OAK RIDGE National Laboratory

Amenazas cibernéticas al transporte e innovadoras soluciones tecnológicas

Pablo Moriano

Investigador Científico

División de Matemáticas y Ciencias de la Computación

Laboratorio Nacional de Oak Ridge

Simposio Regional Sobre Seguridad Física del Transporte en el Caribe, América Central y México (TS-CCAM) 27Abril 2022

U.S. DEPARTMENT OF ENERGY

OAK RIDGE National Laboratory

CONCEPTOS BÁSICOS SOBRE LA SEGURIDAD DE LOS VEHÍCULOS

Red de área del controlador (red CAN)

- Los vehículos modernos tienen muchas unidades de control electrónico (ECU)
- CAN es un protocolo basado en mensajes, y se utiliza en:
  - Complejos industriales
  - Quirófanos
  - Aviones
  - **Vehículos**

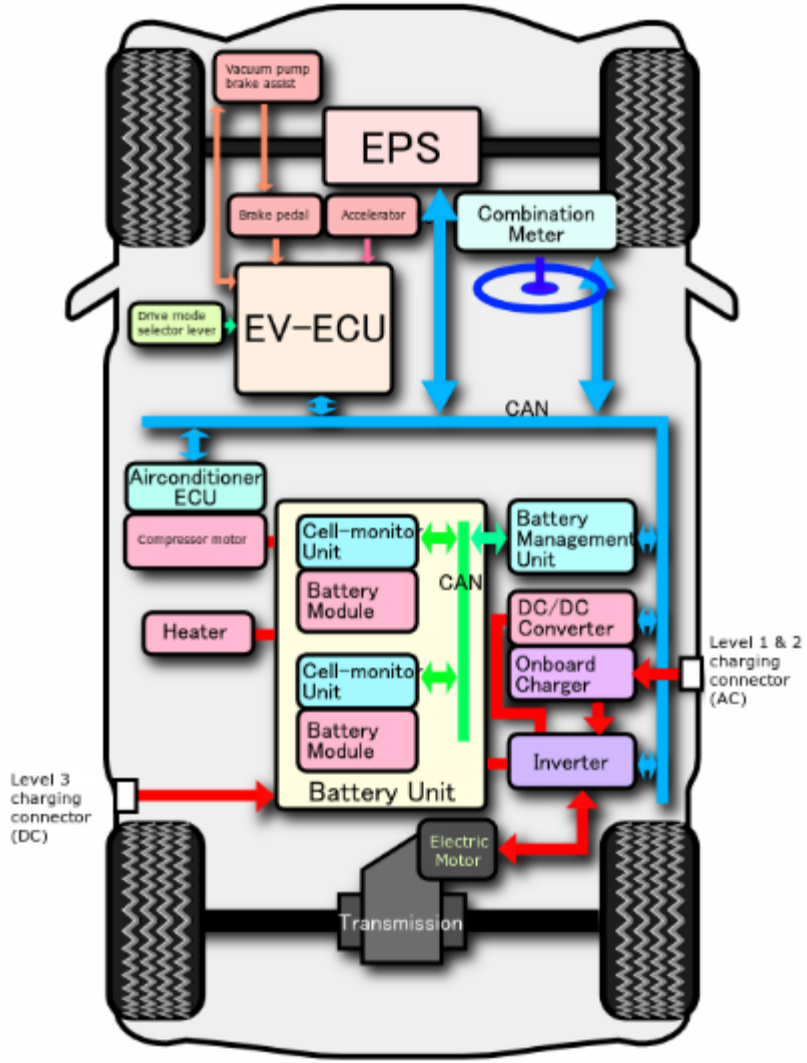


Imagen: Shigeru23, Wikimedia Commons

También se utiliza en vehículos medianos y pesados

Imagen: Robert A. Bridges/ORNL

Laboratorio de seguridad de vehículos del ORNL

Imagen: Carlos Gomez/ORNL

OAK RIDGE National Laboratory

Vulnerabilidades y debilidades de los vehículos

La red CAN del vehículo es vulnerable

- No hay autenticación
- No hay cifrado
- Red de difusión
- No hay información sobre el remitente y el destinatario
- Más bien: seguridad mediante el anonimato

Un ataque simple

Veamos lo que se puede hacer con:

- Hardware de $75
- Muy pocos conocimientos
- Un vehículo moderno

Nada más se envían mensajes aleatorios a una gran velocidad

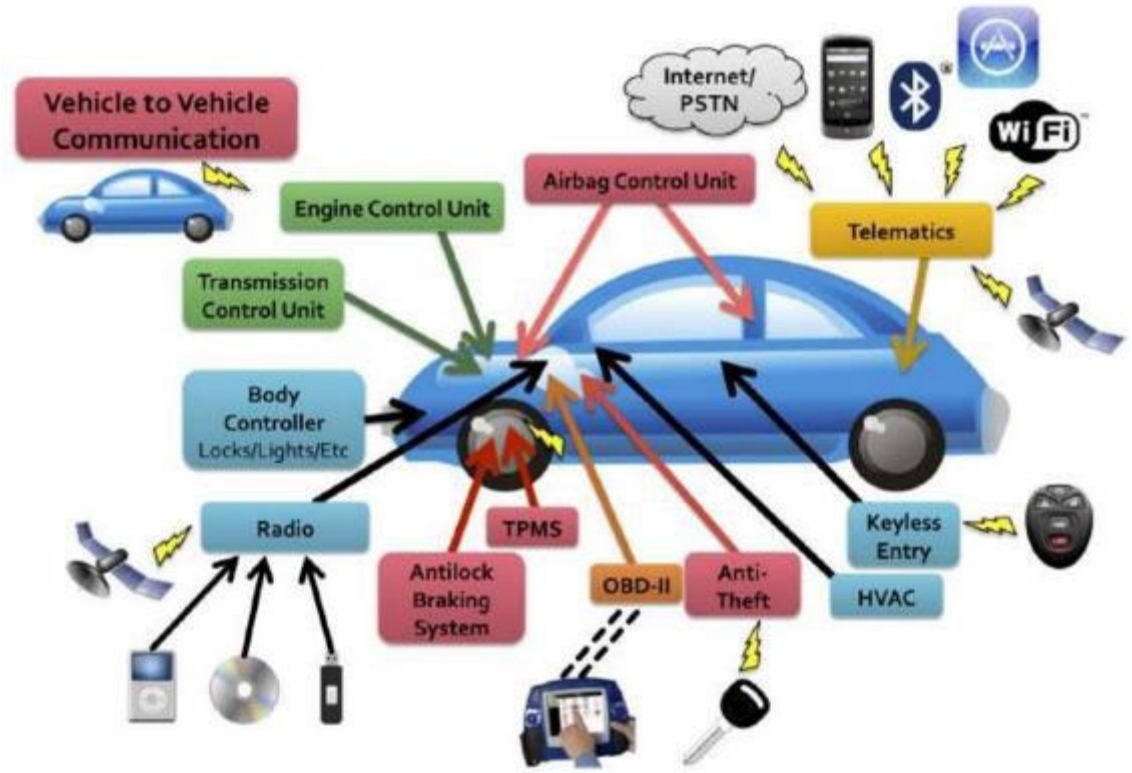
Un ataque simple, segunda parte

Veamos lo que se puede hacer con:

- Hardware de $75
- Muy pocos conocimientos
- Un vehículo moderno

No se envía NINGÚN mensaje; nada más nos conectamos a la red CAN con la tasa de bits incorrecta

Superficie de ataque de un vehículo



Vehículo moderno

S. Checkoway *et al.*, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", Simposio sobre seguridad, USENIX, vol. 4, págs. 447-462, 2011.

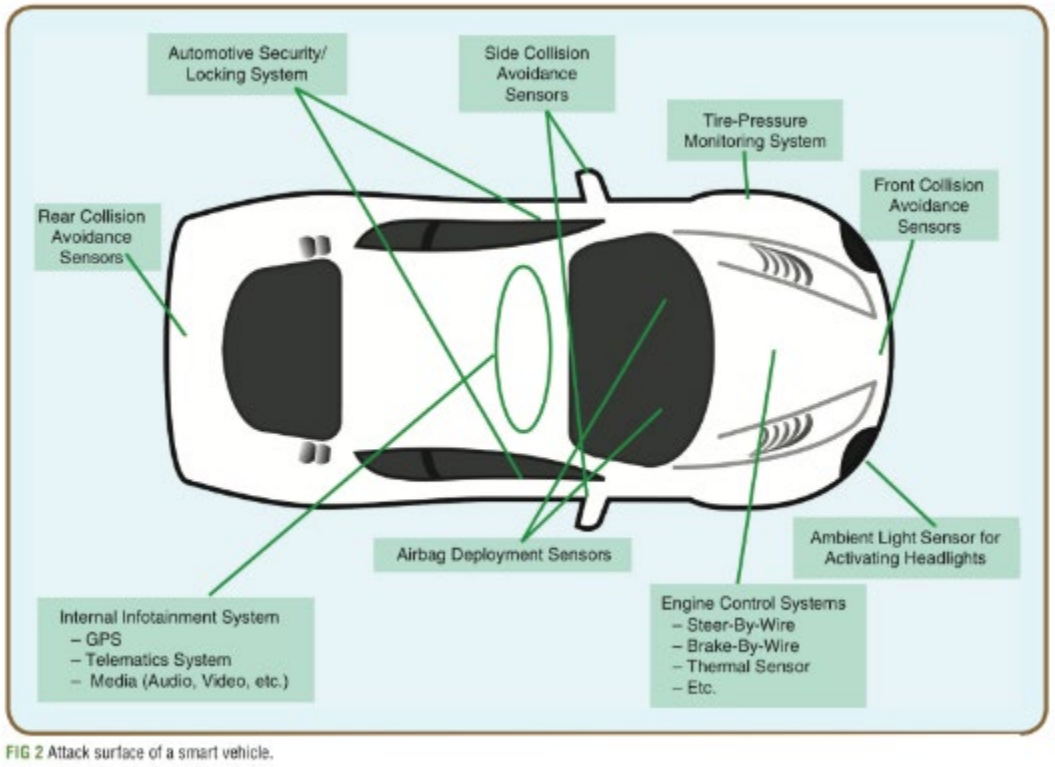


FIG 2 Attack surface of a smart vehicle.

Vehículo inteligente

D. A. Hahn, A. Munir y V. Behzadan, "Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges," revista *IEEE Intelligent Transportation Systems*, pp. 1–1, 2019, doi: 10.1109/MITS.2019.2898973.

Tipos de ataques (las investigaciones se enfocan en diversos ataques a vehículos)

G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij y T. Vuong, “A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles,” *Ad Hoc Networks 2019*, vol. 84, p. 27 mar. 2019

TABLE II
INDICATIVE SECURITY THREATS USED FOR EVALUATION OF IDS FOR VEHICLES

Attack	Description	References
Wormhole	Force a node to transmit its data through a rogue tunnel by pretending to be the shortest and authentic route	[23], [24], [25]
Blackhole	Compromise a node to drop all packets travelling through it without informing their sources	[26], [27], [25], [28], [23]
Greyhole	Compromise a node to selectively drop some packets travelling through it without informing their sources	[29],[28],[27]
Rushing attack	Flood a network with malicious messages so that they are delivered before a legitimate message is received and acknowledged	[29]
Sybil Attack	Generate multiple pseudo-identities in a vehicular network that relies on a reputation system for assessing reliability of information	[24], [25], [27]
Denial of Service (incl. message flooding)	Disrupt communication typically by overwhelming the network with large volumes of meaningless or false data, such as fake alert messages about road accidents and congestion	[30], [31], [32], [26], [33], [27], [34], [35], [36], [37]
Bus-off attack	Exploit the error-handling scheme of in-vehicle networks, by deceiving an uncompromised ECU into thinking it is defective, and eventually forcing itself or even the whole network to shut down	[38]
Message Distortion	Generate distorted reliability message in a vehicular network and activate distribution of this message to a neighbouring vehicle	[39]
Timing attack	An integrity attack that alters message timeslots	[40]
Replay attack	A valid data transmission, such as a command or a sensor reading, is recorded and maliciously repeated at a later point.	[15], [41], [42], [43], [44]
Command Injection	Request execution of existing command with malicious intent, typically to affect actuation	[30], [15], [31], [32]
Impersonation (or masquerade or spoofing) attack	An adversary assumes successfully the identity of one of the legitimate nodes in the vehicular network	[41], [45], [44], [46], [36], [47], [48], [49]
Packet Duplication	Transmit unnecessary network messages to exhaust bandwidth or trigger unnecessary processing	[24], [23], [25]
Selective Forwarding	Retransmit data selectively in a vehicular network	[24], [23], [25]
GPS Jamming	Jam legitimate GPS signals; possibly followed by GPS spoofing	[28]
GPS Spoofing	Transmit false GPS signals to disrupt or hijack navigation of a GPS-dependent vehicle, such as a UAV	[28]
Fuzzing (Fuzz testing)	Send random messages to the in-vehicle network to trigger critical instructions in a brute force manner)	[21]
False Data Injection	Transmit false data to trigger malicious events or affect situational/environmental awareness	[28]
False Information Dissemination	Transmit false data, e.g. a reputation score, to affect a collaborative process in a network	[28], [50]

Ataques organizados por investigadores

Los hackers Miller y Valasek desactivan de manera remota un Jeep Cherokee en la autopista (2015)

Video:
https://www.youtube.com/watch?v=ysAam9Zmdv0

Investigadores de KeenLab atacan un Tesla en Black Hat y demuestran un "espectáculo navideño no autorizado" (2017)

Video:
https://www.youtube.com/watch?v=VH4KgW-GchU

Ataques organizados por investigadores (investigaciones recientes en el descubrimiento de ataques a vehículos)

TABLE 1
SUMMARY OF THE IN-VEHICLE NETWORK EVENTS

1st author	Year	Vehicle	Foothold	Threat Model	Attack Impact
Burakova [18]	2016	2006 Class-8 semi-tractor and 2001 school bus	OBD-II	Physical	Taking cont engine rpm,
Yan [17]	2016	Tesla Model S	Sensors	Physical	Trigger a cra
Higgins [20]	2015	Chevrolet Impala	OBD-II	Physical	The driver v speedometer
Greenberg [8], and Miller [10]	2013	Ford Escape, Toyota Prius	OBD-II	Physical	Disable brak steering whe manipulate v
Koscher [13]	2010	2009 model year passenger car	OBD-II	Physical & Remote (with prior physical access)	Take contro controller; e
Greenberg [1], and Miller [11]	2015	2014 Jeep, Cherokee	Entertainment system –Cellular (Wi-Fi hotspot)	Remote	Take contro control of th system, trai driver privac the GPS coo
Jafarnejad [19]	2015	Renault Twizy 80	OVMS	Remote	Move the v speed of th changing m the throttle
Checkoway [14]	2011	2011 model moderately priced sedan	OBD-II, Media player, Bluetooth, and Cellular	Remote	Complete co surveillance

Kelarestaghi, Kaveh Bakhsh et al. "Vehicle Security: Risk Assessment in Transportation". Junta de Investigaciones en Transporte, 98 Reunión Anual, 2019.

TABLE I
EXPERIMENTAL ATTACKS TO AUTOMOBILES

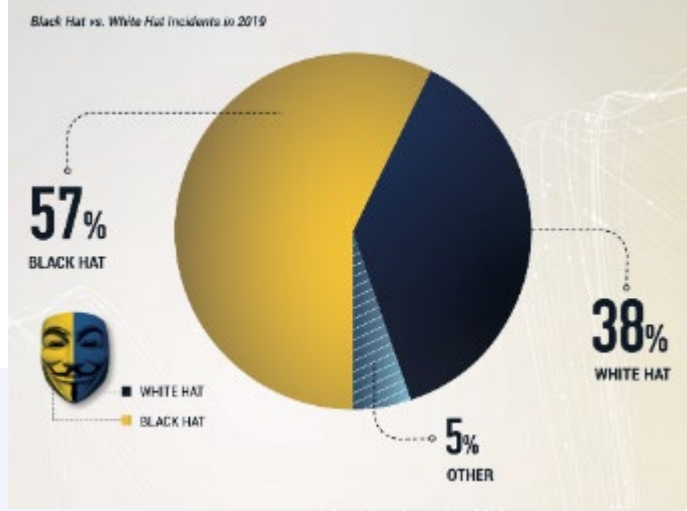
Example	Categories	Attacker surface	Security threats	Contributions
Rouf et al. (2010) [28]	Physical layer	Tire-pressure Monitoring Systems (TPMS)	TPMS spoofing TPMS tracking	The attack mode-based on sensor data is implemented.
Petit et al. (2015) [29]	Physical layer	Perception systems: camera and LiDAR	Blinding attack Jamming attack Replay attack Spoofing attack	The countermeasures are given.
Checkoway et al. (2011) [9]	Data-link layer	OBD port Bluetooth Cellular	System failure	Multiple attack entrances to the vehicle were analyzed.
Cho et al. (2016) [30]	Data-link layer	CAN physical layer	Denial-of-service (DoS) attack	Bus off attack is proposed.
Hoppe et al. (2008) [31]	Application layer	CAN bus interface OBD port	Frame sniffing Replay attack	Control the window lift, warning lights, and ABS; stop these functions.
Koscher et al. (2010) [4]	Application layer	OBD port	Frame sniffing Replay attack DoS attack Frame injection Frame falsifying	Control body, control module, radio, and engine.
Woo et al. (2015) [32]	Application layer	Bluetooth Wi-Fi OBD port (OBD scan tool)	Frame sniffing Replay attack DoS attack Frame injection Frame falsifying	Implement wireless attack. Control dash board, engine, and handle control. Security enhancement protocol is proposed.
Keen Security Lab (2017) [33]	Application layer	Wi-Fi	Remote wireless access Intrusion into the control system	Fully controlled vehicle.

Wu, Wufei et al. "A survey of intrusion detection for in-vehicle networks." revista *IEEE Transactions on Intelligent Transportation Systems* 21.3 (2019): 919-933.

Ataques en la vida real

- Los incidentes de ciberseguridad automotriz:
  - Han aumentado ***siete veces desde 2016***
  - ***Se duplicaron en 2019***
  - Son perpetrados cada vez más por ciberdelincuentes (no investigadores); ***más del 50% de los incidentes fueron perpetrados por delincuentes en 2019***
  - "Los ataques remotos han superado de manera constante los ataques físicos desde 2010, y representan el 82% de todos los ataques de 2019."

INFORME MUNDIAL DE CIBERSEGURIDAD AUTOMOTRIZ DE UPSTREAM SECURITY



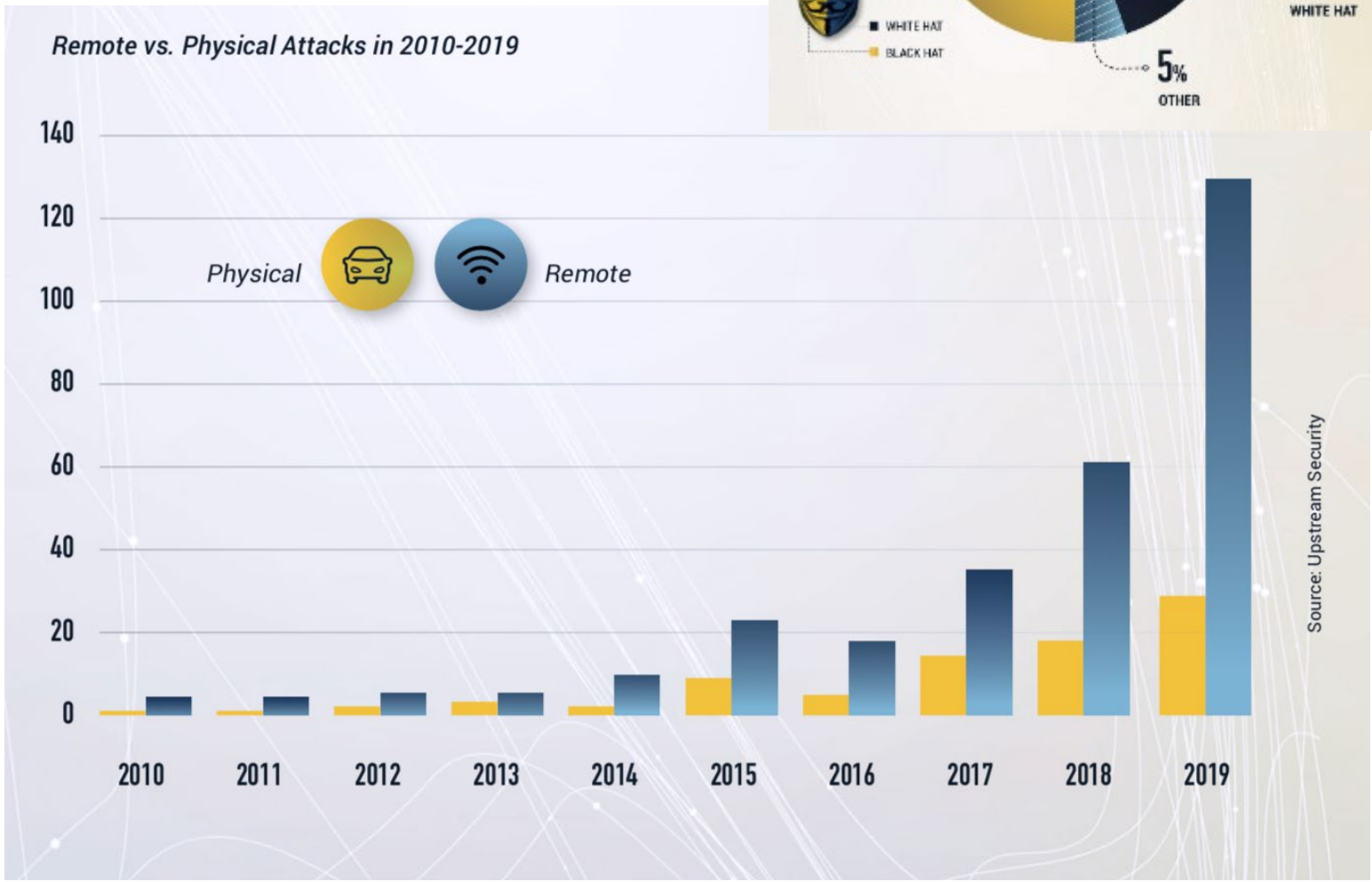


Ilustración: Upstream Security

OAK RIDGE National Laboratory

Ataques en la vida real

- Ejemplos específicos:
  - Privacidad
  - Ejército
  - Camiones
  - Robo
  - Flota con mando a distancia

Gran impacto en la seguridad de los materiales nucleares y radiactivos durante el transporte

- Posibles atacantes:
  - Delincuentes en busca de un beneficio económico inmediato
  - Agentes de inteligencia patrocinados por estados (espías) involucrados en el espionaje estatal o industrial
  - Terroristas interesados en causar el mayor daño posible
  - Usuarios finales interesados en utilizar los datos del vehículo como una nueva fuente de ingresos

Prácticas de ciberseguridad automotriz:

- En la actualidad, los fabricantes originales NO están abordando las vulnerabilidades
- Según una encuesta realizada por Ponemon en 2018 a cerca de 600 "profesionales encargados de contribuir con (o evaluar) la seguridad de los componentes automotrices":

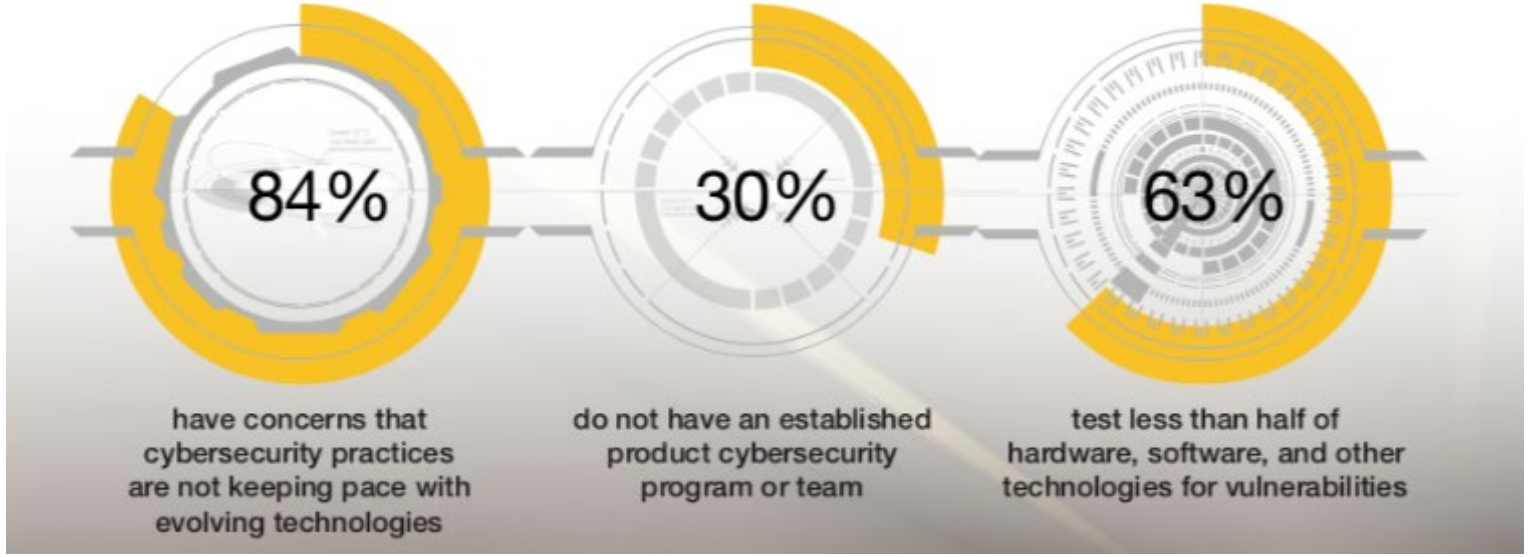


Ilustración: Sinopsis

"En su opinión, ¿cuál es la probabilidad de que, en el siguiente año, ocurra un ataque contra la tecnología automotriz desarrollada o utilizada por su organización?"

• ***Very likely***	***27%***
• ***Likely***	***35%***
• Somewhat likely	23%
• Not likely	15%

Vulnerabilidades: Impacto y probabilidad

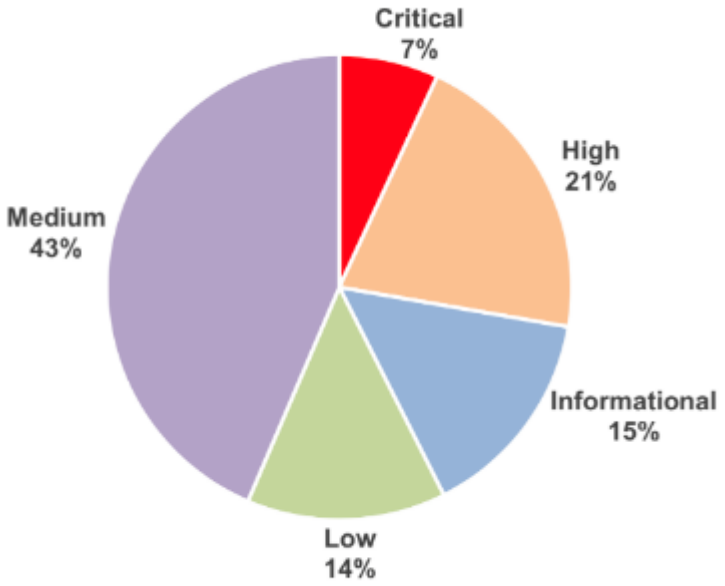


Figure 2 - Vulnerabilities by Likelihood

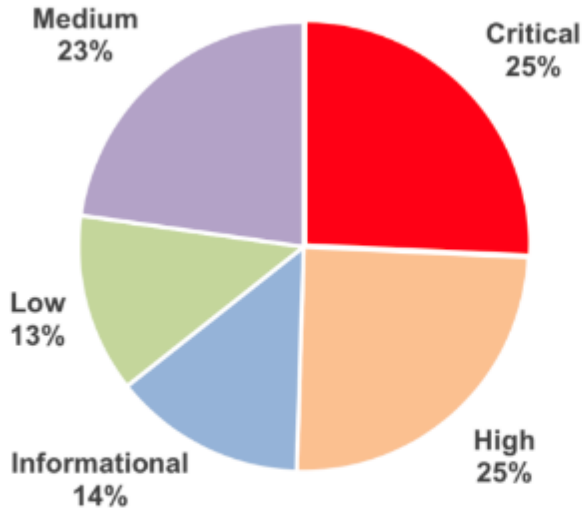


Figure 1 - Vulnerabilities by Impact

Rating (Score)	*Impact*	*Likelihood*
Critical (5)	Extreme impact to vehicle if exploited. Would receive media attention.	Vulnerability is almost certain to be exploited. Knowledge of the vulnerability and its exploitation are in the public domain.
High (4)	Major impact to vehicle if exploited. Could be a regulatory violation.	Vulnerability is relatively easy to detect and exploit by an attacker with little skill.
Medium (3)	Noticeable impact to vehicle if exploited.	An expert attacker could exploit the vulnerability without much difficulty.
Low (2)	Minor impact if exploited, or could be used in conjunction with other vulnerabilities to perform a more serious attack.	Exploiting the vulnerability would require considerable expertise and resources.
Informational (1)	Poor programming practice or poor design decision that may not represent an immediate risk on its own, but may have security implications if multiplied and/or combined with other vulnerabilities.	Vulnerability is not likely to be exploited on its own, but may be used to gain information for launching another attack.

Table 1 – Vulnerability rating system

https://ioactive.com/pdfs/Commonalities_in_Vehicle_Vulnerabilities_WP.pdf

Perspectivas sobre la vulnerabilidad vehicular

- Las funcionalidades de los vehículos están cada vez más electrificadas:

  "Desde 2009, los vehículos tienen ...100 microprocesadores, 50 ECU, 5 millas de cableado y 100 millones de líneas de código"
  http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

- Aumento de la superficie de ataque de los vehículos:

  "En 2022, al menos dos tercios de los automóviles nuevos en las carreteras estadounidenses tendrán conexiones en línea con el sistema crítico de seguridad de los automóviles, lo cual los pondrá en riesgo de ataques mortales."

  https://www.prnewswire.com/news-releases/report-finds-hacking-of-internet-connected-cars-big-national-security-threat-300894261.html

- Los vehículos se están conectando cada vez más:

  "El 55% de los camiones de América del Norte y el 43% de los camiones de Europa estarán conectados en 2025"

  https://www.prnewswire.com/news-releases/connected-and-autonomous-commercial-vehicles-face-daunting-cyber-threats-cautions-frost--sullivan-300770142.html

OAK RIDGE National Laboratory

Cómo defender un vehículo moderno

Un detector sencillo

- Las vulnerabilidades que se explotan fácilmente son fáciles de detectar
- Este detector utiliza características sencillas, basadas en tiempos, para detectar transmisiones anómalas de mensajes

Un detector sencillo, segunda parte

- Las ECU se pueden reprogramar
- Para hacerlo, se deben enviar datos a través del bus, lo cual es fácil de detectar
- Para demostrarlo, utilizamos una herramienta de reprogramación posventa como el nodo adversario
- Nuestro dispositivo utiliza una firma para identificar la reprogramación de la ECU y dar la alerta

(video en la siguiente diapositiva)

Opciones para (investigar) y asegurar la red interna del vehículo

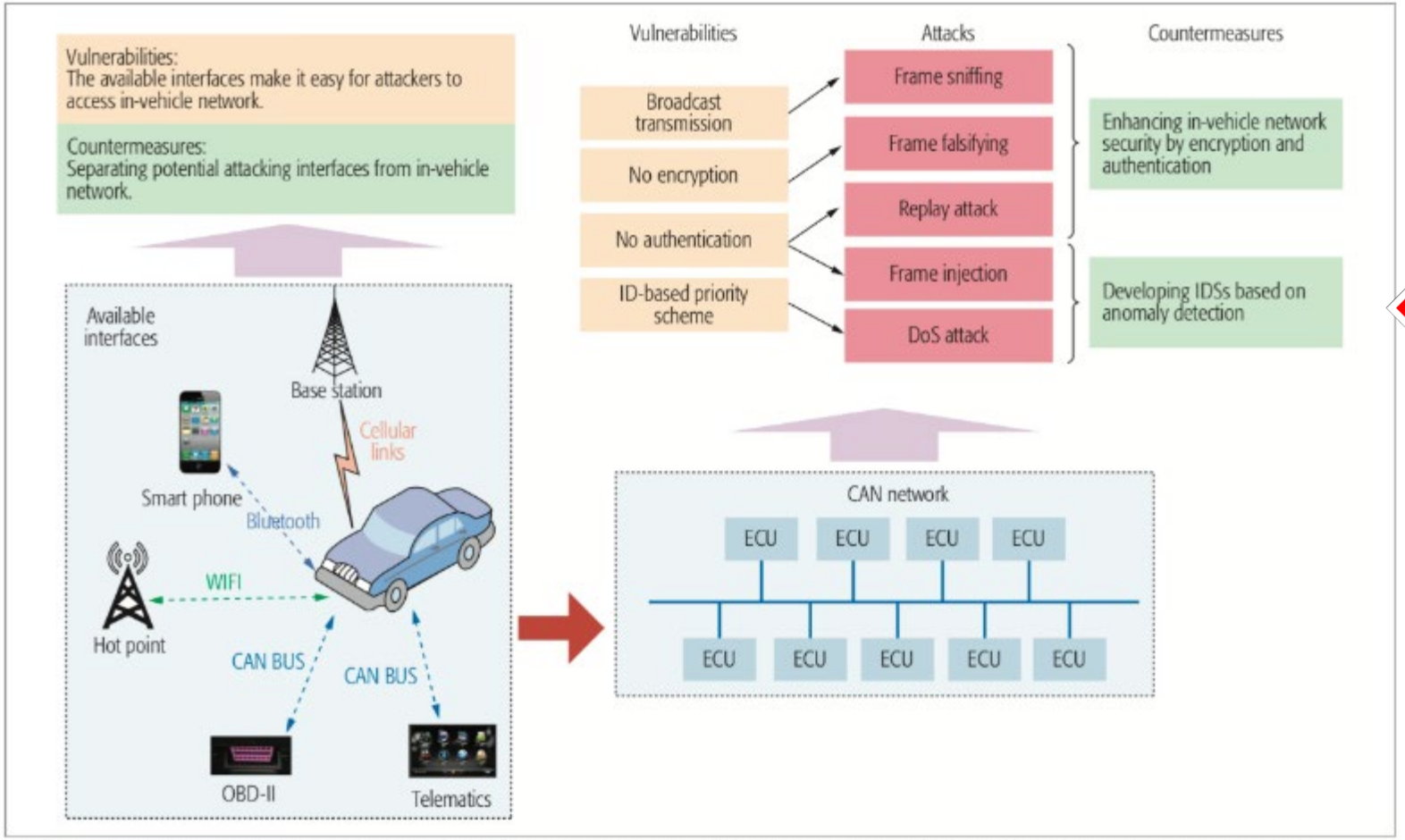


FIGURE 4. In-vehicle network has several intrinsic vulnerabilities, such as broadcast transmission, no authentication, no encryption, ID-based priority scheme and available interfaces, which makes in-vehicle network vulnerable to malicious attacks. Owing to these vulnerabilities, adversaries can easily implement various attacks on in-vehicle network, including frame sniffing, frame falsifying, replay attack, frame injection, and DoS attack. Corresponding countermeasures can be used to protect in-vehicle network from these kinds of attacks, such as encryption and authentication, developing IDS, and separating potential attack interfaces from in-vehicle network.}

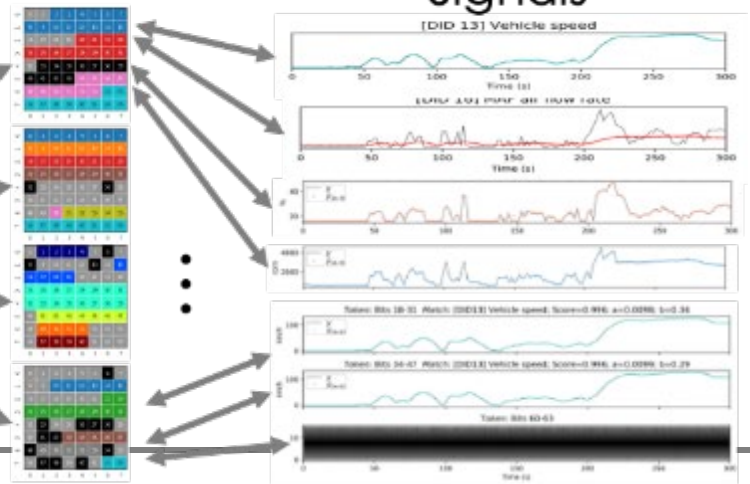
Liu, Jiajia, Shubin Zhang, Wen Sun y Yongpeng Shi. "In-vehicle network attacks and countermeasures: Challenges and future directions." revista *IEEE Network* 31, no. 5 (2017): 50-58.

Proyecto ORNL de detección de intrusiones a vehículos

Paso 1:
Entender datos de red CAN (ingeniería inversa)

CAN data

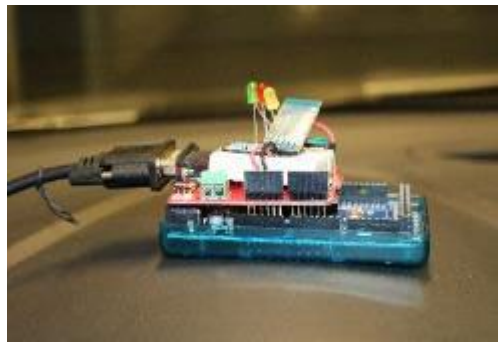
```
(1536160252.263295) can0 223#0020000000000004D
(1536160252.263296) can0 3B7#0000000000000000
(1536160252.263296) can0 2C1#0800E2007DC700F9
(1536160252.265273) can0 2D0#06F6010070000047
(1536160252.268251) can0 020#000007
(1536160252.269250) can0 0B4#0000000054000010
(1536160252.269252) can0 024#01FE020762007F15
(1536160252.269252) can0 025#0FEE000178787893
(1536160252.270291) can0 2C4#038D001F0080615E
(1536160252.271312) can0 262#0000000069
(1536160252.271313) can0 4DC#1D00010700000000
```



Paso 2:
Crear algoritmos de detección

Tipo de ataque	Tipo de detector
• Inyección de código en CAN	• Anomalía en tiempo de mensajes
• Manipulación de señal única	• Anomalía de señal única
• Varias señales manipuladas	• Interrupción o cambios a relaciones entre señales

Paso 3:
Adaptar algoritmos a una tecnología de posventa



OAK RIDGE National Laboratory

OAK RIDGE National Laboratory

Thank you!

Pablo Moriano

Research Scientist

Computer Science and Mathematics Division

Oak Ridge National Laboratory

moriano@ornl.gov

Pablo Moriano

pmoriano.com

@morianop

U.S. DEPARTMENT OF ENERGY