International Journal of Research Publication and Reviews

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

How to Protect Your Smart Car from Hijackers and Car Thieves

[1]Yash Shelar, [2]Asst. Prof. Guari Ansurkar

[1,2]Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

ABSTRACT

This study provides information about smart cars and some the technologies and researches on smart cars. It then describes the modeling of security attacks in smart cars in terms of aggressive profile, attackable objects, attack requirements and security requirements. It also discusses the attack pattern and risk analysis related to vehicle speed ups and the stealing of personal information.

INTRODUCTION

Smart Cars integrates Internet Of Things (IOT) components to bring value-added services to drivers and travellers, These components communicate with each other and with the outside of the vehicle. Over the last few years, there have been many publications about the attacks on automotive systems. Some of these have been shown to be cheaper and easier to show, especially as they are a teenager who opens up and launches a car that remotely connects by using simple equipment.

How Hackers Can Attack Cars

Can a hacker stop your car or shut off your engine while you're driving 70 miles per hour on the freeway? Theoretically, yes. They can do that — and much more. These are just some of the ways hackers can access your vehicle's vulnerable systems and make driving difficult, dangerous, or uncomfortable for you:

1. **Tire pressure monitoring systems**: Tire pressure monitoring systems tell drivers when their vehicle's tires are too low or too high on pressure, offering helpful early warnings to get service. But when attacked, hackers can trigger warning lights and even remotely track vehicles through the monitoring system.
2. **Disabling brakes**: You may control your brake pedal, but microprocessors in your onboard computer really make your brakes work. Hackers who get into your onboard computer can disable your brakes and even stop the engine.
3. **Manipulating vehicle diagnostics**: Repair shops and dealerships today largely rely on onboard vehicle diagnostics systems to perform initial diagnosis of problems. But unscrupulous shops can manipulate your diagnostics system to make it appear that you need them to perform repairs that are not really needed.
4. **Changing the time, a song on the radio, or GPS destination**: With access to your vehicle's systems, it's simple for hackers to make small, but important changes to your vehicle. Something as unnerving as switching your radio station could happen. They can even get into your GPS system and change the destination you're heading to.
5. **MP3 malware**: The music you listen to on your car stereo could hack your vehicle — really. Downloads with malware codes can get into your car's infotainment system and make their way into other systems, including those that control your engine or brakes.
6. **Forced acceleration**: Power locks today often have features such as automatic locking when the car is put into drive or reaches a certain speed. They can also unlock if the airbags have been deployed. Cars with interconnected systems like this are vulnerable to problems such as hackers using power locks to force a car to accelerate.
7. **Extended key fob range**: Wireless key fobs today unlock car doors when the person holding them is close by. However, using radio repeaters, thieves can extend the range of the key fob, unlocking your car doors when you're up to 30 feet away.
8. **Driving data downloads**: Many vehicles, particularly those using GPS or telematics systems, record driving data. If hacked, this information could be used to exploit your privacy and even discover where you live, work, or take your kids to school.

9. **Smartphone access**: Hackers may be less interested in your vehicle's systems and more interested in your vehicle's connected mobile phone — which can give them access to credit card information, passwords, and financial data. If they're able to get into your vehicle's system and find your connected mobile phone, your information may be at risk.
10. **Turning on heat in the summer or air conditioning in the winter**: In extremely hot or cold climates, vehicle air conditioning systems are less about comfort and more about safety. But they are just as vulnerable to hacks as any other system. Hackers can blast hot air in the summer and even turn on seat warmers.
11. **Windshield wiper control**: Windshield cleaning fluid is useful, but not when it's released unexpectedly or continuously. Then, it can be a danger to your visibility. This system, along with your windshield wipers, can be hacked.

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 owner 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:

- **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.
- **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.
- **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.
- **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.
- **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.
- **Stay on top of vehicle recalls**: There has already been one cybersecurity-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.
- **Buy a vehicle with Android Auto or Apple CarPlay**: Using your smartphone 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.
- **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.

1. Car Control Hacks

A car running software, especially software that is connected to a mobile app or the Internet, is at risk of the same vulnerability exploits as any other computer. Protocol or code vulnerabilities are areas of potential weakness in connected car security.

One of the selling features of a smart car is its great infotainment system. The car's infotainment system is connected via protocols, like the MirrorLink protocol, to the driver's/passenger's smartphone to allow music to be played. MirrorLink uses the same type of mechanism that is often used in remote desktop sharing.

Another infotainment initiated attack was discovered by researchers looking at Volkswagen and Audi connected cars. The researchers used the car's Wi-Fi to exploit an exposed port and hijack the infotainment system.

2. Smart Alarm Hack

Pen Test Partners, who perform penetration testing on products to find vulnerabilities, identified an exploit that uses a car's smart alarm system.

They were able to identify critical security vulnerabilities in two of the largest smart alarm systems affecting 3 million vehicles. The vulnerabilities included both security issues, such as unlocking the car and privacy violations exposing the personal data of the car owner.

3. Insecure Associated Apps for Smart Cars

Mobile apps are a potential weak point in smart cars.

Kaspersky took seven connected car mobile apps and analyzed them for vulnerabilities. What they found was shocking. Amongst others, they identified little or no code obfuscation for door unlocking. They also found none of the apps encrypted username and password credentials. One of the main concerns of the exercise was that mobile Trojans could be used in the future to compromise smart cars.

And, it isn’t just cars at risk here. The Xiaomi Electric Scooter connects via Bluetooth to mobile app allowing various functions such as an anti-theft system to switch-on/off. Unfortunately, researchers have identified a flaw that allows a remote hacker (up to 100 meters) to send commands to the scooter via the app without the need for the password.

Preventing Your Smart Car Being Outsmarted

Smart cars are vulnerable to the same issues as other software. And, because components are connected, they offer an expanded attack surface for cybercriminals. As consumers of smart cars, we recommend several things to hack-proof our connected vehicle.

1. Patch and Update

Like any other computer, you should endeavor, wherever allowed, to patch firmware.

Also, always keep mobile phones and associated smart car apps up to date. UConnect, who develop a connected vehicle platform for a number of well-known smart car makes, let you check for updates online. Also, make sure you sign up for manufacturer updates.

2. Deactivate Services

If you aren't using it, deactivate it. Bluetooth, for example, is a possible exploit point for cybercriminals.

3. Secure Your Wi-Fi

Check out the Wi-Fi hotspot used by the car and wherever possible secure it – this includes replacing any default passwords. In addition, make sure you don’t write down any passwords associated with your smart car and leave them in the car.

4. Trust in a Good Mechanic

Malware upload may be more difficult to perform remotely, but it is easier if a malicious insider does it. Take care to find a trustworthy mechanic when you have your smart car serviced.

Smart Car Security by Design

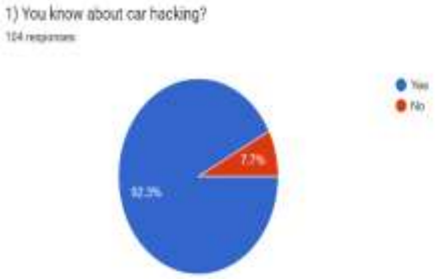
Secure best practices in the automotive industry are a must if we want to ensure a secure driving experience. The manufacturing process, itself, needs to be based on the principle of **‘Security by Design’**. To this end, frameworks and best practice guides are being developed to ensure smart cars have good security built-in, by design.

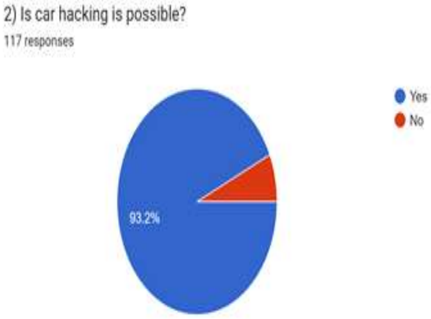
Design Smart, Design Secure

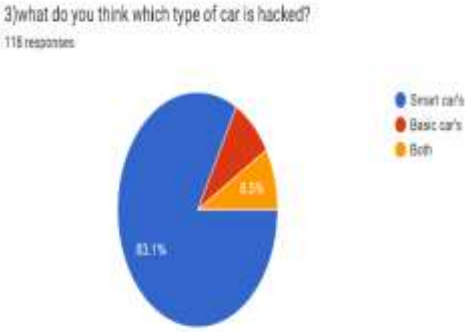
Ensuring that our smart cars give us a secure and privacy-enhanced driving experience means our manufacturers need to ‘design smart’.

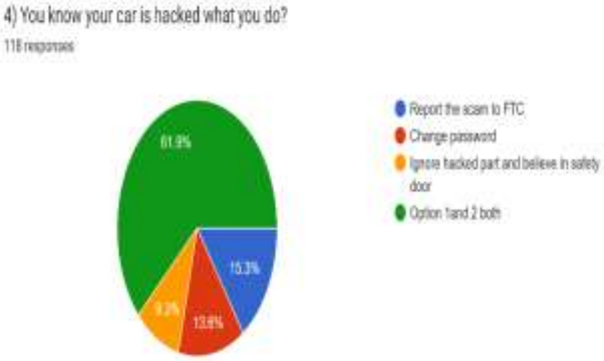
Smart cars are the equivalent of an Internet-connected device on wheels. All of the same vulnerabilities and exploits found in the Internet of Things (IoT) will come to haunt smart cars unless we plug the gaps with Security by Design.

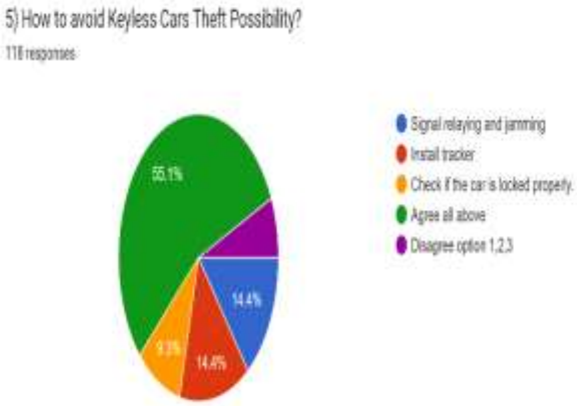
Result :-

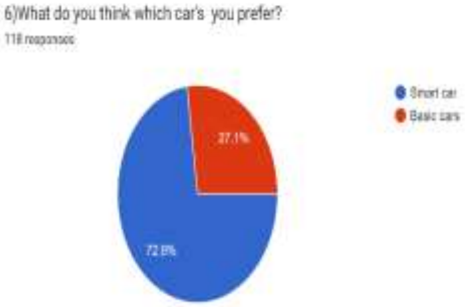

1) You know about car hacking?
104 responses
Yes
No
7.7%
92.3%


2) Is car hacking is possible?
117 responses
Yes
No
93.2%


3)what do you think which type of car is hacked?
118 responses
Smart car's
Basic car's
Both
8.5%
83.1%


4) You know your car is hacked what you do?
118 responses
Report the scam to FTC
Change password
Ignore hacked part and believe in safety door
Option 1and 2 both
61.9%
15.3%
9.3%
13.6%





7). Write something about car hacking? responses

Cars stolen by hacking is dangerous.

Car hacking can be reduce by taking proper measures

Car hacking is the manipulation of the code in a car's electronic control unit (ECU) to exploit a vulnerability and gain control of other ECU units in the vehicle.

Don't know

Not heard about any car hacking case but it's possible in smart car's

Basically car hacking is possible on smart car and in future most of the car are smart if they d

I don't have any ideas of car hacking

Car hacking is still unknown

Car hacking is tough

Hacking is not possible to smart car

Car hacking is difficult to hack

May be difficult to hack

Hacking no idea about that

Possible hacking

Don't know

Sometimes is dangerous to user

I don't no

Not think yet

Not hacking the car

Nothing happened

I don't believe

Not possible

Possible not, but it happens in smart car

Sorry no idea

Hacking

Don't no

Hacking not possible

Hacking is possible on smart car

Hacking don't possible

Improve database security

Yes possible

Hacking is difficult on smart car

Not hacking

Not interested in smart car

Not idea about hacking

Not hacking of smart car

Conclusion –

Cyber security is now the need of hour. Smart cars are the most vulnerable and open to any sort of exploits. One can imagine the situation of being hacked while driving. Even the airbags, brakes and accelerators may not be in one's control on wheel. So, manufacturers need to lay much importance on the CAN bus system by making it more hardware-secured and using secret codes.

By ending all possible ways of attack a hacker can perform on the car, we can patch that vulnerability and could save people.

Smart cars are here to stay. However, the cybersecurity risks they pose must be taken seriously by all distribution chain members. The creation of consistent standards across the automotive industry may help enhance security as manufacturers strike a balance between vehicle innovation and security. Until then, you can use the tips above to protect your smart car and your peace of mind.

Reference

1. Currie R. Developments in car hacking. SANS Institute; 2015.

2. Smith C. The car hacker's handbook: a guide for the penetration tester. No Starch Press; 2016.

3.Jafarnejad S. A car hacking experiment: when connectivity meets vulnerability. In: IEEE globe com workshop; 2015. P.

4. Zhang Y. Controlling a car through objection. In: IEEE 3rd international CONFERENCE on cyber security and cloud computing; 2016. P. 26–9.

5. Martinelli F. Car hacking identification through fuzzy logic algorithms. In: IEEE international conference on fuzzy systems; 2017. P. 1–7.

https://medium.com/@hackersera/the-need-for-cyber-security-in-connected-cars-trucks-and-infrastructure-515eb0a55934

https://www.tarlogic.com/blog/hacking-cars-problem-of-this-era/