Vehicle Cyber Security

Mamta Pednekar[1], Prof. Sarita Sapkal[2]

[1]UG Student, Department of Computer Engineering, MMCOE, Pune
[2]Asst. Professor, Department of Computer Engineering, MMCOE, Pune

---***---

Abstract - *Technology has revolutionized the world changing the lives of people dramatically. There has been no time in history where the lived lives of people had experienced this greatness that technology has made to the automobile sector. Due to the idea of smart cities and technological advancements, we have seen a revolution in the way we drive our vehicles. Vehicle cyber-security consists of the security of vehicles, its networks and communications, and steps taken to avoid the exploitation of the software, hardware and the communication networks which are within the vehicle.*

Vehicles are no longer mechanical devices. Earlier, the entire control of the vehicle was the driver's responsibility but their functionalities can now be handled via software's. We are also seeing that the software companies are now developing software's for the automobile companies for providing automation. As automobile companies are growing more concerned with embedding smart technologies in the modern vehicles, it is giving rise to more vulnerabilities which allow entry of hackers into the vehicle's system which can take control from the driver which may lead to serious and irreversible threats. If it is a software or any product or a device, it has its own disadvantages and defects which can be hackable. Examples of some threats to the vehicle are Engine Shutdown, Locked Doors, Human loss, Loss of money, etc. In order to exploit the system, the hackers need to stay in the same network the car is operating on. But nowadays, it is also possible to hack the system even if the attacker is miles away from the system. This topic is now restricted to four wheeler vehicles only but maybe in the near future, same problems may be evident for airplanes or satellites leading to more devastating problems the world will experience. The problems we will face in the near future will be more but we cannot be reactionary to the technological advancements. Rather, we must find a way to overcome the problems.

Key Words:

ABS(Anti-Lock Braking System), ESP(Electronic Stability Program), ECU(Electronic Control Unit), CAN(Controller Area Network), IDS(Intrusion Detection System), OTA(Over the Air), CVC(Connected Vehicle Cloud)

1. INTRODUCTION

Nowadays, there has been a shift in the choice of vehicles that people buy. Earlier, people used to buy low cost vehicles which could suffice their purpose of travel. It had very less technologies or sometimes absolutely no technologies, but in these days people prefer buying high end vehicles which provide more security and are safer. There has been a change in the mindsets of people. They are becoming more concerned about safety. A lot of technologies have been introduced in these vehicles. Recently, Google had launched a self driving car which is completely automated and is driver- less. Security requirements for road vehicles and especially a driver-less car are more. Active safety systems provide various functionalities which have definitely reduced the road fatalities. Active Safety System such as ABS and ESP are some of the common features in most of the high-end vehicles. ABS and ESP are technologies which helps reduce accidents. Earlier, before ABS, whenever the driver applied brakes, the car used to stop immediately increasing the threat of skidding and accidents. But, in ABS, whenever brakes are applied by the driver in order to completely stop the vehicle, internally the brakes aren't applied instantly but in series of intervals of milliseconds. This avoid skidding and indirectly accidents. Secondly, before ESP, driving a car on a curvy road was dangerous because there were greater chances of the rear part of the car to get displaced or carried away by the curvy road. But, with ESP, this problem is avoided. This feature is mandatory in Sports Utility Vehicles. We can definitely say that these technology and many other have improved Road safety. Decrease of road traffic accidents need to be

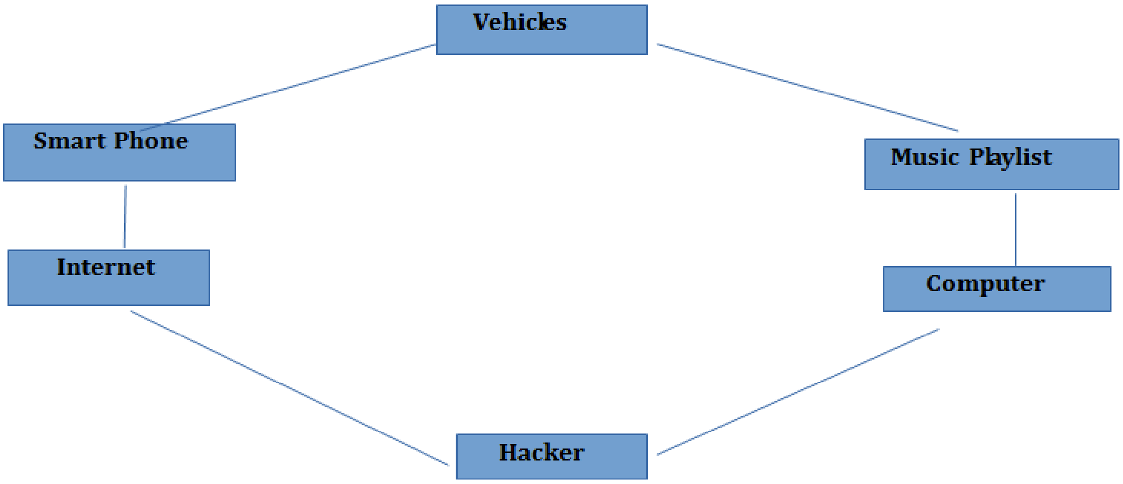


Fig 1.1

considered as a priority area because vehicle cybersecurity is a very serious topic and proper attention is required in this field. In the above figure, the ways of hacking of the vehicle are mentioned. The first way via smartphones which are connected to the internet. This internet can be hacked. The smartphone usually has apps through which we connect to the vehicle. Various companies are providing different applications which varied functionalities such as ConnectNext, OnStar App, etc. Vehicles are also used for infotainment. SO, whenever we play music via laptops or mobile phones, the defects can be hacked.

2. LITERATURE SURVEY

The paper by authors "Driving with Sharks: Rethinking vehicles with Cyber security" by authors Qiang Ni and Mahmoud Hashem Eiza had a lot of illustations but appropriate measures were absent. In this paper, the authors have illustrated the fact that nowadays, vehicles are no longer isolated mechanical machines that are solely used for transportation but now customers are increasingly demanding a seamless connected experience in all aspects of their lives including driving. The ECU units are explained and the various functionalities provided by them is also mentioned briefly. The software's present in the vehicles are hackable.

Some examples provided in the paper are-

1. Cherokee Jeep car uses a software Uconnect. Cherokee Jeep was remotely controlled by the Hackers using a simple 3G connection. The car was placed on the highway and the hackers were 10 miles away from the car. They were able to hack the software as it had a vulnerability.

2. The Mitsubishi Outlander Plug was hacked by a man in the middle attack. The hackers were able to turn the lights on and off and disable the whole theft alarm system leaving the vehicle vulnerable to more attacks.

In the network Architecture, the ways to enter into the system are shown. Cars contain 30 to 100 ECU which communicate among each other in order to perform a particular functionality such as Air Conditioning, AirBags, ABS, ESP, etc. ECU's communicates through the common network. Connection different devices is obtained through USB, Bluetooth, Wi-Fi, 3G/4G etc. Each subsystem of the ECU implements its own communication module to connect to the outside world. There are huge no of communication modules which makes the car functionalities accessible to the outside world.

Some of the Cyber Threats

a)OBD Threats

Car
Problems
OBD Port
Outside World

These ports provide entry into the vehicles functionalities. If these are hacked, the entire network of the vehicle will be accessible.

b)Malware

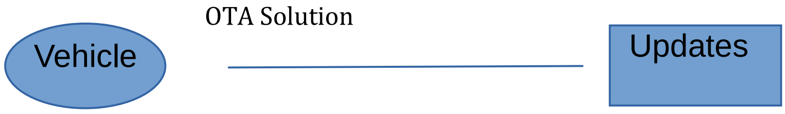
Malware can cause numerous problems. It can affect subsystems, packages, operations and the functionalities of the vehicle.

c)Mobile Applications

Automobile companies are now providing various IoT functionalities via applications. But, if these applications have defects, they may give rise to problems like data leakage or compromising safety or giving authority to a third party to

d)OTA Solution

Most of the updates by the automobile companies are provided to the vehicles through OTA. It allows a code to run. If security is not well implemented, the security is again at risk.



e)Cloud Services

The paper"Cyber-security as an attribute of active safety systems and their migration towards vehicle automation" by Dr I Ibarra*, Dr D D Ward has a brief introduction of the problem, the solutions and proper risk management approach. A brief about Active Safety Systems is given. Various systems like ABS and ESP are explained. Their uses are explained. In this paper also, OBD ports are explained. A car is no longer only used for transportation but also for infotainment industry. An overview of In-vehicle systems and cyber-security implications are given. The paper" Approaches for Vehicle Cyber Security" by Hiro Onishi had explanatory diagrams. Two different ways of hacking were shown and explained thoroughly. This paper focuses on vehicle and smart phone connectivity. The vulnerabilities caused by smart phone is explained. The various softwares of different automobile companies are mentioned. The paper has mentioned guidelines such as-

- Awareness

- Well-defined threats and risk analysis

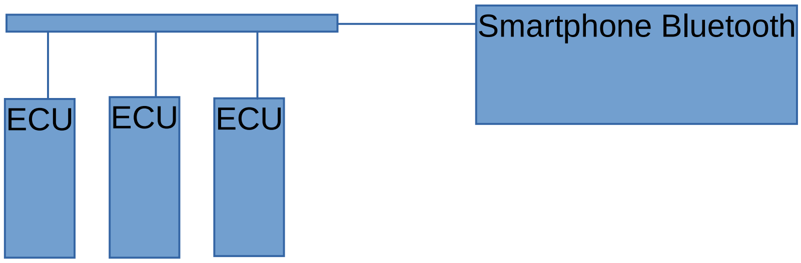
- Cyber security techniques

- Handling and mitigation of cyber threats

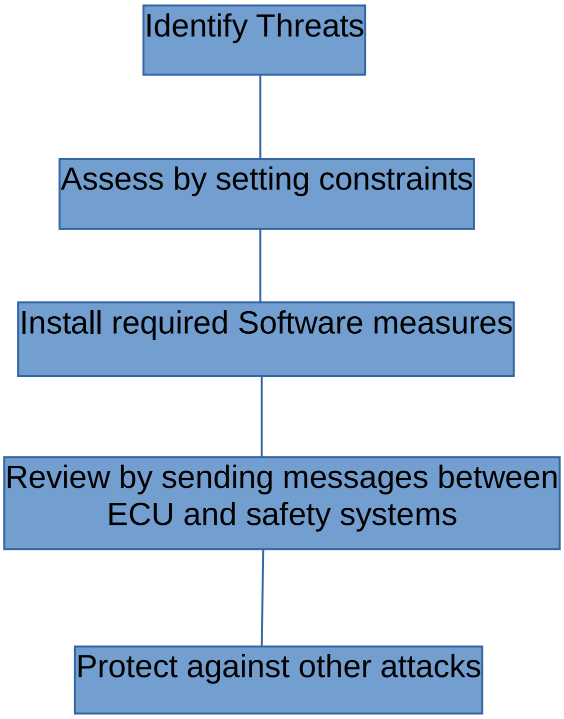
In the paper, "Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks,", the main focus is on the self-driving cars. It has also mentioned the risks of deploying vehicles with less security. In the paper, "Experimental Security Analysis of a Modern Automobile", it is explaining that vehicles are used for manifold of purposes rather than just as a mechanical device. The vehicles are suffering from major potential risks. The common problems that the cars are facing is mentioned and have also tried to explain the ways in order to overcome these problems. In the paper, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," the various solutions and its limitations are explained briefly. Also, malware and cloud is also explained.

3. SYSTEM ARCHITECTURE

Vehicles nowadays are controlled by hundreds of ECU's that form an internal network of devices within the vehicle in order to perform a particular functionality such as Airbag Control Unit, Infotainment System, ESP, ABS, etc. The ECU's communicate with other ECU's in order to achieve the function. A common netwrok is usually used for this purpose. But this may also increase the risk of a new cyber threat leading to more problems than solving them.



4. ALGORITHM/ FLOWCHART


Identify Threats
Assess by setting constraints
Install required Software measures
Review by sending messages between ECU and safety systems
Protect against other attacks

A car is now equipped with lot more functionalities than ever before. It has made life simpler but also has given rise to problems. Some of the steps in order to overcome these are to solely identify the problem and to find out whether the similar problem has been experienced before. If not, then assess the possibilities of overcoming it. Moreover, finding the most feasible security solution for it and testing the system with the new solution.

5. CONCLUSION AND FUTURE WORK

Firewalls are one the most common prevention systems for a system as it can block specified kinds of attacks and sites through packet filtering. They are both hardware and software based. IDS products are designed to detect network attacks. Two factor authentication is a method for mitigating unauthorized access to a system or sensitive information. It requires some software like a password or PIN, and some hardware like a card, dongle, cellphone. This reduces the unauthorized access to the system. Improving the security measures, will reduce unauthorized hacks. Active safety systems reduces the road fatalities significantly, as they improve the vehicle performance in critical situations where the driver may not otherwise be able to react in time.

Advantages:

1. It is possible and a necessity to use strong security measures and mechanisms in ordinary networks to protect the system.

2. Technology and various systems have improved safety and security

3. Reduced accidents and subsequently the human loss also.

4. Have made life easier.

5. Easily control the functionalities of the vehicles like starting or stopping the vehicle with a click.

Disadvantages:

1. High-end vehicles are costly which many people cannot afford.

2. ECUs in the vehicle are not developed from the same vendor. Thus, we cannot design one security solution for the whole system.

3. The functionalities should be provided at low cost so everyone can afford it and make use of it.

4. With the advent of technological advancements, there has been a significant change in the customer needs. People now buy high end vehicles which ensure safety and security. But these safe systems which are handled via software are also hackable which may cause huge and irreversible losses because if it is a software or a mechanical device or a product, it may have its disadvantages.

5. Software must be well-tested so that it has minimum defects.

6. Softwares must be complex which can reduce their chances of being hacked.

7. Connecting outside devices with vehicles networks are making them more vulnerable which can cause various problems like data leakage, etc.

REFERENCES

[1] M. Hashem Eiza and Q. Ni. Driving with sharks: Rethinking connected vehicles with vehicle cyber security. IEEE Vehicular Technology Magazine, 12(2):45–51, June 2017.

[2] I. Ibarra and D. D. Ward. Cyber-security as an attribute of active safety systems and their migration towards vehicle automation. In 8th IET International System Safety Conference incorporating the Cyber Security Conference 2013, pages 1–5, Oct 2013.

[3] H. Onishi. Approaches for vehicle cyber security. In 2014 IEEE Conference on Communications and Network Security, pages 506–507, Oct 2014.

[4] C.W.Axelrod, "Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks,"Proc . Of the 2017 IEEE LISAT Conference, Farmingdale, NY, May 2017.

[5] E.Vinsel, "The man who invented intelligent traffic control a century too early." IEEE Spectrum, July 21, 2016

[6] K. Koscher, A. Czeskis, F.Roesner,S. Patel, and T.Kohno, "Experimental Security Analysis of a Modern

Automobile", IEEE Symposium on Security and Privacy, 2010

[7] A. Greenberg, "Hackers remotely kill a Jeep on the highway – with me in it," WIRED, July 21, 2015. [Online].Available: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

[8] D. Lodge, "Hacking the Mitsubishi Outlander PHEV hybrid," PenTestPartners, June 05, 2016. [Online]. Available: https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv

[9] T. Zhang, H. Antunes and S. Aggarwal, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," IEEE Internet of Things, vol. 1, no. 1, Feb 2014, pp.10-21