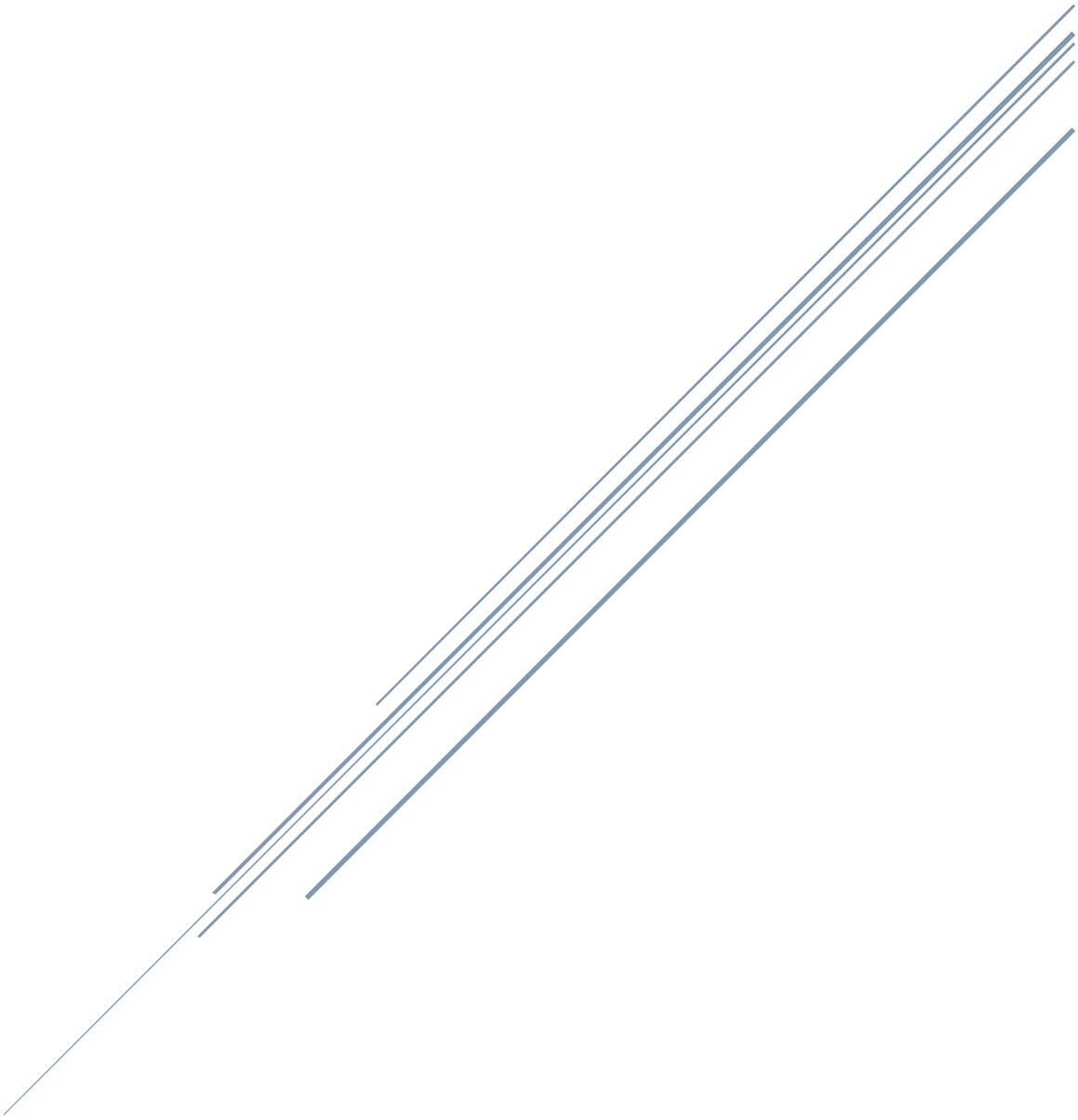
# AUTOMOTIVE CYBER SECURITY



Cole Baker

# Table of Contents

Introduction to Automotive Security ..... 2

References ..... 7

# Introduction to Automotive Security

We use vehicles to get everywhere nowadays, but do we ever stop to think about the security of our vehicles, and I'm not talking about making sure you locked your doors and put your windows up. I'm talking about the cyber security of your car. Cars today are essential a computer with wheels, all new model cars have a computer that controls everything from the cruise control to the door locks. So, what does this mean for us? The short answer, hackers can do the same things they might do to the computer sitting on your desk, to your car. This is a very scary thought, because yes, there could be personal information located on that computer on your desk, that could be used against you or make you broke. But doing these kinds of things to a vehicle, is a much scarier thought. You are just driving down the road and suddenly have no control over your car. And what's happening is some hacker is using your car as a real life video game. We spend a lot of money and time making sure our phones and computers are kept safe, sometimes we forget about the computer that takes us everywhere. As vehicles become more advanced and the more technology that is added into our cars, the more of a risk this becomes. All these new technologically advanced features being in cars make our lives easier, and in some cases safer. But are all these really necessary? While having a car that drives itself or a car that will stop if a kid runs out in front of you is cool and safe, when you're not thinking of how all this technology is works and is the technology itself safe. We hope the answer is yes, so we can drive to work everyday without worrying about the chance of our car being used as a remote control car.

How does all these new features being put into todays vehicles effect the future? If you ask most people, they'll say something like, "It will make getting around easier and the roads safer". But is that really true? Maybe it will make driving easier like cruise control did, but there are still all of the cyber security risks that come with these new features. I personally think that all these new features are interesting and cool, but I don't think they're necessary. They take away from the driving experience, add more distractions, as well as create vulnerabilities that never excited before. An attacker with the right knowledge and equipment, could do anything they wanted the on bored computers in your car. Expanding your attack surface. As vehicles become more advanced, we get closer to the world we see in futuristic movies where the cars drive themselves. But we also get closer to the movies where a hacker take control of a car and drivers it into another. I hope that one day we think about our cars just like we think about our computers. You never know, we might be able to buy antivirus for our cars someday. There are security systems in place within vehicles to prevent attackers from gaining access to the vehicles controls, but there are still ways around these systems, a backdoor or a vulnerability within the computer. For instance, newer cars use key fobs to get in and start the car. Those keys are always searching for the vehicle it is coding to, it is possible with the right equipment to intercept the signal that the key is giving off. The key is constantly sending out a signal, waiting to get a response back from the car. If someone is watching for that signal, it can be taken and used on their own key to gain access into a vehicle.

One of the scariest thoughts about this is thinking about all the possible systems that could be taken control of, or what could happen. At first some people might think that this doesn't happen a lot, but once you start looking ton this, you can see that this is more common then you first thought. The US department of transportation has released a few documents on cyber security best practices. These documents cover things like, "Vulnerability / Exploit / Incident Response Process" and "Self-Auditing". "Vulnerability / Exploit / Incident Response Process" is a process and a set of guidelines they have set in place for determining and testing any vulnerabilities in a vehicles computer system. The "Self-Auditing" part of the document, outlines a few steps and different things that we should do ourselves to keep up to date on cyber security for our vehicles. These include, software updates and security patches, as well as doing self risk assessments. There is also a law for any automotive manufactures that use a computer system to operate key features of the vehicle, such as the accelerator or an assistive parting system, that states if there is a vulnerability within the software or a computer component that is criterial for the operation of the vehicle, they much either release a security patch or recall the car, just like any other part of the vehicle. There was also a section within this document that I found particularly interesting, section 6.7.2 which covers the car key itself, it states that any key (physical or digital) or password which gives access to the vehicle or its computer systems, should not be able to be used with any other vehicle. (Cyber Security Best Practices for Modern Vehicles, 2016)

There have been a few noted occasions where a vehicles key fob has been hacked or has been documents as being able to be hacked. For instance, when Tesla released the Model S, its first fully electric sedan. Teslas are some of the most technologically advanced cars you can buy, its main feature being the autopilot system. But according to a paper released by the KU Leuven university, researcher was able to read the signals from nearby Tesla Model S key fobs and essentially cloned the fob, which gave them the ability to use the car just like if you had the real key. Since the release of the car, Tesla has patched this vulnerability but that isn't to say there isn't still a vulnerability that hasn't been found yet, just like any other computer. These university researchers didn't do this to be malicious, more of to show that it is possible for this to be done, even for a car as advanced as the Tesla. This just highlights the fact that these kinds of attacks are possible, all these researchers had to do was stand around the person with the key and they were able to perform this clone of the key. So, what's to stop this from happening to you? Hopefully the manufacture has well encrypted all the signals being given off by the key. (Greenburg, Hackers Can Steal a Tesla Model S in Seconds by Cloning its Key Fob, 2018)

Key fobs are the only part of the vehicle that can be targeted, any part of the vehicle controlled by a computer can be hacked. A lot of older cars are aren't affected by these kinds of attacks as much due to not having a lot of computers controlling the car, older cars have a lot more mechanical parts which made cyber security in vehicles kind of irrelevant until modern cars came about.

These modern cars are a lot more vulnerable to cyber attacks. Back in 2016 two researchers, hacked into a Jeep Cherokee using the navigation system which was connected to the assistive parking feature and was always looking for a Bluetooth connection, and completely suit off the transmission while it was in motion. After the results of their research was published, the FBI and DOT investigated further into the possibility of automotive cyber attacks, they warned that drivers should be aware of any potential cyber security vulnerabilities associated with their vehicle. After this event with the jeep, Chrysler released a recall and mailed out USBs with a security patch to fix this vulnerability and prevent this from happening again. This was just to show again that these kinds of things are possible. The same kind of thing happened to a Corvette, when a device that mechanics use to determine errors in a vehicles dashboard, such as the check engine light. Using this device, the researchers were able to access the computer systems that controlled the breaks and completely shut them off. (Greenburg, The FBI Warns That Car Hacking is a Real Risk, 2016)

We don't think about all the possible ways our cars can be affected by cyber security attacks, just like our computers. We need to start thinking of our cars as if they were a computer, being that's what they are now. And as cars have more technology added into them, we will need to understand the risks that come with having all these new fancy features in our cars. As much as these features can make driving safer, there are also all the cyber security risks that come with them.

# References

*Cyber Security Best Practices for Modern Vehicles*. (2016, October). Retrieved from National Institute of Standards and Technology Cybersecurity : file:///C:/Users/baker/Downloads/812333_CybersecurityForModernVehicles.pdf

Greenburg, A. (2016, March 3). *The FBI Warns That Car Hacking is a Real Risk*. Retrieved from Wired: https://www.wired.com/2016/03/fbi-warns-car-hacking-real-risk/

Greenburg, A. (2018, September 10). *Hackers Can Steal a Tesla Model S in Seconds by Cloning its Key Fob*. Retrieved from Wired: https://www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob/

*Vehicle Cyber Security*. (2018, August 15). Retrieved from NHTSA: https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

Weeks, C. (2018, July 19). *How to pervent your car from being hacked*. Retrieved from AVG: https://www.avg.com/en/signal/how-to-prevent-your-car-from-being-hacked-avg