자동차 시스템을 위한 HTA 기반 보안에 대한 연구

카욘도마틴 [1], 최진명 [2], 백윤흥 [3]
[1] 서울대학교 전기정보학과 박사과정
[2] 서울대학교 전기정보학과 석사과정
[3] 서울대학교 전기정보학과 교수

kayondo@snu.ac.kr, jmchoi@snu.ac.kr, ypaek@snu.ac.kr

Analyzing HTA-Based Security for Automotive Systems

Martin Kayondo[1], Jinmyung Choi[1], Yunheung Paek[1]
[1]Dept. of Electrical and Computer Engineering, Seoul National University and Inter-University Semiconductor Research (ISRC), Seoul National University

Abstract

Recently, automotive security is gerning significant attention due to the gradual surge in cyberattacks on automotive systems experienced by the industry over the past few years. These cyberattacks stem from the widened attack surface especially caused by increased connectivity and architectural complexity in modern automotive systems. Hardware Trust Anchors (HTAs), a known security technology in the cyber space, have been suggested as a candidate means to prevent automotive cyberattacks. In this paper, we analyze the effectiveness of HTAs in preventing automotive cyberattacks, and the current challenges adopting existing HTAs for automotive security. Simultaneously, we shed a light on complementary cyber defenses that may accompany HTAs to further enhance automotive security.

1. Introduction

The automotive industry has undergone significant transformation due to recent technological advancements. Modern automotive systems are now equipped with cutting-edge features such as Advanced Driver Assistance Systems (ADAS), autonomous driving capabilities, over-the-air (OTA) software updates, and feature-on-demand (FOD) services, among others. While these innovations enhance driver comfort, they also require substantial computing power and connectivity, demands that previous system architectures could not accommodate.

As a result, the automotive Electrical/Electronic (E/E) architecture has grown increasingly complex. It now includes application processors with sophisticated operating systems (OS) to manage compute-intensive tasks, as well as real-time processors for time-sensitive operations. Additionally, many features depend on external connectivity, further complicating the network topology of automotive systems.

One of the most significant consequences of these advancements is the increased attack surface of modern vehicles. With enhanced connectivity, cars are more vulnerable to remote cyberattacks. Moreover, the complexity of the architecture and networking increases the likelihood of exploitable software bugs and network vulnerabilities. Consequently, automotive cyberattacks have surged, leading to significant financial losses for both manufacturers and consumers. Morover, the growing popularity of autonomous vehicles and the increasing reliance on software to control critical safety features also means potential dangers of cyberattacks could escalate to life-threatening situations, including fatal accidents.

In response to this rising threat, regulatory bodies and manufacturers have turned to Hardware Trust Anchors (HTAs) to mitigate automotive cyberattacks. HTAs have long been used in other systems to mitigate cyberattacks. They protect systems by relying on hardware-based solutions for sensitive data storage and providing secure cryptographic services such as key generation and data encryption before transmission. Today, all vehicles sold in Europe are now required to have an HTA for certification [1].

This paper analyzes the effectiveness of HTA-based security in the automotive sector and examines the challenges in implementing HTAs in modern automotive systems. Specifically, we focus our analysis on comparing traditional and modern automotive system architecture and security, and provide an insight into the challenges defending modern automotive systems. We finally make an in-depth analysis of HTA-based security solutions for automotive systems.

2. Automotive Systems and Security Challenges.

Automotive systems are composed of hundreds of electronic control units (ECUs) networked together on in-vehicle networks (IVNs). ECUs control components such as the actuators, door locks and braking systems.

IVNs employed rely on several protocols such area network (CAN), ethernet, FlexRay etc., and each is applied depending on the required bandwidth and safety speed constraints. The systems are equipped with a central ECU called the gateway for routing network packets/messages

among the other ECUs. CAN is the predominant protocol used for sharing control and data messages among ECUs. It is preferred for its simplicity and ability to transmit control messages fast enough meeting hard real-time deadlines. However, CAN security is questionable at best and hard to implement due to the constraints of the payload size and speed requirements. Since ECUs are controlled by CAN messages, it is easy for an attacker with access to the CAN buses to inject control messages directed at specific components. For traditional automotives without wireless external connections, attacks on the CAN bus were achievable through physical connections such as the mandated On-Board Diagnostics (OBD) unit in European vehicles. A physical attacker can easily connect an analysis tool to the ODB port and sniff CAN packets. A motivated attacker can also craft attacks that inject control messages into the CAN bus through the OBD port. Some modern vehicles retain the existing CAN protocol for ECU communication, while others use the CAN-Flexible Data rate (CAN-FD). Similar CAN network attacks on traditional automotive systems still plague modern vehicles.

However, modern vehicles with external connectivity have an even larger attack surface. Remote attackers can connect to the car through available remote connections, such as the OBD dongle facilities, and hack their way to the CAN bus. With such access, they can still inject control messages or eavesdrop on the bus for vehicle information just as successfully as physical attackers.

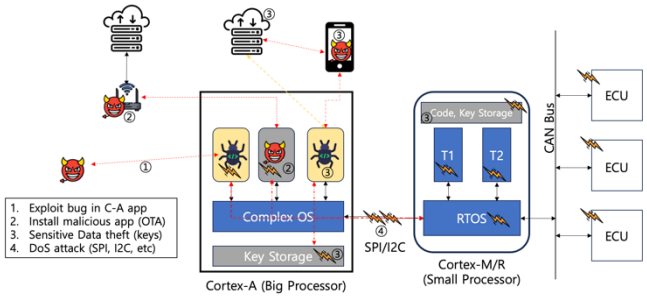
Modern automotive systems also provide advanced features such as advanced driver assistance systems (ADAS) in-vehicle infotainment (IVI) and autonomous driving among others. Such features require high computing resources, hence vehicles supporting such systems are equipped not only with high-performance processors but also with complex software. The drawback of such complex systems is the presence of exploitable vulnerabilities and difficulty of debugging. Therefore, with increases software and hardware complexity, even more attack vectors are introduced. For example, as explained by [2], a remote attacker can exploit a vulnerability in a complex application that provides one of the above-mentioned advanced features, and leverage that vulnerability to execute malware remotely (1 in Figure 1). Such malware may be diverse in purpose and goal, ranging from injecting control messages into the CAN bus, to stealing owner information.

Finally, modern automotive systems support over-the-air (OTA) complex software and firmware updates. Not shockingly, it has been revealed by [2] that a determined attacker can leverage the OTA installation process to install malware on an automotive system, if necessary security measures are not in place (2 in Figure 1).

3. Automotive System Security

There have been efforts to enhance automotive security. Several works approach this challenge from the network viewpoint. These solutions analyze CAN network packets are different layers to establish authenticity before forward, at reception or before sending them. Additionally, [3] proposes a trusted execution environment (TEE)-based solution for verifying CAN messages before they are sent by low-powered ECUs, rather than focusing on the CAN network, authors propose disallowing malicious packets from being sent at all. Other basic solutions include software hardening, use of memory safe language for software and firmware development to prevent memory bugs, and among others.

A special and gradually growing solution is employment of hardware trust anchors for automotive security. In 2015, the European Union mandated installation of HTAs in all automotives intended for the region's market. Different HTA models are presented, including the Full, Medium and Light models.



(Figure 1) Possible attacks on an automotive ECU.

4. HTAs and Automotive Security

Hardware trust anchors are specialized hardware modules designed to enforce security by storing cryptographic keys, verifying signatures, and performing secure operations. The cryptographic keys stored within hardware trust anchors are often referred to as the "root of trust" because they serve as the foundation for other security mechanisms within the system.

4.1 Hardware Trust Anchors in Automotives

One of the primary reasons hardware trust anchors are particularly suitable for automotive security is their resistance to tampering. Unlike software-based solutions, which can be exploited by attackers who gain access to the system, hardware trust anchors are often equipped with tamper-resistant features that make it extremely difficult for adversaries to compromise the system without physically dismantling the device.

Generally, like other general purpose HTAs, automotive HTAs are meant for secure information storage to prevent attackers from stealing sensitive information even after breaking into the vehicle network. Leveraging their cryptographic capabilities, automotive manufactures aim to employ HTAs mostly for cryptographic security solutions. Different HTA models have different features, but here we focus on the EVITA Full model. Such as model is expected to support the following features:

A) Secure random key generation for generation truly random security keys.
B) A secure non-volatile memory for storing sensitive data such as security keys.
C) Cryptographic engine for cryptographic operations.
D) A secure internal clock.

As listed in [1], examples of existing HTAs include discrete hardware trusted platform modules (TPMs) for intensive cryptographic computation and secure non-volatile storage, hardware security modules (HSMs) such as those

attached to processors by NXP, and TEE-based solutions such as those based on ARM TrustZone.

In terms of security, automotive vendors aim to mitigate cyberattacks such as those explained above as follows:

1. Sensitive information theft (Privacy theft): By relying on the secure storage (NVM) of the HTA, sensitive information such as cryptographic keys can be protected from attackers.
2. Control Message Injection and Eavesdropping: Eavesdropping can be deterred by using the HTA cryptographic engine to (de)encrypt control messages before transmission and on reception.
3. OTA Update Hijacking and Malware Installation: HTAs can be used to secure firmware updates and ensure the authenticity of communications between vehicles and the software backend infrastructure. [5, 6] illustrate how a TPM and light weight HTAs such as HSMs can be combined to achieve secure OTA automotive firmware updates.

4.2 Challenges Adopting Existing HTAs for Modern Automotives:

For traditional automotives, adopting HTAs was as easy as using cryptographic engines embedded in microcontrollers. For example, most traditional automotive systems relied on ARM Cortex-M processor-based microcontrollers, which in turn were equipped with cryptographic engines such as security hardware engines (SHEs).

For modern automotive systems, however, due to the complex architecture, designers must consider protection for all the involved execution processors. For example, [5, 6] use a discrete TPM for compute-intensive security tasks such as asymmetric cryptographic operations, and SHEs or device identifier composition engine (DICE) for light-weight security operations such as device attestation.

Considering automotive systems have hundreds of ECUs, this design proves costly because it requires each ECU with a high-performance processor to be accompanied by a discrete TPM as an HTA for security. Obviously, in [5, 6] the mentioned TPM is used for secure OTA updates only, and therefore only one of the kind is required. Any attempt to expand the HTA features throughout the vehicle soon requires multiple discrete TPMs for compute intensive security tasks. Thus, the only design advantage observable in [5, 6] is the fact that microcontroller based HSMs and SHEs are already a standard requirement as earlier mention, and thus are already existing in most automotive systems.

Another challenge regards the integration of the diverse security features and levels provided by the different architectures. While [5, 6] clearly state the purpose of the TPM and that of DICE or SHEs, it is unclear how to expand their design for a general-purpose security HTA beside securing OTA updates.

Finally, it is unclear how the communication between the TPM and the low-end HTAs can be secured.

Ultimately, our conclusion is that rather than discrete HTAs tailored for different processing power levels, there is need for an economical and efficient combined HTA system that suits the modern automotive architecture.

4.3: Beyond Vehicle-Local HTAs:

In-vehicle HTAs alone can only provide local security but they have their limits. It is important for the reader to recognize that they alone do not provide full security. Especially for modern automotive systems which have become cyber-physical systems with high connectivity. For example, as explained in [2], it is possible to attack a vehicle by first compromising the backend server. A compromised server can be leveraged to release compromised ECU firmware updates. It may also be leveraged to send malicious control commands to the vehicle. Therefore, as it is important to install HTAs in the vehicle itself it is equally important to install trust anchors in the backend servers. Additionally, modern automotives allow the user control over personal devices such as smartphones. As in the backend server case, compromised user devices connected to the vehicle may be leveraged to attack the vehicle (3 in Figure 1).

Finally, as already explained, HTAs provide cryptographic solutions. Software making requests to the HTA, and the HTA firmware itself must be vulnerability free. [7] explain how they discovered exploitable vulnerabilities in hardware security modules. In the case of software querying the HTA, such can be compromised through control hijack attacks and code injection. After a high jacking, the software can be leveraged to query the HTA for security sensitive data such as cryptographic keys.

4. Conclusion:

In this paper, we present the challenges facing automotive security. We especially explore the security status of modern automotive systems and possible attacks. We then analyze the possibility of using hardware trust anchors to thwart automotive cyberattacks and compare HTAs for traditional automotive systems with those needed to match the requirements for modern automotives. We also shed a light on other security solutions required to complement HTAs to ensure safer automotive systems.

ACKNOWLEDGEMENT

This research was supported by Korea Planning&Evaluation Institute of Industrial Technology(KEIT) grant funded by the Korea Government(MOTIE) (No. RS-2024-00406121, Development of an Automotive Security Vulnerability-based Threat Analysis System(R&D)). This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (RS-2023-00277326). This work was supported by the BK21 FOUR program of the Education and Research Program for Future ICT Pioneers, Seoul National University in 2024. This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) under the artificial intelligence semiconductor support program to nurture the best talents (IITP-2023-RS-2023-00256081) grant funded by the Korea government (MSIT). This work was supported by Inter-University Semiconductor Research Center (ISRC). This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.RS-2024-00438729, Development of Full Lifecycle Privacy-Preserving Techniques using Anonymized Confidential Computing).

참고문헌

[4] Checkoway, Stephen, et al. "Comprehensive experimental analyses of automotive attack surfaces." *20th USENIX security symposium (USENIX Security 11)*. 2011.

[1] Plappert, Christian, Andreas Fuchs, and Ronald Heddergott. "Analysis and evaluation of hardware trust anchors in the automotive domain." *Proceedings of the 17th*

International Conference on Availability, Reliability and Security. 2022.

[3] Mishra, Tanmaya, Thidapat Chantem, and Ryan Gerdes. "Teecheck: Securing intra-vehicular communication using trusted execution." *Proceedings of the 28th International Conference on Real-Time Networks and Systems*. 2020.

[2] Jing, Pengfei, et al. "Revisiting automotive attack surfaces: a practitioners' perspective." *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2024.

[5] Plappert, Christian, and Andreas Fuchs. "Secure and Lightweight Over-the-Air Software Update Distribution for Connected Vehicles." *Proceedings of the 39th Annual Computer Security Applications Conference*. 2023.

[6] Plappert, Christian, and Andreas Fuchs. "Secure and Lightweight ECU Attestations for Resilient Over-the-Air Updates in Connected Vehicles." *Proceedings of the 39th Annual Computer Security Applications Conference*. 2023.

[7] Daniel Teuchert, "Finding Vulnerabilities in the HSM", https://www.code-intelligence.com/webinar/hsm-vulnerabilities#access, 09.2024