A Cyber Security Analysis Methodology for Evaluating Automobile Risk Exposures

Kameron Tillman, Jason Staggs, and Sujeet Shenoi(✉)

University of Tulsa, Tulsa, Oklahoma, USA
sujeet@utulsa.edu

Abstract. Modern automobiles incorporate numerous sensors, actuators and electronic control units that work in concert to provide safe, efficient and comfortable driving experiences. Automobile convenience features introduce network connectivity via short-range wireless communications protocols and the Internet, potentially exposing the automobile electronics to remote attacks in addition to physical attacks. New attacks on modern automobiles are constantly being developed; their potential impacts range from inconvenience to severe injury and death.

This chapter describes a security analysis methodology for rapidly evaluating the risk exposures of modern automobiles. The methodology considers the automobile attack surfaces comprising the attack vectors that provide access to automobile targets and the potential impacts resulting from successful attacks on the accessed targets. Key features of the security analysis methodology are that it is holistic and rapid, and can be applied by individuals with limited expertise in automobile technologies and cyber security.

Keywords: Automobiles · Security Assessment Methodology · Attack Vectors · Targets · Attacks · Impacts · Risk Exposure

1 Introduction

Every year, new automobile models are introduced with the latest technologies, advanced safety, convenience and comfort features and ubiquitous connectivity to the Internet, Wi-Fi networks and mobile communications networks [19]. The introduction of highly-networked computing systems capable of controlling critical automobile functionality such as steering and braking in environments that formerly comprised hardwired electromechanical components raises significant security concerns. Automobile attack surfaces have also grown as convenience features provide external connectivity. In addition to physical attacks, it is possible to attack automobile systems remotely with adequate expertise, equipment and access.

Security researchers have developed and continue to develop novel automobile exploits. Passive keyless entry system attacks using inexpensive software-defined radios have been used to steal high-end automobiles [23]. Remote attacks that

Published by Springer Nature Switzerland AG 2024
J. Staggs and S. Shenoi (Eds.): ICCIP 2023, IFIP AICT 686, pp. 195–220, 2024.
https://doi.org/10.1007/978-3-031-49585-4_10

disable electronic stability control systems have been demonstrated on Volkswagen automobiles [2]. Door unlocking/locking, exterior lighting and internal audio controls in Tesla automobiles have been remotely exploited [24]. The 2015 Jeep Grand Cherokee attacks remotely operated windshield wipers, engine and braking controls leading to a safety recall of 1.4 million automobiles [16,17].

While automobile exploits garner considerable attention, it is difficult for individuals and organizations to directly engage this knowledge to comprehend and evaluate the risk exposures of automobiles available for purchase, lease or rent. What is needed is a security analysis methodology that accommodates the complex, diverse and ever-changing cyber anatomies, configurations and features of automobiles, and that can be applied by individuals with limited expertise in automobile technologies and cyber security.

Several security analysis methodologies have been proposed to quantify the risk exposures of modern automobiles (see, e.g., [18,40]). However, the methodologies primarily provide composite numerical risk estimates. The principal problem with such estimates is that they do not express the true risk, which is best conveyed semantically in terms of the attack surfaces of automobiles, the various targets that can be accessed and the impacts of successful attacks on the targets.

This chapter describes a security analysis methodology for evaluating the risk exposures of modern automobiles. The methodology considers the automobile attack surfaces and the potential impacts resulting from successful attacks on the accessed targets. The methodology, which requires little if any expertise in automobile technologies and cyber security for its application, enables rapid risk assessments of automobiles available for purchase, lease or rent.

2 Related Work

Koscher et al. [21] investigated the physical attack surfaces of modern automobiles. Their research involved invasive automobile disassembly and extracting automobile components to identify vulnerabilities, attack strategies and potential attack impacts.

Checkoway et al. [9] focused on the cyber attack surfaces of modern automobiles. They developed and leveraged automobile component software exploits to extract critical information such as automobile location data.

Valasek and Miller [37] also investigated the cyber attack surfaces of modern automobiles. Their research involved invasive automobile disassembly to determine automobile attack surfaces.

In contrast, the proposed automobile security analysis methodology engages generic, albeit configurable, attack surfaces with additional attack vectors and configurable targets that may be attacked to cause negative impacts. The security analysis methodology relies on detailed descriptions of the cyber anatomies of modern automobiles that specify their network architectures, underlying systems and networks, network connectivity and the many physical and cyber attack vectors that constitute their attack surfaces.

The security analysis methodology does not require invasive automobile disassembly, vulnerability discovery or attack execution. Indeed, it can be applied

by individuals with limited technical expertise in automobile technologies and cyber security. Importantly, the methodology can be completed within hours instead of days or weeks, enabling individuals and enterprises to quickly evaluate risk exposures and make informed choices when selecting automobiles for purchase, lease or rent.

3 Automobile Cyber Anatomy

Automobile networks are diverse and can be complex due to their proprietary sub-networks and protocols. This section describes a generic automobile network specification that models the diverse networks in modern automobiles in order to conduct realistic security analyses without tedious modeling efforts.

A modern automobile network has three principal sub-networks, High-Speed Controller Area Network (High-Speed CAN), Low-Speed CAN and Media Oriented Streaming Transport (MOST) network, which are typically interconnected via a gateway. The automobile network also provides an on-board diagnostics (OBD) interface.

3.1 High-Speed CAN

The High-Speed CAN is used for critical applications such as automobile acceleration and braking. Advanced driver assistance systems connect to the High-Speed CAN bus and interface with critical automobile controls to assist drivers with automobile operation. Examples of advanced driver assistance systems in a High-Speed CAN include the forward collision system, adaptive cruise control system, lane keep assist/departure warning systems, automatic parking system, engine start-stop system, electronic parking brake system and blind spot detection system:

- **Forward Collision System:** The forward collision system employs detection and ranging sensors that monitor driving conditions and alert drivers to potential frontal collisions [26]. Audible and visual warnings are triggered upon potential collision detection, providing drivers with additional time to react to adverse situations. If a collision is imminent, the forward collision system may engage the brakes automatically to mitigate the danger.
- **Adaptive Cruise Control System:** Figure 1 (left-hand side) illustrates the operation of the adaptive cruise control system. The system employs detection and ranging sensors that monitor vehicles traveling in front of the automobile in order to maintain a safe following distance. When a vehicle is detected, adaptive cruise control accelerates or decelerates the automobile as necessary to maintain a safe following distance. When no other vehicles are detected in proximity, the automobile travels at the set cruising speed. Some adaptive cruise control systems can bring automobiles to a complete stop in emergency situations [26].

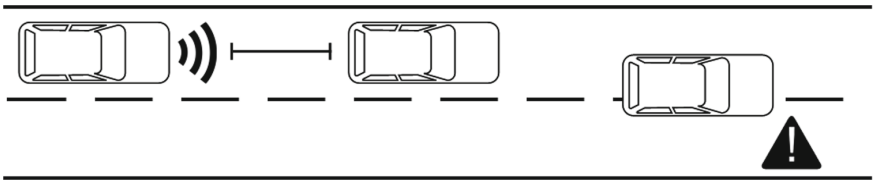

Fig. 1. Adaptive cruise control (left) and lane keep assist (right).

- **Lane Keep Assist/Departure Warning Systems:** Figure 1 (right-hand side) illustrates the operation of the lane keep assist system. The system employs vision sensors to monitor lane markings on the roadway [26]. If a driver moves from a lane without using a turn signal, the lane keep assist system steers the automobile to the center of the lane. Lane departure warning, an advanced driver assistance system similar to lane keep assist, alerts the driver when the automobile moves out of its lane [26].
- **Automatic Parking System:** The automatic parking system employs detection and ranging sensors to determine whether or not a parking spot can accommodate an automobile [26]. After a parking spot has been deemed suitable, the automatic parking electronic control unit computes the steering maneuvers and actuates the steering wheel to complete the parking operation. No steering input by the driver is required to park the automobile.
- **Engine Start-Stop System:** The engine start-stop system employs ignition controls to automatically shut down and restart an engine to reduce engine idling time and emissions. The system shuts down the engine during long stops, such as when waiting at a traffic light or in heavy traffic. When pressure on the brake pedal is released, the engine is restarted automatically and driving may resume [10].
- **Electronic Parking Brake System:** The electronic parking brake system employs actuators to engage the brakes and replaces the manual handbrake with an electronic control. The electronic parking brakes are integrated with other advanced driver assistance systems to enable rapid automatic braking. The brakes may engage automatically when an automobile is parked and the engine is shut down [33].
- **Blind Spot Detection System:** The blind spot detection system employs detection and ranging sensors to monitor automobile blind spots, areas where driver visibility is hampered or obfuscated. The system issues a visible alert when a blind spot is detected [26]. It also issues visible and audible alerts when a driver attempts to merge towards an automobile in the proximity of a blind spot.

3.2 Low-Speed CAN

The Low-Speed CAN supports non-critical applications such as the climate control, power mirror control, windshield wiper control and lighting control systems.

A Local Interconnect Network (LIN) is used to connect Low-Speed CAN bus devices to auxiliary components. For example, the LIN connects the power mirror control system to individual mirrors and connects the lighting control system to the headlights and taillights [30].

3.3 MOST Network

The MOST network connects devices that provide external network connectivity and automobile interfaces. Devices commonly connected in a MOST ring include the telematics system, infotainment system, Wi-Fi module, Bluetooth module and microphone array:

- **Telematics System:** The telematics system enables communications with external systems and networks. Modern automobile telematics systems are equipped with cellular modems for cellular network connectivity. In 2020, approximately 91% of the automobiles sold in the United States were equipped with cellular modems [20]. Modern automobiles with telematics systems support convenience features such as remote unlocking/locking and keyless ignition using a smartphone [26].
- **Infotainment System:** The infotainment system provides a human-machine interface for automobile applications software. The system presents live information (e.g., weather and traffic data) and entertainment options (e.g., media playback and AM/FM radio tuner). An infotainment system is often located at the center of the dashboard and is controlled via a touch screen, physical buttons or voice commands [30].
- **Wi-Fi Module:** The Wi-Fi module enables Wi-Fi hotspot network tethering functionality. A client device connects to the Wi-Fi hotspot in an automobile to obtain cellular network connectivity via the telematics system [38]. The Wi-Fi module also enables Wi-Fi connectivity, enabling an automobile to connect to a wireless network to stream media and download updates.
- **Bluetooth Module:** The Bluetooth module enables mobile device connectivity, media streaming and hands-free voice calling.
- **Microphone Array:** The microphone array enables a driver to interface with the infotainment system via voice commands. The microphone array can also be used to make hands-free voice calls.

3.4 On-Board Diagnostics Interface

The OBD interface is the primary entry point to the automobile network. OBD-II, the latest implementation, enables real-time reporting of automobile system data. It leverages the High-Speed and Low-Speed CANs to interact with practically every system in an automobile network [30].

4 Attack Vectors

Several physical and cyber attack vectors can be leveraged to access systems in automobile networks. Since multiple critical and non-critical automobile systems

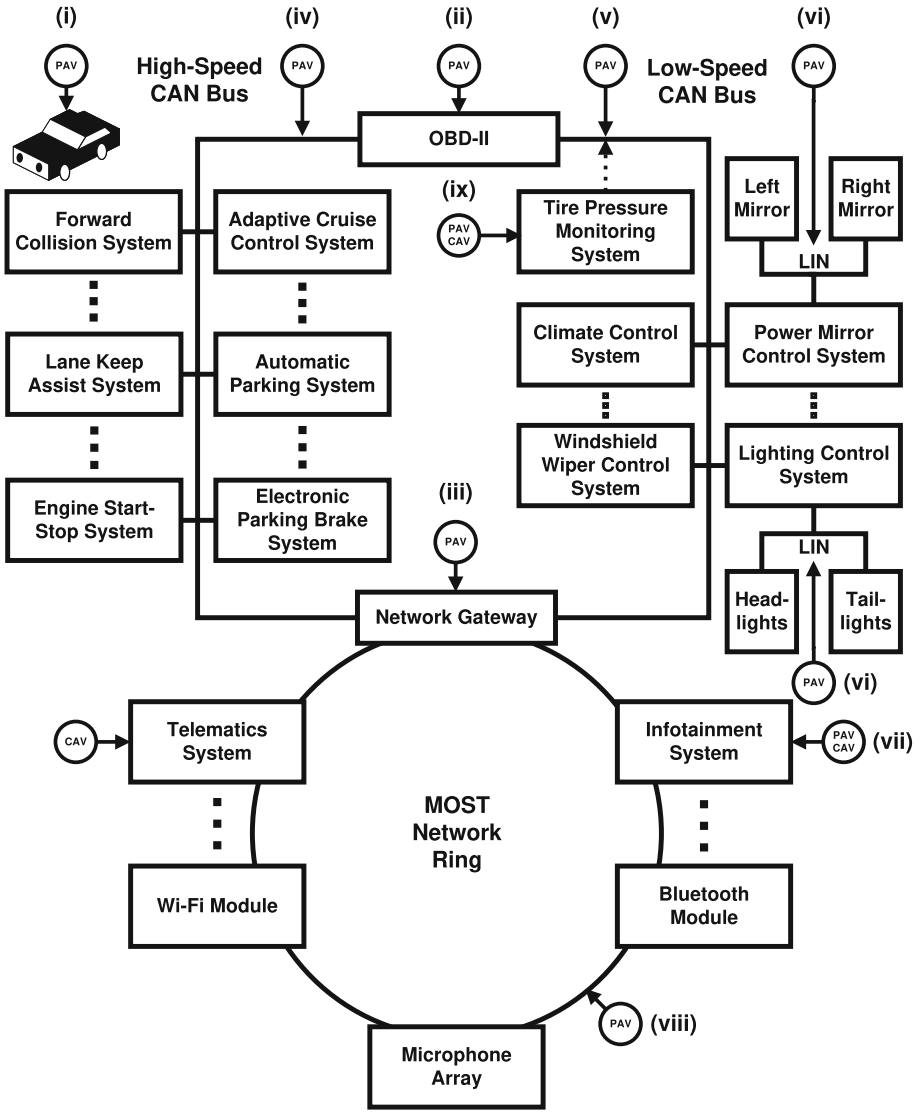

Fig. 2. Physical and cyber attack vectors providing access to automobile targets.

are interconnected, access to one system can be leveraged to access and target other systems and cause negative impacts to an automobile and its occupants.

Figure 2 shows the physical attack vectors (PAVs) and cyber attack vectors (CAVs). Because the focus is on normal (unmodified) automobiles, supply chain compromises of automobile systems and parasitic device implants in automobile systems are not considered.

4.1 Physical Attack Vectors

Koscher et al. [21] specified the physical attack surfaces of modern automobiles as of 2010. Additionally, they identified several vulnerabilities and demonstrated the negative impacts of successful attacks. In contrast, this work describes a generic, albeit configurable, attack surface for modern automobiles through 2022 models with additional physical attack vectors that cover new automobile technologies and designs, along with configurable targets that may be attacked to cause negative impacts.

Table 1 shows the physical attack vectors that provide access to automobile targets, which include the automobile interior, automobile networks and interconnected automobile systems. A physical attack vector provides hands-on access to a targeted system, following which an attack that exploits a vulnerability in the system may be executed to cause negative impacts. Access to the targeted system may also be leveraged to access and subsequently attack other connected automobile systems.

The physical attack vectors that provide access to automobile targets include physical access to the automobile interior, OBD interface, network gateway, High-Speed CAN, Low-Speed CAN, LIN, infotainment system, MOST network and tire pressure monitoring system (TPMS):

- **Physical Access to Automobile Interior:** Physical access to an automobile interior enables all the other attack vectors to be leveraged. An automobile interior may be accessed via graceful entry or forced entry. Graceful entry may employ a paired key fob, physical key or personal identification number keypad, which disengage the anti-theft system. A key fob relay attack [23] provides graceful entry to an automobile interior because it circumvents the anti-theft system. Forced entry, which may employ locksmith or invasive tools to gain access, does not disable the anti-theft system.
- **Physical Access to OBD Interface:** Physical access to an OBD-II interface enables interactions with practically every system in the High-Speed and Low-Speed CANs. OBD-II access may also enable communications with MOST network systems via the network gateway.
- **Physical Access to Network Gateway:** Physical access to a network gateway enables interactions with systems in the High-Speed and Low-Speed CANs as well as MOST network systems.
- **Physical Access to High-Speed CAN:** Physical access to a High-Speed CAN enables interactions with the interconnected critical automobile systems. High-Speed CAN systems may be distributed across multiple, segmented High-Speed CAN buses [37]. Therefore, access to one segmented High-Speed CAN bus may not enable interactions with systems in other segmented High-Speed CAN buses.

  Since a High-Speed CAN does not have authentication, addressing and message encryption schemes [6], CAN wiretapping can be leveraged to circumvent the OBD-II interface to gain direct High-Speed CAN bus connectivity [30]. In fact, malicious interactions with High-Speed CAN systems are easily accomplished.

Table 1. Network and target access provided by physical attack vectors.

Attack Vectors	Network Access	Target Access
Physical Access to Automobile Interior	*Direct Access* HS-CAN, LS-CAN LIN, MOST	ADAS, Other HS-CAN Systems, LS-CAN Systems, TPMS
Physical Access to On-Board Diagnostics Interface	*Direct Access* HS-CAN, LS-CAN, LIN, MOST	ADAS, Other HS-CAN Systems, LS-CAN Systems, TPMS, Microphone Array
Physical Access to Network Gateway	*Direct Access* HS-CAN, LS-CAN, LIN, MOST	ADAS, Other HS-CAN Systems, LS-CAN Systems, TPMS, Microphone Array
Physical Access to High-Speed CAN (HS-CAN)	*Direct Access* HS-CAN	ADAS, Other HS-CAN Systems
	Indirect Access LS-CAN, LIN, MOST	LS-CAN Systems, TPMS, Microphone Array
Physical Access to (LS-CAN)	*Direct Access* LS-CAN, LIN	LS-CAN Systems, TPMS
	Indirect Access HS-CAN, MOST	ADAS, Other HS-CAN Systems, Microphone Array
Physical Access to LIN	*Direct Access* LIN	LS-CAN Systems, TPMS
	Indirect Access LS-CAN	LS-CAN Systems, TPMS
Physical Access to Infotainment System	*Direct Access* HS-CAN, LS-CAN, MOST	ADAS, Other HS-CAN Systems, LS-CAN Systems, TPMS, Microphone Array
	Indirect Access LIN	LS-CAN Systems, TPMS
Physical Access to MOST Network	*Direct Access* MOST	Microphone Array
	Indirect Access HS-CAN, LS-CAN, LIN	ADAS, Other HS-CAN Systems, LS-CAN Systems, TPMS
Physical Access to TPMS (Connected)	*Direct Access* LS-CAN	LS-CAN Systems, TPMS
Physical Access to TPMS (Isolated)	*Direct Access* No Systems and Networks	TPMS

ADAS: Advanced driver assistance HS-CAN systems, HS-CAN: High-Speed CAN, LS-CAN: Low-Speed CAN

- **Physical Access to Low-Speed CAN:** Physical access to a Low-Speed CAN enables interactions with the interconnected non-critical automobile systems. Low-Speed CAN systems may be distributed across multiple, segmented Low-Speed CAN buses [37]. Therefore, access to one segmented Low-Speed CAN bus may not enable interactions with systems in other segmented Low-Speed CAN buses.
- **Physical Access to LIN:** Physical access to a LIN enables interactions with interconnected auxiliary systems and devices. A LIN may contain a master node that serves as a bridge to a Low-Speed CAN bus. In this case, physical access to the LIN would also enable interactions with systems in the connected Low-Speed CAN bus [30].
- **Physical Access to Infotainment System:** Physical access to an infotainment system enables interactions with automobile applications software. The infotainment system provides optical storage media slots, Secure Digital (SD) card slots and USB ports for media and update purposes [22]. The system may have a web browser for accessing local and remote websites. Physical access to the infotainment system in the MOST network may be leveraged to interact with systems in the High-Speed and Low-Speed CANs [30].
  Valasek and Miller [38] exploited a vulnerability in a 2015 Jeep Grand Cherokee infotainment system update mechanism using USB removable media. The attack enabled a custom software installation that provided privileged access to the infotainment system as well as all the other systems in the MOST network and High-Speed and Low-Speed CANs.
  Dimov [11] launched a denial-of-service attack on a Tesla Model 3 automobile using the automobile's web browser to connect to a malicious website. The infotainment system froze upon accessing the malicious website and disabled critical data reporting, including speedometer readings and battery status.
- **Physical Access to MOST Network:** Physical access to a MOST network enables interactions with the telematics system, infotainment system and microphone array. Physical tapping of a MOST network is difficult because the network employs a range of communications media. Smith [30] has suggested that MOST network systems should be targeted directly instead of via communications media. In an automobile with a network gateway, MOST network access enables subsequent access to the systems and devices in the High-Speed and Low-Speed CANs and connected LINs. Otherwise, access is limited to MOST network systems.
- **Physical Access to TPMS:** Physical access to a TPMS enables interactions with the TPMS and, possibly, Low-Speed CAN systems. Figure 2 illustrates the two possibilities for TPMS connectivity in automobile networks. Specifically, a TPMS may be isolated from all the automobile networks or it may be connected to the Low-Speed CAN [37].
  A TPMS utilizes sensors that measure and report tire pressure. The system warns the driver when one or more tires have low pressure. All passenger automobiles in the United States manufactured after 2007 require the installation of TPMSs [28].

Table 2. Network and target access provided by cyber attack vectors.

Attack Vectors	Network Access	Target Access
Cyber Access to	*Direct Access* HS-CAN, LS-CAN, MOST	Advanced Driver Assistance HS-CAN Systems, Other HS-CAN Systems, LS-CAN Systems, TPMS, Microphone Array
	Indirect Access LIN	LS-CAN Systems, TPMS
Cyber Access to Infotainment System	*Direct Access* HS-CAN, LS-CAN, MOST	Advanced Driver Assistance HS-CAN Systems, Other HS-CAN Systems, LS-CAN Systems, TPMS, Microphone Array
	Indirect Access LIN	LS-CAN Systems, TPMS
Cyber Access to TPMS (Connected)	*Direct Access* LS-CAN	LS-CAN Systems, TPMS
Cyber Access to TPMS (Isolated)	*Direct Access* No Systems and Networks	TPMS

HS-CAN: High-Speed CAN, LS-CAN: Low-Speed CAN

4.2 Cyber Attack Vectors

Checkoway et al. [9] and Valasek and Miller [37] have described the cyber attack surfaces of modern automobiles as of 2011 and 2014, respectively. Checkoway et al. [9] also specified several attacks and demonstrated their negative impacts. In contrast, this work describes a generic, albeit configurable, attack surface of modern automobiles through 2022 models with additional cyber attack vectors that cover new automobile technologies and designs, along with configurable targets that may be attacked to cause negative impacts.

Table 2 shows the cyber attack vectors that provide access to automobile targets, automobile networks and interconnected automobile systems. A cyber attack vector provides remote access to a targeted system, following which an attack that exploits a vulnerability in the targeted system can be executed to cause negative impacts. Access to a targeted system may also be leveraged to access and subsequently attack other connected automobile systems. The cyber attack vectors in an automobile network include cyber access to the telematics system, infotainment system and connected (as opposed to isolated) TPMS:

- **Cyber Access to Telematics System:** Cyber access to a telematics system enables remote interactions with MOST network, High-Speed CAN, Low-Speed CAN and LIN systems. Valasek and Miller [37] demonstrated that the telematics system of a 2015 Jeep Grand Cherokee telematics system can be accessed from anywhere with cellular network coverage. Connected vehicle services such as GM OnStar provide remote functionality, including door locking/unlocking, engine ignition and vehicle disabling in the event of theft [41]. Since connected vehicle services are made possible by the telematics system, access to the system enables the exploitation of all the connected vehicle services functionality.
- **Cyber Access to Infotainment System:** Cyber access to an infotainment system enables remote interactions with automobile applications software. Cyber access to the infotainment system in a MOST network may be leveraged to interact with systems in the High-Speed and Low-Speed CANs [30]. Cyber access to the infotainment system also enables connectivity to the Wi-Fi and Bluetooth modules.

  The Wi-Fi module provides Wi-Fi hotspot and Wi-Fi connectivity functionality. The Wi-Fi hotspot enables client devices to obtain cellular network connectivity via the telematics system. Wi-Fi connectivity enables an automobile to connect to a wireless network to stream media and download updates. Wi-Fi communications have ranges of hundreds of feet [25]. Services running on exposed ports may be accessible via the Wi-Fi hotspot and Wi-Fi connectivity, and are susceptible to exploitation. Vanhoef and Piessens [39] demonstrated vulnerabilities in Wi-Fi Protected Access (version 2), an outdated, but widely implemented, Wi-Fi security protocol that enables unauthorized network access and data interception.

  The Bluetooth module enables mobile device connectivity, media streaming and hands-free voice calling. Bluetooth communications have ranges of about 33 ft. The Bluetooth software stack has historically had vulnerabilities that can be exploited by denial-of-service and arbitrary code execution attacks [14].
- **Cyber Access to TPMS:** Cyber access to a connected TPMS enables interactions with the TPMS and, possibly, Low-Speed CAN systems. Figure 2 illustrates the two possibilities for TPMS connectivity in automobile networks. Specifically, a TPMS may be isolated from all the automobile networks or it may be connected to the Low-Speed CAN [37].

  A TPMS incorporates sensors that measure tire pressure and reports the pressure values via radio frequency communications. It is possible to reverse engineer TPMS messages and transmit false tire pressure data [37]. Automobile tracking capabilities via TPMS have been researched, but they appear to be impractical [3].

Table 3. Automobile network target functionality.

Target	Functionality
High-Speed CAN Systems	
Forward Collision System	Braking, Warning
Adaptive Cruise Control System	Acceleration, Braking
Lane Keep Assist System	Steering
Lane Departure Warning System	Warning
Automatic Parking System	Steering
Engine Start-Stop System	Ignition
Electronic Parking Brake System	Braking
Blind Spot Detection System	Warning
Telematics System	Remote Communications
Infotainment System	Information Reporting
Low-Speed CAN Systems	
Tire Pressure Monitoring System	Warning
Climate Control System	Comfort
Power Mirror Control System	Auxiliary Components
Windshield Wiper Control System	Auxiliary Components
Lighting Control System	Auxiliary Components
Telematics System	Remote Communications
Infotainment System	Information Reporting
MOST Network Systems	
Telematics System	Remote Communications
Infotainment System	Information Reporting
Microphone Array	Cabin Audio

5 Targets and Impacts

This section identifies the principal targets in a modern automobile network and describes the impacts of successful impacts on the targets.

5.1 Targets

Table 3 shows the targets in the High-Speed CAN, Low-Speed CAN and MOST network along with their functionality.

The High-Speed CAN connects several critical automobile systems. Advanced driver assistance systems that connect to the High-Speed CAN are the most attractive targets for attackers who wish to compromise automobile safety.

The Low-Speed CAN connects several non-critical automobile systems that can be targeted. The targets also include auxiliary devices implementing climate control and anti-theft functionality that are operated by Low-Speed CAN systems [37].

Table 4. Automobile network potential impacts.

Network	Targets	Potential Impacts
High-Speed CAN (HS-CAN)	*Direct Access* Advanced Driver Assistance HS-CAN Systems, Other HS-CAN Systems	Hazardous Operation, Non-Hazardous Operation
	Indirect Access LS-CAN Systems, TPMS, Microphone Array	Non-Hazardous Operation, Unauthorized Entry, Unauthorized Surveillance
Low-Speed CAN (LS-CAN)	*Direct Access* LS-CAN Systems, TPMS	Non-Hazardous Operation, Unauthorized Entry
	Indirect Access Advanced Driver Assistance HS-CAN Systems, Other HS-CAN Systems, Microphone Array	Hazardous Operation, Non-Hazardous Operation, Unauthorized Surveillance
LIN	*Direct Access* LS-CAN Systems, TPMS	Non-Hazardous Operation, Unauthorized Entry
MOST Network	*Direct Access* Microphone Array	Unauthorized Surveillance
	Indirect Access Advanced Driver Assistance HS-CAN Systems, Other HS-CAN Systems, LS-CAN Systems, TPMS	Hazardous Operation, Non-Hazardous Operation, Unauthorized Entry

The MOST network connects systems that enable external network connectivity and the microphone array. The microphone array may be used via the infotainment system and connected vehicle services to transmit live automobile cabin audio. Connected vehicle services have been used by law enforcement to acquire evidence in criminal investigations [7].

5.2 Impacts

The negative impacts of compromising automobile network targets are hazardous and non-hazardous automobile control, unauthorized surveillance and unauthorized entry. Table 4 shows the potential impacts of attacks on targets in the High-Speed CAN, Low-Speed CAN, LIN and MOST network.

6 Methodology and Implementation

This section describes the security analysis methodology and its implementation.

Telematics Communication Interface Control Module	**In the passenger compartment, left side of vehicle, under instrument panel on driver's side**

Fig. 3. Service manual entry specifying a target location.

6.1 Methodology

The security analysis methodology involves four steps, automobile target specification, automobile status specification, attack vector chaining and realization, and attack specification and impact analysis:

– **Automobile Target Specification:** This step involves the specification of the targets in an automobile of interest. Modern automobiles come with varying options and configurations, as a result, some targets may not be present in the automobile of interest and a few targets may be located in different networks. This step eliminates the targets that are not present in the automobile of interest and configures the existing targets in the various automobile networks.
The targets in a modern automobile can be specified after reviewing engineering documentation such as its user manual, service manual and wiring diagram:
  - *User Manual:* An automobile user manual lists the automobile systems and their functionality, and provides guidance on their use during automobile operation. A physical copy is typically located in the automobile glove compartment. Alternatively, a digital copy may be retrieved from the automobile manufacturer website at no cost.
  - *Service Manual:* A service manual provides detailed guidance about automobile service and maintenance procedures for the main automobile systems, which provide valuable information about potential targets. Service manuals are available for purchase online and at automobile parts stores. A service manual is useful for determining whether or not potential targets are installed in an automobile. Figure 3 shows a service manual entry specifying the location of the telematics system in an automobile.
  - *Wiring Diagram:* A wiring diagram, which specifies the connections of electrical components, also provides details about the electronic components (potential targets) installed in an automobile. Figure 4 shows a wiring diagram that specifies the connectivity of the telematics system in an automobile.
  Wiring diagrams may be available online. Alternatively, the diagrams may be purchased directly from automobile manufacturers or from third-party vendors.

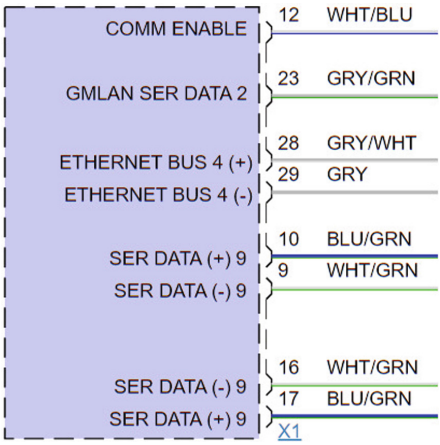

Fig. 4. Wiring diagram showing telematics system connectivity.

Examining automobile fuse blocks also assists in automobile target specification. A fuse block distributes electricity to all automobile systems and each fuse in the fuse block provides overcurrent protection for an automobile system (target). An automobile typically has at least two fuse blocks. One fuse block may be located in the engine bay near the 12 V battery whereas the other fuse block may be located in the cabin near the dashboard [12].

Fig. 5. Automobile fuse block.

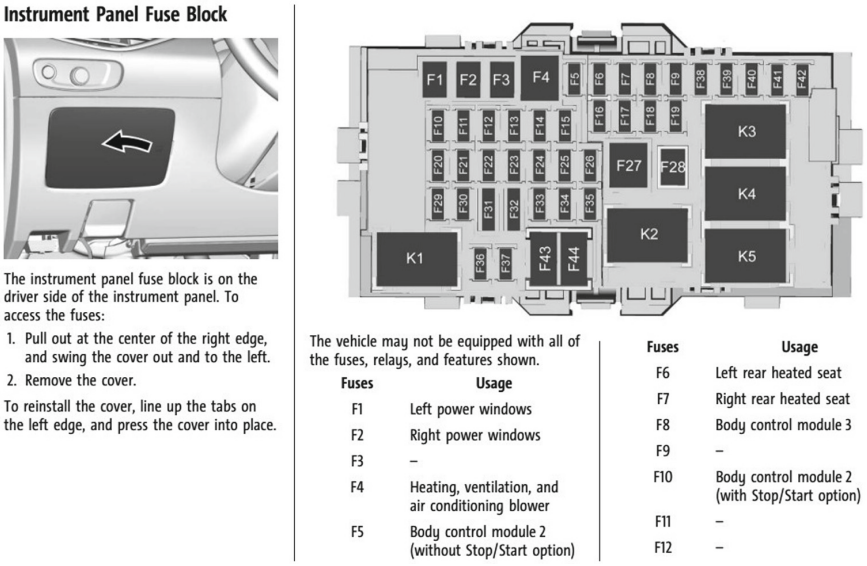

Fig. 6. User manual fuse block diagram.

Figure 5 shows an automobile fuse block. Each fuse block socket is assigned to an electrical system. The engineering documentation specifies the location and purpose of each fuse block socket.

Figure 6 shows a user manual listing each fuse socket location and fuse purpose. If a fuse block socket assigned to a target system in an automobile has a fuse installed, the target can be assumed to be present in the automobile. Otherwise, the target is unlikely to be present.

- **Automobile Status Specification:** This step involves the specification of the automobile status, which includes whether it is stationary or moving and whether or not it is possible to achieve engine ignition. Note that an automobile may be attacked when it is stationary or moving. Also, certain attack vectors are not realizable without automobile engine ignition. Clearly, engine ignition is active in a moving automobile. Engine ignition can be achieved in a stationary automobile by leveraging some of the physical access to automobile interior subvectors or the cyber access to telematics system vector via its connected vehicle services subvector.
- **Attack Vector Chaining and Realization:** This step chains individual attack vectors and subvectors to determine target reachability. This is followed by the specification of the realized attack vectors to identify the automobile targets that become accessible.
- **Attack Specification and Impact Analysis:** This step involves the specification of attacks on the accessible automobile targets. The attacks produce impacts – hazardous operation, non-hazardous operation, unauthorized entry and unauthorized surveillance – depending on target functionality and attack

High Severity Targets	Medium Severity Targets	Low Severity Targets
Adaptive Cruise Control	Exterior Lighting	Anti-Theft
Alternator	Horn/Panic Alarm	Blind Spot Detection
Anti-Lock Braking	Pedestrian Warning (Electric/Hybrid)	Climate Control
Automatic Parking	Turn Signals	Electronic Stability Control
Electronic Parking Brake	Windshield Wiper	Heads-Up Display
Engine Control Unit		Infotainment System
Engine Start-Stop		Instrument Cluster
Forward Collision		Interior Lighting
Four-Wheel Drive		Lane Departure Warning
Four-Wheel Steering		Microphone Array
Lane Keep Assist		Pedal Adjustment
Powertrain		Power Mirrors
Standard Cruise Control		Power Windows
Trailer Control		Remote Ignition
		Seat Adjustment
		Seatbelt/Seat Weight Detection
		Steering Wheel Adjustment
		Telematics System
		Tire Pressure Monitoring System

Fig. 7. Automobile target specification view.

type. Section 5.2 presents the potential impacts caused by successful attacks on automobile targets.

6.2 Implementation

A user-friendly visualization tool was written in Microsoft Excel and Visual Basic Scripting Edition to support automobile security analyses. In particular, the tool supports configurable security analyses, conveying automobile risk exposures in terms of their attack surfaces, exploitable targets and impacts. The tool accommodates the specification of diverse automobile cyber anatomies and configurations. The attack vectors, targets and impacts are customizable to support new technologies and advanced safety, convenience and comfort features as they are incorporated in automobiles.

Figure 7 shows the automobile target specification view that lists the available targets and provides options to connect targets (checked boxes) and disconnect targets (unchecked boxes). Because a disconnected target is omitted from further consideration in the methodology, this feature supports what-if analyses.

	ENGINE IGNITION
☑	Stationary Automobile
☐	Moving Automobile

Fig. 8. Automobile status specification view.

Access	Realize	Req. Ignition	Attack Vector	Networks
▩	▩	☑	Physical Access to High-Speed CAN	HS-CAN
▩	▩	☑	Physical Access to Low-Speed CAN	LS-CAN
▩	▩	☑	Physical Access to LIN	LS-CAN, LIN
▩	▩	☑	Physical Access to MOST Network	MOST
▩	▩	☑	Physical Access to Network Gateway	HS-CAN, LS-CAN, LIN, MOST
☑	☑	☐	Physical Access to On-Board Diagnostics Interface	HS-CAN, LS-CAN, LIN, MOST

Fig. 9. Attack vector chaining and realization view.

Figure 8 shows the automobile status specification view, which provides stationary or moving automobile options. A stationary automobile attack is selected (checked box). Note that engine ignition is highlighted, corresponding to the default situation that the stationary vehicle is off.

Figure 9 shows the attack vector chaining and realization view. As mentioned above, individual attack vectors and subvectors are chained to determine target reachability. The require ignition component determines whether engine ignition is needed (checked box) or not needed (unchecked box) before an attack vector may be realized. The black boxes indicate the attack vectors that are not accessible or realizable until engine ignition is gained. The physical access to OBD attack vector is realizable because ignition is not required for physical access.

Execute	**Surveillance**
Execute	**Eavesdropping**
Execute	**Denial-of-Service**
Execute	**Message Injection**

Fig. 10. Attack execution subview.

Figure 10 shows the attack execution subview of the attack specification and impact analysis view. Four attacks, surveillance, eavesdropping, denial-of-service and message injection, may be executed on accessible targets to produce impacts:

- **Surveillance Attack:** A surveillance attack collects information about an automobile and/or its occupants. Examples include automobile location and cabin audio, including occupant conversations. A surveillance attack has a non-hazardous operation impact.
- **Eavesdropping Attack:** An eavesdropping attack collects messages transmitted between automobile targets. The messages could be analyzed to develop and execute additional attacks. An eavesdropping attack has a non-hazardous operation impact.
- **Denial-of-Service Attack:** A denial-of-service attack interrupts automobile network communications, resulting in a hazardous operation impact.

Low Severity Targets	Impacts		
Anti-Theft	NHO	UE	
Blind Spot Detection	NHO		
Climate Control	NHO		
Electronic Stability Control	NHO		
Infotainment System	NHO		
Instrument Cluster	NHO		
Interior Lighting	NHO		
Lane Departure Warning	NHO		
Microphone Array	NHO		US
Power Mirrors	NHO		
Power Windows	NHO		
Remote Ignition	NHO		
Seat Adjustment	NHO		
Seatbelt/Seat Weight Detection	NHO		
Steering Wheel Adjustment	NHO		
Telematics System	NHO	UE	US
Tire Pressure Monitoring System	NHO		

Fig. 11. Attack specification and impact analysis view.

– **Message Injection Attack:** A message injection attack transmits crafted messages for a malicious purpose, resulting in a hazardous operation impact.

Figure 11 shows the attack specification and impact analysis view, which displays the targets and their potential impacts. The targets and their associated attack impacts are highlighted in different colors according to their status. The four types of targets and their associated impact status are:

– **Disconnected Target:** A disconnected target is highlighted in black. A disconnected target is not present in the automobile and, therefore, is neither accessed nor attacked.
– **Accessible Target:** A target that is potentially accessible by an (unrealized) attack vector is highlighted in light gray. The impact, highlighted in light gray, indicates that the potential exists for a negative outcome if an attack vector is realized to access the target and a successful attack is executed on the target.
– **Accessed Target:** A target that has been accessed via a realized attack vector is highlighted in gray. The impact, highlighted in gray, indicates that the potential exists for a negative outcome because an attack vector enabling access the target is realized, providing an opportunity to attack the target.
– **Attacked Target:** A target that is successfully accessed and attacked is highlighted in dark gray with white text. The impact, highlighted in dark gray with white text, indicates that the negative outcome is realized.

7 Case Study

The visualization tool was used to conduct security analyses of five representative automobiles that consider their attack surfaces, targets and impacts. The automobiles were selected due to their presence in U.S. Government fleets. The automobiles comprise two vehicle classes, sport utility vehicles and sedans, representing a combined 26% of U.S. Government fleets during the 2020 fiscal year [36]. The five automobile models represent three motor groups with a combined 39% of the U.S. market share in 2021 [32].

The case study considers stationary automobiles in a rental car scenario where the automobile key fobs are available. Physical access to the automobile interior via the key fob attack vector is leveraged and realized, following which engine ignition is achieved. Subsequently, the physical access to the OBD interface and physical access to the network gateway attack vectors are both leveraged and realized. After the attack vectors are realized, surveillance, eavesdropping, denial-of-service and message injection attacks are executed on the automobile targets. The impacts of successful attacks include hazardous operation (HO), non-hazardous operation (NHO), unauthorized entry (UE) and unauthorized surveillance (US).

7.1 Automobile Security Analyses

This section describes the five automobiles in the case study and presents the results of the automobile security analyses that consider surveillance, eavesdropping, denial-of-service and message injection attacks. For security reasons, the makes and models of the five automobiles are not specified. Table 5 shows the high, medium and low severity targets present in the five automobiles.

- **Automobile A:** Automobile A is a domestic, full-size sport utility vehicle with a six-cylinder engine. The spacious automobile seats up to eight passengers.
- **Automobile B:** Automobile B is a domestic, full-size sport utility vehicle with an eight-cylinder engine. The spacious automobile seats up to eight passengers.
- **Automobile C:** Automobile C is a domestic, full-size sedan with a four-cylinder engine. The automobile seats up to five passengers.
- **Automobile D:** Automobile D is a domestic, full-size sedan with a six-cylinder engine. The automobile seats up to five passengers and is optimized for performance.
- **Automobile E:** Automobile E is a domestic, mid-size sport utility vehicle with a six-cylinder engine. The spacious automobile seats up to seven passengers.

Table 5. Automobile targets.

Target	Automobile				
	A	B	C	D	E
High Severity Targets					
Adaptive Cruise Control					✓
Alternator	✓	✓	✓	✓	✓
Anti-Lock Braking	✓	✓	✓	✓	✓
Automatic Parking					✓
Electronic Parking Brake	✓	✓			
Engine Control Unit	✓	✓	✓	✓	✓
Engine Start-Stop	✓	✓	✓		
Forward Collision		✓			✓
Four-Wheel Drive	✓				
Four-Wheel Steering					
Lane Keep Assist	✓				✓
Powertrain	✓	✓	✓	✓	✓
Standard Cruise Control	✓	✓	✓	✓	✓
Trailer Control	✓	✓			
Medium Severity Targets					
Exterior Lighting	✓	✓	✓	✓	✓
Horn/Panic Alarm	✓	✓	✓	✓	✓
Pedestrian Warning					
Turn Signals	✓	✓	✓	✓	✓
Windshield Wiper	✓	✓	✓	✓	✓
Low Severity Targets					
Anti-Theft	✓	✓	✓	✓	✓
Blind Spot Detection					✓
Climate Control	✓	✓	✓	✓	✓
Electronic Stability Control	✓	✓	✓	✓	✓
Heads-Up Display					
Infotainment System	✓	✓	✓	✓	✓
Instrument Cluster	✓	✓	✓	✓	✓
Interior Lighting	✓	✓	✓	✓	✓
Lane Departure Warning	✓				✓
Microphone Array	✓	✓	✓	✓	✓
Pedal Adjustment					✓
Power Mirrors	✓	✓	✓	✓	✓
Power Windows	✓	✓	✓	✓	✓
Remote Ignition	✓	✓	✓	✓	✓
Seat Adjustment	✓	✓	✓	✓	✓
Seatbelt/Seat Weight Detection	✓	✓	✓	✓	✓
Steering Wheel Adjustment	✓	✓			✓
Telematics System	✓	✓	✓		
Tire Pressure Monitoring System	✓	✓	✓	✓	✓

7.2 Risk Comparison

Table 6 shows the numbers of high severity, medium severity and low severity targets in the five automobiles in the case study. The automobiles are listed in rank order based on the total number of targets with ties being broken based on the numbers of high severity, medium severity and, finally, low severity targets.

As expected, Automobile A, a high-end sport utility vehicle with loaded features, is tied for the most number of targets and has the most number of high severity targets. Automobile E, a high-end sport utility vehicle with loaded features, is tied for the most number of targets and has just one high severity target less than Automobile A. A key security feature of Automobile E is that it does not have a telematics system, which reduces its attack surface and exposure to remote attacks due its lack of cellular network connectivity. Automobile B is also a high-end sport utility vehicle but not as loaded as Automobiles A and E; it has just one less high severity target and one less low severity target than Automobile A.

Automobiles C and D are economy sedans with fewer features than Automobiles A, B and E. Automobile D has the fewest targets overall. Also, it does not have a telematics system, which reduces its attack surface and exposure to remote attacks.

Table 7 shows the types and numbers of impacts realized by successful surveillance, eavesdropping, denial-of-service and messaging attacks on the five automobiles in the case study. Note that the automobiles are listed in rank order based on the total number of impacts.

The results in Table 7 parallel those in Table 6. As expected, the high-end sport utility vehicles with loaded features have significantly more negative impacts than the economy sedans. Automobiles D and E that do not have telematics systems have less exposure to surveillance attacks than the other automobiles. Eavesdropping attacks, which are passive in nature, induce non-hazardous operation impacts on all five automobiles.

In contrast, denial-of-service and message injection, which are active attacks, induce numerous hazardous operation impacts. Message injection attacks are more serious than denial-of-service attacks because they target the anti-theft system, microphone array and telematics system, inducing additional impacts.

Table 6. Automobile targets.

Automobile	High Severity Targets	Medium Severity Targets	Low Severity Targets	Total
Automobile A	10	4	16	30
Automobile E	9	4	17	30
Automobile B	9	4	15	28
Automobile C	6	4	14	24
Automobile D	5	4	13	22

Table 7. Automobile attack impacts.

Automobile	Surveillance Attack Impacts	Eavesdropping Attack Impacts	Denial-of-Service Attack Impacts	Message Injection Attack Impacts	Total
Automobile A	NHO: 1; US: 2	NHO: 30	HO: 10; NHO: 30	HO: 10; NHO: 30; UE: 2; US: 2	117
Automobile E	NHO: 1; US: 1	NHO: 30	HO: 9; NHO: 30	HO: 9; NHO: 30; UE: 1; US: 1	112
Automobile B	NHO: 1; US: 2	NHO: 28	HO: 9; NHO: 28	HO: 9; NHO: 28; UE: 2; US: 2	109
Automobile C	NHO: 1; US: 2	NHO: 24	HO: 6; NHO: 24	HO: 6; NHO: 24; UE: 2; US: 2	91
Automobile D	NHO: 1; US: 1	NHO: 22	HO: 5; NHO: 22	HO: 5; NHO: 22; UE: 1; US: 1	80

HO: Hazardous operation, NHO: Non-hazardous operation, UE: Unauthorized entry, US: Unauthorized surveillance

8 Conclusions

The incorporation of highly-networked computing systems that automatically control vital functions in modern automobiles raises significant security concerns. Unfortunately, because modern automobiles have complex and diverse cyber anatomies, configurations and features, it is difficult to comprehend and evaluate their risk exposures.

The security analysis methodology described in this chapter engages generic, albeit configurable, automobile attack surfaces along with configurable targets that may be attacked to cause negative impacts. In particular, the methodology relies on detailed descriptions of the cyber anatomies of modern automobiles that specify their network architectures, underlying systems and networks, network connectivity and the many physical and cyber attack vectors that constitute their attack surfaces. Reachability analysis is employed to chain the realizable attack vectors and determine all the accessible targets. Attack opportunities made possible by the realized physical and cyber attack vectors are identified, following which the impacts on an automobile and its occupants are determined.

The security analysis case study illustrates the advantages of the methodology. In particular, the methodology provides rapid insights into the risk exposures of modern automobiles in terms of attack surfaces, targets and impacts, enabling risk comparisons between automobiles of diverse makes and models. Additionally, the methodology facilitates cyber operations and cyber defense

postures on automobiles. Cyber operations analysts can leverage the methodology as a playbook to develop sophisticated targeting of automobiles. Cyber defense analysts can draw on the attack vectors, reachable targets and possible attacks and their impacts to steer efforts directed at reducing risk by helping articulate and prioritize mitigations and security controls. The methodology also supports effective security analyses without drawing on extensive subject-matter knowledge, expensive experimentation and complex computations. Individuals and enterprises can rapidly assess and compare the complex security environments of automobiles as they consider alternatives for purchase, lease or rent. Additionally, it is possible to evaluate the security environments of new automobiles with evolving technologies, systems and features.

Acknowledgment. This research was supported by the National Science Foundation under Grant no. DGE 1501177.

References

1. Alfa Network, AWUS1900, Taipei City, Taiwan (2022). (www.alfa.com.tw/products/awus1900)
2. Allan, M.: "Serious" security flaws expose popular Ford and VW cars to hackers, Banbury Guardian, 13 April 2020
3. Ashworth, J., Staggs, J., Shenoi, S.: Radio frequency identification and tracking of vehicles and drivers by exploiting keyless entry systems. Int. J. Crit. Infrastruct. Prot. **40** (2023). Article no. 100587
4. Blanco, S.: Car hacking danger is likely closer than you think, Car and Driver, 4 September 2021
5. Bosch, CAN Specification, Version 2.0, Stuttgart, Germany (1991). (esd.cs.ucr.edu/webres/can20.pdf)
6. Bozdal, M., Samie, M., Aslam, S., Jennions, I.: Evaluation of CAN bus security challenges. Sensors **20**(8) (2020). Article no. 2364
7. Brewster, T.: Cartapping: How feds have spied on connected cars for 15 years, Forbes, 15 January 2017
8. California Air Resources Board, On-Board Diagnostic II (OBD II) Systems Fact Sheet, Sacramento, California, 19 September 2019. (ww2.arb.ca.gov/resources/fact-sheets/board-diagnostic-ii-obd-ii-systems-fact-sheet)
9. Checkoway, S., et al.: Comprehensive experimental analyses of automotive attack surfaces. In: Proceedings of the Twentieth USENIX Security Symposium, pp. 77–92 (2011)
10. Cowell, K.: Engine stop/start systems on non-hybrid vehicles, Car and Driver, 4 March 2011
11. Dimov, D.: Tesla Model 3 vulnerability: What you need to know about the web browser bug, Infosec Blog, Infosec Institute, Madison, Wisconsin, 5 August 2020. (resources.infosecinstitute.com/topic/tesla-model-3-vulnerability-what-you-need-to-know-about-the-web-browser-bug)
12. Duffy, J.: Modern Automotive Technology. Goodheart-Wilcox Company, Tinley Park (2017)
13. Ettus Research, USRP B210 (board only), Austin, Texas (2022). (www.ettus.com/all-products/ub210-kit)

14. Garbelini, M., Chattopadhyay, S., Bedi, V., Sun, S., Kurniawan, E.: Brak-Tooth: Causing Havoc on Bluetooth Link Manager, Vulnerability Disclosure Report, Singapore University of Technology and Design, Singapore (2021). (asset-group.github.io/disclosures/braktooth/braktooth.pdf)
15. Great Scott Gadgets, Throwing Star LAN Tap, Lakewood, Colorado (2022). (greatscottgadgets.com/throwingstar)
16. Greenberg, A.: Hackers remotely kill a Jeep on the highway - With me in it, Wired, 21 July 2015
17. Greenberg, A.: After Jeep hack, Chrysler recalls 1.4M vehicles for bug fix, Wired, 24 July 2015
18. HEAVENS Consortium, Healing Vulnerabilities to Enhance Software Security and Safety, Volvo Technology, Goteborg, Sweden (2016). (www.autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf)
19. Jeffs, J.: A history of ADAS: Emergence to essential, IDTech-Ex, Cambridge, United Kingdom, 4 January 2022. (www.idtechex.com/en/research-article/a-history-of-adas-emergence-to-essential/25592)
20. Kosche, C.: How many connected cars are sold worldwide? Smartcar Blog, Smartcar, Mountain View, California, 15 April 2021. (www.smartcar.com/blog/connected-cars-worldwide)
21. Koscher, K., et al.: Experimental security analysis of a modern automobile. In: Proceedings of the IEEE Symposium on Security and Privacy, pp. 447–462 (2010)
22. Lin, T., Chen, L.: Common attacks against car infotainment systems. Presented at the Automotive Linux Summit (2019)
23. Linder, C.: Five impressive ways criminals use wireless signals to steal everything - Even your car, Popular Mechanics, 27 November 2019
24. McFarland, M.: Teen's Tesla hack shows how vulnerable third-party apps may make cars, CNN, 2 February 2022
25. Mitchell, B.: What is the range of a typical Wi-Fi network? Lifewire, New York (2020). (www.lifewire.com/range-of-typical-wifi-network-816564)
26. Moller, D., Haas, R.: Guide to Automotive Connectivity and Cybersecurity: Trends, Technologies, Innovations and Applications. Springer, Cham (2019)
27. MZD-AIO Contributors, MZD-AIO, GitHub (2020). (github.com/Trevelopment/MZD-AIO)
28. National Highway Traffic Safety Administration, 49 CFR §571.138 - Standard No. 138, Tire Pressure Monitoring Systems, Washington, DC (2011). (www.govinfo.gov/content/pkg/CFR-2011-title49-vol6/pdf/CFR-2011-title49-vol6-sec571-138.pdf)
29. Richards, P.: A CAN Physical Layer Discussion, Application Note AN228, Microchip Technology, Chandler, Arizona (2002). (ww1.microchip.com/downloads/en/appnotes/0228a.pdf)
30. Smith, C.: The Car Hacker's Handbook: A Guide for the Penetration Tester. No Starch Press, San Francisco (2016)
31. Software Radio Systems, srsRAN 22.04 Documentation, Cork, Ireland (2022). (docs.srsran.com/en/latest)
32. Statista, Estimated U.S. market share held by selected automotive manufacturers in 2021, Hamburg, Germany (2022). (www.statista.com/statistics/249375/us-market-share-of-selected-automobile-manufacturers)
33. Taylor, J.: There's no stopping the electric parking brake, Auto Service Professional, 16 February 2018
34. Tutorials Point, Ethical hacking - Wireless hacking, Hyderabad, India (2022). (www.tutorialspoint.com/ethical_hacking/ethical_hacking_wireless.htm)

35. UAB 8 Devices, Korlan USB2CAN, Vilnius, Lithuania (2022). (www.8devices.com/pro ducts/usb2can_korlan)
36. U.S. General Services Administration, FY 2020 Federal Fleet Open Data Set, Washington, DC (2021). (www.gsa.gov/cdnstatic/FY2020FederalFleetReport.xlsx)
37. Valasek, C., Miller, C.: A Survey of Remote Automotive Attack Surfaces. Technical White Paper, IOActive, Seattle, Washington (2014)
38. Valasek, C., Miller, C.: Remote Exploitation of an Unaltered Passenger Vehicle. Technical White Paper, IOActive, Seattle, Washington (2015)
39. Vanhoef, M., Piessens, F.: Key reinstallation attacks: forcing nonce reuse in WPA2. In: Proceedings of the Twenty-Fourth ACM Conference on Computer and Communications Security, pp. 1313–1328 (2017)
40. Wang, Y., Wang, Y., Qin, H., Ji, H., Zhang, Y., Wang, J.: A systematic risk assessment framework of automotive cybersecurity. Autom. Innov. **4**(3), 253–261 (2021)
41. Yarkoni, O.: The danger of connected car mobile apps to OEMs and smart mobility services, Upstream Blog, Novi, Michigan, 19 January 2022. (www.upstream.auto/blog/mobile-apps-pose-major-threat)