Open Access

Journal of Artificial Intelligence & Robotics

Article type: Review Article

Cyber security challenges to future mobility of artificial intelligence

Jae Cheon Lee, PhD*

Professor, Center Future Mobility's Fusion Technology Innovation, Inha University, In cheon, S. Korea.

***Corresponding Author: Jae Cheon Lee**

Center Future Mobility's Fusion Technology Innovation Inha University, In cheon, S. Korea.

Email: ljc@inha.ac.kr

Received: Sep 04, 2024

Accepted: Oct 07, 2024

Published Online: Oct 14, 2024

Website: www.joaiar.org

Volume 1 [2024] Issue 1

Introduction

Today's Connected Autonomous Vehicles (CAVs) and collaborative robots are considered smart things because they are networked and have the ability to send and receive data over the network. Moreover, due to Software Defined Vehicle (SDV), which originated with Tesla cars, one of the biggest challenges in the future of mobility is ensuring the security and reliability of the vehicles against cyber attacks [1].

Furthermore, the adoption of Artificial Intelligence (AI) and Machine Learning (ML) as technologies for next-generation connected intelligent transportation systems (C-ITS) is increasingly exposing vehicles and V2X infrastructure to a wide range of sophisticated cyber attacks [2]. According to a report published in 2021, remote cyber attacks have been on the rise since 2010, accounting for 79% of all attacks from 2010 to 2020 and 77.8% of all attacks in 2020 alone [3]. Recently, machine learning-based approaches have gained popularity to provide In-Vehicle Network (IVN) security. AI-powered systems can detect and respond to cyber threats more efficiently, enabling organizations to proactively protect their sensitive information and networks. Machine learning algorithms attempt to try to mimic human learning systems by finding patterns in past incidents and making decisions based on them. The future direction of machine learning in an IVN was pointed to the area of defending malware in CAVs [4-5]. In this article, the hierarchy of automotive IVN systems and the cyber security threats of each layer in order to deeply defend automotive cyber security using AI technologies in the future are presented first. Then the cyber security countermeasures for each layer are introduced.

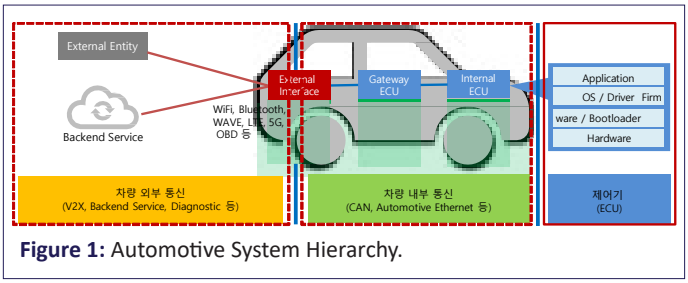

Figure 1: Automotive System Hierarchy.

Automotive system hierarchy and cybersecurity threats by layer

The general system hierarchy of a modern automobile can be broadly categorized as vehicle external communications, vehicle internal communications, and controller area. The external communication layer is where devices connected via external communication interfaces such as WIFI, LTE, OBD, etc. can be utilized as a means to attack the automotive system, and there are various threats such as information leakage, data forgery, and replay attacks of communication messages related to external automotive services. The internal communications layer can be utilized as a means to attack the vehicle's internal systems by connecting malicious devices to the vehicle's internal communications network, and there are a variety of threats, including eavesdropping on communications messages related to the vehicle's internal systems, replay attacks, forged message injection attacks, and denial of service attacks.

At the controller layer, electronic control devices can be attacked through internal and external communication channels connected to the controller or through the debug port on the controller, and threats include firmware tampering, malicious software installation, and memory dumping.

Citation: Cheon Lee J. Cyber security challenges to future mobility of artificial intelligence. J Artif Intell Robot. 2024; 1(1): 1007.

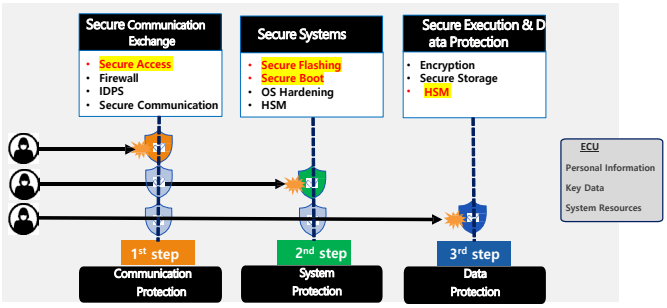

Figure 2: Cyber security technologies by layer.

Automotive interior security technology

To safeguard automotive internal systems from cyber security threats, consider applying a layered cyber security response technology based on a defense-in-depth strategy: As a protective measure for the communication layer, apply Secure Access technology, which authenticates that devices accessing internal systems from external communications are authorized devices, to establish a secure communication environment. As a secondary protection measure, we apply Secure Flashing technology, which verifies that software updates are manufacturer-approved, and Secure Boot technology, which verifies that software running at system boot is manufacturer-approved, to build a secure system environment. As a final third level of protection, applies hardware security module HSM technology to securely protect and store data and a secure application execution environment within the controller.

With these layered protection mechanisms, automotive interior systems can be considered a secure platform.

Access control

The concept of access control in Secure Access is the control of the flow of information between the subject, such as a user or device, and the object, such as a resource, system, or data, to which the subject is attempting to access, and refers to the process of identification, authentication, and determining whether the subject is a legitimate subject and has the appropriate authorization when attempting to access a particular resource. It is commonly utilized in information technology environments as an access control mechanism to secure communications between users, devices, applications, and networks.

As a security technique to control unauthorized access, authentication must be performed on the diagnostic device, and typical authentication methods include device authentication based on a simple username and password, one-time device authentication based on a mutually shared secret key with a challenge-response method, and certificate-based device authentication. Secure Access provides higher security than other authentication methods by performing certificate-based device authentication, and the main security technologies are as follows: #1 Public Key Infrastructure (PKI) is a complex environment of secure systems that provides encryption and electronic signature of messages, and provides the infrastructure to prove identity through certificates issued by a Certificate Authority (CA). Electronic signatures are used to ensure the integrity of data and authentication of its origin by utilizing private keys. Security features provided by certificate-based e-signatures include signer authentication, message integrity, and non-repudiation. The operation procedure of 'Secure Access' is briefly described as follows: 1) the terminal device sends the certificate (Certificate) and Certificate Revocation List (CRL) issued by the certificate authority to the controller. 2) The controller verifies the electronic signature validity of the received end device certificate with the certificate authority's public key that was previously injected into the controller. 3) Validate the validity of the received certificate, including the certificate's validity period, certificate chain, and certificate revocation list (CRL). 4) If the validation is successfully completed, access to the controller system is allowed only for requests from the end device.

Secure flashing

As cars have become more electrified, the importance and complexity of the software at the heart of the system has increased dramatically. As more features rely on software, so do the requirements for feature enhancements, bug fixes, security patches, and more. To do this, the controller (ECU) of an automotive system can update the firmware or software of the automotive system to a new version via reprogrammable flash memory. However, the use of the car's external communication channels for software downloads has increased the potential for attacks such as illegal software downloads or the injection of tampered software, and if the software being updated is not sufficiently validated, the cyber security threat to the car will increase significantly. As a measure to secure automotive systems, it is necessary to ensure the authenticity and integrity of downloaded firmware or software data. This is where the Secure Flashing feature comes into play. Secure Flashing is the ability to securely apply a new firmware or software version to a device when a software update is required for an automotive controller, without first verifying that the software being updated has been approved by the manufacturer and that the data has not been tampered with. As a security technique for controlling firmware manipulation in ECUs, Secure Flashing utilizes cryptographic techniques to verify the software to be updated in the controller. The main security features used in Secure Flashing are hash functions, symmetric key ciphers, and electronic signatures. Secure Flashing only performs software updates for firmware that is approved and validated by the vehicle manufacturer (OEM). The following is a brief description of the Secure Flashing operation procedure. 1) The OEM encrypts the source data of the software to be updated using a symmetric key shared in advance with the controller. 2) A hash algorithm is used to generate a hash value of the original data. 3) Generate an electronic signature value by encrypting the hash value with the vehicle manufacturer's private key. 4) Package this with the encrypted software data to create an image for distribution. 5) The image is sent to the controller over-the-air (OTA) or via a diagnostic tool. 6) The controller decrypts the encrypted software data using the pre-stored symmetric key of the vehicle manufacturer. 7) The electronic signature value attached to the image is then decrypted with the public key of the vehicle manufacturer to extract the original hash value. 8) Generate the hash value of the original decrypted data using the rehash algorithm. 9) Finally, the hash value of the original data is compared (verified) with the hash value generated by the controller to verify the authentication and integrity of the data. 10) If the hash values are the same, the software is confirmed to be untampered and sent from a trusted source, and the controller's software is updated.

Secure boot

The process of starting software on a computer or embedded system is known as "booting". If firmware or software is booted with tampered with, it could allow an attacker to cause it to behave differently from the manufacturer's intent, jeopardizing the safety of passengers or even stealing critical vehicle or user information. Boot kit and Root kit attacks are the primary threats that can occur during the controller's system Boot up process. A Boot kit is a type of Root kit that aims to infect a system's boot process. It is designed to run when the system starts, replacing or modifying the legitimate boot loader with its own malicious code so that it can run before the operating system loads. This can be done by filling the Master Boot Record (MBR) with meaningless strings to make it unbootable, or by infecting the Boot Sector to bypass or disable the system's security solutions, such as antivirus programs. A root kit is a collection of malware and software tools that enable unauthorized access and control of a system. Root kits can gain super administrator privileges within a system and can manipulate system resources and alter operating system functionality, effectively hiding their presence from security measures and antivirus software.

Secure Boot utilizes digital signature technology as a way to verify authentication and integrity during software loading at boot time. Electronic signatures ensure the integrity and authenticity of data and are used to verify that a message has not been altered in transit and that it came from the correct source. The main key cryptographic techniques behind these electronic signatures are the hash function and public key cryptography. When loading data for each step in the #1 boot process, Secure Boot validates it by comparing the hash value of the original data generated by the hash algorithm with the hash value obtained by decrypting the encrypted hash value with the vehicle manufacturer's public key. If the values compared are correct (i.e., the same), the next step is executed; if not (i.e., different), no boot is performed. If all validations in the following steps pass, the system starts normally. If any of the steps fail, the system will not boot any further.

Hardware security modules (HSMs)

In general, general-purpose HSMs are physical hardware security devices that perform tamper-resistant tasks to protect cryptographic processes by generating, securing, and managing keys used to encrypt and decrypt data, and generating digital signatures and certificates. They are physical hardware security devices that have been utilized in the Information Technology (IT) industry for a long time. For example, in the banking industry, #2 encryption is required for many different services, such as customer information management or internet banking user accounts. Storing encryption keys separately for each service increases the security risk. To solve this problem, the HSM keeps all keys secure and prevents them from leaking to the outside world. It also works by #4 requesting the HSM to perform the necessary encryption or decryption operations, and then #5 the HSM performs those operations and returns the results. Automotive HSMs provide the same security features as general-purpose HSMs in traditional information technology environments. However, the difference is that general-purpose HSMs are installed in PCI slots as cards or in server Where as automotive HSMs are system on a chip (SoC) and are mounted directly on the controller.

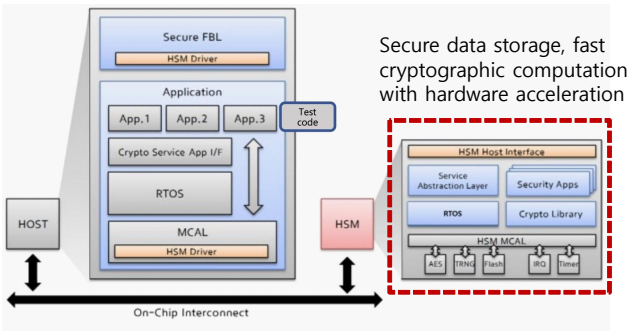

Figure 3: Automotive HSM.

In addition, it has a dedicated, highly secure HSM, Random Access Memory (RAM), Read Only Memory (ROM), and performs a series of operations through a dedicated Central Processing Unit (CPU) that is separate from the Host System. It is relatively safe from threats from potential attackers because it performs a series of operations through a dedicated Central Processing Unit (CPU). This structure ensures secure data storage in addition to secure data storage, it also enables high-speed processing of cryptographic operations using hardware acceleration. The main security technologies provided by HSMs are: First, cryptographic operations, Second, HSMs support hardware-based encryption, which enables encryption and Third, decryption operations to be performed quickly and securely. This helps to protect sensitive data and keep it secure during data transmission. And e-signatures and authentication. HSMs handle e-signature generation and verification to ensure data integrity and identity authentication. This helps establish the authenticity of electronic documents and transactions. Next is integrity verification. HSMs are used to verify the integrity of the system and data, ensure that the system or files have not been tampered with, and detect unauthorized changes. It also enables secure key management. HSMs securely store and manage cryptographic keys, and keep sensitive keys more secure than software or other devices. This helps minimize key exposure and unauthorized access and increase data security. Now let's talk about some of the technology applications based on automotive HSMs. Automotive HSMs excel at computational tasks that use cryptography. For example, when implementing Message Authentication Code (MAC)-based security features, they can securely store the secret key needed to generate the message secret key required to generate the authentication code, or securely store sensitive personal information such as user payment information within an in-vehicle infotainment (IVI) system.

Finally, it can serve as the root of trust for key cyber security applications such as Secure Boot, Secure Flashing, Secure OTA, and more.

Concluding remarks

This article presented the hierarchy of automotive IVN systems and the cyber security threats at each layer, and introduced the cyber security countermeasures adopted by automakers for each layer: secure access for a secure communication environment, secure flashing and secure boot for a secure system environment, and HSMs for a secure execution environment and data protection. With the commercialization of AI chips, cyber security technologies for future mobility and collaborative robots that combine advanced AI technologies such as machine learning and deep learning are expected to be greatly activated and commercialized in the near future.

References

1. Cybersecurity in automotive: Mastering the challenge, McKinsey & Company. 2020.
2. Siddiqui F, Khan R, Sezer S. Bird's-eye view on the autonomous cybersecurity landscape and challenges in adopting AL/ML. 6th International Conference on Fog and Mobile Edge Computing. 2021.
3. Upstream Security's Global Automotive Cybersecurity Report. 2021. http://upstream.auto/2021report/.
4. Refat R U D, Elkhail A A, Malik H. Machine learning for automotive cybersecurity: challenges, opportunities and future directions. AI-enabled Technologies for Automotive and Connected Vehicles, Lecture Notes in Intelligent Transportation and Infrastructure, Springer Nature AG. 2023; 547-567.
5. Olukemi A, Broklyn P, Adablanu S. The intersection of artificial intelligence and cybersecurity. Easy Chair No. 14095. 2024.
6. Auto Crypt HSM (Hardware Security Module). Product Introduction, Autocrypt Co. In-Vehicle Security for SDV. 2024.