Journal of Fundamental and Applied Sciences

ISSN 1112-9867

Available online at http://www.jfas.info

Research Article

Special Issue

EXTERNAL ATTACKS ON AUTOMOTIVE SYSTEM THROUGH WIRELESS COMMUNICATION CHANNELS

N. Q. Mohd Noor[1], K. Kamardin[1,2,*], S. Mohd Daud[1], N. N. Amir Sjarif[1], N. A. Ahmad[1], A. Azmi[1], S. Mohd Sam[1]

[1]Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur

[2]Wireless Communication Centre, Universiti Teknologi Malaysia, Kuala Lumpur

Published online: 01 February 2018

ABSTRACT

The reliance of today's automotive system on electronics control system is expected to make the cars to be state-of-the-art vehicle. However, this technology dependency results in the cars to be exposed to attacks by the hacker through the manipulation of electronics system. Previously, for the attacker to compromise car's system, he/she must access the car directly and internally. However, with the incorporation of wireless technologies such as Bluetooth and cellular into automotive system for example in its telematic units, the attacks are evolved from internal attacks into remote attack where the adversary does not have to internally access the car's system. This paper analyses the vulnerabilities of the automotive system by the remote attacks performed through Bluetooth and cellular. Once the vulnerabilities were analyzed, the threats imposed by these vulnerabilities are accessed. Two scenarios namely theft and surveillance are used to exemplify the threats that are carried by the vulnerability of the automotive system to the remote attacks. From the vulnerability analysis and threat assessment, it can be deduced that the automotive system is vulnerable to attacks and proper countermeasure must be taken to curb the implication from the attacks.

Author Correspondence, e-mail: kamilia@utm.my

doi: http://dx.doi.org/10.4314/jfas.v10i2s.2

Keywords: Hardware Trojan, Insertion, Third-part IP, Trust.

1. INTRODUCTION

Modern cars are electronically controlled by state-of-the art computer systems consisting unprecedented amount of codes running on processors that are constantly connected to the internal networks. Although this structure is significantly beneficial in the aspect of efficiency, safety and cost, it is vulnerable because it is exposed to new attacks. For example, it is demonstrated in the work of Koscher et. al [1] that an attacker could connect to a vehicle's internal network to maliciously manipulate the critical computer system such as safety critical elements such as the engine and brakes. This kind of threat along with various examples of threats as described in [1] are known as the threat model. Threat model is used to understand types of threats that a system is exposed to understand how vulnerable the system is. Previously the threat models [2] are limited to direct physical access to car's internal network. However, with the existence of wireless network capability for automotive system, cars are al so exposed to the remote attacks. Thus, the threat model underlying past works [2, 3, 4] has encountered vital and reasonable criticism such as in Charette's work [5]. It is understood that focusing only on the physical connection made by the attackers to a car's internal computer network is quite unrealistic. Furthermore, it is found that attackers use wireless network capability to perform hybrid computer-based and non-computer-based attacks such as cutting the brake lines through the automotive electronics system [6].This scenario portrays a significant gap in knowledge and practicality of attacks. It raised the question such as to what extent are remote attacks using wireless network possible, to what extent are the practicality of the attacks, and what vectors represent the greatest risks? Is the etiology of such vulnerabilities the same as for desktop software? To fill in the gap, a set of possible remote attacks through wireless network modalities namely short-range wireless access and long-range wireless access are systematically modelled as threats. For each access vector category, the vulnerability of the car is analyzed by demonstrating the ability to compromise vulnerabilities in hands-free Bluetooth functionality and via calling the car's cellular modem.

In this paper, the vulnerabilities of the automotive system due to remote access via wireless network and threats imposed on the vulnerabilities are assessed. This report is presented as following: Section I introduces the exposure on the automotive system on external attacks through

wireless network. Section II mainly presents background of the attacks on the automotive system. This section discusses the related literatures on both the internal and remote attacks. Section III explains the vulnerability analysis on both short-range and long- range wireless channels. Section IV evaluates the threats imposed on the described vulnerabilities in Section III. This section also projects two possible scenarios to assess the severity of the threats. The conclusion from this experiment is concluded in Section V.

2. BACKGROUND

Heterogeneous combination of digital components which is known as Electronic Control Units (ECUs), control a broad range of functionalities in automotive system, including the brakes, lighting, drivetrain and entertainment. Charette predicted that there are up 70 engine control units (ECUs) that have million lines of code in modern luxury vehicles [7]. Common wired network such as Controller Area Network (CAN) [8] or FlexRay bus [9]. By utilizing CAN and FlexRay bus, critical safety feature such as pre-tensioning of seat-belts when a crash is forecasted can be implemented along with non-critical convenience feature such as automatic radio volume variation as a function of speed. Concurrently, this design offers a wide internal attack surface because each component has at least implicit access to every other component on a given bus. There are a number of research literatures have explained how this design might be compromised resulting from the components used in the design [10, 11, 12, 13, 14]. The compromised design is demonstrated by spoofing messages to isolated components in the lab [15]. In a recent study by Francillon, Danev & Capkun [16], it is demonstrated that if an adversary successfully accesses the automotive system bus wirelessly, he/she could maliciously exploit critical components across the entire car and induce risky behavior such as forcefully engaging or disengaging individual brakes without driver input through series of experiments on a complete automobile [16]. The wireless attack surface for automotive wireless interfaces can operate over short ranges i.e Bluetooth and long ranges i.e cellular. One of the example is Roufet al.'s analysis of the wireless Tire Pressure Monitoring System (TPMS) in a modern vehicle [17]. Although originally their work was focused on the privacy effect of TPMS broadcasts, they by chance caused the ECU that managed TPMS data to stop working using wireless signals. In another example, such as portrayed in the work of Francillon et al [18], computer security issues around car theft are highlighted by demonstrating relay attacks against keyless entry systems and the attacks by the engine immobilizers on the

RFID-based protocols [19, 20, 21] to recognize the correct ignitionkey.

In parallel to this, there have been research works that consider the attacks that are associated with long range wireless namely cellular using addressable channel. The attacks through this channel happen by the remote telematics systems that produce unceasing connectivity through cellular data and voice networks [22]. These systems offer a wide range of features that support safety features by reporting crash, diagnostically alerting of mechanical issues, remotely tracking and disabling, and accessing data hands-free such as weather or location. These cellular channels are advantageous for attackers because these channels can be accessed over random distance in massive ways. These channels typically have relatively high bandwidth with distinct address and support both interactive data and control exfiltration [23].

3. VULNERABILITY ANALYSIS

The vulnerability analysis is performed based on two threat models which are short-range wireless and long-range wireless access. Since there are a few numbers of short-range and long-range wireless access available, the scope of the vulnerability analysis is limited to Bluetooth for short-range wireless access and cellular for long-range wireless access.

3.1. Bluetooth-based Attacks

Bluetooth is a standard protocol in most vehicles sold by all main automobile manufacturers that is used to support hands-free calling and is typical. In hardware, the lowest architectural level of the Bluetooth protocol is usually implemented. On the other hand, in software, the management and services component of the Bluetooth stack is implemented instead. The Class 2 devices are used with a range of 10 meters in automotive system, which can be stretched through amplifiers and directional antennas as portrayed in [24]. Like in many modern cars, the built-in Bluetooth allows the occupants' cell phones to connect to the car as such in which they are used to perform hands-free calling. These Bluetooth functionalities are built into the automotive telematics unit. The access to the telematics ECU's Unix-like operating system can be gained through reverse engineering [25]. Once the telematic unit is accessed, the program responsible for handling Bluetooth capability is recognized. It is found that the program contains a copy of a famous embedded implementation of the Bluetooth protocol stack and a sample hands-free application through analyzation of the program [25]. Where the weaknesses are likely to exist, the interface to this program and the rest of the telematics system are seen to be custom-built [25]. In managing a

Bluetooth configuration command, there are about 20 calls to strcpy to the stack in the program that can are usable. Thus, any paired Bluetooth device can use this weakness to perform arbitrary code on the telematics unit. Two practical methods for using this attack are performed using two sub-classes of the short-range wireless attack vector; (a) indirect short- range wireless attacks and (b) direct short-range wireless attacks.

3.1.1. Direct short-range wireless attacks: The weakness which was identified in [1] needs the attacker to utilize a paired Bluetooth device. To pair the attackers' device to the car's Bluetooth system is quite challenging. Nonetheless, the car's Bluetooth subsystem was exteriorly designed to support hands-free calling and thus may normally be paired with one or more smart phones. It is estimated that an attacker can independently compromise one of those smart phones and utilize it attacker as an initiation for manipulating the car's telematics unit and the ECUs through compromising of smart phone. A simple Trojan horse application on the HTC Dream (G1) phone running on Android 2.1 is implemented in [1] to assess this attack vector. The application seems to be harmless but it silently monitors for new Bluetooth connections to the telematics unit. Once the telematic unit is identified, the attack payload is sent. Thus, it is agreed that smartphones can be a feasible medium for utilizing a car's short- range wireless Bluetooth weaknesses.

3.1.2. Indirect short-range wireless attacks: This attack requires the attacker to remotely use the Bluetooth weakness without access to any paired device. There are two steps needed for the indirect attacks to successfully compromise the car's telematic unit. The first step requires the attacker to obtain the car's Bluetooth MAC address. Next, the attacker must furtively pair his or her own device with the car. In [2], both USRP-based software radio and open-source Bluesniff [23] package are used to discover the car's Bluetooth MAC address when the car is the proximity of a formerly paired device such as smartphone. Another way to sniff the car's Bluetooth MAC address by monitoring the Bluetooth traffic generated when previously paired device turns on its Bluetooth unit, irrespective of the existence of the car. Aside from the MAC address, the PIN for pairing must also be obtained to successfully pair to the car's telematic unit. If the driver would like to pair a new device under normal use, he may put the vehicle into pairing mode through a well-documented user interface and the car will provide a random PIN in return which is manually added to the phone. This PIN however, could be brute-forced this PIN as described in [22] at a rate of eight to nine PINs per minute, for an average of approximately 10 hours per car; this rate is limited entirely by the response time of the vehicle's Bluetooth stack. Any driver intervention is

not required for this pairing process and any person in the car will unnoticeably be paired. Although this attack is time exhausting and requires the car(s) under attack to be on the move, it is also parallelizable whereby attacker could detect the MAC addresses of all cars within the same area covered by the first car. If a parking garage is left by a thousand cars per day, then it is expected that the PIN could be brute-forced for at least a car per minute [22]. Upon completing this pairing, the attacker can inject a payload on the paired channel an exploit to compromise the vehicle[22].

3.2. Cellular-basedAttacks

For long-range wireless channels attacks, the focus is on the vehicle's telematics unit with built in cellular capabilities. Today's contemporary vehicle has the capabilities to enable diverse safety and convenience features such as calling for help upon crash. However, long- range communications channels also open the possibility to be targeted by potential attackers. In this section, the operation of these channels is discussed with the emphasis on the reverse engineering that take place. A combination of software flaws that allows a total remote compromise through the cellular voice channel is also demonstrated. The car's telematics unit is supplied with a cell phone interface for wide-area connectivity. In telematic's unit, the Internet related functions such as navigation and location-based services are performed using 4G data functions. The voice channels are utilized for critical telematics functions such as crash notification since this channel provides connectivity over the broadest service coverage. Since the voice channel is in analog form, the automotive manufacturers usually utilize Airbiquity's aqLink software modem to perform analog-to-digital conversion and vice versa [23]. To generate a sensible data connection between the car's telematics unit and a remote Telematics Call Center (TCC) ran by the manufacturers, the Airbiquity's software is utilized. In its Gateway program that governs both voice and data cellular communication, the telematics unit integrates the aqLink code.

A simple, in-band, tone-based signaling protocol is utilized to switch the call into data mode since a single cellular channel is used for both voice and data [23]. Even though a tell- tale light and audio announcement is employed to signify that a call is in progress, the in- cabin audio is muted when data is transmitted. The unit utilizes a so-called "stealth" mode which does not produce any sign that a call is in progress for pure data calls such as telemetry and remote diagnostics. There are two kinds of vulnerabilities namely vulnerability in the gateway and vulnerability in authentication that are induced by the cellular attacks.

3.2.1. Vulnerability in the Gateway: As mentioned earlier, packet sizes up to 1024 bytes is explicitly supported by the aqLink code. However, since the command messages are formatted to be smaller, the custom code that connects the aqLink to the Command program presumes that packets will never surpass 100 bytes. This exposes the packets to another exploitable stack-based buffer overflow vulnerability. Through this attack, the upper-level authentication checks that is run by the Command program is totally bypassed because it is occurred at the bottom level of the protocol stack. To prevent this exploit from working in practice, there is one key gap. The key gap is by choosing the buffer overflow to send over 300 bytes to the Gateway program [24]. The best case scenario for the attack is it requires about 14 seconds to be performed because the aqLink protocol has a maximum effective throughput of approximately 21 bytes a second [25]. In order to prevent the attack, the Command program sends the caller an authentication request upon receiving a call and, unexpectedly, the connection is effectively terminated if a response within 12 seconds is not transmitted. Thus, data can not be sent adequately fast over an unauthenticated link to overflow the vulnerable buffer.

3.2.2. Vulnerability in the Authentication: Consider a call is made to the vehicle and data mode is activated, a random three bytes authentication challenge packet will be sent by the vehicle as the first command message sent prior to starting authentication timer. During normal operation, in order to generate a response, the challenge is hashed by the TCC hashes along with a 64-bit pre-shared key. While polling for an authentication response, the Command program will reject any other packet to avoid other command messages to be sent [26]. The Command program will send an error packet if a wrong authentication response is received or if a response is not received within the preset time limit. The unit halts from sending any data when this packet is acknowledged. The code that generates authentication challenges is examined after a number of failed attempts to derive the shared key and the responses are evaluated [26]. Both code and responses contain errors that were adequate to create a vulnerability. It is a key flaw whenever the telematics unit starts, random number generator is reinitialized and seeded with the same constant each time [26]. Therefore, the same expected response is produced when multiple calls to a car is made while the telematics unit is off. As a result, an attacker can monitor a response packet t hrough sniffing the cellular link during a TCC-initiated call and is ready to rerun that response in the coming attack. In addition to that, the code parsing authentication responses

comprises of atrocious bug that allows infiltration without determining a correct response first [26]. Uniquely, there were certain challenges that are procedurally generated but yield incorrect responses will be recognized as valid response. The challenge was unique each time where 1 out of 256 trials produced the wanted structure if the random number generation is not re-initialized [26]. Thus, the authentication test could be bypassed after an average of 128 calls and the exploit is occurred again without driver's realization [26]. However, this attack is difficult to be executed if the vehicle is not ignited [26] because the telematics unit was dormant after the first call ended thereby, the random number generator must be re-initialized before a second call could be made.

3.2.3. In summary, the way of the vehicles' telematics unit employed the aqLink code opened several vulnerabilities that allows a remote exploit. For example, there is an inconsistency in number of packet sizes that are supported by the aqLink software and the buffer that were assigned by the telematics client code. This inconsistency could be exploited to send adequately long payload by performing the authentication prior to set the ample timeout value for phone's call [7]. After approximately 128 calls, it is possible for an attacker to accurately predict the authentication challenge due to the mistake in the logic's of the unit's authentication system.

4. THREAT ASSESSMENT

Based on the vulnerabilities discussed, threats are primarily considered at a technical level. Access gained to a car's internal network provides sufficient means for compromising its systems such as lights, brakes, and engine are shown in [16]. In this article, it is shown that an adversary can compromise a car's system with no physical access to the car but through a range of external communications channels. It is crucial to understand how serious the threats to induce such kinds of vulnerability to the car's system. However, there is no obvious ways to predict threats from such unknown attacks. Nevertheless, the capabilities of performing attacks that bring about such threat can be evaluated. For example, it can be predicted that in hypothetical "cyber war" or terrorist scenarios; such as enormous number of vehicles are infected and as a result, the brakes are simultaneously disengaged while driving at top speed [17]. Due to limited number of real scenarios in these types of attacks, the threat imposed is highly speculative.

Table 1. Exfiltration and Cost from Attacks

Channel	Range	Implemented Control/Trigger	Exfiltration	Cost
Bluetooth	Short	Remote control using the presence of MAC addresses	Yes	Low
Cellular	Long	Gateway and authentication flaws allow broadcast and remote control	Yes	Low

Table I tabulates the exfiltration and cost from the attacks through Bluetooth and cellular. It can be seen form the table that for both Bluetooth and cellular, the attack is in the form of remote control. However, the triggers are different because as for Bluetooth, the remote access is triggered by MAC addresses while for cellular, the trigger comes from the gateway and authentication flaws. The attack on both channels exfiltrate the system but the cost of the effect is low. To further evaluate the exfiltration and cost of these attacks, two scenarios namely financially motivated theft and third-party surveillance are considered.

4.1. Theft

Using both Bluetooth and cellular capabilities, it is feasible to enable theft by sending a on-demand door-unlock command to a vehicle. However, an advanced vehicle thief may be aware that remote manipulation can be performed to significantly affect both scale and business model. For instance, the thief might opt to simultaneously exploit multiple vehicles via war dialing rather than exploiting the only one targeted vehicle. Because of the gateway and authentication flaws, the attacker might coordinate each car to make a connection to the central server thereby hacked its Vehicle Identification Number (VIN) as well as GPS coordinates. The VIN comprises of the year, model and make of each vehicle and therefore its value. By having these information, the thief could browse through sets of vehicles, classify and locate the most valued vehicle and finally address door-unlock and self-ignite commands. An enterprising thief might also provide services to other thieves using his/her expertise to identify valuable cars. Although this scenario seems hypothetical, a complete attack in which a vehicle's security protection can be remotely disabled by a thief to permit his/her partner to get into the vehicle and drive it away were evaluated in [27]. The attack was performed by compromising the telematics unit to unlock the doors, ignite the engine, unfasten the shift lock solenoid which typically halts the vehicle from phasing out of park, and manipulate the packets utilized in the vehicle's startup protocol [27]. In this case, the

accomplice can only drive the “stolen” car forward and backward because the steering column was still locked [27] but the gravity of these attacks is more than enough to demonstrate the vulnerability of the automotive system.

4.2. Surveillance

An attacker who compromises vehicle’s telematics unit has the capability of capturing data from the in-vehicle microphone which typically utilized for hands-free call. Using these data, he/she could bypass the authentication and perform surveillance on the data over the gateway. In addition to this, by performing analytics on the data, the attacker could continuously acquire the location of the vehicle and actively track the whereabouts of the driver. These possibilities, which were experimentally conducted and tested in [28], could be useful to corporate spies, paparazzi, private investigators and such who seek to pry on the private conversations within the target automobiles. Furthermore, without knowing exact location of the target vehicle, the manipulation techniques as elaborated in the theft scenario could also be adapted to perform the eavesdropping. For example, Google executives may be eavesdropped by an attacker by filtering a set of compromised vehicles and linking them down the another set of vehicles that are also luxurious and parked in the Google parking lot at 10 am [28]. The location of those same vehicles at 7 p.m. could be at the driver’s house, permitting the attacker to determine the driver’s identity through commercial credit records. It is suspected that the process of identifying promising targets for eavesdropping is quite fast using this technique.

5. CONCLUSION

Based on the vulnerabilities and their associated threats, it can be concluded that the usage of wireless communication for automotive system resulted in the cars to be hacked remotely. Although the impact cost of the attacks from the wireless channel is low, still it can induce huge amount of losses if countermeasures are not taken. Thus, the manufacturer should enhance the security system of the cars by anticipating these remote attacks.

6. ACKNOWLEDGEMENT

This work was funded by Universiti Teknologi Malaysia (UTM) and Ministry of Higher of Education (MOHE) under grant no. Q.K130000.2538.15H97.

7. REFERENCES

[1] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy. IEEE Computer Society, May2010.

[2] BBC. Hack attacks mounted on car control systems. BBC News, May 17,2010.

[3] S. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin, and M. Szydlo. Security analysis of a cryptographically enabled RFID device, USENIX Security 2005, pg 1–16, July2005.

[4] R. Boyle. Proof-of-concept CarShark software hacks car computers, shutting down brakes, engines, and more. Popular Science, May 14, 2010.

[5] R. Charette. This car runs on code, Feb.2009.

[6] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. Manzuri Shalmani. On the power of power analysis in the real world: A complete break of the KeeLoq code hopping scheme. Crypto ’08, vol. 5157 of LNCS, pages 203–20. Springer- Verlag, Aug.2008.

[7] CAMP Vehicle Safety Communications Consortium. Vehicle Safety communications project task 3 final report, Mar.2005.

[8] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel. A practical attack on KeeLoq. Eurocrypt ’08, vol. 4965 of LNCS, pg. 1–18. Springer-Verlag, Apr.2008.

[9] FlexRay Consortium. FlexRay communications system protocol specification ver. 2.1, Dec.2005.

[10] P. R. Thorn and C. A. MacCarley. A spy under the hood: Controlling risk and automotive EDR. Risk Management, Feb.2008.

[11] M. Wolf, A. Weimerskirch,C. Paar. Security in automotive bus systems, ESCAR 2004, Nov.2004.

[12] M. Wolf, A. Weimerskirch, and T. Wollinger. State of the art: Embedding security in vehicles. EURASIP Journal on Embedded Systems, 2007.

[13] Y. Zhao. Telematics: safe and fun driving. Intelligent Systems, IEEE, 17(1):10–14, Jan./Feb.2002.

[14] N. Falliere, L. O Murchu, and E. Chien. W32.Stuxnet dossier version 1.3, Nov.2010.

[15] U. E. Larson and D. K. Nilsson. Securing vehicles against cyber attacks, CSIIRW’08, pg. 30:1– 30:3. ACM Press, May2008.

[16] A. Francillon, B. Danev, and S. Capkun. Relay attacks on passive keyless entry and start

systems in modern cars. In A. Perrig, editor, NDSS 2011. ISOC, Feb.2011.

[17] T. Hoppe, S. Kiltz, and J. Dittmann. Security threats to automotive CAN networks – practical examples and selected short-term countermeasures, SAFECOMP 2008, vol. 5219 of LNCS, pg.235–248. Springer-Verlag, Sept. 2008.

[18] ISO. ISO 11898-1:2003 - Road vehicles – Controller area network. Int. Org. Standardization,2003.

[19] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: implementation, performance, and research challenges. IEEE Comms Magazine, 46(11):110–118, 2008.

[20] J. Leyden. Boffins warn on car computer security risk. The Register, May 14,2010.

[21] P. Magney. iPod connections expected in more than half of U.S. car models in2009.

[22] J. Markoff. Stung by security flaws, Microsoft makes software safety a top goal. The New York Times, Jan.2002.

[23] C. Mundie. Trustworthy computing.

[24] NPR. 'Rifle' sniffs out vulnerability in bluetooth devices. All Things Considered, Apr 13, 2005.

[25] M. Raya, J.-P. Hubaux. Securing vehicular ad hoc networks. Jour. Comp. Sec., 15(1):39–68, 2007.

[26] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study, USENIX Security 2010, pages 323–338. USENIX Association, Aug.2010.

[27] D. Spill and A. Bittau. Bluesniff: Eve meets alice and bluetooth. In D. Boneh, T. Garfinkel, and D. Song, editors, WOOT 2007, pages 1–10. USENIX Association,2007.

[28] J. Vijayan. Update: Android gaming app hides Trojan, security vendors warn. Computerworld, Aug. 17, 2010.

How to cite this article:
Mohd Noor N Q, Kamardin K, Mohd Daud S, Amir Sjarif N N, Ahmad N A, Azmi A, Mohd Sam S. External attacks on automotive system through wireless communication channels. J. Fundam. Appl. Sci., 2018, *10(2S), 11-23.*