Mercyhurst University

Automotive System Security:

A Comprehensive Breakdown of Automotive Security Testing

Connor Patchen and Jadyn Moore

CIS 499 Senior Project

April 29th, 2024

The automobile is a cornerstone of modern technology. The necessity to create a way to ease travel was a prominent issue in the late 1800s, and a man named Karl Benz would take on this challenge head first. Although there were previous entries, this was the first true example of what we define as an automobile. This is due to the fact that it was the first one to have an internal combustion engine, as opposed to the typical steam engine cars we were used to. In July 1886, the first report of one of these machines being driven hit the newspapers. This was great news, as we finally had something that was far more reliable and capable than a horse. The possibilities were endless, and soon many of the wealthiest were seen driving cars. This creation would go on to revolutionize what we know as travel entirely. Although revolutionary, there was not much going on technologically in this early example of a car. When compared to some of the automotive marvels we have today, the technology is night and day, but this was a pivotal starting point for the future of the automobile.

The first instance of security related innovations within cars dates all the way back to the 1900s. The removable steering wheel was invented to discourage potential thieves. The owner of the vehicle would detach the steering wheel from their car before doing daily tasks. This was a solid deterrent because without any other security features, thief's would simply be able to hop in the car and drive off. While this was a step in the right direction for vehicle security, there was quite the downside. The glaring issue with this invention was that it was impractical for both sides, as the owner would have to bring this inconvenient wheel anywhere they went. Luckily for the next adaptation of security, we find a much more long term solution. Heading into the 1920s,

locks on doors would be the next innovation in the automotive industry. Since these locks were early models, they were quite easy to pick, but an innovation that would be a staple in every car of the future. These locks of the future would become much harder to breach, as innovations such as central locking systems alongside transponder keys, which would greatly further the security of our cars. For instance, the central locking system was made, so the owner did not have to go around and lock every door of their car individually. The transponder keys opened the floodgates for users to remotely access different aspects of their cars such as popping the trunk or unlocking/locking their doors. These two seemingly simple technologies would become necessary inventions for every car of the future.

While there have been plenty of physical security innovations in cars, the first electronic related innovation within cars dates back to the 1940s, when electronic ignitions were being developed. Electronic ignitions played a pivotal role in the efficiency of cars. This is due to its reliability, as key components of the car such as engine performance and fuel efficiency were drastically increased due to this introduction. A few of the more pivotal ones include the introduction of anti-brake systems, and onboard diagnostics. The anti-brake systems were certainly pivotal for increasing the safety of our cars, whereas on-board diagnostics (OBD) greatly increased the users' ability to understand what fixes their car may need. The process of going from such minimal electronic usage in cars to touchscreens and fully customizable features seems to really get rolling in the late 60s. In 1968, Volkswagen released the first car with an engine computer. Their type III model used the Bosch D-Jetronic electronic fuel injection (EFI) system, which had three systems; the air intake system, fuel system, and

electronic control system. Shortly after this addition, we would begin to see more entertainment related additions to vehicles. The early 1970s started off great with the addition of cassette tape stereos. While this was a technology introduced in 1968, they garnered most of their popularity between the 70s and 80s. Introduced by Philips, this is one of those groundbreaking inventions for when we think of cars, as many people love to crank up the volume in their cars to make the drive feel less tasking. There are so many great car scenes in shows and movies that have some of our favorite characters depicted singing their favorite songs in the car with such passion. This element adds the very personal connection between car and owner, assisting in what makes the automobile such a pleasure to drive.

These features of course were very important for creating the basis of what we know cars as, but the innovations following these creations help bring everything all together. For instance, the airbag was introduced all the way back in the early 1970s, yet we didn't see any monitors for empty seats/seats that had children in them until 1997. This is the year that Mercedes introduced their occupant sensor, and the next year they would introduce whiplash protection. Another innovation of this time came in 1992, where we would finally see a different headlight be used. They were known as the High Intensity Discharge Lamps, which were noted to be much brighter than its predecessors. Other innovations such as OBD II would tell users exactly what was causing their engine issues. This was a technology introduced in 1996, just a few years before we entered the era of more computer oriented introductions of the late 2000s.

While these incredible inventions and innovations have been vital in assisting our driving experience, the more things added to cars meant the higher potential that some

of these adjustments may open the door to vulnerabilities. For instance, in 2015 a duo of hackers breached a Jeep Cherokee. Charlie Miller, a Cybersecurity engineer at X (formerly known as Twitter) and Chris Valasek, Director of Vehicle Safety Research at Ioactive collaborated on this project to see if they could remotely control a Jeep Cherokee. The two developed a software to remotely access the vehicle and adjust everything in the car, from something simple such as the radio to shutting the transmission off entirely. Given that this was a simulated exercise, the potential for this to do any real harm was slim, but that's not always going to be the case in such a situation. A malicious actor could easily turn this into something out of a horror film, adapting such a code to attack more than one car at once, potentially leading to injury, or even death. Knowing that this was a study done by two men on their own leads us to believe that a team of talented hackers could use this to inflict serious harm.

Another study done by a collection of researchers found many top end automobiles such as Land Rover, Mercedes-Benz, Porsche, Rolls-Royce among other top car manufacturers. The team was able to access these cars and start/stop the vehicles, flash headlights, among other intrusive actions. Very impressively, this was done by collecting just the VIN number on the automobiles. On vehicles such as Genesis and Hyundai, they were able to do these same commands simply using the owner's email address. The researchers also found that there was a way to breach the car using the Sirius XM remote functionality feature as a workaround into controlling these cars. Although it was patched within 24 hours, it is worth noting the potential that this had to be found in the wrong hands and used for wrongdoing.

In another realm of cyber that was breached in this hack is the Personally Identifiable Information (PIA) leaked from customers accounts. For Acura, Honda, Kia, Infiniti, and Nissan, researchers were able to view customer names, addresses, phone numbers, and email addresses by using the VIN number. The problem with these bits of information leaking onto the internet leave customers susceptible to potential attacks at any given moment. With 1.2 million customers being impacted, there would undoubtedly be an immense kickback towards the company. While this study had quite a wide scope of affected customers, a different article from Data Leak Lawyers tells us the story of a whopping 10 million U.S. vehicle owners' personal data being exposed. This study comes from security researchers at Kromtech Security who stated the leaked PII included customer names, addresses, home and work numbers, dates of birth and gender. Kromtech researcher Bob Diachenko stated, "Criminals are now using leaked or hacked data to obtain unique identifiers for a vehicle and then 'cloning' a VIN to make a stolen car appear to be perfectly legal." From this statement, we understand there is reason to have a fair level of worry about customers losing their entire vehicle to a bad actor, capable of obtaining sensitive information through relatively simple means.

Following the viewing of an interview conducted by David Bombal, we were able to garner a true understanding of a hands-on experience of a brilliant mind. The man he interviewed, Sam Curry, was able to give us insight into his world of hacking. His research began at 2am on a college campus when Sam and his friends thought of hacking scooters they found. Through a vulnerable HP request, the boys were able to query every scooter at once. As they fired up hundreds of scooters at once, the beeping and lights of scooters went ballistic. They looped this request and throughout the night

the scooters remained beeping. They thought about how they could remotely honk their car from their mobile device, and the research on how to breach cars was underway. Car companies such as Kia, Honda, Infinity, Nissan, Acura, showed plenty of vulnerabilities simply using a car's VIN or email address. Flashing lights, unlocking the car, and stealing the car were all listed as vulnerabilities prompted by this hack. With Mercedes-Benz, they created an account and could view internal dealer portals. Rolls-Royce allowed full configuration of employee accounts when breached. Although 2FA was implemented, there was a loophole that allowed the boys to breach through this security measure. To prevent more widespread breaches such as this, the Canadian Government is going to ban the device called the Flipper Zero, which allows you to emulate an API and use it whenever you want. People are using this to unlock cars and start their engines without even having to physically breach anything.

Eventually, the boys were ashamed that they hadn’t targeted any semi-trucks. Through a GPS tracking service named Spireon, they were able to affect an estimated 15.5 million semi trucks using administrative privileges. Hacking the truck starters, they were able to start the engine, unlock the vehicle remotely, and read any device location. One of the negative aspects noted from this breach would be food trucks being halted. Such an issue could cause a multi-billion dollar impact in just a day.

The centralization of remote management for cars means that once there is one car company breached, many others would follow. Tesla is noted as the most difficult software to breach, as they had a stronger implementation of system security. The one breach Sam did find was regarding Tesla sim cards. There is a product titled “Jasper” that allowed this breach, and allowed the group to kill the internet in any Tesla by simply

using the VIN number. Kia, on the other hand, was noted as one of the easiest to breach. Kia has fallen victim because anybody can emulate a key pair from anywhere in the world just using the VIN number. This breach would allow someone to watch the car's cameras, and the victim would have not been alerted of the breach whatsoever.

David proposes a great question when regarding the smaller group that Sam works with. If these boys were able to create such potential havoc, how much damage a nation-state could cause. This is a problem we have discussed earlier, yet something we have yet to see implemented on a grand scale. We do at least see the impact of improper security implementations, as Land Rovers in the United Kingdom are not able to get insurance. This has forced owners having to get their own independent insurance because insurance providers will not insure them because they are the most stolen vehicle. Such an ongoing issue will surely prompt an upscale in cybersecurity implementation within modern cars, an issue that will ramp up in the future.

As the interview goes on, Sam introduces us to a potential danger of this remote access, relating to the remote start. With how simple it is to gain someone's VIN or email, there is a targeted attack that has true potential. The access to remote car starting raises a potential hazard because if a car is in the garage, and it was started, it could fill the air with CO2. Say a family is asleep and someone with negative intentions breaches this vehicle. The lack of security provisions would directly tie back to the manufacturer of the car, leaving them with the weight of a homicide.

Another example of a modern day breach of automobiles occurred just this year in Tokyo at the first ever Pwn2Own hacking event. This event took place at the annual Automotive World Conference. There was one million dollars on the line to any team

that was able to gain access to Tesla's network. As mentioned before, Tesla is often considered to have the most secure network out of any car, and they frequently boast about such an achievement. However, like Sam, a team called team Synacktiv was able to gain access not once, but twice. They were awarded $450,000 for their efforts. Throughout the entire event, $1,323,750 was awarded to multiple teams of elite hackers due to their abilities of using an astounding 49 different zero-day hacks to gain access to multiple forms of automotive devices. Some of the devices successfully hacked were the JuiceBox 40 Smart EV charging station, ChargePoint Home Flex, Ubiquiti Connect EV Station, Automotive Grade Linux, and Sony XAV-AX5500 infotainment system. This poses a rather scary outcome for the general public however, because if these elite hackers were able to gain access to all of these devices in a relatively short time span with zero-day attacks for money, who is to say they would not do the same thing to cause harm if they were offered the right amount of money.

Technology is improving everyday in every aspect of our lives, this includes inside our vehicles. In today's automotive world, we are seeing more cars with technology that we typically would just see on our cell phones. Features such as Bluetooth, Wi-Fi, and LTE are just some of the examples. While this can make our drives easier and entertain our passengers. It raises the risk of attacks and increases the importance of protecting our vehicles from external actors. The greatest category of vehicles that are susceptible to this are cars that carry self-driving abilities. While autonomous cars may cause less accidents than human error and increase our convenience. A cyber attack that takes the control of a mass of self-driving cars could be extremely deadly.

There is a standard to address this issue however, it is called ISO/SAE 21434. It is from 2021. Created by the International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE), the purpose of this standard was to accomplish a few baseline topics as they relate to cybersecurity in electrical components of automotive vehicles. Those topics include “defining cybersecurity policies and processes”, “manage cybersecurity risk”, and “foster a cybersecurity culture”. This standard was created to ensure that automotive vehicles will be resilient to cyber threats just like any other computer or network would be.

The National Highway Traffic Safety Administration (NHTSA) has also taken a significant interest in vehicle cybersecurity. They have acknowledged the drastic increase in the amount of autonomous driving vehicles on the road and have decided to raise awareness about it by educating the public on what cybersecurity in the automotive industry means. Although it is not just self driving that must be protected. As mentioned earlier many cars are now equipped with bluetooth, wifi, and LTE features. However, features such as collision warning systems, automatic braking, and auto parking also rely heavily on key sensors that need protection. The NHTSA lays out their plans in hopes to collaborate with the automotive industry in a multi layered approach. These steps include “A risk-based prioritized identification and protection process for safety-critical vehicle control systems”, “Timely detection and rapid response to potential vehicle cybersecurity incidents on America’s roads; Architectures, methods, and measures that design-in cyber resiliency and facilitate rapid recovery from incidents when they occur”, and “Methods for effective intelligence and information sharing across the industry to facilitate quick adoption of industry-wide lessons learned. NHTSA

encouraged the formation of Auto-ISAC, an industry environment emphasizing cybersecurity awareness and collaboration across the automotive industry.” (NHTSA). The risk based approach can be compared to what we see in modern risk assessments for businesses. Where you take all of your assets and assign them a score based on their importance to the system and the likelihood that it could be compromised. Then either using a quantitative approach wherein a numerical value would then be assigned to determine the overall risk that asset face, or a qualitative approach where the chance of risk would be assigned based on a low-moderate-high scale. Conducting a risk based approach for vehicles could be slightly different however. It can be argued that each and every asset in a motor vehicle is key to the safety of a human life. Compared to a regular risk based assessment for example, if some sensitive data such as a credit card number were to be leaked, that is something that carried a high value on the asset register, but it theoretically is not going to endanger the life of a person as they can simply get a new card. The second feature in their plan is to have a system in place to quickly detect and respond to possible cybersecurity incidents on the roads. Systems like this can already be seen in applications like Onstar and Life360, which have crash detection features and will send emergency response automatically. If this technology could be combined with something like an incident response plan, cyber anomalies on the road could be quickly detected and dealt appropriately with. The emergency response team will also likely have an exact location of the issue and can respond with either emergency personnel or a cyber response to fix the issue. Third, they talk about implementing a system of enhanced information sharing and effective intelligence that would allow the industry to quickly share any lessons learned from a theoretical attack.

The automotive industry is gigantic, but there are many different manufacturers that all develop their vehicles differently. Having a policy like this in place will allow those differences to be set aside in the name of safety. Something that happens to a Tesla could quickly be shared to Ford and General Motors in order to prevent them from falling victim to the same attack. The NHTSA also encouraged the foundation of Auto-ISAC, a policy to help emphasize cybersecurity in the automotive industry and encourage that collaboration mentioned above.

Auto-ISAC stands for Automotive Information Sharing and Analysis Center. Auto-ISAC was created by 14 OEMs back in 2015, however, it is not even close to being the only ISAC out there. ISACs began to be formed in 1998 as the result of a Presidential Directive. That directive stated that public and private organizations must come together to share information about threats, vulnerabilities, and events in order to protect the infrastructure of the United States. (Auto-ISAC Inc.). We can see that the timing of the creation of ISACs was around the time that the internet started to become very mainstream in the US. Lots of average people were beginning to have access to their own PCs and many businesses were making the switch to technology based infrastructures. Since the creation 26 short years ago, technology has rapidly evolved and continues to do so right before our eyes. This is why ISACs in general are necessary. According to the Auto-ISAC website, it is “An industry-driven community to share and analyze intelligence about emerging cybersecurity risks to the vehicle, and to collectively enhance vehicle cybersecurity capabilities across the global automotive industry, including light- and heavy-duty vehicle OEMs, suppliers and the commercial vehicle sector.” (Auto-ISAC Inc.). What this means is that Auto-ISAC is an organization

that many corporations such as GM, Ford, BMW, Honda, and others are a part of that all collaborate together to make advancements in vehicle cybersecurity. In other aspects of these companies, they would likely keep their discoveries/advancements secret in order to be the company that is responsible for the so-called next big thing in the automotive field. However, in this case it is important that these companies are able to push their differences aside and come together for the advancement of safety in all motor vehicles. Hopefully, more corporations make the choice to join Auto-ISAC. Recently Amazon was just admitted as one of the newest members which is great news as Amazon is one of the largest corporations in the world and their advancements in many different fields should bode very well for everyone involved.

Now the field of Automotive Cybersecurity is an ever advancing field that is going to have to constantly be innovating, in order to keep up with new zero-day attacks from criminals trying to gain access to automobiles. Along with the vulnerabilities mentioned earlier, such as bluetooth, wifi, and automatic driving, there are some other vulnerabilities that also need to be looked into that are drastic to make sure they are protected by a form of cyber security. Diving deeper into the topic of automatic driving, we need to look at the components involved with it. Mainly, these components are the electric steering and braking features. These features could be readily accessed by those wireless features that were aforementioned, such as bluetooth, or even by a device connected with a USB port. There is a new feature that is starting to be noticeably included in the new General Motor vehicles, hands free highway driving. While this is not a full autonomous feature that makes the car drive on normal roads, it still allows the driver to take their hands off the wheel while traveling at high speeds.

The vehicle will also make its own lane changes and automatically slow down or speed up depending on the flow of traffic. This is arguably more dangerous than a normal autonomous driving car due to the high speeds at which you are traveling, one small slip up could be likely extremely fatal. Even vehicles that are not as advanced as this and offer no form of hands free driving could still be potential targets as even the minor systems could be run electronically, such as the tire-pressure system, or other features that would typically pop up on your dashboard to let you know something is wrong with the car. Imagine falling victim to an attack without even knowing and your car doesn't properly tell you about the oil level in the car, or that an O2 sensor is no longer filtering the air being blown in the car. There are multiple methods that automobile companies are going to have to make sure they follow in order to lower the risk of an attack as much as possible. These practices are found all throughout the cyber industry in general, and cars are no exception. The first method that must be followed is making sure the vehicles can receive secure software updates. All the time, vehicles are downloading software updates over the cloud, and companies make sure those updates are delivered swiftly, and securely. The best way to accomplish this is public key infrastructure, or PKI. The corporations can use their own private key to put a digital signature on the update, so that way when it is sent to the receiver in the vehicle, the vehicles will use a publicly available key that will decrypt the signature and assure the downloader that the update did indeed come from the manufacturer. This is a common method used in the field of cyber security when used to transmit data, so it makes sense to use it in this case as well, especially when it deals with the safety of human life. Along with secure updates, the manufactures cannot just simply rely on PKI when it

comes to making sure the right software features reach their correct destinations. Manufacturers must also make sure that all the software on the vehicle already is supposed to be there. They can achieve this by using a secure boot method. Each time the car's system boots, it should run through a process that verifies the integrity and the authenticity of all the software that is booting. This way, if something malicious was installed on the vehicle without the owner’s permission or knowledge, the vehicle can alert the user and it can be dealt with in the proper manner. Companies next need to be constantly monitoring their vehicle networking as well. In newer cars that have infotainment systems integrated into them, there are several network connections that need to be made in order for them to properly function. These vehicles now connect out to the cloud using wireless connections. These connections include MACsec, IPsec, and TLS. Now, if we take a look at the future of autonomous driving, it goes without saying that there will need to be many policies in place and methods used by vehicle owners and manufacturers to ensure a safe future. Something we could see in the near future is someone sending a request to their vehicle from their cell phone, or other mobile device that would call the car to come pick them up at a designated location. In order to accomplish this, an encrypted message needs to be sent to the vehicle along with a digital signature that the car acknowledges. Possible problems with this feature is that if someones private key that they use to call the car was stolen, this would be quite the easy method for the wrong person to get their hands on another person's vehicle. A set of recommended guidelines that has been made in the world of automotive security was created by the United Nations. It is called UNECE R156 and it covers all of the guidelines for the secure boot and updates that were mentioned previously. Another set

of guidelines released by the UN was the predecessor UNECE R155. This set covers how cybersecurity management systems should govern over security in an automobile. It also talks about how risk analysis should be looked at when talking about security for vehicles. The current plan is for the European Union to officially adopt these guidelines at some point in mid-2024. Also as I mentioned earlier, these risks that vehicles are going to start facing are likely to not be just limited to one company only, which is why the Auto-ISAC is going to be extremely important in constantly creating new guidelines that will help keep our roads and our vehicles safe and secure in such an unpredictable world.

Throughout this paper, we looked into a variety of cybersecurity related innovations within the automotive field. Beginning with the history, we garnered a grasp of the most essential pieces of the automobile, along with how the innovations that time provided us with shaped the cars we have today. Following this, we began to grasp not only what automotive system security is, but how vital it is implemented in today's vehicles. A further examination leads us to finding real world examples of where this security has been tested. We examined some of the different regulations and guidelines that have been created and adopted around the world in order to limit these attacks on vehicles, as well as where we can go from here to make sure the risk always stays as low as possible. As we know, in the world of cyber security, it is physically impossible to eliminate all risk, but there are always going to be endless methods created and practiced to make sure it stays as low as possible. The most important thing to remember about automotive cyber security is that human lives are on the line at all times, and just a small incident could be fatal. We need to stay vigilant and treat this

topic very seriously if we are to live in a world where our cars and trucks drive themselves.

References

History portion:

Cavanaugh, J. (2021, June 29). *The history of Car Locks*. Action Lock Doc. https://www.actionlockdoc.com/blog/the-history-of-car-locks/

Curry, S. (2023, January 3). *Web hackers vs. the auto industry: Critical vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and more*. Sam Curry | Web Application Security Researcher. https://samcurry.net/web-hackers-vs-the-auto-industry/

Electronic ignition system-construction, diagram, working, uses. Testbook. (n.d.). https://testbook.com/mechanical-engineering/electronic-ignition-system#:~:text=Electronic%20ignition%20enhances%20engine%20performance,used%20in%20conventional%20ignition%20systems

G, M. (2019, July 16). *A brief history of car security systems*. Black Knight Global Tracking Systems. https://www.blackknighttracking.com/post/2019/07/10/a-brief-history-of-car-security-systems

Gold, A. (2017, November 11). *When did cars get computerized?*. Autotrader. https://www.autotrader.com/car-news/when-did-cars-get-computerized-264028#:~:text=Electronics%20to%20the%20Rescue&text=Electronic%20ignitions%20were%20initially%20developed,which%20also%20had%20it%2C%20was

Group, M.-B. (n.d.). *Benz Patent Motor Car: The first automobile (1885–1886): Mercedes-Benz Group*. Mercedes-Benz Group. https://group.mercedes-

benz.com/company/tradition/company-history/1885-1886.html#:~:text=On%20January%2029%2C%201886%2C%20Carl,1

Markus, F. (2023, June 15). *The top automotive tech breakthroughs of the 1990s*. MotorTrend. https://www.motortrend.com/features/top-automotive-technical-breakthroughs-of-the-1990s/

Stewart, B. (2016, September 21). *The 15 most important automotive tech milestones of the last 25 years*. Popular Mechanics. https://www.popularmechanics.com/cars/g2778/most-important-automotive-tech-milestones/

The history of Car Technology (with Infographic): Driving seat. Jardine News. (n.d.). b https://news.jardinemotors.co.uk/lifestyle/the-history-of-car-technology

Examples of breaches

10 million US vehicle owners' personal details leaked from unprotected database. Data Leaks, Breaches & Hacks. (2017, July 11). https://www.dataleaklawyers.co.uk/blog/10-million-us-vehicle-owners-personal-details-leaked-unprotected-database#:~:text=Approximately%2010%20million%20U.S.%20vehicle,%27critical%20and%20sensitive%20information%27

Arghire, I. (2023, January 5). *16 car makers and their vehicles hacked via telematics, apis, infrastructure*. SecurityWeek. https://www.securityweek.com/16-car-makers-and-their-vehicles-hacked-telematics-apis-

infrastructure/#:~:text=The%20hacks%20targeted%20telematic%20systems,over%20the%20course%20of%202022

Kovacs, E. (2022, December 1). *Several car brands exposed to hacking by Flaw in Sirius XM Connected Vehicle Service*. SecurityWeek. https://www.securityweek.com/several-car-brands-exposed-hacking-flaw-sirius-xm-connected-vehicle-service/

Miller, C., & Valasek, C. (2015, July 21). *Hackers remotely kill a Jeep on a Highway | Wired*. YouTube. https://www.youtube.com/watch?v=MK0SrxBC1xs&t=305s

Winder, D. (2024, January 27). *Tesla hacked as electric cars targeted in $1 million hacking spree*. Forbes. https://www.forbes.com/sites/daveywinder/2024/01/27/tesla-hacked-as-electric-cars-targeted-in-1-million-hacking-spree/?sh=1f4b729d22e8

Modern Usage/ ISO 21434/ Auto ISAC/ Future

Automotive isac. Automotive ISAC. (n.d.). https://automotiveisac.com/

Road vehicles — Cybersecurity engineering. ISO. (2021, August). https://www.iso.org/obp/ui/en/#iso:std:iso-sae:21434:ed-1:v1:en

Taller, H. (2023, August 9). *The importance of cybersecurity in the automotive industry*. PTC. https://www.ptc.com/en/blogs/alm/the-importance-of-cybersecurity-in-the-automotive-industry

Vehicle cybersecurity. NHTSA. (n.d.). https://www.nhtsa.gov/research/vehicle-cybersecurity

Witten, B. (2023). *Positioning Automotive Cybersecurity for the future*. Aptiv. https://www.aptiv.com/docs/default-source/white-papers/2023_aptiv_whitepaper_cybersecurityevolution.pdf?sfvrsn=ba563737_3

Bombal, David. “Hackers Remotely Hack Millions of Cars!” *YouTube*, YouTube, 17 Mar. 2024, www.youtube.com/watch?v=MBj546UptEA.