Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

On Vehicular Security for RKE and Cryptographic Algorithms: A Survey

Kunal Karnik
PCCOE
Pune, India

Saurabh Kale
PCCOE
Pune, India

Manandeep
PCCOE
Pune, India

Ajinkya Medhekar
PCCOE
Pune, India

***Abstract*—Lately, automobile security was similar to theft prevention, but the software tech within the automobile growing exponentially, to understand visions of the connected car, security is now becoming a key factor for safety. And safety is undoubtedly the primary concern of each vehicle manufacturer. Reading about experiments which depicted vehicles being remotely hacked via connected telematics unit, we determine the execution of malicious code that allows the attacker to have control on the vehicle. As the vehicles are been integrated with more and more electronics and electrical devices, they are at risk of various cyber attacks. To cooperate with each other, these electronic devices require a communication channel, which can be wired or wireless. In terms of wireless devices, the most common systems prone to attacks are Remote Keyless Entry (RKE) and Passive Remote Keyless Entry (PRKE) systems. These days, almost every car has RKE used for unlocking/locking the car doors. However, there are several threats to wireless communication channels. Therefore, vehicle manufacturers need to attend security issues and give them a maximum amount of priority. This paper describes RKE, PRKE systems, attacks and threats related to communication channels and study of various symmetric cryptographic algorithms which can be used in the countermeasure of the threats.**

Keywords*—*Vehicular Security, Remote Keyless Entry (RKE), Passive Remote Keyless Entry (PRKE), Symmetric Cryptographic Algorithm.

I. INTRODUCTION

The automobile industry is one of the fastest-growing industries that has been contributing significantly to the world's economy. Modern-day vehicles are growing increasingly connected, with capabilities to sync with mobile phones and other facilities too. Along with many advantages that connected vehicles provide, they have also created more opportunities for hackers to hack or steal vehicles. Many well know car manufacturers' cars have been hacked and exploited successfully. Volkswagen (VW) vehicles were discovered to have flaws with RKE that would enable attackers to unlock VW vehicles. In 2015, security researchers Charlie Miller and Chris Valasek hacked a Jeep Cherokee and took control of it and forced it to stop in the middle of traffic. Also, Chinese researchers demonstrated their ability to remotely hijack the brakes of Tesla Model S.

For achieving ever-present computing wireless networking plays an important role. The network devices embedded in environments provide continuous connectivity and services, and hence improving the quality of life. Radio-Frequency Wireless Identification service which is used to bind devices with a unique serial number and encoded within a tag. RFID uses radio frequency to communicate between the tag attached on a device and RFID reader that identifies the unique RFID tag which can be used for identifying and tracking the implanted object. RFID's don't just denote EPC tags, but a wide spectrum of wireless devices or varying capabilities. Higher-end RFID devices can offer cryptographic functionality and can support the authentication protocol. Modern cars embed complex electronic systems to improve driver safety and comfort. Areas of serious public and manufacturer interest include access to the car (i.e. entry within the car) and authorization to drive (i.e., start the car). Key fob, which may consist of mechanical part is used to lock and unlock the car by sending radio frequency to the car transceiver.

Our contributions. There are three main contributions in this paper. First, from the perspective of an attacker, different types of attacks related to vehicle locking mechanism are discussed. The classification chart can be used to identify the type of attacks. Second, we present different types of keys used in vehicles in detail. Third, we elaborate on the different cryptographic algorithms for RKE security mechanism.

Organization of the paper. Rest of the paper is organized as follow. Section II describes the background and related work. Section III lists the different types of keys. Section IV list the possible threats on Remote Keyless Entry (RKE). Section V describes the symmetric cryptographic algorithm and followed by the conclusion in Section VI.

II. BACKGROUND WORK

Zeinab et al. have provided an up-to-date review on attacks related to the communication of devices and described how to avoid them. They have proposed a three-layer framework (communication, sensing, and control) through which automotive security threats can be understood. They explained individual attacks that are performed on each of the three layers. Glocker et al. proposed a challenge-response based authentication protocol for the RKE system. They used Symmetric-key cryptography. Leferink et al. described the vulnerability of Remote Keyless Entry Systems against Pulsed Electromagnetic Interference. They concluded that remote keyless entry systems are highly vulnerable to pulsed interference as compared to continuous interference. They proposed an improved receiver design which consists of synchronous receivers, which are not very sensitive to pulsed interference. Verdult et al. have shown several vulnerabilities in Hitag2 transponders that enable an adversary to retrieve the secret key. They proposed three attacks that extract the secret key under different scenarios. They have implemented and successfully executed these

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

attacks in practice on more than 20 vehicles of various make and model.

III. TYPES OF KEYS

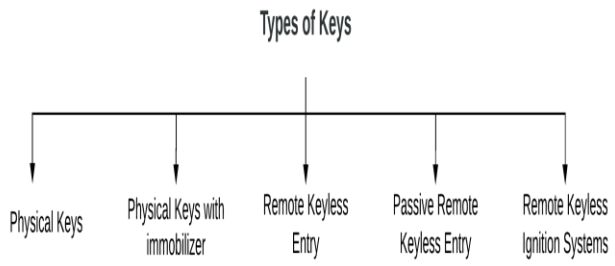

Fig 1: Types of Keys

1. Physical Keys:
Physical Keys were traditionally used, providing methods of access and authorization and lock systems, whereby inserting an accurate key into the door and ignition locks, the user was ready to enter and drive the car. [4] Within the last decade, this technique has been replaced with remote access in which users are ready to open their car remotely by pressing a button on their key fobs. These systems, granted authorization to drive mainly on basis of a physical key and lock system.

2. Physical keys with immobilizer:
Physical keys with immobilizer chips are used to stop key copying. A key with an immobilizer has a metal key rather than an immobilizer (RFID transponder) embedded into the plastic part of the key. The immobilizer communicates

with the steering column to enable the fuel injection system. [4] The immobilizer is a passive device that uses electromagnetic induction from interrogation signals transmitted by the reader. This system was created to prevent car thefts such as hot wiring because the car won't start unless it has successful authentication by the RFID chip.

3. Remote Keyless Entry (RKE):
An RKE is some kind of an electronic lock which is alternative to using a traditional mechanical key that controls access to a building or vehicle. A Remote Keyless Entry System consists of a key fob and a car transceiver that locks and unlocks the vehicle. The user presses a button on the key fob to lock or unlock the car instead of locking or unlocking the car with a traditional key. The key fob mainly consists of an RKE antenna, RF transponder, immobilizer, buttons and battery for power supply. RKE mainly uses Radio Frequency Identification (RFID) for its working. The RKE systems mostly work on frequencies (433/315/868 MHz). Whenever the user presses a button on the key fob, a signal containing some data is sent to the receiver in the car over a frequency. After that, the data is checked and compared by the receiver in the car and certain actions are performed (locking/unlocking) car doors.

4. Passive Remote Keyless Entry (PRKE):
Passive Remote keyless entry (PRKE) is an automotive security system that operates automatically when the user is in proximity to the vehicle. It can unlock the door on approach or when the door handle is pulled and can also lock it when the user walks away from the car on exit. The user can store PRKE device in the pocket or bag, unlike a standard Remote Keyless Entry (RKE) device, which requires the user to hold the device and press a button to lock or unlock the vehicle. Passive keyless entry systems typically involve an RF (radio frequency) key fob but there are also smart cards and mobile apps designed for PRKE. To detect each other the PRKE key fob and the vehicle module both contain transceivers that communicate wirelessly. The transceiver in the vehicle sends encoded messages continuously and when key fob is in its range it responds. To open the doors the encrypted messages must be correct and they identify the vehicle and key fob. PRKE also provides a feature of keyless start of vehicle, where the driver requires to simply push a button to start the ignition.

5. Remote Keyless Ignition Systems (RKI):
Remote Keyless Ignition Systems (RKI), also called Passive Keyless Entry and Start Systems (PKES) or Smart Key, are devices that have the capabilities of an RKE but also do not require metal to start the car. In this system, the car owner must have the key in their pocket to unlock the door without pressing any button on the key. Some cars require that the key fob be placed in the ignition slot, while others just require it to be inside the car to start the ignition. There is a security risk for the "automatic" car unlocking or ignition because an attacker may be able to steal the car when the car owner is nearby (i.e. filling up fuel or loading the trunk).

IV. TYPES OF ATTACKS

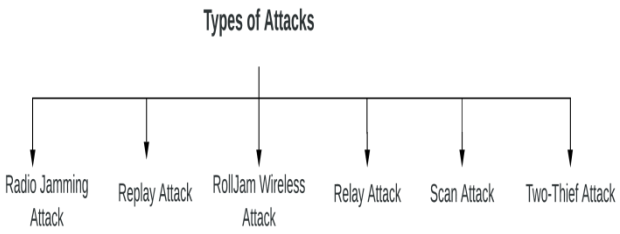

Fig 2: Types of Attacks

1. Radio Jamming Attack:
Most communication signals are vulnerable to attacks that disrupt synchronization which is done by jamming or denial of service attacks. Jamming uses continuous radio signals to cause disturbance in the communication device. The communication devices remain occupied and the transmitter stops the transmission when it senses the receiver is busy or has received a corrupted signal. Typically jamming attacks are classified in two categories: active jamming and passive jamming. An active jammer's goal is to keep the channel busy regardless of whether the channel is being used or not.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

For example, the attacker can continuously send strong radio signals to increase the signal-to-noise-plus-interference ratio at the receiver side. A passive jammer on the other hand observes the channel activity and starts jamming only when the channel is being used. This is a relatively easy attack which jams the locking signal from the key to lock or unlock the car. The attacker just needs a transmitter that transmits garbage code at an equivalent frequency because the key fob to jam the signal. The attacker must be close enough to the car so as to jam the signal. For this attack, the attacker can't start the car, but they will steal any possession left within the car by the owner. Most cars make a specific sound and/or flash their lights once they are locked using the fob, so the owner of the car should notice when the car doesn't lock successfully which undermines this attack.

2. Replay Attack:
A replay attack is a category of network attack in which an attacker detects a data transmission and fraudulently has it delayed or repeated. The delay or repeat of the data transmission is carried out by the sender or by the malicious entity, which intercepts the data and retransmits it. In other words, a replay attack is an attack on the security protocol using replays of data transmission from a different sender intended into the receiving system, thereby deceiving the participants into believing they have successfully completed the transmission of data. Replay attacks help attackers to gain access to a network, gain information or complete a duplicate transaction. A replay attack is also known as a playback attack. In replay attack the frequency sent by the victim is captured by the attacker and the replayed back. The frequency used to open the car locks when captured and replayed back will open the car lock even if the victim is not present at that moment. Hackers employing replay attacks do not necessarily need to decrypt original signals, since they are only intercepted and re-transmitted. As the original data typically comes from an authorized user, the network's security protocols treat the attack as if it were a normal data transmission.

3. RollJam Wireless Attack:
The RollJam hack was created by Samy Kamkar. The RollJam device is available for $32. It is a radio device that's designed to overcome the "rolling codes" security in keyless entry systems, alarm systems, and garage door opening systems. Rolling codes solved the problem of fixed codes. These are random generated codes which solved the issue of the replay attack. Still, hackers found vulnerabilities in rolling code generation systems, leading to rolling jam attacks. The RollJam is performed by placing the radio device which is supposed to be hidden on or near the target vehicle or garage, waiting for the legitimate user to use his/her key. The fob won't work on the primary try but will unlock or lock the vehicle on the second try. The RollJam first jams and stores the primary signal or first signal sent from the key fob and fails to unlock the door; therefore, the user naturally presses the button again. On the second press, the RollJam again jams the signal and stores the second code and broadcasts its first code, unlocking the door. The user is not aware of the malicious activity being performed. The RollJam attacker can then return at any time to retrieve the device and replay the intercepted code from the victim's fob to unlock the car or garage. It will unlock the car because the second code sent is still unused and unique.

4. Relay Attack:
Passive Keyless Entry and Start (PKES) systems allow the driver to lock and unlock the car by keeping the car key fob in his/her pocket. There are two variants of physical-level relays, wired and wireless. In a basic relay attack, messages are relayed from one location to another to make one entity appear closer to the other. Samples of relay attacks have been shown on MasterCard transactions and nodes between wireless sensor networks (WSN). The attack consists of first demodulating the signal, transmitting it as digital information using RF then, modulating it near the victim tag. Therefore, the attackers can gain access and authorization to start and drive the car without the ownership of appropriate credentials. The described relay attack is not easily traced, unless the car keeps a log of recent entries and records exchanged signals (e.g., for later analysis). Similarly, it will be difficult for the owner to prove that he/she is not the one that opened and used the car since we cannot track down the physical entry of the person.

5. Scan Attack:
This type of attack is the simplest one. A scan attack is critical for systems that use a rolling code technique. A rolling code technique is sending a different code to the transceiver each time when the button on the key fob is pressed. In this attack different codes are sent to the car transceiver as long the sent code matches with code of car transceiver. The time taken to unlock the car with this attack "depends on the number of bits used for code-generation method, and the number of trials conducted by the intruder".

6. Two-Thief Attack:
The Two-Thief Attack is the most known attack. In this attack, one thief stands next to the car while the other one stands next to the car owner. Assume that the car owner is a hundred meters away from the car. Both thieves use devices to amplify signals. The door handle is pulled by the thief who is near to car. By pulling the door handle, the car transceiver sends an interrogation message to the Customer-Identification Device (CID) which is like a key fob, kept in the car owner's pocket. The amplifier of the thief standing next to the car amplifies the signal so that it can be received by the amplifier of the thief that stands next to the car owner, though the CID is outside the transmission range. After amplifying, it will be forwarded to the CID. The CID responds with a valid code that will be transmitted to the car transceiver over the amplifier devices of the thieves.

V. CRYPTOGRAPHIC ALGORITHM

1. AUT64 cipher:
AUT64 is a block cipher of 64-bit with 120-bit of secret key used for RKES system i.e. remote keyless entry systems. The cipher is closed source and proprietary and hence was

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

reverse engineered to crypto-analyze it. AUT64 was identified to be a proprietary block cipher and was found to be used in most Volkswagen. AUT64 was the reverse engineered from the Mazda "Module 142" immobilizer system. The firmware was recovered from the Motorola MC68HC05B6 microcontroller used in this immobilizer box using a standard programmer. Then, the firmware binary was loaded into the IDA Pro disassembler to perform analysis. All of the important cryptographic subroutines were located and the AUT64 algorithm and protocol was reconstructed. The figure below shows the AUT64 Feistel network construction and Feistel function used for cryptographic purpose.

2. KeyLoq algorithm:
KeeLoq algorithm is currently used rolling code concept for locking and unlocking vehicles. The algorithm is embedded into HSC301 chip. It transmits 66-bit data to the receiver with first 34-bit data not encrypted and remaining 32 bits encrypted with the key size of 64-bit. While this approach prevents the replay attack in the system, it may lead to other passive or active attack. Two considerations are taken into account: double encryption is made in the last 32-bit data and single encryption is made in the last 64-bit data. The symmetric cryptographic approach is considered for encryption and decryption process. The same 64-bit key is considered for the entire process.

3. Secret Unknown Cipher:
Unclonable unit such as Physical Unclonable Function (PUF) has been used for authentication and key storage. A PUF uses physical diversity within each object and produces unique and unpredictable mapping to each response. The responses of PUF are unpredictable as it depends on operating conditions such as voltage, temperature and radiation. Secret Unknown Cipher (SUC) is a self-created internal permanent digital structure which can encrypt and decrypt, where aging effects are negligible, and hence, they are consistent in the whole lifetime of digital products. In SUC creation process, one unknown irreversible cipher from a vast library of theoretically infinite classes of ciphers is installed in SUC, which can process key derivation, encryption or decryption, authentication code and similar cryptographic operations.

4. Playfair Cipher:
The Playfair is a substitution-based cipher. It consists of two steps. The first step is to generate the Key Square (5*5). It is a 5*5 grid which includes alphabets and will act as the key. Each of the 25 alphabets must be unique. The starting alphabets in the grid are the alphabets that are in the key and in the order in which they appear. The second step includes the algorithm to encrypt the given plain text. The plain text is split in pairs of two and if there exist an odd string, then Z is added at the end of the letter. There are certain rules for encryption.

- If both letters are in the same column then take the letter below each one.
- If both letters are in the same row then take the letter to the right of each one.
- If rule 1 and rule 2 are not satisfied then form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

The problem with Playfair Cipher is that it can be easily exploited with the aid of frequency analysis, if the language of the plaintext is known.

There are other symmetric cryptographic algorithms available which can be used to provide security to RKE. Some algorithms might be fast but lack safety factor. Other algorithms like Triple Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, Twofish, International Data Encryption Algorithm (IDEA) can be tested with RKE to analyze time, space and safety factors.

VI. CONCLUSION

In this paper, we described the RKE and PRKE systems, along with various attacks being performed against the locking car mechanism that are threats to vehicular security. Attacks on wireless networks\frequency in various ways have effects that are significantly different. For instance, a radio jam attack will not allow the attacker to steal any kind of possession. On the other hand, a roll jam attack can be more dangerous in terms of stealing and controlling the functionality of the fob. In summary, different attacks are designed for different technology (working on the fob), some attacks may be hard to detect; a powerful attack will certainly result in more loss of the victim. There are many more attacks available on the car locking mechanism or zero-day attack can be found anytime on any technology. It is seen that RKE is vulnerable in terms of communication medium used i.e. wireless and also there is a limitation of the cryptographic algorithms to be used. The more the cryptographic algorithms used, the more will be the cost and power consumption of devices in which it is to be integrated. Besides, hacking the key fob jamming the signals is also a common way to gain access to vehicle. PRKE systems also are vulnerable due to the increased connectedness of a car to the internet. Vehicle thefts are mostly done by exploiting the weaknesses in the infotainment, navigation systems.

ACKNOWLEDGEMENT

We express our sincere thanks to our Seminar Guide Prof. Santosh Sambare for his encouragement and support throughout our seminar, especially for the useful suggestions given during the course of seminar and having laid down the foundation for the success of this work.
We would also like to thank our Research & Innovation coordinator Prof. Dr. Swati Shinde and Seminar Coordinator Prof. Pallavi Dhade for their assistance, genuine support and guidance from early stages of the seminar. We would like to thank Prof. Dr. K. Rajeshwari, Head of Computer Engineering Department for her unwavering support during the entire course of this seminar work. We also thank all the teaching and non-teaching staff members for their help in making our seminar work successful. We also thank all the web communities for enriching us with their immense knowledge.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

REFERENCES

[1] Danesh J. Esteki. "Requirements for Keyless Jamming Mitigation", 2011.
[2] Tobias Glocker and Timo Mantere. "A Protocol for a Secure Remote Keyless Entry System Applicable in Vehicles using Symmetric-Key Cryptography", arXiv:1612.00993v1 [cs.IT], 3 Dec 2016.
[3] Stefan van de Beek and Frank Leferink. "Vulnerability of Remote Keyless-Entry Systems against Pulsed Electromagnetic Interference and Possible Improvements" In IEEE Transactions on Electromagnetic Compatability, 2016.
[4] Roel Verdult and Flavio D. Garcia. "Gone in 360 Seconds: Hijacking with Hitag2" Radboud University, 2017.
[5] Jinita Patel and Manik Lal Das. "On the Security of Remote Key Less Entry for Vehicles", In IEEE International Conference on Advanced Network and Telecommunication Systems (ANTS), 2018.
[6] Vanesa Daza and Xavier Salleras. "LASER: Lightweight And SEcure Remote keyless entry protocol", 2019.
[7] P. Kartik and P. Shanthi Bala. "A new design paradigm for provably secure keyless hash function with subsets and two variables polynomial function", 2019.
[8] Zeinab El-Rewini and Karthikeyan Sadatsharan. "Cybersecurity challenges in vehicular communictaions", 2019.
[9] Juan Wang and Karim Lounis. "CSKES: A Context-based Secure Keyless Entry System", In 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), 2019.
[10] J. Ad Hoc "Jamming and Anti-jamming Techniques in Wireless Networks: A Survey", Ubiquitous Computing, 2017.
[11] Aur´elien Francillon, Boris Danev, Srdjan Capkun "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars", Department of Computer Science ETH Zurich 8092 Zurich, Switzerland, 2018.
[12] Madhumitha Sri Selvakumar, Rohini Purushoth Kumar, Gunasekaran Raja, "Effective Cryptography Mechanism for Enhancing Security in Smart Key System", Department of Computer Technology, Anna University, MIT Campus, Chennai, 2018.
[13] Christopher Hicks, David Oswald and Flavio D. Garcia, "Dismantling the AUT64 Automotive Cipher", 2018.