International Journal of Scientific and Research Publications, Volume 10, Issue 12, December 2020
ISSN 2250-3153

Cyber Security Challenge in an Automobile

Laiba Pervez, Aiza Khan and Noor ul Ain
Department of Computer Software Engineering, MCS,
National University of Sciences and Technology, Islamabad, Pakistan.
Email: laibaawan12@gmail.com, aizaahmed154@gmail.com, nooryousaf178@gmail.com

DOI: 10.29322/IJSRP.10.12.2020.p10815
http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10815

***Abstract*—Automobiles such as smart cars have become tremendously complex, as they are allowing us to connect our phones to user interfaces of car and connect with external networks as well. Unfortunately, the interconnectivity of cars, embedded processors and systems developed in the vehicles have become targets of cybersecurity attacks making it the biggest challenge with respect to cooperative automotive industry. The real issue is caused when a spoofed message is injected in the internal network of the system compromising the security of the automobile. This paper will aim at providing a solution to secure the private information of each automobile by using cryptographic algorithm for authenticating the message. Upon successful failing of the cyber-attack a notification will be displayed to the User Interface (UI) of the automobile to keep the user aware of the situation.**

Keywords: Automotive, Security Attacks, Advance Encryption Standard (AES)

I. Introduction

Automobiles have evolved from transportation means to objects for a design consisting of individual, public and social spaces. With the rise of insightful transportation frameworks, the focal point of automobile design has moved from the structure of independent vehicles to the structure of consistent cross-vehicle transportation frameworks, typified by the integration of infrastructure, people, vehicles, urban areas and environment [14]. This combination of computer technology and automobile innovation has raised numerous issues about cyber-attacks in automobile playing a significant job in the development and utilization of automobile technologies.

Each activity in the vehicle can possibly be shared and reused which has stirred a continuous discussion about the amount of information sharing that must stay in the hands of an individual and what job automobile User Interfaces (UIs) play in this. A spoofed message containing virus or malware can be injected to the telematics unit of the automobile that communicate with the help of Controller Area Network (CAN), a vehicle bus that helps micro-controllers communicate with each other. This way the attacker can take control of the automobile as there is no message authentication system present on the CAN. It is significant, that our future vehicles and their supporting keen infrastructure, software and hardware foundations are designed to guarantee protection and security while fulfilling the need for extensibility, working normally under both normal and critical operating situations [1], [9].

An extensive literature review was done to identify the challenges of the automobile. The focal points of this exploration are the cybersecurity dangers, which is the biggest challenge with respect to cooperative automated vehicles. Whenever the cyber-attack happens, it can possibly cause more harm than the cyber-attack occurred in the non-automated system in light of the fact that a driver will not be able to handle the malfunctioning attack if he/she is totally disconnected from driving. Cybersecurity aims to avert unapproved access to digital gadgets like PCs, cell phones, and laptops, wireless communication protocols and other wireless routers [1].

In order to minimize the knowledge gaps to maintain a high standard of future cyber-security in an autonomous vehicle [5] and to secure the private information of each automobile this paper will aim at providing two contributions. At first a symmetric, cryptographic algorithm will be implemented for authenticating the messages. Both the communicating devices will exchange a secret key before a secure communication is developed. The key size can be 128,192 or 256 bits and is encrypted in rounds is depending on key size. The main goal will be to make the spoofed messages and cyber-attacks detectable and waste them before they damage the security of the system. Secondly, upon successfully rejecting the cyber-attack a notification will be displayed on the UI of the automobile to keep the user aware of the situation. This added feature will give a sense of safety to the user.

The remaining structure of paper is organized as follows. Background is discussed in Section II, while related work is described in Section III of the paper. Section IV presents the proposed solution, and Section V evaluates the proposed solution. Section VI constitutes the Conclusion.

II. Background

The advancement of new technologies such as Artificial Intelligence, IoT and cloud technologies, new innovation in the autonomous vehicle industry is demanded. The main focus is to improve the security while driving, reducing the human error, speech recognition for Human-Machine Integration (HMI) and the reliability of vehicles containing On-Board Diagnostic (OBD) systems.

The interconnectivity of these devices leads to some potential vulnerabilities, threats and security risk to networks as well. These networks also include sensor networks, financial networks and traffic control features. A cyber-attack can start with controlled technology tools that are embedded in AVs such as electrical window controls, which are now controlled by Engine Control Units (ECUs) as embedded systems. Some cyber-attacks involve the use of malware like

computer viruses, worms, Trojan horses, spyware and adware; there are also denial-of-service attacks, phishing, and man-in-the-middle attacks [1]. Control Area Network (CAN) attacks happen when an attacker targets the control bag system, warning lights and electric window lifts. As embedded systems are software-oriented so the security should be taken as compulsory. System should know which threat is safety failure and security attack after identifying so the system should react accordingly [7].

Computational strategies cause a potential of vulnerabilities and threats when used in the different connected autonomous vehicles. A revolutionary change in technologies requires many computing resources in order to achieve a successful mechanism for automobile systems [8].

Fig 1. shows an attack on even a single Electronic Control Unit (ECU) can corrupt the whole system since ECUs are connected with external interfaces and communicate through Controller Area Network (CAN).

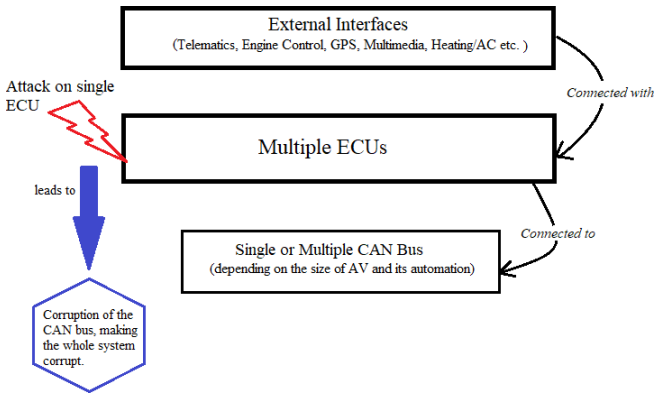


Fig. 1: AV system framework.

Securing the product quality first has always remained important in software development activities, whereas focusing on the cyberattack on information and running vehicles is less important in the traditional industry. Many companies are now following ISO 26262 and Automotive SPICE for the safe operations of vehicles and controlling processes as well.

III. Literature Review

Communication is not merely limited to communication between cars (vehicle-to-vehicle (V2V)), nor to communication between cars and the infrastructure (vehicle-to-infrastructure (V2I)) in fact autonomous vehicles now communicate with each other and share information about the environment. The environment information is collected entirely from on-board sensors without any active communication with other vehicles or the infrastructure. Fig 2 shows possible communication security issues within a vehicle, vehicle to vehicle (V2V) and intelligent vehicle communication with infrastructures. The possibility of a cyber-attack increase with the increase in the degree of automation of a vehicle [12], [14].

Fig. 2: Security issues in communication

A fully autonomous system needs to ensure to bring the vehicle to a safe state whenever some critical hazard happens. The fusion system can help in order to identify the expected attacks but when there are only two sources of information with respect to vehicle state and one they are compromised due to cyber attack, then in this situation, the system will not be able to identify which one is valid.

Another challenge that was identified was spoofing of GPS systems used in vehicles where an attacker impersonates signals and provide the false locations. EMP attacks, medium threats and attack on the navigation system were also found. In [6] researchers with respect to autonomous interface challenges address some essential questions focusing on how the autonomous system will be able to know our daily routine schedule and act on it without even asking from us? A critical challenge arises with data sharing between connected cars. Though car to car connectivity helps in developing applications related to safety such as collision avoidance, it also provides loopholes for unauthorized access to personal data and activities occurred during driving.

In [11] a researcher found various potential vulnerabilities in Tire Pressure Monitoring System and Garcia found a vulnerability in a key-less entry system that allows cloning the remote control for unauthorized access of vehicle.

[2] explains that by attacking the sensors of the autonomous vehicle the attacker can create platform suicides and DOS attacks can be performed easily then. In [4] researchers have focused on Denial of Service DOS attack on networks. Some of the attacks found included Sybil attack in which multiple messages are sent through one node to another in order to leave the road, node impersonation and sending false information. To mitigate the attacks, a model is proposed by the researchers in [4] containing On-Board Unit (OBU) connected on vehicle nodes in order to make effective decisions when some cyber-attack occurs.

Groza and Murvay [3] explain a variety of techniques to secure the CAN bus from the cyber- attacks such as key sharing, cryptographic passwords and CAN authentication.

In [13], Researches have proposed a framework called Ve-

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10815

cure Fig.3, to protect the Control Area Network from spoofed messages injection attack and they evaluated it by using free scales automobile development board, in their research Denial of Service attack, where a large number of bogus messages are sent to the CAN were not considered since their primary goal was to inject a spoofed messages.

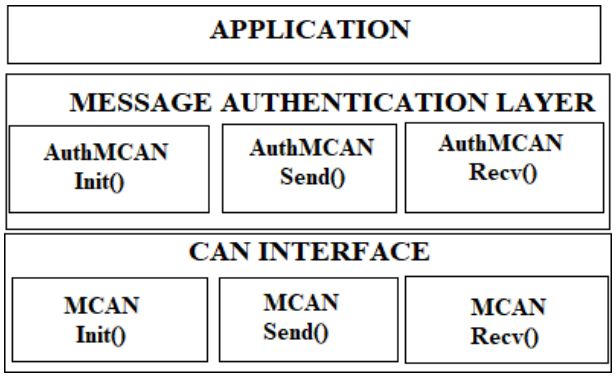


Fig. 3: Vecure Architecture [14]

Some researchers in [10], [8] proposed biometrics to secure the communication between AVs like Face Recognition and Iris Detection mechanisms but these techniques have several limitations.

A comparison Table I has been shown below stating the knowledge gaps found during the literature review of the already proposed solutions. The solutions are checked against a few defined parameters.

TABLE I: Comparison Table

Parameters	Fingerprinting Physical Signals	VeCure
Authentication System in CAN bus	Use of biometrics. No authentication on CAN.	Message authentication mechanism on CAN protocol.
Time management	Undefined	Online message processing overhead is only 50us.
Key sharing techniques	No keys required.	A secret symmetric key generated to authenticate each received message.
Notification to User	None	None

IV. Proposed Solution

Automotive vehicles are vulnerable. Our data, location and confidential information can be access by any hackers who hacked our system. So our problem is to secure our data from cyber security attacks. To secure data from such attacks cryptography methods such as one time pad, diffie hellman key exchange and blowfish etc. We are going to use Advance encryption standard (AES) algorithm for our problem statement. AES algorithm is a symmetric encryption algorithm. In cryptography, AES is a computer security standard defined by National Institute of Standards and Technology (NIST).

In 1997, a competition was held by National Institute of Standard and Technology in order to choose the AES so that it should supersede the Data Encryption Standard (DES). Symmetric keys of different sizes are utilized with block of 128 bits of input data. The size of key can be 128,192 or 256 bits and number of rounds is dependent on key size. It uses 10,12,14 rounds with its number of size. The implementation of key pairing mechanisms and the rounds in ECU and CAN will keep the data and information confidential and protect the system from hackers. An abstract, systematic structure of the implementation using AES is depicted in Fig 4.

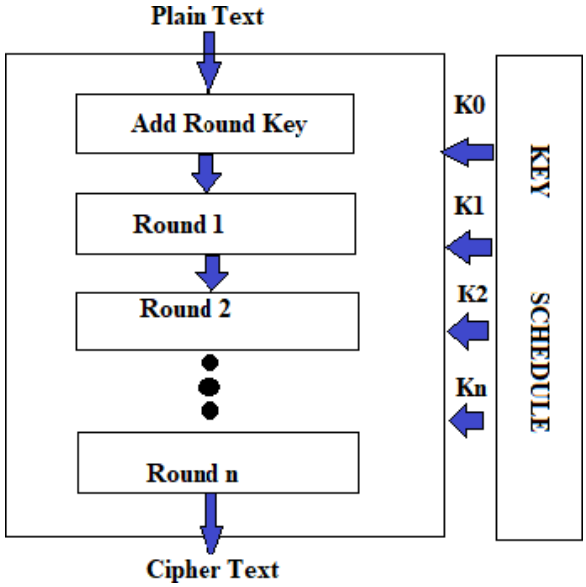


Fig. 4: AES Structure

The detailed description of this structure requires both the communicating devices to exchange a secret key before a secure communication is developed . A key encapsulation mechanism or a random number is generated by the receiver and sender devices or micro-controllers. Message authentication mechanism will check the received message for its key and compare it. If the keys are matched successfully, the message will be forwarded and displayed to the driver on the UI of the vehicle.

If an unauthorized devices or vehicle has sent a spammed message, the key will not match at the receiver's end. The CAN protocol will reject the message eventually. In such a case, a cautious notification will be displayed on the vehicle's UI to the driver, keeping him aware of the situation. This visualization of the circumstances has not yet been proposed in the earlier solutions.

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10815

Fig 5 shows the detailed structure of the solution.

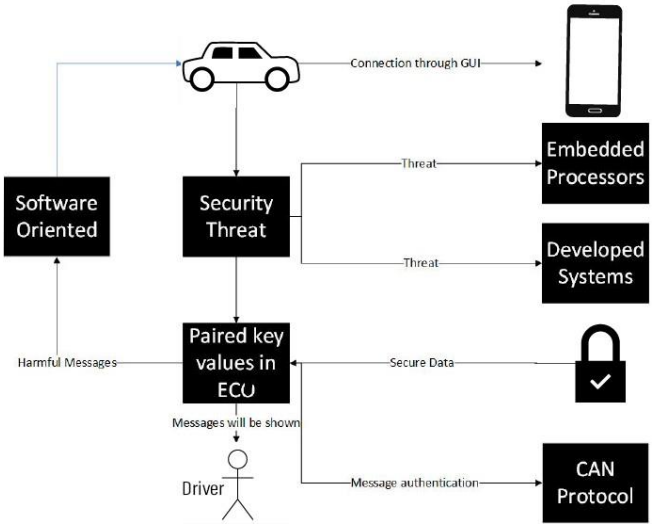


Fig. 5: Detailed Structure

In contrast to Asymmetric Algorithm, which are considered to be too slow for the time critical automobile CPS application, Advanced Encryption Algorithm being symmetric not only gives a highest performance in smaller data but also in large data as well.

V. Evaluation and Prototype

In this section, we have evaluated our proposed technique. We tried to bridge the knowledge gap found in the earlier solutions as no visualization way was found previously which could give a sense of safety to the user. For this purpose, we have used Justinmind prototype tool to show how the notification of message will be displayed on the UI of automobile. Once the hacker tries to inject any hacked message, the message authentication mechanism on the CAN protocol will reject the keys and a caution message "You have been saved from Cyber Attack" will be popped on the UI as depicted in Fig 6. This message will aware the driver about the adversary and help him remain precautious.

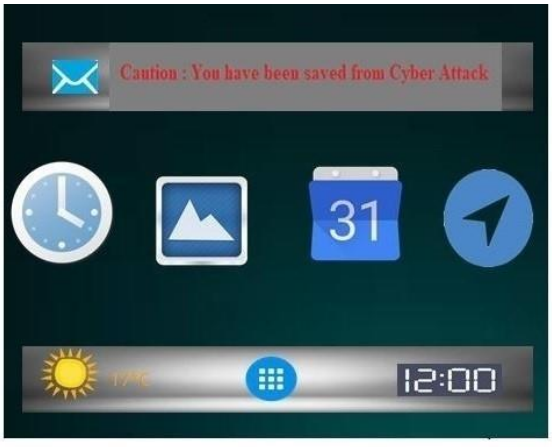


Fig. 6: Caution message on UI of vehicle

Fig 7 shows a message on automobile's UI to change the lane because of the traffic.

Fig. 7: Secured message on UI

For testing the algorithm, MATLAB has been used for simulating the result. To compare our proposed solution, a substitution cipher algorithm was taken to show the encrypted message sent to the automobile. In Fig 8, substitution cipher algorithms have encrypted our message "Please change the lane, traffic ahead" into encrypted message.

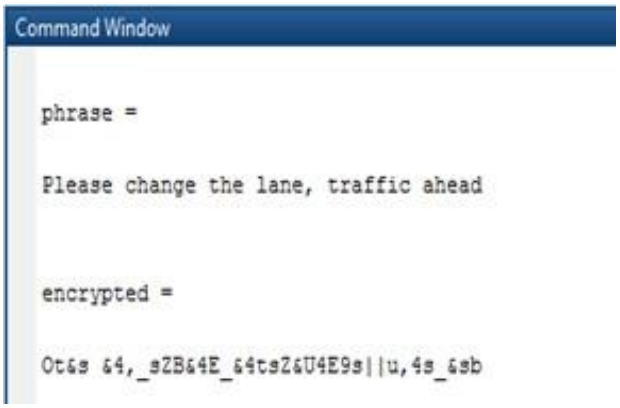


Fig. 8: Substitution cipher on Message

We simulate the result on MATLAB where a cipher text was created for all printed character. We have used pt for plain text or message and ct for cipher text. An index is assigned to every character of our message and then it is further encrypted.

ind(i)=strmatch(phrase(i) , pt, 'exact')
encrypted = char (ct (ind))

In substitution cipher, a brute force attack can easily happen. An attacker can guess the message by sending different pass phrases. They can inject different spoofed messages in order to threat the driver.

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10815

Fig 9 shows the code of our substitution cipher.

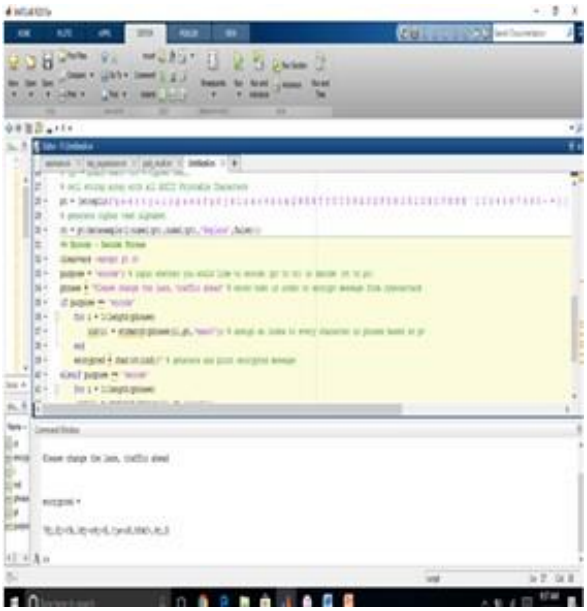
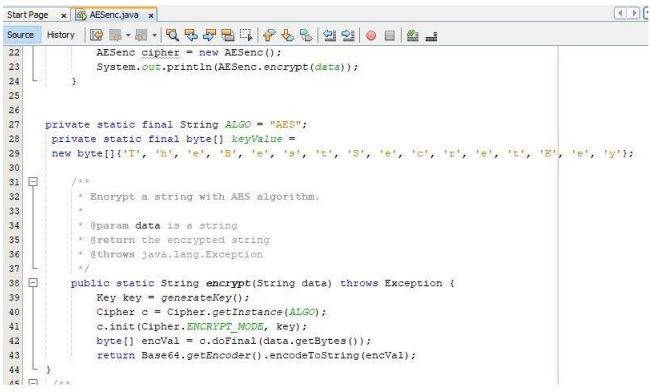


Fig. 9: Simulation of result on MATLAB

We used NetBeans to simulate the block cipher algorithm called AES-128. A message “Please change the lane, traffic ahead” will be encrypted by different round keys and XOR. AES-128 will create a threat free network by not only securing our information but also making it difficult for the attacker to decrypt the message. Fig 10 shows our encrypted message on net beans.

```
run:
Please change the lane, traffic ahead
VXPe+8wdpW8HC/+Emrc/moZAFEm+rrzenO8KpPPB6QbVdziEx/WvdN8OI/CVLd2b
BUILD SUCCESSFUL (total time: 14 seconds)
```

Fig. 10: Encrypted message



```
Start Page | AESenc.java
Source | History
22          AESenc cipher = new AESenc();
23          System.out.println(AESenc.encrypt(data));
24      }
25
26
27  private static final String ALGO = "AES";
28   private static final byte[] keyValue =
29   new byte[]{'T', 'h', 'e', 'B', 'e', 's', 't', 'S', 'e', 'c', 'r', 'e', 't', 'K', 'e', 'y'};
30
31      /**
32       * Encrypt a string with AES algorithm.
33       *
34       * @param data is a string
35       * @return the encrypted string
36       * @throws java.lang.Exception
37       */
38      public static String encrypt(String data) throws Exception {
39          Key key = generateKey();
40          Cipher c = Cipher.getInstance(ALGO);
41          c.init(Cipher.ENCRYPT_MODE, key);
42          byte[] encVal = c.doFinal(data.getBytes());
43          return Base64.getEncoder().encodeToString(encVal);
44      }
45      /**
```

Fig. 11: Encrypted message

A base64 in our code will implement the encoding for both upper and lowercase letter. A secret key class represents the key providing independently. It is constructed through an array byte. Comparative to substitution method, our proposed algorithm stands out as a more secure one. During our implementation, the only drawback that we found was some delay in performance time of our proposed cryptographic algorithm. But a few seconds of delay can be compromised by the security of the network.

VI. Conclusion

In this paper we proposed the use of AES algorithm to secure the data theft and cyber attacks in the vehicles. The main idea of this solution is to implement a mechanism of message authentication using paired key values in the ECU which communicates with CAN protocol. Any harmful, hacked messages injected to an ECU or OBD-II port will be notified visually to the driver on the interface of the vehicle. This solution will help the driver recognize the attack and also take precautionary measures.

For future work, this solution can be used by the researchers for implementing this proposed model and test it according to the standards.

References

[1] Automotive cyber security: An iet/ktn thought leadership review of risk perspectives for connected vehicles.

[2] T. Padir L. Lai-T. R. Eisenbarth A. M. Wyglinski, X. Huang and K. Venkatasubramanian. Security of autonomous systems employing embedded computing and sensors. *IEEE Micro*, vol. 33(no. 1,):pp. 80–86, 2013.

[3] B. Groza and P. Murvay. Security solutions for the controller area network: Bringing authentication to in-vehicle networks. *IEEE Vehicular Technology Magazine*, 13(1):40–47, March 2018.

[4] Irshad & Ab Manan Jamalul-Lail Hasbullah, Halabi & Soomro. Denial of service (dos) attack and its possible solutions in vanet. *International Journal of Electronics and Communication Engineering*, Vol:4(No:5), 2010.

[5] K.Wilson I.Parkinson, P.Ward and J.Miller. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation System*, 2017.

[6] A. L. Kun, S. Boll, and A. Schmidt. Shifting gears: User interfaces in the age of autonomous driving. *IEEE Pervasive Computing*, 15(1):32–38, Jan 2016.

[7] Irina-Georgiana Oancea and Emil Simion. Challenges in automotive security. In *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pages 1–6, June 2018.

[8] Jamal Raiyn. Data and cyber security in autonomous vehicle networks. *Transport and Telecommunication*, volume 19(no. 4):325–334, 2018.

[9] S. Ray, Wen Chen, J. Bhadra, and M. A. Al Faruque. Extensibility in automotive security: Current practice and challenges. In *2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2017.

[10] D. Rotar and H. Popa Andreescu. Face recognition in automotive applications. In *2018 20th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, pages 355–359, September 2018.

[11] M. Scalas and G. Giacinto. Automotive cybersecurity: Foundations for next-generation vehicles. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, 2019.

[12] M. Singh and S. Kim. Security analysis of intelligent vehicles: Challenges and scope. In *2017 International SoC Design Conference (ISOCC)*, pages 13–14, Nov 2017.

[13] Q. Wang and S. Sawhney. Vecure: A practical security framework to protect the can bus of vehicles. In *2014 International Conference on the Internet of Things (IOT)*, pages 13–18, Oct 2014.

[14] Q. Zeng, B. Jiang, and Q. Duan. Integrated evaluation of hardware and software interfaces for automotive human–machine interaction. *IET Cyber-Physical Systems: Theory Applications*, 4(3):214–220, 2019.