Anna Weiksner

30 April 2023

The Dilemma of Connected Cars: Addressing the Inherent Risks of Connected Devices

Picture this: It's a clear sunny day and you need to go get groceries. You grab your phone, and your phone connects to your car through bluetooth and automatically unlocks. You drive to your local ACME and park your car. When you walk away towards the store, your phone disconnects from Bluetooth and the car locks itself like it always does. After 20 minutes, you walk out with a full cart of groceries. Your car isn't where you left it. You figure you must have forgotten where you parked it, but after 20 minutes of walking around the parking lot, you can't find it. Since you usually leave your airpods in the car you check the location of your airpods. Your car is on the highway. Without you in it. Even though you locked it and were only gone for 20 minutes. When you call the police, they check the security cameras and see someone open your car door and drive away. This is perplexing because you know that your car locks as soon as you get out, and even if they could get in physically, it won't drive without your phone in it. Through the security feed you see that when you pulled in, there was a teenager seated on a park bench near the edge of the parking lot with a computer. As soon as you entered the store, he ran a program that unlocked your car. He got into it and drove away and is now on his way to sell it. In the past, the risk of remote break-in has been so low that no one has been forced to fix this. However, the increase in connected cars and improvements in technology is leading to increased vulnerabilities. There should be more regulations and incentives in place so that car companies are motivated to protect their products against cyber attacks.

As the numbers and capabilities of connected cars increase, vulnerabilities will increase exponentially. According to an article by Marina Constantinoiu for Israel21c, from 2018 to 2021, cyberattacks increased 225% and 85% of attacks were carried out remotely. A 2018 article by

Upstream reported that there were 330 million connected cars at the time. They projected it to jump to 775 million by 2023(Kim). According to Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense by Kyounggon Kim, ¼ billion vehicles have some sort of internet capabilities, accounting for ¼ of all vehicles(Kim). Cars with internet capabilities are classified as IoT Devices which is short for Internet of Things. They send and receive data from users and other devices and they are designed to have limited computational power.

However, cars are a lot more complex than most IoT devices because they are much more mechanically complex. The book *Lifecycle Security for Software Engineers* by Kaustubh Dhondge divides software components into two categories: control systems and driving systems. The control system consists of Electronic Control Units(ECUS) which control the physical systems including the engine and sensors, door, seat, power lock, airbag, air condition system, and light control, anti-lock brake system, engine control unit, and transmission control unit. To connect the ECUs, the Controller Area Network(CAN) transfers data among them. The driving systems control software to improve the user's driving experience including light detection, gps, reverse video camera, radio, and radar(Dhondge).

In order to attack a vehicle, hackers first find a vulnerability and attack it to gain access to the vehicle's system. For example, a Security Week article described how hackers took advantage of a bug in the SiriusXM, a satellite radio system, in 16 different common car brands including BMW, Honda, Ford, and Toyota. Once they are inside the vehicle, they find a path that gets them access to the feature they want and inject malicious code that prevents a normal vehicle function, executes an unauthorized action, or steals user information. In the case from the Security Week article, once the hackers got through the radio, they were able to get the Vehicle Identification

Number which allowed them to remotely start and stop the engine, lock and unlock the vehicle, flash the lights, honk, and retrieve the location of the car(Aghire).

Many common vulnerabilities are due to a desire to be lightweight. Part of this is by necessity: a few extra seconds in deploying an airbag can mean the difference between life or death for a passenger. However, it also means that there is less room for proper security. In his article, “Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective”, Cybersecurity expert Samrat Acharya describes the STRIDE Threat model which : Spoofing(entered the system disguised as a trustworthy source), tampering(changing a process), repudiation(malicious manipulation of actions), denial of service(preventing a process from happening), and elevation of privilege. Most of these are related to faulty authentication, or logging into an account without the proper credentials. Authentication is required between two parties communicating especially when they are accessing a protected service in order to ensure a secure environment. For example, if the software leaves ports open after information has been sent, it can lead to the introduction of viruses, spyware, and ransomware and allow hackers to manipulate sensitive data, intercept private communication, and execute a denial of service(dOS) or man in the middle(MITM) attacks. Acharya’s article also points out that because cars are large physical devices, attackers can also use the physical weaknesses of cars to elevate their level of privilege and help them access the cars data. For example, a criminal could steal a car and then hack into it and steal physical information much more easily or inject malware through an electric charger(Acharya). A scammer could sell fake parts with malware online that would make the car’s software more vulnerable. Secure authentication is one of the biggest risks in cybersecurity and should be prioritized over lightweight design.

Many people are unaware of the risks that their high-tech vehicles come with. Most people are aware of the risks of having their car broken into and take precautions such as locking it and parking it in safe places. Very few consider any similar precautions to keep their car safe from hackers even though many attacks are preventable by only using trustworthy sources and keeping physical devices protected. In 2017, reporter Geoffry Fowler paid someone to hack into his own vehicle in order to find out what information his car had stored about him and found GPS history, call and message history, music streaming log-in credentials and contact information.There was no information about this anywhere in his vehicle manual or on the manufacturers website which is common across most major car brands because there is no regulation about consumer consent or security of cars(Blanco). This isn't helped by the fact that most people are careless about their information. According to a USA Today article by Rebekah Sanders, when people rent cars on vacation, many people log into the car infotainment services but do not log out when their rental ends leaving their information available for future users to access(Sanders). Attacks resulting from leaving information are far too common given how much is known about the importance of privacy.

Many car companies are also not aware of the risk of cyberattack. As outlined in "Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense", most car companies and component manufacturers employ very few cybersecurity experts on their team meaning that they don't really have people qualified to identify problems. In fact, many car companies resort to asking ethical hackers to expose vulnerabilities for them. Even when vulnerabilities are discovered, they are often overlooked because they slow cars down and they are not shared with other companies who may have products with similar vulnerabilities because they are more concerned with outcompeting their competitors(Kim). This makes cybersecurity slower and more costly because each company has to individually develop security features. According to a person at a supplier company in the UK interviewed for the Cybersecurity for Autonomous Vehicles report, “Because they have to get the vehicles out to market quick, and they have to compete with all their competitors and stuff like that, it has built a situation where security is taking a side door. It has taken fifteen years for the UK vehicle industry to consider safety properly. There is more of a safety culture now than there was, but there is no security culture”(Kim). In addition, there is no additional profit from implementing cybersecurity features. Since the public is also unaware of the risks of a vulnerable car, they are unwilling to pay extra for protections the way they would for four wheel drive or a smaller blindspot. Even if people were interested in paying for these features, cybersecurity features are hard to quantify and advertise.

The most important thing for car companies to improve is secure authentication. One potential solution suggested by the article “IOT Security: Review, Blockchain Solutions, and Open Challenges” would be storing credentials on the blockchain which would be especially helpful for systems that involve exchanging data externally like bluetooth. While blockchain is most commonly used for cryptocurrency, it also has cryptography applications without requiring a lot of memory. The blockchain is a virtual ledger that tracks transactions between devices. It provides a log of transactions, access management, data trading and key management. Each block of data is time stamped and validated which gives the system more opportunities to check that the block comes from a trusted source. It provides a list of transactions and a hash(unique identifier) to the previous block of data which enables identity access and management. All data is encrypted using an elliptic curve SHA-256 hash which is a form of encryption that is one of the hardest to break(Khan). This also allows the system to receive information from many sources and make sure that they are trustworthy.

In addition, many common attacks can be prevented by simple things such as minimizing unnecessary features and keeping track of the size and frequency of information transmitted through the system. This would help detect attacks like distributed denial of service(DdoS) where an attacker overwhelms a system by sending repeated packages of information quickly. The article "IOT Security: Review, Blockchain Solutions, and Open Challenges" recommends a system that could also measure signal strength and compare it to the signal strength of trusted sources in order to determine whether the signal is coming from a trusted strength(Khan). While measuring signal strength and managing packet ratios wouldn't prevent all attacks, it would make many common attacks significantly more difficult.

One way to ensure that car companies are motivated to implement cutting edge security features would be a unified threat model. All companies would be required to conform to this model, incentivizing them to protect their customers. One example of such a method is the Threat Analysis and Risk Assessment(TARA) that the United Nations Economic Commission has proposed for Europe(Zelle). This provides concrete analysis that makes security measurable. It divides security for cars into five categories: Cryptographic Keys, Wireless on-car interfaces and communications, on-car ECUS, and On-car sensors. Each category has requirements that a car must meet in order to be considered secure. For example, wireless on-car interfaces and communications are measured based on the feasibility of intercepting gps, bluetooth, radio and wifi information. Each attack is given a rating based on how long the attack takes to execute, the amount of expertise required, the difficulty of the attack, equipment required, and probability of success(Zelle). For example, extracting cryptographic keys from the hardware security model is rated “very low” because it should take around 3 years with a very limited window of opportunity to start, require multiple experts who know confidential information about car security, and require specialized equipment. On the other hand, disabling the camera is rated “high” because it takes less than one week, requires a “layman's” amount of knowledge, most of which is public, and can be done with basic equipment(Zelle). TARA would allow companies to publish quantitative data about how safe their car is and consumers could use this data to be aware of the safety of the software of the car before they purchase. This would incentivize car manufacturers to implement cybersafety features.

National governments can also help protect consumers through regulations on cybersecurity. They can require car companies to share information about vulnerabilities with other car companies and publish information about attacks. National governments need to require this because most companies are more concerned with outperforming the competition than the general well-being of the public. They are unwilling to give other car companies information about vulnerabilities and solutions because that allows competitors to improve their products. This will also improve communications between car companies and part manufacturers who don’t always give car companies all of the information about problems with their products. Similarly, they will try to hide attacks that make them look bad. If governments require publicity about these attacks, people will see these attacks and become motivated to protect themselves by buying cars that publicize safety features and preventing important information from being stored on their car. Car companies will then be able to charge extra for cybersecurity features and increase profits, motivating them to further improve cybersafety. In addition to requiring the sharing of information, the government should also require that car companies solve known vulnerabilities immediately. This can work similarly to recalls on broken parts where manufacturers are required to notify owners within 60 days of discovering a vulnerability and owners are given financial compensation or a way to fix the issue free of charge. Governments need to protect the safety of their populations through mandating digital security for cars.

Finally, more effort needs to be placed on educating the public about their vehicles' cybersecurity risks. This can be done the same way people are educated about internet privacy. This could include giving more publicity to attacks in the news to educate people about the consequences and scare them into protecting themselves. My hometown, Greenwich, Connecticut, has a huge problem with stolen cars because many people accidentally leave their keys in their cars. Local car thieves have devices that can detect keys left in cars if the keys work wirelessly which they use to break into the car. As a result, the town police put signs up everywhere reminding people to bring their keys inside and mass emails are sent out every time a car gets stolen to remind people to be careful. Similarly, schools can educate children about the risks and simple solutions. In addition, car manufacturers should include what data is stored in cars in a disclaimer in their owner manuals. Once they know more, people will start being careful with cars similar to the way they are careful with their online passwords. Consumers who are educated about cybersecurity will also be more likely to purchase a car that advertises cybersafety and more likely to pay extra for more safe vehicles, motivating car manufacturers to build safer cars.

There is a huge amount of inherent risk associated with "convenience features" such as mobile apps that can unlock cars, bluetooth connections, and self-driving features. Most cars have a lot less computational power than most computers, meaning that there is a lot less room in the software for protection. Add that to the fact that a car is a very expensive, important piece of equipment that you do not want stolen, and you have a dilemma. As new technologies are created, cars are becoming more and more connected to the internet. One such feature is self-driving software. Imagine a congested highway where a number of the cars are self-driving. Now imagine the power a hacker could have if they were able to take control of these cars. Before we allow self-driving cars to enter the market, not only does the probability of such an attack need to be close to zero, but there also need to be regulations to prevent future technological advances from creating a way for such an attack and a process to develop further protections. Before car companies develop more technologies, they need to increase protections against hackers. No one would park a car in the city and go to lunch without locking it. The same should apply to the cybersecurity of a car.

Works Cited

Acharya, Samrat, et al. "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective." Ieee Access, vol. 8, 2020, https://doi.org/10.1109/ACCESS.2020.3041074.

Arghire, ByIonut. "16 Car Makers and Their Vehicles Hacked via Telematics, Apis, Infrastructure." *SecurityWeek*, 5 Jan. 2023, https://www.securityweek.com/16-car-makers-and-their-vehicles-hacked-telematics-apis-infrastructure/.

Blanco, Sebastian. "Washington Post Hacked into a Chevy Volt to Show How Much Cars Are Spying on Their Owners." *Car and Driver*, Car and Driver, 29 Nov. 2021, https://www.caranddriver.com/news/a30260730/chevy-volt-hacked-data-collection/.

Constantinoiu, Marina. "Cyberattacks on Cars Increased 225% in Last Three Years." *ISRAEL21c*, 24 Feb. 2022, https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/.

Dhondge, Kaustubh. "Vulnerabilities in IoT Security." *Lifecycle IOT Security for Engineers*, Artech House, Norwood, 2021.

"IOT Security: Review, Blockchain Solutions, and Open Challenges." *Future Generation Computer Systems*, North-Holland, 26 Nov. 2017, https://www.sciencedirect.com/science/article/pii/S0167739X17315765?via%3Dihub.

Kim, Kyounggon, et al. "Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense." Computers & Security, vol. 103, 2021, https://pure.coventry.ac.uk/ws/files/29922758/Binder6.pdf.

Morris, David, et al. “Cybersecurity Threats in the Auto Industry: Tensions in the Knowledge Environment.” Technological Forecasting & Social Change, vol. 157, 2020, https://doi.org/10.1016/j.techfore.2020.120102.

Sanders, Rebekah L. “Car Renters Beware: Bluetooth Use Can Reveal Your Private Data.” *USA Today*, Gannett Satellite Information Network, 30 Jan. 2018, https://www.usatoday.com/story/money/cars/2018/01/30/car-renters-beware-bluetooth-use-can-reveal-your-private-data/1080225001/.

Smith, Craig. *The Car Hacker's Handbook*. No Starch Press, 2016.

Zelle, Daniel, et al. “Threatsurf: A Method for Automated Threat Surface Assessment in Automotive Cybersecurity Engineering.” Microprocessors and Microsystems, vol. 90, 2022, https://doi.org/10.1016/j.micpro.2022.104461.