ACCEPTED FROM OPEN CALL

Wireless Telematics Systems in Emerging Intelligent and Connected Vehicles: Threats and Solutions

Qian Luo and Jiajia Liu

Abstract

Intelligent and Connected Vehicles (ICVs), which are equipped with various wireless communication technologies and many smart systems, significantly improve the driving experience. Nevertheless, due to the potential vulnerabilities in their advanced cyber physical features and growing numbers of interfaces, malicious attacks can be easily implemented toward ICVs, in particular by utilizing the interfaces of wireless telematics systems. Remote vehicle attacks can even be launched by a malicious application or a smart connected device. Toward this end, we provide in this article an essential tutorial summarizing the threats, attacking methodologies, and promising solutions specifically for wireless telematics systems in the emerging ICVs.

Introduction

Nowadays, Intelligent and Connected Vehicles (ICVs) are widely used in daily life. ICVs, which are equipped with various wireless communication technologies (e.g., V2X communications) and many smart systems (e.g., advanced driver assistant system (ADAS)), are no longer mere mechanical devices. Lots of computerized components/systems directly or indirectly connecting with wireless and other expanded interfaces greatly increase the car's intelligence and connectivity. For example, the Buick LaCrosse and Buick Regal, a type of ICV, provide users with many assist systems such as forward collision alarm (FCA) and collision mitigation brake (CMB), which can automatically brake to avoid collision or to reduce the damages caused by the collision. Tesla, if connecting with cellular or WiFi, enables users to remotely control car doors, air conditioners, lights and so on via a smartphone.

However, ICVs also present more security threats. Advanced cyber physical features and the growing numbers of interfaces, although able to provide great driving experiences and many conveniences, may increase the vulnerabilities of ICVs. For instance, the authors in [1] indicated that adversaries may exploit such features or interfaces to eavesdrop users' private information or even compromise a vehicle's internal network to control the ICV. As reported in 2015, Chrysler had to recall 1.4 million vehicles and pay heavy fines because of the existing security loopholes in its vehicles. If vehicle attacks were to happen, not only the privacy and the lives of users would be compromised, but also the brand and reputation of the automobile manufacturers would be damaged. Thus, the security of ICVs has been attracting intensive research interests from both academia and industry.

Wireless telematics systems, among all surfaces of ICVs, may be easily utilized as portals of remote intrusion. A malicious smartphone application can be utilized to perform long-range wireless attacks on ICVs [2]. Interfaces such as Bluetooth and cellular can also be used to remotely compromise vehicles [3]. As also verified in [4–6], remote vehicle attacks could be conducted by exploiting the interfaces of wireless telematics systems to access a vehicle's internal network. Once gaining access to a vehicle's internal network, adversaries can easily implement malicious operations, such as stopping the engine, sudden braking and steering. In light of this, we provide in this article an essential guide summarizing the threats, attacking methodologies, and promising solutions specifically for wireless telematics systems in the emerging ICVs.

The remainder of this article is organized as follows. The following section presents a short introduction to ICVs and wireless telematics systems, and then we summarize the threats and attacking methodologies. A malware attack on a popular IVI including specific attack procedures and experimental results is then presented as an illustrative case study. We provide promising solutions addressing the security threats, and conclude the article in the final section.

Wireless Telematics Systems in Intelligent and Connected Vehicles

Intelligent and Connected Vehicles

In addition to extending the in-vehicle network to enable versatile communications with the outside world, ICVs may even be equipped with more intelligent services such as adaptive cruise control (ACC) and lane keeping assist (LKA). An architecture of ICVs can be found in Fig. 1, in which all electronic components are connected through a controller area network (CAN) bus and can be compromised by a malicious attack. Electronic control units (ECUs) are embedded devices

Digital Object Identifier:
10.1109/MWC.2018.1700364

Qian Luo and Jiajia Liu (corresponding author) are with the State Key Laboratory of Integrated Services Networks, Xidian University.

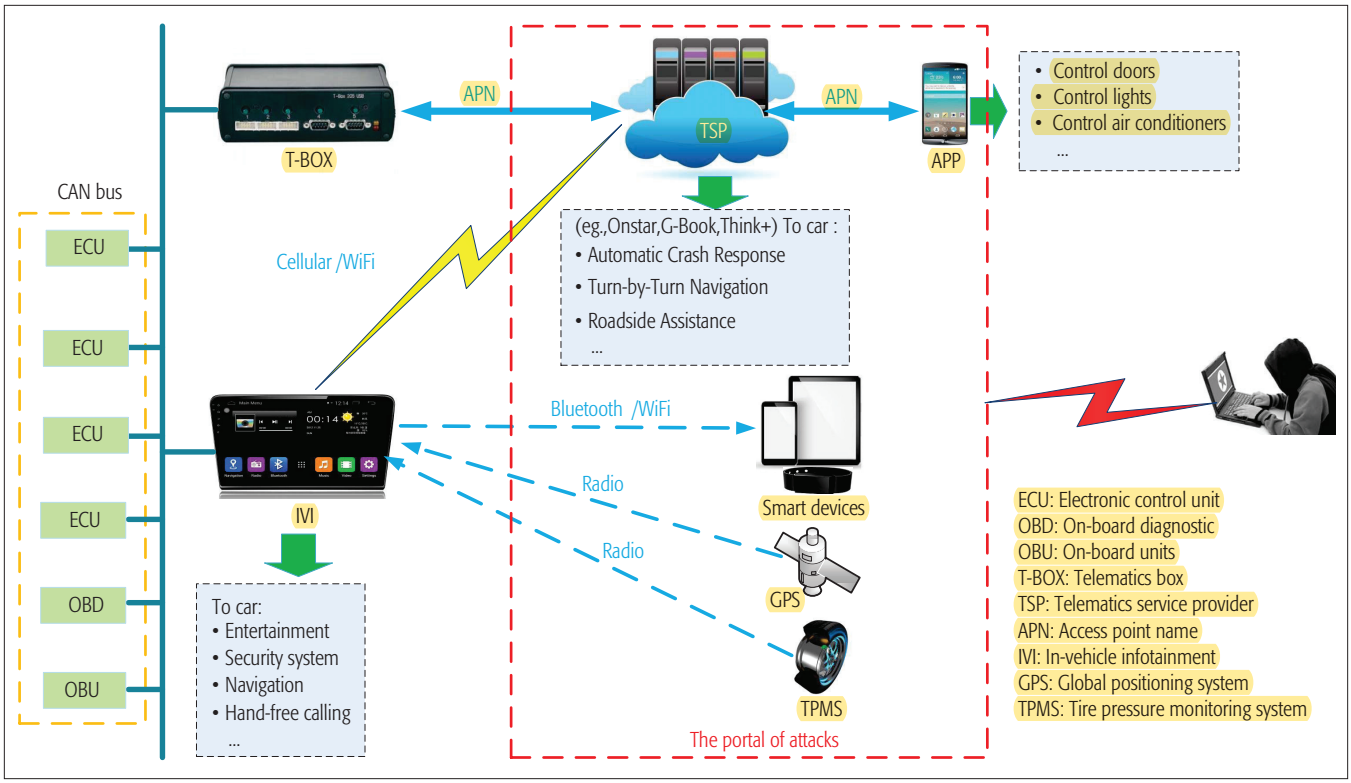

FIGURE 1. The figure shows a typical architecture of Intelligent and Connected Vehicles (ICVs). The left part displays the in-vehicle network. In the right part, the wireless telematics systems including TSP and IVI are going to have more and more wireless interfaces (e.g., Bluetooth, WiFi, Radio) to connect vehicles to outside, each of which may become the portal exploited by attackers to invade vehicles remotely.

consisting of sensors and actuators, designed to monitor vehicle conditions and control vehicle behaviors, respectively. Since the CAN bus and ECUs compose the in-vehicle network, attacks that were implemented toward the CAN and ECUs can directly control the vehicle [7, 8]. On-board diagnostics (OBD), collecting the CAN bus data via the OBD scan tool for trouble diagnosis, was also utilized as a portal to attack [7]. On-board units (OBU), although providing ICVs with vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications for more convenient and safer driving in the near future, may also cause the attacks to be transmissible. Being standard equipment on almost all ICVs, wireless telematics systems, including the telematics service provider (TSP) and in-vehicle infotainment (IVI), can also increase the likelihood of a car being attacked. In addition, many other advanced cyber physical features adopted in ICVs for assisted driving, such as forward collision warning (FCW), the park assist system (PAM), and the passive anti-theft system (PATS), can also become vulnerable entries to access an automobile's physical attributes [4].

Wireless Telematics Systems

Wireless telematics systems, as developed to provide ICVs with wireless communications, remote services, entertainment and so on, mainly consist of a TSP and IVI, which are introduced as follows.

Telematics Service Provider: A TSP is a platform enabling vehicles to exchange data with remote cloud servers via wireless communication. As shown in the top right of Fig. 1, through the specialized access point name (APN), the TSP can communicate with the telematics box (T-BOX) and specific smartphone apps, providing a better driving experience and more convenience. Owing to the fact that the T-BOX can directly communicate with the in-vehicle network, much data, including user profile data, vehicle data, and service data, can be uploaded to the TSP and stored in cloud servers. Conversely, with the help of the T-BOX, the TSP can supply remote services to vehicles. For example, OnStar, a type of TSP applied broadly in Buick and Chevrolet vehicles, provides vehicles with permits for automatic crash response, turn-by-turn navigation, roadside assistance, and so on. Similar popular systems include G-BOOK from Toyota, think+ from Luxgen, and Sync from Ford. In addition, the TSP can also process remote requests received from specific smartphone apps, which enables users to remotely control car behaviors such as starting the engine and locking the doors.

Usually, the TSP connects to IVI to offer real-time information to drivers via a cellular network or WiFi, such as real-time traffic, stolen vehicle tracking, and navigation assistance. However, the TSP is vulnerable and may cause users' privacy to be compromised, or even vehicles to be remotely controlled.

In-Vehicle Infotainment: Unlike previous entertainment systems, the present IVI, composed of a host, an LCD display, keyboards, antennas, and so on, is actually an integrated information processing system, which adopts a specialized vehicle-mounted CPU, and connects to both the in-vehicle network (CAN-BUS) system and outside Internet services. Also, in order to facilitate users'

Interface	Reference	Attacking component	Attacking methodologies	Threats
Media system	Miller and Valasek. 2015, [4]	The radio	Malware attack; unauthorized attack	Control the functions of the radio
Bluetooth	Checkoway *et al*., 2011, [3]	IVI	Sniffing attack; unauthorized attack	Remotely control vehicle; snoop users' privacy
Cellular (e.g., 2G/3G/4G)	Checkoway *et al.*, 2011, [3]	Telematics unit	Malware attack; unauthorized attack	Broadcast and single-vehicle control
WiFi/Internet	Nie *et al.*, 2017, [6]	IVI	Internet attack; unauthorized attack	Compromise in-vehicle systems; remotely control vehicle
USB	Checkoway *et al*., 2011, [3]	ECU firmware	Malware attack	Harm other electronic systems in vehicle
GPS	Simon *et al*., 2017, [13]	IVI	Spoofing attack; jamming attack	Mislead drivers' destinations; hijack valuable vehicles or goods
FM/AM/XM/DAB	Fernandes *et al*., 2013, [9]	Car radio	Malware attack	Control car radio
TPMS	Ishtiaq *et al*., 2010, [15]	IVI	Spoofing attack	Trigger tire pressure warning messages
SMS (Short Message Service)	Ian *et al.*, 2015, [10]	Telematics unit	Spoofing attack	Remotely control vehicle
APPs	Damon *et al.*, 2016, [5]	IVI	Malware attack	Control driver's smartphone connected to IVI; send malicious messages into in-vehicle network

TABLE 1. Threats in the interfaces of wireless telematics systems.

operations, a touchscreen and several advanced functions such as automatic speech recognition are included in IVI. From the bottom left of Fig. 1, one can observe that IVI accesses the in-vehicle network via a CAN connector (inside IVI) which allows IVI to exchange data with the CAN bus to assist driving, so that IVI, such as BMW's iDrive, Benz's COMAND, and Jeep's Uconnect, not only have a non-negligible impact on entertainment, but also on vehicle control, driving, and security.

For the above reasons, it is very possible for adversaries to remotely control vehicle by attacking IVI. What's more, the various interfaces of IVI, including Bluetooth, WiFi, cellular, Global Positioning System (GPS), tire pressure monitoring system (TPMS), and third-party IVI apps, may also worsen the security threats of ICVs. Attackers can exploit these interfaces or the smart devices connected to IVI (e.g., smartphone, smartband, ipad), as a portal to intrude into the CAN bus and obtain vehicle control authority. An example can be found in the Uconnect on the Jeep Cherokee [4].

Threats in Wiereless Telematics Systems

Potential Threats in Interfaces

Research in ICV security has drawn extensive attention and obtained remarkable achievements in recent decades. In particular, Koscher *et al*. [7] invaded two 2009 Chevy Malibu and demonstrated in real cars that malicious messages could be injected into the CAN bus, causing automotive functions to be compromised and the driver's inputs to be overridden, such as disabling the brakes and stopping the engine. In the following year, Checkoway *et al*. summarized the external attack surfaces for a modern automobile [3]. There were in total three types of surfaces that can be used to execute codes on the vehicle to obtain access into the internal network of ICVs, including indirect physical access (e.g., CD player, USB and iPod), short-range wireless access (e.g., Bluetooth, TPMS, WiFi) and long-range wireless access (e.g., FM, satellite radio, remote telematics systems). Later, a 2010 Ford Escape and a 2010 Toyota Prius were attacked by Miller and Valasek [8]. Specifically, the authors controlled the braking, acceleration, dash board, and steering by compromising the complementary technologies such as automatic parallel parking and lane keep assist. At the BlackHat 2014 conference, Miller and Valasek further analyzed the remote attack surfaces of automobiles for different vehicle models such as Ford, the Toyota Prius, and BMW [1].

Motivated by these studies [1, 3], ensuing research interest was mainly concentrated on how to exploit the growing number of ICVs' external surfaces for attacking ICVs. In [9], Fernandes *et al*. showed that attacks can be implemented by FM to control the car radio. In 2015, Miller and Valasek exploited the Sprint network to remotely attack a Jeep Cherokee [4], in which Jeep's IVI system named Uconnect was compromised to send malicious messages to the CAN bus, causing the vehicle's various functions to be controlled (e.g., slow down, brake, turn off the engine). It is noted that the attacks in [4] could even be extended to other vehicles as long as they are connected via cellular communications. Koscher *et al.* proved that a single component of wireless telematics systems might also provide the portal to compromise the vehicle [10]. Furthermore, it was reported that BMW's ConnetedDrive and Audi's MegamosCrypto were intruded.

Once connected to IVI, the user's smartphone can also be abused by attackers, through which malicious messages may be injected into the vehicle's internal network remotely [5]. In [2], Woo *et al*. took control of the target vehicle via a malicious application installed on a smartphone, which was Bluetooth paired with an OBD scan tool. The remote attacks on the Tesla Model S further illustrated that IVI's interfaces can be exploited to invade a vehicle's internal network. In [6], Nie *et*

al. utilized the vulnerabilities of a browser on Tesla's IVI to compromise both the parking and driving modules. In addition, the "Key Reinstallation Attacks (KRACK)" loophole of WiFi exposed in [11] and the attack vector "BlueBorn" of Buletooth reported in [12] may also be exploited by adversaries to take complete control of the target IVI and intrude vehicles. Note also that IVI based attacks, although sometimes unable to get into the vehicle's internal network, are still non-negligible. As summarized in [13], fake GPS signals can be fabricated, which may cause the diver to travel to the wrong destination and valuable vehicles or goods to be hijacked.

As summarized in Table 1, any one of these interfaces, if compromised, will cause disastrous consequences. Our attacking is based on a popular third-party IVI app, which will be introduced in detail later.

Attacking Methodologies

Malware Attacks: Malware may exist in various forms such as viruses, worms, and spyware, which can be injected into ICVs to launch malicious attacks via the interfaces of wireless telematics systems (e.g., media player, USB, WiFi). By utilizing the known/unknown vulnerabilities of these interfaces, wireless telematics systems can be exploited as portals to conduct malware attacks. As reported in [3], in light of the input vulnerabilities of media player firmware, the researchers added to music files delicately designed malware, which ran and sent malicious CAN messages into an in-vehicle network when the IVI plays these music files. Note also that malware can spread into the vehicle's system when removable media (e.g. U-disk), if infected with malware, is used to update the ECU firmware through the USB port. As indicated in [10, 6], it is possible for adversaries to remotely inject malware into a vehicle by a malicious update server or a browser of IVI. Once injected into a vehicle, malware may disable the vehicle's security mechanisms (e.g. the anti-theft system), or even directly send malicious CAN messages to compromise the vehicle [14].

Unauthorized Attacks: Generally speaking, an unauthorized attack is implemented by exploiting the vulnerabilities of interfaces or components in the wireless telematics system to violate access regulations and to obtain the ability to execute arbitrary codes on the vehicle. An example can be found in [3] where the authors utilized the vulnerabilities of the CD player, the Bluetooth stack and the telematics unit, and invaded the vehicle by conducting an unauthorized attack. Miller and Valasek in [4] exploited the vulnerabilities of D-BUS systems to execute codes on the head unit of Uconnect (the IVI of Jeep), which resulted in the car's radio, heating, air conditioner, and so on, being controlled.

Internet Attacks: Internet attacks, including phishing, SQL Injection and Cross Site Script, are mainly implemented on cellular/WiFi connected wireless telematics systems to snoop privacy data. As proposed in [6], with the help of a fake WiFi hotspot, it is possible to attack the vehicle remotely by hijacking the traffic of IVI's browser.

Sniffing Attacks: Sniffing attacks refer to intercepting network packets or Bluetooth packets. Under sniffing attacks, the communications between the TSP and IVI may be eavesdropped or even tampered with. As demonstrated in [3], the car's Bluetooth MAC address was first obtained via sniffing and then used in a remote invasion.

Spoofing Attacks: Spoofing attacks can be initiated by an adversary, who fabricates false data such as addresses and signals to override the real data/signals sent to the target device. As shown in [13], a spoofing attack was conducted to mislead navigation where the target position data was gradually tampered with using the growing number of fake GPS signals.

Jamming Attacks: Jamming is aimed at blocking the wireless communication channel from transmitting the original information. Under this attack, it is quite difficult for receivers to distinguish the legal information. For example, one can make plenty of radio noises on the GPS frequency with the jamming attack in [13].

Denial of Service (DoS)/Distributed Denial of Service (DDoS) Attacks: DoS/DDoS attacks usually create a large amount of useless data, causing network congestion that prevents the target device from communicating with others. It is mainly conducted toward the connection between IVI and the TSP (via WiFi/cellular), resulting in communication disruption between the vehicle and the remote cloud servers.

Experimental Study

General Idea of the IVI Attack

After a comprehensive survey, we found that most third-party IVI apps have similar update processes, in which many vulnerabilities may exist. In particular, the third-party IVI app will send a request to its cloud server to check for a newer version when it begins to start running or when the button to check for a newer version of the app is pressed. If the IVI connects with cellular/WiFi, a response packet will then be returned to the app by the cloud servers. However, all update sessions of the third-party IVI apps can be distinctly observed and obtained via network sniffer tools (e.g. Fiddler and Wireshark). By carefully investigating these update sessions, one can find flaws and utilize them to fool the IVI APP into accepting an update package containing delicately designed malware by redirecting the target app's update traffic toward a malicious server.

Detailed Attacking Process

Based on the above observation, we present an experimental malware attack. A popular IVI running Android OS was selected as our target. Two illustrative effects of our malware attack are to remotely send arbitrary information to pop up on the target IVI, and to remotely change the wallpaper of the target IVI. In Fig. 2, one can find our attacking steps, which are described in detail as follows.

Set up a Wireless Local Area Network (WLAN): We have almost no requirement on the router in setting up a WLAN, and an ordinary wireless router is sufficient.

Analysis of Captured Packets: We analyze the traffic between the IVI app client and cloud servers by capturing packets with Fiddler, an excellent http protocol proxy tool. With the help of this tool, we can capture all the sessions. Packet-cap-

After a comprehensive survey, we found that most third-party IVI apps have similar update processes, in which many vulnerabilities may exist. In particular, the third-party IVI app will send a request to its cloud server to check for a newer version when it begins to start running or when the button to check for a newer version of the app is pressed.

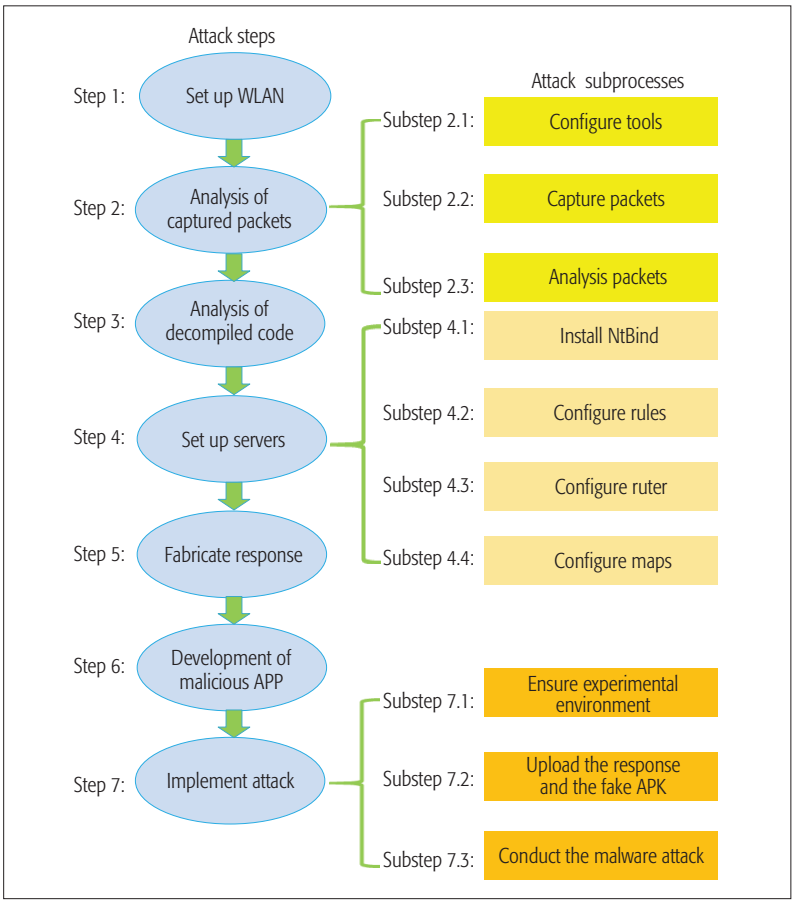

FIGURE 2. The figure illustrates the malware attack process. The left part shows the steps of attack from up to down, and the right shows the detailed process of each step.

ture and analysis include the following steps.

Step 1: Install Fiddler on one laptop in the WLAN, then set up a proxy on the IVI including its proxy server IP address as well as proxy port, which are the same as the Fiddler.

Step 2: Run Fiddler on the laptop first, then start the target app and begin to capture packets.

Step 3: By observing the update sessions of the target app, we can obtain the host name and the URL address of the destination cloud server in request messages, and the response body of checking newer version results, which is a JSON file contained in response messages returned by the cloud servers. We can then fabricate a response packet of identical format by imitating this JSON file, which includes important information such as appname, version, appurl, and so on.

Analysis of Decompiled Codes: After getting the target APK, we use AndroidKiller to decompile it. The processes of the target app, sending requests to check for a newer version, parsing the JSON file returned by the cloud servers, and downloading the newer version to complete the installation, are the key points that we need to understand.

Set up Servers: By now, critical information has been obtained by us. Next, we begin to set up a domain name server (DNS) to redirect client request traffic toward our own server containing the malicious malware.

Step 1: Install NtBind on one desktop, which acts as a DNS server in the LAN system.

Step 2: Edit configuration files according to NtBind's rules. Note that only one mapping, i.e., the host name of the IP address of our malicious server, needs editing.

Step 3: Configure the wireless router. Set the IP address of the preferred DNS server to that of the fake DNS server.

Step 4: It is necessary to test the configuration results above. A DNS server is set up successfully if and only if the DNS server resolves the host name of the real update cloud server to the IP address of the malicious server.

We install Tomcat on another desktop, which acts as a malicious server in the WLAN system. Then we modify the listening port of Tomcat to 80.

Fabricate Response: By analyzing the update response packets, we use a servlet to generate a JSON file of the same format. Note that the value of appurl in the JSON file should be replaced with the URL of our fake app (including malware) and the servlet program should be deployed on the malicious server.

Development of Malicious App: In order to make users install the new APK unhesitatingly, disguising malware as a newer version APK of the target APP is essential. Therefore, we design the package name, the icon and the version messages of our fake app in exactly the same way as the official app.

Implement Attack: Once all these preparations are done, the attack can be implemented.

Step 1: Ensure that the malicious server and the fake DNS server are connected to the WLAN, and wait for the time when the target IVI also accesses the WLAN.

Step 2: Configure the response packet deployed on the malicious server and upload the malicious app.

Step 3: Open all servers to conduct the attack. After receiving the request packets for the newer version from the IVI app, we initiate the malware attack.

RESULTS

Experimental Environment: According to the above description, our experimental environment consists of a WLAN, a fake DNS server, a malicious server, a popular IVI of Android OS 5.1.1, and a very popular third-party IVI music app. We set up a WLAN with a TP-Link router, built a DNS server with ntBind 9.1.1, and developed a malicious server with Tomcat 7.0, which are all connected to the WLAN.

Experimental Results: We found that the target app successfully accepted the fake response from our malicious server. Once the malware-infected update package was installed on the IVI and started running, we could implement our attack remotely. Then, we could remotely send messages to pop up on the screen of the IVI as illustrated in Fig. 3a, and send pictures to change the wallpaper of the IVI as shown in Fig. 3b. Other malware can also be injected in the same way, which means more destruction can be conducted on the IVI such as eavesdropping, snooping, or even sending malicious messages into vehicle's internal network.

Discussion

From our experiment, one can note that the online application updates in wireless telematics systems also expose serious security threats for ICVs. For this reason, it is extremely necessary to consider the security of Over-the-Air technology, which may be an essential function in future ICVs. Besides providing online upgrades for applications in wireless telematics systems via WiFi or cellular networks, OTA also offers online updates to operating systems, firmware (e.g., ECUs, Telematics units, T-BOXs), data packets (such as maps) or even encryption keys in ICVs. For example, the Tesla Model S uses OTA technology to upgrade in-vehicle microelectronic devices online such as miniature ECUs and Machine-to-Machine (M2M) modules.

In addition, one of the most important features of OTA is that each vehicle will certainly receive an update notification sent by the OTA center as long as these vehicles are in the channel. Once the OTA system exists, security issues, not only the privacy of users, would be compromised. Also the physical functions or smart devices (e.g., ADAS, navigation) of ICVs would be directly affected. Adversaries, for instance, may conduct vehicle attacks similar to ours by utilizing the potential vulnerabilities of OTA to fabricate update packets and inject contaminated packets into wireless telematics systems. Then, all vehicles in the OTA channel may be damaged or even completely controlled.

Solutions

For wireless telematics systems, we summarize some solutions that may improve the security of ICVs.

Interface Security

As discussed earlier, almost all interfaces of wireless telematics systems have the possibility of being exploited to compromise ICVs, so improving the security of these interfaces is becoming urgent. For this purpose, we present two possible schemes as follows.

Restrict Access: One of the most common methods is to restrict access into some important interfaces. For instance, the Bluetooth interface should not be allowed pairing attempts unless it is manually placed in pairing mode. Similarly, interfaces such as WiFi and cellular should use delicately designed mechanisms of authentication and encryption to keep their communications from being hijacked, snooped or tampered with. In addition, the interfaces connecting with the in-vehicle network should be monitored and restricted when communicating with the outside world. For example, a filter can be deployed into these interfaces to prevent illegal messages from accessing the vehicle.

Use Stricter Rules: It is also an effective approach for some interfaces to use stricter rules so as to reduce vehicle attacks. For example, the browser of Tesla's IVI uses AppArmor and iptables to make attacks extremely difficult to implement.

Threats from Third-Party APPs

IN addition to the interfaces, the third-party apps, that are installed on wireless telematics systems can also make ICVs vulnerable to security threats

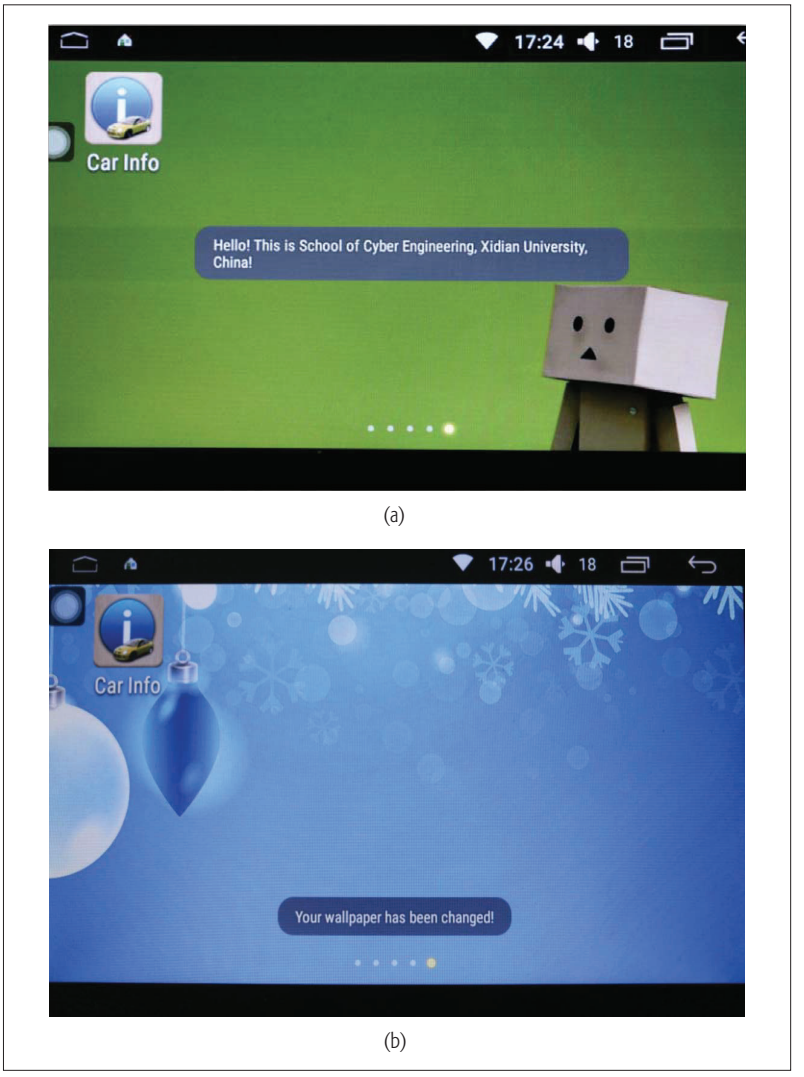

FIGURE 3. The figure shows the experimental results of our remote malware attack: a) Remotely sending messages to pop up on the IVI screen; b) Remotely changing the wallpaper of the IVI.

if they are injected with malware or designed with vulnerable application program interfaces (APIs). In order to reduce threats from third-party apps, we suggest two possible methods as follows.

Restrict the Openness: One possible solution is to restrict the openness of wireless telematics systems to third-party apps. In particular, wireless telematics systems should only install third-party apps designed with code security, resource file security, data storage security, and data transmission security. For example, if the target app's codes are obfuscated or protected by shell code, our attack may not be successful.

Use Safe Update Framework: A safe update framework should also be used in these third-party apps to restrain malware from being mounted on vehicles. Specifically, these apps should verify the signature, package name and data integrity of the newer APK before running the program to install the newer version.

Cloud Security

Security threats presented by cloud services in wireless telematics systems, which may cause privacy leakage or vehicle attacks, are also non-neg-

Users should be aware of vehicular security knowledge so as to reduce the threats of vehicle attacks. For instance, users should carefully connect a vehicle or even not connect it with the free WiFis near roads, supermarkets, hotels, and so on, which may be a malicious access point (AP). Users should refuse the access requests of devices whose security cannot be identified.

ligible. It is important to improve the security of information including data storage in the TSP and the communication between the TSP and the ICV. Because of this, we take into account two possible methods for these two aspects.

Encrypt Data via Private Key: For the security of data storage, one possible method is to encrypt data via private key to prevent users' privacy data from being stolen. Furthermore, only the registered and authenticated users can access this private key.

Communication Limitation: As for communication security, one possible method is to put strict limitations on the communication latency/delay so as to keep packets from being captured or snooped.

People Security Consciousness

We propose two suggestions from different aspects, which are summarized as follows.

Enhance Developers' Code Robustness: Not only should the interfaces of wireless telematics systems be hardened, but also the underlying code platform, in which vulnerabilities may exist. To avoid increasing vulnerabilities, developers should consider unsafe factors when programing, such as not using unsafe functions, and should carefully use frameworks, codes and library files developed by the third-party.

Enhance Users' Security Consciousness: Users should be aware of vehicular security knowledge so as to reduce the threats of vehicle attacks. For instance, users should carefully connect a vehicle or even not connect it with the free WiFis near roads, supermarkets, hotels, and so on, which may be a malicious access point (AP). Users should refuse the access requests of devices whose security cannot be identified (such as an U-disk with malware).

Conclusions

In this article, we investigated the security threats to wireless telematics systems in emerging ICVs and proposed some solutions. We analyzed various threats and attack methodologies via different interfaces in wireless telematics systems. A malware attack was conducted on a popular IVI, in which malware could be remotely injected into IVI, and the results corroborated that our malware can remotely send messages to pop up on the screen of IVI and send pictures to change the wallpaper of IVI.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61771374, 61771373, and 61601357), in part by the China 111 Project (B16037), and in part by the Fundamental Research Fund for the Central Universities JB171501.

References

[1] C. Miller and C. Valasek, "A Survey of Remote Automotive Attack Surfaces," *Proc. BlackHat*, 2014, pp. 1–94.
[2] S. Woo, H. J. Jo, and D. H. Lee, "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, Apr. 2015, pp. 993–1006.
[3] S. Checkoway *et al.*, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," *Proc. USENIX Security Symposium*, 2011.
[4] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," *Proc. BlackHat*, 2015, pp. 1–91.
[5] S. Mazloom *et al.*, "A Security Analysis of an In-Vehicle Infotainment and App Platform," *Proc. USENIX Workshop on Offensive Technologies*, 2016.
[6] S. Nie, L. Liu, and Y. Du, "Free-Fall: Hacking Tesla from Wireless to Can Bus," *Proc. BlackHat*, 2017, pp. 1–16.
[7] K. Koscher *et al.*, "Experimental Security Analysis of a Modern Automobile," *Proc. IEEE S&P*, 2010, pp. 447–62.
[8] C. Miller and C. Valasek, "Adventures in Automotive Networks and Control Units," *Proc. DEFCON*, 2013, pp. 1–101.
[9] E. Fernandes, B. Crispo, and M. Conti, "FM 99.9, Radio Virus: Exploiting FM Radio Broadcasts for Malware Deployment," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, June 2013, pp. 1027–37.
[10] I. D. Foster *et al.*, "Fast and Vulnerable: A Story of Telematic Failures," *Proc. USENIX Workshop on Offensive Technologies*, 2015.
[11] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA," *Proc. ACM CCS*, 2017, pp. 1313–28.
[12] Armis, "The Attack Vector 'Bluebrone' Exposes Almost Every Connected Device," Sept. 2017; available: https://www.armis.com/blueborne/
[13] S. Parkinson *et al.*, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," *IEEE Trans. Intell. Transp. Syst.*, 2017, to be published, DOI: 10.1109/TITS.2017.2665968.
[14] T. Zhang, H. Antunes, and S. Aggarwal, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," *IEEE Internet Things J.*, vol. 1, Feb. 2014, pp. 10–21.
[15] I. Rouf *et al.*, "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study," *Proc. USENIX Security Symposium*, 2010, pp. 323–38.

Biographies

Jiajia Liu [S'11, M'12, SM'15] is currently a full professor at the School of Cyber Engineering, Xidian University. His research interests cover wireless mobile communications, FiWi, IoT, and so on. He has published more than 50 peer-reviewed papers in many prestigious IEEE journals and conferences, and currently serves as an associate editor for IEEE TC & TVT, an editor for *IEEE Network*, and a guest editor of IEEE TETC & *IEEE IoT Journal*. He is a Distinguished Lecturer of IEEE ComSoc.

Qian Luo received her B.S. degree in computer science from North University of China in 2016. She is currently working toward the M. degree in the School of Cyber Engineering, Xidian University. Her research interests include vehicular network security and vehicle navigation security.