Item – ECU

Attack Surfaces:

The attack surfaces for attacking a vehicle's ECU component vary widely, as each vehicle has between 20 and 100 of (Miller & Valasek, 2014). These attacks particularly involve remote attacks on the ECU as the final target, and nothing to do with attacks on vehicle networks such as CAN.

- Passive Anti-Theft System (PATS)
- Tire Pressure Monitoring System (TPMS)
- Remote Keyless Entry/Start (RKE)
- Bluetooth
- Radio Data System
- Cellular/Wi-Fi/Apps
- Telematics

Possible Ways to Attack:

Several methods of attacking ECUs exist, but many of the attack surfaces are very small, wouldn't be very effective, or would be difficult to achieve. The CAN protocol is vulnerable to different types of attacks, often due to its bus-type topology so that is a common method for attacking an ECU in a vehicle. Other ECU attacks are described in further detail. Not all of the attack surfaces listed above are mentioned in this section since a couple of them are described in later sections.

The PATS may be vulnerable to a DoS attack. In most cars today, there's a chip in the key that talks to a sensor on the steering column, which is wired into the instrument cluster ECU. The key and ignition sensor exchange RF signals to authenticate in order for the vehicle to start (among other components being able to activate). If a DoS attack was performed on the PATS, then the car simply wouldn't start, even with the right key. The attack surface is very small and would likely be primarily exploited for vehicle theft, and not remote code execution (Miller & Valasek, 2014).

The TPMS can be attacked in a few different ways. One attack would be to trick the car into thinking there's a problem with the tires, or with the TPMS itself. Another attack method is to crash and brick the ECU associated with the TPMS, but according to Miller's and Valasek's research, the attack surface for remote code execution is pretty small. However, the TPMS isn't always connected to the vehicle's network – which would then eliminate the vulnerabilities – and is *only* able to light up the warning signal for the driver to see that there's a problem (Miller & Valasek, 2014).

Bluetooth is noted by Miller and Valasek as one of the "biggest and most viable attack surfaces on the modern automobile," because of Bluetooth's complexity and underlying data. Also, attackers can test their attacks very easily given the fact that pretty much every vehicle made in the recent history is Bluetooth capable. There are two attack methods mentioned by the authors: The first of which is the most dangerous and involves an unpaired phone and any attacker can exploit this. The other method is to exploit after a phone has been paired, which is less of a threat since user interaction is involved. The attack surface of Bluetooth in automotive vehicles is very large and has been known to have several vulnerabilities since its inception (Miller & Valasek, 2014).

Radio Data System vulnerabilities vary between vehicles, but most of them receive more than just audio signals (Miller & Valasek, 2014). They often receive GPS, AM/FM radio, satellite radio, etc. Although it may be simple to interrupt or send signals to the radio data system, they're not likely to have any real

effect on the system. Per the research analysis, while you could control the vehicle's audio control module (ACM), there isn't much damage you could do, if any (Miller & Valasek, 2014).

Successful Experiments:

A successful attack on the ECU of a 2013-model Japanese hybrid vehicle by exploiting a vulnerability in the controller area network (CAN) protocol, which has a bus topology. In summary, the vulnerability is that ECUs can't easily distinguish a regular CAN message from a spoofed CAN message (Iehira et al., 2018). The reason for this is because CAN messages don't include source addresses and only have a CAN ID as the destination address. Additionally, the CAN message is a broadcast on the bus, so the ECU that receives the message can't know the source, which opens the door for spoofing attacks (Iehira et al., 2018).

The researchers experimented with the car to exploit the CAN protocol's vulnerability to target the engine speed by displaying an arbitrary value on the tachometer when the vehicle was stopped (i.e., the regular message represented 0 RPM and the spoofed message represented 6000 RPM in this experiment). The most effective method from their lab trials was used in the live car experiment and included two components: the spoofing and essentially temporarily disabling the ECU responsible for sending regular messages (Iehira et al., 2018). They successfully achieved this by performing a bus-off attack in one frame which, in the CAN protocol, puts the ECU into a passive error state so that it cannot interfere with other ECUs on the bus, thus allowing for an uninterrupted stream of spoofed messages to reach the destination ECU (Iehira et al., 2018).

Success was measured by their ability to send spoofed messages, remain undetected, and keep the tachometer pointing at the spoofed value (6k RPM) rather than the regular value (0 RPM). Using one of the other methods they tested in their lab experiments, they were unable to prevent the regular messages from being transmitted, therefore resulting in the tachometer to fluctuate between the regular value and the spoofed value (Iehira et al., 2018).

Mitigations Against Attacks:

As noted by the authors of the successful experiment explained above, they plan to conduct studies in the future to prevent vehicles from those attacks. I looked at published work from each of the authors and couldn't find any additional published research. However, when doing research in preventing attacks on the CAN protocol (which was exploited to attack the ECUs in the vehicle) I found research by different authors that directly address this vulnerability. This counterattack relies on the fact that there is a low probability for consecutive errors in a short period of time, which they use to detect the bus-off attack (Takada et al., 2019) – this method is also sometimes referred to as anomaly detection. Upon detection of the bus-off attack, the researchers proposed counterattack is to perform a bus-off attack *on the attacker* exactly one frame prior to when the attacker's bus-off attack frame is set to transmit. Therefore, the attacker will be transitioned to the bus-off state prior to the targeted ECU, thus preventing the attack from executing at all (Takada et al., 2019).

Item – Cellular Connectivity in the Car

Attack Surfaces:

The attack surface for vehicles with cellular connectivity is very large. Attackers can target vulnerable applications, find open ports to send malicious traffic, web-based attacks, and many more, depending on the level of connectivity the car has, which varies widely among makes and models (Miller & Valasek, 2014). Furthermore, telematics systems in vehicles are another form of cellular connectivity and have their own vulnerabilities, increasing the total attack surface for the vehicle.

Possible Ways to Attack:

Newer vehicles increasingly include Telematics/Cellular/Wi-Fi capabilities which can include things like GM's OnStar, retrieval of traffic and weather data, and sometimes it can establish a Wi-Fi hotspot in the vehicle. Cellular connectivity creates an extremely broad range for attacks (Miller & Valasek, 2014). Researchers have been successful in remote exploits on telematics units which have the ability to remotely transfer data and voice (using the microphone) to a remote location without user interaction, which means attackers can send their own remote commands if their exploit is successful (Miller & Valasek, 2014).

Another issue that has become very common is to find vehicles with internet access and the ability to use applications that were previously only available on smart devices (tablets/phones) and computers. This new tech being implemented more commonly in vehicles today opens the door for attacks that weren't previously a concern for vehicles such as web browser exploits, malicious applications, internet service exploitation, and the list will continue to grow (Miller & Valasek, 2014). Perhaps the biggest issue with this is the fact that attackers already understand the exploitation methodologies since they're largely vulnerable to the same attacks as smart devices and computers are (Miller & Valasek, 2014).

Successful Experiments:

White hat hackers Chris Valasek and Charlie Miller were able to run Nmap against a 2014 Jeep Cherokee's Wi-Fi hotspot and found open ports. This particular Cherokee has the ability to open a web browser, effectively opening it up to web-based attacks (Miller & Valasek, 2014). The vast majority of car owners won't think to disable open ports and that alone gives attackers a way into the car's network to attack various components. Miller and Valasek wrote a zero-day exploit that allows them to remotely hack the entertainment system of the 2014 Jeep Cherokee (or virtually any Chrysler vehicle that has Uconnect) via the cellular connectivity and they performed the experiment on a vehicle being driven by WIRED contributor, Andy Greenberg. After successfully attacking the vehicle, they controlled the vehicle's steering, transmission, and its brakes (Greenberg, 2015). All of this was done with several miles of separation between the vehicle and the attackers, it required no parts being added to the vehicle, nothing in the vehicle needed to be changed to allow the exploit, or anything of that nature; they were built that way which means thousands of Chrysler vehicles could have been attacked this way. This particular vulnerability has since been patched, but Uconnect had a vulnerable service which allows a remote party to query it for information about the vehicle such as the VIN or GPS. However, it also allows them to send CAN messages after gaining access to the car remotely, which is how they control the vehicle's operation (Greenberg, 2015). They measured their success by successfully controlling the vehicle's air conditioning, music selection and volume, speedometer reading (didn't match actual

speed), steering controls, disabling the brakes, and disabling the acceleration of the vehicle. Andy Greenberg was unable to control the car at all as he was driving down a highway and had to come to a rolling stop, turn the vehicle off and back on again in order to continue driving. This was an experiment, and the hackers took things much easier than they could have and it was *still* a dangerous experiment. Imagine what would happen if a state-backed hacker group decided to perform a massive attack on thousands of vehicles with the intention of hurting the drivers. It would be catastrophic to say the least.

Mitigations Against Attacks:

The vulnerability that led to the absolutely terrifying success of the attack described in the previous section was patched by Chrysler prior to the vulnerability being publicly disclosed. However, this patch is not automatically installed and can only be installed by drivers via a USB drive with the patch on it; and therefore, they must first know that the vulnerability exists (Greenberg, 2015). Miller and Valasek noted that there could be many more vulnerabilities as vehicles increase their connectivity in the future and that research needs to be done in this area to ensure the safety and security of these vehicles that could most certainly result in loss of human life. So the most sure-fire method of mitigating against these types of attacks is to avoid vehicles that have wireless connectivity to the internet. While that may not be ideal (or even possible after a few more years), it is definitely the best way to avoid falling victim to attacks such as these. However, for the majority of people who either can't avoid the tech, don't really care whether it's there or not, or those who actually really enjoy the benefits of having it, the best mitigation strategy is to put more funding into researching vulnerabilities before implementing new tech in vehicles, enabling automatic software updates over the air to patch vulnerabilities that are discovered later on, and to impose drastic punishment on vehicle hackers in an effort to deter them. In fact, the state Senate of Michigan proposed two bills that would result in life sentences for those who are caught hacking into a car's electronics system (Khandelwal, 2016). Since the vulnerability described in the last section has been patched and the vulnerabilities of future vehicles remain unknown at this time, it's difficult to pinpoint specific mitigation strategies, so increased research is necessary as new tech is developed for these vehicles over time.

<u>Item – Key Fob</u>

Attack Surface:

The attack surface of keyless entry/start technology is relatively small with respect to remote code execution, which means attackers can't exploit vulnerabilities in keyless entry systems to take full control of the vehicle or anything of that nature (Miller & Valasek, 2014). Based on my research, short-range radio transmission that allows the key fob to communicate with an ECU within the car from up to 20 meters away is the only attack surface associated with key fobs.

Possible Ways to Attack:

Remote Keyless Entry/Start (RKE) is pretty much standard on modern vehicles. There have been several examples of RKE attacks in past years and have been relatively simple to perform. Attackers are able to exploit vulnerabilities in the RKE authentication method which can potentially allow them to record the RF signal when the car's owner used it to unlock/lock their vehicle and then the attackers could replay the signal to gain access to the vehicle (Ibrahim et al., 2019). Another possible attack – which isn't nearly as concerning – is a denial of service which would block the key fob from being able to lock/unlock/start

the vehicle (Miller & Valasek, 2014). Miller's and Valasek's analysis states that the attack surface for remote code execution is small with regard to RKE.

Successful Experiments:

An experiment conducted by researchers was successful in jamming, recording, and replaying a signal to gain entry to a vehicle (Ibrahim et al., 2019). First, the attacker installs a jammer device on the vehicle to jam the key fob's frequency. The next step is to jam and record the signal when the driver attempts to lock/unlock their car. Lastly, the attacker replays the previously recorded signal which allows them to hijack the vehicle. The only unknown element that the attacker needs to find out is the frequency of communication that the car brand uses, but that is relatively trivial and can be found by conducting tests (Ibrahim et al., 2019). Using cheap and readily available equipment, the researchers were able to successfully hijack the six vehicles they used in their experiment, each with varying levels of difficulty with respect to distance between the logger and the key fob and between the key fob and the jammer (Ibrahim et al., 2019). They measured their success by their ability to successfully hijack the vehicle, and their method improved upon another method from their research by jamming all attempts by the driver to unlock the doors with the key fob, forcing them to use the mechanical key to unlock the doors and start the vehicle (Ibrahim et al., 2019). This aspect is important since previous strategies fail once the user attempts to use the key fob later when the jammer isn't present which resets the codes, rendering their recording useless.

Mitigations Against Attacks:

Mitigating this attack is very difficult (Ibrahim et al., 2019). Some researchers suggest using a jammer detector, but that would likely be extraordinarily rare for someone to have, realistically speaking. Alternatively, if the driver suspects that this attack is occurring, they could check spots under the vehicle for the jammer (researchers found the back of the vehicle produced the best results) and remove it. Some of their attack trials required very short distances (5-10 meters between the jammer and key fob and 1-3 meters between the key fob and the logger) to have consistent success, so locating the attackers would be relatively easy as well. This attack also relies on the fact that communication frequencies are consistent in certain continents which makes it much easier for attackers to be successful on a very wide range of vehicles (Ibrahim et al., 2019). Perhaps it would be best for automakers to use a wider range of frequencies in their key fobs, and possibly even alternate the frequency so that the jammer would only affect one frequency at most, allowing their key fob to successfully communicate with the vehicle and allow them to drive away.

References

Greenberg, A. (2015, July 21). *Hackers Remotely Kill a Jeep on the Highway—With Me in It | WIRED* [Tech Blog]. WIRED. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Hashem Eiza, M., & Ni, Q. (2017). Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. *IEEE Vehicular Technology Magazine*, *12*(2), 45–51. https://doi.org/10.1109/MVT.2017.2669348

Ibrahim, O. A., Hussain, A. M., Oligeri, G., & Di Pietro, R. (2019). Key is in the Air: Hacking Remote Keyless Entry Systems. In B. Hamid, B. Gallina, A. Shabtai, Y. Elovici, & J. Garcia-Alfaro (Eds.), *Security and Safety Interplay of Intelligent Software Systems* (pp. 125–132). Springer International Publishing. https://doi.org/10.1007/978-3-030-16874-2_9

Iehira, K., Inoue, H., & Ishida, K. (2018). Spoofing attack using bus-off attacks against a specific ECU of the CAN bus. *2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)*, 1–4. https://doi.org/10.1109/CCNC.2018.8319180

Khandelwal, S. (2016, May 2). *Car Hackers Could Face Life In Prison. That's Insane!* The Hacker News. https://thehackernews.com/2016/05/car-hacker-prison.html

Miller and Valasek—A Survey of Remote Automotive Attack Surfaces.pdf. (n.d.). Retrieved October 12, 2020, from http://ftpcontent.worldnow.com/wbbh/documents/Remoteattacksurfaces.pdf

Miller, C., & Valasek, C. (2014). *A Survey of Remote Automotive Attack Surfaces*. 94.

Takada, M., Osada, Y., & Morii, M. (2019). Counter Attack Against the Bus-Off Attack on CAN. *2019 14th Asia Joint Conference on Information Security (AsiaJCIS)*, 96–102. https://doi.org/10.1109/AsiaJCIS.2019.00004