Enhancing Remote Keyless Entry Security through a Lightweight PUF based Mutual Authentication Mechanism

Rajath K, Sahana S Hegde, Shreya S, Swetha M, Mrs. Supriya Suresh
Student, Student, ,Student, Student, Lecturer,
Computer Science Engineering,
,KS School of Engineering and Management, Banglore , India

Abstract - : Cars equipped with keyless entry systems enable users to access their vehicles without traditional keys. Among these systems, the Remote Keyless Entry (RKE) system stands out as a popular choice. However, vulnerabilities like replay attacks can compromise RKE systems that rely on fixed codes for unlocking. Even systems using rolling codes are susceptible to Roll Jam attacks. To counter these threats, we propose a straightforward and secure mutual authentication method leveraging Physical Unclonable Functions (PUFs). Our suggested technique undergoes rigorous security analysis, proving its resilience against common threats. Furthermore, we conduct a comparative analysis of its computational efficiency against existing systems. Key terms include Roll Jam assault, replay attack, remote keyless entry (RKE) system, mutual authentication, and physical unclonable function (PUF)..

Index Terms - Remote Keyless Entry ,PUF ,Mutual Authentication Mechanism, Electronic Control Units (ECUs), On-Board Diagnostic (OBD),Internet Of Things ,Arduino Board, Python ,AES Encryption Algorithm, Registration phase, Authentication phase, Key fob.

I. INTRODUCTION

Over time, automotive electronics have expanded to enhance user experience in cars. While these advancements offer convenience, they've also opened up new opportunities for potential attacks. Current car systems, including Electronic Control Units (ECUs), radio channels, keyless entry, Bluetooth, and On-Board Diagnostic (OBD) ports, present various vulnerable points that attackers can exploit. Both physical and remote assaults on vehicles are feasible. Particularly, attackers can exploit keyless entry systems using affordable equipment and software without requiring physical proximity. Consequently, attackers historically focus on these keyless entry devices due to the tangible risks associated with them. This research investigates security vulnerabilities present in keyless entry systems and proposes a solution to fortify their defenses. Keyless entry systems enable vehicle locking and unlocking without the need for physical keys. These systems typically manifest in two main types: Passive Keyless Entry and Start (PKES) systems and Remote Keyless Entry (RKE) systems. In RKE systems, users utilize a key fob to press a button for locking or unlocking the car door, while PKES systems automatically unlock the door when the key fob is in close proximity to the vehicle. Both PKES and RKE systems have encountered documented attacks, but our focus within this study is primarily on the vulnerabilities associated with RKE systems. The initial RKE system generations employed static codes within their RF signals, leaving them vulnerable to replay attacks wherein an adversary records and replays these signals to gain vehicle access. Such replay attacks are relatively straightforward for adversaries to execute. To counter this, rolling codes replaced static codes as a preventive measure against replay attacks. With the depression of the key fob's unlock button, a new rolling code is generated each time, allowing only one instance of unlocking the car with that specific rolling code. Notably, two popular rolling code schemes, NXP's Hitag-2 and Microchip Technology's KeeLoq, have been widely adopted. Nevertheless, attempts have been made to compromise the security of RKE systems employing rolling codes. The RollJam attack demonstrated that specialized equipment can compromise even RKE systems reliant on rolling codes. To safeguard RKE systems against such attacks, this paper proposes an authentication mechanism leveraging Physical Unclonable Functions (PUFs) as the fundamental basis for authentication. PUF is a primitive hardware security system that uses randomness introduced during production to extract secrets. PUFs do not retain the answers in memory; instead, they map input challenges to responses. PUFs have therefore been applied to security applications across various domains

II. LITERATURE SURVEY

In 2020 Alexandra Balan and Florin Sandu The integration of multicore processors and peripherals from multiple intellectual property core providers as hardware components of IoT multiprocessor systemson-chip (SoC) represents a source of security vulnerabilities for the in-chip communication. This paper describes the concept and the practical results of a SoC security implementation that is illustrative for IoT applications. The mechanism employed in this approach uses physically unclonable functions (PUF) and symmetric cryptography in order to encrypt the transferred messages within the SoC between the microprocessor and its peripherals. The mechanism is experimentally validated at FPGA level, the paper describing also an implementation scenario for an IoT ARM based device[2].

In 2020, Ferucio Laurenţiu Ţiplea, Cristian Andriesei and Cristian Hristea" Security and Privacy of PUF-Based RFID Systems" PUF-based RFID schemes often fall short of achieving basic privacy levels compared to symmetric cryptography. Formal models are crucial for analyzing security flaws, emphasizing the need for rigorous cryptographic treatment in PUF-based RFID system [3].

In 2020,Kunal karnik ,Saurabh kale, Manandeep, Ajinkya medhekar" On vehicular security for RKE and Cryptographic algorithms :A survey" Cars that connect to the internet are handy but can be easily hacked. Instances like VW RKE flaws, Jeep Cherokee takeover, and Tesla brake hijacking highlight vulnerabilities. Some famous cars had issues like being unlocked remotely or even controlled by hackers. RFID helps identify devices but needs strong security to let only authorized people use the car [4].

In 2021,Kyle Greene, Deven Rodgers, Henry Dykhuizen, Quamar Niyaz, Khair Al Shamaileh, and Vijay Devabhaktuni" A Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic ",Enhanced RKE system uses timestamping, XOR encoding to counter threats. Rigorous testing proves its superiority over conventional systems, assuring robust security, and reliability for remote entry users against potential vulnerabilities [5].

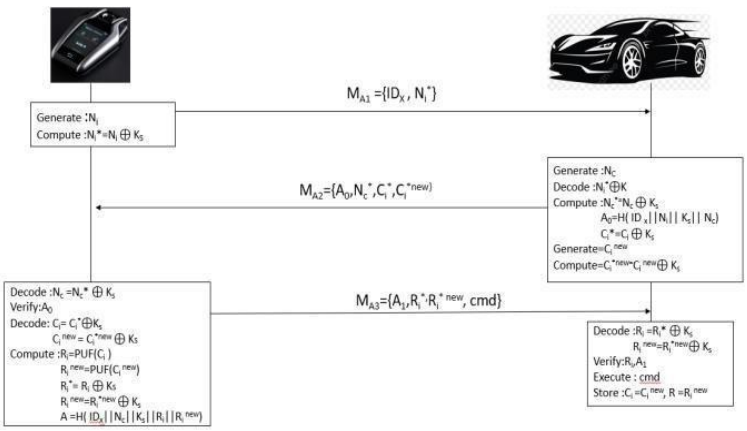
In 2022 Pramila B , Thanmay M Shetty , Bhoomika B, Pallavi k, "Physical Unclonable Design for Key Generation for AES Encryption Algorithm" Due to the fact that the keys needed to encrypt or decode data must be kept on hardware along with the design, cryptographic algorithms that are frequently stored on hardware devices are easily hacked .This makes creating a solution to the key storing issue more important. A physical unclonable function is suggested as a remedy [6]

III. REGISTRATION PHASE

[A]Registration phase

Step 1: The key fob constructs a message, MR1 , comprising IDx and a registration request, which is then transmitted to the car.A **Step 2**: When MR1 is received from the key fob, the car receiver creates a challenge, Ci, and uses it to form a message, MR2, which is then dispatched to the key fob.
Step 3: The key fob generates Ri = PUF(Ci) and sends Ri to car with MR3.
Step 4: Upon receiving MR3 from the key fob, the car receiver stores the ID IDx along with the challenge-response pairs (Ci, Ri). Subsequently, the car receiver generates a key, Ks, and sends it to the key fob using message MR4.
Step 5: Upon reception of MR4 from the car's receiver, the key fob saves the key Ks. This key will be utilized in subsequent verification procedures

IV. REGISTRATION PHASE



[b]Registration phase

Step 1: Upon pressing the key fob button, a unique value Ni, known as a nonce, is created. Subsequently, the key fob calculates Ni*=(Ni ⊕Ks) and constructs the message MA1 containing {IDx, Ni*}.

Step 2: Upon reception of MA1, the car receiver decrypts Ni by performing Ni = Ni* ⊕ Ks. Subsequently, the receiver generates a new nonce, Nc, and calculates Nc* by executing Nc* = Nc ⊕ Ks. Following this, the receiver computes an authentication parameter, which involves creating a secure hash of a concatenated message. The involves merging the parameters IDx, Ni, Ks, and Nc, and deriving the hash (A0 = H(IDx ‖ Ni ‖ Ks ‖ Nc)) as the authentication parameter.A0 serves as the authentication parameter for the car receiver.

Step 3: Upon receiving MA2, the key fob proceeds to decipher Nc by computing Nc = Nc* ⊕ Ks and verifies the authentication parameter, A0. Upon successful verification, the key fob decodes Ci by performing Ci = Ci* ⊕ Ks and Ci = Ci*new ⊕ Ks. Next, utilizing its PUF, the key fob generates responses corresponding to the received challenges as Ri = PUF(Ci) and Rinew = PUF(Cinew). Subsequently, the key fob computes Rinew = Ri ⊕ Ks and Ri*new = Rinew ⊕ Ks.

Step 4: Upon reception of MA3, the receiver proceeds to decipher Ri by computing Ri = Ri* ⊕ Ks and Rinew = Ri*new ⊕ K1. Subsequently, it validates both the response, Ri, and the authentication parameter, A1. If the validation fails, the authentication process halts

V.CONCLUSION

Across the aforementioned papers, we delved into the vulnerabilities targeting RKE systems. Our focus was on presenting a streamlined approach that maintains essential security elements. Specifically, we introduced a mutual authentication system leveraging PUFs designed for Remote Keyless Entry systems. Through a thorough examination of its security and performance, our analysis confirms the effectiveness of employing PUFs to establish an efficient authentication system for RKE setups.

VI.REFERENCES

[1] Rohini Poolat Parameswarath and Biplab Sikdar" A PUF-based Lightweight and Secure Mutual Authentication Mechanism for Remote Keyless Entry Systems",2022

[2] Alexandra Balan and Florin Sandu "A PUF-based cryptographic security solution for IoT systems on chip",2020

[3] Ferucio Laurențiu Țiplea, Cristian Andriesei and Cristian Hristea" Security and Privacy of PUF-Based RFID Systems",2020

[4] Kunal karnik ,Saurabh kale, Manandeep, Ajinkya medhekar"On vehicular security for RKE and Cryptographic algorithms :A survey",2020

[5] Kyle Greene, Deven Rodgers, Henry Dykhuizen, Quamar Niyaz, Khair Al Shamaileh, and Vijay Devabhaktuni" A Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic",2021

[6] Pramila B, Thanmay M Shetty ,Bhoomika B, Pallavi K "Physical Unclonable Design for Key Generation for AES Encryption Algorithm",2022