An Empirical Study on Automotive Cyber Attacks

Aman Singh
Department of Electrical Engineering &Power Automation Indian Institute of Technology-Delhi
Delhi, Indian

Madhusudan Singh
Yonsei Institute of Convergence Technology
Yonsei University
Songdo, South Korea
Madhusudan.singh@ieee.org

***Abstract*—There has been various technological advancements in the field of autonomous vehicles. Which increase the possibility of the introduction of these vehicles in the market in some years. Moreover, then we will surround all with numerous autonomous vehicles and other intelligent systems making our life easier. They will include various networked embedded systems connected to internet running on numerous algorithms. These systems may contain vulnerabilities and threats that can be exploited. Therefore, these systems must be developed in order to minimize all the possible threats and vulnerabilities. In this study, we will majorly focus on the Cyber-Security vulnerabilities and threats that are possible in automotive electronics.**

***Index Terms*—Cyber-Physical Systems, Automotive, Cyber-attacks, Security, Vulnerabilities, Threats, Automotive Electronics.**

I. Introduction *(Heading 1)*

In recent years, some major advancements have been seen in the field of automotive electronics. And soon we will see autonomous automobiles on the roads. Cyber-Physical Systems (CPS) are one of the things that will greatly influence automobile industry. These systems have millions of applications in which users can be benefited. And this will have the direct impact on the users and they will eventually become an integral part of this system [1]. There will be the transfer of various types of physical data from the users to the servers and this will help them to act for the benefit of users. For example, giving health-related information to the user. In this system, users will interact thousands of electronic devices on a daily basis. This extent of interaction poses a crucial question that's needed to be addressed. Is this interaction safe for the users? The answer to this question depends on how these systems are developed. If these systems have vulnerabilities, then an attacker can exploit these vulnerabilities to harm the user. So we have to make sure that these systems are safe and do not have any vulnerabilities that can be exploited. To make this happen, first, we will have to study what are the various electronic systems that we are going to use to make our CPS. And then we will have to test these systems to see if they are free from any possible vulnerabilities, threats or cyber-attacks.

In this paper we have briefly described various security attacks that are possible on an automotive system, and measures to prevent these attacks.

II. Cyber-Physical Systems (CPS)Type Style and Fonts

The term 'Cyber-Physical Systems' was coined by Helen Gill at the National Science Foundation in the US in the year 2006. This was originally derived from the term cybernetics, which was coined by an American mathematician, Norbert Weiner.

A computer system connected to the internet that interacts with the physical world is called CPS. Integrating CPS in our society can have the huge impact on our living standards. It can also create new markets and rapidly increase our growth. CPS have applications in various fields as shown in fig.1. They can be used in automated vehicles with the motive to cause less pollution, include more safety features and to enhance quality entertainment in the vehicles. Homes can be equipped with these systems to help care for old and sick people, which will enable them to live independently. With an increase in the implementation of CPS [2], millions of new jobs will be created all over the world.

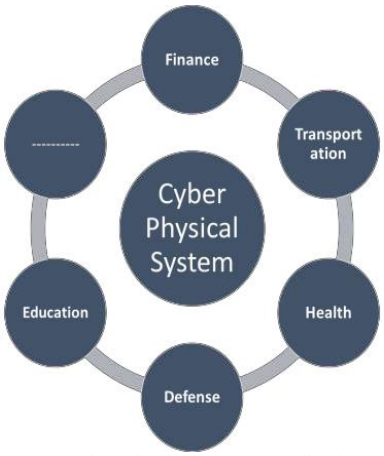

Fig. 1. Cyber-Physical System application

CPS has applications in various fields. CPS engineering can play a very important role in various fields being it a communication sector or the transportation, or the hospitals, all of them will be highly affected by the implementation of the CPS. Implementing a CPS is a very difficult job. Since it requires acquiring complete knowledge of CPS engineering and it is very expensive.

In some years, CPS engineering will completely transform the automobile industry. They will be an integral part of any vehicle. CPS engineering will work on making automobile

safer, easy to use, improving entertainment, controlling it remotely, improving engine management system and many more aspects.

III. Automotive Electronics

The automobiles that are currently present in the market have various electronic components in them but these components are not utilized to their full potential due to which they have very limited uses [3]. But in some years they will become an indispensable part of the vehicles which will do plenty of functions aiming to improve usability as well as the security of the vehicles [4]. The electronics present in the automobiles can be divided into four major sections. Which are briefly described below. In fig. 2 has shown some of the automotive electronics components.

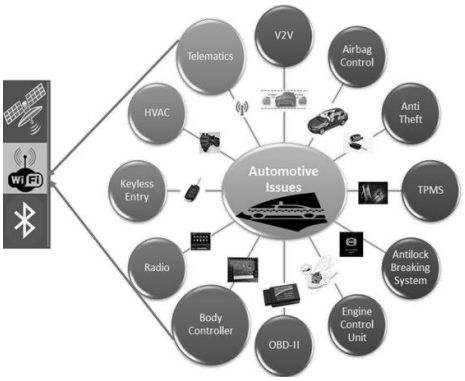

Fig. 2. The automotive electronics components example

A. Powertrain Systems

These systems affect driving experience as well as vehicles performance. This section comprises of Engine Control Module and Transmission Control Module. Engine Control Module has sensors that senses various physical parameters, which are, send to the processing unit, which processes these data and accordingly controls the actuators for the optimal performance of engine [5] Transmission Control Module is given input by the driver by applying brakes, clutches, accelerators, gears or the power switch. Which then processes and control the actuators according to input. Fig. 3 has shown the upgradation of the powertrain.

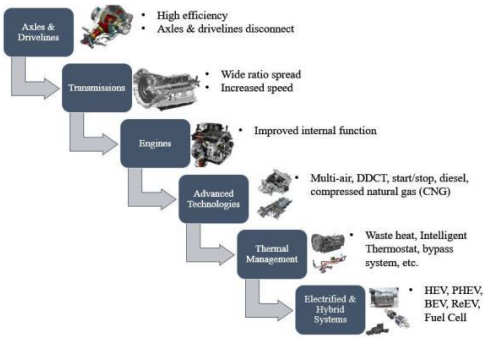

Fig. 3 Powertrain technology upgradation [5]

B. Body and Convenience Systems

These systems provide convenience to the users for various operations and hence improves the usability of the vehicles. This section comprises of light control, Heating Ventilation/Air Condition (HVAC), Power operated systems (seat and door) and remote keyless entry (RKE) alarm etc. These systems play important role in providing different facilities to the user and it is expected that this section will further expand to include many other facilities, which will allow users to interact with the vehicles more effectively [6].

C. Safety Systems

These systems improve the safety of the users and provide better control over the vehicle. This section comprises of Anti-Lock Braking System (ABS), Electric Power Assisted Steering (EPAS), Airbags, Driver assistant systems etc. ABS allows the driver to use the steering wheel while applying brakes which proves to be very useful in numerous cases. EPAS uses electric motors, which moves the wheels left and right according to the input given through the steering wheel. Airbags are one of the biggest safety feature introduced in the automobiles since its discovery. Whenever an accident occurs sensors the sends the signal to the processing unit which then actuates the airbags to move out. All these processes are completed within a fraction of seconds. There are various Driver Assistant Systems like forward collision warning, lane departure warning, front car departure alert and many more. These systems have been very useful in assisting the drivers while driving.

D. Infotainment Systems

These systems are mainly used for entertainment purpose while they also assist the user for various tasks. This section includes Telematics, In-car Multimedia, and Navigation. Telematics system captures and stores driver's data. Insurance company to set insurance price for the car, which will be a win-win situation for both of them, can use this data. They can also be used to take safety measures if the user is in danger. In-car Multimedia mainly includes the audio and visual systems placed in the automobiles, which are used for entertainment purposes. Navigation systems have proved to be very useful for the drivers when they go to any new place.

IV. Vulnerabilities,, Threats and Cyber Attacks

When these automobiles will become autonomous then these systems will start sending data over the internet to the servers. In addition, these servers working on several algorithms will manage these data to smoothly control the vehicle. Moreover, there comes the possibility of having some vulnerabilities and threats in this system that can be exploited. Therefore, these systems should be developed in such a way that they are secure. A system is said to be secure if adheres to the principles of the CIA triad. This triad stands for Confidentiality, Integrity and Availability. All the possible

dangers that may compromise the CIA triad are called threats. Moreover, Vulnerabilities are the weaknesses in the system that may cause a threat to be exploited. So it's time to look over the various possible vulnerabilities, threats and cyber-attacks that may take place [7].

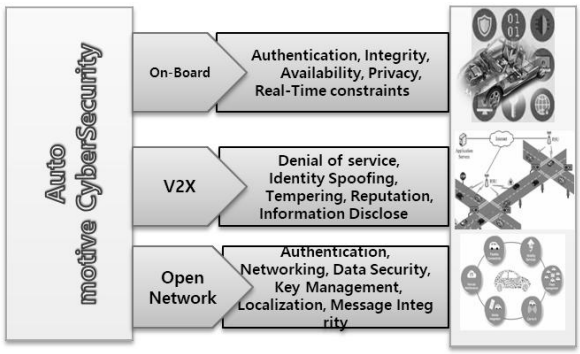

Fig.4. Automotive cyber-security threats.

A. Vulnerabilities

A security mechanism should be such that it completes it is target of protecting the system without compromising with the user needs. For example, multiple identification processes may frustrate the user and effect the overall productivity. Therefore, security models are designed in three general ways and are explained below.

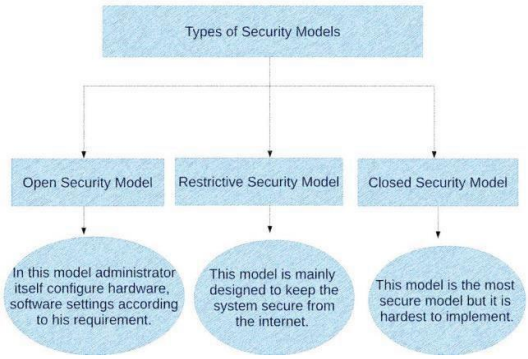

Fig.5. Different types of Security Models

An electronic system has mainly three types of vulnerabilities.

1)*Networks Technology Weaknesses:* These weaknesses are usually found in TCP/IP protocol, Operating System and Network Equipment. TCP/IP protocols were badly designed, so they are inherently insecure. Mainly HTTP, FTP, ICMP, SNMP, SMTP and SYN floods have major weaknesses. Some old operating systems also have major issues that are needed to be addressed. These operating systems are UNIX, LINUX, Macintosh, Windows NT, 9x, XP and OS/2. Network Equipment like routers, firewalls and switches have security weaknesses that are needed to be fixed. These weaknesses mainly include the Password Protection, Lack of Authentication, Routing Protocols and Firewall Holes [8].

2) *Configuration Weaknesses:* Many possible configuration weaknesses are needed to be checked by the administrator of the system. The Administrator must be aware of the configure element, configure process and the vulnerabilities that are possible in the system during configuration process and configuration element. Unsecured user accounts may lead to exposure of account information to the intruders across the network. System accounts must not have common passwords that can be easily cracked. Enabling JavaScript in the browser may allow attacks through hostile JavaScript while visiting untrusted sites, IIS, Apache, FTP and attacks can also be made through terminal services. Many products have default settings that have vulnerabilities. Misconfiguration of the network equipment also poses problems.

3) *Security Policy Weaknesses:* While operating any system one should keep in mind to follow the security policy of the system that has been defined by the security developer. But it is the security developer's responsibility to make the security usable to the user so that the user need not have taken any wrong measures which in turn compromises the security. A security policy must also be in written forms to help users. Sometimes it is difficult to implement security policy due to political battles and inadequate monitoring and auditing done by IT companies which leads to the insecurity of the data. Sometimes legal actions are taken against these companies. Installing software's from untrusted sites also create security holes in the systems. Disaster recovery plan should also be made to recover from any mishap.

B. Threats

There are four possible primary threats to a system. They are Unstructured Threats, Structured Threats, External Threats and Internal Threats [9]. They are briefly described below:

1) *Unstructured Threats:* These type of threats are itself created by the companies to check security and sometimes for challenging a hacker's skill.

2) *Structured Threats:* The attackers to exploit the system for various purposes create these types of threats. They are very experienced and use advanced hacking techniques to steal the information.

3) *External Threats:* These threats are from the attackers who do not have administrative access to the system. To gain access they attack into the network connected to the internet.

4) *Internal Threats:* These threats are from the attackers that have unauthorized access to the system either with the account on the system and sometimes they have physical access too.

V. Possible Cyber Attacks in Automotive Technology

The hackers to steal the information from the system perform Cyber Attacks. Hackers use various techniques to hack the systems. These are discussed below:

A. Malware Injection

Malware is short for Malicious Software. These are computer code which is incorporated to steal the information

from the system illegally or to corrupt it. They are of various types such as viruses, spyware, adware, Trojan horses, ransomware, scareware, worms etc. They are injected into the system through emails, pen drives, CDs, DVDs etc. They are usually specific to their behavior. Anti-Malware software can be used to prevent attacks.

B. Phishing Attacks

In a phishing attack, an attacker sends an email containing some malicious files. They normally send email to the person disguising as someone familiar with the person. This increases the possibility of opening that file and hence infecting the system.

C. SQL Injection

SQL injection attacks works if the server has vulnerabilities that permits SQL server to run malicious codes. We can even get usernames and passwords of the server through SQL injection.

D. Denial of Service Attacks

Denial of Service attacks compromises the Availability principle of the CIA triad. In this attack attacker floods the server with more traffic than it was built to handle. This crashes the server. And users are unable to access the server.

E. Man-in-the-Middle Attacks

Whenever a user makes a connection to the server, it is given a unique session ID which help in transferring data back and forth. An attacker tries to steal this unique session ID to steal the data which is being transferred.

F. Credentials Reuse

These days' users create hundreds of login accounts on several websites. Since it is nearly impossible to create different login credentials for every different website. So they reuse the same login credentials for all the websites. So attackers can crack the login credential of the user from a vulnerable site and reuse them on some secured sites like banking sites.

G. Trust Exploitation Attack

In this type of attack, an attacker first takes control of the system which is trusted by the target system. Then attacks the target system by taking the advantage of trust relationship between these systems.

VI. Conclusion

Until date, few attempts have been made to devise an autonomous vehicle but all of them either have defects or they are under testing stage. Tesla Motors came out with autopilot feature in their cars in October 2015. But these cars were only useful for limited access highways and not for urban driving. Because the autopilot feature could not detect pedestrians or cyclists. Google is also trying to make autonomous vehicles. Other companies like Google, Uber, Audi, BMW, Volkswagen and many others have also revealed their prototypes but all are under testing stage. Most of the tech companies have stated that they would be ready with their fully functioning autonomous vehicles by 2020. Presently, this technology contains various vulnerabilities that are needed to be seen. Driver-less technology will revolutionize the transport industry in the coming future, so they must have security which can't be compromised. The analysis of the automotive systems provides the information of what are the probable attacks that can be deployed to compromise security of the system and probable measures to avoid them.

References

[1] B. Mokhtar, M. Azab, Survey on Security Issues in Vehicular Ad hoc Networks, Alexandria Engineering Journal, Elsevier, PP. 1115- 1126, 2015

[2] J. Blum and A. Eskandarian: The Threat of Intelligent Collisions. IT Professional, vol. 6, no. 1, January/February 2004, 24–29.

[3] M. Raya and J.-P. Hubaux: The Security of Vehicular Ad Hoc Networks. Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, 2005.

[4] S. Arya1 and C. Aryal, "Malicious Nodes Detection In Mobile Ad Hoc Networks", Journal of Information and Operations Management, ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012, pp-210-212.

[5] B. lee, I. Day Auburn Hills, may 6 – 7 2014, Fiat Chrysler Automobiles.

[6] S. Ghansela "Network Security: Attacks, Tools and Techniques", Ijarcsse Volume 3, Issue 6, June 2013.

[7] S. Yousefi, et al., Vehicular ad hoc networks (VANETs): challenges and perspectives, in: ITS Telecommunications Proceedings, 2006 6th International Conference on, 2006, pp. 761–766.

[8] X. Sun, et al., Secure vehicular communications based on group signature and ID-based signature scheme, in: Communications, 2007. ICC'07. IEEE International Conference on, 2007, pp. 1539–1545.

[9] K. Biswas, M.L. Ali, Security threats in mobile Ad Hoc Network, Department of Interaction and System Design School of Engineering, march 2007, pp. 9–26.