Article

# Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security

Hashem Eiza, Mahmoud and Ni, Qiang



*Hashem Eiza, Mahmoud ORCID: 0000-0001-9114-8577 and Ni, Qiang (2017) Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security. IEEE Vehicular Technology Magazine, PP (99). p. 1. ISSN 1556-6072*

It is advisable to refer to the publisher's version if you intend to cite from the work.
http://dx.doi.org/10.1109/MVT.2017.2669348

# Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security

**Mahmoud Hashem Eiza, University of Central Lancashire**
**Qiang Ni, Lancaster University**

*In a public service announcement on March 17, 2016, the Federal Bureau of Investigation (FBI) jointly with the Department of Transportation and the National Highway Traffic Safety Administration, released a warning over the increasing vulnerability of motor vehicles to remote exploits*[1]*. Engine shutdown, disable brakes and door locks are few examples of the possible vehicle cyber security attacks. Modern cars grow into a new target for cyberattacks as they become increasingly connected. While driving on the road, sharks (i.e., hackers) only need to be within communication range of your 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 cyber security threats including malware attacks, On-Board Diagnostic (OBD) vulnerabilities, and auto mobile apps threats. We illustrate the In-Vehicle network architecture and demonstrate the latest defending mechanisms that are designed to mitigate such threats.*

## Introduction

Nowadays, vehicles are no longer isolated mechanical machines that are solely used for transportation. Consumers are increasingly demanding 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 smart phones and Bluetooth devices, connected vehicles represent an eco-system 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 Internet of Things (IoT). On the other side, 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 bring many improvements in terms of functionality and convenience, it also brings a new cyber threat plane into life where vehicles become a new target for attackers/hackers [1].

As software starts to permeate more functions in the modern vehicles that are Internet connected, we propose to play the following game of words: 1) If you see the word "software", replace it with "hackable"; and 2) 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 try to attack and/or hack into your vehicle and may cause a real damage that cannot be recovered. Since it is a life-threatening issue (i.e., considered as a lethal cyberattack), in April 2016, the Michigan state Senate has proposed two bills that introduce life sentences in prison for people who hack into vehicles' electronic systems [2].

**Figure 1** *Hackers remotely kill a Cherokee Jeep on highway with the driver in it using a simple 3G connection [3]*

Figure 1 shows an example of a demonstrated cyber security attack against a Cherokee Jeep car on a highway, also known as cyber carjacking. 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 ten miles away [3]. They were able to remotely control the car functions using a simple 3G connection exploiting a vulnerability in the *Uconnect* software. *Uconnect* is Internet connected software that controls the navigation and the entertainment system 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 next section, to disable the brakes and take control over

[1] Internet Crime Complaint Centre (IC3) | Motor Vehicles Increasingly Vulnerable to Remote Exploits, Mar. 17, 2016. [Online]. Available: http://www.ic3.gov/media/2016/160317.aspx

the steer wheel, and finally sent it to a ditch as showed in Figure 1. 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. There are other attacks that have been recently reported against other manufacturers' vehicles. Examples of the most recent reported attacks are:

- Last summer, June 2016, the 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 few global master keys that can be recovered from ECUs. This way, the attacker can clone a Volkswagen Group remote control and, by eavesdropping on a single signal sent by the original remote, he/she can gain unauthorised access to the vehicle.
- Through a vulnerability in *NissanConnect* mobile application, which controls Nissan Leaf electric vehicle, attackers took control over the heater in the car and turned it on all the time 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, he/she 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, was able to interfere with the laser 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 bring a self-driving car at full speed to stop thus, disabling the car. Self-driving cars depend on LIDAR systems, which create a 3D map, to navigate and see if there is any potential hazard or obstacle as can be seen in Figure 2. Petit simply fired 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 stopped at once. This attack worked up to 100*m* away in any direction and did not require a tightly focused beam.

Hence, physical access to the car is no longer a pre-condition to hack into it. Sharks on the road only need 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 steer wheel and disabling brakes, a simple and sudden airbags deployment while driving on a highway represents a lethal cyberattack that could cause the vehicle to crash and costs lives.

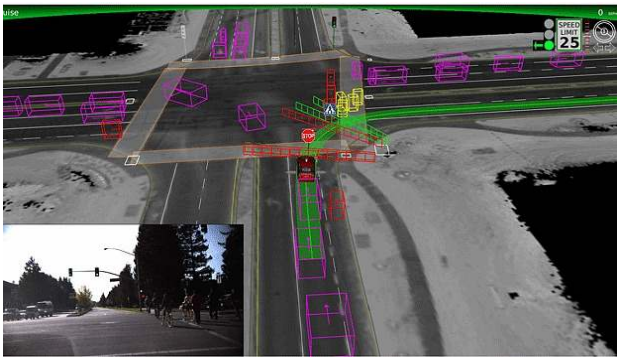


**Figure 2** *What a self-driving car sees when turning right [8]*

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 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 legalisations, and put vehicle IT at the centre of the development process. Yet, more efforts are needed to address vehicle cyber security concerns.

## In-Vehicle Network Architecture (Automotive Network)

To develop an understanding of the potential entry points (i.e., attacking points) 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 between 30 to 100 ECUs, which are embedded computers, that communicate among each other creating the In-vehicle network [10]. ECUs' inter-communication is essential to efficiently monitor and configure different vehicular subsystems. Figure. 3 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 each of which controls a specific functionality in the vehicle. For instance, ECUs that control airbags deployment and Antilock Braking System (ABS) are found in the vehicle safety subsystem, while ECUs that provide engine control and suspension control are found in the powertrain subsystem.

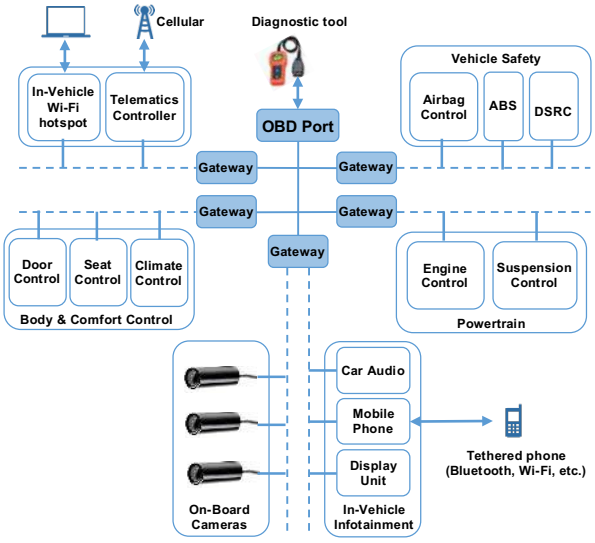


**Figure 3** *In-Vehicle (Automotive) Network Architecture [11]*

To guarantee the desired functionality and on-time response to critical events, ECUs of the same or different subsystems need to communicate among each other. Based on the time-sensitivity of the provided functionality, different In-vehicle sub-networks are utilised. For instance, high-speed Control Area Network (CAN) is used for time-critical engine control, safety subsystems, and powertrain, while for less time-sensitive body and comfort control subsystem a Local Interconnect Network (LIN) is used [11]. To support audio, video and on-board cameras, Media-Oriented Systems Transport (MOST) and Ethernet are employed in the IVI subsystem. These networks are interconnected through gateways that control messages flow among the subsystems as showed in Figure. 3. At the same time, these gateways are interconnected through a high-speed CAN buses.

Given the recent trends of connecting different devices through USB, Bluetooth, Wi-Fi, 3G/4G etc., 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 On-Board Diagnostic (OBD) ports that are utilised for vehicle inspection, ECU firmware updates and repair. Furthermore, OBD port allows full access to the In-vehicle network.

Thus, the variety and the increasing number of connection points in each In-vehicle network subsystem make the vehicle more accessible from the outside world. 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 securing functions on the same vehicle. Moreover, restrictions such as limited computational power and storage capabilities should be considered.

## Cyber Threats Vectors against Connected Vehicles

As we have explained before, connected vehicles have a broad cyberattacks surface where attacker can gain control over the vehicle. Remote key entry, Wi-Fi, Bluetooth, Dedicated Short Range Communications (DSRC), OBD, USB, and Auto mobile apps are few examples of attacks entry points against connected vehicles as illustrated in Figure 4.

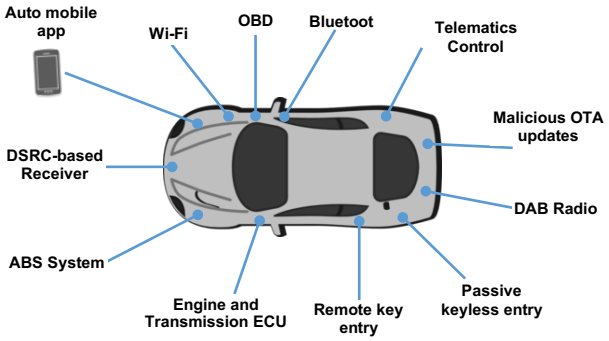


**Figure 4** *Connected Vehicles Security – Potential Cyber Threat Vectors*

In the following, we explain four cyber threats vectors against connected vehicles: OBD threats, DSRC security issues, malware attacks, and mobile auto apps threats.

### *OBD Threats*

The implementation of OBD is mandatory in vehicles sold in the US since 1996, in the European Union since 2001 for gasoline powered-vehicles, and for the diesel-powered ones 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 network within the vehicle. These OBD dongles can be purchased by anyone and they are fairly cheap. 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 above-mentioned attack in [12] requires physical access to the vehicle, modern cars now allow OBD dongles to be remotely controlled by Wi-Fi connection from a computer. In [13], vulnerabilities in the API of a *pass-thru* device (i.e., OBD dongle) allow the attacker to inject a malicious code into it. This malicious code makes the *pass-thru* device emitting malicious packets on the CAN buses every time it is plugged into a different vehicle. In a recent survey [14], over 50% of the surveyed OBD dongles, are vulnerable to hacking. Weak encryption, exposed keys, and communication hijacking are 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 DSRC On-Board Unit (OBU). DSRC communications utilise several standards such as IEEE 802.11p Wireless Access in Vehicular Environment (WAVE) for PHY and MAC functions, IEEE 1609.2 for security services, and IEEE 1609.3 for network services.

To achieve its goal, DSRC equipped vehicles are expected to communicate (i.e., send/receive/relay) information to other DSRC equipped vehicles and/or infrastructure such as Road-Side Units (RSU). This principle opens the door for malicious nodes to either hack into DSRC equipped vehicle or cause damages by sending fake safety information. Therefore, IEEE 1609.2 defines standard mechanisms to authenticate and encrypt messages in DSRC. Nevertheless, attacks such as Denial-of-Service (DoS) are still possible. In [15], Lyamin *et al.* investigated the jamming DoS attacks in IEEE 802.11p 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, GPS spoofing, location tracking, masquerading, and black holes are few examples of threats to DSRC equipped vehicles. Hence, 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 amount 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 the users cannot turn it on, cause driver distractions by arbitrarily turning on the in-car audio and tuning the volume up, disable vehicle safety functions such as the ABS, lock the vehicle's door and request a ransom to open it, and send fake safety data to other vehicles on the road [11].

In the connected vehicle, any communication interface can be a potential entry point for a malware. This includes OBD ports, remote ECU firmware and software updates (i.e., OTA), 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]. Thus, we cannot assume that connected vehicles that are using Linux are completely immune to malware threats.

### *Auto Mobile Apps Threats*

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]. Vehicles vendors are offering a wide range of auto mobile apps that leverage 3G/4G connections and/or Wi-Fi to communicate with your 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 *NissanConnect* app vulnerability explained above). Besides that, a successful attack against a downloadable auto mobile application (e.g., inject a malicious code or plant a Trojan horse) in Apple Appstore or the Google Play Store would have serious consequences on the security of the connected vehicle, which may use that infected app.

Moreover, it is noticeable that most of the recent reported attacks against connected vehicles have been conducted through an auto mobile app vulnerability. The method the mobile app uses to connect to the car plays a crucial role deciding how secure using this app is. Most auto mobile apps that allow remote access to the car utilise a web service hosted by a service provider. This web service then connects to the car using 3G/4G 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 geo-locating the vehicle using its AP SSID and capturing the Pre-Shared Key (PSK) between the car's Wi-Fi AP and the mobile app. Hence, gaining unauthorised access to the vehicle's functions as in the Mitsubishi Outlander PHEV hack [4], which was explained earlier.

## Defending/Protection Mechanisms

While it is possible to use strong security measures and mechanisms in ordinary networks to protect it, the limited processing power of the In-vehicle network subsystems does not allow the same. 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 via Figure. 3.

Recently, three main approaches have emerged to protect/defend connected vehicles against cyber security threats, and respond as quickly as possible to the reported hacks. In the following, we illustrate these three approaches in detail.

### *OTA Solution*

One of the biggest challenges that face the auto industry is to retrofit protection mechanisms in vehicles that were not secure or need to be secured against a recent threat/vulnerability.

This may include software fixes, firmware upgrades, and security patches. To address this challenge and avoid costly recalls, more vehicles' manufacturers start using the OTA updates.

While OTA updates represent a reasonable solution to respond to cyber threats in connected vehicles, it suffers a major problem. Fixing vulnerabilities using OTA updates is a security risk. When OTA is 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 must be in place. This is also called Secure OTA (SOTA), which has been the focus of many research efforts lately.

### *Cloud-based Solutions*

Since it is not feasible to protect each In-vehicle subsystem individually, centralised 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 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, CVC filters the contents of the web surfing traffic to make sure that no viruses or malwares could infect the vehicle. Figure 5 shows an overview of the CVC system.

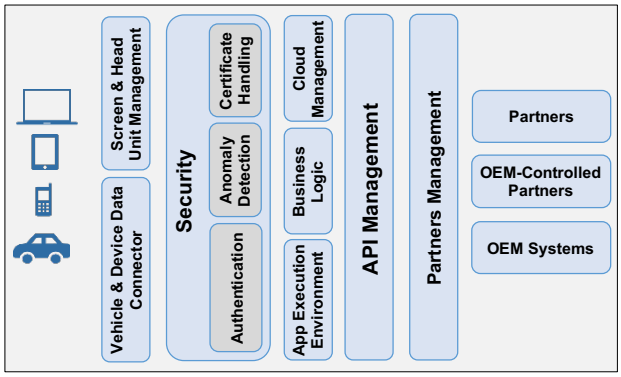


**Figure 5** *Ericsson Connected Vehicle Cloud Overview [16]*

In [11], Zhang *et al*. proposed a cloud-assisted vehicle malware defence framework since it is impractical to rely on the vehicle itself to defend against malware. The authors present lightweight malware defence functions, in terms of processing power and storage, that operate in the vehicle. With the assistance of a security cloud, the on-board malware defence functions will have full access to a wide range of malware defence 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 Ericsson CVC system [16].

While the cloud-based solutions to secure connected vehicles look very promising, there are three main issues to examine. First, 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). Secondly, 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 assumed that vehicles are connected to the cloud-based system all the time via the Internet. This may not be possible everywhere and would incur high costs for consumers.

### *Layer-based Solution*

Finally, the National Highway Traffic Safety Administration (NHTSA) has launched a research programme that takes a layered approach to cyber security for motor vehicles [17]. According to NHTSA, this layered approach reduces the probability of attacks and mitigates the potential ramifications of a successful one. The programme focuses on four main areas at the vehicle level: 1) preventive measures and techniques such as 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; and 4) assessment of solutions where information about successful hacks from partners can be collected and analysed to assess the effectiveness of the current protection mechanisms.

## Conclusion

Vehicle cyber security is a very serious subject area that needs more investigation and research efforts from academia, auto industry and governmental bodies. Damages of automotive cyberattacks can be severe and irreversible as it concerns 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 communications interfaces allow sharks to hack into vehicles and take control. Some attempts to devise solutions to protect/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.

## References


[1] S. Nathan, "Hackers after your car? Tackling automotive cyber security," The Engineer, Sept. 24, 2015. [Online]. Available: https://www.theengineer.co.uk/hackers-after-your-car-tackling-automotive-cyber-security/ [Accessed 2016 03 21]

[2] S. Khandelwal, "Car Hackers Could Face Life In Prison. That's Insane!," The Hacker News, May 01, 2016. [Online]. Available: http://thehackernews.com/2016/05/car-hacker-prison.html [Accessed 2016 05 23]

[3] A. Greenberg, "Hackers remotely kill a Jeep on the highway – with me in it," WIRED, July 21, 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [Accessed 2015 09 30].

[4] D. Lodge, "Hacking the Mitsubishi Outlander PHEV hybrid," PenTestPartners, June 05, 2016. [Online]. Available: https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/ [Accessed 2016 08 14].

[5] FD. 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, "Nissan disables Leaf electric car app after revelation that hackers can switch on the heater to drain the battery," Thisismoney, Feb. 26, 2016. [Online]. Available: http://www.thisismoney.co.uk/money/cars/article-3465459/Nissan-disables-Leaf-electric-car-app-hacker-revelation.html [Accessed 2016 06 27].

[7] R. Link, "Is Your Car Broadcasting Too Much Information?," Trend Micro Inc., July 28, 2015. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/is-your-car-broadcasting-too-much-information/?_ga=1.215918871.1268134788.1466680640 [Accessed 2016 06 27].

[8] S. Curtis, "Self-driving cars can be hacked using a laser pointer," The Telegraph, Sept. 08, 2015. [Online]. Available: http://www.telegraph.co.uk/technology/news/11850373/Self-driving-cars-can-be-hacked-using-a-laser-pointer.html [Accessed 2016 06 25].

[9] TU-Automotive Ltd, TU-Automotive Cyber Security Europe, 2-3 November 2016, ICM - Internationales Congress Center München, Germany. [Online]. Available: http://www.tu-auto.com/cyber-security-europe/ [Accessed 2016 06 25].

[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 DSN-W*, Budapest, June 2013, pp. 1-12.

[11] T. Zhang, H. Antunes and S. Aggarwal, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," *IEEE Internet of Things*, vol. 1, no. 1, Feb 2014, pp. 10-21.

[12] D. K. Nilsson and U. E. Larson, "Simulated attacks on can buses: vehicle virus," in *Proc. Int. Conf. on Communication Systems and 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, T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Security*, San Francisco, CA, 2011.

[14] W. Yan, "A Two-year Survey on Security Challenges in Automotive Threat Landscape," in *Proc. IEEE ICCVE*, Shenzhen Oct. 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 Commu. Letters*, vol. 18, no. 1, pp. 110-113, Jan. 2014.

[16] Ericsson, "Connected Vehicle Cloud Under the Hood," Ericsson, 2015. [Online]. Available: http://archive.ericsson.net/service/internet/picov/get?DocNo=28701-FGD101192 [Accessed 2016 04 18]

[17] National Highway Traffic Safety Administration, "Cybersecurity Best Practices for Modern Vehicles," Report No. DOT HS 812 333, Washington, DC, Oct 2016. [Online]. Available: https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf [Accessed 2017 01 10]



***Mahmoud Hashem Eiza*** *(mhashemeiza@uclan.ac.uk) received the M.Sc. and Ph.D. degrees in Electronic and Computer Engineering from Brunel University London, U.K., in 2010 and 2015, respectively. He is a Lecturer in Computing (Computer & Network Security) at the School of Physical Sciences and Computing, University of Central Lancashire (UCLan), Preston, U.K. Prior to that, He was a Research Assistant in Cyber Security with the Department of Computer Science, Liverpool John Moores University, Liverpool, U.K. His research interests include computer and network security, with specific interests in QoS and security and privacy in Vehicular Networks, Smart Grids, Cloud Computing, and Internet of Things.*

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