International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

# Data Acquistion through Connectivities in Cars

**Kaushik Chhappaniya[1], Manjiri Kshirsagar[2], Mugdha Doke[3] Guided by Aishwarya Gore[4]**

*[1,2,3]Student, Second Year EXTC, Pune Vidyarthi Griha's College of Engineering and Technology, Pune-09*
*[4]Penetration Tester, Newton's Apple, Pune, Maharashtra, India*

---

**Abstract -** *This is the era of the integrating different fields. Internet cars or connected cars are controlling the market. Not only the smartphone but also the car holds a lot of user's data. Hacking of the car is now a days bit easier for threatening the society.*

***Key Words:*** *Internet cars, Hacking*

## 1. INTRODUCTION

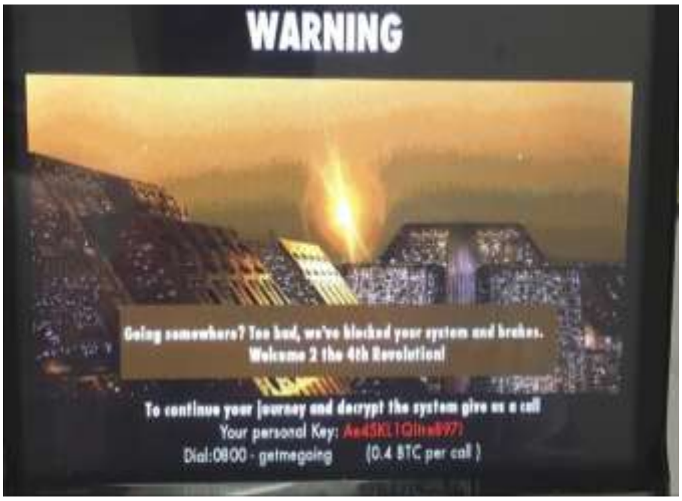
The Automotive cyber security is an emerging branch integrated of automotive and Cyber security .Having a great combination of cyber physical systems and connectivity in modern vehicles and mechanical equipment. But here's the mess the digital modernization in connected cars is not only opening a new branch but also creating a new field for the threat vectors .These are capable of critically affecting the functionality and safety of vehicles and also manipulating the other parameters.

Cyber security needed in a sense to protect vehicle components and vehicle-related data from illegal access, data acquisition, interference and modification. The report collects the threats to the system and has a brief discussion on it right from the data of nodes, sensors, Electronic Control Unit, software application protection and secure network connectivity (V2X, Bluetooth protocols, Wi-Fi protocols).

### 1.1 Need to Study It

Now a days a research done taken to identify possible cyber security vulnerabilities are pointing towards, that not only machines, smartphones, desktops but also cars can also be 'hacked'. This is a new threat to automotive industries.

As complexities in the vehicles is increasing day by day the available surface to attack on the car security increases. A single vulnerable device can leave an entire automobile industry open to attack, and the potential exposure ranges from inconvenience to massive safety breakdowns. This creates the threat to the society in a way that:-



WARNING

Going somewhere? Too bad, we've blocked your system and brakes.
Welcome 2 the 4th Revolution!

To continue your journey and decrypt the system give us a call
Your personal Key: Ae4SKL1QIira8971
Dial:0800 - getmegoing (0.4 BTC per call )

Fig-1: Hacked System

This can be seen in upcoming days if no primitive care is taken .So hacked car is not only a hacked infotainment system but also a very 'harmful weapon' .In the sense hackers can change the route and change the controls and they can also control the whole car (including brakes and accelerators

## 2. THE DATA OF USERS STORED IN THEIR VEHICLES:

| | |
|---|---|
| Event data records | On-board Diagnostic information |
| Location information | In cabin Information |
| Apps | User Recognition |
| External information | |

### 2.1 Event data records:-

These EDRs came into picture since 1990s.Till today EDR's are in 90% of the cars. They store information w. This information includes speed, accelerator, break position, seat belt usage and deployment of the airbags. EDRs are intended to provide the crucial information to investigate the crash.

### 2.2 In-Cabin information:-

Many of today's vehicles contain sensors inside the vehicle cabin. Microphone cameras and other devices can collect the data of the occupant. These sensors may be required for the emergency services and hands free use.

The hard drive storage of the car is storing all the above information.

### 2.3 User Recognition:-

1] Some of the today's cars with advanced systems recognize their user by physical characteristics.

2] The combination of the different devices like the smart phone and key. (In Evoque –Range Rover)

3] This may include physical or biometrics like face, fingerprint or voice.(face recognition in jaguar, land over, biometric sets in Bently , Driver state warning in Hyundai, biometric vehicle access in Porsche, voice recognition in Bentley ,Morris Garages, Aston Martin)[1]

4] These sensors can also track the movement of the user's eyes so as to check whether the user is asleep or not. Driver monitoring system recognizes driver and signs of distraction. [2]

5] The car may automatically adjust the seats and infotainment according to your everyday use.

### 2.4 Apps:-

Many of today's vehicles give you the freedom to install third party apps in your car infotainment like Apple CarPlay, Android Auto, Spot angels. Vehicles also allow an interface in apps in your smartphone .This apps have their special app privacy policies.

### 2.5 On-Board diagnostic information

All vehicles after 1996 are legally required the on-Board information diagnostic port (OBD-ll). Located generally underneath the driver's dashboard. It stores information like where you travel how aggressively you apply brakes .The information stored in it can be retrieved by inserting physically a device into it.

### 2.6 Location information: -

The location of your vehicle based on the GPS and your destination can be collected. Also the route the user takes can be collected. Your home, work and favorite places are also saved in your car system.

1) Set destination on schedule, live car tracking, location sharing[3]

### 2.7 External information:-

Modern vehicles may contain cameras and sensors that collect the information about the surrounding of the driver like assisted braking Rear-Parking detection, detect road or weather conditions ,lane markings and obstacles ,traffic condition and much more. Surrounding view cameras on under the mirror in number of cars. [4][5]

## 3. WIRELESS HACKING

WiFi plays a huge role in the hacking system. It works as a medium through which intruder can attack .Wireless networks are those networks which are connected to each other but not via the wires.eg in laptops, printers. The standard 802.11 specifies an over-the-air interface between a mobile device wireless client and a base station or between two mobile device wireless clients.

The tools used are generally used are wireshark, aircrack, wifimap, wifitap, wifiite, wpacleansmali, dex2jar [6]

### 3.1 Wireless Standards:

**1] SSID(Service Set Identifier):** It is the name of a wireless local area network (WLAN).All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. SSID is also known as ESSID (Extended Service Set Identifier).

**2]BSSID (Basic Service Set Identifier):** A BSSID is nothing but just a MAC address (Media Access Control) or Physical Address of the Wireless Access Point or the Wireless router. This is a unique 48 bit key provided by the manufacturer of the device. It can be in the form of Hexadecimal. I.e. 0-9, A-F

**3] BEACONS:** These are the wireless packets which are broadcasted to maintain the connectivity with the Wireless Access Point and Client Systems.

**4] CHANNEL:** It is the frequency at which the Wireless Signal travels through air. It can vary as per the changes in the surrounding air.

**5] DATA PACKETS:** These are the packets which are sent and received for the transfer of data between Wireless Access Point and Client Systems. All the data communicated between two computers travels in the forms of data packets.

### 3.2 Use in Infotainment and Having Hands Free Interaction in Cars

#### 1) Automotive Voice Assistant

Now a days voice assistant are come up along with the vehicles as we have in Android Devices and iPhone .It detects by just calling by any specific phrase or message (like hey MG). The voice assistant can recognize many of languages and work on your voice too. Using voice assistant we can open close the windows, doors, sunroofs, change AC temperature and also many more operations. Important features of Voice Assistant:

1.1 Drivers use Bluetooth to connect their smartphones to their car systems to make hands-free calls.

1.2 Getting directions and navigation is also the important feature of voice assistant. In A Class Mercedes cars we could just use three words to navigate a location.

1.3 Sending text messages

1.4 Playing Music.

1.5 Asking for local recommendations.[7]

**2) Embedded support for LTE**

Vehicles now days come up with a support of embedded SIM card The M2M or Machine to Machine SIM card is paired with the Internet Protocol (IPv6/IPv4). This keeps the vehicle connected to the internet and the world. LTE has so many advantages but the issue is LTE depends on **Multiple Input Multiple Output** (MIMO) antennas, which are too complex. The novelty of LTE system is itself a great challenge new network developments launching every day but still LTE is popular technology. The developers are look for programmable and more secured LTE modules that will allow them embedded application and to communicate with others.[8]

**3) Emergency call:-**

Cars like MG Hector have an E-Call emergency response system that alerts a SOS in case of an accident. Also when the airbags are deployed, e-call is activated and a text message is sent along with the location of the car. Also, a text message is sent to the registered emergency contact numbers to notify the respective people about the mishap. The main advantage of E-Call is the GPS positioning of the vehicle which needs the help. The road accidents could reduce by 10% and therefore saves 2,500 lives per year.

[9][10]

### 3.3 Types of Connectivity:-

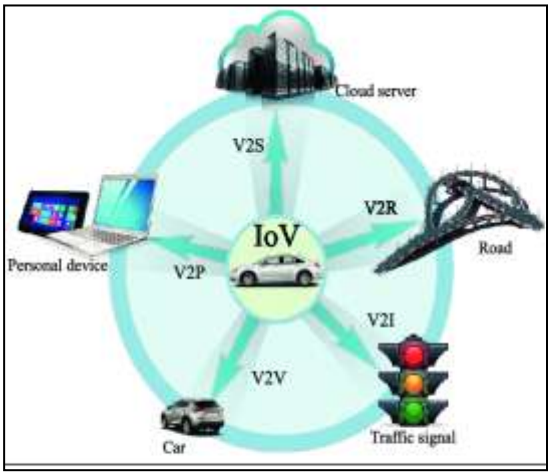


Fig-2 Types of connectivity

There are 5 ways a vehicle can be connected to its surroundings and communicate with them:

1. V2I (Vehicle to Infrastructure): The technology captures data generated by the vehicle and provides information about the infrastructure to the driver. The V2I technology communicates information about safety, mobility or environment-related conditions.

2. V2V (Vehicle to Vehicle): The technology communicates information about speed and position of surrounding vehicles through a wireless exchange of information. The goal is to avoid accidents, ease traffic congestions and have a positive impact on the environment.

3. V2C (Vehicle to Cloud): The technology exchanges information about and for applications of the vehicle with a cloud system. This allows the vehicle to use information from other, though the cloud connected industries like energy, transportation and smart homes and make use of IoT.

4. V2P (Vehicle to Pedestrian): The technology senses information about its environment and communicates it to other vehicles, infrastructure and personal mobile devices. This enables the vehicle to communicate with pedestrians and is intended to improve safety and mobility on the road.

5. V2X (Vehicle to Everything): The technology interconnects all types of vehicles and infrastructure systems with another. This connectivity includes cars, highways, ships, trains and airplanes.

## 4. ATTACK PROSPECTS:

1] Cars can be hacked and all the controls right from the steering, brakes, accelerator, transmission ,sunroof, windshield, and all the other controls. [11]

2] Information can be hacked and modified to increase sales by the companies and also by the user to change the statistics, this includes the distance travelled and other data through which they can fool the insurance companies.

3]Key fob hacking is a new method by using which attacker can enter a car without actually having its original key and steal the car.(uses jammer and intercepting the signal ).

4]Sometimes attacker don't hack the car intentionally .They do it just to get fame or for fun.

5]An attacker can hack the infotainment system of the car and change all the user data. Like the home and work and other locations in the map.

6]Also an attacker can change the route by hacking the infotainment system and can create a fatal threat to the user.

7]The ECU's in the cars are increasingly day by day and they can be hacked and the audio, video played can be changed.

8]By using the surrounding sensors in the car personal data could be hacked and then the victim can be blackmailed.

### 4.1 Prevention:

**Intrusion detection system(IDS)—**

**IDS** is the simplest way to prevent vulnerability and have the ability in detecting the attacks efficiently. Generally, IDS monitors the activities in the network or directly on the host, detects, and raises the alarm if there are any unexpected events occurred in the system. These unusual events, known as intrusions are they resist their way so that unauthorized access can be obtained.

The intrusions may come from internal, which resides inside the targeted system components having legal access privilege to the network, whereas external intruders may come from the outside of the targeted network, attempting to gain illegal access to the system components. It has categories as follows-, 1. Signature-, 2. Specification- and hybrid-based. There are 2 categories in IDS 1.Passive 2.Active

Passive IDS **only detects** the attack on the other hand active IDS takes **preventive action** on the attack. A typical IDS's architecture is made of sensors, a detection engine, and finally a reporting module. The sensors are implemented either in the network (network-based IDS) or directly at end node (host-based IDS).

**Hardware Security modules (AUTOSAR System)—**

It is a physical firewall made up of microcontrollers. Normally it has its own ram and has area for program code and data. It has timers, hardware accelerators for cryptographic algorithms. It can access the complete hardware of the host. It connects the host system as a firewall. This makes the system secure, authenticated startup of host monitors. The main use of HSM is it is freely programmable. With the help of cryptography(code writing or solving) we perform data transformation which cannot be accessed by unauthenticated users.[12][13]

**Machine learning:-**

Today's most trending point machine learning (ML) can be opted in this industry also ,to prevent the user from being the victim. We can implement a system which can test the user's car against attacks. The developed system will attack and find out the vulnerabilities and then solve it .likewise the designed system can collect lots of test samples which the system will learn and implement a immune system which will protect against the threat of upcoming vulnerabilities .

## 5. CONCLUSION

Hence we conclude this research creating awareness in individuals about their data stored in their cars and also the ways in which the data can be hampered. The connections they make through the features given in their cars are used to hack their cars. This is witnessing dangerous mishaps in the society.

## ACKNOWLEDGEMENT

We wish to record our deep sense of gratitude and profound thanks to ***Dr. Mrs. M. P. Atre****, Electronics and Telecommunication Department, PVG's COET, Pune, Maharashtra, India for showing keen interest, inspiring guidance, constant encouragement with our work during this completion of paper.*

## REFERENCES

[1]https://www.biometricupdate.com/201907/biometric-technology-in-development-for-several-auto-applications

[2] https://www.valeo.com/en/driver-monitoring/

[3]https://www.kia.com/in/uvo.html#uvo-introduction

[4]https://www.autobytel.com/car-buying-guides/features/10-cars-with-a-surround-view-camera-132305/

[5] https://www.buycarparts.co.uk/sensors-pr

[6] https://tools.kali.org/too`ls

[7] https://blog.soundhound.com/how-drivers-are-actually-using-voice-assistants-in-cars-bb1e3972301b

[8] http://embedded-computing.com/articles/lte-the-drivers-seat/

[9] https://www.mgmotor.co.in/ismart

[10] https://veillecarto2-0.fr/2018/04/01/ecall-the-geolocated-emergency-call-becomes-mandatory-inside-cars/

[11]https://www.youtube.com/watch?v=MK0SrxBC1xs&feature=youtu.be

[12]https://en.wikipedia.org/wiki/Hardware_security_module

[13]https://www.edn.com/hardware-security-modules-unleash-autosar/

[14] Information Security principles and practices ByMark Merkow,Jim Breithupt

[15] Wireless Hacking Exposed By Johnny Cache, Vincent Liu

[16] Hacking a Terror Network.

[17] Wi-Fi Protocols.