Enhancing Automotive Cybersecurity: Exploring Hardware Security Primitives for Resilient and Trusted Vehicle Systems

Tamal Sutradhar Rudra
ID:212120005
Department of Computer Science and Engineeering
Notre Dame University Bangladesh)
Dhaka, Bangladesh
tamal212120005@student.ndub.edu.bd

Tanvir Jahan Alin
ID:212120008
Department of Computer Science and Engineeering
Notre Dame University Bangladesh
Dhaka, Bangladesh
alin212120008@student.ndub.edu.bd

***Abstract*—The integration of electronic systems and connectivity features in the automotive industry has propelled advancements in vehicle technology. However, this evolution has introduced new vulnerabilities, exposing vehicles to potential cyber threats. This paper explores the significance of enhancing automotive cybersecurity through the implementation of hardware security primitives. Making cars safe from attacks is a complicated subject that many researchers are studying. In this article, we'll discuss the current ways to keep vehicles secure using hardware modules and unique physical functions.**

***Index Terms*—Hardware Security, Cybersecurity, Cyberattack, Trusted Platform Module (TPM), Physically Unclonable Functions (PUFs)**

I. Introduction

In recent years, the automotive industry has witnessed a rapid increase in the integration of electronic systems and connectivity features in vehicles. While this trend has brought numerous benefits, it has also exposed vehicles to new cybersecurity risks. As vehicles become more connected, they become vulnerable to cyberattacks, which can have severe consequences on both driver safety and privacy. Therefore, it is crucial to enhance automotive cybersecurity to ensure resilient and trusted vehicle systems.

II. Hardware Security Primitives

One auspicious approach to enhance automotive cybersecurity is the use of hardware security primitives. Hardware security primitives are physical components or features integrated into the vehicle's hardware design to provide additional layers of security. These primitives can help prevent, detect, and mitigate cyberattacks by safeguarding critical vehicle functions and data.

A. HARDWARE MODULES

Hardware Module is a one kind of physical device that is used for extra security to secure the sensitive data. Mainly, it generate cryptographic key to authentication, encrypt or decrypt any kind of application or database.

Securing the generated keys are also a challenge for the system. The keys generated by the modules cannot be predicted by any kind of application or AI(Artificial Intelligence). It strictly has to be unique and random. The copy of the key generated by the module must be stored in secured storage so that it can be used if the key is compromised. After the key has been used the key should be permanently destroyed.

Researchers from the E-Safety Vehicle Intrusion Protected Applications (EVITA) project put forward a vehicular hardware security module .[13] Their module is a cryptographic co-processor, that is designed to be connected on vehicular communication and it comes with three different variation- ”full”, ”medium”, ”light”. The full version has everything to secure vehicular communication. The ”medium” version has the security on inter-vehicular communication. And the ”light” version only secure the interactions between ECUs and the sensors and actuators.This design has subsequently served as a source of inspiration for more recent implementations of vehicular Hardware Security Modules (HSMs).

B. Trusted Platform Module(TPM)

Trusted platform modules (TPM) are cryptographic co-processors specifically created to embed security within larger computer systems. TPMs are permanently integrated into the system and cannot be removed. The TPM specification was initially intended for general-purpose computer systems. However, incorporating TPMs directly into vehicles poses challenges because of the limited computational resources and real-time demands specific to automotive environments. As an alternative, researchers have taken inspiration from the TPM specification to create hardware security modules (HSMs) tailored for vehicles. These vehicle-specific HSMs are designed for seamless integration into automotive systems and typically include a subset of the cryptographic components found in traditional TPMs.

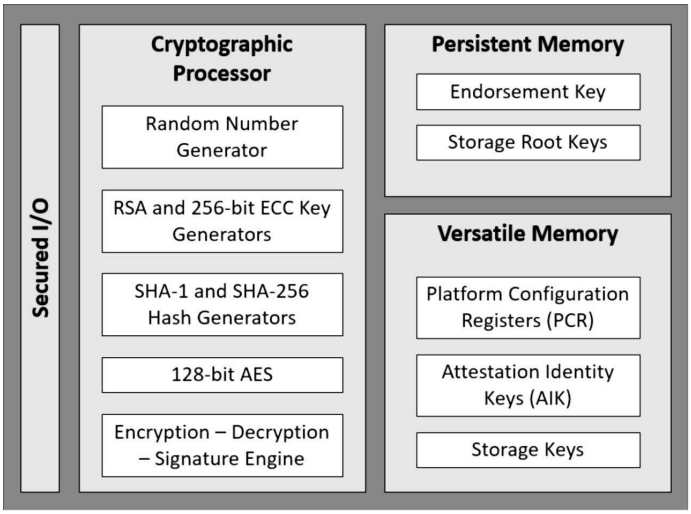

Fig. 1. Necessary Elements of TPM 2.0

C. Physically Unclonable Functions

Physical unclonable functions (PUFs) can be likened to a kind of hash function, where a particular input produces a unique output. Within PUFs, the inputs are referred to as 'challenges,' and the outputs are termed 'responses. '[9] Together, a challenge and its corresponding reply are referred to as a challenge-response pair (CRP). A physically unclonable function (PUF) is considered robust when it has a significant quantity of CRPs. In an ideal scenario, it would have an exponential number of CRPs so that an n-bit strong PUF would have 2n CRPs. On the other hand , a weak PUF has a very limited number of CRPs (typically just one).[10]

III. PUFs for Security in Vehicles

Physically unclonable functions (PUFs) offer a range of possible applications in automotive security and can be custom-designed for integration into these systems. [7] The special qualities inherent to PUFs make them suitable for applications that would be unfeasible using traditional technology. This section will point out some of the possible security uses of PUFs, including storing keys, creating pseudonyms, and enabling vehicle-to-vehicle communication.

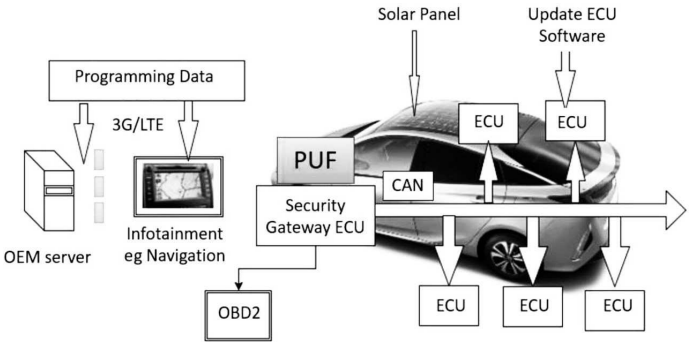

Fig. 2. Incorporation of PUF technology to ensure the security of software updates in the automotive industry.[12]

A. Using PUF for Safe Data Storage

Scientists have suggested the utilization of physically unclonable functions (PUFs) as a means to store private keys for use in vehicle communication. [5] Conventional key storage techniques usually rely on secure memory. However, their approach enables the safe storage of keys in memory that isn't inherently secure. This is accomplished by generating keys based on the responses of a physically unclonable function (PUF), which guarantees that an attacker would need to have the physical device itself to retrieve the key. [9] The suggested techniques include the use of either a strong PUF or a weak PUF. [5]

In the article written by Petit and colleagues, they suggest a different way to store data. [11] In this approach, the unique response generated by the PUF is employed to create a pseudonym consisting of a public key and a private key pair. A central Certificate Authority (CA) issues a certificate as evidence that it has confirmed the legitimacy of this pseudonym. This certificate can be included in communications with an outside entity. [9]

B. Using PUF for Communication Between Vehicles

Scientists have suggested using PUFs as a component in a bigger communication system that can prevent attacks from groups of adversaries. [4] In this scenario, a vehicle communicates with nearby vehicles. To ensure the right vehicles receive these messages, sensors are used to visually connect each message with the correct vehicle. This visual connection helps the vehicle determine where the other vehicles are located relative to itself. This information is useful for responding to warning messages from those vehicles.

1) PUF in inter-vehicular Communication: Scientists have suggested a method for incorporating Physically Unclonable Functions (PUFs) into a broader communication system with the capability to thwart coalition attacks by adversaries.[4] In a coalition attack, multiple adversaries mimic the sender and recipient by intercepting and subsequently relaying messages to their intended targets. In the described scenario, a specific vehicle is engaged in communication with other nearby vehicles. To ensure the legitimacy of these communications, sensors are used to visually link each message to the correct vehicle, providing a relative location understanding of the communicating vehicles. This knowledge can be valuable for the receiving vehicle in responding to warning messages from its counterparts.
2) Incorporating PUF with ECU: The researchers propose a method to stop Denial of Service (DoS) attacks on the CAN bus by introducing the capability to verify the identity of connected ECUs.[1] The suggested approach involves the allocation of a unique identifier (ID) to every Electronic Control Unit (ECU) connected to the CAN bus. Each ID is linked to specific challenge-response pairs (CRPs) generated by Physical Unclonable Functions (PUFs) integrated into each ECU. A centralized reference monitor (RM) securely stores copies

of these IDs and CRPs for all ECUs within a trusted platform module (TPM). This data is established and loaded during the vehicle's assembly process. To initiate communication on the CAN bus, any ECU must undergo authentication by the RM.

A similar strategy, as proposed in, employs PUFs within individual ECUs to create private/public key pairs for each ECU and a central server.[6] These key pairs are initially used to register each ECU's ID with the server. Subsequently, the server authenticates communication sessions between ECUs.[8]

However, adversaries, even if they merely forward intercepted messages without altering them, can deceive targeted vehicles into visually associating with the adversary instead of the actual intended recipient. This deceptive practice can pose risks, particularly when vehicles are responding to emergency warnings like sudden braking.

To mitigate these issues, the researchers propose the development of a message authentication method that is non-forwardable, rendering it immune to coalition attacks. Vehicles are issued certificates by a trusted Certificate Authority (CA), containing physical characteristics for vehicle identification and challenge-response pairs (CRPs). When a vehicle seeks to initiate communication, it shares its certificate with the intended recipient. The recipient processes the information from the certificate and configures a laser based on the challenge parameters within the certificate. The recipient's laser stimulates the optical Physical Unclonable Function (PUF) on the sending vehicle and records the response. If the recorded response aligns with the response in the certificate, the receiving vehicle authenticates the sender. This process is then reversed, with roles swapped, allowing the sending vehicle to authenticate the receiving vehicle.

However, there's a potential issue. Adversaries can forward messages, making the targeted vehicles mistakenly connect to the adversary instead of the intended recipient. Even if adversaries simply forward messages without altering them, the attacked vehicle may wrongly identify the adversary as the intended communication partner. This could be dangerous, especially when the attacked vehicles need to respond to emergency warnings, like sudden braking maneuvers.

IV. Discussion and Final Thoughts

Even the fundamental building blocks of hardware security, such as TPMs, HSMs, and PUFs, can have their own security weaknesses due to design flaws.Recently, scientists uncovered two ways to breach TPMs by exploiting new design flaws that can be fixed with firmware updates. [6]Furthermore, numerous widely used cryptographic algorithms, like RSA, in TPMs and HSMs, can be exploited by quantum attacks. [2] Machine learning-based modeling attacks have been demonstrated to compromise the security of multiple PUFs.[3]These weaknesses introduce further complexities in design but are not insurmountable obstacles. The elements examined in this study offer a strong basis for the creation of security systems for vehicles.[8]

V. Conclusion

In conclusion, the exploration of hardware security primitives as a means to enhance automotive cybersecurity presents a promising path towards building resilient and trusted vehicle systems in today's increasingly connected automotive landscape. The adoption of security measures such as Secure Boot, Trusted Execution Environment (TEE), and hardware encryption offers tangible benefits in safeguarding critical vehicle functions and data from cyber threats.

By implementing these hardware security features, automakers can provide a safer and more secure driving experience for consumers. Resilient systems capable of detecting and recovering from cyberattacks minimize the potential disruptions to vehicle functionality. Concurrently, trusted systems foster a strong sense of confidence in the security and privacy of the vehicle, bolstering the trust between drivers and their automobiles.

As the automotive industry continues to evolve, it is imperative to prioritize and invest in robust cybersecurity measures to address the evolving threats. Hardware security primitives play an indispensable role in this endeavor, ensuring that vehicles remain at the forefront of innovation while preserving the safety and privacy of their occupants. In doing so, the industry can move forward with the assurance that automotive cybersecurity remains a top priority in the ever-connected and technology-driven world of automobiles.

References

[1] Aishwarya et al. "Authentication of electronic control unit using arbiter physical unclonable functions in modern automobiles". In: *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*. 2016, pp. 1–9.

[2] Lily Chen et al. *Report on post-quantum cryptography*. Vol. 12. US Department of Commerce, National Institute of Standards and Technology …, 2016.

[3] Jeroen Delvaux. "Machine-learning attacks on polypufs, ob-pufs, rpufs, lhs-pufs, and puf–fsms". In: *IEEE Transactions on Information Forensics and Security* 14.8 (2019), pp. 2043–2058.

[4] Shlomi Dolev et al. "Optical PUF for vehicles non-forwardable authentication". In: *Dept. Comput. Sci., Ben-Gurion Univ. Negev, Beersheba, Israel* (2015), pp. 15–02.

[5] Michael Feiri, Jonathan Petit, and Frank Kargl. "Efficient and secure storage of private keys for pseudonymous vehicular communication". In: *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*. 2013, pp. 9–18.

[6] Seunghun Han et al. "A bad dream: Subverting trusted platform module while you are sleeping". In: *27th USENIX Security Symposium (USENIX Security 18)*. 2018, pp. 1229–1246.

[7] Carson Labrado and Himanshu Thapliyal. “Design of a piezoelectric-based physically unclonable function for IoT security”. In: *IEEE Internet of Things Journal* 6.2 (2018), pp. 2770–2777.

[8] Carson Labrado and Himanshu Thapliyal. “Hardware Security Primitives for Vehicles”. In: *IEEE Consumer Electronics Magazine* 8.6 (2019).

[9] Carson Labrado and Himanshu Thapliyal. “Hardware security primitives for vehicles”. In: *IEEE Consumer Electronics Magazine* 8.6 (2019), pp. 99–103.

[10] Enahoro Oriero and Syed Rafay Hasan. “Survey on recent counterfeit IC detection techniques and future research directions”. In: *Integration* 66 (2019), pp. 135–152.

[11] Jonathan Petit et al. “On the potential of PUF for pseudonym generation in vehicular networks”. In: *2012 IEEE Vehicular Networking Conference (VNC)*. IEEE. 2012, pp. 94–100.

[12] Hiroyuki Tomiyama. “PUFbased Security Enhancement for Automotive Software Update”. In: *Int. Forum MP-SoC Softw.-Defined Hardware* (Jul. 30, 2015).

[13] Marko Wolf and Timo Gendrullis. “Design, implementation, and evaluation of a vehicular hardware security module”. In: *Information Security and Cryptology-ICISC 2011: 14th International Conference, Seoul, Korea, November 30-December 2, 2011. Revised Selected Papers 14*. Springer. 2012, pp. 302–318.