Cyber Security of Technologies In the Modern Vehicle

Christopher C. Schmid

Abstract: Traffic and automotive safety in the vehicular fields of the United States and the world have drastically increased over the last decade. In the United States alone there were over 3 trillion miles driven in 2016, and over 250 million vehicles registered. With so many miles driven and cars on the road, it is imperative that automotive corporations incorporate safety features such as merging assistance, tire pressure monitors and priority assignment management for emergency vehicles to ensure a safer road experience for the consumer. It is also paramount for automotive corporations to include new luxury style amenities, such as in-vehicle infotainment systems, to stay relevant as they release their newest A-1 level goods against their competitors. Even though the intentions for these automotive technological advances are pure, there is always going to be sinful folk trying to find vulnerabilities to exploit, especially in new technologies. In this paper, the focus is to shed light on some of the prominent vehicular safety and luxury implementations. The three contrivances probed in this study are Mirrorlink, TPMS, and WAVE. This study will describe each system in a manner of what its' intended purpose is and its' benefit to the consumer. How each system operates, will then be analyzed in detail, which will bring this study to inquiring what the possible and commonly believed vulnerabilities of each system are. Lastly, this study will investigate what systems have known legitimate vulnerabilities and what is being done to remedy the ailments.

I. Introduction

Up until the early 90's the automotive vehicles were not much more than a metal bucket with wheels and if you got lucky you had a button to wind your windows down. That was all changed by the introduction of the CAN bus (Controller Area Network Bus) to the automotive industry. The CAN bus is a standard designed to allow microcontrollers and devices to communicate with each other in applications without a host computer [1]. The concept founded by German auto parts company BOSCH. The big game changer with this modern technology was that the vehicles electronic control units (ECU's) were able to work together with nothing more than a simple standard being put into place [1]. Some examples of these are the airbag ECU, the Anti-Lock ECU and Onboard Diagnostic connector (OBD). As well as the CAN bus being a convenient alternative to having a central computer, it was also, for the most part, relatively secure. Any device added to the CAN bus network would be proprietary to the manufacturer so the language would more than likely be obscure to the perpetrator. Also, there was little to no implementation of wireless frequencies throughout the CAN bus, and mostly everything was hard wired together [2]. Modern Cars today have upwards of 3 miles of cables (Mostly all CAN bus related) [2]. This number would continue to rise as vehicles would continue to become more intelligent, through more onboard electronic components, ranging from navigation systems to entertainment systems to in-car sensors. The amount of wiring is dropping drastically due to wireless technology. More and more sensors and devices are communicating with the CAN bus via a wireless signal. Although this will benefit the gas mileage, due to there being less wire weight, it is making troubleshooting errors easier, as well as a slew of other benefits. On the other hand, it does open up notable cybersecurity vulnerabilities. Some of the hot topics of vehicular vulnerabilities include Mirrorlink, the tire pressure monitoring infrastructure, and WAVE. Mirrorlink is a device interoperability standard that offers integration between a smartphone and a car's infotainment system. The prevailing theory is that Mirrorlink is exportable due to its lack of a secure device pairing method. The tire pressure monitoring system is the system in place to alert your dashboard that a tire is low. The standard theory is that the wireless tire pressure control systems are interceptable with relative ease under the right circumstances via radio waves or Bluetooth. The newest models of vehicles as early as 2012 are being rolled off of the lots and onto the streets with the new industry standard called WAVE (wireless access in vehicular environments). WAVE is used for vehicles to communicate with other vehicles for the purpose of lane departure warning messages and vehicles to correspond with infrastructures for the purpose of tolls and traffic flow continuity. All 3 are part of a contingency plan for a safer future on the road and a better driving experience that alternatively has the potential to be exploited by a talented man with a screen and a keyboard.

The Automotive Industry is more vulnerable to cyber security threats today than ever before courtesy of the employment of new technologies such as the most current wave of safety protocols, convenience implementations, and infotainment devices. The following study will detail these systems and display the possible vulnerabilities of them to maintain the confidentiality, integrity, and availability of the entire infrastructure for the sake of the consumer.

II. VULNERABILITIES OF VEHICLE INFOTAINMENT SYSTEMS

In the past, if you wanted to listen to music, you were blessed with the opportunity to choose your preferred genre then have news and commercials forced upon you with traditional FM radio. Then there was the evolution of the cassette and the CD, which were great except you were limited to only the songs that you cherished most and were willing to pay for. After that came along the MP3 player and the alike that allowed you to download any song you could imagine on the internet for about a dollar a song (usually about 100 cents less than that). Then you could listen to it on command. The only downfall of this was that you had to go out of your way to download the music to your player device before you got in the car. Then on top of that, the hassle of plugging it into the stereo and having to turn on the radio separately from your player device was once again too much effort on the part of the consumer, and that is where Mirrorlink comes in. Mirrorlink (Created by Connected Car Consortium) is an in-vehicle-infotainment standard primarily used to integrate your smartphone into your vehicle's infotainment system [3]. Some of the capabilities of Mirrorlink include GPS navigation, call control, app-based games, entertainment and for the most part anything you can do on your smartphone, can be manipulated via the Mirrorlink screen on the dash of your car. (The protocol that supports this is called Virtual Network Computing [3]. (VNC)) As of 2016, over 80% of vehicle manufacturers equip their vehicles with Mirrorlink [4]. Many automakers have Mirrorlink installed but disabled for their flavor of IVI (In-Vehicle-Infotainment) Ford Sync, Toyota Entune, and BMW Connected Drive to name a few [3]. Although Mirrorlink is disabled, there is a video on YouTube with over 60,000 views that effortlessly shows you how to enable Mirrorlink in your car [4]. Enabling Mirrorlink is often done ethically by tuning companies. Once enabled, they can use Mirrorlink to root into than CAN bus of the vehicle and manage the intricacies of the motor, braking, steering, and etcetera to improve performance [4]. Hackers with similar access would have the ability to manipulate safety critical components from a linked smartphone just as well. The ease of access reasonably constitutes a legitimate concern from a consumer standpoint. In fact, the only two protocols embodied in Mirrorlink built to maintain integrity to the intended user is DAP (Device Attestation Protocol) and Content Attestation [3]. The purpose of DAP is to assure that the connecting device has the appropriate software and hardware to pair with Mirrorlink. The purpose of content attestation is to eliminate the possibility of a man in the middle attacks by the client of the VNC relationship (the IVI device) initiating a challenge-response protocol with the VNC server (the smartphone) periodically [3].

In 2016, three students from George Mason University attempted to find copies of files on the firmware and then investigate what interfaces could be useful for debugging as well as infiltration [3]. They started the experiment with a 2015 store bought IVI agent [3]. (They did not release the make or model of the device because they were not attempting not to bash the company. The goal of the team was to secure the entire IVI industry better because most of the industry has similar vulnerabilities [3].) The device that the team was attempting to penetrate had Mirrorlink disabled on it by default and was running off of a proprietary protocol [3]. To enable Mirrorlink, they needed a USB drive, a YouTube video and 15 minutes. Once Mirrorlink was enabled they identified the NOR flash chip that contained the BIOS, a boot-loader, and two root certificates. One of the root certificates deriving from Mirrorlink, the other from the automotive manufacturer [3]. Due to the implementation of this key infrastructure, it would be unfeasible for a malicious hacker to attempt to install a malicious image unless he was able to generate a validly signed key from the automotive manufacturer [3]. While the Team was exploring the executables of the kernel, user applications and the image itself they discovered that AppMain.exe (a background subroutine process) gave them access to Developer Mode (DevMode) [3]. They also found the password displayed in plain text in the file itself [3]. Once in DevMode, they were able to access the Windows CE GUI, the same GUI the developers use to create and debug Mirrorlink [3]. From there they were able to access the CAN bus and launch several attacks, such as disabling and enabling the brakes, turning the engine on and off, and rolling down the windows. The students were able to perform these attacks on a 2008 Chevy Impala as well as a 2010 Toyota Prius, a 2013 Toyota Prius, and a 2010 Ford Escape [3]. The same team of George Mason University students found two interfaces that were useful for debugging and infiltrating, JTAG (Joint Test Action Group) and UART (Universal Asynchronous Receiver/Transmitter) [3]. Via JTAG they were able to access all the addressable memory of the system as well as CPU registers [3]. Via UART they were able to access boot-sequence messages and other debugging messages [3]. The team did a very partial release of what ports they were able to export and how they did it for the sake of giving the companies a chance to remedy their shortcomings.

If you think that you would not need, or even want such a device in your daily driver, think again. As of January first, 2017, the state of California began enforcing a law mandating that if you are talking on the phone while driving, you must do it hands-free. That gives you the option of letting your call go to voicemail or joining the era of new technology and answering your telly via Mirrorlink. If you are a law-abiding citizen in the state of California, and you would like to conform to the new rules of the road by syncing your smartphone with your car. The logical thing to do is get on the eBay and acquire an infotainment device for as cheap as 200 dollars. Buying things cheap is all well and good but keep in mind that what you pay for is what you get. Although many of the cheaper brands may offer similar capabilities as the top of the line industry standards, you very well could be sacrificing many security vetting intricacies.

III. Vulnerabilities of Tire Pressure Monitoring Systems

As of 2008, in the United States and 2012 in the European Union, it has become mandatory of all automakers to have tire pressure monitors (TPM) installed in all new vehicles. TPMs are battery-powered sensors installed in the rear of the valve stem in each tire. They display the inflation level of tires by sending updates via the CAN bus. Below is an illustration of the device inside of the tire (figure 1 [2]). Due to the nature of a tire continually rotating it would be impractical to have wires running to the CAN bus; thus the communication is done via an RF (Radio Frequency) signal (TPMs running on Bluetooth is a myth). The thought behind this mandate is that there would be an overall increase in road safety and fuel efficiency [2]. After all, properly inflated tires will have a shorter braking distance, improved traction and will reduce rolling resistance. The convenience of knowing the inflation of your tires from inside our vehicle is all dandy aside from the fact that there is an RF signal running astray from your vehicle that can be reached up to 40 meters away by anybody and could be exploited by an unethical computer jock.

Fig. 1. Illustration of a tire pressure monitor [2].

Securing protocols such as 802.11p concerning Vehicle-to-Vehicle and Vehicle-to-Infrastructure communication has been taken seriously in all aspects of the development, from the protocols themselves to the architectural deployment of the services. A deployed in-car sensor system such as TPM has received little attention from the security side of the development community. The reasoning for this is the thought that primarily, it would be innocuous to embezzle or spoof the data from a TPM. At worst the perpetrator would be able to identify your real-time tire pressure and send a signal to the central car computer popping on your low tire pressure light. The second reason being that the metal frame of the vehicle might minimize the already fairly short transmission range pushed by the small battery powered TPMS and would make infiltration that much more arduous [2].

A team of college students from Rutgers University set to investigate whether the security flaws of TPMs were, in fact harmless, or if the lax security was putting consumers in danger. There were three exploits that the students thought could be taken advantage of via the TPM infrastructure.

- Vehicle Tracking
- Jamming or spoofing
- Access to the CAN bus and safety critical ECU's

In the student's experiments while using only a GNU (GNU's not UNIX) radio and a USRP (Universal Software Radio Peripheral) they were able to discover that the communications were running on standard modulation schemes and protocols that are unencrypted. There was also no evidence of input validation or any other fundamental security practice. The students were also able to communicate freely with the TPMs devices from 10 meters away with a cheap antenna. Also from 40 meters away with a low noise amplifier, meaning that an unethical key puncher would smoothly be able to spoof and jam the signal being transmitted from the TPM and from there infiltrate the rest of the ECU infrastructure. As far as tracking goes, each TPM sends packets with a 32-bit identifier making it mostly original, but not completely like a MAC (Media Access Control), or ipv6 (Internet Protocol Version 6) address would be. The originality of the identifiers makes tracking via TPM not only possible but more economical than an aerial visual vehicle tracking technic. (In theory) [2]

Although the students did find some glaring security vulnerabilities, there was a great deal of integral continuity through the form of the general behavior of the tire pressure monitoring systems. The way that TPMs communicate is by being "woken up" by a short range LF (low frequency) signal at 125 kHz from the central TPM antenna once the TPM antenna is given the signal from the TPM ECU. The location of the TPM antenna is traditionally on the rear window of the vehicle. The TPM is asleep most of the time. The "wake up" only occurs when the car is running its initial power on sync, and periodically (every 60-90 seconds) when the vehicle is at speeds of 40km/h (25MPH) or higher. This behavior is by design with the intent of making the small battery in the TPS last for the lifetime of the valve stem in the wheel. Once the TPM is awake it will communicate with the central TPM antenna (usually over a frequency of either 315MHz or 415MHz along with frequency shift keying and amplitude shift keying) by sending its sensor ID (the 32-bit identifier) and the payload data (the tire pressure). If the ID matches one of the IDs, the TPM ECU synced with initially at power on will accept the data and display the low tire pressure light if need be. The nature of the TPM infrastructure makes it fairly impractical to track vehicles with a stationary TPM reading device at an off ramp or in a parking lot. If you assume the signal sent reaches the reading apparatus; the attack will still more than likely be rendered useless because of the signal sending so infrequently. Also, the 32-bit unique ID is not intended to mark each TPM individually but instead identify the position of each TPM in proximity to where it is in the car for the TPM ECU. The students were, in fact, able to spoof the TPM signal to the TPM ECU. The ECU only accepts packets with an ID that it recognizes from one of its tires. An antenna and a low noise amplifier can easily sniff, and

then attain the ID of any tire. Once you have obtained an ID, all that you need to do is send a packet with the alert bit turned on regardless of what you spoof the PSI to be and the dashboard light will activate. The simplicity of spoofing packets illustrates that it is unlikely there is any input validation used by the TPM infrastructure. Even with the easily fooled TPM system, the students were still unable to affect any ECU aside from the TPM's ECU due to its high level of sandboxing. In conclusion, you do not need to concern yourself with the thought of a hacker taking control of your brakes via your Tire pressure monitors, only the mild inconvenience of him turning on your low tire pressure light until you drive out of his transmission range [2].

IV. Vulnerabilities of Wireless access for vehicular environments

In the United States, the automotive field is an exponentially expanding industry. In 2016, over 85 % of households own at least one vehicle, and 16.4 million new vehicles were sold to consumers and introduced to the streets. Although there are many cars on the road and over 3 trillion miles are traveled annually by Americans, there are fractionally only a small number of traffic accidents (Estimated 5.5 million). Fractionally the number of fatalities was low as well (Estimated 33 thousand) [5]. Statistically, it is about as safe to fly in an airplane as it is to ride in an automobile mile when compared with fatalities per mile traveled. Every year there are hundreds of millions of dollars spent on safety testing and implementations by automotive makers on collision based safety applications such as airbags and safety crunch zones. In spite of these efforts proving beneficial every day, there is still room for improvement. That is where WAVE comes into play with technologies such as collision avoidance and post-collision emergency dispatching. WAVE (Wireless Access in Vehicular Environments) is the core protocol for several services [6]. The two primary services are V2V (Vehicle to Vehicle and V2I (Vehicle to Infrastructure). The purpose of both of these systems is generally for improved safety in situations such as the following [6].

- Warning for hazardous conditions via alerts (such as congestions, accidents, obstacles, etc.),
- Merging assistance,
- Intersection safety,
- Speed management,
- Rail crossing operations,
- Priority assignment for emergency vehicles.

These systems are not integrated into the road systems of the United States or in Europe, yet predominantly due to the government owning the 5.9 GHz spectrum, which would be the most desirable range of these systems. Internet service providers also want the 5.9 GHz band for the purpose of expanding the implementation of autonomous cars. The FCC is currently working multiple outcomes in which both infrastructures could flourish [5].

OBUs (On Board Units) and RSUs (Roadside Units) construct WAVE. The OBU's communicate with other OBU's for the service of V2V. OBU's communicate with RSU's for V2I [6]. This type of network, with no central controller, is known as a VANET (Vehicular Ad-Hoc Network). A VANET is necessary for the automotive environment because of the highly dynamic nature and the requirements of such little delay that a central controller would not be able to provide. VANET communication functions on an IEEE 802.11 protocol sculpted for this implementation specifically created for WAVE called 802.11p (also known as Dedicated Short-Range Communication or DSRC) [5]. 802.11 For WLANs and 802.3 for Ethernet traditionally uses CSMA (Carrier Sense Multiple Access) for its MAC (Media Access Control) collision avoidance. IN CSMA a node will listen to the channel for a given period. Once the channel is free of traffic, the node will send its packets. If another node sends its packets at the same time, the packets will collide, and the data will become corrupt. Then notifications will be sent to each node. At that point, each node will begin a timer set to a locally generated random time in milliseconds. Once that time is up, it will restart the process and check to see if the channel is clear and send its packets again. It is very rare for both nodes to generate the same resend time. This process is unsuitable for V2V communication, because of its inherent network delay even with a 100% fully functional environment. Because vehicles are going to be barreling down the road at 70MPH, changing lanes and potentially putting people's lives in danger, the updates and data transmissions need to be instant. In response to this flaw, Hakan Lans developed STDMA (Self-Organizing Time Division Multiple Access). STDMA uses an algorithm that is decentralized, yet unpredictable, making it not ideal for an office or infrastructure LAN, but very suitable for things such as collision avoidance between vehicles and other instances that need to be transmitted in real-time [5].

In any situation where wireless communication is present, any technicians first thought should always be "What can be done to maintain the confidentiality, integrity, and authentication of the data and service being provided." Unlike the previously talked about services, Mirrorlink, and tire pressure monitors, the 802.11p Task Group built WAVE with security in mind. Regarding confidentiality, each OBU has an entirely randomized IP (Internet Protocol) and MAC address. The 48 bit long MAC address will be created new and randomly generated every time there is a MAC collision or every 5 minutes, whichever comes first, to prevent vehicle tracking Via the OBU. PKI (public key infrastructure) ameliorates the terms of integrity and authentication and has been around since the early 90's. PKI is a set of rules and procedures used to create, administer, and revoke digital certificates. There is also some security built into WAVE by the nature of how it operates. Packets in transmission need to be quickly interpreted by the network; thus they need to be short, which makes it particularly hard on a perpetrator attempting to sniff the network [7].

V. Conclusion

In this paper, I presented that complete cyber security is of the most sought-after ambitions of all automotive companies as they continue to adopt and construct more technologies progressively. As Dwight D. Eisenhower our 34th president stated perfectly, “We will bankrupt ourselves in the vain search for absolute security.” The new technologies discussed in this study include Mirrorlink infotainment systems, tire pressure monitors, and WAVE Infrastructures. This paper displayed that Mirrorlink seems to be the least secure of the three, with the three college students from George Mason University successfully being able to infiltrate a generic infotainment system; and from there proceed through the CAN Bus to achieve some legitimate maliciousness such as start the engine and manipulate the brakes. This paper displayed that although the tire pressure monitoring is susceptible to manipulation, due to the high level of sandboxing within the infrastructure, there is no need at this point for any consumer concern. Lastly, this paper displayed that WAVE technologies have been implemented with security having the utmost importance on the technician’s minds, as they use the tried and true method of ensuring confidentiality and integrity with the usage of Public Key Infrastructure and also ensuring availability with the creation of IEEE standard 802.11p. My hope is that these analyses presented the reader a better understanding of some of the technologies that are present in daily driving, as well as the security measures taken to keep the consumer safe.

References

[1] Klinedinst, “On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle,” [Online.] Available: https://insights.sei.cmu.edu/cert/2016/04/onboard-diagnostics-risks-and-vulnerabilities-of-the-connected-vehicle.html

[2] Rouf, “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study,” [Online]. Available: http://www.winlab.rutgers.edu/~Gruteser/papers/xu_tpms10.pdf.

[3] Mazloom, Rezaeirad, Hunter,”A Security Analysis of an In Vehicle Infotainment and App Platform,” [Online.] Available: https://www.usenix.org/system/files/conference/woot16/woot16-paper-mazloom.pdf

[4] Sweeny,”Researchers Uncover Car Infotainment Vulnerability,” [Online.] Available: http://www.darkreading.com/vulnerabilities---threats/researchers-uncover-car-infotainment-vulnerability/d/d-id/1326807

[5] Khairnar, Kotecha, “Performance of Vehicle-to-Vehicle Communication using IEEE 802.11p in Vehicular Ad-hoc Network Environment,” [Online.] Available: https://arxiv.org/ftp/arxiv/papers/1304/1304.3357.pdf

[6] Yitasa, “Vehicle to Infrastructure interaction (V2I),” [Online.] Available: http://www.mogi.bme.hu/TAMOP/jarmurendszerek_iranyitasa_angol/math-ch09.html#ch-9.3.1

[7] Li, Mirhashemi, Laurent, Gao, “Wireless Access for Vehicular Environments,” [Online.] Available: http://www.mehrpouyan.info/Projects/Group%205.pdf