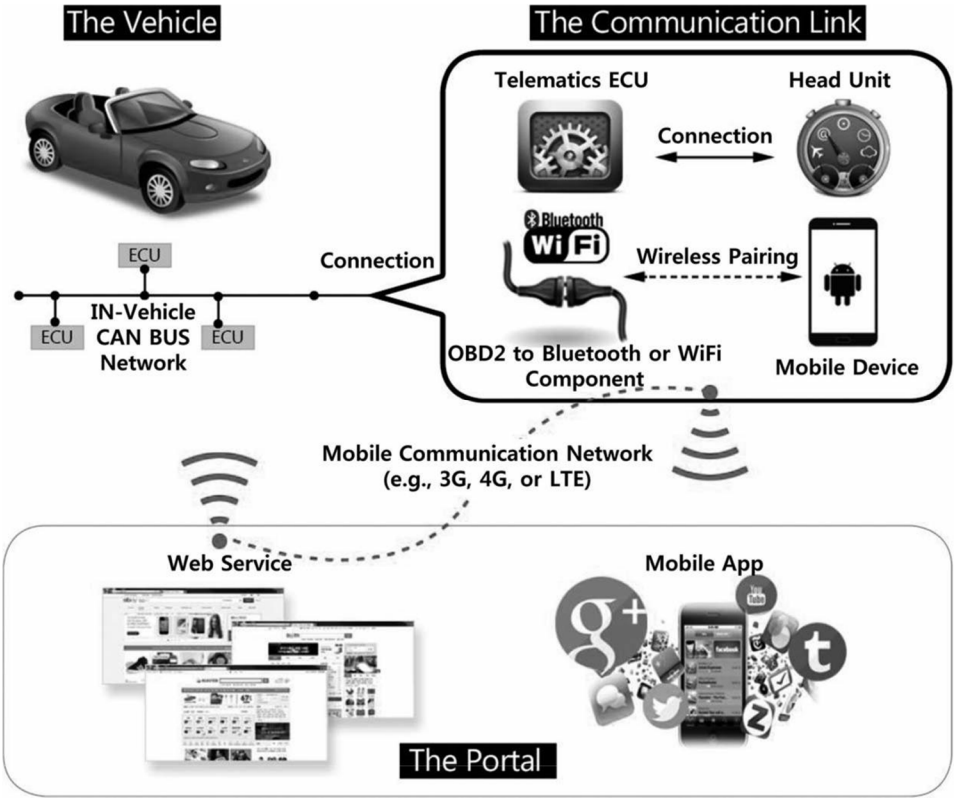
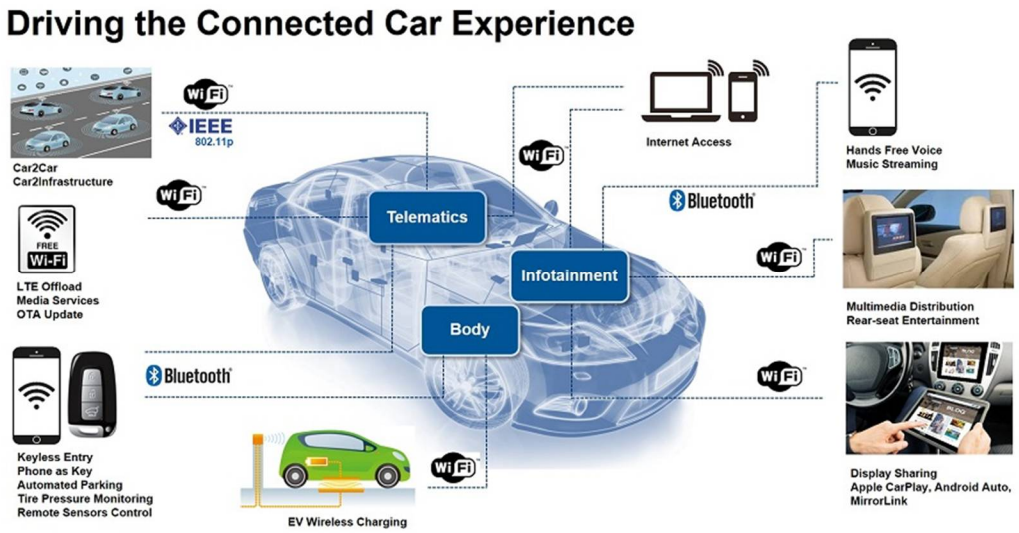


Figura 14. CAN conectado a redes externas mediante INFOTAINMENT ECUs, fuente: (CYPRESS, 2015)



En la red GMLAN se incorpora un dispositivo telemático, el cual cumple con todas las normas de GM es decir cuenta con diagnostico vehicular y cuenta con el stack de VECTOR, el objetivo de este dispositivo es proveer seguridad al usuario del vehículo, monitoreo en ruta y diagnostico vehicular, a través de una plataforma la cual tiene acceso el usuario cuando paga el servicio. El sistema de rastreo satelital que consta del dispositivo telemático se detalla en la figura 15. Existen diferentes tipos de dispositivos telemáticos, los cuales viene abreviados por sus siglas UU, P5, P7, P8, y sus funcionalidades se encuentran en la figura 16

Figura 15.Sistema de posicionamiento vehicular. Fuente: Propia

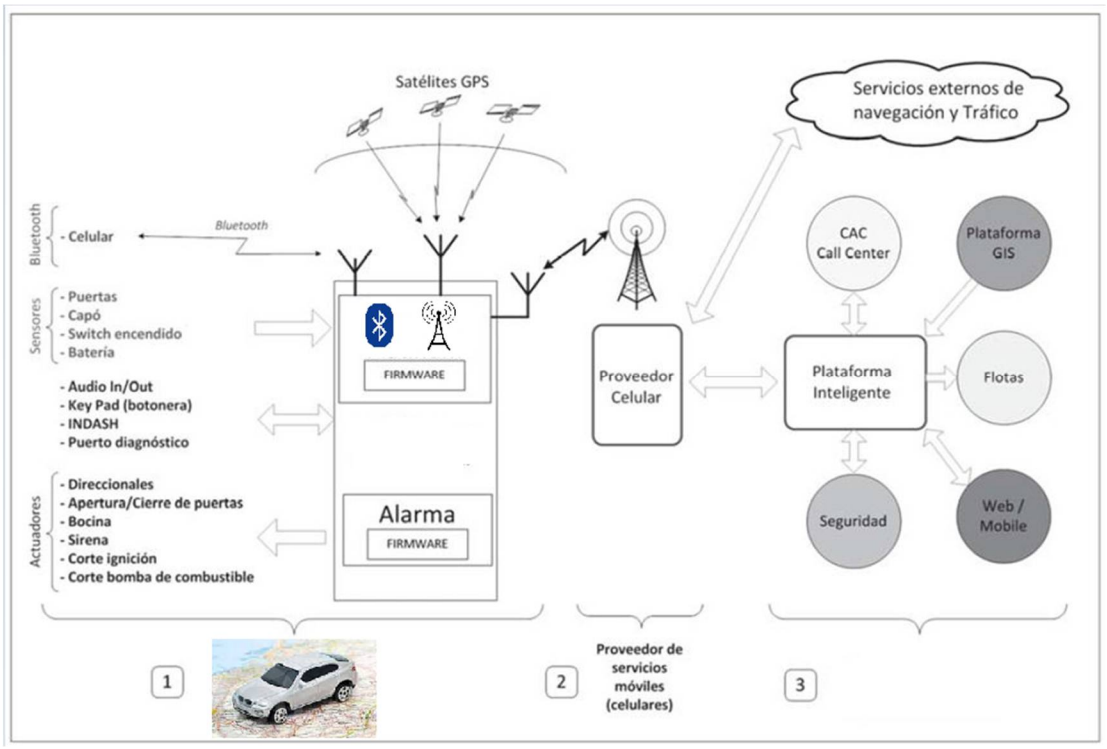
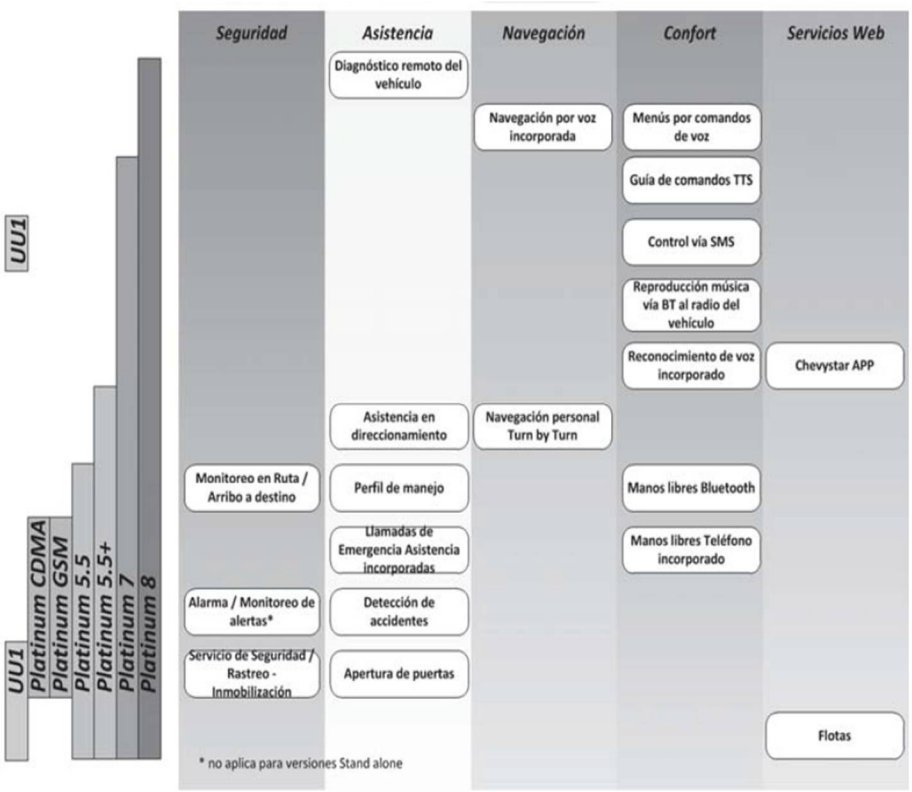


Figura 16.Servicios telemáticos. Fuente: Propia



El dispositivo telemático se comunica a través de mensajes de texto o de GPRS a un servidor llamado “COM SERVER”, como muestra la figura 17. La interacción entre la el COMM SERVER y el dispositivo telemático se lo realiza mediante la mensajería llamada O2V y V2O. Estos mensaje de texto tiene una cabecera de inicio “$”, el protocolo que COM Server y el dispositivo utilizan, el identificativo del vehículo, los datos y el por último un *checksum*, esto se muestra en la figura 18

Figura 17. Sistema BACKOFFICE. Fuente: Propia.

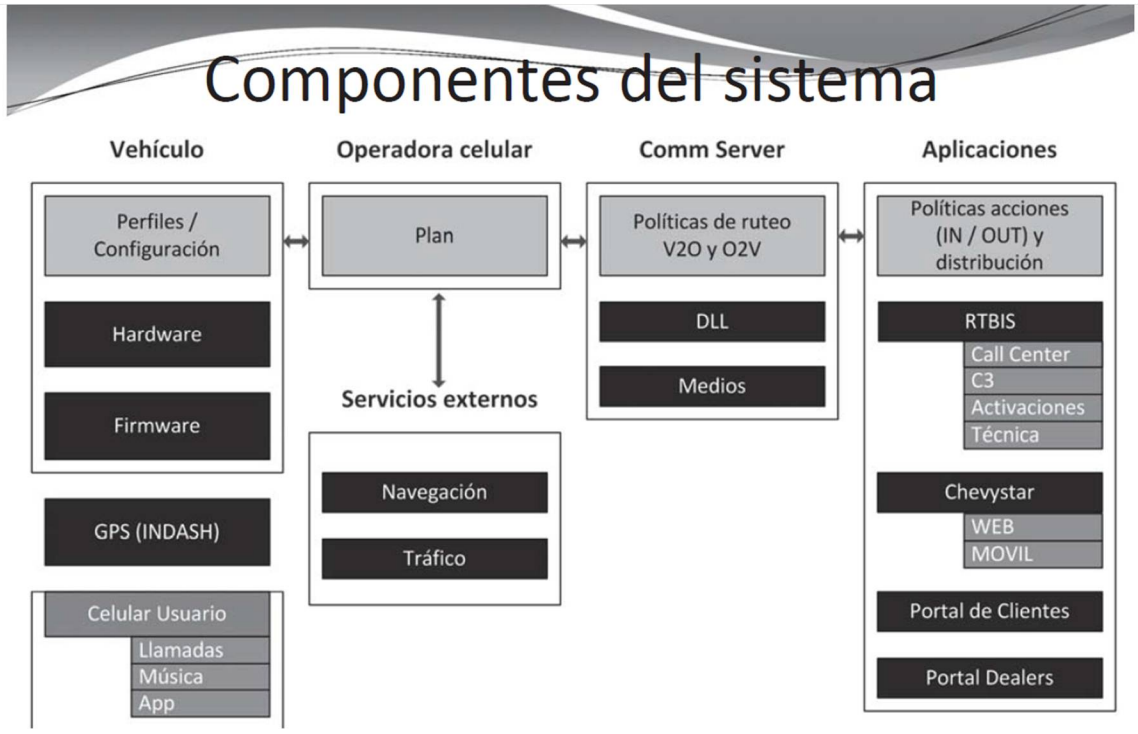
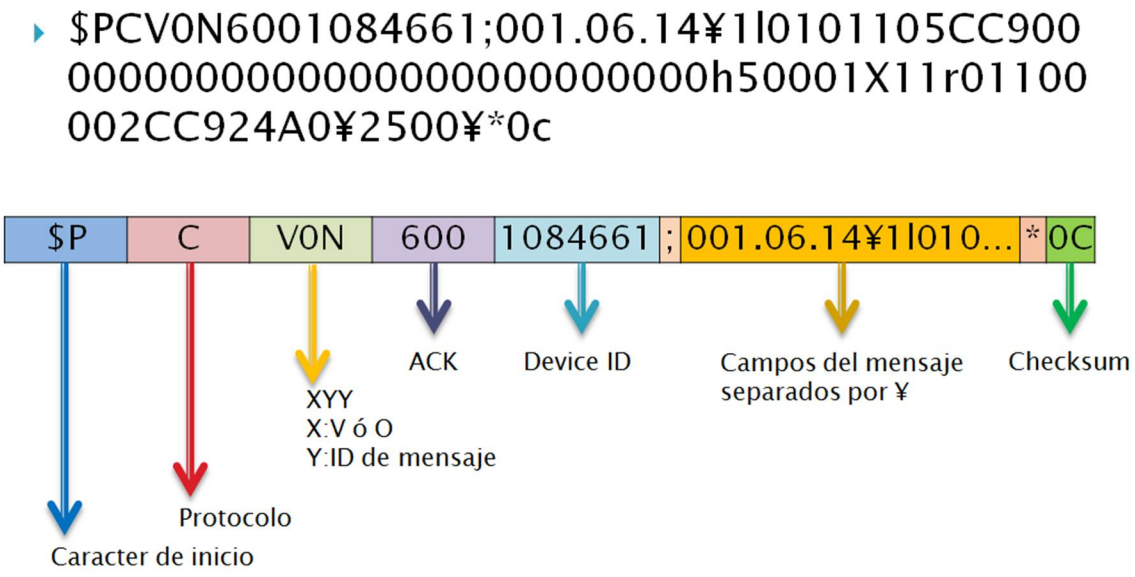


Figura 18.Arquitectura de un mensaje. Fuente: Propia



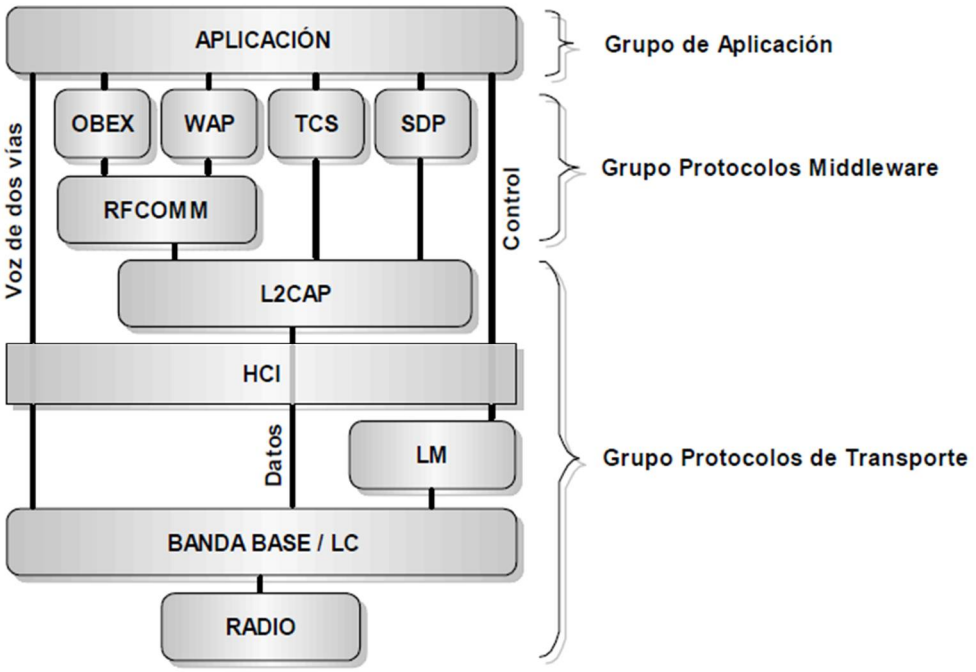
Uno de los servicios que brinda el sistema telemático para el confort del usuario son manos libres mediante el protocolo de comunicación Bluetooth. Este una tecnología inalámbrica basada en ondas de radiofrecuencia, la cual tiene un bajo costo de implementación y muy poco consumo de corriente, es por esto que es ideal para comunicaciones a cortas distancias y se adapta muy bien dentro del sistema vehicular. (Varela & Domínguez, 2002).

Todo dispositivo Bluetooth cuenta con un transmisor de potencia de aproximadamente 1mW para un alcance máximo de 10 metros, Trabaja en frecuencias de 2.4Ghz con una tecnología FHSS (Espectro expandido y saltos de frecuencia), teniendo un número máximo de conexión de 8 dispositivos por piconet y hasta 10 piconets.

La pila del protocolo Bluetooth se encuentra constituida por varias capas, las cuales se agrupan en 3 partes, la primera llamada transporte, segunda Middleware y por último la capa

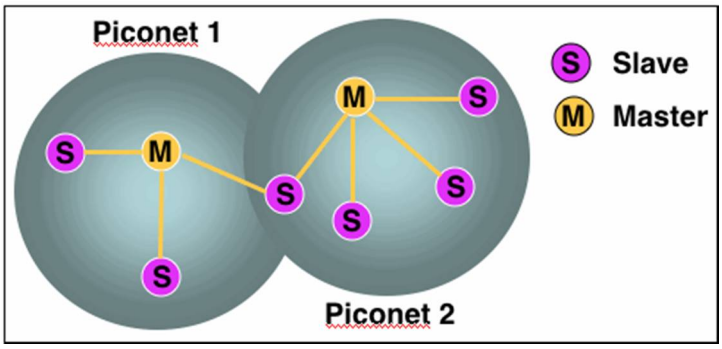
de Aplicación. El único dato que no pasa por todos los grupos es el audio ya que con esto se garantiza la calidad del servicio, ver la Figura 19. (Linarez & Quijano, 2004)

Figura 19. Pila de protocolo Bluetooth: Fuente: (Linarez & Quijano, 2004)



Una red piconet, está compuesta por dos o más dispositivos Bluetooth que, comparten el mismo canal y solo puede existir un maestro y los demás serán esclavos. El dispositivo que es maestro se encarga de establecer la comunicación eligiendo hop adecuado, canal, etc, ver Figura 20.

Figura 20. Ejemplo de Piconet. Fuente: Propia



El protocolo de capa de adaptación y control lógico de enlace (L2CAP por sus siglas en inglés) está superpuesto sobre el protocolo de banda base y reside en la capa de enlace de datos. L2CAP proporciona servicios de datos orientados a conexión y sin conexión a protocolos de capa superior con capacidad de multiplicación de protocolos, operaciones de segmentación y re ensamblaje, y abstracciones grupales. L2CAP permite protocolos y aplicaciones de nivel superior para transmitir y recibir paquetes de datos L2CAP de hasta 64 kilobytes de longitud.

Se admiten dos tipos de enlaces para la capa de banda base: enlaces orientados a conexión síncrona (SCO) y enlaces de conexión asincrónica sin conexión (ACL). Los enlaces SCO admiten tráfico de voz en tiempo real utilizando ancho de banda reservado. Los enlaces de ACL admiten el tráfico de mejor esfuerzo. La especificación L2CAP se define solo para los enlaces ACL y no se prevé la compatibilidad con los enlaces SCO. (BLUETOOTH, 2018)

1.2.4. Normativas ISO

1.2.4.1. ISO 26262:2011

Esta normativa nace para cumplir con las necesidades específicas del sector de aplicaciones de sistemas eléctricos y/o electrónicos (E/E) dentro de los vehículos de carretera. La normativa se aplica a todas las actividades durante el ciclo de vida de seguridad de los sistemas relacionados con la seguridad compuestos por componentes eléctricos, electrónicos y de software.

La seguridad es uno de los temas clave del futuro en el desarrollo del automóvil. Las nuevas funcionalidades, no solo en áreas como la asistencia al conductor, la propulsión, el control de la dinámica del vehículo y los sistemas de seguridad activa y pasiva, están cada vez más cerca del dominio de la ingeniería de seguridad del sistema. El desarrollo y la integración de estas funcionalidades fortalecerán la necesidad de procesos de desarrollo de sistemas seguros y la necesidad de proporcionar evidencia de que se cumplen todos los objetivos razonables de seguridad del sistema.

Con la tendencia de aumentar la complejidad tecnológica, el contenido de software y la implementación mecatrónica, existen riesgos crecientes a partir de fallas sistemáticas y fallas de hardware aleatorias. ISO 26262 incluye una guía para evitar estos riesgos al proporcionar requisitos y procesos apropiados.

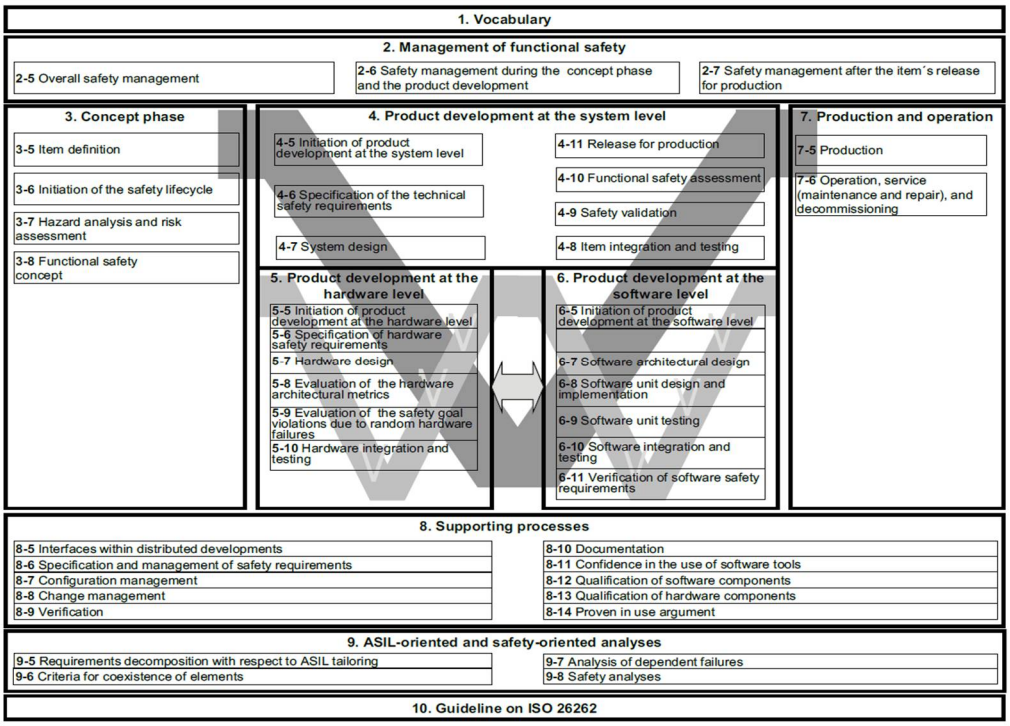
La seguridad del sistema se logra a través de una serie de medidas de seguridad, que se implementan en una variedad de tecnologías (por ejemplo, mecánica, hidráulica, neumática, eléctrica, electrónica, electrónica programable) y se aplican en los diversos niveles del proceso de desarrollo. (BS ISO 26262, 2011)

ISO 26262:

a) Proporciona un ciclo de vida de seguridad automotriz (gestión, desarrollo, producción, operación, servicio, desmantelamiento) y admite la adaptación de las actividades necesarias durante estas fases del ciclo de vida;
b) Proporciona un enfoque basado en el riesgo específico del automóvil para determinar los niveles de integridad [Niveles de Integridad de la Seguridad del Automóvil (ASIL)];
c) Utiliza ASIL para especificar los requisitos aplicables de ISO 26262 para evitar el riesgo residual irracional;
d) Proporciona requisitos para las medidas de validación y confirmación para asegurar que se alcance un nivel de seguridad suficiente y aceptable;
e) Proporciona requisitos para las relaciones con los proveedores.

La Figura 1 muestra la estructura general de la edición ISO 26262:2011. Se basa en un modelo V como modelo de proceso de referencia para las diferentes fases del desarrollo del producto

Figura 21. Visión general ISO 26262, fuente: (BS ISO 26262, 2011)



1.2.4.2. ISO 27002:2013

Es un estándar Internacional que está diseñado para que las organizaciones lo utilicen como referencia para seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información o como documento guía para organizaciones que implementan controles de seguridad de la información comúnmente aceptados. Este estándar también está destinado a utilizarse en el desarrollo de directrices de gestión de la seguridad de la información específicas de la industria y la organización, teniendo en cuenta su entorno de riesgos de seguridad de la información específica.

Las organizaciones de todos los tipos y tamaños (incluidos los sectores público y privado, comerciales y sin fines de lucro) recopilan, procesan, almacenan y transmiten información de muchas formas, incluidas las electrónicas, físicas y verbales (por ejemplo, conversaciones y presentaciones).

El valor de la información va más allá de las palabras escritas, números e imágenes: el conocimiento, los conceptos, las ideas y las marcas son ejemplos de formas intangibles de información. En un mundo interconectado, la información y los procesos relacionados, sistemas, redes y personal involucrados en su operación, manejo y protección son activos que, como otros activos comerciales importantes, son valiosos para el negocio de una organización y consecuentemente merecen o requieren protección contra diversos riesgos.

Los activos están sujetos a amenazas deliberadas y accidentales, mientras que los procesos, sistemas, redes y personas relacionadas tienen vulnerabilidades inherentes. Los cambios en los procesos y sistemas de negocios u otros cambios externos (como nuevas leyes y regulaciones) pueden crear nuevos riesgos de seguridad de la información. Por lo tanto, dada la multitud de formas en que las amenazas pueden aprovechar las vulnerabilidades para dañar a la organización, los riesgos de seguridad de la información siempre están presentes. La seguridad efectiva de la información reduce estos riesgos al proteger a la organización contra amenazas y vulnerabilidades, y luego reduce los impactos a sus activos.

La seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, que incluyen políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles deben establecerse, implementarse, monitorearse, revisarse y mejorarse, cuando sea necesario, para garantizar que se cumplan los objetivos de seguridad y comerciales específicos de la organización.

En un sentido más general, la seguridad efectiva de la información también asegura a la gerencia y otras partes interesadas que los activos de la organización son razonablemente seguros y están protegidos contra daños, actuando así como un habilitador comercial.

Esta Norma Internacional proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización. Este Estándar Internacional está diseñado para ser utilizado por organizaciones que tienen la intención de:

a) Seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información.
b) Implementar controles de seguridad de la información comúnmente aceptados;
c) Desarrollar sus propias pautas de gestión de la seguridad de la información.

La normativa posee 14 dominios con 35 objetivos de control y 114 controles

1) La política de seguridad.
2) Los aspectos organizativos de la seguridad de la información.
3) La gestión de activos.
4) La seguridad ligada a los recursos humanos.
5) La seguridad física y ambiental.
6) La gestión de las comunicaciones y de las operaciones.
7) Los controles de acceso a la información.
8) La adquisición, desarrollo y mantenimiento de los sistemas de información.
9) La gestión de incidentes en la seguridad de la información.
10) La gestión de la continuidad del negocio.
11) Los aspectos de cumplimiento legal y normativo.

1.2.5. Estado del Arte

Las unidades de control electrónico automotriz (ECU) han sido el foco de muchos investigadores de seguridad que han demostrado la capacidad de afectar la operación determinista de los sistemas ciber físicos de vehículos. Se han descubierto fallas en el diseño de software que tienen impactos directos a la seguridad funcional de un vehículo. El rápido aumento en la conectividad de datos dentro de un automóvil moderno ha ampliado la superficie de ataque, permitiendo a los adversarios el acceso remoto a las redes de vehículos y al software del sistema de control. En el análisis “Evaluation of Software Vulnerabilities in Vehicle Electronic Control Units” (Edwards, Kashani, & Iyer, 2017) los autores indican los resultados del análisis de código estático realizado en el código fuente del software de producción automotriz usando estándares de codificación de referencia tales como las pautas de codificación segura MISRA y CERT C, en un intento de identificar los errores de software más importantes que probablemente permanezcan en el vehículo, como vulnerabilidades de seguridad de día cero.

En la revista publicada de la IEEE (Hashem Eiza & Ni, 2017), se da a conocer en manera teórica de como los ECUs conectados a diferentes redes externas del vehículo tiene vulnerabilidades adquiridas y con esto ser potencialmente vulnerables en la red CAN. Los autores ilustran los posibles daños vehiculares, daños el motor, los frenos deshabilitados, las puertas cerradas, etc.

Los estudios sobre seguridad vehicular han sido conducidos principalmente por proyectos financiados con fondos europeos (por ejemplo, SEVECOM, PRECIOSA, EVITA y OVERSEE) durante los últimos diez años. El proyecto EVITA (E-safety Vehicle Intrusion ProTected Applications) definió específicamente los requisitos de seguridad y desarrolló

soluciones apropiadas para redes de a bordo de vehículos. Entre estas soluciones, se desarrolló EVITA-MEDIUM-HSM para implementar un entorno de comunicación seguro entre las ECU (EVITA, 2015). Sin embargo, EVITA no proporciona una arquitectura de seguridad específica para un protocolo de comunicación particular. Observamos que una técnica de seguridad utilizada para el entorno general de TI no se puede aplicar inmediatamente a CAN, ya que tiene características únicas, como una carga de datos limitada. Por lo tanto, es necesario diseñar una técnica de seguridad eficiente incluso cuando se usa EVITA-MEDIUM-HSM.

La fragilidad potencial del entorno automotriz se vio analizada por varios grupos en un contexto académico, los cuales han descrito posibles vulnerabilidades en los sistemas automotrices, por ejemplo, (Hilpert, Thoroe, & Schumann, 2011), (Hoppe, Kiltz, & Dittmann, 2011), proporcionan contribuciones valiosas para enmarcar el espacio del problema de privacidad y seguridad del vehículo, especialmente al delinear las limitaciones de seguridad del popular protocolo de bus CAN, así como posibles instrucciones para asegurar los componentes del vehículo.

1.2.6. Adopción de una Perspectiva Teórica.

La perspectiva teórica que se adopta, se basa en el análisis realizado en “Experimental Security Analysis of a Modern Automobile” (Koscher, Czeskis, Roesner, & Kohno, 2010) la cual a través de una investigación en la arquitectura de comunicación de un determinado vehículo, utilizan un ECU de la red para poder alterar su funcionamiento y mediante micro-controlador, realizan los ataques. Este estudio apoyará con el manejo de las diferentes herramientas diagnóstico las cuales capturan tramas y las replican, se difiere porque en este

investigación no se usará micro-controladores sino herramientas de diagnósticos que son capaces de escribir y duplicar tramas.

Se apoyará con el estudio de “Techniques in hacking and simulating a modern automotive controller area network” por (Abbott-McCune & Shay, 2016) en el cual simula una red vehicular con el protocolo CAN y desarrollan sus propias herramientas para poder alterar el funcionamiento de un vehículo simulado. Obteniendo como resultado variaciones en el comportamiento del radio, vidrios y encendido del carro.

También se usara la investigación “Driving with Sharks” por (Hashem Eiza & Ni, 2017) y “In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions” por (Liu, Zhang, & Sun, 2017), las cuales proponen un procedimiento para validar el el funcionamiento correcto de todo vehículo que usa CAN con el obejtivo de conocer si tiene un efecto malicioso, aún más en “Driving with Sharks” ya se nombra al dispostivio telemático como un punto crítico en la seguridad de la información

Por último se tomará el estudio teórico que realiza “I Can Detect You: Using Intrusion Checkers to Resist Malicious Firmware Attacks” (Shila, Geng, & Lovett, 2016) en donde parten de la primicia que el protocolo CAN es totalmente vulnerable a través del estudio del arte de diferentes artículos científicos y proponen una solución teórica basada en los pesos de transmisión de los mensajes en el protocolo sin embargo una solución teórica no es el objetivo de esta investigación pero la base teórica es muy amplia la cual ayudará para entender el protocolo CAN.

1.2.7. Marco Conceptual

El marco conceptual estará guidado mediante los siguientes conceptos

CAN-BUS, El sistema está orientado hacía el mensaje y no al destinatario. La información en la línea es trasmitida en forma de mensajes estructurados en la que una parte del mismo es un identificador que indica la clase de dato que contiene. Todas las unidades de control reciben el mensaje, lo filtran y solo lo emplean las que necesitan dicho dato. Cuando el bus está libre cualquier unidad conectada puede empezar a trasmitir mensaje. (Muñoz Vizhñay, 2013)

GMLAN que significa (Red de área local de motor general) es un protocolo de capa de aplicación y transporte que utiliza CAN para servicios de capa inferior. Los servicios de capa de transporte incluyen la transmisión de mensajes multi-CAN-frame basados en el esquema de mensajes de multi-tramas ISO 15765-2. Fue desarrollado y es usado principalmente por General Motors para comunicación y diagnóstico en el vehículo. (VECTOR, 2017)

ECUs telemáticos, Una central electrónica, también conocida como unidad de control electrónico o ECU (del inglés electronic control unit), es un dispositivo electrónico normalmente conectado a una serie de sensores que le proporcionan información y actuadores que ejecutan sus comandos. Cuenta con software cuya lógica le permite tomar decisiones (operar los actuadores) según la información del entorno proporcionada por los sensores. Los ECUs telemáticos tienen como idea primaria ser conectados a la red vehicular para verificar el posicionamiento, analizar y realizar entrenamiento del vehículo. (Hashem Eiza & Ni, 2017)

Bluetooth es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2.4 GHz. (Edwards, Kashani, & Iyer, 2017)

1.2.8. Hipótesis

Mediante un análisis de vulnerabilidades a la red vehicular GMLAN CAN BUS y a sus interfaces de comunicaciones OBD-II y Bluetooth basados en la norma ISO 26262 e ISO 27002, permitirá a los desarrolladores conocer los riesgos de seguridad y los efectos de estos en los usuarios finales. La adopción de una propuesta de cambio permitirá reducir los riesgos de seguridad.

CAPITULO II

MÉTODO

2.1. Tipo de Estudio

Exploratorio: El presente trabajo de investigación tiene un tipo de investigación exploratorio el cual tiene objetivo identificar adecuadamente las vulnerabilidades de la red vehicular GMLAN CAN BUS y los problemas que generarán dichas vulnerabilidades al ser utilizadas de forma inadecuada. Para esto se realizó un estudio documental sobre las diferentes formas de ataques y métodos que usaron diferentes autores en artículos científicos, en los se encuentran involucrados los dispositivos telemáticos y/o diferentes ECUs.

En el análisis bibliográfico indica que, varios autores realizaron un software malicioso para alterar los mensajes de comunicación en la red vehicular complementando las diferentes experimentaciones de seguridad con un análisis de vulnerabilidad dan como resultado que la red CAN puede ser alterada, como indica en “Techniques in hacking and simulating a modern automotive controller area network” (Abbott-McCune & Shay, 2016). Otros autores logran alterar la APP del dispositivo telemático y con esto enviar tramas no autorizadas a la red vehicular y con ello obtener acceso al vehículo (Woo, Jo, & Hoon, 2015). La investigación desarrolla por (Shila, Geng, & Lovett, 2016) es la que mejor abordada el tema de seguridad en el protocolo CAN, indican teóricamente las falencias y proponen un cambio en el protocolo añadiendo cabeceras de seguridad en los mensajes de comunicación para detectar anomalías, “Evaluamos el rendimiento de seguridad del software *Intrusion Checkers* en el protocolo

CAN, el cual posee varias vulnerabilidades ejecutando un ataque de código complejo en una función de biblioteca del sistema vulnerable.”.

A más de esto se llevó un estudio documental sobre los problemas reportados en la empresa que desarrolla dispositivos telemáticos, en los cuales se evidencia que el dispositivo es susceptible a la alteración de sus interfaces de comunicación, como son Bluetooth, GPS, mediante alteración en sus tramas de comunicación. (Anexo E)

2.2. Modalidad de investigación

La modalidad de investigación que se adopta es de tipo documental, gracias al estado del arte, en el cual se indica las diferentes investigaciones realizadas a las vulnerabilidades de la red vehicular CAN y los análisis documentales de la empresa desarrolladora del dispositivo telemático en donde se evidencian fallas y un posible ataque de un agente externo a la empresa. Cabe resaltar que, en las investigaciones realizadas por los autores tomaron esta misma modalidad de investigación como es el ejemplo de “I Can Detect You: Using Intrusion Checkers to Resist Malicious Firmware Attacks” (Shila, Geng, & Lovett, 2016) y “In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions”.

Por último, se seguirá una investigación de campo, utilizando datos que serán adquiridos en el modelo de automóvil GM TRACKER 2017, los cuales se analizarán para conocer su comportamiento y se aplicaran diferentes metodologías de intrusión para alterar el funcionamiento normal del vehículo.

2.3. Método

El método utilizado es el Inductivo – Deductivo, se parte de un análisis documental, en donde se evidencia las diferentes vulnerabilidades del protocolo CAN, y algunos autores (Hashem Eiza & Ni, 2017) (Woo, Jo, & Hoon, 2015), indican problemas en los dispositivos telemáticos. También se evidencia un análisis de fallas mediante software malicioso inyectado por un agente externo.

A partir del análisis documental que se realizó a la empresa que desarrolla dispositivos telemáticos, se evidencia fallas en la comunicación Bluetooth, CAN, teniendo tramas erróneas y una posible alteración del funcionamiento del dispositivo telemático por un agente externo (sección 1.1.1.1).

Para finales del año 2017, los autores (Liu, Zhang, & Sun, 2017) dan a conocer un resumen de las investigaciones más relevantes acerca de los ataques cibernéticos en la red vehicular. La aparición de redes en el vehículo, que están compuestas por buses de red de área de controlador (CAN) y una gran cantidad de ECU, reduce significativamente la dificultad de diseñar, reparar y reacondicionar vehículos. Si bien debido a las vulnerabilidades intrínsecas de las redes en los vehículos y las interfaces cada vez más ricas para conectar las redes de los vehículos al exterior, los ataques adversos se pueden implementar fácilmente en las redes de los vehículos. Tales ataques causan serias amenazas a la seguridad del automóvil y la privacidad de los conductores. La investigación proporciona una guía detallada, explica los conceptos básicos, presenta las vulnerabilidades de las redes en el vehículo y un resumen de los ataques. Termina proporcionando contramedidas para las redes de los vehículos y señala desafíos y direcciones futuras.

En la tabla 2 se indica la metodología que usaron en las diferentes investigaciones para vehículos con tienen una red CAN, interfaz OBD, y concluye con un resumen del hallazgo en el análisis de vulnerabilidades.

Tabla 2. Ataques a la red CAN, (Liu, Zhang, & Sun, 2017)

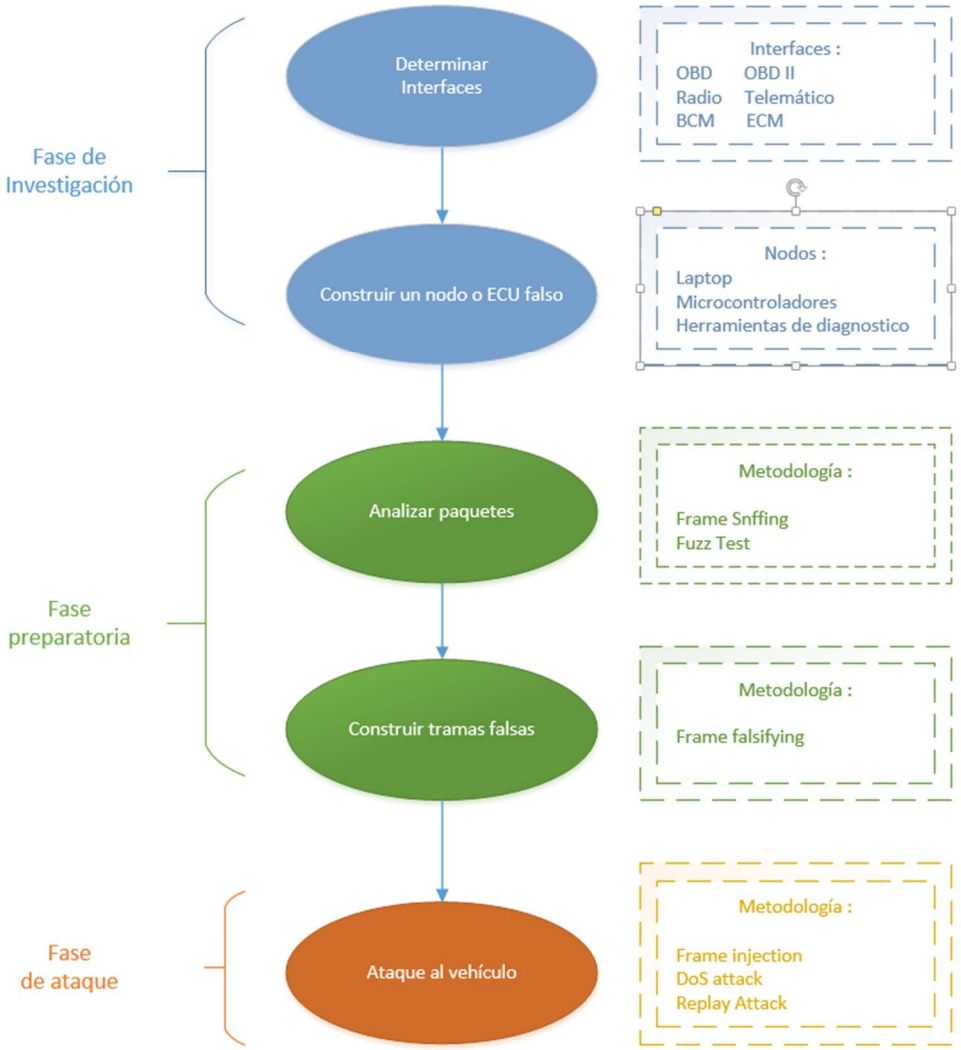
Referencia	Ambiente	Interface	Metodología de Ataque	Contribución
(Hoppe & Dittmann, Sniffing/replay attacks on can buses: A simulated attack on the electric window lift classified using an adapted cert taxonomy, 2007)	Simulado	BUS CAN	Frame sniffing Replay attack	Implement frame sniffing and replay attack; Control window lift.
(Hoppe, Kiltz, & Dittmann, 2010)	Extracción de componentes reales de un carro	CAN BUS OBD port	Frame sniffing Replay attack	Control the window lift, warning lights and air bag systems
(Koscher, Czeskis, Roesner, & Kohno, 2010)	Carro real	OBD port	Frame injection Frame falsifying	Control body control module, radio, engine
(Woo, Jo, & Hoon, 2015)	Real car	OBD port (OBD scan tool)	Frame sniffing Frame injection	Implement wireless attack; using a mlaware App in android

La presente investigación utilizará la metodología mencionada por los diferentes autores para poder realizar un análisis de vulnerabilidades, el procedimiento general se divide en tres fases. La fase de investigación, la cual debe estar basada en un nodo, construyendo un nodo malicioso el cual puede detectar el tráfico en el bus CAN. En la fase preparatoria, de acuerdo con el análisis de tráfico se construye tramas falsas o duplicando tramas que contiene acciones. La última la fase de ataque, los adversarios pueden implementar los tipos de ataques

mediante la inyección de estas tramas. El resumen se indica en la figura 22 la cual es un detalle de la metodología a ser usada.

Esta investigación siguiendo la metodología descrita aportará con un análisis de vulnerabilidades a la red vehicular GMLAN la cual está basada en CAN, mediante su puerto OBD II, se analizará a través de un "fuzz testing" su ECU telemático ONSTAR. Difiere de otros utilizaron ya que ellos utilizaron una red CAN y ECUs como ECM, RADIO o BCM.

Figura 22. Metodología en la investigación, fuente: propia



2.4. Población y Muestra

Población: El parque automotriz del ecuador, según los datos del INEC en 2017, se encuentra en 2.056.213 de automóviles

Muestra: Vehículos de GM que poseen GMLAN CAN BUS

2.5. Selección de Instrumentos de Investigación

Al utilizar un método exploratorio en la presente investigación, se utilizó el análisis documental, por lo que los instrumentos de investigación fueron, artículos científicos publicados en su mayoría en la IEEE, tesis universitarias, documentación de la empresa que desarrolla dispositivos telemáticos.

2.6. Validez y Confiabilidad de los Instrumentos

La validez de los documentos utilizados, así como los artículos científicos y documentación de la empresa del presente trabajo de investigación, son detallados a continuación:

Los artículos científicos utilizados en el presente trabajo de investigación, son documentos científicos que han sido publicados y avalados previamente por entidades, con lo que se tiene una validación por pares. Validación como la Librería Digital IEEEXplore, el motor de búsqueda académico de Bielefeld (BASE), Universidad de CHALMERS, Universidad Austral De Chile, Universidad de Tecnología de Auckland, Universidad de Korea (South Korea), Universidad Edith Cowan (Australia).

Las tesis utilizadas en el presente trabajo de investigación, han sido publicadas y avaladas por universidades reconocidas como son: Universidad Nacional del Centro de la

Provincia de Buenos Aires (Argentina) la Universidad Politécnica de Madrid (España) y la Universidad De Las Fuerzas Armadas (ESPE).

Los artículos de investigación han sido aprobados por revistas reconocidas. Tal es el caso, del artículo de la Universidad Nacional de Singapur, publicado en la Revista Asiática de Asuntos Públicos (Asian Journal of Public Affairs), el estudio realizado en la Universidad de Korea, el cual fue publicado en la revista Cybertrust y los resultados publicados por la revista IEEE “DRIVING WITH SHARKS”.

2.7. Procesamiento de Datos

El análisis llevado a cabo en el presente trabajo de investigación se indicó a través de un estudio documental, en donde indican varias falencias en el protocolo CAN estando expuestos a diferentes ataques para ser manipulados de manera lógica un obtener un acceso no autorizado al vehículo y un daño en el funcionamiento, como se indicó en la sección 1.1.1.1, 1.2.5 y 2.11.1.2

En lo referente a las vulnerabilidades lógicas, el estudio realizado “Evaluation of Software Vulnerabilities in Vehicle Electronic Control Units” (Edwards, Kashani, & Iyer, 2017) indica que los ECUs han sido el foco de muchos investigadores de seguridad y han demostrado la capacidad de afectar la operación determinista de los sistemas ciberfísicos, en los cuales se han descubierto fallas en el diseño del software que tienen impactos directos a la seguridad funcional. Con el rápido aumento en la conectividad de datos dentro de un automóvil moderno ha ampliado la superficie de ataque, permitiendo a los adversarios el acceso remoto a las redes de vehículos y al software del sistema de control.

El estudio de “A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN” (Woo, Jo, & Hoon, 2015) enseña que desafortunadamente los problemas de seguridad no se han tratado adecuadamente en CAN y la apariencia del entorno del automóvil conectado a redes externas (por ejemplo, redes móviles 3G / 4G), permite a un adversario realizar un ataque inalámbrico de largo alcance utilizando vulnerabilidades de CAN, muestra que un ataque inalámbrico de largo alcance es físicamente posible utilizando un vehículo real y una aplicación de teléfono inteligente malicioso se encuentran conectados. También proponen un protocolo de seguridad para CAN como contramedida diseñada de acuerdo con las especificaciones de CAN actuales.

Adicional a esto en el artículo “Intrusion Prevention System of Automotive network CAN bus” (Shay & Abbott-McCune, 2017) demuestra que la red CAN pueden verse comprometidas de una manera que podría poner en peligro a los ocupantes del vehículo. Un exploit llevó a un retiro de automóviles costoso que afectó a más de un millón de vehículos, permite a los delincuentes robar coches sin físicamente penetrarlos. Si bien aún no se han producido muertes, los hackers podrían desencadenar un accidente que involucre lesiones graves o incluso la muerte. El bus CAN conecta varias unidades de control electrónico, cada ECU introduce vectores de ataque en la red automotriz general.

Sobre del análisis de vulnerabilidades que se desea realizar se toma como base la investigación realizada por “Experimental Security Analysis of a Modern Automobile”, (Koscher, Czeskis, Roesner, & Kohno, 2010) , demuestra que un atacante puede infiltrarse virtualmente en cualquier ECU. Se realizó una gama de experimentos, tanto en laboratorio como en pruebas en carretera, demostrando la capacidad de controlar una amplia gama de funciones automotrices, incluyendo la desactivación de los frenos, el frenado selectivo de

ruedas individuales a pedido, la detención del motor y pronto descubrieron que es posible eludir protecciones de seguridad de red rudimentarias dentro del automóvil.

Y por último se toma el estudio de “In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions” (Liu, Zhang, & Sun, 2017), en el cual demuestra que el vehículo está compuesto por una red CAN y una gran cantidad de ECUs, aseguran que existen vulnerabilidades en estas, demostrando una serie de ataques que son una amenaza a la seguridad del automóvil y la privacidad de los conductores, proporciona una guía detallada, explicando conceptos básicos, presentando las vulnerabilidades de las redes en el vehículo y un resumen de las metodologías de ataque. Finalizando con las contramedidas para redes de vehículos y señalando los desafíos y direcciones futuras.

Por todo lo anteriormente expuesto, se cuentan con todos los elementos necesarios para proceder con el plan de investigación.

CAPÍTULO III

RESULTADOS

3.1. Levantamiento de la Información

Para efectos de la investigación se utiliza un modelo de vehículo Chevrolet Tracker 2017, un todo terreno compacto abreviado con las siglas SUV. El motor es un 1.8 litros de 140hp, 129 lb-pie, cuenta con una radio marca BYOM 2, encendido automático, BUS GMLAN, puerto OBD II y sistema de rastreo satelital que incluye el servicio por un año gratis al adquirir el automóvil. El sistema de rastreo satelital tiene un sistema Bluetooth 4.0 el cual es usado como manos libres, llamadas telefónicas y acceso a los contactos de un teléfono móvil; también posee un contrato con una operadora móvil el cual da acceso GPRS y SMS para el servicio de rastreo y diagnóstico vehicular. En la figura 23 se indica el vehículo

Figura 23. Vehículo Chevrolet Tracker usado en la investigación, fuente: propia

Para el análisis de la red del vehículo se utilizará una herramienta de diagnóstico vehicular, ésta se conforma mediante un Hardware y Software. El Hardware consta de un cable de conexión OBD y un puerto de conexión USB para la computadora, y/o una conexión Bluetooth, el nombre de la herramienta es NeoVi Fire 2 y se observa en la figura 24.

Figura 24. Nevo Vi, fuente: www.intrepid.com

El software es licenciado y permite la traducción de las tramas CAN de un formato hexadecimal a ASCII, el nombre del programa que se utiliza es VehicleSpy, éste debe ser configurado con una base de datos para la interpretación de las tramas CAN, en este caso los modelos GM 2017 tienen una base de datos cuya versión es V7.4.5. Se configura el software y el hardware de la herramienta de diagnóstico como se indica en la figura 25 y figura 26

Figura 25. Configuración NEOVI, fuente: propia

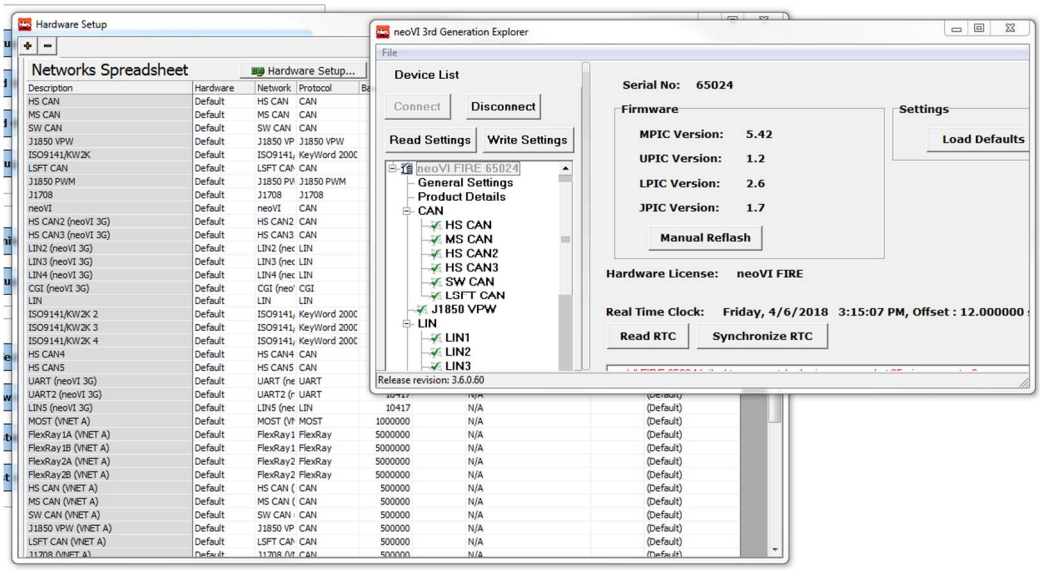
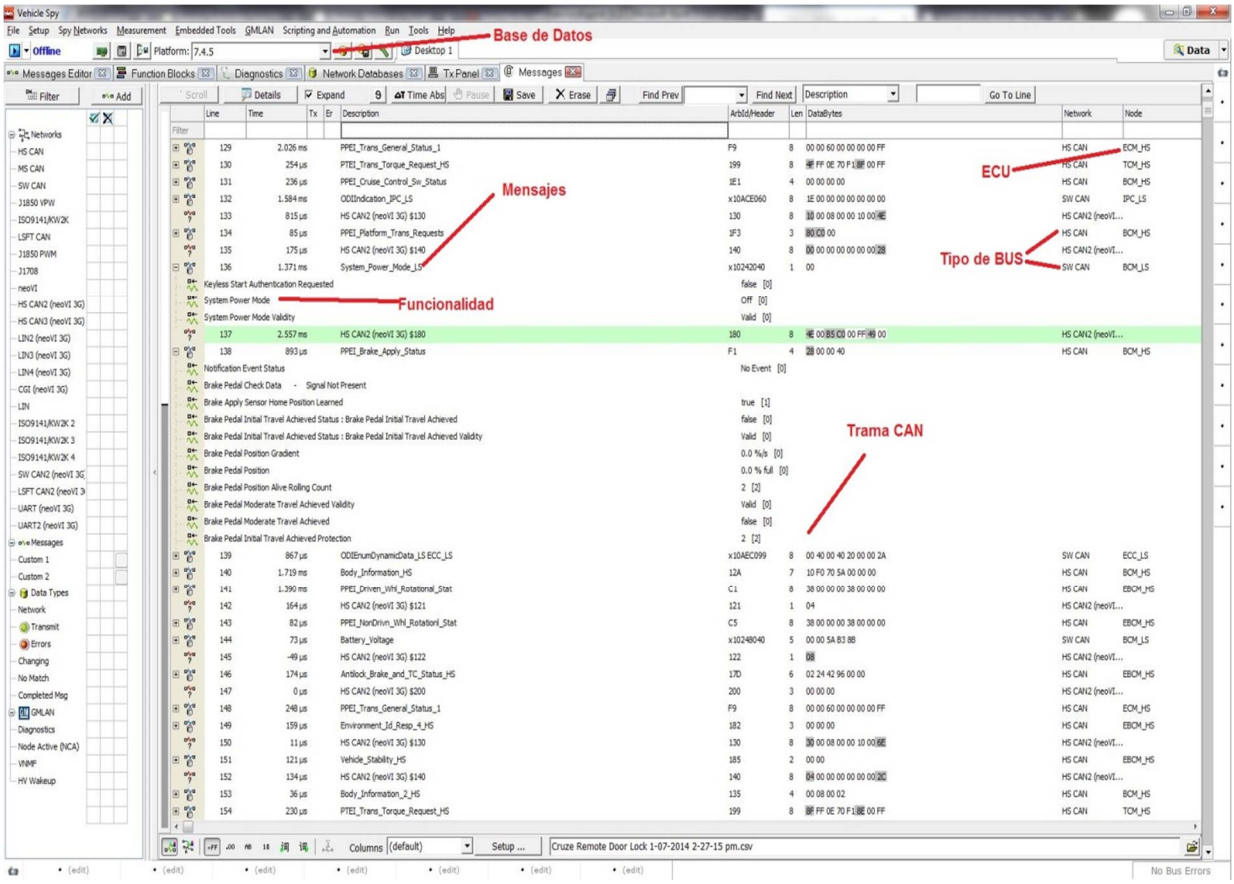


Figura 26. “Vehicle Spy”, software para interpretación de datos CAN, fuente: propia

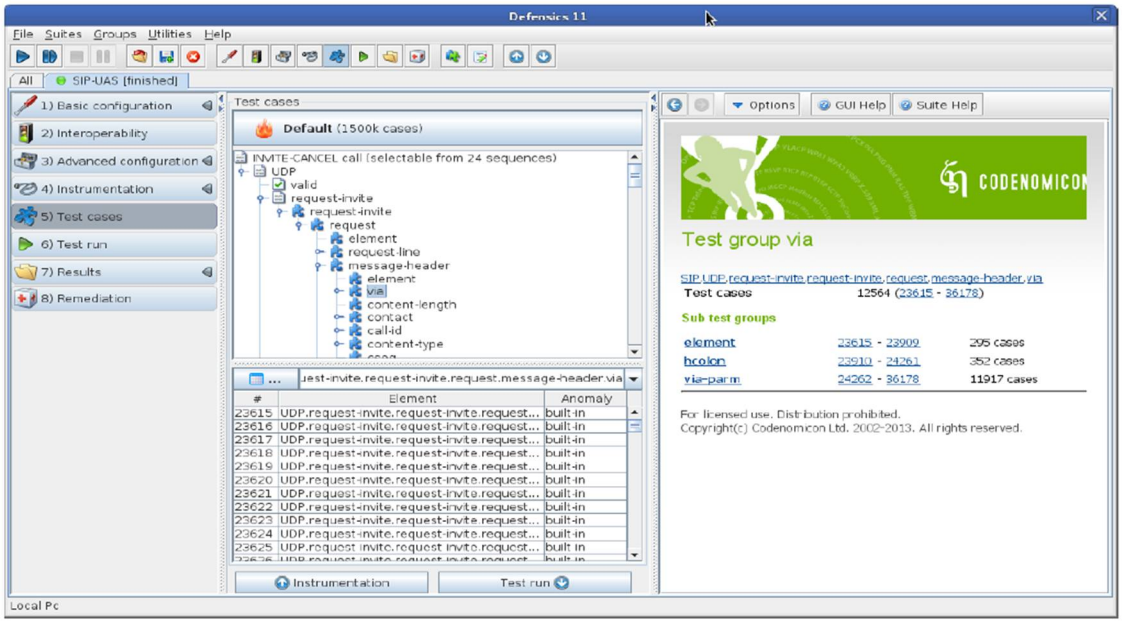


Para realizar el análisis a la interfaz Bluetooth del dispositivo telemático, se utilizará un software de pruebas automáticas el cual envía datos al azar, inválidos o erróneos como entrada del dispositivo telemático, a ese tipo de prueba se la conoce como “fuzz testing” o “*fuzzer*”. El programa que se utilizará para realizar el “*fuzz testing*” es “Codenomicon Defensics” de la compañía Codenomicon, este software permite realizar pruebas sobre distinto protocolos de comunicación CAN, L2CAP, HTTP, etc, su plataforma es basada en java, la dificultad que se encuentra en esta plataforma es su instalación ya que debe ser con un “*dongle*” Bluetooth autorizado por el programa y 2 tipos licencias, la primera que se utiliza para ejecutar el software de modo “*offline”* permitiendo una ejecución de hasta 10 pruebas y la segunda licencia en modo “*online”*. El *dongle* Bluetooth que se usa es versión 4.0, el cual se conecta a la laptop ver en la figura 27.

Figura 27. Dongle Bluetooth, fuente: Propia

Al tener el *dongle* conectado y la licencia correcta el programa permite seleccionar que tipo de pruebas se desea realizar como se puede observar en la figura 28.

Figura 28.Tipos de pruebas, fuente: propia



En síntesis para obtener información acerca de la red vehicular se utilizará las siguientes herramientas

- Vehículo GM 2017, modelo Tracker
- Sniffer de tramas de CAN, NeoVi Fire 2
- Software para analizar y alterar las tramas CAN, VehicleSpy con su base de datos V7.4.5
- Analizador de tramas Bluetooth, “fuzzer Codenomicon”
- Laptop y celular

3.1.1. Descripción de los ataques realizados

Para iniciar el proceso de ataque en la red vehicular GMLAN se usará el método indicado en la sección 2.3 en la figura 22, de acuerdo a los siguientes pasos:

- Selección de la interfaz, es importante indicar la interfaz por la cual se debe acceder a la red GMLAN, para este caso en particular se lo realizará a través del puerto OBD II y la interfaz Bluetooth del dispositivo telemático.
- La herramienta de diagnóstico vehicular adecuada para simular y analizar los nodos de la red GMLAN, es NeoVi. Esta herramienta comprende de un software y un hardware con lo cual permite la simulación de ECUs o nodos en GMLAN, la adquisición de datos, edición, calibración y monitoreo del BUS GMLAN.
- El tipo de ataque estará basado en función de los datos adquiridos a través de la herramienta de diagnóstico vehicular producto de un “sniffing”, con ello se podrá determinar el escenario y el tipo de ataque a ejecutarse como “frame falsifying” y envío de mensajes de texto para la apertura de puertas, control de pito y luces.
- Las consecuencias de los ataques serán conocer los tipos mensajes que circulan por la red BUS GMLAN, perturbar el funcionamiento normal del vehículo y las falencias en seguridad de la red BUS GMLAN.

3.1.1.1. Primer Ataque

El primer ataque se realiza mediante “Frame Sniffing”, tiene como finalidad encontrar que ECUs se encuentran conectados y que tramas se intercambian en el BUS, el resumen se detalla en la *tabla 3*

Tabla 3. *Primera Vulnerabilidad, fuente: propia*

Acción	Detalle
Ataque	Frame Sniffing
Herramientas Usadas	Hardware NeoVi Fire Laptop Software VehicleSpy
Interfaz	GMLAN Puerto OBDII
Procedimiento	Conectar el Neovi Fire en el puerto OBD II. En el Software Vehcile Spy, configurar el tipo de BUS que se desea reconocer (GMLAN) y la base de datos 7.4.5 para la interpretación de las tramas. Colocar en modo escucha de tramas, "run" en el programa VehicleSpy.
Resultado	Las tramas de los distintos ECUs viajan sin ninguna encriptación, dando a conocer que los ECUs conectados en el vehículo son: ECM, BCM, IPC, ONSTAR, RADIOHEAD Al conocer las tramas se puede verificar que acciones se están ejecutando a tiempo real en el carro ejemplo: Carro Encendido, Freno activado, etc

Mediante la herramienta de diagnóstico vehicular se logra realizar “sniffing” y se comprueba que los ECUs instalados en el vehículo Tracker son ECM, BCM, IPC, ONSTAR, RADIOHEAD, entre otros, los cuales se detallan en la figura 29. Estos ECUs contienen una cabecera de inicio llamada “source id”, como se puede observar en la figura 30.

Figura 29. ECUs en un vehículo GM. Fuente: (VECTOR, 2017)

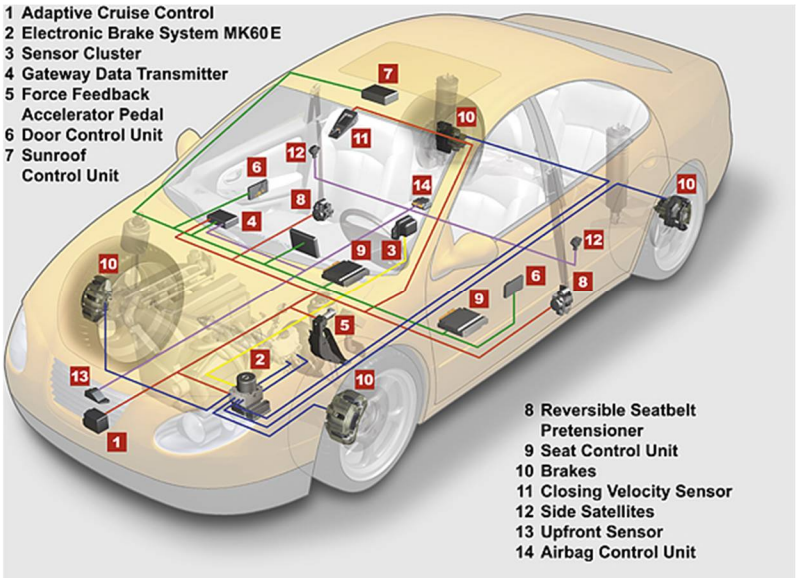
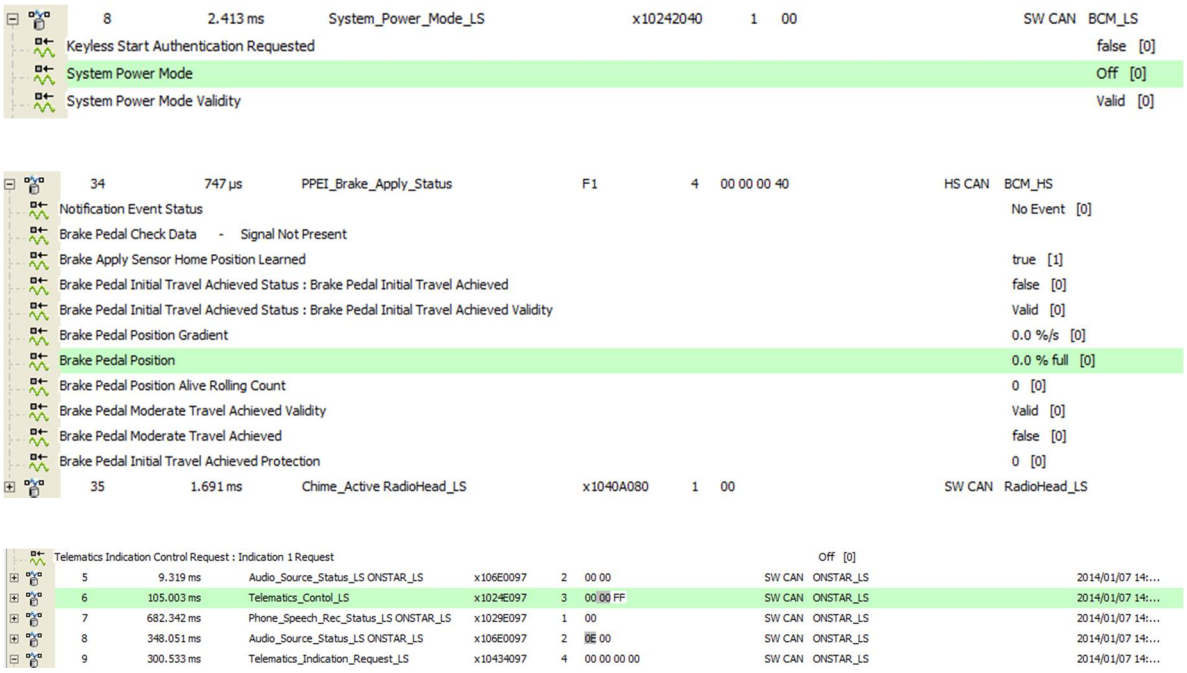


Figura 30. Resumen de ECUs, ArbID. Fuente: Propia

Descrición	Modulo	GMLAN BUS	Source Id
Body Control Module	BCM	LS, HS	$40
Engine Control Module	ECM	HS	$11
Instrument Panel Cluster	IPC	LS, HS	$60
ONSTAR	ONSTAR	HS, LS	$97
Radio	RadioHead	LS	$80

El BCM es Gateway entre las dos redes HS (high speed) y LS (low speed) de GMLAN, éste comanda las acciones del vehículo y es el “cerebro” del carro, el ECM realiza las funciones para frenar y acelerar el vehículo, y por último ONSTAR es quien realiza las funciones de entretenimiento, diagnostico remoto y rastreo satelital. Como se puede observar en la figura 31, el BCM indica que el carro se encuentra apagado o con ignición en OFF, la trama es 0x10242040. El ECM indica que no está acelerado el vehículo y ONSTAR indica que el control remoto del carro fue aplastado para abrir puertas.

Figura 31.Datos de la trama GMLAN, fuente: Propia



3.1.1.2. Segundo Ataque

El propósito del segundo ataque que se realiza es perturbar el funcionamiento normal del vehículo, alterando las tramas que envía normalmente los ECUs, este ataque se lo conoce como "*frame falsifying*" y consta de dos procedimientos. El primero encenderá el vehículo sin una llave de acceso y se detalla en la tabla 4.

Tabla 4. Vulnerabilidad de alteración de tramas, fuente: propia

Acción	**Detalle**
Ataque	Frame Falsifying
Herramientas Usadas	Hardware NeoVi Fire Laptop Software VehicleSpy
Interfaz	GMLAN Puerto OBDII

Procedimiento	Conectar el Neovi Fire en el puerto OBD II. En el software VehicleSpy, en la opción "Edición de Mensajes", crear un nuevo mensaje, será similar al que se logró interceptar en el ataque uno. El primer mensaje a alterar es "system_Power_Mode", y se colocará en modo RUN. Se envía el mensaje con la opción "transmit" del software.
Resultado	Cuando se envía el mensaje "system_Power_Mode" en modo RUN, los dispositivos asumen que el vehículo está encendido y el carro se coloca en modo de encendido.

El encendido del vehículo tiene asociado la trama del mensaje llamado “system_Power_Mode” del BCM, se inyecta una trama falsa y se indica a todos los ECU que el vehículo se encenderá y todos los dispositivos y el motor del carro se pondrán en modo “ON” (ver figura 33).

Figura 32.Trama carro en ON, fuente: propia

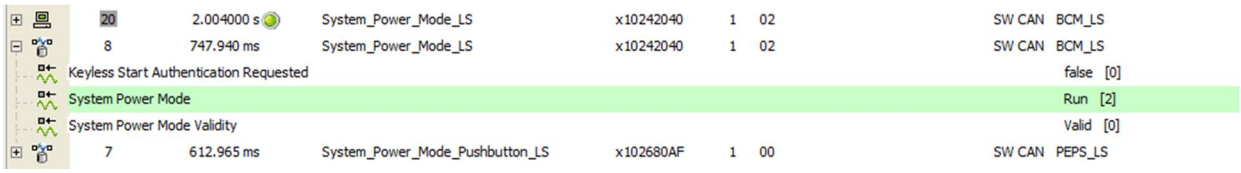
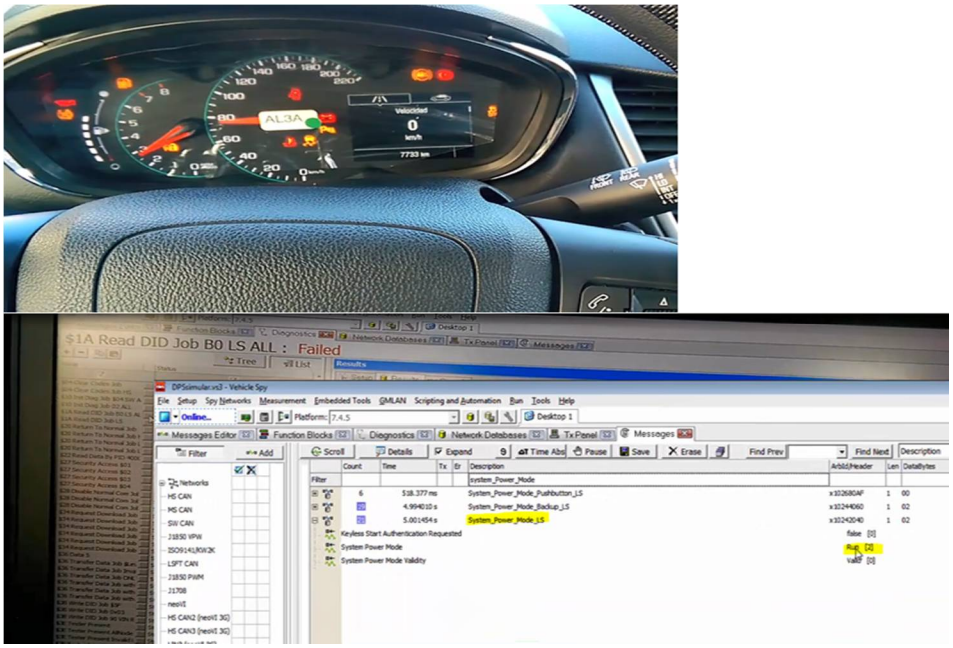


Figura 33. Encendido del vehículo. Fuente: propia



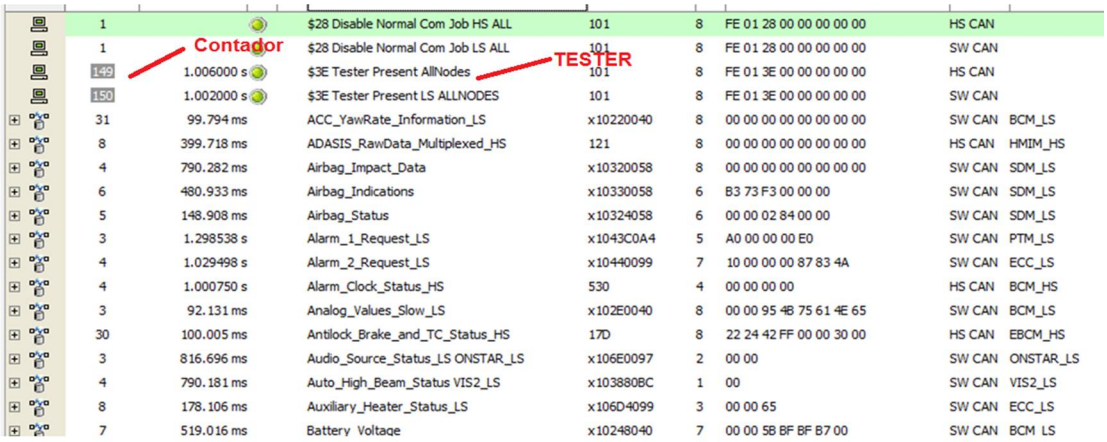
El segundo procedimiento es desactivar todas las funcionalidades del vehículo, se lo realizara falsificando la trama “TesterPresent”, esto se detalla en la siguiente tabla

Tabla 5. Segundo procedimiento, Frame Fasifying, fuente: propia

Acción	Detalle
Ataque	Frame Falsifying
Herramientas Usadas	Hardware NeoVi Fire Laptop Software VehicleSpy
Interfaz	GMLAN Puerto OBDII
Procedimiento	Conectar el Neovi Fire en el puerto OBD II. En el software VehicleSpy, en la opción "Edición de Mensajes", crear un nuevo mensaje, será similar al que se logró interceptar en el ataque uno. Segundo mensaje para ser alterado es "TesterPresent", y se colocará en modo RUN. Se envía el mensaje con la opción "transmit" del software.
Resultado	Cuando se envía el mensaje " TesterPresent ", los ECUS en el vehículo se desactivan y no realizan ninguna acción

El segundo modo de alterar el funcionamiento GMLAN, es falsificando un ECU llamado TESTER, éste indica que un sistema de diagnóstico se encuentra conectado a través del puerto OBD-II y puede realizar diferentes funciones como solicitar información de los estados a los ECUs, como posicionamiento GPS, estado del motor, identificadores de serie, problemas, etc. Se envía una trama falsa indicando que el "Tester" se encuentra conectado y desea desactivar todos los ECUs para realizar un mantenimiento al vehículo. Como se puede observar en la siguiente figura se envía la trama falsa "*tester present*" y el contador de tramas GMLAN no avanza sino solo los mensajes del TESTER, es decir todos los ECUs se encuentran apagados y el vehículo se inmoviliza.

Figura 34.Trama para inmovilizar el vehículo, servicio de diagnóstico número $28, fuente propia



3.1.1.3. Tercer Ataque

La intención de este ataque es desarmar y abrir las puertas del vehículo con un mensaje de texto como se detalla en la tabla 6. Para esto se debe enviar e inyectar una trama a GMLAN y se consigue mediante el dispositivo telemático.

Tabla 6. Vulnerabilidad a través de SMS, fuente: propia

Acción	Detalle
Ataque	Frame falsifying
Herramientas Usadas	Hardware NeoVi Fire Laptop Software VehicleSpy Teléfono móvil con acceso a SMS
Interfaz	GMLAN Puerto OBDII Red Móvil del dispositivo Telemático
Procedimiento	El procedimiento consta de dos parte Primera Parte, captura de información: Se configura el mensaje $24D$1A$58, en el software VehicleSpy en la opción de "Edición de Mensajes" Al enviar éste mensaje, el ECU telemático responde con su número celular "0958692582" Se configura otro mensaje "$24D$1A$08 en el software, y la respuesta que se tiene por parte del ECU telemático es el ID del vehículo **2372016.** Segunda Parte, envío de SMS: Con la información obtenida de Númer Celular e ID del vehículo se crea y se envía un SMS, con la información de apertura de puertas $PEO0L**02372016**;0101LI1¥*1f
Resultado	Al enviar el SMS con los datos indicados, las puertas se abren y el vehículo se encuentra en un estado de desarmado para que cualquier intruso ingrese.

Como se indicó en el marco teórico, todos los ECUs cuentan con servicios de diagnóstico vehicular, en los cuales se puede conocer su configuración, errores y reconfigurar su funcionamiento, se usará el servicio $1A para conocer información del dispositivo telemático.

Mediante "*sniffing*" se conoce que en la red GMLAN existe un ECU ONSTAR, y se puede enviar una trama falsa simulando un ECU TESTER. Esto se realiza enviando una petición de servicio de diagnóstico $1A como se indica en la figura 35. La trama es ***$24D$1A$58*** y se envía al dispositivo telemático y tiene como intención solicitar el número celular asociado al vehículo.

El dispositivo telemático recibe la información y contesta con una trama de respuesta (ver figura 36), la cual está en hexadecimal 0x30393538363932353832, cuando se la transforma en ASCII se obtiene el número celular el cual es 0958692582.

Figura 35. Configuración para acceso a datos, fuente: propia

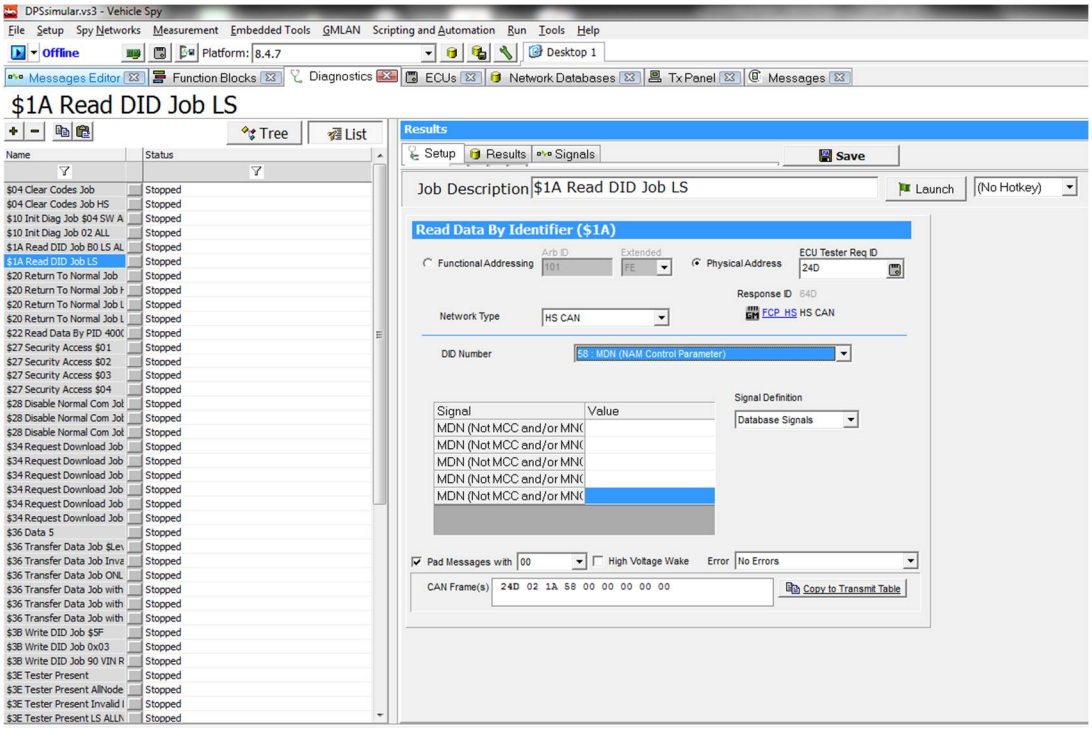
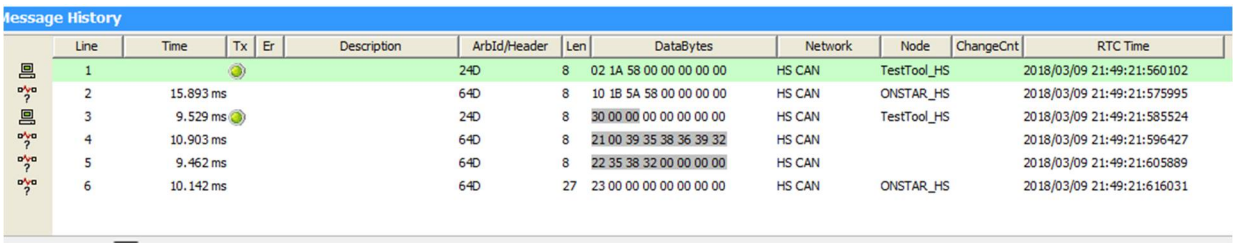
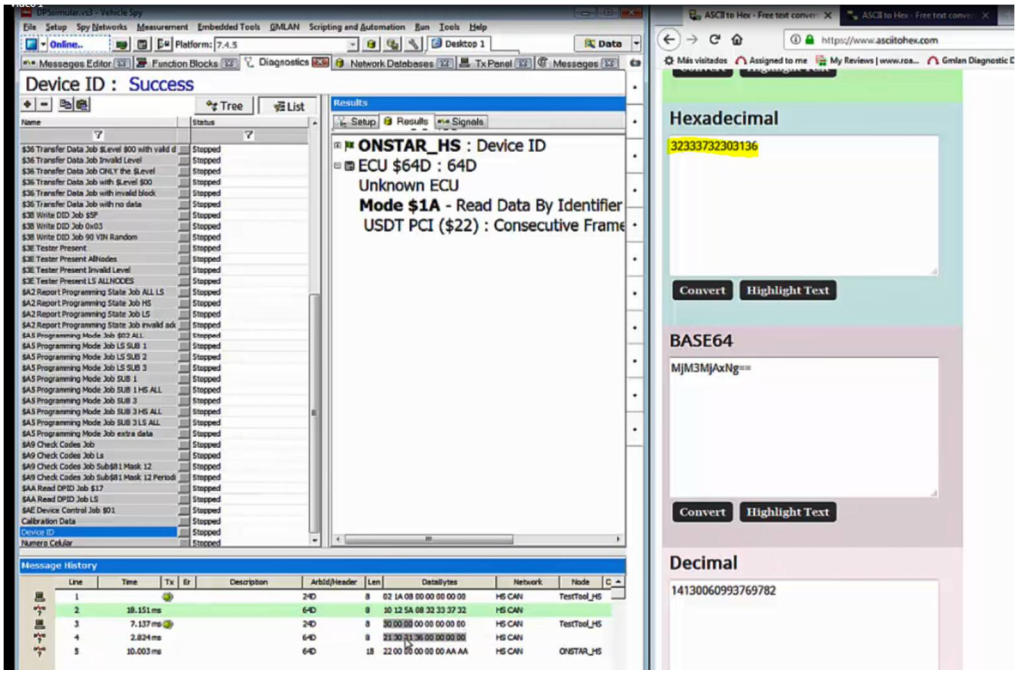


Figura 36.Número celular del vehículo, fuente: Propia



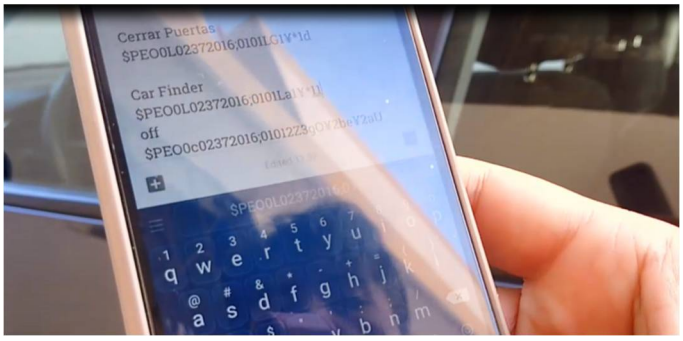
Para conocer el ID del vehículo se envía de la misma manera una trama solicitando el ID del vehículo "***$24D$1A$08***" y el dispositivo telemático contesta que es 2372016.

Figura 37. Identificativo del vehículo. Fuente: propia



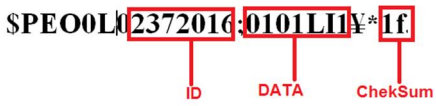
Con esta información es posible formar mensajes de texto O2V que el dispositivo telemático recibe mediante la red móvil para ejecutar funciones, como es "*car finder*" "open doors". En la figura 38 se muestra los mensajes de texto listo para ser enviados.

Figura 38. Comandos de apertura de puertas un "car finder". Fuente: propia



En la figura 39 se indica que el celular asociado es 0958692582, y el ID del vehículo es el 2372016, y la trama por mensaje de texto es **$PEO0L02372016;0101LI1¥*1f.** Cuando Se envía esta información las puertas del vehículo se abren. A este ataque se lo conoce como "frame injection"

Figura 39. Mensaje de apertura de puertas, fuente propia



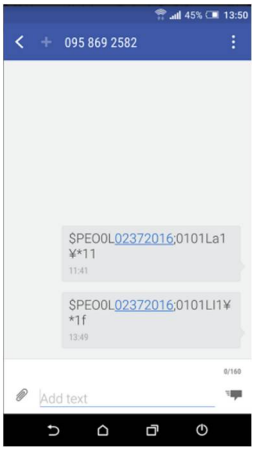
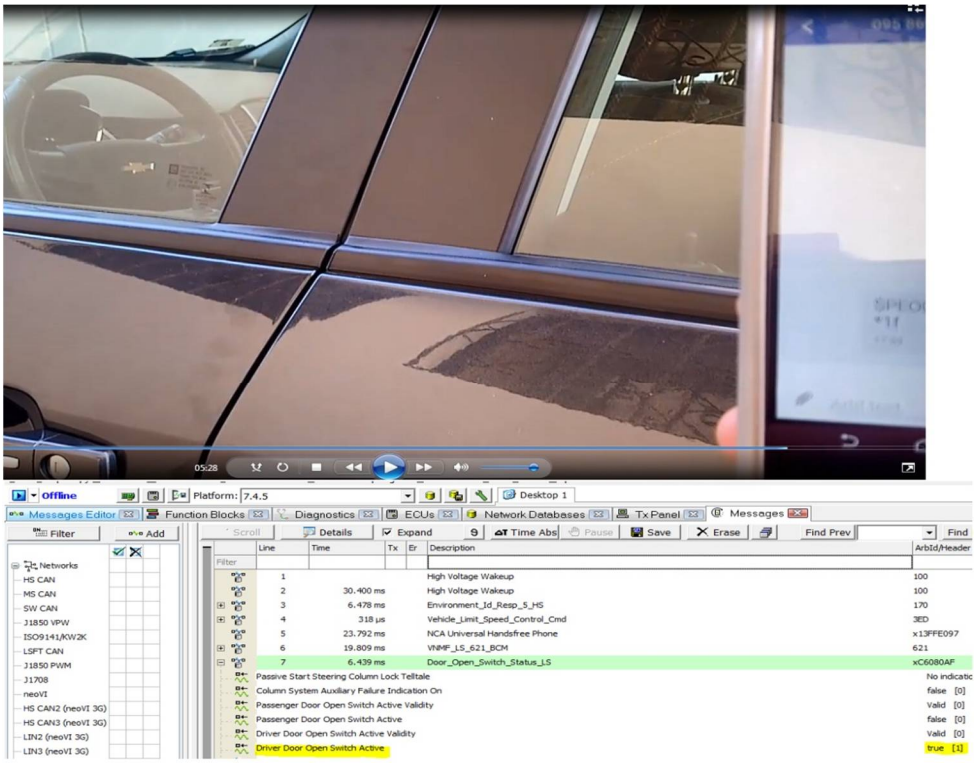


Figura 40. Apertura de puertas, fuente: propia



3.1.2. Fuzz testing en Bluetooth

El objetivo de esta prueba es encontrar las vulnerabilidades y problemas que tiene el protocolo de comunicaciones Bluetooth en el dispositivo telemático enviando datos erróneos o al azar en toda la pila del protocolo, se monitorea el dispositivo telemático en busca de problemas tales como bloqueos o fallas. Para esto se utilizan los “fuzzers” los cuales son programas que toman entradas estructuradas, en un formato de archivo o protocolo y distingue la entrada válida de la no válida. El “fuzzer” genera entradas semi-válidas que son "lo suficientemente válidas" porque el protocolo no las rechaza directamente, pero crea comportamientos inesperados más profundos en el programa y son "lo suficientemente inválidas" para exponer casos de esquina que no se han tratado adecuadamente.

El “fuzzer” a ser utilizado se llama “Tester de Codenomicon”, esta herramienta configurada adecuadamente y seleccionando el tipo de pruebas y la severidad que desea tener (ver figura 41), ejecuta un set de pruebas para analizar el comportamiento de la pila de Bluetooth en el dispositivo telemático. El resumen de la ejecución de la prueba se detalla en la tabla 7.

Figura 41.Escalas de anormalidad fuzz testing, fuente: propia

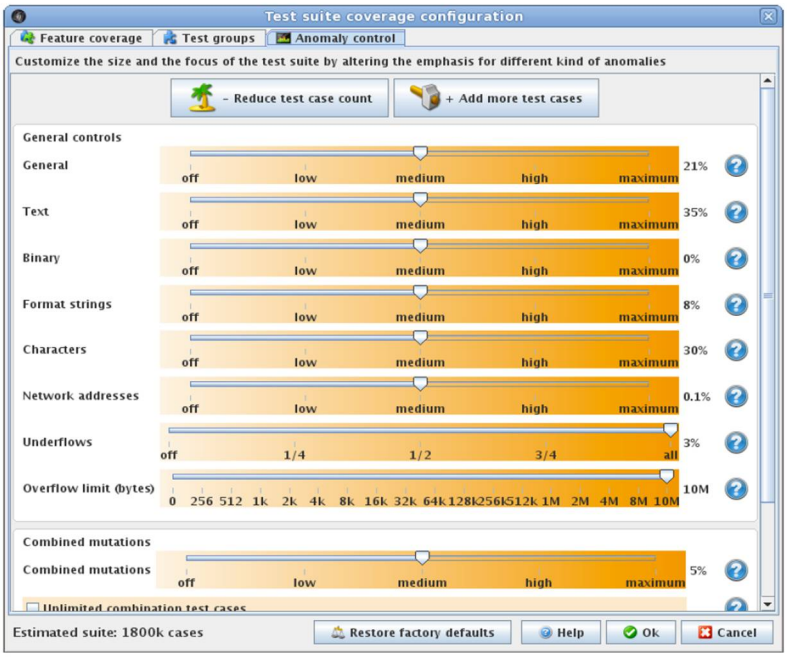
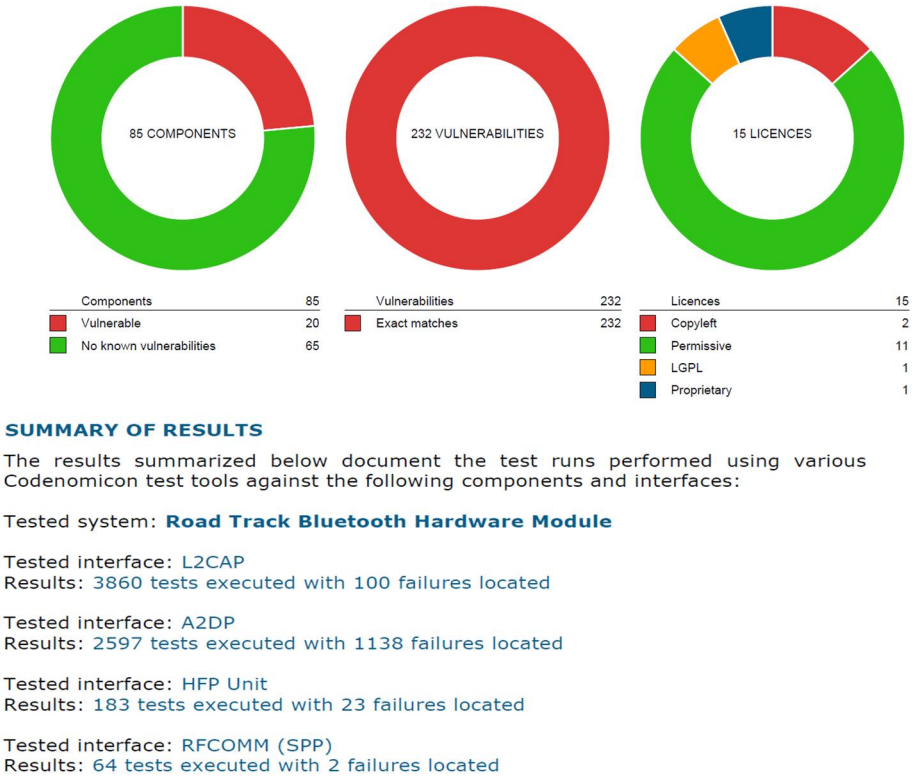


Tabla 7. Análisis de vulnerabilidades en Bluetooth, fuente propia

Acción	Detalle
Ataque	Fuzzer
Herramientas Usadas	Hardware NeoVi Fire Laptop Software VehicleSpy Software Codenomicon Bluetooth
Interfaz	Bluetooth Dispositivo Telemático
Procedimiento	Conectar el dongle Bluetooth en la laptop Emparejar dongle Bluetooth con Bluetooth del dispositivo telemático Configurar la severidad de las pruebas Configurar que tipos de pruebas y en que capas de Bluetooth se desea realizar las pruebas Ejecutar las pruebas
Resultado	Al terminar las pruebas, se encontraron 232 fallos en la interfaz Bluetooth del dispositivo telemático Una de estas pruebas es la más crítica, ya que el dispositivo telemático deja de funcionar. El software envío muchas tramas erróneas en la prueba L2CAP y el dispositivo no pudo procesar quedando inhibido. El vehículo al no recibir ninguna señal en el BUS del dispositivo telemático, piensa que este fue sustraído o robado entrando en un modo de inmovilización.

Al iniciar la prueba "*fuzz*", el programa corre todas las pruebas seleccionadas, esto puede tomar desde minutos hasta días, dependiendo de la profundidad de cada caso y el tipo de tramas que se desea afectar. Para la presente investigación se realizó una prueba con anormalidad media y se ejecutó pruebas para los protocolos L2CAP, AD2DP, HFP y RFCOMM. En un total de 6704 pruebas se encontraron 1263 fallas en la comunicación de los diferentes protocolos.

Figura 42. Resultados de pruebas en Bluetooth, fuente: propia



Para todas las pruebas el dispositivo telemático se pudo recuperar y su funcionamiento no alteró el comportamiento en el BUS GMLAN, excepto en una prueba que fue para L2CAP. Al momento de emparejar el *dongle* Bluetooth con el dispositivo telemático, la capa L2CAP la cual lleva la información para comunicar con la capa superior RFCOMM, envió datos e inyectó algunas tramas erróneas y el dispositivo telemático dejó de funcionar, se quedó en un

bucle infinito del código de programa y deja enviar datos al BUS GMLAN. Al no enviar ninguna información al BUS, todos los dispositivos piensan que fue “extraído” o “robado”, colocando al vehículo en un estado de inmovilización por robo como se puede observar en el figura 43.

Figura 43. Trama de inmovilización GMLAN, fuente propia

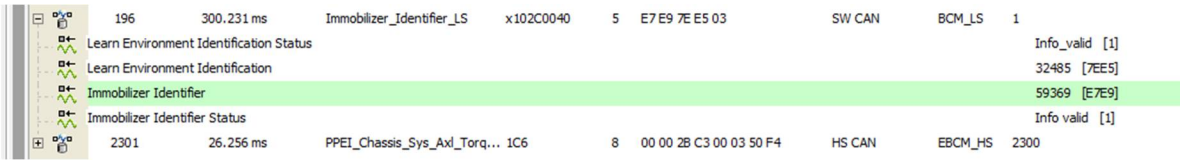


Figura 44. Prueba de L2CAP, fuente: propia

test-case-	test-group	index	status	input-eve	input-octe	output-ev	output-oc	diagnosis	time	cvss	instrumer	log-line	hash
35:40.9	l2cap.connect-disconnect.connection-request.ACLData.Identifier	1436				2	24	fail	38.707	9.3	7	28919	ab76d84b6e38e45d
36:20.7	l2cap.connect-disconnect.connection-request.ACLData.Identifier	1455				2	24	fail	38.729	9.3	7	29542	355d92e54be679a5
37:05.6	l2cap.connect-disconnect.connection-request.ACLData.Source-CID	1557				2	24	fail	46.711	9.3	8	32330	79120caedbd9f79b
37:53.5	l2cap.connect-disconnect.connection-request.ACLData.Source-CID	1577				2	24	fail	40.045	9.3	7	32986	8dce4852d9c10ffc

Es decir el vehículo se quedó inmovilizado por un problema en la trama L2CAP de Bluetooth dando a conocer una vulnerabilidad en el dispositivo telemático el cual afecta al usuario final.

Para finalizar la sección de levantamiento de información se realizó un resumen en un video de los problemas encontrados en la red vehicular, el cual se adjunta como anexo de la presente investigación.

3.2. Presentación y análisis de resultados

Esta sección del trabajo de investigación se centra en la presentación y análisis de los datos obtenidos en la sección 3.1. Los resultados obtenidos se detallan en la siguiente tabla donde se especifica el ambiente de pruebas, la interfaz utilizada, el tipo de ataque realizado y los resultados obtenidos que pueden ser explotados en un entorno real

Tabla 8. Vulnerabilidades encontradas, fuente: propia

No. Vulnerabilidad	Ambiente	Interfaz	Metodología de ataques	Resultado
1	Vehículo Tracker	OBD-II GMLAN CAN BUS	Frame sniffing	Acceso a las tramas de datos de los ECUS
2	Vehículo Tracker	GMLAN CAN BUS OBD-II	Frame falsifying	Simulación de ECUs conectados al BUS GMLAN Control de encendido del carro
3	Vehículo Tracker	OBD-II GMLAN CAN BUS	Frame falsifying	Inmovilización vehicular Alteración de funcionamiento del panel
4	Vehículo Tracker	OBD-II	Frame falsifying	Acceso a la información de ONSTAR (ID y número celular) Apertura remota de puertas
5	Vehículo Tracker Laboratorio	Bluetooth / ONSTAR	Fuzz Testing	Daño al equipo telemático mediante su interfaz de Bluetooth, inmovilizando al vehículo

Para realiza el análisis y determinar el riesgo de cada una de las vulnerabilidades, en el sector automotriz se utiliza la norma ISO 26262:2011 como se indicó en el punto 1.1.6 y en 1.2.4.1 toda empresa que se dedica al sector automotriz debe estar basado en esta norma, la cual tiene como objetivo garantizar la seguridad funcional de un sistema eléctrico/electrónico en un vehículo motor

- Cubre los aspectos de seguridad funcional de todo el proceso de desarrollo (incluyendo actividades como la especificación de requisitos, diseño, implementación, integración, verificación, validación, y configuración).
- Proporciona un enfoque específico del automóvil basado en el riesgo para la determinación de las clases de riesgo (Automotive Safety Integrity Level, ASIL).

- Utiliza ASIL para especificar los requisitos de seguridad necesarios del elemento para el logro de un riesgo residual aceptable.
- Proporciona requisitos de las medidas de validación y confirmación para garantizar que se está alcanzando un nivel de seguridad suficiente y aceptable.

ISO 26262 está basada en riesgo, donde el riesgo se evalúa cualitativamente y se definen las medidas de seguridad para evitar o controlar fallos sistemáticos y para detectar o controlar los fallos de hardware aleatorios, o mitigar sus efectos. Esta evaluación se realiza mediante ASIL. Para ISO26262 un riesgo se basa en, Severidad por Frecuencia y por Control estas 3 pautas dan el concepto de ASIL. Entonces se denota que ASIL está definida por cuatro niveles, ASIL A, ASIL B, ASIL C y ASIL D, en donde se denota el nivel más bajo de inseguridad es ASIL A y el nivel más alto es ASIL D, en la figura 45 se indica cómo se conforma ASIL y un diagrama de calor en donde se indica el nivel de riesgo para cada nivel.

Figura 45. Cálculo ASIL, fuente: (BS ISO 26262, 2011)

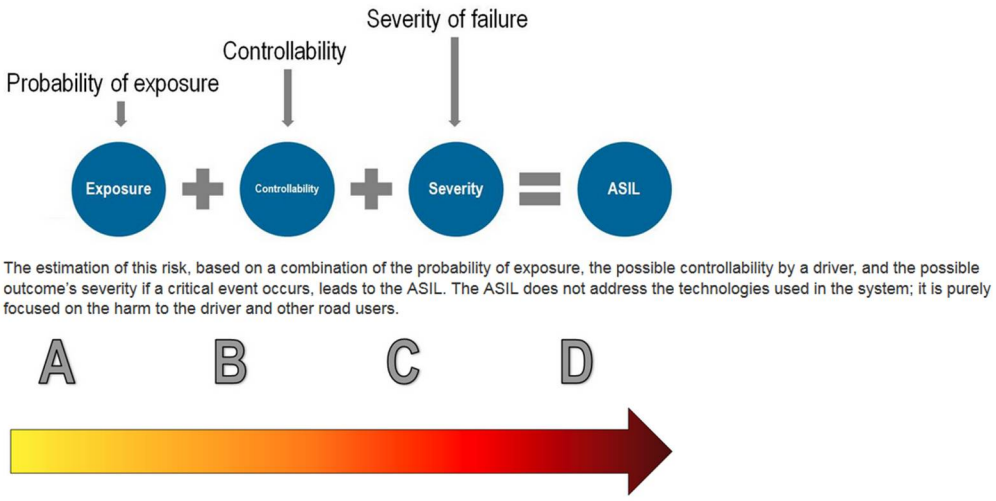


Figura 46. Ponderaciones de ASIL, fuente: (BS ISO 26262, 2011)

SEVERITY	S0	S1	S2	S3	
	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries	
EXPOSURE	E0	E1	E2	E3	E4
	Incredible	Very low probability	Low probability	Medium probability	High probability
CONTROLLABILITY	C0	C1	C2	C3	
	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable	

Una vez realizado el cálculo en base a las ponderaciones dada en según la figura 46, la norma ISO posee una matriz de riesgo como se indica en la siguiente figura 47, en donde se debe ubicar en qué cuadrante la vulnerabilidad reside, entonces se denota nuevamente que ASIL está definida por cuatro niveles, **ASIL A, ASIL B, ASIL C y ASIL D**, es decir son niveles de inseguridad. A más de esto en la matriz de riesgo se indica un nivel llamado "**Quality Management**" por sus siglas **QM**, según la normativa denota que no requiere ser analizada la vulnerabilidad ya que no tiene ningún riesgo.

Figura 47. Matriz de Riesgo ASIL, fuente: ISO 26262

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Las ponderaciones para las vulnerabilidades encontradas se dan de acuerdo a parámetros que lo que recomienda la norma y la experiencia de GM India (Vehicle Cybersecurity Testing, Red Team),

El cálculo de ASIL para Vulnerabilidad 1

- Una severidad S1, en caso de que suceda se tendría lesiones leves y moderadas
- Exposición E3, una probabilidad media
- Control C1, Simplemente Controlable
- Resultado de ASIL, QM

El cálculo de ASIL para Vulnerabilidad 2

- Una severidad S1, en caso de que suceda se tendría lesiones leves y moderadas
- Exposición E2, una probabilidad baja
- Control C1, Simplemente Controlable
- Resultado de ASIL, QM

Cálculo de ASIL para Vulnerabilidad 3

- Una severidad S1, en caso de que suceda se tendría lesiones leves y moderadas
- Exposición E3, una probabilidad media
- Control C2, no tan controlable
- Resultado de ASIL, QM

Cálculo de ASIL para Vulnerabilidad 4

- Una severidad S1, en caso de que suceda se tendría lesiones leves

- Exposición E3, una probabilidad media
- Control C3, difícil de controlar
- Resultado ASIL A

Cálculo de ASIL para Vulnerabilidad 5

- Una severidad S2, grave y amenaza la seguridad de la vida del usuario
- Exposición E3, una probabilidad media
- Control C3, difícil de controlar
- Resultado de ASIL B

En la tabla 9 se encuentra un resumen de las ponderaciones y resultados obtenidos.

Tabla 9. Riesgos encontrados, fuente: propia

No.	Metodología de ataques	Resultado	Severidad	Exposición	Control	ASIL
1	Frame sniffing	Acceso a las tramas de datos de los ECUS	S1	E3	C1	QM
2	Frame falsifying	Simulación de ECUs conectados al BUS GMLAN	S1	E2	C1	QM
3	Frame falsifying Frame injection	Control de encendido del carro Inmobilización vehicular Alteración de funcionamiento del panel	S1	E3	C2	QM
4	Frame falsifying Frame injection	Acceso a la información de ONSTAR (ID y número celular) Apertura remota de puertas	S1	E3	C3	ASIL A
5	Fuzz Testing	Daño al equipo telemático mediante su interfaz de Bluetooth, inmovilizando al vehículo	S2	E3	C3	ASIL B

CAPITULO IV

Propuesta de Control y mitigación de riesgos

El propósito del control de riesgo es analizar el funcionamiento, la efectividad y el cumplimiento de las medidas de protección, para determinar y ajustar sus deficiencias. En esta sección se usa la norma ISO 26262:2011 e ISO 27002:2013. Como se indicó en el punto 3.2 en lo referente a la norma que se debe utilizar para el análisis y control de riesgos es la ISO 26262, pero existen ciertas vulnerabilidades que esta norma no las toma en consideración y es aquí donde se debe complementar con la norma ISO 27002, esta norma consiste en una guía de buenas prácticas que permiten a las organizaciones mejorar la seguridad de su información define una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones.

Para la presentación de las propuestas de control y mitigación de riesgos se realizará desde el ASIL más crítico al menos crítico.

4.1. Primera Propuesta de Control

De acuerdo a la tabla 9 en el CAPÍTULO III, existen 5 riesgos con sus respectivas ponderaciones, el riesgo más alto es el número 5, con ASIL B. Para poder mitigar este riesgo se toma como recomendación el punto 8.4.5 de la norma ISO 26262-6:2011 el cual indica:

"*El diseño e implementación de la unidad de software se verificará de acuerdo con la Cláusula 9 de la norma ISO 26262-8: 2011 y aplicando los métodos de verificación enumerados en la siguiente tabla*

Table 9 — Methods for the verification of software unit design and implementation

	Methods	ASIL			
		A	B	C	D
1a	Walk-through[a]	++	+	o	o
1b	Inspection[a]	+	++	++	++
1c	Semi-formal verification	+	+	++	++
1d	Formal verification	o	o	+	+
1e	Control flow analysis[b,c]	+	+	++	++
1f	Data flow analysis[b,c]	+	+	++	++
1g	Static code analysis	+	++	++	++
1h	Semantic code analysis[d]	+	+	+	+

[a] In the case of model-based software development the software unit specification design and implementation can be verified at the model level.

[b] Methods 1e and 1f can be applied at the source code level. These methods are applicable both to manual code development and to model-based development.

[c] Methods 1e and 1f can be part of methods 1d, 1g or 1h.

[d] Method 1h is used for mathematical analysis of source code by use of an abstract representation of possible values for the variables. For this it is not necessary to translate and execute the source code.

„

(pág. 13)

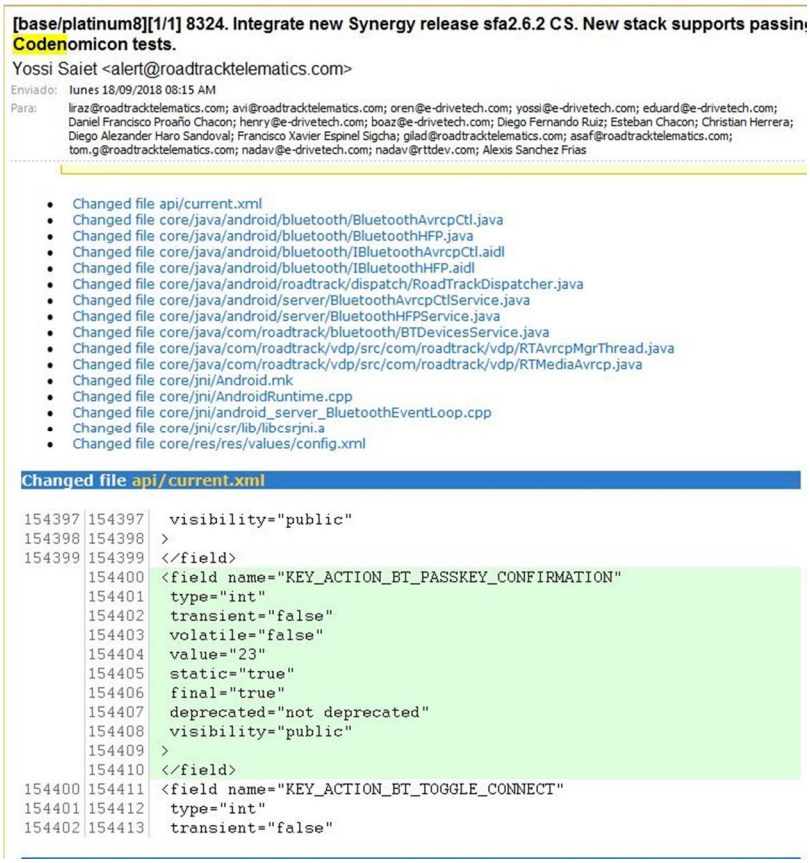
Es decir, se debe realizar un análisis de código estático al software del dispositivo telemático con cada versión que se incluya en los modelos de vehículo de GM. El fuzzer *Codenomicon* debe incluirse como parte del desarrollo del software del dispositivo telemático A más de esto se debe solventar el problema, enviando un parche a los dispositivos telemáticos instalados en los vehículos y corrigiendo el problema en las futuras versiones, como se recomienda en el punto 7.4.15, ISO 26262:2011.

Una acción para dar el cumplimiento a lo mencionado en la norma ISO 26262:2011 párrafo 8.4.5, en la compañía que desarrolla los ECUs telemáticos se realizó una validación a todo el código a través de la ejecución de pruebas de escritorio, se presentó una propuesta de cambio en el módulo que maneja la comunicación Bluetooth (ver figura 48). La propuesta fue validada y aceptada por el equipo de desarrollo de software de dicha empresa, actualmente el cambio se encuentra en la fase de pruebas QA (calidad y aceptación de producto) y al término de esta fase se creará un parche de seguridad y se incluirá en futuras versiones de los

dispositivos telemáticos. Se tiene previsto que los modelos de vehículo GM 2019 que cuenten con un dispositivo telemático no tendrán esta vulnerabilidad.

Se debe tomar en consideración que el parche de seguridad solventa el problema en cualquier vehículo que tenga instalado un dispositivo telemático. La empresa que desarrolla estos dispositivos, debe ser responsable en instalar tanto en futuras versiones como en vehículos que ya hayan sido adquiridos y se estén usando.

Figura 48. Parche de seguridad en Bluetooth, fuente: propia



[base/platinum8][1/1] 8324. Integrate new Synergy release sfa2.6.2 CS. New stack supports passin Codenomicon tests.

Yossi Saiet <alert@roadtracktelematics.com>

Enviado: lunes 18/09/2018 08:15 AM

Para: liraz@roadtracktelematics.com; avi@roadtracktelematics.com; oren@e-drivetech.com; yossi@e-drivetech.com; eduard@e-drivetech.com; Daniel Francisco Proaño Chacon; henry@e-drivetech.com; boaz@e-drivetech.com; Diego Fernando Ruiz; Esteban Chacon; Christian Herrera; Diego Alexander Haro Sandoval; Francisco Xavier Espinel Sigcha; gilad@roadtracktelematics.com; asaf@roadtracktelematics.com; tom.g@roadtracktelematics.com; nadav@e-drivetech.com; nadav@rttdev.com; Alexis Sanchez Frias

- Changed file api/current.xml
- Changed file core/java/android/bluetooth/BluetoothAvrcpCtl.java
- Changed file core/java/android/bluetooth/BluetoothHFP.java
- Changed file core/java/android/bluetooth/IBluetoothAvrcpCtl.aidl
- Changed file core/java/android/bluetooth/IBluetoothHFP.aidl
- Changed file core/java/android/roadtrack/dispatch/RoadTrackDispatcher.java
- Changed file core/java/android/server/BluetoothAvrcpCtlService.java
- Changed file core/java/android/server/BluetoothHFPService.java
- Changed file core/java/com/roadtrack/bluetooth/BTDevicesService.java
- Changed file core/java/com/roadtrack/vdp/src/com/roadtrack/vdp/RTAvrcpMgrThread.java
- Changed file core/java/com/roadtrack/vdp/src/com/roadtrack/vdp/RTMediaAvrcp.java
- Changed file core/jni/Android.mk
- Changed file core/jni/AndroidRuntime.cpp
- Changed file core/jni/android_server_BluetoothEventLoop.cpp
- Changed file core/jni/csr/lib/libcsrjni.a
- Changed file core/res/res/values/config.xml

Changed file api/current.xml

```
154397 154397   visibility="public"
154398 154398  >
154399 154399  </field>
       154400  <field name="KEY_ACTION_BT_PASSKEY_CONFIRMATION"
       154401   type="int"
       154402   transient="false"
       154403   volatile="false"
       154404   value="23"
       154405   static="true"
       154406   final="true"
       154407   deprecated="not deprecated"
       154408   visibility="public"
       154409  >
       154410  </field>
154400 154411  <field name="KEY_ACTION_BT_TOGGLE_CONNECT"
154401 154412   type="int"
154402 154413   transient="false"
```

4.2. Segunda Propuesta de Control

Para el riesgo 4, el cual puede abrir puertas remotamente tiene una ponderación de ASIL A, compromete un posible robo del vehículo y

Para mitigar el riesgo con ponderación ASIL A (apertura de puertas, posible robo de vehículos). Se recomienda adoptar el numeral 10.1.1 de la norma ISO 27002:22013; que tiene que ver con la aplicación de comunicaciones cifradas, es decir la comunicación que se mantiene entre el BUS GMLAN, dispositivo telemático y la red móvil debe ser cifrada o al menos debería existir un método de autenticación que permita interactuar de manera segura con el usuario. Al adoptar esta recomendación se minimizará el riesgo de acceso con otros números celulares no autorizados para apertura remota de puertas además se estaría cumpliendo el punto 8.5.1 de ISO 26262-4:2011 el cual indica que el sistema debe integrarse como una sola unidad con seguridad en todos los puntos de comunicación.

Como acción para dar el cumplimento a esta propuesta se mantuvo reuniones de trabajo con el equipo de seguridad de la empresa GM, en donde se expuso dicho riesgo y la propuesta de cifrado de datos o autenticación en el proceso de comunicación. Actualmente se encuentra en un proceso de evaluación sin una fecha estimada de cambio.

4.3. Tercera Propuesta de Control

Por último, para los riesgos 3, 2, 1, aunque tiene una ponderación para ISO 26262 de QM y no requiere de un análisis, el tener acceso a un puerto de comunicaciones en una red es problemático ya que puede obtenerse cualquier información y utilizar de manera maliciosa. Es por esto que en la norma ISO 27002:2013 en el punto 9.4 Control de Acceso a sistemas y aplicación y 11.1.4 Protección Contra Amenazas Externas, recomienda que el acceso a la información debe estar restringida y la seguridad física debe estar protegida. Se recomienda que el puerto OBD II, tenga una protección física mediante un cierre con candado y el acceso debería ser la llave del vehículo.

Para el diagnostico vehicular se recomienda crear un protocolo de autentificación entre los ECUs mediante un algoritmo de verificación el cual funcionaría de la siguiente manera:

- Los ECUs contiene dos números de 5 bytes de longitud almacenados en su memoria, a este números se los llamarán Semilla y Llave.
- La relación que guarda la Semilla y Llave puede ser algún algoritmo de encriptación.
- En el momento que un TESTER desea conocer alguna información acerca de cualquier ECU (ONSTAR, RADIO, ECM, BCM, etc), debe solicitar la Semilla, y el TESTER debe calcular mediante un algoritmo la “Llave”, y enviar al ECU que desea acceder.
- Si la Llave coincide con la almacenada en memoria, se puede acceder a la información caso contrario se deniega cualquier petición.
- En la figura 49, se puede observar cómo funcionaría el algoritmo

Figura 49. Diagrama para acceso de información, fuente: propia

Como acción para dar el cumplimento a esta propuesta se expuso el funcionamiento lógico del protocolo de autenticación entre los ECUs, teniendo la aceptación por parte del equipo técnico. Actualmente se encuentra en la fase de desarrollo y luego de las diferentes validaciones que se realicen en la fase de QA, este protocolo de autenticación formará parte de la nueva versión de seguridad para el dispositivo telemático.

3.3. Resumen de control y mitigación de riesgos

Se proponen 3 controles para mitigar los riesgos encontrados los cuales se detallen en siguiente cuadro

Tabla 10. Propuestas de mitigación de riesgos, fuente: propia

Riesgos	Detalle	Propuesta de cambio	Estado del control
1	Captura de tramas entre ECUs	Restringir acceso a OBD-II Implementar un algoritmo de autentificación entre ECUs	En desarrollo
2	Alteración del funcionamiento normal del coche. Encendido del vehículo sin llaves de acceso	Restringir acceso a OBD-II Implementar un algoritmo de autentificación entre ECUs	En desarrollo
3	Alteración del funcionamiento normal del coche. Inmovilización Vehicular	Restringir acceso a OBD-II Implementar un algoritmo de autentificación entre ECUs	En desarrollo
4	Apertura remota de puertas a través de un mensaje de texto (SMS)	Implementar un proceso de encriptación o autorización en la comunicación entre el dispositivo telemático y la empresa que los desarrolla.	En proceso de validación
5	Inmovilización vehicular por tramas erróneas en la interfaz Bluetooth del dispositivo telemático	Realizar una corrección en el código del Bluetooth y enviar un parche de actualización a los dispositivos telemáticos.	Cambios de código aceptado, esperando la salida de una nueva versión

Conclusiones

1. Los objetivos de la presente investigación fueron cumplidos, utilizando diferentes métodos para realizar un análisis de vulnerabilidades a la red GMLAN como es “frame sniffing”, “frame falsifying”, “fuzz testing”. Con las herramientas de diagnóstico adecuadas se logró investigar la red GMLAN dando como resultado los ECUs conectados al vehículo. Se concluyó que el dispositivo telemático tiene una vulnerabilidad en el protocolo Bluetooth la cual inmoviliza el vehículo. Para finalizar se desarrollaron recomendación de seguridad basados en normas ISO para poder mitigar el riesgo.
2. El objetivo principal de esta investigación fue analizar la falta de seguridad en el protocolo GMLAN CAN-Bus, en particular, la falta de seguridad en el ECU telemático, el experimento se centró en la posibilidad de que un hombre no autorizado pueda conectar al Bus GMLAN con la capacidad de enviar mensajes falsificados. Como resultado, las vulnerabilidades pueden dar al atacante acceso a toda la red y la capacidad de escribir y leer mensajes.
3. Los resultados han demostrado que utilizando las herramientas de diagnóstico vehicular de acceso público, pueden conectarse con éxito al BUS GMLAN para detectar mensajes o eventos de la red. Conociendo estos mensajes se falsifican los datos y se envían como provenientes de dispositivos legítimos, comportándose de la misma manera como los mensajes que son enviados por los dispositivos realmente conectados al vehículo. Existiendo una inmovilización vehicular y un encendido no autorizado al vehículo.
4. El análisis de vulnerabilidad al dispositivo telemático lo cataloga en un nivel ASIL B, a este resultado se llega mediante las pruebas “fuzz” realizadas al protocolo de

comunicación Bluetooth y el envío de mensajes de texto por personas no autorizados que evidenciaron un inmovilización vehicular, apertura de puertas y control de luces/pito. De nota una falencia en el desarrollo el protocolo BLUETOOTH de la compañía que desarrolla ECUs telemáticos.

5. Se obtuvieron un total de 5 vulnerabilidades en el vehículo, las cuales se asignaron un valor de riesgo de acuerdo a la norma ISO 26262:2011, dos de estas obtuvieron valores críticos, ASIL B y ASIL A. Para las cuales se realizaron 3 recomendaciones para mitigar los riesgos de acuerdo a las normas ISO 26262:2011 e ISO 2002:2013, una de estas recomendaciones elimina el riesgo en la interfaz Bluetooth.
6. Aunque exista evidencia de la falta de seguridad en los vehículos y sus protocolos de comunicación, aún se requieren más investigaciones para proporcionar un entorno automotriz más seguro y prevenir ataques maliciosos. Este proyecto puede continuarse para demostrar que los ataques de denegación de servicio son prácticamente posibles en el protocolo GMLAN CAN BUS y para demostrar sus consecuencias. Además, la investigación también podría analizar la posibilidad de implementar un mecanismo de seguridad para poder resistir los ataques de hombre en el medio y de denegación de servicio. Esta característica de seguridad puede tomar en consideración las claves de encriptación privadas y públicas que se codificarán en el firmware de todas las ECU.

Recomendaciones

1. Toda estrategia o gestión de cambio que se genere a nivel de código en la implementación de nuevas funcionalidades con nuevos beneficios para el usuario final, debe estar alienadas bajo un modelo de seguridad basado en las normas ISO 26262 e ISO 27002, a fin de mitigar futuros riesgos con ASILs críticos.
2. Se debe crear un plan de actualización de dispositivos telemáticos en los modelos de vehículos GM Tracker 2017 que cuenten con BUS GMLAN.
3. Es importante crear escenarios donde se planteen análisis de vulnerabilidades a la red GMLAN para responder de una manera proactiva con parches de seguridad como contramedidas y reducir los riesgos a los usuarios finales.

Bibliografía

Abbott-McCune, S., & Shay, L. (2016). Techniques in hacking and simulating a modern. *IEEE*, 40 - 48.

Asamblea Constituyente. (s.f.). Contitución de la Repúbllica del Ecuador. Capítulo sexto. Derechos de libertad Art. 66.- Numeral 19. Pag.49. Ecuador.

Asamblea Nacional del Ecuador. (10 de Febrero de 2014). Código Orgánico Integral Penal (COIP). Sección Tercera, Delitos contra la seguridad de los activos de los sistemas de información y comunicación. Artículo 230.-. Numeral 1. Pag. 37. *Suplemento Registro Oficial No. 180.* Quito, Pichincha, Ecuador.

BLUETOOTH. (02 de Febero de 2018). *Bluetooth SIG*. Obtenido de https://www.bluetooth.com/specifications/assigned-numbers/logical-link-control

Bray, J., & Sturman, C. (2013). *Bluetooth 1.1: Connect Without Cables (2nd Edition).* Arizona: Prentice Hall.

BS ISO 26262. (2011). ISO 26262. *ISO 26262*. ISO org.

Caizatoa Chulca, M. F., & Méndez Flores, X. D. (12 de Abril de 2014). Diseño e implementación de un prototipo de monitoreo de automóviles empleando el estándar OBD-II. *Diseño e implementación de un prototipo de monitoreo de automóviles empleando el estándar OBD-II.* Quito, Pichincha, Ecuador: ESPE.

CYPRESS. (13 de Julio de 2015). *Automotive Wireless*. Obtenido de CYPRESS: http://www.cypress.com/products/automotive-wireless

Edwards, J., Kashani, A., & Iyer, G. (27 de Octubre de 2017). Evaluation of Software Vulnerabilities in Vehicle Electronic Control Units. Miami, Estados Unidos: IEEE.

EVITA. (Octubre de 2015). *EVITA*. Obtenido de http://evita-project.org

Gallagher, S. (30 de Juli0 de 2015). *ARS TECHNICA*. Obtenido de https://arstechnica.com/information-technology/2015/07/ownstar-researcher-hijacks-remote-access-to-onstar/

Greenberg, A. (21 de Julio de 2015). *WIRED*. Obtenido de WIRED: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Greenberg, A. (21 de Marzo de 2016). *WIRED*. Obtenido de WIRED: https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/

Hashem Eiza , M., & Ni, Q. (2017). Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. *IEEE Vehicular Technology Magazine*, 45 - 61.

Hilpert, H., Thoroe, L., & Schumann, M. (2011). Real-time data collection for product carbon footprints in transportation processes based on OBD2 and smartphone. Conf. Syst. Sci.

Hoppe, T., & Dittmann, J. (Junio de 2007). Sniffing/replay attacks on can buses: A simulated attack on the electric window lift classified using an adapted cert taxonomy.

Hoppe, T., Kiltz, S., & Dittmann, J. (2011). Security threats to automotive CAN. En *Security threats to automotive CAN* (págs. 11-25). Rel. Eng. Syst. Safety.

Hoppe, T., Kiltz, S., & Dittmann, T. (5 de Julio de 2010). Security Threats to Automotive CAN Networks — Practical Examples and Selected Short-Term Countermeasures. Alemania: Proc. SAFECOMP.

ISO 27002. (2013). ISO 27002:2013. *ISO 27002:2013*. ISO org.

Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (20 de MArzo de 2010). Experimental Security Analysis of a Modern Automobile. *Experimental Security Analysis of a Modern Automobile*. San Diego, California, Estados Unidos: IEEE.

Kulkarni, P., Rajani, R., & Varma, K. (23 de Agosto de 2016). Development of On Board Diagnostics (OBD) testing tool to scan emission control system. Pune, India: IEEE.

Linarez, R., & Quijano, J. (2004). IMPLEMENTACIÓN DEL PROTOCOLO BLUETOOTH PARA LA CONEXIÓN INALÁMBRICA DE DISPOSITIVOS ELECTRÓNICOS PROGRAMABLES. *Scientia et Technica*.

Liu, J., Zhang, S., & Sun, W. (28 de Septiembre de 2017). In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions. *IEEE Network*, 50 - 58.

MICROCHIP. (2012). *A CAN Physical Layer Discussion.* Arizona: MICROCHIP.

Muñoz Vizhñay, F. (12 de Octubre de 2013). Estudio para simular una Red CAN con aplicación en comunicación de dispositivos electrónicos en el automóvil. Cuena, Azuay, Ecuador.

National Instrument. (16 de Febrero de 2016). *National Instruments*. Obtenido de NI Formula Collegiate Design Series Community: https://forums.ni.com/t5/NI-Formula-Collegiate-Design/DIAdem-201-Analyzing-CAN-Data-in-DIAdem/gpm-p/3509483

Pazul, K. (2018). *Controller Area Network (CAN) Basics.* Arizona: Microchip.

Shay, L., & Abbott-McCune, S. (24 de Octubre de 2017). Intrusion prevention system of automotive network CAN bus. West Point, New York, New York, Estados Unidos: IEEE.

Shila, D., Geng, P., & Lovett, T. (15 de Septiembre de 2016). I Can Detect You: Using Intrusion Checkers to Resist Malicious Firmware Attacks. Miami, Estados Unidos: IEEE.

Strandberg, K., Olovsson, T., & Jonsson, E. (2018). Securing the Connected Car: A Security-Enhancement Methodology. *IEEE Vehicular Technology Magazine*, 13-18.

Technosolutions. (2 de Septiembre de 2016). *SlideShare*. Obtenido de SlideShate: https://www.slideshare.net/mbedlabsTechnosoluti/can-bus-65612867?from_action=save

Varela, C., & Domínguez, L. (2002). Redes Inalámbricas. *Redes Inalámbricas*. España.

VECTOR. (12 de 11 de 2017). *VECTOR*. Obtenido de VECTOR: https://vector.com/vi_index_en.html

Woo, S., Jo, J., & Hoon, D. (08 de Septiembre de 2015). A Practical Wireless Attack on the Connected Car. *IEEE Transactions on Intelligent Transportation Systems*, págs. 993 - 1006.

Zhang, Y., Ge, B., & Li, X. (25 - 26 de Junio de 2016). Controlling a Car Through OBD Injection. Beijing, China: IEEE.

Anexos A

Evidencia de problemas en el dispositivo telemático

Anexo A
-platinum8-6016-Spor

Anexo B

Evidencia de problemas en el dispositivo telemático

Anexo B -
platinum8-6077-L2CA

Anexo C

Evidencia de problemas en el dispositivo telemático

Anexo C-
platinum8-9495-Error

Anexo D

Evidencia de problemas en el dispositivo telemático

Anexo D-
platinum8-6076-Stres

Anexo E

Evidencia de problemas en el dispositivo telemático

Anexo F

Video de vulnerabilidades