DRIVING WITH SHARKS

Rethinking Connected Vehicles with Vehicle Cybersecurity

Mahmoud Hashem Eiza and Qiang Ni

Digital Object Identifier 10.1109/MVT.2017.2669348
Date of publication: 24 April 2017

In a public service announcement on 17 March 2016, the Federal Bureau of Investigation jointly with the U.S. Department of Transportation and the National Highway Traffic Safety Administration (NHTSA) released a warning regarding the increasing vulnerability of motor vehicles to remote exploits [18]. Engine shutdowns, disabled brakes, and locked doors are a few examples of possible vehicle cybersecurity attacks. Modern cars grow into a new target for cyberattacks as they become increasingly connected. While driving on the road, sharks (i.e., hackers) need only to be within communication range of a vehicle to attack it. However, in some cases, they can hack into it while they are miles away. In this article, we aim to illuminate the latest vehicle cybersecurity threats including malware attacks, on-board diagnostic (OBD) vulnerabilities, and automobile apps threats. We illustrate the in-vehicle network architecture and demonstrate the latest defending mechanisms designed to mitigate such threats.

Hackable, Exposed Vehicles

Currently, vehicles are no longer isolated mechanical machines used solely for transportation. Consumers increasingly demand a seamless connected experience in all aspects of their lives including driving. With the introduction of telematics, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, and the integration of smartphones and Bluetooth devices, connected vehicles

While increasing autonomy and connectivity in vehicles brings many improvements in terms of functionality and convenience, it also brings with it a new cyberthreat.

represent an ecosystem that is part of a fully connected world. In fact, connected vehicles are an integral part of the smart city vision and a node in the world of the Internet of Things. Meanwhile, the vehicles themselves are now controlled by hundreds of electrical control units (ECUs) that form an internal network of devices within the vehicle. While increasing autonomy and connectivity in vehicles brings many improvements in terms of functionality and convenience, it also brings with it a new cyberthreat, as vehicles become a new target for attackers or hackers [1].

As more software applications are integrated into modern vehicles, we propose to play the following game of words: if you see the word "software," replace it with "hackable"; and if you see the word "connected," replace it with "exposed." As it stands, you can imagine that while driving your hackable, exposed modern car, you are surrounded by sharks. These sharks can try to hack into your vehicle and may cause real damage that cannot be reversed. Since this is a life-threatening issue (i.e., considered a lethal cyberattack), in April 2016, the Michigan state senate proposed two bills that introduce life sentences in prison for people who hack into vehicles' electronic systems [2].

In July 2015, two researchers, Charlie Miller and Chris Valasek, hacked into the Cherokee Jeep from Miller's basement while the car itself was placed on the highway 10 mi away [3]. They were able to remotely control the car functions using a simple third-generation (3G) connection exploiting a vulnerability in the Uconnect software. Uconnect is Internet-connected software that controls the navigation and entertainment systems in the vehicle. Through the discovered Uconnect's cellular vulnerability, which represents the attacking entry point, they had the ability to rewrite the firmware of the adjacent chip in the car's head unit. Consequently, they sent commands through the in-vehicle network, which is illustrated in the "In-Vehicle Network Architecture" section, to disable the brakes, take control over the steering wheel, and finally send the vehicle into a ditch. This cyber-carjacking incident caused the recall of 1.4 million cars.

In fact, it is not only the problem of Chrysler vehicles with Uconnect software. Similar attacks have been recently reported against other manufacturers' vehicles. For example, in June 2016, a Mitsubishi Outlander plug-in hybrid electric vehicle (PHEV) was hacked. Security researchers at Pentest Partners [4] performed a man-in-the-middle attack between the PHEV's mobile app and the PHEV's Wi-Fi access point (AP). After replaying various messages from the mobile app, they figured out the binary protocol used for messaging. Consequently, they were able to turn the lights on and off and disable the whole theft alarm system, leaving the vehicle vulnerable to more attacks.

Garcia et al. [5] showed that almost 100 million Volkswagen vehicles sold between 1995 and 2016 are vulnerable to remote, keyless-entry hacks. Volkswagen vehicles depend on a few global master keys that can be recovered from ECUs. This way, the attacker can clone a Volkswagen remote control and, by eavesdropping on a single signal sent by the original remote, gain unauthorized access to the vehicle.

Through a vulnerability in the NissanConnect mobile application, which controls Nissan Leaf electric vehicles, attackers took control over the heater in the car and repeatedly turned it on to drain the battery. This incident forced Nissan to disable that application [6]. An attacker within the SmartGate in-car Wi-Fi range of the SmartGate-enabled Škoda car can steal information about the car [7]. Moreover, the attacker can lock out the car's owner from the SmartGate system. Finally, using a laser pointer and a Raspberry Pi, Jonathan Petit, a security researcher, is able to interfere with the light detection and ranging (LIDAR) systems of the self-driving car to trick it into thinking that there are obstacles (i.e., other cars or pedestrians) ahead of it [8]. This trick can cause a self-driving car at full speed to stop, thus disabling the car. Self-driving cars depend on LIDAR systems, which create a three-dimensional map to navigate and avoid any potential hazard or obstacle in the Petit simply fires his laser pointer, which is pulsed by the Raspberry Pi, at the self-driving car. When it is picked up, the LIDAR unit is tricked into seeing illusory objects when turning right. Consequently, the car immediately stops. This attack worked up to 100 m away in any direction and did not require a tightly focused beam.

Physical access to the car is no longer a precondition to hack into it. Sharks on the road need only to be in communication range of the targeted vehicle (e.g., its Wi-Fi range) to gain important information and even take control of the vehicle's most critical functions. However, in some cases, like in the Uconnect software attack, the sharks can be miles away from the targeted vehicle. Besides taking over control of the steering wheel and disabling the brakes, a simple and sudden airbag deployment while driving on a highway represents a lethal cyberattack that could cause the vehicle to crash and claim lives.

In practice, besides recalling the vulnerable cars and offering over-the-air (OTA) updates, the auto industry should respond in a better way to avoid embarrassing hacks and costly recalls. The last reported incidents

were the motive for a series of events that brought together many car manufacturers along with law agencies and governmental bodies (e.g., see [9]). The aim of these events was to put in place an effective strategy to share information, raise threat awareness across the auto industry, listen to consumers' concerns about security and privacy, learn about the required legislation, and put vehicle information technology at the center of the development process. Yet more efforts are needed to address vehicle cybersecurity concerns.

In-Vehicle Network Architecture (Automotive Network)

To develop an understanding of the potential entry points (i.e., attacking points) that the hackers can expose in the modern car, in this section, we illustrate the in-vehicle network architecture, also known as the *automotive network*, in detail. Modern cars contain 30–100 ECUs, which are embedded computers that communicate with each other, creating the in-vehicle network [10]. The ECUs' intercommunication is essential to efficiently monitoring and configuring different vehicular subsystems. Figure 1 shows that the in-vehicle network is composed of many electronic subsystems, including embedded telematics, body and comfort control, vehicle safety, powertrain, on-board video cameras, and in-vehicle infotainment (IVI) [11]. Each subsystem contains many ECUs,

BESIDES RECALLING THE VULNERABLE CARS AND OFFERING OVER-THE-AIR UPDATES, THE AUTO INDUSTRY SHOULD RESPOND IN A BETTER WAY TO AVOID EMBARRASSING HACKS AND COSTLY RECALLS.

each of which controls a specific functionality in the vehicle. For instance, the ECUs that control the airbag deployment and the antilock braking system (ABS) are found in the vehicle safety subsystem, while the ECUs that provide engine control and suspension control are found in the powertrain subsystem.

To guarantee the desired functionality and on-time response to critical events, ECUs of the same or different subsystems need to communicate with each other. Based on the time sensitivity of the provided functionality, different in-vehicle subnetworks are utilized. For instance, a high-speed controller area network (CAN) is used for time-critical engine control, safety subsystems, and powertrains, while a local interconnect network is used for the less time-sensitive body and comfort control subsystems [11]. To support audio, video, and on-board cameras, media-oriented systems transport and Ethernet are employed in the IVI subsystem. These networks are interconnected through

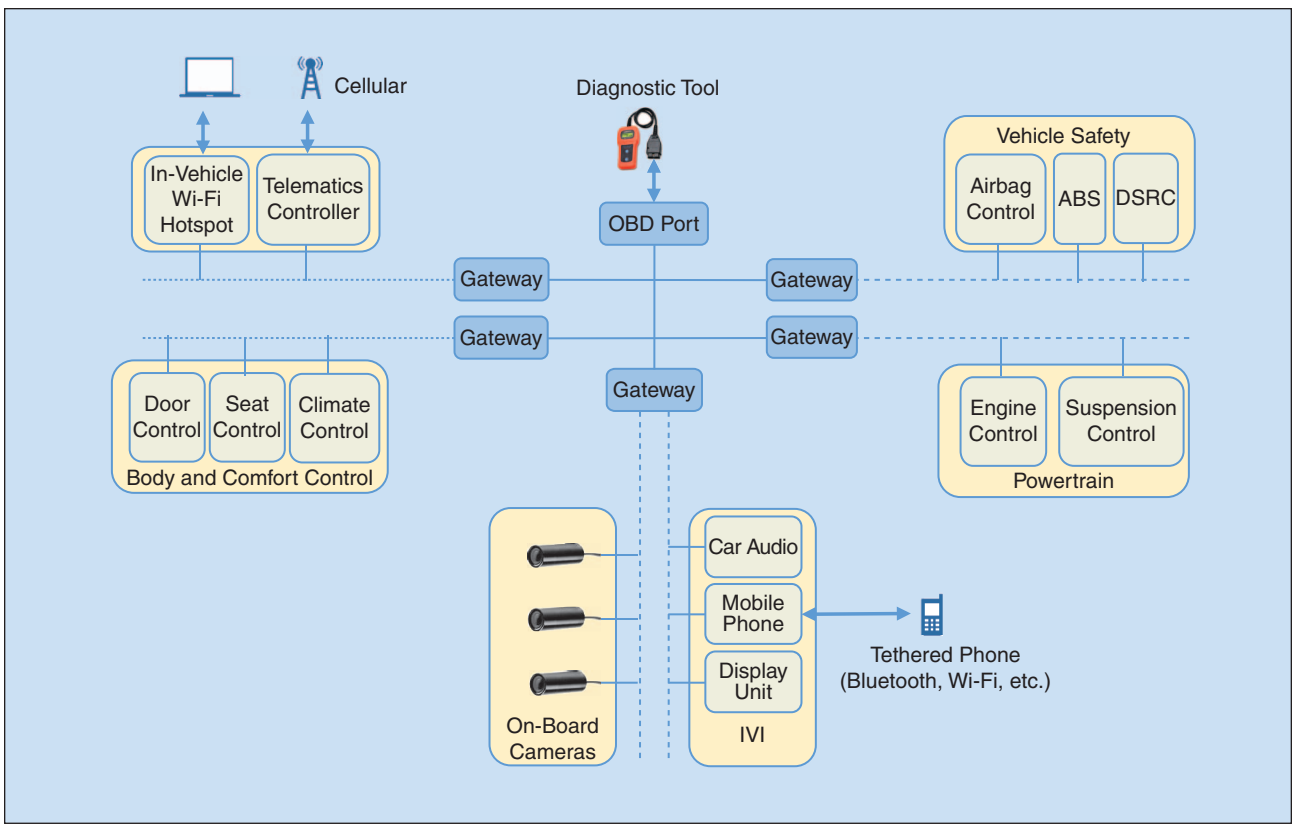

FIGURE 1 In-vehicle (automotive) network architecture [11].

MODERN CARS CONTAIN 30–100 ECUs, WHICH ARE EMBEDDED COMPUTERS THAT COMMUNICATE WITH EACH OTHER, CREATING THE IN-VEHICLE NETWORK.

gateways that control the messages that flow through the subsystems as showed in Figure 1. At the same time, these gateways are interconnected through high-speed CAN buses.

Given the recent trends of connecting different devices through universal serial buses (USBs), Bluetooth, Wi-Fi, 3G, fourth-generation (4G), and fifth-generation (5G) [19], and so on, each in-vehicle network subsystem implements its own communication module to connect to the outside world. For instance, IVI allows both wireless communication through Bluetooth and wired communication through USB. Cellular communication is implemented in the embedded telematics subsystem that can offer a Wi-Fi AP. Moreover, modern vehicles are now fitted with OBD ports that are utilized for vehicle inspection, ECU firmware updates, and repair. Furthermore, the OBD port allows full access to the in-vehicle network.

As a result, the variety and the increasing number of connection points in each in-vehicle network subsystem make the vehicle more accessible from the outside world and, consequently, more vulnerable to different cyberattacks. Indeed, each communication interface with the outside world should be protected. However, protecting each entry point separately will result in duplicate security functions on the same vehicle. Moreover, restrictions such as limited computational power and storage capabilities should be considered.

Cyberthreat Vectors Against Connected Vehicles

As previously explained, connected vehicles have a broad cyberattack surface where the attacker can gain control over the vehicle. Keyless, Wi-Fi, Bluetooth, dedicated short-range communications (DSRC), OBD systems, USBs, and automobile apps are a few examples of attack entry points for connected vehicles, which are illustrated in Figure 2. In the following sections, we explain four cyberthreat vectors against connected vehicles: OBD threats, DSRC security issues, malware attacks, and mobile auto apps threats.

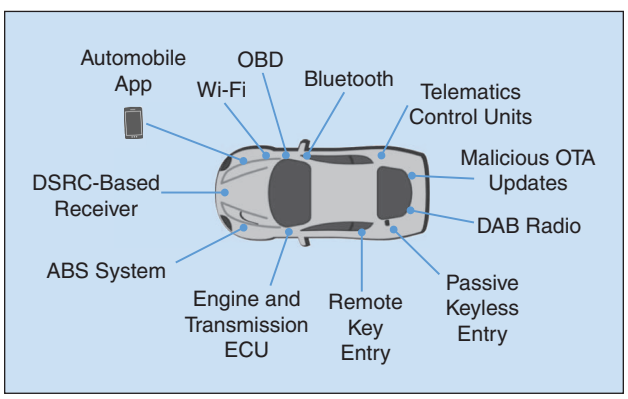

FIGURE 2 The connected vehicle's security–potential cyberthreat vectors. DAB: digital audio broadcasting.

OBD Threats

The implementation of OBD systems has been mandatory in vehicles sold in the United States since 1996, in gasoline-powered vehicles in the European Union (EU) since 2001, and in diesel-powered vehicles in the EU since 2004 [10]. The OBD port is primarily used to allow cars to report any problem in its infrastructure and communicate the diagnostic data collected by its sensors to the outside world. This allows the service provider to fix the reported problems. OBD dongles are used to interface with the OBD port and consequently access the CAN within the vehicle. These OBD dongles can be purchased by anyone, and they are fairly inexpensive. OBD ports are considered as entry points to attack the ECUs that are connected to the CAN buses. The authors in [12] showed how an automotive virus can be injected into the ECUs through the OBD port and trigger specific messages on the bus (e.g., door locks) when specific conditions are met.

While the attack in [12] required physical access to the vehicle, modern cars now allow OBD dongles to be remotely controlled by a Wi-Fi connection from a computer. In [13], vulnerabilities in the application program interface of a pass-through device (i.e., an OBD dongle) allowed the attacker to inject a malicious code into it. This malicious code made the pass-through device emit malicious packets on the CAN buses every time it was plugged into a different vehicle. In a recent survey [14], more than 50% of the surveyed OBD dongles were vulnerable to hacking. Weak encryption, exposed keys, and communication hijacking were the top three security flaws in these dongles.

DSRC Security Issues

V2V and V2I communications are key technologies to offer a class of safety services for connected vehicles that can prevent collisions and save lives. DSRC technology has been developed for use in V2V and V2I communications, where each vehicle is assumed to be equipped with a DSRC on-board unit. DSRC communications utilize several standards such as IEEE 802.11p [20] wireless access in vehicular environment for physical layer and medium access control functions, IEEE 1609.2 [21] for security services, and IEEE 1609.3 [22] for network services.

To achieve its goal, DSRC-equipped vehicles are expected to communicate (i.e., send, receive, and relay) information to other DSRC-equipped vehicles and/or infrastructure such as roadside units. This principle opens the door for malicious nodes to either hack into DSRC-equipped vehicles or cause damages by sending fake safety information.

Therefore, IEEE 1609.2 [23] defines standard mechanisms to authenticate and encrypt messages in DSRC. Nevertheless, attacks such as denial of service (DoS) are still possible. Lyamin et al. [15] investigated the jamming DoS attacks in IEEE 802.11p that are possible when a malicious node corrupts the exchanged safety messages in a platoon. Furthermore, they proposed a simple, real-time detector of jamming DoS attacks in vehicular networks. Besides jamming DoS attacks, malware, global positioning system spoofing, location tracking, masquerading attacks (when a malicious node uses a fake identity to trick other nodes to send/receive false information) and black hole attacks (a type of DoS attack where a malicious node drops all messages that are supposed to relay to other nodes, thus, disturbing the service) are a few examples of threats to DSRC-equipped vehicles. Therefore, more research efforts in collaboration with the auto industry are needed to mitigate such attacks.

Malware Attacks

Malware can affect the connected vehicle in many ways. It can exploit known vulnerabilities in the design and implementation of in-vehicle network subsystems and components, the software update packages of ECUs, and the vulnerabilities in the operating systems used in the vehicle. The number of malicious actions that can be performed by malware is endless. For instance, malware can disrupt the normal operation of vehicle features such as locking the in-car radio so that users cannot turn it on, causing driver distractions by arbitrarily turning on the in-car audio and turning the volume up; disabling vehicle safety functions such as the ABS; locking the vehicle's doors and requesting a ransom to open them; and sending fake safety data to other vehicles on the road [11].

In the connected vehicle, any communication interface can be a potential entry point for malware. This includes OBD ports, remote ECU firmware and software updates (i.e., OTA updates), removable media ports, and embedded web browsers. It is worth noting that more vehicles are using Linux-based operating systems, which are more resilient to malware attacks than other operating systems like Microsoft Windows and Android. However, malware attacks on Linux have been on the rise [11]. Therefore, we cannot assume that connected vehicles using Linux are completely immune to malware threats.

Automobile Apps Threats

Original equipment manufacturer (OEM)-endorsed connected car solutions such as Apple's CarPlay and Google's Android Auto interfaces will bring more integrated, but potentially vulnerable, mobile apps into the connected vehicle [14]. Vehicle vendors are offering a wide range of automobile apps that leverage 3G/4G/5G connections and/or Wi-Fi to communicate with a car and run diagnostic tests. However, these apps carry a lot of risk and security vulnerabilities that can cause personal data leakage and malware infection (e.g., the previously described NissanConnect app vulnerability). Besides that, a successful attack against a downloadable automobile app (e.g., injecting a malicious code or planting a Trojan horse) in the Apple Appstore or the Google Play Store would have serious consequences on the security of the connected vehicle, which may use that infected app.

Keyless, Wi-Fi, Bluetooth, dedicated short-range communications, OBD systems, USBs, and automobile apps are a few examples of attack entry points for connected vehicles.

Moreover, it is notable that most of the recently reported attacks against connected vehicles have been conducted through an automobile app vulnerability. The method that the mobile app uses to connect to the car plays a crucial role in deciding how secure using the app is. Most automobile apps that allow remote access to the car utilize a web service hosted by a service provider. This web service then connects to the car using a 3G/4G/5G mobile data connection. However, some vehicles do not use cellular connections or web services. Instead, they allow mobile apps to connect directly to the car's Wi-Fi AP and control its functions. If it is implemented poorly, this method is vulnerable to many security and privacy attacks, such as geolocating the vehicle using its AP service set identifier and capturing the preshared key between the car's Wi-Fi AP and the mobile app, hence, gaining unauthorized access to the vehicle's functions, as in the Mitsubishi Outlander PHEV hack [4] explained previously.

Defending/Protection Mechanisms

While it is possible to use strong security measures and mechanisms in ordinary networks to protect a connected vehicle, the limited processing power of the in-vehicle network subsystems does not allow this. Furthermore, ECUs usually come from different vendors. Thus, it is not feasible to design one security solution for the whole system. One suggestion is to isolate the in-vehicle physical network to make sure that infecting one subsystem will not affect the entire network. However, this is not feasible with the increasing need for those subsystems to communicate among each other as explained in Figure 1. Recently, three main approaches have emerged to protect or defend connected vehicles against cybersecurity threats and respond as quickly as possible to the reported hacks. In the following sections, we illustrate these three approaches in detail.

SOME ATTEMPTS TO DEVISE SOLUTIONS TO PROTECT AND DEFEND CONNECTED VEHICLES AND RESPOND TO REPORTED HACKS ARE VERY PROMISING.

An OTA Solution

One of the biggest challenges facing the auto industry is to retrofit protection mechanisms in vehicles that were not secure or need to be secured against a recent threat or vulnerability. This may include software fixes, firmware upgrades, and security patches. To address this challenge and avoid costly recalls, more vehicles' manufacturers have started using the OTA updates.

While OTA updates represent a reasonable solution to respond to cyberthreats in connected vehicles, it suffers a major problem. Fixing vulnerabilities using OTA updates is a security risk. When OTA updates are delivered to the connected vehicle, it means that a remote code is allowed to execute. Thus, if security is not well implemented around the OTA updates, it can lead to serious consequences. Some security mechanisms such as authenticating the OTA update use a secure protocol to deliver it and cryptographically verify the OTA update. This is also called *secure OTA*, and it has been the focus of many recent research efforts.

Cloud-Based Solutions

Since it is not feasible to protect each in-vehicle subsystem individually, centralized solutions have emerged to protect the in-vehicle network and, consequently, the connected vehicle. For instance, Ericsson has developed a cloud-assisted solution called the *connected vehicle cloud* (*CVC*) system [16]. The CVC system establishes a new channel between the vehicle and a variety of services and support provided by partners and OEM-controlled partners. The security layer provided in the CVC ensures that the communication between the vehicle and the system is encrypted. It also contains an anomaly detection unit to detect any malicious attempt to hack into the vehicle. Finally, through a secure gateway, the CVC filters the contents of the web surfing traffic to make sure that no viruses or malwares could infect the vehicle. Figure 3 shows an overview of the CVC system.

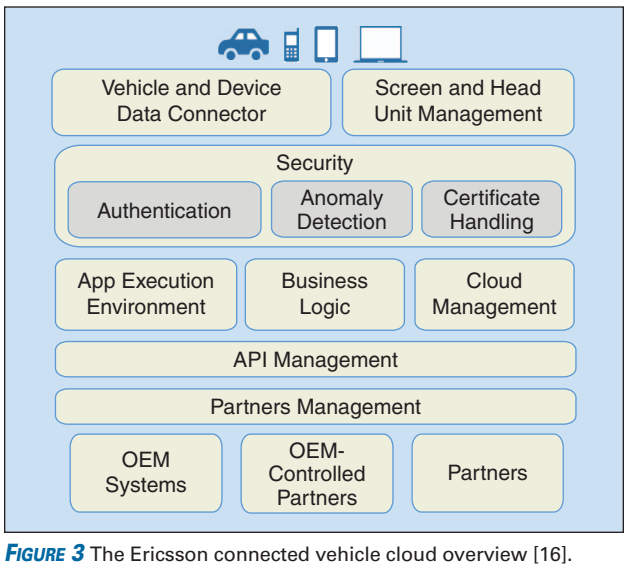

FIGURE 3 The Ericsson connected vehicle cloud overview [16].

Zhang et al. [11] proposed a cloud-assisted vehicle malware defense framework since it is impractical to rely on the vehicle itself to defend against malware. The authors presented lightweight malware defense functions, in terms of processing power and storage, that operate in the vehicle. With the assistance of a security cloud, the on-board malware defense functions will have full access to a wide range of malware defense mechanisms and an up-to-date large malware information database. This eliminates the limited storage problem in the in-vehicle network. It is also suggested that the traffic can be routed through the security cloud to filter out any viruses or malware before reaching the connected vehicle as in the Ericsson CVC system [16].

While the cloud-based solutions to secure connected vehicles look very promising, there are three main issues to examine. First, the communications overhead and the delay incurred by routing the traffic through the cloud services need more investigation (e.g., routing V2V and V2I traffic to the cloud to defend against DSRC attacks is impractical). Second, these solutions heavily depend on the fact that the cloud-based systems are secure. However, if the cloud-based system is infected with a malware, it will spread to all its connected vehicles and could lead to severe damages. Finally, these solutions assume that vehicles are connected to the cloud-based system all the time via the Internet. This may not be possible everywhere and could incur high costs for consumers.

A Layer-Based Solution

Finally, the NHTSA launched a research program that takes a layered approach to cybersecurity for motor vehicles [17]. According to the NHTSA, this layered approach reduces the probability of attacks and mitigates the potential ramifications of a successful one. The program focuses on four main areas at the vehicle level:

1) preventive measures and techniques such as the isolation of safety-critical subsystems to mitigate the effects of a successful attack
2) real-time intrusion-detection measures that include a continuous monitoring of potential intrusions in the system
3) real-time response methods that aim to preserve the driver's ability to control the vehicle when the attack is successful

4) assessment of solutions where information about successful hacks from partners can be collected and analyzed to assess the effectiveness of the current protection mechanisms.

Conclusions

Vehicle cybersecurity is a very serious subject area that needs more investigation and research efforts from academia, the auto industry, and government bodies. The damages from automotive cyberattacks can be severe and irreversible, as they concern human lives. While manufacturers are looking to equip modern vehicles with more connectivity and smart functions, vulnerabilities are increasing rapidly. These vulnerabilities in wired and wireless communication interfaces allow sharks to hack into vehicles and take control. Some attempts to devise solutions to protect and defend connected vehicles and respond to reported hacks are very promising. However, more work and collaboration are still required to protect our connected vehicles and consequently our lives on the roads.

Author Information

Mahmoud Hashem Eiza (mhashemeiza@uclan.ac.uk) received his M.Sc. and Ph.D. degrees in electronic and computer engineering from Brunel University London in 2010 and 2015, respectively. He is a lecturer in computing (computer and network security) at the School of Physical Sciences and Computing, University of Central Lancashire, United Kingdom. Prior to that, he was a research assistant in cybersecurity with the Department of Computer Science, Liverpool John Moores University, United Kingdom. His research interests include computer and network security, with specific interests in quality of service, security, and privacy in vehicular networks, smart grids, cloud computing, and the Internet of Things.

Qiang Ni (q.ni@lancaster.ac.uk) received his B.Sc., M.Sc., and Ph.D. degrees in engineering from Huazhong University of Science and Technology, Wuhan, China, in 1993, 1996, and 1999, respectively. He is a professor of communications and networking with the School of Computing and Communications, Lancaster University, United Kingdom. He previously led the Intelligent Wireless Communication Networking Group at Brunel University London. His main research interests include wireless communications and networking. He has published more than 120 papers in his areas of interest. He was an IEEE 802.11 Wireless Standard Working Group voting member and a contributor to the IEEE wireless standards.

References

[1] S. Nathan. (2015, Sept. 24). Hackers after your car? Tackling automotive cyber security. *Engineer.* [Online]. Available: https://www.theengineer.co.uk/hackers-after-your-car-tackling-automotive-cyber-security/

[2] S. Khandelwal. (2016, May 1). Car hackers could face life in prison. That's insane! *Hacker News.* [Online]. Available: http://thehackernews.com/2016/05/car-hacker-prison.html

[3] A. Greenberg. (2015, July 21). Hackers remotely kill a Jeep on the highway—With me in it. *WIRED.* [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[4] D. Lodge. (2106, June 5). Hacking the Mitsubishi Outlander PHEV hybrid. *PenTestPartners*. [Online]. Available: https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/

[5] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock it and still lose it—On the (in)security of automotive remote keyless entry systems," in *Proc. 25th USENIX Security*, Austin, TX, 2016.

[6] R. Hull. (2106, Feb. 26). Nissan disables Leaf electric car app after revelation that hackers can switch on the heater to drain the battery. *This is Money.* [Online]. Available: http://www.thisismoney.co.uk/money/cars/article-3465459/Nissan-disables-Leaf-electric-car-app-hacker-revelation.html

[7] R. Link. (2015, July 28). Is your car broadcasting too much information? *Trend Micro.* [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/is-your-car-broadcasting-too-much-information/?_ga=1.215918871.1268134788.1466680640

[8] S. Curtis. (2015, Sept. 8). Self-driving cars can be hacked using a laser pointer. *Telegraph.* [Online]. Available: http://www.telegraph.co.uk/technology/news/11850373/Self-driving-cars-can-be-hacked-using-a-laser-pointer.html

[9] TU-Automotive Ltd. (2016, Nov. 2–3). TU-automotive cyber security Europe. [Online]. Available: http://www.tu-auto.com/cyber-security-europe/

[10] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," in *Proc. IEEE Dependable Systems and Networks Workshop*, Budapest, 2013, pp. 1–12.

[11] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 10–21, Feb. 2014.

[12] D. K. Nilsson and U. E. Larson, "Simulated attacks on can buses: Vehicle virus," in *Proc. Int. Conf. Communication Systems Networks*, Langkawi, Malaysia, 2008, pp. 66–72.

[13] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Security*, San Francisco, CA, 2011, p. 6.

[14] W. Yan, "A two-year survey on security challenges in automotive threat landscape," in *Proc. IEEE Int. Conf. Connected Vehicles Exposition*, Shenzhen, China, 2015, pp. 185–189.

[15] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 110–113, Jan. 2014.

[16] Ericsson. (2015). Connected vehicle cloud under the hood. [Online]. Available: http://archive.ericsson.net/service/internet/picov/get?DocNo=28701-FGD101192

[17] NHTSA. (2016, Oct.). Cybersecurity Best Practices for Modern Vehicles. [Online]. Available: https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

[18] Federal Bureau of Investigation. (2016, Mar. 17). Motor vehicles increasingly vulnerable to remote exploits. [Online]. Available: http://www.ic3.gov/media/2016/160317.aspx

[19] M. H. Eiza, Q. Ni, and Q. Shi. "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no.10, pp. 7868–7881, Oct. 2016.

[20] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802-11p:20802.11, 2016.

[21] *IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*, IEEE Standard 1609.2, 2016.

[22] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services*, IEEE Standard 1609.3: 221609.3, 2016.

VT