The Underlying Vulnerabilities of Smart Cars and Proposed Solutions

Michael Guerrero
University of Delaware

Michael Figura
University of Delaware

Abstract

In the ever changing world of technology, security is not only evolving but also becoming more and more necessary in different facets of technology. One such facet where security has come a long way is computer software. Some of the first computers were secured with extremely basic encryption methods such as DES (data encryption standard), which was the very first standard established for securing information on computers. Now, an algorithm like this can be cracked in seconds and modern day computers can be secured with algorithms that are unrealistic and, in some cases, nearly impossible to crack. While some areas of security have improved with technology, others have fallen severely behind. One such area is the security of modern day vehicles, which has fallen behind significantly with respect to today's advanced vehicle technology, especially within the past few decades. Since the focus of both automobile consumers and manufacturers is cost and efficiency, more resources have been put towards improving the technology of vehicles rather than their security. This has caused tremendous advancements in today's vehicles that appeal to consumers. However, in some cases the current security of a car is the same as that of a car produced a decade or so in the past. If this were to occur with computer security, for example, the consequences would be catastrophic and affect billions of people. Although automobile hacking is currently less common, the consequences of each event can be much more physically dangerous, highlighting the need to focus more on improving car security in the near future.

The plethora of new advancements in automobile technology has opened up a floodgate of vulnerabilities, leaving modern day vehicles more accessible to hackers with each new piece of technology implemented in the vehicle. This dates back to the early 1970s with the creation of the first ECU (electronic control unit) which was initially used to help regulate emissions to abide by the Clean Air Act of 1970. Since then ECUs have completely revolutionized the way automobiles function and modern day vehicles may have over a hundred ECUs all of which perform different tasks.While the implementation of ECUs is a huge advancement for the automobile industry it has not come without its fair share of problems. Since the system of a vehicle is made of interconnected ECUs which control the majority of a car's functionality, this is the main point of attack for an adversary looking to access a vehicle. For this reason

we have decided to make the focus of this paper on the vulnerabilities in ECUs and how they can be corrected, as it is quite likely the most efficient way to completely secure the entire system of a vehicle in the future. In this paper we will discuss the current and future state of ECUs and what we believe must be done in order to counteract potential hacks before any real-life harm occurs.

I. Introduction

Initially used to regulate fuel emissions, ECUs have come a long way in improving the functionality of modern day vehicles. As more ECUs were added to serve different purposes, vehicles were able to not only become cheaper but also much more efficient. As more and more ECUs became implemented, these ECUs became interconnected in a network within a vehicle. Eventually, there became such a large number of ECUs that subsystems within a car began to form based on the purpose each ECU served. This further increases the efficiency and functionality of vehicles, which is extremely important because ECUs must function in real time so that a driver experiences virtually no delay when using a function of the car. Originally these networks that were formed had no way of communicating with the outside world. Since then, the advent of the IoT (internet of things) has lead to a more connected virtual world, opening up these networks to the outside environment. Because these networks of ECUs are now open they have become much more vulnerable to attacks. Initially the security implemented in ECUs was designed very minimalistically due to the fact that they were on a closed network but since then not much has been added to make up for the new features. With the IoT cars are now communicating with various other technologies such as other cars, infrastructure (road signs, traffic lights, etc.) and other devices (phones and other application based technologies). We classify these types of communications as V2V (vehicle to vehicle), V2I (vehicle to infrastructure) and V2X (vehicle to other devices). The IoT is becoming increasingly prevalent in car models year after year, and is a very integral part of vehicle security. Below we reiterate the different communications in more detail.

Vehicle to Vehicle (V2V)

V2V communication relies on using vehicular ad-hoc networks (VANETs) to broadcast information to other vehicles on the road making the roadway safer [1]. This was first introduced in 2001 to pass data amongst cars on the road. Since then, many companies have experimented with and implemented communication between vehicles. This could become problematic in the future. Currently a single car may be compromised however as cars become more interconnected a hacker will potentially be able to gain access to multiple cars by utilizing the car that was initially

compromised. In addition, autonomous vehicles incorporate a technology called LiDAR, which is another example of V2V communication. LiDAR uses lasers that produce light and functions similarly to a radar to accurately detect objects (citation). While this technology is extremely helpful it introduces an entire new set of vulnerabilities.

Vehicle to Infrastructure (V2I)

V2I communication is the concept of connecting vehicles on the road with the infrastructure around them such as traffic lights. In the future it is predicted that this system of communication will become widely used and as vehicles get further connected to each other they may eventually become connected with the infrastructure around them in order to make driving safer and more efficient. A modern example of this that is widely used is the E-ZPass. This enables cars to pass through toll stations without having to stop, which helps the flow of traffic tremendously on large highways and removes the hassle of stopping to pay the toll. The E-ZPass gets displayed in the vehicle and V2I communication occurs when each device is scanned by a sensor set up on every toll booth. Eventually, if all vehicles were connected to a central network, it would allow traffic lights to save energy by dimming or shutting off when no cars are nearby and also giving emergency vehicles higher priority in order to allow them to safely pass through traffic to arrive at their destination by changing lights [1]. All of this is extremely useful in furthering safety on the road while also decreasing traffic and emissions. While a traffic light can be used to help increase efficiency if an attacker gains access to it, he or she could tamper with it illegally and even cause harmful accidents on the road. As with V2V communication, there are a plethora of benefits, but also plenty of risks due to flaws in the security of both the vehicles and infrastructure.

Vehicle to Other Devices (V2X)

The third and last main form of communication is V2X which involves connectivity between the vehicle and any type of network enabled device. Some examples of this technology are bluetooth and WiFi connectivity. This has impacted the vehicle industry significantly more than the other forms of communication, as smart phone connectivity is integrated into nearly every modern day vehicle. Some vehicles even have the ability to connect to the internet directly. An example of one such technology is MirrorLink, a protocol that applications use in order to connect with an in vehicle infotainment (IVI) system. The smartphone acts as a server and the vehicle acts as a client and mirrors the display of the phone onto the infotainment system of the car. MirrorLink uses DAP (device attestation protocol) in addition to content attestation, which uses certificates to authenticate the server to the client and a pair of messages

that allow the client to verify the received content from the server. A set of public and private keys are also exchanged to ensure that devices connecting to the vehicle are trusted users. Going even further, there is an added layer of security to prevent man in the middle attacks. Despite these multiple layers of security MirrorLink is still vulnerable. If an adversary is able to obtain a similar vehicle or simply a vehicle with a similar IVI system, it would not be difficult to find and exploit vulnerabilities in the system and use them to gain access to the target vehicle. One of the vulnerabilities that were found in recent IVI systems was the Micom CAN controller firmware which can be directly updated without any verification. When users attempt to update the system, no authentication or verification checks are found and thus there is virtually no protection from a malicious update. It was also found that the CAN controller also contains no key exchange or any form of encryption, causing massive vulnerabilities in the security of the system. [2] These are some of the many vulnerabilities involving the CAN (controller area network), which we will explain in more detail later on in the paper. Smartphone connectivity is becoming more and more common in vehicles each year, and while at first it was only through Bluetooth and WiFi connectivity, more recent advancements such as MirrorLink have created more vulnerabilities.

Recent technology has allowed the IoT to become extremely prevalent in today's vehicle and it is only becoming more and more integrated as newer vehicles are produced. All of these advancements can be attributed back to the invention of the ECU in 1970. The very first ECUs managed basic engine functions and brought improvements in performance and fuel efficiency. The need for them stemmed from the Clean Air Act, which was passed the same year as the ECU and imposed strict emission regulations. The early ECUs gathered data, monitored system and regulated vehicle systems. Initially starting as a microcontroller, the ECU has expanded into almost every aspect of the modern day vehicle. An ECU works by taking an input from a sensor and computing the data for the task at hand. In many cases, multiple ECUs must connect to each other in order to carry out tasks. One such example of this communication is between the gas pedal and the engine of the car, a signal is sent when the gas is pressed. The engine ECU receives the signals from the ECU that monitors the accelerator and is able to vary the fuel usage to be more efficient. Depending on the complexity of the car it can contain anywhere from 30 to 100 ECUs. [3] The higher end of this range is approaching the current limit of ECUs as there is finite space in the cars to hold the wires and ECUs. This has caused manufacturers to move towards virtualization, which allows functionalities that would typically be put on hardware to be run digitally in order to save space. While this provides vehicles with more capabilities it also opens up more potential

vulnerabilities. [4] The change from ECUs communicating on a closed network to an open network also bred more vulnerabilities. Initially, they were designed with the intent to just communicate with each other, but advancements in technology have made the network more accessible. These advancements include the aforementioned types of communications. Because of this there are many more access points for an adversary, especially in scenarios where the vehicle must connect to the outside world. Car software updates, third party app usage, and even direct connection to the internet in more modern cars are just a few ways that a car can be exposed to potential hackers. The consequences of these attacks can range from stolen vehicles to property damage or even accidents on the road. An experiment done in 2011 showed that researchers were able to gain access to a vehicle and locate it with GPS as well as unlock and start the vehicle. In July 2015 two researchers were able to hack into a Jeep Cherokee from a basement 10 miles away and remotely control the cars functions using a simple 3G connection exploiting a vulnerability in the Uconnect software. Uconnect is a software that controls the navigation and entertainment system in the vehicle with connection to the internet. By using this as an access point they were able to rewrite the firmware of the adjacent chip in the car's head unit. This exploit eventually caused the recall of 1.4 million vehicles. A year after this, the Mitsubishi Outlander Plug in Hybrid Electric Vehicle was hacked using a man in the middle attack between the car's mobile app and WiFi access point. The attackers were able to disable the theft alarm system leaving the vehicle vulnerable. Another exploit found by researchers that affected vehicle models dated back to 1995 enabled them to take advantage of the keyless entry system of the vehicle and physically break into the car. One of the only malicious attacks to date is when an angry ex-employee was able to access over one hundred cars and completely wipe their data, known as 'bricking' them. It is clear that vulnerabilities in the ECU are prominent and have real consequences. The majority of potential hacks on vehicles lead back to the lack of security in ECUs, which is why they are the main motivation for this paper.

II. The Problem With Current ECUs

As briefly mentioned earlier, ECUs have a plethora of security flaws, which makes them one of the most vulnerable aspects of security in modern day vehicles. The three main categories for attacking cars, as proposed by McAfee, are remote attack surfaces, cyber physical features and in-vehicle network architectures. ECUs are a vital part of the in-vehicle network architecture. [4] When ECUs and different buses are accounted for they form nearly the entirety of this architecture. As a result of this, in addition to the fact that the upper limit of ECUs able to physically fit in a vehicle is being approached, manufacturers

began grouping ECUs together in order to save space and increase the efficiency of the ECUs that require communication with each other or different parts of the vehicle. While this grouping may be able to significantly improve a vehicle's performance and allow for more functionalities, it also presents one of the greatest security vulnerabilities in modern day vehicles. If a hacker is able to gain access to any ECU through a single point in the vehicle, he or she would be able to send commands to other ECUs, essentially gaining control of the entire vehicle. Due to the lack of encryption in the buses, there is no way to verify if the messages being sent are legitimate are not. With relative ease an attacker can find out what network messages control each functionality of the vehicle and can manipulate them at will. ECUs are distributed among various buses and depending on the vehicle, are oftentimes grouped by location, different functionalities, or a variation of both. The main buses in modern day vehicles are the Local Interconnect Network (LIN), Controller Area Network (CAN), Media-Oriented System Transport (MOST), and FlexRay. The LIN controls functions that are not highly data-intensive such as door locks and mirror adjustment, CAN controls mid-speed functions such as the body systems and engine of the vehicle, MOST controls high-speed functions such as multimedia and electronic dashboards, and FlexRay controls safety functionalities such as electronic steering and braking. [5]

ECUs are interconnected throughout all of these buses, so it holds true that if one bus becomes compromised the others may also be easily compromised. The CAN bus, created in 1986, is particularly relevant as it contains ECUs with important functionalities such as the engine of the vehicle and contains minimal protection from an adversary. The CAN bus is responsible for connecting all of the ECUs together in a much more efficient manner. Before the advent of the CAN bus all of the ECUs were connected via point-to-point wiring. The implementation of this new technology resulted in weight reductions of over one hundred pounds for supporting car models. Unlike most networks the CAN bus doesn't work off of requests, but rather by certain devices continuously reading and outputting data. For example, the tachometer doesn't request the engine's rpm through the CAN bus; the engine's ECU constantly broadcasts it and the tachometer just reads it off the CAN bus. This gives the appearance that it is continuously changing and can happen many times a second. At any given time the CAN bus can be transporting thousands of unique signals from one to eight bytes in length. As a result of this the CAN bus is typically a very noisey, bandwidth-intensive environment. A typical CAN frame is made up of about twelve to fourteen different fields. Important fields worth mentioning are the arbitration field, control field, data field, CRC field and the start/end of frame fields. These fields are all varying lengths ranging from just one bit to

fifteen. The arbitration field contains eleven bits that identify the instruction and assign it a priority, as well as another single bit that determines if the ECU sending the signal must deliver or receive the message. The control field is mainly used to determine how many bits were sent from the ECU, as the length of the signal sent can vary. The data field is the section of bits that actually contains the message that is being transmitted or received. This is the part of the data sent by the CAN bus that ECUs send and obtain. The CRC field stands for cyclic redundancy check, and contains sixteen bits that determine how often the signal should be transmitted, which can vary up to many times a second, or be much fewer. The start/end field is the final field which contains a single bit that indicates the beginning and the end of a frame on the CAN bus. [6] With this information an attacker can spoof CAN messages and control a vehicle's functionalities. This is made trivial by the CAN bus's lack of encryption, authentication and segmentation. A lack of encryption opens up many security vulnerabilities that an adversary could exploit, as once the system is accessed there is little to prevent a hacker from reading and analyzing the data contained in the vehicle. One of the more critical flaws is authentication because without it there is no way to verify the frames being sent on the CAN bus, allowing attackers to easily spoof them. A lack of segmentation of the network allows attackers to easily infect large chunks of the network.This is largely due to the high level of interconnection between all the ECUs in the car. The fact that the ECUs are put into groups on the CAN bus saves a lot of space and weight in the vehicle. However, the fact that the ECUs are all in a network means that a hacker will easily be able to access multiple ECUs by utilizing connections between them. With the progression of technology the IoT has become much more prevalent in vehicles. This makes the network more open, in turn causing ECUs to be more susceptible to attacks. Early on, researchers found that a hardwired connection through the OBD (on board diagnostics) port was required in order to connect to a vehicle and inject malicious code. However, since the network of ECUs is now open, attackers can breach a vehicle indirectly through Wi-Fi or Bluetooth. Some vehicles allow mobile applications to connect directly to the car's Wi-Fi API and control its functions. If the method of implementation is done poorly, this makes the vehicle vulnerable to many security and privacy attacks. One example previously mentioned is MirrorLink, but others include Android Auto, Apple CarPlay, UPnP (Universal Plug and Play). These are all standardized protocols for smartphones to connect to the car. [2] Bluetooth is another common access point for an attacker, mainly due to the fact that the PIN numbers for cars often lack proper password security and are easy to crack by performing a brute force attack. Once a hacker has gained access to a vehicle's bluetooth system, he or she can find valuable information. This information

can range from things about the vehicle's network to leaks in privacy data. A vehicle is particularly vulnerable whenever a device is connecting to it via WiFi or bluetooth. An adversary can utilize this gateway in order to obtain semantics about the vehicle such as encryption data, and this is a common attack point for vehicles. In recent times, as autonomous vehicles become more prevalent, new vulnerabilities are being introduced through LiDAR, DSRC-based receivers, GPS and IMUs (Inertial Measurement Units). A car's LiDAR system sends out a signal, waits to receive it, then calculates the distance of objects relative to the car using the time it takes. An attacker can send false signals to trick the system into thinking an object is there, making the car come to a stop, which could have devastating consequences. DSRC-based receivers are popular among many cars on the road and allow communication to other DSRC equipped vehicles or infrastructure. DoS attacks, malware, location tracking, masquerading and black holes. [3] GPS is also fairly common among modern cars and is susceptible to spoofing as well as jamming. GPS spoofing is when hackers send a signal that they falsely crafted in order to mislead the GPS system. This can mislead a driver or even allow an adversary to locate or track a vehicle. Finally, inertial measurement units (IMUs) contain data from the gyroscope and accelerometers. This data can be changed and cause the vehicle to slow down. As these vehicles improve even further they must process more data, making it more likely for a scenario in which a vulnerability can be exploited to occur. Some such scenarios include two researchers being able to breach into and control a Jeep Grand Cherokee, the CAESS experimental analysis, researchers as well as adversaries locating and breaking into a vehicle and the Miller & Valasek physical/remote hack. The attack done by researchers on the Jeep Grand Cherokee is by far the most famous example of an attack on a vehicle. This is due to the fact that it caused the aforementioned recall of about 1.4 million vehicles. However, it also demonstrates the lack of security in these vehicles as well as the lack of effort the manufacturers are willing to put into. Initially, the same team of researchers was able to break through the car's security system through a direct hardwired connection as early as 2010. When the findings were presented this was not considered a large enough threat, so the researchers then demonstrated that once a hardwired connection was established the vehicle could be controlled remotely from miles away. It was not until the team was able to both access and control the vehicle remotely in 2015 that manufacturers were finally forced to recall the vehicles containing these vulnerabilities. This is one of the only occurrences of actions being taken due to the exploitation of these vulnerabilities, which are found in nearly every vehicle. In 2010, a research group from the CAESS (Center for Automotive Embedded Systems Security) found it was

possible to inject messages on the CAN bus and thus have control of certain functionalities of the vehicle. This was done through trial and error, and it was found that if enough messages are sent and received, eventually an attacker would be able to deduce which signals cause which functionality and then send those messages at will. For example, once the signal for turning a car's headlights on and off is figured out, all an attacker must do is transmit this signal to the vehicle in order to make it obey the commands. This trial and error style of attack can be done with little prior experience in car hacking. The researchers that performed this experiment received criticism for the experiment from both car manufacturers and the public, claiming that the research was incomplete. A year later the group performed the same experiment again in more detail and even acknowledged the criticism they received. The second paper failed to gain much attention from both the media and the auto industry despite the fact that important findings were published. [6] An interesting experiment to note is in 2011, when researchers were able to locate and access a vehicle by using both the GPS signal and keyless entry system of the vehicle. (9) This exact same method of attack was used by a group of hackers in the Netherlands shortly afterwards to locate and steal multiple Tesla vehicles, demonstrating that if nothing is done about these research findings it is only a matter of time until they translate into malicious attacks. The last example we mention is the Miller & Valasek physical hack, which consisted of two researchers physically connecting to the car's OBD-II port and reverse engineering the CAN bus communications. They first monitored the CAN bus for various messages to get an idea of which packets control which functions of the car. They then were able to send copied packets to execute certain commands within the car and eventually craft CAN packets of their own to manipulate the vehicle. Although the methods of attack in all of these examples are slightly different, they are all centered around the CAN bus and thus the ECUs of a vehicle. This is why improvement in the security of these ECUs is fundamental for the future of vehicle safety.

III. The Current Solutions

As vehicle cybersecurity is a relatively new and unexplored area, ECUs currently lack many necessary protective measures. This absence of security is also in part due to a lack of effort by manufacturers themselves as well as legal complications and regulations surrounding the production and assembly of the vehicles. Current laws hold car manufacturers liable for hacking incidents, which hinders the progression of developing new technology that could secure current technology as well as be useful in other fields. Additionally, since hacking is not a physical type of attack, there are not concrete rules to protect from it. This becomes more complicated due to

the fact that each hack may be completely different than other hacks that were attempted before it. Below, we will go into more detail about these multiple complications that may hinder progress in development, and are thus directly related to current and future solutions dealing with the security of ECUs.

Complications

Arguably the largest complications faced by any company or manufacturer are due to laws, regulations, and other legal setbacks. This is especially true in the case of vehicle security. Laws in place only account for the manufacturers themselves as well as the customers and other persons in the vehicles. However, vehicle hacking now introduces a third party that could potentially cause harm to the passengers of a vehicle. The laws of today are not completely up to date with this fact. If a passenger were to become injured due to a malicious cyber attack, it would not be considered his or her fault, and thus the manufacturers themselves would be held completely liable. As the issue of car security becomes more prevalent, the legalities surrounding it are being talked about more. Even so, there remains a large grey area about who is at fault, especially since these kinds of attacks can be very difficult to trace back to the attacker. For example, lawsuits have been filed against both General Motors and Toyota claiming that the vehicles they produced had security vulnerabilities. In both cases the companies won off the basis that hacking is so prevalent that it would only be a matter of time before vehicles would be able to become breached. [8] However, if an actual attack had occurred and damage had been done to a person or people, the outcome of the potential lawsuit may shift, again putting the manufacturer at fault. One proposed solution dealing with some of these legality issues is that the manufacturer must display that adequate effort was put forward towards preventing such an attack. This would allow manufacturers to hold themselves to a higher security standard without hindering them from seeking out new, more advanced features for vehicles. It may take years for laws to provide a concrete cybersecurity standard for the manufacturing of vehicles, which is why legal issues are definitely worth mentioning as a complication for current solutions.

Besides leagilites, other complications include the many various manufacturers involved with producing ECUs. The counterfeiting of electronic parts and components is a big problem. These parts often lack the necessary security measures and thus expose the car to more risk. Some ways of eliminating this risk are using authorized distribution channels, track and trace, and continuity of supply. Authorized distribution channels are used for the procurement of all components (software and hardware) used in the car.

Track and trace is used to detect critical components and parts used directly in the car's security. Finally, continuity of supply is the idea of planning ahead to make parts for spares and maintenance to ensure that the security doesn't become outdated. In addition to these three ways, the risk of faulty parts can be further prevented by breaking down the supply chain into four main parts. From the raw materials used to make each chip all the way up until parts are shipped, tracking each step makes it easier to focus on keeping components up to standards. However, this is made complicated by the large number of standards and organizations that produce them. With so many organizations involved there are sometimes overlaps between standards, but also conflicts amongst different standards. [4] This makes it more difficult for manufacturers to follow and creates discrepancies amongst parts, which is bad for the overall security of the car.

Another complication arises from the lack of motivation these manufacturers have to improve the security of their vehicles. Since car hacking is not very prevalent in society, the public doesn't know much about it and thus can not pressure for change. This in combination with the money and time saved from skimping out on security to produce more features forms the root of the cybersecurity problem in automotive technology. As a result of all of this, the cybersecurity of vehicles is outdated by multiple years when compared to that of a smartphone or computer, a problem which will continue to get worse unless something is done about it.

What Is Being Done Now

One defense mechanism being implemented now is over-the-air (OTA) updates. Over the air updates allow remote code execution by the manufacturer in order to keep vehicles up to date with fixes to the software, upgrades to the firmware, and security patches. While the effects of this method of security are bountiful, there is a high level of risk involved with sending updates OTA. These updates require another level of security within vehicles since they are distributed by connecting and sending out code to multiple vehicles. If this is not implemented in a secure manner it could result in severe consequences. Knowing this, researchers have focused their efforts more toward secure over-the-air (SOTA), which involves secure protocols in delivering updates and authenticating these updates to ensure that the code comes from the original source.

Cloud-based Solutions are another proposed solution because they provide a layer of security that filters the content of web traffic for viruses/malware and detects anomalies. This layer also encrypts the traffic between the network and the car. In addition to security benefits, a cloud-based

approach would solve one of the current issues faced in the vehicle industry, which is the inability to contain increasingly more sizeable and complex components within each individual vehicle. The ability to connect to the cloud would allow vehicles to save a large amount of storage within the vehicle's internal network, allowing for more advanced features within the vehicle itself. While these benefits are massive, it is unlikely that a cloud-based approach will be used in the near future due to current technology not being advanced enough to make it completely viable. Firstly, while the use of cloud-based updates provides high scalability as well as enhancements to the security of vehicles, if they are not implemented with absolute protection the consequences can become just as large as the benefits, if not worse. If an attacker is able to gain access to the cloud used for a group of vehicles he or she would be able to attack all vehicles in this group since the cloud-based approach produces a central point in which all vehicles involved are connected to. This becomes an issue because with this approach, if a single vehicle is able to become breached, multiple vehicles could potentially be at risk through connection via the cloud. In addition to the security risks of the cloud, this form of protection would also need a near-constant connection to the internet to be effective, which could cause high costs for both consumers and manufacturers. Most major countries are covered by massive networks of roads that allows drivers to travel to virtually anywhere within them. Modern day internet service providers and cellular towers are unable to cover this massive expanse of land, and thus it is possible that while a driver passes through a low-service area, the vehicle's connection to the cloud is lost. This segways into the issue of delays caused by connecting to the cloud. As mentioned earlier, it is absolutely imperative that all functionalities of a vehicle happen in real time, and even a few microseconds of delay can cause consequences. Connecting to the cloud would only increase delays within the vehicle, making this a risky solution with modern day technology. While these drawbacks make the feasibility of cloud-based solutions unlikely under current conditions, future advancements in technology may enable them to be the most effective solution pertaining to vehicle security.

A more encompassing plan is a layer-based solution, which was proposed by the national highway traffic safety administration. As is typical with most systems, having multiple layers of security within and around vehicles not only greatly decreases the chances of a successful attack, but also limits what an adversary can do once the vehicle in question has successfully been breached. The proposed solution contains four main layers of security; isolating critical safety subsystems, real-time intrusion detection, real-time response methods, and collection of information about successful hacks. This is

arguably one of the best solutions put forth to date. However, not much has been done to implement these features, most likely due to the difficulty of implementing them on such a large scale. [3]

The automotive industry has started taking defensive measures in order to protect connected cars, but many of the proposed solutions are not concrete and come with many flaws. This is mostly due to the lack of prior incidents as well as simply a lack of push from, and knowledge of the subject, by the public. This has caused manufacturers to overlook these flaws in favor of more advanced features within vehicles. However, we fear the industry may be falling into a rabbit hole, as these more advanced features will often require more advanced security measures to protect them.

IV. Our Proposed Solution

We wanted to take a more holistic approach when addressing the problem, since there is no one specific weak point to smart car security. From encrypting the messages being sent on the CAN bus to authenticating all outside connections to the car, we wanted to make sure we covered each possible point of entry for an attacker. While difficult to quickly implement on a large scale, our concern was more so on making a thorough solution that could be the standard for the automotive industry.

Our approach starts at the brains of much of the cars functionality, the ECU. Securing the ECU with a basic firewall is a good place to start. Preventing off chance intrusions in the can bus from causing significant damage. We plan on minimizing this further by encrypting the messages sent on the can bus. These are both tricky to implement because the ECUs have to operate within microseconds in some cases. A delay could cause a vehicle malfunction and possibly lead to more serious consequences on the road.

Changing the scope a bit, we focused on the outside connections the car has with potentially hazardous networks. As mentioned in the current problems section above, a big entry point for attackers is through mobile devices and other internet-connected devices. If we implement client-server certificates, this would lower the risk for unauthorized devices to connect to the vehicle.

The combination of these potential solutions gives us the ability to leave no stone unturned when it comes to securing vulnerabilities. A lot has to change on a much larger scale to make an impact, such as government intervention or an agreement between car manufacturers. Cause while a more secure ECU is feasible it doesn’t mean it will be readily accepted by the car industry.

Works Cited

[1] Bajaj, Ruhi K, et al. “Internet Of Things (IoT) In the Smart Automotive Sector: A Review.” *IOSR Journals*, 2018, www.iosrjournals.org/iosr-jce/papers/Conf.CRTCE%20-2018)/Volume%201/7.%2036-44.pdf?id=7557.

[2] Mazloom, Sahar, et al. “A Security Analysis of an In Vehicle Infotainment and App Platform.” *Http://Damonmccoy.com/*, 2015, damonmccoy.com/papers/ivi-woot.pdf.

[3] Eiza, Max & Ni, Qiang. (2017). Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security. IEEE Vehicular Technology Magazine. 12. 45-51. 10.1109/MVT.2017.2669348.

[4] Clare, David, et al. “Automotive Security Best Practices.” *McAfee*, June 2016, www.mcafee.com/enterprise/en-us/assets/white-papers/wp-automotive-security.pdf.

[5] Alam, Md Swawibe Ul. (2018). Securing Vehicle Electronic Control Unit (ECU) Communications and Stored Data.

[6] Currie, R. (2015, December 5). Developments in Car Hacking. In sans.org. Retrieved from https://www.sans.org/reading-room/whitepapers/internet/developments-car-hacking-36607

[7] Amara, Dinesh & Chebrolu, Naga & R, Vinayakumar & Kp, Soman. (2018). A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities.

[8] Wenzelt, S. L. (2017, May). NOT EVEN REMOTELY LIABLE: SMART CAR HACKING LIABILITY. In illinoisjltp.com. Retrieved from http://illinoisjltp.com/journal/wp-content/uploads/2017/05/Wenzel.pdf