The Connected Vehicle:

Vulnerabilities, Future, and Security

Cory Church

April 16, 2017

Abstract

This paper will focus on the threats and vulnerabilities in the new field of connected cars. With most car manufacturers trying to push out connected cars as quickly as possible it is becoming apparent that they may not be putting as much time and money into the security of their vehicles. In the paper, several vulnerabilities that have been discovered and tested will be discussed and we will see how these we patched in the cars that were affected. We will also consider how companies can better secure their vehicles before putting them into mass production. Lastly, the paper will try to see if the benefits of having our cars connected to the internet out way the risks and what it means for the future of self-driving cars.

Keywords: connected car, vulnerabilities, security

In a time where we are connecting everything we own to the internet, it is only a matter of time before every car is connected also. This sounds like a good idea on the surface; but how secure is it really? With advancements in connected vehicles happening faster than ever it is time that we take a closer look at these vehicles and the security around them. We must look at if we can trust the companies creating these vehicles take the proper precautions in protecting them from attacks. In this paper, I will put most of the focus on privacy concerns, vulnerabilities, the future of the connected car, and securing vehicles in a connected future.

The first thing we must look at is a brief history of how connected cars came to be. The first step to fully connected cars came about in 1996 when OnStar was founded as a subsidiary of General Motors. OnStar was founded as a telematics company, a company that uses telecommunication systems to transfer information. The primary focus of OnStar was to provide assistance in an emergency situation. This was a time when not everyone had cell phones and OnStar provided a way to contact emergency services during an accident. As time went on the systems in cars became more advanced; by 2003 OnStar added vehicle diagnostics and turn-by-turn direction services ("How OnStar Works", 2006). This was the start of having cars completely connected to the rest of the world. In 2014 Audi released the first car to have an OnStar 4G LTE connection. This provided users the ability to use the car as a Wi-Fi hotspot but also exposed the car to the internet. With the implementation of more technology into vehicles, it has allowed these systems to control more aspects of the vehicle. Today the OnStar system can remotely slow down or disable your vehicle with their Vehicle Assistance Feature ("OnStar Security"). OnStar is not the one connected vehicle solution; many automakers have there on form of connected cars. The vehicles have what are known as infotainment centers that have access to features of the vehicle and can have applications installed on them. However, these

features are typically expensive options that not all car buyers can afford. Plug-and-play add-ons have been very popular the past few years. The device plugs into the vehicles OBDII port and usually is paired with a smartphone application. Features added by these devices include tracking, engine starting and stopping, unlocking/locking doors, and adding Wi-Fi to your car ("Connected Car offers plug-and-play remote vehicle access", 2015). These systems in cars are getting more advanced with every new iteration of vehicles. So, while connected vehicles are allowing users to have more features in the car they are also giving the cars computer system more access to the vehicle's infrastructure.

Before we can look at the vulnerabilities of a connected vehicle we must look at how cars in general work so we can see how the vulnerabilities affect the vehicle. While the technology inside the vehicle has become more advanced a person would assume that the vehicle's infrastructure would have been updated as well; however, that is not the case. The underlining infrastructure of the car has remained relatively the same since the mid-1980s. The tasks in a car are performed my Electronic Control Units (ECUs) these devices communicate on the Controller Area Network which is commonly referred to as the CAN Bus. The CAN Bus allows ECUs to communicate without the need for a centralized computer (Mucevski, 2015). Since this is a bus system only one node can transmit at a time. If one node is transmitting, then all others on the network are switched to reviving nodes to intercept the message. The CAN Bus terminated at the On-Board Diagnostics (OBDII) port

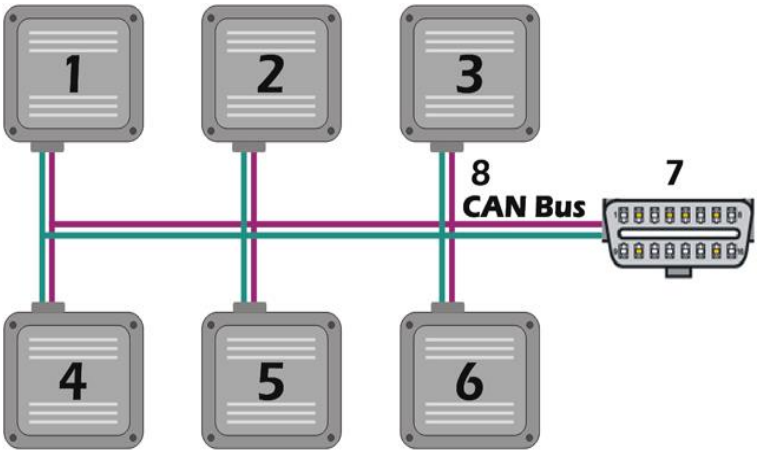

Figure 1: CAN Bus

(Figure 1) which is required on any car made after 1996 (Mucevski, 2015). This port is what allows an add-on to be plugged in and control a certain aspect of the CAN Bus. The built-in infotainment centers in newer vehicles work in a similar way. They are not connected to the OBDII port but instead have a direct connection to the CAN Bus built-n to their circuitry. The connected systems send communications over the CAN Bus to control aspects of the car. With control over the CAN Bus one of the things, the connected system can start and stop the vehicle engine with the remote application.

Now that we have covered how a connected vehicle uses the CAN Bus to interact with different components of the car let's look at privacy in connected vehicles. As more and more vehicles are becoming connected privacy concerns have arisen from the general public. The data that your car collects about you is not normally stored on the car itself. This data is uploaded to the cloud for remote storage. Per an article published in the Association for Computing Machinery Journal, a connected car can upload more than 20GB of data per hour (Coppola & Morisio, 2016). This data not only includes diagnostic information about your vehicles but can also include GPS locations and personal information associated with your vehicle and device connected to it. In the same article, it is stated the about 37% of people surveyed do not want a connected car because they are afraid of data leaks (Coppola & Morisio, 2016). So, your vehicle is loading quite a bit of information per hour to a remote site for storage. Users are now questioning if the information their vehicle have is kept in a safe manner. With all the information that can be collected by connected cars, automakers are going to have to be responsible for how they handle the information. Vehicle makers are going to have to be transparent with the information that they collect about customers and what information the vehicle stores. The manufacturer also must provide a secure way to store vast amounts of

information about the vehicles. For many car makers, this is something they have never taken on before so it will provide a challenge that must be overcome for vehicles and data to be secure.

Now that we have seen some of the privacy concerns associated with connected cars we will look at some of the vulnerabilities with these vehicles. As with any device connected to the internet, there are many vulnerabilities in connected cars. The infotainment centers in new vehicles allow for third-party applications to be installed in the car. It is possible for these apps to be more vulnerable than the car itself and may allow a way for attackers to penetrate the system. Similar to embedded apps in the vehicle itself any malicious app that you have on your phone that is connected to your vehicle has the potential of doing harm to your car also (Coppola & Morisio, 2016). As I discussed earlier you can buy devices to plug into your car's OBD port to monitor your vehicle. These devices can be less than 15 dollars. However, if the device you buy for your car is a compromised device it could be used to collect your information or upload malicious code. These devices are often sold from unknown company based in China so they may not be as secure as the customer would think. In addition to the compromising applications and OBDII port, many vehicles are being shipped with wireless access. The Wi-Fi access in cars makes them susceptible to the vulnerabilities that all wireless networks face. Security issues have not been mitigated in vehicles CAN Buses even though the messages sent over this system can be life-threating. With the implementation of 4G connectivity in vehicles, it enables a hacker to perform long-range exploits on the vehicle's CAN Bus (Woo, Jo, & Lee, 2015).

Now that we have looked at a few of the generic vulnerabilities that can affect the connected car. Now we are going to look in-depth at an exploit that was researched and unveiled at the Blackhat conference in 2015. This exploit deals with select models of Chrysler's vehicles that have an infotainment system known as Uconnect and a 4G connection for the use of Wi-Fi

in the vehicle. A vulnerability in the system allowed hackers to gain access to any information stored there such as phone and GPS records. Once the Uconnect system is compromised attackers could navigate to the vehicles CAN system to take remote control of the vehicle's functions. It is estimated that the vulnerability could have affected close to half a million cars. There were several problems in the Uconnect's software but the major flaw was one that allows for remote connections via a cellular network. So how did the researchers discover this vulnerability? When running netstat on the vehicle the researchers noticed many open ports a lot of which were proprietary to Chrysler and one that stuck out to them port 6667 (Figure 2). Knowing that there was not an IRC server on the vehicle the researcher dug deeper and found that this port was being used as D-Bus over IP. A D-bus allows for remote procedure calls to be sent to the vehicles meaning that code can be executed on the vehicle from another location (C. Miller and C. Valasek, 2015). Traditional a D-Bus does allow for authentication; however, Chrysler's programming allowed for anonymous login without a password. The vehicle used Sprint's network for its 4G connection. This made it where the vehicle had to be accessed on Sprint's network using a hotspot on the attacker's laptop Once gaining access to the D-bus, remote code can be executed to control many elements of the CAN system in the car. In the white paper by the researchers, they talk about the difficulty they had figuring out how to send a command to the CAN system to control the vehicle (C. Miller and C. Valasek, 2015). However, once this was

```
# netstat
Active Internet connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        State
tcp        0      0  144-103-28-21.po.65531 68.28.12.24.8443       SYN SENT
tcp        0     27  144-103-28-21.po.65532 68.28.12.24.8443       LAST ACK
tcp        0      0  *.6010                 *.*                    LISTEN
tcp        0      0  *.2011                 *.*                    LISTEN
tcp        0      0  *.6020                 *.*                    LISTEN
tcp        0      0  *.2021                 *.*                    LISTEN
tcp        0      0  localhost.3128         *.*                    LISTEN
tcp        0      0  *.51500                *.*                    LISTEN
tcp        0      0  *.65200                *.*                    LISTEN
tcp        0      0  localhost.4400         localhost.65533
ESTABLISHED
tcp        0      0  localhost.65533        localhost.4400
ESTABLISHED
tcp        0      0  *.4400                 *.*                    LISTEN
tcp        0      0  *.irc                  *.*                    LISTEN
```

Figure 2: Netstat

figured out they could control pretty much control every function of the vehicle from acceleration to shutting off the engine. With vulnerabilities like this one being found more research needs to be completed before these cars go to market. I think that is a good thing that people are trying to hack these vehicles and report the problems to the automakers. If It was not for the whitehat hackers, then these vulnerabilities would eventually be found by individuals that would exploit them or sell them to over people.

Even with these vulnerabilities, car manufacturers are pushing forward with the advancement of connected cars. Many automakers including Ford, General Motors and Volvo are in pursuit of fully autonomous vehicles. Even companies that are not traditional automakers, such as Google and Uber, are trying to develop autonomous vehicles before anyone else. The major player in the autonomous car competition is Tesla. Tesla already has semi-autonomous cars on the road that allow the car to mostly drive itself including steering and acceleration. The caveat to this is that a drive must be behind the wheel at all times. This system is also only designed to work on roads like the interstate where the car is traveling straight for the majority of the time. Late 2016, Tesla announced that all their cars in production will come equipped with all hardware required to be autonomous including surround cameras, ultrasonic sensors, and a radar. Elon Musk, Tesla's founder, stated that by the end of 2017 a Tesla will be able to drive from LA to New York with no human intervention. In addition to autonomous cars, a lot of manufacturers are focusing on a connected car infrastructure. Currently, connected cars only focus on connecting the car to its operators and providing benefits to the user such as Wi-Fi. In development is a system that connects all vehicles together using a Dedicated Short Range Communications channel that operates on a reserved spectrum (Pina, "PDF"). This communications channel will allow cars to communicate with each other alerting the car and

driver of hazards around them. These hazards could include other vehicles merging into your lane, heavy braking in front of you, or even when traffic lights are about to change. This infrastructure is going to be useful in implementing an environment where autonomous vehicles can strive. With every vehicle connect to one another the cars will be able to communicate with each other and better predict what is going to happen.

With connected cars becoming widely available and more features being added yearly we will need better ways to secure these vehicles in the coming years. One step that could be taken is to replace the outdated systems. The CAN bus systems currently in vehicles do not provide any authentication encryption or confidentiality. This means if someone has access to your OBDII port then they can get all the information off your car and possibly take control of its functions. Also, the CAN bus does not have source and destination addresses. Each control unit simply sends its messages and all other units must decide if it is related to them or not. This means there is no way to tell where the source of the message is. Anyone with access to the CAN bus can send the control messages to each ECU and have control of your vehicle. A fix that came out a couple of years ago is CAN-FD this is a new CAN system that adds fields for the source and destination MAC in the CAN frame providing at least some security in who sends the frame and where it goes (Mooney, 2015). This solution is not highly adopted and still does not provide any authentication and MAC addresses can be spoofed easily. Another solution to the problems with CAN Bus is to replace it with an Ethernet solution. This solution would make it where vehicles could use the same security measures that traditional Ethernet networks use. These measures include ACLS, VLANs, and port security making the car's infrastructure much more secure (Mooney, 2015). Overall most of the responsibility falls on the car maker to provide securely connected access in their vehicles but users must also use caution when installing

applications to their car just like they would their computer. I think that the Ethernet solution would be a good alternative to the Can Bus. Ethernet is implemented in all business environment and residents. There are already protocols in place to secure and monitor Ethernet networks. These protocols could be moved over to the car based environment.

So, in closing; the connected vehicle is growing at an exponential rate and the security around the vehicles is staying stagnate. With the growing threats to connected vehicles, I think car manufacturers need to focus on improving the security implemented in their vehicles and into developing a more secure car infrastructure.

References

*****C. Miller and C. Valasek. Remote Exploitation of an Unaltered Passenger Vehicle. In Black Hat USA Briefings, 2015.

Connected Car offers plug-and-play remote vehicle access. (2015, February 1). Retrieved April 15, 2017, from http://www.itsinternational.com/categories/utc/products/connected-car-offers-plug-and-play-remote-vehicle-access/

*****Coppola, R., & Morisio, M. (2016). Connected Car. ACM Computing Surveys, 49(3), 1-36. doi:10.1145/2971482

How OnStar Works. (2006, February 08). Retrieved April 15, 2017, from http://auto.howstuffworks.com/onstar1.htm

OnStar Security. (n.d.). Retrieved April 15, 2017, from https://www.onstar.com/us/en/services/security.html

Mooney, J. (2015, October 19). Securing the Future of the Connected Car. Retrieved April 15, 2017, from https://www.wirelessdesignmag.com/article/2015/10/securing-future-connected-car

Mucevski, K. (2015, December 8). Automotive CAN Bus System Explained. Retrieved April 15, 2017, from https://www.linkedin.com/pulse/automotive-can-bus-system-explained-kiril-mucevski

Pina, M. (n.d.). HOW CONNECTED VEHICLES WORK [PDF]. Department of Transportation.

*****Woo, S., Jo, H. J., & Lee, D. H. (2015). A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN. IEEE Transactions on Intelligent Transportation Systems, 16(2), 1-14. doi:10.1109/tits.2014.2351612