A study of Total Security Platform to Protect Autonomous Car and Intelligent Traffic System

Keon Yun and Myung Cheol Lim*

Penta security, Republic of Korea

Email: kyun@pentasecurity.com, mclim@pentasecurity.com*

Received: October 02, 2023; Revised: November 25, 2023; Accepted: December 15, 2023;
Published: December 30, 2023

Abstract

Advancements in ultra-high-speed, low-latency 5G communication at 28GHz, pivotal for enabling autonomous driving, are currently under active development, heralding the imminent integration of this technology into our daily lives. The emergence of autonomous driving promises an array of services and enhanced comfort. However, the increasing proximity of autonomous driving to our societal fabric unveils a significant gap in security measures essential to shield self-driving cars and the interconnected intelligent transportation system from cyber threats. As autonomous vehicles transition from concept to service, the paramount importance of bolstering security measures becomes evident. Consequently, our focus centers on the development and research of security technologies aimed at robustly safeguarding against potential cyber attacks targeting the communication between infrastructure and vehicles.

Keywords: 5G security, autonomous vehicle, intelligent transportation system.

1 Introduction

An increasing demand for cooperative autonomous driving (C-ITS) arises to facilitate seamless autonomous vehicle operation and mitigate traffic congestion. This involves the systematic gathering, processing, and dissemination of transportation infrastructure-derived data to autonomous vehicles [1]. However, the integration of C-ITS services has extended cybersecurity vulnerabilities from traditional IT environments to roadways and vehicles due to their connectivity with external networks. To counteract these expanded cybersecurity threats in the transportation domain, considerable efforts are underway in the development of various C-ITS security technologies. The United Nations Conference on Automotive Standards (WP.29) has introduced "UN Regulation No. 155: Cybersecurity Regulation," mandating software updates for cybersecurity in connected cars, thereby establishing internationally binding standards for the automotive industry.

Commencing from July 2020, automakers are required to obtain certification for the Cyber Security Management System (CSMS) to attain Vehicle Type Approval (VTS) for new vehicles registered in UNECE member states. The ongoing standardization of ISO 21177 and ISO 24102, defining security technologies for ISO/SAE 21434 and ITS stations, signifies an imminent expansion of cybersecurity practices beyond vehicles to encompass the entire transportation infrastructure, including Roadside Units (RSU) for C-ITS security.

This evolution necessitates comprehensive research into security technologies bridging vehicles and infrastructure [2]. Hence, this study primarily focuses on leveraging machine learning techniques

to fortify communication security and detect anomalous behaviors within Vehicle-to-Everything (V2X) interactions. Figure 1 shows the architecture of security elements.

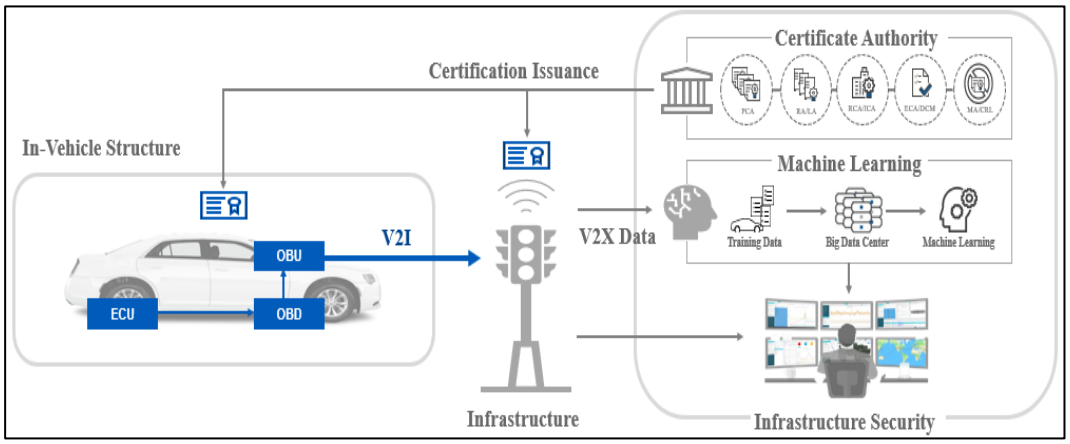

Figure 1. Security elements of the proposed architecture

In our paper, we emphasize two pivotal facets of security. Firstly, the V2X communication domain encompasses three distinct categories: inter-vehicle, intra-infrastructure, and infrastructure-to-transportation center communication. These channels exchange vehicle characteristic data, underscoring the criticality of ensuring integrity and availability. Our proposed solution addresses this by innovating a certificate issuance technology facilitating secure authentication among these entities. Specifically, we advocate the use of IEEE 1609.2 certificates for vehicle-to-infrastructure authentication and X.509 certificates for infrastructure-to-infrastructure authentication, aligning with established standards while developing compliant certificate technology.

Secondly, our research focuses on advancing V2X data collection technology derived from vehicles, specifically designed to identify anomalous behavior in autonomous vehicles. The identification of aberrant vehicle behavior necessitates a substantial corpus of data for comprehensive learning. To meet this demand, we present methodologies geared towards efficient data acquisition from vehicles. Categorically, V2X data is segmented into two classes: internal vehicle-generated data and external environmental data. To address these disparate data sources, we engineer prototypes of an On-Board Diagnostics (OBD) system for internal data collection and an On-Board Unit (OBU) collector for external data acquisition. These prototypes are designed to enhance the comprehensive collection of V2X data from diverse sources. The acquired dataset serves as the foundation for machine learning applications. Primarily comprising vehicle speed, location coordinates, and heading parameters, this dataset encapsulates the real-time status of vehicles. Anomalous behavior detection is achieved by scrutinizing diverse scenarios, including abrupt fluctuations in speed and heading, incongruous location data, and manipulation of vehicle information. Upon detecting irregular behavior within the infrastructure, notifications are relayed to the Roadside Unit (RSU) to ascertain the abnormal status of neighboring vehicles. The RSU incorporates the Enhanced Data rates for GSM Evolution (EDGE) system. This system facilitates the establishment of a cooperative network amongst RSUs, effectively decentralizing various tasks traditionally reliant on cloud-based environments [3]. By distributing these tasks across multiple entities, the EDGE system enhances operational efficiency and promotes a more robust and interconnected RSU network. Furthermore, this information is transmitted to the central control center, enabling comprehensive assessment of abnormal vehicle conditions on the road network.

2 Security Techniques for Ensuring Automotive Security

This section elucidates diverse research methodologies imperative for ensuring the security of vehicle networks, particularly in the context of self-driving automobiles. Specifically, network security, boot security, and remote security represent critical security paradigms essential for the deployment of autonomous vehicles in operational service.

2.1 Zero Trust Network Access (ZTNA)

ZTNA (Zero Trust Network Access) [4] stands as a pivotal technology safeguarding networks. It revolutionizes remote access security by granting entry to an organization's applications, data, and services based on precise access control policies, in stark contrast to traditional VPN (Virtual Private Network) approaches that provide access to entire networks. ZTNA excels by confining access solely to specific services or applications, adhering to these core principles.

- Network and Application Isolation: ZTNA meticulously segregates network and application spheres, mitigating risks associated with compromised devices. It sanctions access solely to authenticated users for designated applications, curtailing potential threats.

- Outbound-Only Connections: By permitting outbound connections exclusively, ZTNA shields network and application infrastructure from unauthorized users. This strategy avoids IP exposure, fortifying network security significantly.

- 1:1 Application Access: Authenticated users gain access limited to user-specific applications, circumventing excessive access and potential infiltration by malware or other security threats.

Software-Defined Perimeter (SDP), a prominent component of ZTNA, has garnered substantial attention lately. SDP, a security technology centered around identity-based resource access control, delineates a virtual perimeter around network resources. By establishing software-defined boundaries, irrespective of physical location, it safeguards organizational infrastructure from external intrusions. SDP architecture substantially diminishes the attack surface, fortifying both internal and external network security. SDP, composed primarily of a controller and host components, orchestrates communication between SDP hosts. These hosts, divided into Initiating SDP Hosts (IH) and Accepting SDP Hosts (AH), enable controlled communications. IH collaborates with the controller to ascertain permissible hosts for connection, while AH exclusively accepts communications sanctioned by the controller. Some SDP architectures deploy gateways as hosts facilitating connections between devices or users.

The diversity within SDP encompasses various models, each offering distinct advantages. For instance, the client-gateway model utilizes an AH as a gateway between servers and IH, ensuring server protection and securing client-gateway connections across varied network configurations. Tailoring SDP models to suit specific organizational environments enhances overall security, providing adaptable protection by applying diverse models.

2.2 Secure Boot

Secure Boot represents a pivotal technology ensuring the validation of encrypted signatures for both the Linux kernel and system image. Prior to initiating system control, it permits the execution exclusively of authenticated files, thereby fortifying system security. Following the system's boot sequence, the kernel and system files undergo scrutiny during command file execution. In the event of compromised integrity, restoration to the original image becomes feasible.

- During boot-up, the entire system undergoes scrutiny to validate the integrity of the autonomous driving system.

- The system state, ascertained through parameters like system image and hash values, is recorded for future reference, enabling comparison with the current system state to detect potential tampering or alterations.

- Verification of integrity encompasses critical elements such as bootloader, OS image, kernel image, and key settings values.

Secure Boot implementation primarily necessitates robust measures for bootloader integrity verification, OS integrity validation, and application integrity assurance. These functions collectively contribute to fortifying system security and maintaining the sanctity of the autonomous driving environment.

2.3 Remote Attestation

In the realm of Trusted Computing, Remote Attestation technology emerges as a cornerstone function. It facilitates platforms equipped with a Trusted Platform Module (TPM) to remotely validate the trustworthiness of the interconnected platform. The TPM safeguards a distinctive key, the Endorsement Key (EK), pivotal for authentication. However, employing this key for authentication can potentially compromise extended functionality and anonymity support. To address this concern, an Attestation Identity Key (AIK) is generated and utilized to preserve the TPM's uniqueness and facilitate authentication. Notably, a single TPM can accommodate multiple AIKs, allowing diverse authentication based on the authorizing entity.

EK(Endorsement Key)

- 2048-bit RSA key

- Exclusively authorized by TPM production, preventing the extrication of secret keys from the TPM.

- Access to both public and private keys is strictly regulated, accessible only under TPM protection.

- Generated externally using TPM_CreateEndorsementKeyPair command.

AIK(Attestation Ident Key)

- 2048-bit RSA key

- Infinitely generable within the TPM, requiring knowledge of the 160-bit authentication value for utilization.

- Employed for signing values generated within the TPM, such as PCR (Platform Configuration Register).

Through the amalgamation of EK and AIK, the TPM verifies the secure state of communicating entities on connected platforms. When a platform user solicits a service, a verification process is initiated by dispatching a random number value and a proof request message. The platform securely guards the received random number value, the approximate measurement log denoting the current state, and the PCR value, transmitting them to the verifier. This transmission is accomplished by the

signer directing information to the verifier-operated AIK. Upon reception of the PCR value, the verifier cross-validates the dispatched random number value and authenticates, via privacy CA, the AIK as a key from a trusted platform. Additionally, confirmation of the AIK-signed PCR values' derivation and alignment with the PCR value's measurement logs serves to validate the platform's credibility.

3 Research result

In the course of this research, we developed two distinct design prototypes (Figure 2): an On-Board Diagnostics (OBD) system, tailored for internal vehicle data acquisition, and an On-Board Unit (OBU) system, specifically designed for external vehicular data collection. The OBU system is engineered to utilize data by amassing comparative datasets in accordance with the SAE J2735 standards, aiming for optimal recording of the collected data. A pivotal focus of our data analysis is centered on the Basic Safety Message (BSM) dataset, which serves as the primary source for identifying and understanding abnormal vehicular behaviors.

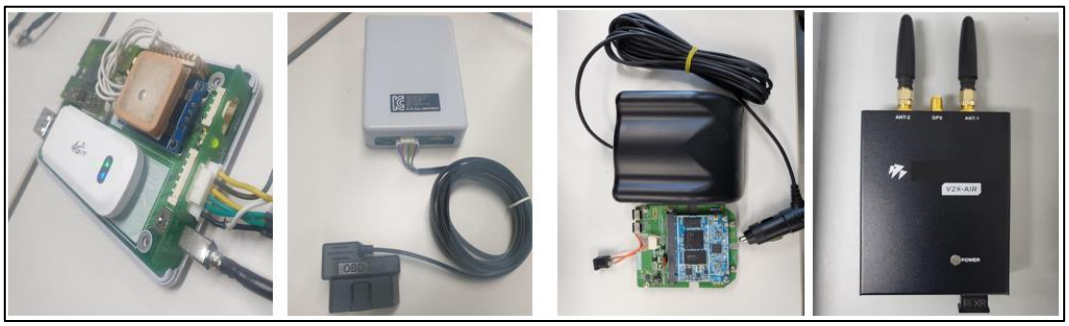

Figure 2. OBD/OBU data collector

In this study, we have meticulously developed specialized scenarios to analyze anomalous behavior and have subsequently collected the requisite data for machine learning from our meticulously designed prototypes. Figure 3 shows the result of anomalous behavior analysis. The data employed for this learning process predominantly comprises the Basic Safety Message (BSM) data, as delineated in the SAE J2735 standards [5]. Within this framework, the learning algorithm particularly focuses on the Heading and Angle values from the BSM as key features. Furthermore, the study involved the training and subsequent performance evaluation of four distinct machine learning models: Oneclass-SVM, K-Means, HDBSCAN, and Minisom. The comparative analysis of these models provides valuable insights into their effectiveness in the context of vehicular data analysis.

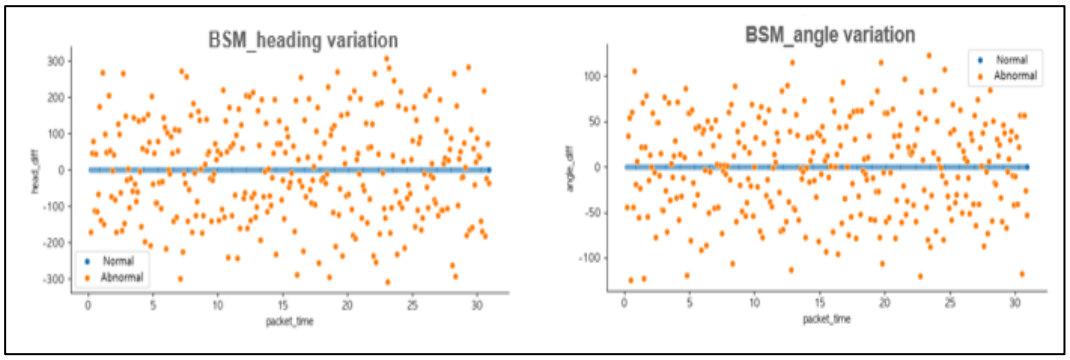

Figure 3. Anomalous behavior analysis result

4 Conclusion

As autonomous vehicles increasingly integrate into our daily lives, the imperative for comprehensive security measures to safeguard against potential cyber threats becomes paramount. The primary objective of such security protocols is to ensure user safety, thereby fostering stability and public trust in the expanding realm of autonomous vehicular services. This paper has presented an extensive exploration of automotive operation security, including inter-vehicle communication safeguards and solution strategies. Significantly, the study recognizes key milestones in the evolution of external security perimeters within the domain of autonomous driving. This includes advancements in secure boot technology and remote authentication methods. Furthermore, the paper delves into the application of machine learning techniques, emphasizing their potential in enhancing vehicular functionality and safety standards. Looking ahead, as the 5G network continues to proliferate, its integration into vehicular communication systems is anticipated. This advancement is likely to usher in a new era of vehicular connectivity, necessitating the parallel evolution of security techniques. Our research aims to contribute to this dynamic field, endeavoring to develop robust security strategies that align with the advancements in 5G technology and autonomous vehicle development.

Acknowledgement

This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2020-0-00304, Development of Total Security Platform To Protect Autonomous Car and Intelligent Traffic System Under 5G Environment)

References

[1] Husain, S.S., et al., Ultra-high reliable 5G V2X communications. IEEE Communications Standards Magazine, 2019. 3(2): p. 46-52.
[2] Qian, Y., F. Ye, and H.-H. Chen, Security in V2X communications. 2022.
[3] Kong, X., et al., Mobile edge cooperation optimization for wearable internet of things: a network representation-based framework. IEEE Transactions on Industrial Informatics, 2020. 17(7): p. 5050-5058.
[4] Stafford, V., Zero trust architecture. NIST special publication, 2020. 800: p. 207.
[5] SAE International. J2735_202309: V2X Communications Message Set Dictionary, SAE International, 2023.