INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING AND TECHNOLOGY (IRJET) E-ISSN: 2395-0056
VOLUME: 07, SPECIAL ISSUE | JUNE 2020 WWW.IRJET.NET P-ISSN: 2395-0072
International Conference on Recent Trends in Science & Technology-2020 (ICRTST - 2020)
Organised by: ATME College of Engineering, Mysuru, INDIA

"A Study on Cyber Security for Sovereign Vehicles"

Impana Appaji[1], P Raviraj[2]

[1]Research Scholar, GSSSIETW, Mysuru and Asst.Prof., ATMECE, Mysuru, INDIA.
Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, INDIA.
[2]Professor, Dept. of CSE, GSSSIETW, Mysuru, INDIA.

ABSTRACT : As the technology develops, connectivity with the physical world is gradually increasing in the cyber world, and city infrastructure become smarter due to the increase of hyper-connection technology. Research on autonomous vehicle technology for freedom of movement has been exploding. Attackers are making various attempts to hack autonomous vehicles as it becomes new targets. In the past few years, various attacks on autonomous vehicles have been studied, and at the same time, research on the security aspects of securing autonomous vehicles has been conducted continuously. Attacks on autonomous vehicles can cause direct physical harm to a person. Autonomous vehicles are important not only for communication systems inside cars, but also for automotive and external communication. However, few studies have systematically organized studies of attacks and defenses against autonomous vehicles. The research on the existing autonomous vehicle attacks showed that the direction of the autonomous vehicle attack is mainly the attack on the communication method of communicating with autonomous vehicles such as V2X from the elements of the existing simple autonomous vehicles. As communication technologies such as 5G evolve, future attacks on autonomous vehicles will continue to be attacked on 5G-related communications.

KEYWORDS

Autonomous vehicles, Self-Driving cars, Automatic control system, Autonomous driving systems components, V2X communications, Cyber risk

I. INTRODUCTION

In the history of mankind, a round object made of wood is found in the Mesopotamian ruins around 3500 B.C. In 1769, when the French engineer Nicolas Joseph Cugnot invented the world's first steam car, invented for the purpose of towing cannons, the history of cars began. Then 110 years later, in 1885, Karl Benz developed the world's first gasoline car, and in 1888, when John Boyd Dunlop invented pneumatic tires, the history of automobiles was drastically changed. Ford developed the mass production of automobiles from 1909 to 1919 in Highland Park , the beginning of the 20th century, leading to the birth of modern cars. With the development of consumer communication in the 21st century, smart automobiles have been born with the addition of mechanical internet, social services, and 5G communication network as well as the software capability.

Figure 1: The overview of attack surface for autonomous vehicles

Most of the existing researches have mainly focused on intrusion detection techniques to defend against attacks on the internal elements of autonomous vehicles. Due to the development of big data and communication technologies, techniques for detecting abnormalities using artificial intelligence and machine learning are gradually being developed. It is progressing toward research. Since autonomous vehicles will become a key element of the smart world and 5G era, it is very important to examine the history of attack and defense research on autonomous vehicles.

Three important elements of an autonomous vehicle can be classified into a control system for the vehicle itself, an autonomous driving system, and a communication between the vehicle and external elements. Here, we will look at automobile control systems, autonomous driving systems, and communication technologies between automobiles and the outside world.

II. AUTOMOTIVE CONTROL SYSTEMS

The automotive control system consists of an in-vehicle network that connects the main devices and devices. Key modules in the vehicle are Body Control Modules (BCM) and Power-train Control Modules (PCM). Body control modules include door control, seat control, power locks, airbag, air condition, and light control. Power-train Control Modules include Anti-lock Brake System (ABS), Engine Control Unit (ECU) and Transmission Control Unit (TCU). All such control systems are referred to as electronic control units (ECUs). ECU contains the Central Timing Module (CTM), Central Control Module (CCM), Brake Control Module (BCM), Transmission Control Module (TCM), Power-train Control Module (PCM), Electronic/Engine Control Module (ECM), Suspension Control Module (SCM), General Electronic Module (GEM), Body Control Module (BCM) and others. Generally, small and medium-sized vehicles include approximately 50 ECUs. At least 70 ECUs are included in the luxury car. Some cutting-edge vehicles have up to 80 ECUs with new functions. An in-vehicle network is that connects electronic control units and transfers data between ECUs.

Network	LIN	CAN	D2B	FlexRay	Ethernet	MOST	IDB	LVDS
Maximum date rate	19.2 Kb/s	1 Mb/s	11.2 Mb/s	20 Mb/s	100 Mb/s	150 Mb/s	400 Mb/s	655 Mb/s
Topology	Linear bus	Linear bus, Star, Ring	Ring	Linear bus, Star, or Hybrid	Linear bus, Star	Ring	Linear bus, Star, Ring	Point to Point
Cost	Low	Medium	High	High	Medium	High	High	High

Table 1: Inter-Vehicle wired interconnection technologies in autonomous driving

The in-vehicle network includes Local Interconnect Network (LIN), Controller Area Network (CAN), D2B, FlexRay, Ethernet, MOST, IDB and LVDS as shown in Table 2. Kim *et al.* describes characteristics, bus protocol and node structure for LIN, CAN, and FlexRay. The CAN bus serves as a key network for delivering data between the ECUs in the vehicle, such as a person's spine. Most of the currently known car hacking attacks are mainly attacks on CAN. The CANprotocol is a data communication ISO standard and is registered as ISO 11898. Bosch began developing CAN bus in 1983. Robert Bosch GmbH invented CAN bus protocol in 1986, and it is originally designed for automobiles. In 1988, the BMW 8 series was the first production vehicle to adopt a CAN-based communication system. The CAN is using as a core network for body systems, engine management, and transmission.

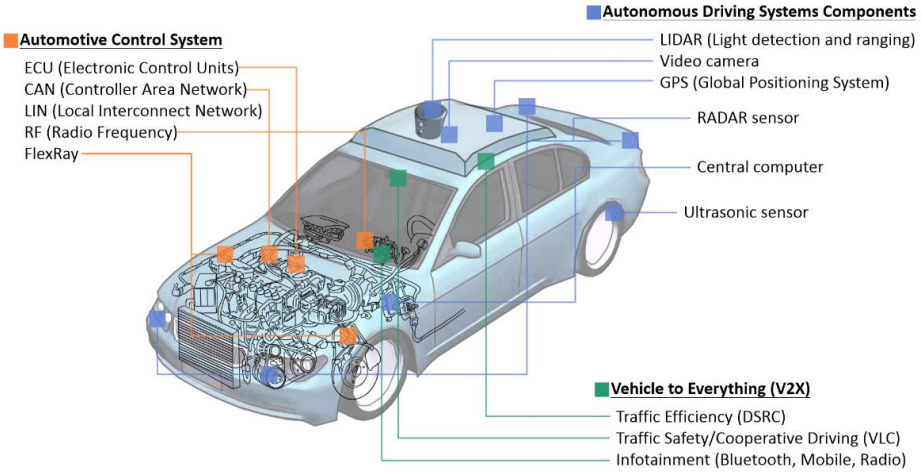

Figure 2: Types of Attacks for autonomous vehicles

III. AUTONOMOUS DRIVING SYSTEMS COMPONENTS

The most important key components in autonomous vehicles are cameras, sensors and GPS. Slightly more detailed are GPS, stereo camera, Radio Detection and Range (RADAR), Light Detection and Ranging (LIDAR) sensor and humanmachine interface. In autonomous vehicles, GPS (Global Positioning System) is a very important factor that informs the car of its current location and the location of other cars. Autonomous vehicles have algorithms for driving. RADAR radiates electromagnetic waves periodically. Then, the electromagnetic waves reflected from the object are read to confirm the distance and height between the objects. LIDAR (laser imaging detection and ranging or optical detection and ranging) is a technique that uses light to sense objects and measure distances. RADAR uses electromagnetic waves to send it around and then uses it to detect obstacles, LIDAR sends the light around and uses it to come back to make the image of the surrounding situation and send it to the computer. According to the economist, the self-driving car is composed of GPS, RADAR, LIDAR, video camera, central computer and ultrasonic sensor as seen from Table 3.

IV. V2X COMMUNICATIONS TECHNOLOGIES

The network communication between the car and the external terminal is called the Vehicle to Everything (V2X). MacHardy et al. surveyed regulation, research, and remaining challenges for the V2X access technologies. The V2X contain aVehicle-to-Vehicle (V2V) ,Vehicle-to Infrastructure (V2I) communications, and a Vehicle-to-Network communication (V2N) as shown in

Fig. 2. The VANET, Vehicle Ad-hoc NETworks area, is an area of great interest for researchers of a V2X communications. VANET uses Dedicated Short-Range Communications (DSRC) and is based on the IEEE 802.11p standard. IEEE 802.11p is a standard for wireless communications and further reinforces the IEEE 1609 family of standards. In the Wireless Access in a Vehicular Environment (WAVE), the IEEE 1609 standard defines various elements. It defines the standards, architecture, and interfaces for secureVehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications.

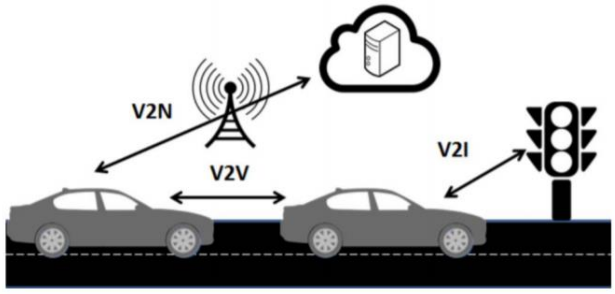

Figure 3: A simple illustration of V2X communications

V. SECURITY GUIDELINES & INTERNATIONAL STANDARDS

Many security guidelines have been made regarding automobile security, and international standards are actively discussing automobile security standards. The National Institute of Standards and Technology (NIST) cyber security risk management framework regarding modern vehicles for vehicle security guideline is published by the National Highway Traffic Safety Administration (NHTSA) of U.S. Department of Transportation in 2014. This technical report describes the vehicle sector cyber security issues and activities. In addition, this report also suggests the application method of the NIST risk management framework to the vehicle sector. NHTSA release new cyber security best practice for modern vehicles in 2016. In this report, NHTSA addresses the automotive industry cyber security guidance.

The Automotive industry cyber security guidance consists of seven detailed tables of contents. Each detailed contents are

(1) The vehicle development process with explicit cyber security considerations,

(2) Leadership priority on Product cyber security,

(3) Self-auditing,

(4) vulnerability/exploit/incident response process,

(5) Information sharing,

(6) Vulnerability reporting/ disclosure policy and

(7) Fundamental vehicle cyber security protections.

VI. INTRUSION DETECTION FOR AUTONOMOUS DEFENSE

In 2012, Ling and Feng proposed a malicious detection algorithm for CAN bus. The proposed algorithm detects the attack using frequency calculated by CAN ID of the message. A list of CAN ID used in the bus is obtained in advance so that an attack can be detected early by observing the appearance of an CAN ID that has not been used before. The algorithm was implemented in CANoe simulator by using CAPL. In 2013, Studnia et al. introduced a brief overview of possible attacks that are already known and experimented against vehicles and some protection mechanism. The key idea is to deploy a gateway and used as an IDS. However, applying a gateway to the CANbus can cause problems due to unintended performance degradation. The defense mechanism proposed in this paper is not implemented in practice. In 2015, Maglaras presented an architectural concept of DIDS designed for VANET. The modules of proposed DIDS are installed in the RSU and in the vehicle, respectively. The authors mainly focus on performance issues that can occur during implementation rather than attack detection methods.

In 2016, Berlin et al. introduced a security management system that they were developing. The use cases include a special event of attack and stolen credentials. Song et al. proposed a lightweight algorithm to detect injection attack on in-vehicle network based on time intervals of CAN messages. First, the authors measured and calculated the time period of the message by CAN ID on a normal status. The results are used as thresholds to identify intrusion. The work has a limitation that detection algorithm should have pre-knowledge about interval by *Arbitration_ID* for each vehicle. Remarkably, the dataset from a commercial vehicle is uploaded on their website so other researchers can reproduce the authors work.

VII. RESULTS ON SURVEY

In the security aside for autonomous driving vehicles, we divided into defense literature as the following categories. Security Architectures, Intrusion Detection, Anomaly Detection, and Review and Survey papers as shown below.

Defense Category	Authors	Year	Approach and Limitation
Review/Survey	Kleberger	2011	Surveys for network, architectural, IDS, honeypots, threats and attacks.
	Studnia	2013	Communication protocols in embedded automotive networks
	Engoulou	2014	VANET security surveys
	Schoitsch	2015	Cyber -security co-engineering and standardization
	Coppola and Morisio	2016	Connected car: Tech, Issues, future trends
	Eiza and Ni	2017	Latest vehicle cyber security threats and defending mechanisms
	Parkinson	2017	Vulnerabilities identified and mitigation techniques
	Tomlinson	2018	CAN IDS Survey
	Lu	2018	A survey on trust management models in VANET
	Abu Talib	2018	Literature review on Internet-of-Vehicles communication
	Mawonde	2018	A Survey on vehicle security systems

ACKNOWLEDGEMENT

This paper and the research behind it would not have been possible without the exceptional support of my supervisor, Dr. P Raviraj, Professor, GSSSIETW, Mysuru. His enthusiasm, knowledge and exacting attention to detail have been an inspiration and kept my work on track. I am also grateful for the insightful comments offered by Dr. S. Meenakshi Sundaram, Head of

Research centre, Dept. of CSE, GSSSIETW, Mysuru. We are also thankful to the Visvesvaraya Technological University, Belagavi, Karnataka, India for the support and guidance of doing this research work. I would like to express my special thanks of gratitude to our principal Dr. L Basavaraju for his continuous support. Thank you.

CONCLUSION

The history of automobiles has been long, but it has not been so long since self driving technology has come to our reality. The autonomous driving technology has been discussed since 1900, and various technologies such as ECU and V2X have been continuously researched and developed. Recently, international standardization activities for autonomous vehicles have been actively discussed since 2015. Research on automobile attacks has been attempted on a variety of attack surfaces, beginning with the study of Hoppe et al. and Nilsson 2008, to the recent study of Cheah in 2018. The first car attack was primarily the attack on the interior of the car such as ECU and CAN. In recent years, as autonomous driving technology has developed, attacks on external communication such as V2X have been studied extensively. As the attack technology for autonomous vehicles continues to emerge, defensive methods are also being studied. The security research on autonomous vehicles has proposed the method of specification based detection in the paper of UE Larson in 2008 and has been continuously studied since then to propose the method of GAN based intrusion detection system in the paper of Seo in 2018 recently. Autonomous vehicle security model has been studied from the model using intrusion detection system, which is a traditional security model, to the function of security model combining artificial intelligence, machine learning and deep learning technology such as BN and DBN.

REFERENCES

[1] Abu Talib, M., Abbas, S., Nasir, Q., Mowakeh, M.F., 2018. Systematic literature review on internet-of-vehicles communication security. International Journal of Distributed Sensor Networks 14, 1550147718815054.

[2] Administration, N.H.T.S., et al., 2016. Cybersecurity best practices for modern vehicles. Report No. DOT HS 812, 333.

[3] Al-Kahtani, M.S., 2012. Survey on security attacks in vehicular adhoc networks (vanets), in: 2012 6th International Conference on SignalProcessing and Communication Systems, IEEE. pp. 19.

[4] Al-Khateeb, H., Epiphaniou, G., Reviczky, A., Karadimas, P., Heidari,H., 2018. Proactive threat detection for connected cars usingrecursive bayesian estimation. IEEE Sensors Journal 18, 4822 4831.

[5] Amoozadeh, M., Raghuramu, A., Chuah, C.N., Ghosal, D., Zhang, H.M., Rowe, J., Levitt, K., 2015. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Communications Magazine 53, 126–132.

[6] Bacchus, M., Coronado, A., Gutierrez, M.A., 2017. The insights into car hacking.

[7] Bariah, L., Shehada, D., Salahat, E., Yeun, C.Y., 2015. Recent ad-vances in vanet security: a survey, in: 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), IEEE. pp. 1–7.

[8] Bayer, S., Enderle, T., Oka, D.K., Wolf, M., 2015. Security crash test-practical security evaluations of automotive onboard it components. Automotive-Safety & Security 2014 .

[9] Bécsi, T., Aradi, S., Gáspár, P., 2015. Security issues and vulnerabilities in connected car systems, in: Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2015 International Conference on, IEEE. pp. 477–482.

[10] Berlin, O., Held, A., Matousek, M., Kargl, F., 2016. Poster: Anomaly-based misbehaviour detection in connected car backends, in: 2016 IEEE Vehicular Networking Conference (VNC), IEEE. pp. 1–2.

[11] Boudguiga, A., Klaudel,W., Boulanger, A., Chiron, P., 2016. A simple intrusion detection method for controller area network, in: 2016 IEEE International Conference on Communications (ICC), IEEE. pp. 1–7.

[12] Briciu, C.V., Filip, I., 2014. The challenge of safety and security in automotive systems, in: 2014 IEEE 9th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI), IEEE. pp. 177–181.

[13] Brooks, R.R., Sander, S., Deng, J., Taiber, J., 2009. Automobile security concerns. IEEE Vehicular Technology Magazine 4, 52–64.

[14] Burakova, Y., Hass, B., Millar, L., Weimerskirch, A., 2016. Truck hacking: An experimental analysis of the ^SAE` j1939 standard, in: 10th ^USENIX` Workshop on Offensive Technologies (^WOOT` 16).

[15] Cheah, M., Shaikh, S.A., Bryans, J., Nguyen, H.N., 2016. Combining third party components securely in automotive systems, in: IFIP International Conference on Information Security Theory and Practice, Springer. pp. 262–269.

[16] Cheah, M., Shaikh, S.A., Bryans, J., Wooderson, P., 2018. Building an automotive security assurance case using systematic security evaluations. Computers & Security 77, 360–379.

[17] Cheah, M., Shaikh, S.A., Haas, O., Ruddle, A., 2017. Towards a systematic security evaluation of the automotive bluetooth interface. Vehicular Communications 9, 8–18.

[18] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., et al., 2011. Comprehensive experimental analyses of automotive attack surfaces., in: USENIX Security Symposium, San Francisco.

[19] Cho, K.T., Shin, K.G., 2016. Fingerprinting electronic control units for vehicle intrusion detection, in: 25th ^USENIX` Security Symposium (^USENIX` Security 16), pp. 911–927.

[20] Choi,W., Joo, K., Jo, H.J., Park, M.C., Lee, D.H., 2018. Voltageids: Low-level communication characteristics for automotive intrusion detection system. IEEE Transactions on Information Forensics and Security 13, 2114–2129. doi:10.1109/TIFS.2018.2812149.