International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey on Security Threats in Automotive Embedded System

Anjumol T Many

Asst. Professor, Dept. of Computer Applications, MES College Kottayam, Kerala, India

ABSTRACT

Today’s vehicles are more reliant on computers than ever before. So manufacturers must take steps to improve automotive cyber security moving forward. Automotive hacking is the vulnerabilities within the software, hardware and communication systems of automobiles. Modern automobiles contain hundreds of on-board computers processing everything from vehicle controls to the infotainment system. These computers called Electronic control units (ECU), communicate with each other through multiple networks and communication protocols including the Controller Area Network (CAN) for vehicle component communication such as connections between engine and brake control: Local Interconnect Network (LIN). In the advancement of industry, connection and demand of automobile is increasing rapidly, with that the threat and vulnerabilities in the automotive system is also elevating. In this theoretical study, we will discuss about the privacy and threats which can be implement on the vehicles. We will also see how the traditional security solution id different from the automotive cyber security solutions. And also see how we can secure our vehicles from the vulnerabilities as well as how to protect from hackers models, which will give findings for the vulnerabilities in the system.

INTRODUCTION

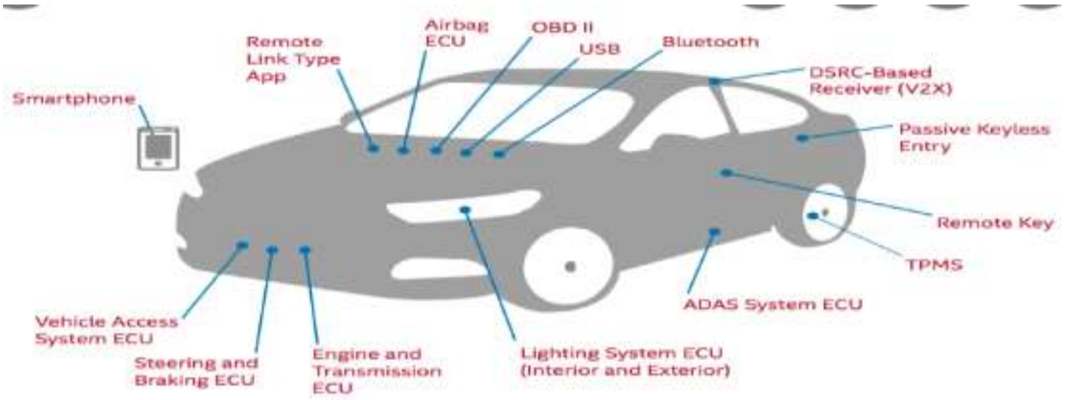
The world of Cyber Security revolves around the industry standard of confidentiality, integrity, and availability, or CIA. Privacy means data can be accessed only by authorized parties; integrity means information can be added, altered, or removed only by authorized users; and availability means systems, functions, and data must be available on-demand according to agreed-upon parameters. The main element of Cyber Security is the use of authentication mechanisms. For example, a user name identifies an account that a user wants to access, while a password is a mechanism that proves the user is who he claims to be. As data breaches, hacking, and cybercrime reach new heights, companies are increasingly relying on cyber security specialists to identify potential threats and protect valuable data. It makes sense, then, that the cyber security market is expected to grow from $152 billion in 2018 to $248 billion by 2023.

A hacker taking control of your car remotely and stealing it seems straight out of a movie script[1]. But, that is exactly what is happening in reality in the past few years. Hackers have adapted themselves to this new tech and have found ways to hack it, obviously. As technology is advancing every minute, modern cars are becoming increasingly advanced and automated. But are modernized cars really secure?

There have been certain cases where cybercriminals were prosecuted for using a laptop to hijack Jeep cars. It is very easy for hackers to take control of the vehicle, steer it, change gears, engage the brakes, and steal it. After experimenting with connected vehicles for years, security researchers have concluded that automated cars are vulnerable to several risks. Experiments have shown that cars can be compromised with different methods, through remote or physical access, or the vehicle’s supporting app[2] .Hacking the vehicle also gives the cybercriminals access to the owner’s trip data, which owners might want to keep private. It will be not be surprising to know that automotive cyber-attacks have grown rapidly, with the graph 225% in 2021, when we Compares to 2018. It is the trend for it , which has caused a new sensation in the automotive cyber security sector, as well as it has been predicted to increase up to 530 Crores in 2026. This is why it is being noticeable and hackers or cyber-criminals are paying more attention towards it, because ,in case, if any gap they find in the system they can easily access the vehicle or can hack the personal information related to that vehicle and use it for different motive. Whenever we connect our vehicles to be connected via internet ,there is a high chance of hackers taking advantage of it and make it the best use of that. This is majorly happening thing to taking up the system into control remotely and make it work according to themselves. Because of that it is really necessary to have good study and knowledge upon the hacking part as well along with the building of the system. Hackers are also trying their new technology for the better enhancement of hacking the system. There are different types of hacktivists, cyber-criminals and group of researchers, who are working on each and every gap to find the vulnerabilities in the system , which caused by connecting via internet or other elemental gadgets.

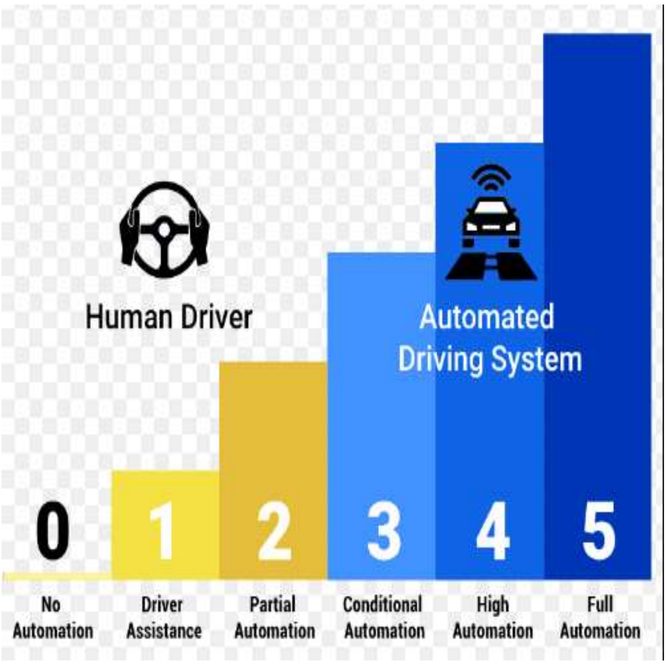
What can be done to prevent such attacks?

Manufacturers have been shielding their research and development, but because of this issue, players in the industry are sharing resources and collaborating on better cyber security practices. They have established the Auto Information Sharing and Analysis Center (Auto-ISAC) and outlined guidelines that will help manufacturers and suppliers be more prepared for cyber security issues. Automotive hacking happens because on the thousands of computers hackers are working on it and making it work to handle or control the system by their own way.



This fig1 shows that by which path of connectivity may lead to hack the system

There are certain level of automation which goes from level 1 to level 5, that is, level 1,2,3,4 and 5 which are Device level , Machine level ,Cell or System level ,Plant level ,and Enterprise level respectively.



This fig2 shows the level of which path works on which part of the system.

Level 0 (No Driving Automation)

Most vehicles on the road today are Level 0: manually controlled. The human provides the "dynamic driving task" although there may be systems in place to help the driver. An example would be the emergency braking system—since it technically doesn't "drive" the vehicle, it does not qualify as automation.

Level 1 (Driver Assistance)

This is the lowest level of automation. The vehicle features a single automated system for driver assistance, such as steering or accelerating (cruise control). Adaptive cruise control, where the vehicle can be kept at a safe distance behind the next car, qualifies as Level 1 because the human driver monitors the other aspects of driving such as steering and braking.

Level 2 (Partial Driving Automation)

This means advanced driver assistance systems or ADAS. The vehicle can control both steering and accelerating/decelerating. Here the automation falls short of self-driving because a human sits in the driver's seat and can take control of the car at any time. Tesla Autopilot and Cadillac (General Motors) Super Cruise systems both qualify as Level 2.

Level 3 (Conditional Driving Automation)

The jump from Level 2 to Level 3 is substantial from a technological perspective, but subtle if not negligible from a human perspective.

Level 3 vehicles have "environmental detection" capabilities and can make informed decisions for themselves, such as accelerating past a slow-moving vehicle. But—they still require human override. The driver must remain alert and ready to take control if the system is unable to execute the task.

Level 4 (High Driving Automation)

The key difference between Level 3 and Level 4 automation is that Level 4 vehicles can intervene if things go wrong or there is a system failure. In this sense, these cars do not require human interaction *in most circumstances*. However, a human still has the option to manually override.

Level 4 vehicles can operate in self-driving mode. But until legislation and infrastructure evolves, they can only do so within a limited area (usually an urban environment where top speeds reach an average of 30mph). This is known as geofencing. As such, most Level 4 vehicles in existence are geared toward ridesharing.

Level 5 (Full Driving Automation)

Level 5 vehicles do not require human attention—the "dynamic driving task" is eliminated. Level 5 cars won't even have steering wheels or acceleration/braking pedals. They will be free from geofencing, able to go anywhere and do anything that an experienced human driver can do. Fully autonomous cars are undergoing testing in several pockets of the world, but none are yet available to the general public.

RELATED WORK

In a follow-up research paper published in 2011, researchers demonstrated that physical access is not even necessary.

- The researchers showed that "remote exploitation is feasible via mechanics tools, CD players, Bluetooth, cellular radio and wireless communication channels allow long distance vehicle control, location tracking, in-cabin audio exfiltration and theft"[3].

EXISTING SYSTEM

- Fiat Chrysler UConnect- UConnect is Fiat Chrysler's Internet connected feature which enables owners the ability to control the vehicle's infotainment/navigation system, sync media, and make phone calls
- General Motors OnStar RemoteLink App- The OnStar RemoteLink app allows users the ability to utilize OnStar capabilities from their Android or iOS smartphones. The RemoteLink app can locate, lock and unlock, and even start your vehicle.
- Keyless Entry- The security researcher Samy Kamkar has demonstrated a device that intercepts signals from keyless-entry fobs and would allow an attacker to unlock doors and start a car's engine.

Attacker Model

The types of attackers that are likely to be present in an automated vehicle system.

1.**Internal Versus External**: The internal attacker is an authenticated member of the network that can communicate with other members. The external attacker is considered by the network members as an intruder and, hence, is limited in the diversity of attacks. Nevertheless, she/he can eavesdrop on the communication

2. **Malicious Versus Rational**: A malicious attacker seeks no personal benefits from the attacks, and aims to harm the members or the functionality of the network.

3. **Active Versus Passive**: An active attacker can generate packets or signals to perform the attack, whereas a passive attacker only eavesdrops on the communication channel (i.e., wireless or in-vehicle wired network).

4. **Local Versus Extended**: An attacker can be limited in scope, even if she/he controls several entities (vehicles or base stations), which make him/her local.

5**. Intentional Versus Unintentional**: An intentional attacker generates attacks on purpose, whereas an unintentional attack is a cyber incident that could be generated by faulty sensors or equipments.

Terrifying Ways Hackers Can Control Your Car!

1. Finding any car via GPS coordinates

2. Turning on your car Stereo system remotely
3. Hacking Car Air Conditioning System
4. Hacking Car Control System
5. Shut down you Car Engine
6. Hacking Car Brakes
7. Failing your Car Brakes
8. Threatening the Car Driver through Display Screen
9. Hacking Car Steering System

PROPOSED SYSTEM

- Keep in touch with your car’s manufacturer
- Update your car’s software
- Store your keyless remote in the fridge (or faraday bag)
- Turn off your car’s Bluetooth and Wi-Fi when not in use
- Hide your car’s Wi-Fi password
- Scan USB drives before plugging them into your car

How to Protect Your Car from Hackers

Hackers aren’t really interested in your car yet. But before long, they may be. As hackers realize they can hold car owners hostage, steal data, and perform malicious acts and theft with car hacking, they may become increasingly interested and skilled at hacking vehicles. While most of the protective measures for cars need to be made at the manufacturer level, there are some things everyday drivers can do to protect vehicles from hacking[5]:

1. **Don’t program your home address into GPS**: It may be convenient, but car thieves and hackers can use your GPS to find your home address. And if they have access to your garage door opener, they can get into more than your car: they can get into your home as well.
2. **Limit wireless or remote systems**: Systems that disable or monitor your vehicle remotely place you at the most risk. While many other systems are hard-wired into your vehicle’s computer, wireless or remote systems are often controlled online and are more vulnerable and attractive to hackers.
3. **Don’t leave your password in your vehicle**: Hacking can happen physically inside your vehicle as well. A car thief who finds your OnStar password, for example, can take over your account. That means the feature that allows you to remotely shut off your engine when you report the vehicle stolen will be useless.
4. **Use reputable shops**: Anyone with physical access to your vehicle and hacking know-how can cause problems for your vehicle. So when you’re leaving your car at a shop, whether for minutes, hours, or days, you’re taking a chance that someone can easily hack it — and even make it appear that you need repairs that really aren’t necessary. They may also be able to get access to information such as your driving data history. Only use shops and dealerships that you know you can trust not to take advantage of your car’s computer systems.
5. **Don’t download untrusted apps or use your car’s Web browser**: Your car’s infotainment system is unprotected and ripe for the picking. Untrusted apps in your infotainment system can introduce malware. You should never use the Web browser on your vehicle, either. Simply use your mobile phone instead while safely parked.
6. **Stay on top of vehicle recalls**: There has already been one cyber security-related vehicle recall for the Jeep Grand Cherokee UConnect entertainment system. The vulnerability left access open to the car’s acceleration, radio, brakes, windshield wipers, and more. Affected customers received a USB device to upgrade their vehicle’s software with new security features. All vehicle owners should keep an eye out for similar recalls.
7. **Buy a vehicle with Android Auto or Apple CarPlay**: Using your smart phone to manage your car’s entertainment system can be more responsible than a freestanding infotainment system. If you’re taking mobile security steps, this will make your system more secure.
8. **Buy an old car and wait for auto manufacturers to catch up**: This may not be a real option for many drivers, but Luddites can simply buy a vehicle that predates many of the connected features that make vehicles vulnerable today while manufacturers get up to speed and learn how to better protect vehicles and their drivers from hacking vulnerabilities.

CONCLUSION

The automotive industry needs to be upgrade more and more ,as these ways are not best of them which will protect the system from every way. It will have to work upon the way hackers think and make themselves one step ahead than what they are going to do. System needs to be cyber protected because in the coming years , we are going to see much more increment in the world getting involved in automotive industry or services more which lead to the more threats towards cyber-attacks. Researcher and Scientist have figured out so many demerits which should not be there, because it is creating miserable problem in protecting it from cyber-criminals or hacktivist. From my point of view , the digital documentation and authentication of the system should go through the check by traditional way, such that hacker can find one-way out, but could not find the whole way to crack the algorithm or the pattern.

References

1. Automotive hacking •https://en.wikipedia.org/wiki/Automotive_hacking
2. Car hacking threatens vision of connected mobility • https://www.ft.com/content/163f08c6-6ce3-11e9-9ff9-8c855179f1c4
3. Carhacked! (9 Terrifying Ways Hackers Can Control Your Car) •https://purplegriffon.com/blog/carhacked-9-terrifying-ways-hackers-cancontrol-your-car
4. Researchers are sounding the alarm on a little-known risk of connected cars •https://www.fastcompany.com/90383517/researchers-are-sounding-the-alarmon-a-little-known-risk-of-connected-cars
5. Car Hacks and How to Protect Yourself • https://www.kaspersky.com/resource-center/threats/car-hacks-and-how-toprotect-yourself
6. Hackers Remotely Kill a Jeep on the Highway—With Me in It •https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
7. How Hackers Exploit Automotive Software to Overtake Cars •https://www.securitymagazine.com/articles/91192-how-hackers-exploitautomotive-software-to-overtake-cars