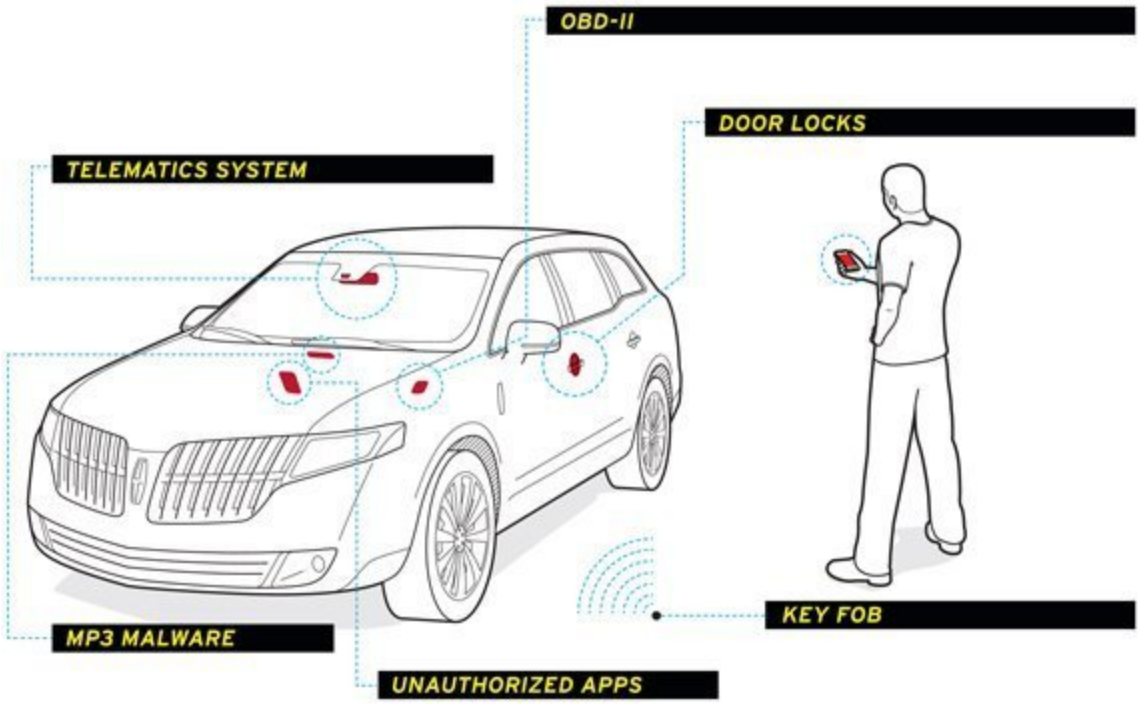
EEL 4789 Ethical Hacking & Countermeasures
Vehicle Hacking Research Paper



Dr. Pons
David Cabreja 3550938
Jose Garduno 3372887
Norvin Holness 3597833
Jose Maldonado 3754544
Jose Tormo 3819111

Introduction

Vehicle hacking is a fairly new subdivision of hacking that has emerged in recent years, it serves to protect or to potentially harm vehicle users. This has come into being due to the development of the new age of vehicles. Across the globe we are now seeing vehicles that are more computerized than ever before. The demand for this new style of vehicles is constantly increasing, because they make life easier for the user. Companies are now making vehicles that you can control remotely from your cellphone, ipad, or laptop. There is also the rapid introduction and encouragement for people to be more eco friendly and to switch from standard vehicles to electric vehicles. Much of the public transportation such as the bus systems in many states mostly consist of electric vehicles, also vehicles such as the Tesla Model S, and the Chevrolet Spark EV are becoming more popular amongst consumers. In the coming future we will see a dramatic shift from the traditional vehicle to the computerized vehicle age.

The downfall of this new era of computerized vehicles, is that they are just computers on wheels, which means that they have vulnerabilities similar to the ones that affect computers. Hackers take advantage of this setback, by trying various methods to wreak havoc on vehicles, for many different motives. Vehicle hacking is the ability to manipulate a computer controlled vehicle remotely, and since nowadays most cars have between 30 and 100 embedded control units in them, they are vulnerable to many attacks. These control units act as cpu's for cars, and also as a gateway to hackers. Essentially the new generation of cars are slowly becoming PC's on wheels. The cyber components that form the interface of these cars are built from the same kind of buggy components that are in personal computers. But unlike a personal computer the control systems that are actually running the car have no notion that an attacker can be on the line, manipulating the vehicle.

The most common ways that vehicles are hacked is through the diagnostic board under the steering wheel. Every software that is installed in a vehicle can be analyzed and controlled by this board. Now that cars are becoming more computerized, the brake, acceleration and steering system have unique software components, and also many vulnerabilities. In most cases hackers will usually hack and infect the computers in the vehicle repair shops, so that those computers can infect the customers vehicles through the diagnostic port. Another way to hack is via the bluetooth system, or using the cellphone network to break into the telematics unit, which would normally be used to provide roadside assistance, and also through the stereo systems. Now that the society is becoming more tech savvy, and the internet is becoming more of a necessity, many public transportation routes, such as the bus systems, air travel systems, railways and so on, provide free public wifi for the convenience of the passengers. Though this might sound comforting, it is also very risky, because in many cases hackers can access and manipulate through the wifi network.

Hacking vehicles can serve as a terrorist, or homicide attack, due to the fact that so many things can be remotely manipulated, and that you cannot just reboot your vehicle when it is being hacked when you're going at extremely high speeds. Hacking has been a mainstay in the PC era. Each day, reports concerning "hacking" grow and have increased dramatically. As our world becomes more advanced technologically, the hacking method has also become more sophisticated. These systems could easily allow hackers to take control of the vehicle, track the vehicle's location, unlock and start the vehicle via

mobile phones, disable emergency assistance, and possibly access devices connected to the vehicle, which includes smartphones, tablets, game consoles, notebooks, and other connected devices that contain valuable personal data and information. In other words, it's basically the same technology development designed for the greater good was used to hack connected devices. This threat however has already been handled by the auto industry through actively designing solutions to combat this issue. To be able to address the concern properly, manufacturing vehicle industry in general is teaming up with other providers to find the right components of software expertise.

Mechanical Targeting

As with everything in our lives, cars are starting to depend exponentially on computers systems to make them better, safer, and more affordable. In comparison to a 1980's vehicle, today's basic car contains a much larger quantity of sensors, data collection units, and programmable control units to handle all the tasks a car needs to do in order to achieve optimum efficiency, power, and safety. But are these machines safe from outside manipulation? In this section, we will go over the two major components in a car's "computerized" system that are vulnerable to attack.

To begin with, ECU's (Engine Control Units) control an engine's internal combustion capabilities to improve performance and efficiency. Early ECU's worked on mechanical and pneumatic means since the technology for micro controllers was not available at the time or was not economically feasible to implement. Today, we see programmable ECU's in every car made because of their affordability, but also bring the risk of being compromised. ECU's vary in location depending on the model and make of the car, forcing hackers to study the car they want to hack in detail. Once located the hacker could use are a variety of techniques to infiltrate the ECU ranging from replacing the ECU with an already hacked one, soldering special hardware, install a "middle man" part between the engine and the ECU, and finally accessing the ECU through the ECU's trouble shooter ("re-flashing"). The most popular way to hack into the ECU today is through the troubleshooter as it allows the hacker access and modify the code within the ECU through a laptop with the use of third party tools or self written scripts. The main issue with this particular method is the need to reverse engineer the manufacturer's code and protocols needed to make any changes.

Other than the ECU, the vehicle bus is one of the most important hackable parts in a car. To put it into perspective, the ECU controls the engine while the vehicle bus controls everything else. Everything from radio, electric car windows and lights are all controlled by the vehicle bus. (Although technically the ECU is part of the vehicle bus, it acts independently most of the time) It's important to note that the vehicle bus does work under a specific protocol so hackers must have knowledge of the way it works. Recently, hackers have found ways to implement cheap microcontrollers such as the raspberry pi into the vehicle bus, allowing modifications to be done in a much easier and safer fashion. For example, if we infiltrate through the vehicle bus we have access to the Telematics System (Used by police to disable stolen cars or to report a crash immediately). Another example would be access to the cars lock system, which we can disable if we had access to the vehicle bus. With control over the system, we could disable its function and allow a car theft to go unreported. Having the ability to control

the bus will allow a hacker to have control over all these electronically driven aspects a car has, leaving the car in a incredibly disabled position.

Uses of exploits

In Tim Burton's Batman Returns there is a scene when Batman parks his car in an empty alleyway and goes off to fight crime. As he is away from the Batmobile, Penguin, an arch-villain, attaches a device to the car. When the Batman returns and is driving his vehicle, the Penguin appears on his screen and the car begins to accelerate faster even though Batman is trying to brake. Although this is a scene from an older movie, today this is a fairly possible scenario, minus the close up on the monitor. When you have access to a car's internal network, you gain access to dozens of vehicle components. By exploiting vulnerabilities that are available, you may be able to:

- Blast the horn of the car
- Cause engine to accelerate
- Prevent car from powering down
- Change speedometer and gas gauge
- Jerk the wheel by disabling power steering
- Slam on brakes
- Tighten seatbelts

This is just a brief look into what can be accessed. Hackers can exploit these things to assault or harass a victim. This can even be used for burglary. Many modern cars have systems such as cruise control that can be exploited to drive the car away from a parked location. Onboard GPS could be used to track a car's location as well, making it even easier for someone to find the car.

Positive Uses

Not all hacking, as we all know, is meant for malicious purposes. Sometimes people hack things to suit their preferences or improve what they are working on/with. In the case of an automobile, gaining access and modifying the electronic control units (ECU) can allow your car to have more miles per gallon. Alternatively, you can raise the horsepower of your engine as well. Changing the oxygen and carbon dioxide input and output levels of engine, which is managed by the ECU, can allow you to do this.

Alberto Garcia and Javier Vidal, presenters at DEF CON 2013, demonstrate their open source exploits to make this all possible in a presentation they title "Dude, WTF in My Car?" To do this, he had bypassed an RSA encryption and flashed the ECU with custom software. Alberto discovered he could do this when he was tired of repeatedly fixing his friends' cars to install custom, aftermarket parts that modified the car. He wanted to make an easy, inexpensive way to do this. His exploit is now open source and available for all to enjoy.

Another legal use for exploiting the system can be to collect information about driver like

average driving speed, radio station usage, GPS locations, and sell or use information. Insurance companies would benefit greatly from this because they can adjust a rate in real time according to your driving habits. Progressive has a similar system in place but not as advanced as what is possible. In a way, this is much like websites track your footprints with cookies online.

Methods of Attack

Once we have explored the idea of successfully gaining access into the computer of a vehicle one begins to wonder how such task can be accomplished. Here we will explore the different methods available to actually gain access to the vehicles' mainframe and engage in an attack to successfully gain unauthorized right of entry.

There are a number of known ways to access a car's mainframe; some of them are through the telematics system, an mp3 malware, unauthorized apps, OBD-II, door locks, and key fob. All of them are currently known methods for gaining access by exploiting some vulnerability. A car is composed of an array of parts that function with some piece of software, by finding the exploits to these parts we are able to secure them better and thus some of these attacks have been already patched in some cases. In essence the information that's been released and explained is for educational purposes and it is not intended to be used since it would be illegal.

The Telematics System is used to notify the police in the case the car has been involved in an accident, or remotely disable the car if said car has been stolen as well as offer diagnostics to the user since it interacts with multiple systems within the vehicle. By gaining access to the telematics system it is possible to control any system connected to the CAN bus, hence one would be able to disable the ignition the same way the anti-theft system.

The MP3 malware, there are now ways to implement malwares into mp3 files and this can become dangerous quickly. If you obtain you mp3's from an unauthorized file sharing site you run the risk of stumbling upon a song with a virus with code to penetrate into the CAN bus and disable your brakes as well as any other system connected to the CAN bus.

Unauthorized apps is an ingenious way to gain access to today's cars. The way the hack works is just as a smartphone, there's thousands of apps developed by third party companies available to download, hence as car markers further develop the infotainment offering through downloadable software an app containing a virus or malware would be able to infect your car without you ever knowing.

ODB-II is the port where diagnostics are transferred and read. The research team at CAESS successfully wrote software that was then installed to the CAN bus through the OBD-II port which was able to literally control everything on the network. This is known as the most direct way to access a car's CAN bus since the code is sent directly to the CAN bus.

Although convenience has become a leading characteristic for the automobile industry it could also be the downfall of a good security system. Today's cars come built with a power-locking mechanism connected to other vehicle systems for the purpose of locking the car doors automatically when the car is in drive and unlock is the airbags deploy. This intercommunication could become a

gateway to breach other systems of the car, therefore, a reverse engineering technique could be deploy and have the power locks force to accelerate the car.

It's almost unbelievable the amount of way one can breach a car. The most vulnerabilities lie in the fact that the systems are all interconnected or have a cause and effect that can be breached and reverse engineered to cause the car to go haywire. The effectiveness of the hacking depends on how good the perpetrator is and how well has the company ensure that the system do not become accessible. It's true that so far the most direct way to hack into a car is by directly plugging oneself to the OBD-II and directly send code in order to take over, yet, today we see cars we Bluetooth systems, internet capabilities, unmanned vehicles that work with sensors, and so on which will make the breach more accessible through a wireless attack.

Future of Vehicle Hacking

Technology simplifies life, but in our current era life revolves around technology. We live in an era where manual functions are being replaced by digital ones. We know the possibilities of a phone, or PC being hacked, but your car is now a potential threat. This is scary, but not as scary of the possibilities the future holds. In the past hackers were able to tap into a BMW factory and override a port in to gain access to the digital key code door lock, without triggering the alarm. They were able to reset and create new codes and drive off with the cars. This is one of the few possibilities of hacking, there is also an automatic link box that can connect to mobile phones in the car and obtain information from the phone like GPS and can tell the driver speed and mileage. This is a potential threat because someone can implant these boxes into cars and steal information from users within the car. Public transportation in the future can also be targeted for hacking users via wifi, because almost all public transport is starting to incorporate wifi. There is a new developing technology, where a user can display the content of their Smartphone unto their windshield via Bluetooth, this is potentially vulnerable. There is developing malware for Bluetooth and this can potentially threaten car security because the Bluetooth connection can easily connect to the car computer and corrupt it. This future windshield display can potentially threaten vehicles. Amazon is trying to implement their Amazon prime air program in which they will deliver their packages in the future via drones. This can potentially create a whole net of hacking exploits, because these drones can be hacked. Also fake drones can be developed containing sniffers to cruise around and steal wifi information from various neighborhoods. These drones can also potentially tap into car systems.

BMW is developing self driving technology, and this can completely compromise a vehicle, because that means a computer has access to all parts of the car. If this system is hacked, that means the hacker will have complete unlimited access to a vehicle and that can compromise vehicle security. Car companies also want to start implementing systems that relay information back like driving speed, how hard a person brakes, and how much they regularly drive. If this system gets hacked this can compromise security and lead to robberies, also potential hackers can change information and charge people in order to deceive insurance companies. 3D printing technology can create a whole new field of hacking by the printing of car parts with implemented hacking tools, and in the future this can become

very common.

Overriding the whole car system is a real thing now on new cars containing computers, but on the future arising technology can only add more possibilities of hacking and vulnerabilities, specially by implementing more connecting to these systems, like wifi, Bluetooth, etc. Military vehicle hacking is something that can disastrous but is also a real thing, new developing technologies can arise to use vehicle hacking warfare.

Works Cited

- "Could Your Car Get a Computer Virus?" *HowStuffWorks*. N.p., n.d. Web. 27 Feb. 2014. <http://auto.howstuffworks.com/car-computer-virus2.htm>
- "Car Hacking: The next Global Cybercrime?" *CNBC.com*. N.p., n.d. Web. 28 Feb. 2014. <http://www.cnbc.com/id/101123279>.
- "The Future of Car Hacking." *Lifehacker*. N.p., n.d. Web. 28 Feb. 2014. <http://lifehacker.com/the-future-of-car-hacking-1485302164>.
- Garcia, Alberto. "Dude, WTF in My Car." DEF CON 2013. DEF CON Hacking Conference. Rio Hotel & Casino, Las Vegas. 2 Aug. 2013. Lecture.
- Mandap, Phoebe. "The Evolution of Hacking: From Computers to Cars." N.p., n.d. Web. <http://siliconangle.com/blog/2011/09/08/the-evolution-of-hacking-from-computers-to-cars-what%E2%80%99s-next/>.
- "Wireless Car Hacking Demonstrated in New Video - Carscoops." *Wireless Car Hacking Demonstrated in New Video - Carscoops*. N.p., n.d. Web. 28 Feb. 2014. <http://www.carscoops.com/2013/08/wireless-car-hacking-demonstrated-in.html>.