Vehicle Communication and Infrastructure Security: Initial Thoughts

Mustafa Saed, Muhammad Rizwan
Hyundai-Kia America Technical Center, Inc.
Superior Township, MI 48198, USA
{msaed, mrizwan}@hatci.com

ABSTRACT— Demand on providing secure communication among vehicles and Vehicle to Infrastructure networks is constantly growing. Electronics Control Units (ECUs) in vehicles need to authenticate each other and the infrastructure to verify they are whom they claim, and they also need to ensure the integrity of the shared safety critical information. Adversaries can masquerade as real subscribers in vehicle to infrastructure networks and broadcast harmful messages to destroy the system. The intent of this paper is to introduce thoughts on enforcing security at various levels in vehicle architecture to prevent hackers from accessing vehicle ECUs to install malicious software and granting unauthorized access to the vehicle systems.

Keywords— Vehicle Network, CAN Bus, Dispatcher, Wireless Communication, Security, Vulnerabilities

I. INTRODUCTION

Security is one of the most critical issues facing automotive companies developing wireless communication systems for everyday applications demanding interface between the customers and the vehicle. Because of the direct interaction between humans and vehicles, engineers need to provide and implement a secure system in the vehicle to let people take full advantage of the new applications and features in their vehicle. Vehicles that are equipped with Telematics system and internet access, such as BlueLink in Hyundai vehicles and OnStar in GM vehicles, are becoming more vulnerable to cyber-attacks. Providing secure systems in vehicles will deter unauthorized parties from accessing vehicles’ communication system and causing hazards in the road. Security concerns are becoming inevitable following the fast development in the technology of the vehicles, especially those equipped with remote access. In addition, allowing physical access to the vehicle’s CAN (Controller Area Network) bus with no consideration for security increases the desire to enhance and develop vehicle security system. With the traditional safety telematics services, stolen vehicle tracking, and diagnostics aimed at the physical protection of vehicles, drivers and passengers are becoming main stakeholder. Awareness is growing with respect to the threat of cyber-attacks and their impact on the physical integrity of persons, especially with Vehicle-to-Vehicle communication and autonomous vehicles. Current vehicle architectures are at risk of wireless security break-ins, but future vehicle architectures and systems will only increase the risk because telematics systems have embedded cell phones and wireless protocols containing private information, such as financial records, pin numbers, credit card information, and birth dates. This risk needs to be mitigated. Protecting our customers’ private information and the vehicle systems from hackers, unauthorized people, and the infectious viruses should have the highest priority. Viruses will have a direct impact on the trustworthiness and quality from the viewpoint of the consumer as well as the vehicle’s safety dynamics, such as the multiple ECU’s and its associated systems depending on accurate and uncorrupted information.

To develop and enhance vehicle security, and provide sophisticated safety system for vehicles, two techniques are foreseeable, inter-vehicle Communication Security to provide secure communication/protocol between the vehicle and the infrastructure via wireless network, and intra-vehicle Communication Security to develop and enhance the security communication/protocol between the telematics unit and the ECUs connected via CAN Bus.

Securing the Inter-Vehicle Communication demands the application of cryptography and data security to the packet data session (TCP/IP) and the voice service. A number of attempts have focused on providing two-way communication security between the vehicle and the infrastructure including the vehicle-to-vehicle (V2V) communication as well. However, the security of the V2V communication still needs more development and enhancement.

Duraisamy et al [1] introduced an idea to implement new hardware, which uses Elliptic Curve Cryptography and Digital Signature Algorithm (ECDSA). Their approach allows two parties, a remote agent and a network embedded system, to establish a 128-bit symmetric key, and encrypt all transmitted data via the Advanced Encryption Standard (AES) algorithm.

The Identity-based Batch-Verification (IBV) technique was proposed by Zhang et al [2]. It uses a private key for pseudo identities to avoid the use of certificates. Each received signature should be verified within 300ms intervals based on the Dynamic Short Range Communication (DSRC) protocol used.

Qian et al [3] invested the features of the Medium Access Control (MAC) layer protocol to achieve both Quality of Service (QoS) and security requirement for vehicular networks safety application. Designing an efficient MAC protocol to achieve safety through vehicular networks is essential.
The above attempts/techniques illustrate the critical security concerns arising from vehicle to infrastructure communication. Because the communication between the vehicle and infrastructure is implemented by using wireless technology, the possibility of vehicle cyber-attack is high. This risk will increase if the security is not considered in the inter-vehicle communication infrastructure. To elucidate this issue and prevent any serious threats to the system, a need for implementing a robust security technique in the inter-vehicle communication and providing a great inter-vehicle communication service to the customers is mandatory [4].

The other security technique that needs consideration in order to provide a robust security system to the vehicle communication, is securing Intra-Vehicle communication. The Intra-Vehicle Communication security compels protecting transmitted data between the vehicle’s ECU’s through the Controller Area Network (CAN) Bus, which is an open and unsecure automotive protocol. In the past, there was no way for accessing the vehicle remotely. The physical access only allowed getting to the vehicle CAN bus via the On-Board Diagnostic port (OBD). Hence, there were no security concerns related to accessing the vehicle CAN bus and tempering with the vehicle’s system. On the other hand, after the enormous changes and development in the wireless technology, the vehicles are impacted by this technology through housing the Telematics unit and allowing it to communicate with the rest of the ECUs in the vehicle via the CAN bus. The CAN bus increases the likelihood for accessing the vehicle CAN bus remotely, which in turn increases the risk of hacking the vehicle and affecting the drivers and vehicles’ occupants’ safety [5].

This paper proposes initial thoughts for performing remote control vehicle operation with two security mechanisms utilizing the Inter and Intra Vehicle Communication. The rest of the paper is organized as follows: Section 2 focuses on automotive multiplexing methods and CAN protocols. The overview on Next Generation Telematics Pattern (NGTP) is presented in section 3. Section 4 discusses security thoughts for vehicle communication and infrastructure. This is followed by discussion in section 5. Finally, section 6 concludes the paper.

II. MULITPLEXING METHODS AND CAN PROTOCOLS

A. Multiplexing Methods

Adopting multiplexing methods in automotive technology becomes the greatest achievement in the potential to make vehicles more efficient by reducing the weight in the power distribution system, and increasing the number of the electronic control units. Multiplexing methods are used to connect many ECUs via the CAN bus in a single or dual wire and allows the two-way communication between each other. There are two primary methods used in Multiplexing: time division and frequency division. The time division method inserts a sample of each channel onto the data stream and the channels are selected for a short period of time. This use is the most accurate form of time sharing amongst various channels and is most prevalent method in the automotive industry. The second method, frequency division, uses a different technique which shares the process amongst various channels where information data can be designated with a carrier frequency through each channel to modulate the wave signals.

The Society of Automotive Engineers (SAE) divided the automotive communication sector into three classes. According to Paret et al [6], Class A can support 100 nodes and is categorized to handle data speeds (baud rate) up to 1 kilobit per second (kbps). However, the lag time, which is the time delta between a transmission request and transmission initiation, is 50 ms. Class A baud rate is used in tail light, turn signals, driver convenience features, and entertainment systems. Class B can support 50 nodes and is categorized to support data speeds upwards of 100 Kb/s. For real time events that require urgent speed with high accuracy values, class C is needed. Its data rate is in upwards of 1 Mb/s. Class C baud rate is used mainly in powertrain systems. Class C does not accommodate new systems such as Collision Avoidance System, Global Position System (GPS), and many other related systems.

Network nodes are transmitting and receiving signals via many types of communication, known as protocols. These protocols are created by a set of rules for coding, address structure, transmission sequence, and error detection and handling. These protocols are also referred to as the transmission medium, transmission speed, and electrical signal requirements depending on whether copper wires or optical fiber is used. When associated with automotive networking, protocols cover a majority of functions assigned to the different layers of the Open System Interconnection (OSI) model.

B. CAN Protocols

The communication between the ECUs in the vehicle CAN bus needs relies on a communication protocol called the Controller Area Network (CAN) protocol. A CAN controller acts as mediator to control the communication between the ECUs in the CAN bus. In CAN, disputes between messages are determined on a bit-by-bit basis in a non-destructive arbitration resulting in the highest priority message gaining access to the bus. There are 2,032 different messages supported by CAN protocol with up to 8 bytes of data. Each CAN message data acts differently from other serial communication protocols. The CAN message does not contain information relating to the destination address. The message contains an identifier, which indicates the type of information available. This feature allows convenient addition or deletion of the intelligent nodes in an automotive system. Furthermore, each node decides whether to read or ignore a CAN message [6].
III. Next Generation Telematics Pattern (NGTP)

NGTP is a new approach for delivering over-the-air services to in-vehicle devices and handsets alike, with the focus on open interfaces across the entire service delivery chain [7]. There are two versions of NTGP. NTGP version 1 permits the supply of new services faster based on the Telematics technology advances. In addition, varying customer needs can be addressed more quickly by substituting old services with new ones without the stress of introducing technical modifications within the vehicle. NTGP version 2 supports openness and flexibility by splitting the parts of the telematics delivery chain, and launching a ‘dispatcher’ to offer a single interface between the vehicle’s telematics unit and the telematics of the service provider. The open interface generated by NGTP also enables the OEMs (Original Equipment Manufacturer) to constantly introduce new services to both legacy vehicles and new models over the whole vehicle lifecycle.

NGTP’s developers has established six objectives dealing with furnishing a technology-neutral pattern and coherent user interface for telematics services, lowering obstacles to collaboration, implementation of new technologies, sustaining legacy systems for connectivity, encouraging innovation, and growing the value for vehicle manufacturers, service providers, content providers, and drivers.

NGTP will enable vehicle manufacturers to use the best offerings from a variety of partners while maintaining a consistent driver experience. The new pattern will also allow service providers (SP) and content providers to sell the same services to multiple vehicle manufacturers. Moreover, NGTP will support legacy systems, allowing older and newer vehicles alike to access new telematics offerings.

In order to foster collaboration and innovation, the specifications that constitute NGTP will be made public under a Creative Commons License. The NGTP group will work with the telematics providers to communicate the specifications, support testing and potential adoption of NGTP.

The NGTP architecture is depicted in Fig. 1. The key component is a technology-neutral intermediary called the Dispatcher (DSPT), which connects the vehicle’s Telematics Unit (TU) to the Service Handler (SH) and Service Integrator (SI).

The communication between the vehicle and the call center or the customer is achieved via multiple interfaces. The Service Integrator unit (SI) is responsible for the communication between the Call Center (CC) unit, Public Safety Access Point (PSAP) unit for 911 calls, Content Provider (CP) unit, and other services. The communication between SI, Customer Data Provider (CDP) unit, and Dispatcher is taken care of by the Service Handler (SH). The Dispatcher (DSPT) is in charge of the communication between the SH, Provisioning Data Provider (PDP), and the vehicle. Further details can be found in [7]. The following example should illustrate this organization.

Fig. 1. NGTP version 2 architecture [7]

Assume that the customer is trying to lock his/her vehicle using a mobile application or the web portal. The following steps will take place in this scenario:

a. Customer logs in with his/her account using mobile app/web portal.
b. Customer sends request to lock the vehicle’s door. This Short Message Service (SMS) is encrypted by the wireless carrier provider, such as Verizon Wireless.
c. The SI will receive the request and forward it to SH after verifying the customer information with the Content Provider (CP).
d. The SH forwards the request to Dispatcher after identifying the customer’s subscription.
e. The Dispatcher will decrypt the SMS message to direct the request to the right vehicle after validating the VIN# and Mobile Dialup Number (MDN).
f. The vehicle will receive the request from the Telematics Units and send it to the Body Control Module (BCM) to execute the request.
IV. SECURITY IN VEHICLE COMMUNICATION AND INFRASTRUCTURE

To achieve the highest possible security level, a security approach is suggested. As shown in Fig. 2, this approach enforces security within the Telematics Module Unit (TMU) and the Body Control Module (BCM). The reason behind using two-level security is to have two defense lines. If the dispatcher is hacked (first-level), the hacker needs to attack the second level of security to gain control of the vehicle’s remote service. This paper will only deal with the security between the dispatcher and the vehicle and not the end to end security (not all the units of Fig. 1).

Encrypted messages are received and decrypted by the TMU. Contained within the TMU protocol is either a seed or a regenerated key which will be exchanged/verified with the BCM at each ignition cycle. OEMs will decide whether to use the seed or regenerated key. There is also a mandatory shared symmetric key (K). The TMU sends an encrypted CAN signal to the BCM, which needs to decrypt and verify the integrity of the CAN signal. Upon successful completion, the CAN message will be sent to the respective ECU for the activation of a remote service.

A. First Level of Security (Dispatcher to Vehicle)

Customers will only send one SMS for their remote service request, such as remote door lock (RDL). This SMS will be delivered to the Dispatcher, who will transform it into two SMS messages using the specific Original Equipment Manufacturer (OEM) encryption policy. The automotive company will decide the encryption method used based on the cost and their ECUs specifications. This encryption is accomplished within the dispatcher and the TMU embedded in the vehicle. Therefore, other partners, such as the Cellular Provider and the TSP, will not have any knowledge of this encryption.

The key exchange will be completed between the dispatcher and the TMU so that encrypted and decrypted communication will only occur between the dispatcher and TMU. SMS1 and SMS2 will be sent at two different times. If SMS1 is sent at \( t_0 \), then SMS2 will be sent at \( t_0 + 30 \) sec with a tolerance of \( \pm 5 \) sec. When the TMU receives the encrypted SMS1 and then SMS2 from the dispatcher, it decrypts SMS1 and SMS2 to obtain the plaintexts R1 and R2 respectively.

B. Second Level of Security (Intra vehicle communication)

In order to prevent hackers from accessing the embedded vehicle computers, a second level of security in the vehicle communication between Module to Module (M2M) communications is proposed. Remote service request requires reaching the second-level security layer to complete the request.

The plaintext R1 and R2 will be employed when decrypting the remote request via the CAN bus. The seed and the shared key have been injected at the manufacturer site and will be used to perform the CAN encryption and authentication. The security approach is described as follows:

1) The TMU stores the new seed \( (S_{i+1}) \) and the one before it \( (S_i) \). The initial seed \( (S_0) \) will be injected in the vehicle (TMU and BCM) at the manufacturing time. At each ignition cycle, the BCM generates a new seed \( (S_{i+1}) \) and sends it to the TMU after encrypting it with symmetric key \( K \). Ultimately, TMU decrypts the received message using \( K \) to get \( S_{i+1} \).
2) The TMU combines \( S_{i+1}, R_1 \) and \( R_2 \), and encrypts \( Y = S_{i+1} || R_1 || R_2 \) using the symmetric key \( K \) to obtain \( M_1 = E_K(Y) \).
3) The TMU finds \( H(Y) \) and appends it to \( M_1 \) to obtain \( [H(Y) \ || \ M_1] \) before sending it to BCM.
4) The BCM decrypts the message received in (3) above to get \( Y \), verifies the hash value, and extracts \( S_{i+1} || R_1 || R_2 \). The \( S_i \) (BCM already has \( S_i \)) and \( S_{i+1} \) are then forwarded to the validation circuit in the BCM.
5) If the validation is successful, the BCM uses R1 and R2 to operate the customer’s remote request. Successful
notification will be sent to the telematics server and the customer.
6) If the validation process fails, the BCM will send a failure notification to the TMU to notify the telematics server and the customer of the failure.

V. DISCUSSION

The future of vehicle security is very critical. To improve security enhancement, many issues need to be taken into consideration. The first needed enhancement concentrates on embracing the Internet Protocol Version six (IPV6) in the vehicle communication, NASPInet, anonymization, behavioral economics/privacy, and cross-domain security involving IT. This approach will definitely enhance the vehicle security approach [8].

Another enhancement to security of the vehicle to infrastructure communication involves using the public key infrastructure (PKI) to address all the related requirements of the operation and devices of the vehicle communication [9]. This could be augmented by implementing and developing the vehicle security certificate lifetime and securing the trusted device profile [10].

An area that seems neglected is the customer's privacy. Customer privacy and the privacy of the information should be protected in all inter and intra vehicle communications [11]. Furthermore, critical data, such as business location, should also be protected [12].

Authentication in vehicle communication, such as the module to module communication, should be enriched. This could be achieved by implementing a robust security approach for the vehicle communication as a future priority [13]. Finally, reporting and updating any newly created vulnerability related to the vehicle communication by monitoring and tracking the communication and the data flow through the vehicle and keeping the customer’s privacy in consideration is a must [13].

VI. CONCLUSION

To enhance the security of telematics system, initial thoughts of In-Vehicle Communication and Infrastructure has been proposed. Future approaches, techniques, and methods needed to improve and enhance this security are discussed. The security features required for the vehicle have been addressed. The paper provided important and practical ideas to make the telematics system a reliable secure system so that customers can take full advantage of all its features. More work will be done as our thoughts are part of a work in progress. Vehicle communication security requirements related to Inter vehicle and Intra vehicle communications will be the focus of our work in progress. Implementing powerful cryptographic protocols will be our main focus to achieve a robust vehicle security system.

REFERENCES