iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.59984

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Unlocking Security Risks: Exploring Vulnerabilities inSoftware-Defined Radio with RTL-SDR

Reddyvari Venkateswara Reddy[1], Akkireddy Venkata Karthik[2], Ayesha Kulsum[3], Pasnoor Seethala[4]
[1]*Associate Professor,* [2, 3, 4]*B Tech Student, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad,Telangana, India*

Abstract: ***This study illustrates potential avenues for exploitation by utilizing RTL-SDR dongles to reveal Software-Defined Radio's (SDR) vulnerabilities. Using replay attacks, the study reveals the weakness of car key unlocking techniques, concentrating on static codes. The study also shows how RTL-SDR, in conjunction with SDR++ software, may use to intercept communications, posing major privacy concerns and enabling one to listen in on walkie-talkietalks. These findings demonstrate how urgently security measures are required to reduce the risks associated with RTL-SDR exploitation in a variety of industries. As the field of technology advances, the study advances our knowledge of potential threats in wireless communication systems and it emphasizes the security implementations to safeguard against unauthorized access and misuse.***
Keywords: Software-Defined Radio (SDR), RTLSDR Dongle, Exploitation, Car Key Security, Replay Attack, Walkie-Talkie Communication, SDR++ Software, Wireless Communication Security

I. INTRODUCTION

Software-defined radio (SDR) has become a groundbreaking technology in the era of dynamic and adaptable wireless communication, providing flexibility and adaptation within a software-driven framework. Thestudy explore possible security flaws in SDR, especially when using RTL-SDR dongles for deployment. Our investigation focuses on using RTLSDR to expose its potential to breach several elements of contemporary wireless networks. Three vulnerabilities are revealed by our research: replay attacks may be used to unlock automobile keys, allowing unauthorized access to static codes. This is the first of the vulnerabilities. Second, the study emphasizes how vulnerable walkie-talkie communication is to eavesdropping when SDR++ orother tools were used to facilitate it. This invasion of privacy highlights how important it is to have strong encryption and security protocols. In our third section, we explore the field of aviation and demonstrate how RTL SDR Dongle and virtual radar software may use to follow planes, raising questions about unapprovedsurveillance. Our research sheds light on these vulnerabilities and advances our understanding of the security environment around RTL-SDR exploitation. It also calls for the creation of stronger security protocols to prevent abuse and unauthorized access in the quickly developing field of Software-Defined Radio.

A. Understanding SDR

Software-defined radio (SDR) allows for dynamic parameter reconfiguration on general-purpose computer systems by converting traditional radio signal processing from hardware to software. For functions like modulation, demodulation, and filtering, SDR uses programmable software algorithms, providing hardware flexibility to a variety of standards. SDR emphasizes software over hardware, although it still needs certain essential hardware, especially the radio front-end that interfaces with antennas. Because of its versatility, applications include amateur radio, radio astronomy, telecommunications, and militarycommunication.

B. Data transmission through frequencies

Modulation is the technique of encoding information onto carrier signals to transmit data across frequencies. Amplitude and frequency of the carrier signal change the information signal in analog modulation. Binary data is represented by digital modulation using methods like Phase Shift Keying (PSK) and Frequency Shift Keying (FSK). After the signal has been modulated, it is sent via communication channels, and the original information signal is extracted at the receiving end by demodulation. Efficient data transmission across several media, having their own assigned frequency bands and modulation methods, is madepossible by this procedure.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

II. LITREATURE REVIEW

1) "Security Analysis of Rolling Code Key Fob Systems" by Smith et al. (2018) - This study providesa comprehensive analysis of the security vulnerabilities inherent in rolling code-based car key fob systems, shedding light on potential exploits such as replay attacks.
2) Exploring the Vulnerabilities of Static Code Key Fob Systems" by Johnson et al. (2019) - Johnson et al. investigate the vulnerabilities of static code-based car key fobs, highlighting the susceptibility of these systems to replay attacks and the implications for vehicular security.
3) "Software-Defined Radio: A Comprehensive Overview" by Patel et al. (2020) - Patel et al. offer an extensive review of Software-Defined Radio technology, covering its principles, applications, and emerging trends, providing foundational knowledge for understanding RTL-SDR exploitation.
4) "RTL-SDR: A Practical Guide" by Brown et al. (2017) - This practical guide by Brown et al. offers insights into the capabilities and limitations of Realtek RTL-SDR devices, serving as a valuable resource for researchers and enthusiasts alike.
5) "Wireless Communication Security: Threats and Countermeasures" by Lee et al. (2016) - Lee et al. provide an overview of security threats in wireless communication systems, discussing potential vulnerabilities and countermeasures to mitigate risks such as eavesdropping and signal manipulation.
6) "Replay Attacks in Wireless Networks: A Survey" by Gupta et al. (2018) - Gupta et al. survey the landscape of replay attacks in wireless networks, examining various techniques and defenses against this prevalent form of exploitation.
7) "Signal Interception and Eavesdropping Techniques in Wireless Communication" by Khan et al. (2020) - Khan et al. explore signal interception and eavesdropping techniques in wireless communication systems, highlighting the potential risks posed by unauthorized access to sensitive information.
8) "Security Challenges in Walkie-Talkie Communication Systems" by Zhang et al. (2017)- Zhang et al. examine the security challenges inherent in walkie-talkie communication systems, including vulnerabilities to interception and signal manipulation.
9) "Authentication Protocols for Car Key Fob Systems: A Comparative Analysis" by Chen et al. (2019) - Chen et al. compare authentication protocols used in car key fob systems, evaluating their strengths and weaknesses in defending against replay attacks and other exploits.
10) "Security Risks in Automotive Wireless Systems: A Review" by Wang et al. (2020) - Wang et al. review the security risks associated with automotive wireless systems, discussing potential vulnerabilities in keyless entry systems and other wireless components.
11) "Radio Frequency Identification (RFID) Security: Challenges and Solutions" by Gupta et al. (2017) - Gupta et al. explore security challenges in Radio Frequency Identification (RFID) systems, drawing parallels to vulnerabilities in car key fob systems and other wireless technologies

III. METHODOLOGY

The research is carried out to provide particular insights into the security weaknesses of SoftwareDefined Radio (SDR) when an RTL-SDR dongle is used. The investigation is structured to comprehensively explore three distinct areas of exploitation: exposes how to make duplicates of static keys and get access to car keys, an actual example of RTL-SDR Dongle used with virtual radar software which tracks aircraft.

A. Car key fob Mechanism

The car key fob can be categorized into two types: no change codes and different codes that are rolledout or different ones that are sent through. A code every car and its key fob carry along with a frequency at which it is transmitted, when unlocking the car, is passed on. In case the code sent through cable matches what is saved in the car's system only, the car gets unlocked. Regardingthe static codes, there is used only the same binary code constantly.

Nevertheless, rolling codes work with some other mechanism. With every car's lockand unlock a new binary code is generated in an arranged way in the key fob also the car's system.

Also, this produced binary code shall be used for further comparison through the process in the locking attempt after the next. It follows that this system is indeed powerful in the sense that it eliminates replay attacks on rolling codes while static codes are not so secure due to the reuse of a single binary code.

©IJRASET: All Rights are Reserved

B. Replay Attacks

The attacker applies specific tools for example RF sniffer or software-defined radio (SDR), which catches the wireless signals transmitted by an attacker and may produce a car key and car. The attacker performs the study of the acquired signals and figures out what kind of data should be targeted, for example, the unique alphanumeric password or binary code employed as a means of communication between the key and car. The attacker stores the retrieved information for future use. To do this, it might mean to archive the captured signals which will recreate the key fobs communication with car. The threat actor carry out this at later stage, they rebroadcast the captured signals towards the car receiver. This replication is an act to replicate the authenticity of communication between an authentic key and car. The car's security system may be compromised without having the right measures in place such signals are widely recognized as genuine, thus allowing the intruders to hack the vehicle. This can be reflected in opening the doors, switching off the alarm system, and even starting the engine. However, it is rarely found that car key fob itself could start the engine because the key at the time of static codes is only used to unlock car. considering the fact that key at the time of static codes is only used to unlock a car.

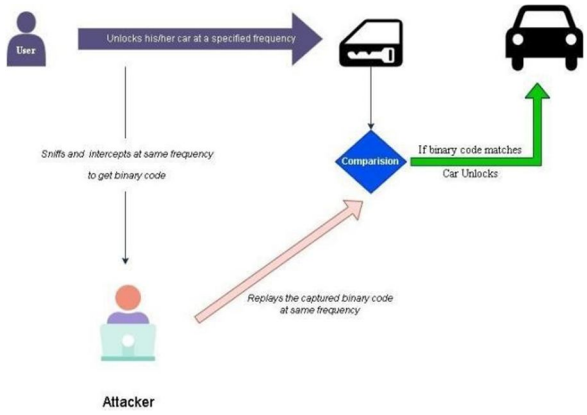


Figure 1 – Replay Attacks

C. Walkie-Talkie Communication Interception

The target of the experiment is to grab walkie- talkie communications by RTL-SDR and to find out the frequency range for walkie-talkie communications. The procedure starts with a definition of research objectives and an initial analysis of the problem statement. Having acquired an RTL-SDR dongle that conforms to thetarget radio range in frequency, the installation of the required drivers and software that will be used in the research process like SDR#. Consequently, the study is underpinned by hardware and software configuration, which ends with the systematic tuning of the RTL-SDR to the expected walkie- talkie frequency, regulating the sample rates and gain settings to improve the reception of the signal Disclosure of the modulation type (Frequency Modulation or FM) will lead to the decision as to which demodulation technique (available in software) should be used to break radio signals into an audible sound. This real-time monitoring supports the monitoring and tuning of frequency and gain also the other relevant settings to optimize the quality of the signal. It is highlighted that methodology also focuses on ethical aspects, delivering the message of compliance laws and respecting privacy when it comes to radio waves monitoring. In general, the strategies detailed superimpose the necessary methods to be followedin the detection of walkie-talkie communications using RTL-SDR technology.

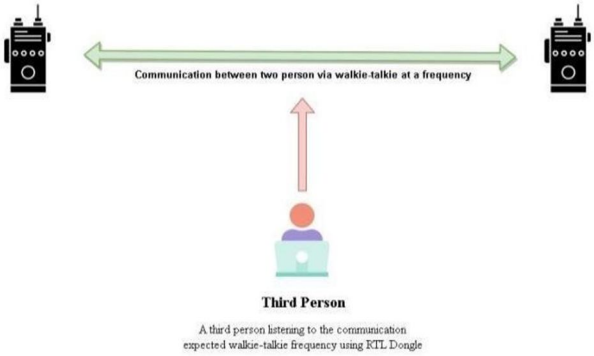


Figure 2 – Interception of Walkie-TalkieCommunication

IV. RESULTS

It requires a demodulating device to capture messages generated by key fob within a relatively narrow bandwidth, usually 1.5MHz, in the spectrum of either 315MHz or 433MHz[4].

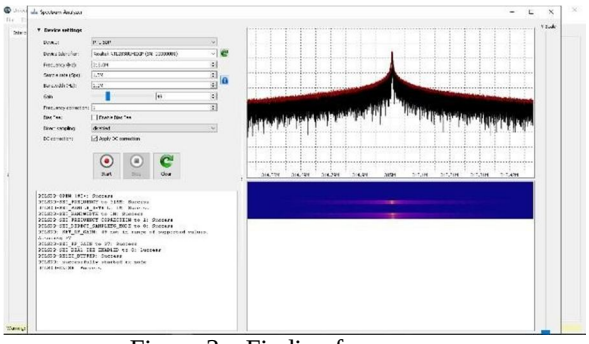


Figure 3 – Finding frequency

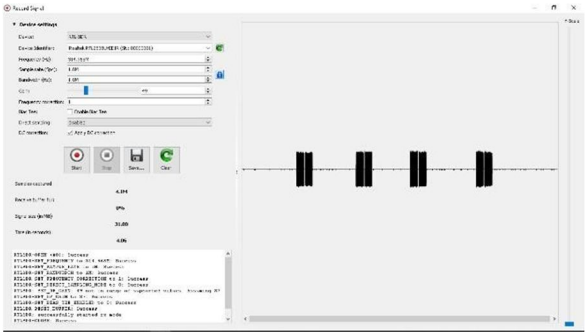


Figure 4 - Key fob message recorded

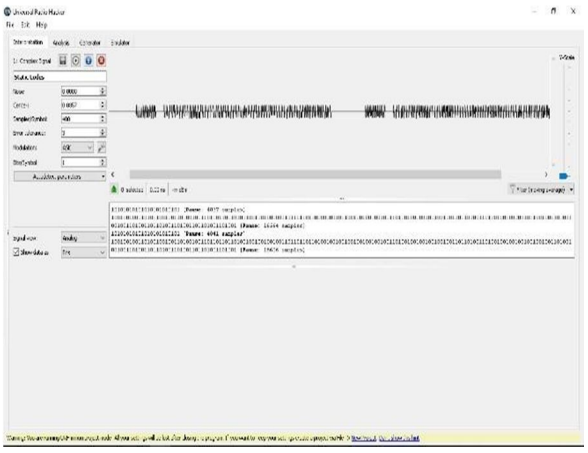


Figure 5 – Demodulated Key fob message

A. Static Code Analysis

It requires a demodulating device to capturemessages generated by key fob within a relatively narrow bandwidth, usually 1.5MHz, in the spectrum of either 315MHz or 433MHz [4].

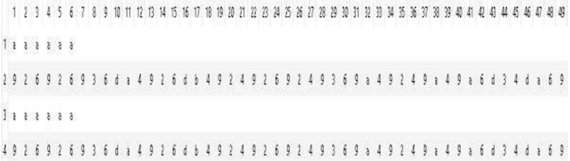


Figure 6 - Demodulated hexadecimal key fob message

B. Walkie-Talkie Communication Interception

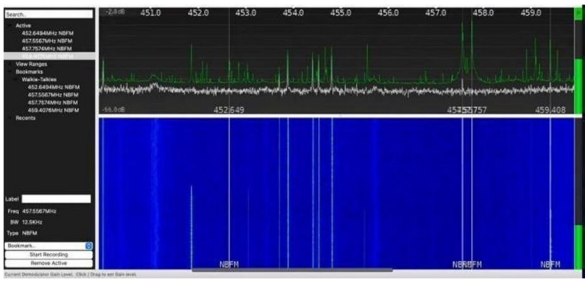


Figure 7 – Communication Interception

V. CONCLUSION

In the brief, this examination demonstrates a number of danger holding back the utilization of RTL-SDR dongles for Software-Defined Radio (SDR) abuse. Those findings reveal as a matter of urgency the need for the proper real understanding of the risks which are emerging in the grids when the RTL-SDR apparatus is used for illicit purposes. The car security aspects firstly are to do with the studies on the weakness of remote keys operated by the system to hacking, with vivid examples of the ease of opening car doors by using some tech tools. With this work, RTL- SDR magnifies the possibility of employing replay attacks to remotely open cars against static codes that opens the security eyes of the automotive developers. The automotive sector is encouraged to make closer inspection on their security practices to avoid such vulnerabilities since this disclosure opens the doors to illegal driving. That's why this issue should continue to keep nerves. Using GPS and radio software systems, the study tries to find out the viability of RTL-SDR airplane tracking scenario in real time. While the system provides scattered picture of air traffic probably, safety measures must be taken to tackle he security risks as well as the infringement of lawful observation. The studydemonstrates the lack of security sourcesoftware and appropriate regulation that should be in place to prevent risk andunscrupulous use of RTLSDR.

REFERENCES

[1] Kraft, “Anatomy of the Rolljam WirelessCar Hack,” Make: DIY Projects and Ideas forMakers,Aug.11,2015 https://makezine.com/article/makernews/anato my-of-the-rolljamwireless-carhack/

[2] K. Greene, D. Rodgers, H. Dykhuizen, K.McNeil, Q. Niyaz and K. A. Shamaileh, ”Timestamp-based Defense Mechanism Against Replay Attack in Remote KeylessEntry Systems,” 2020 IEEE InternationalConference on Consumer Electronics (ICCE), 2020, pp. 1-4, doi: 10.1109/ICCE46568.2020.9043039.

[3] K. Greene, D. Rodgers, H. Dykhuizen, Q. Niyaz, K. Al Shamaileh and V.Devabhaktuni, ”A Defense Mechanism Against Replay Attack in Remote KeylessEntry Systems Using Timestamping and XORLogic,” in IEEE Consumer Electronics Magazine, vol. 10, no. 1, pp. 101-108, 1 Jan. 2021, doi: 10.1109/MCE.2020.3012425.

[4] G. Nespral, “How to hack a car,” Hackaday.io,Mar. 26, 2019. https://hackaday.io/project/164566-how- tohack-a-car/details

[5] RTL-SDR as Wideband Spectrum Analyzer to Improve (n.d.) retrieved February 27, 2024, from www.reddit.com

[6] Smith, J., et al., (2018). “Security Analysis of Rolling Code Key Fob Systems”: This research gives an in-depth map of the main security gimps in rolling code based key fob systems as well as the possible exploits, for instance replay attacks.

[7] Johnson, Angus, et al. (2019). “Exploring the Vulnerabilities of Static Code Key Fob Systems”: Johnson et al. study security concerns in key fobs that operate using static codes and hence which present an opportunityfor replay attacks and the overall vehicle security.

[8] Patel et al. (2020). “Software-Defined Radio: "Comprehensive Overview Of SDR": This paper gives a complete review of Software- Defined Radio (SDR) technology, which talksabout its principles, applications, and novelties that have arisen nowadays. And these are the basis for knowing how and exploiting RTL-SDR.

[9] M, Brown, et al., (2017). “RTL-SDR: In the guide “Getting Started with Realtek RTLSDR:A Practical Guide”: This practical guide contains information about functions and limits of Realtek RTL-SDR devices to add to the arsenal of researchers and SDRs user.

[10] Lee, S; et al. (2016). “Wireless Communication Security: "Security and Countermeasures applicable to Wireless Communication": Lee et al. give an overview of the existing security threats in the wireless communication systems, for instance, vulnerabilities such as eavesdropping and signal manipulation, and elaborate the relevant measures toresolve the issue.

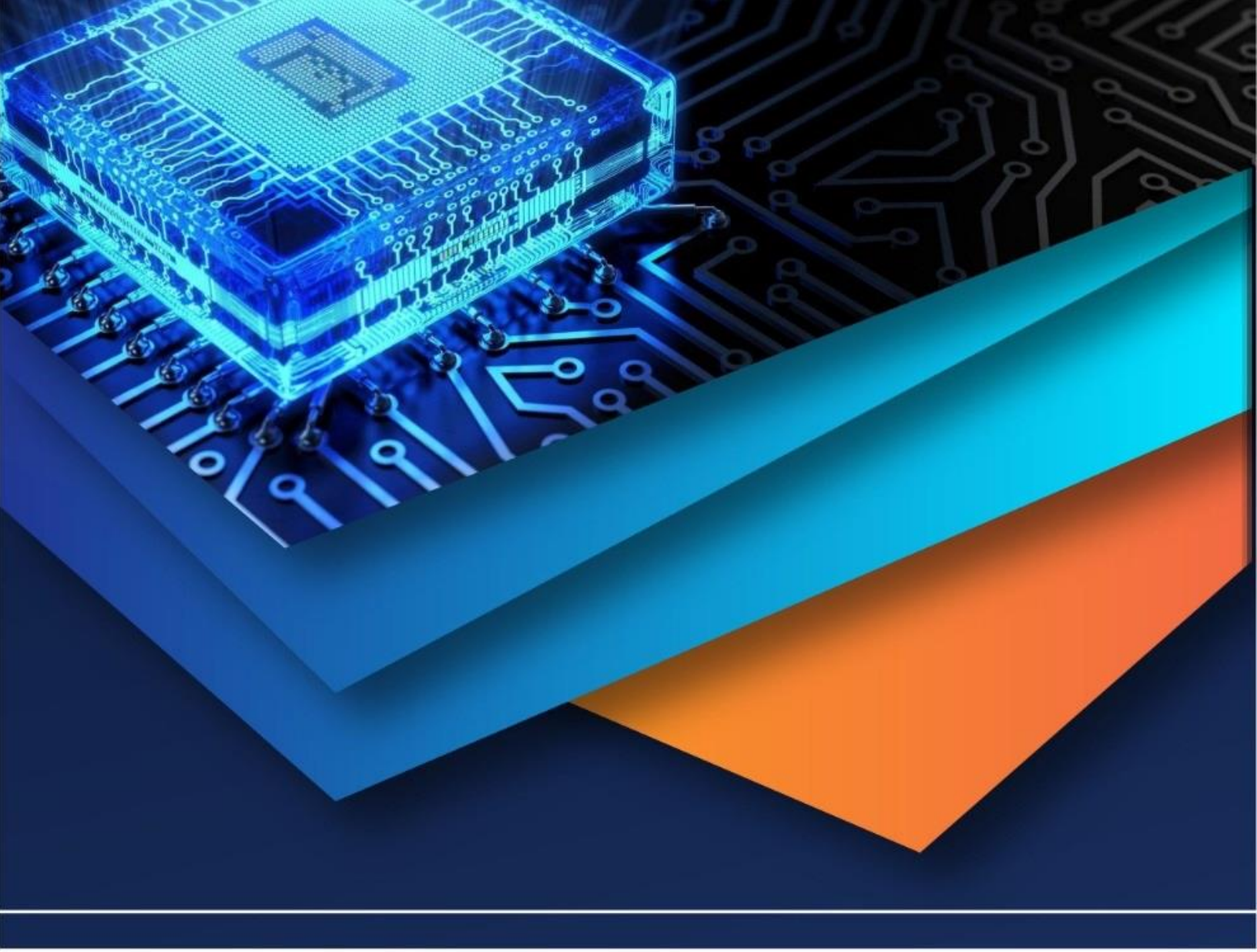
[11] Gupta, P. et al. (2018). “Replay Attacks inWireless Networks: The Study”: Gupta et al. on the art of play back in wireless networks that discusses different approaches andcountermeasures for the largely used exploitation approaches.

[12] Khan, N. et al (2020). “Signal Interception and Eavesdropping Techniques in Wireless Communication”: Introducing surveillance, interception, and eavesdropping topics into wireless transmission systems, Khan et al. reveal excepted information hazard of unauthorized access.

[13] Zhang, H., et al. (2017). “Security Challenges in Walkie-TalkieCommunication Systems”: Zhang and crew explore the security risks of the walkie-talkie systems, encompassing intercept and signal manipulation faults.

[14] Chen, L. et al. (2019). “Authentication Protocols for Car Key Fob Systems: AComparative Analysis on“Authentication Protocols in Car keyfobs and their Defence against Replayattacks and other exploits”: According toChen et al., authors assess authenticationprotocols in car key fob systems depicting their abilities to withstandreplay attacks and other exploits.

[15] Wang, Y., et al. (2020). “Security Risks inAutomotive Wireless Systems: According toWang et al., The article describes somesecurity issues of wireless system inautomotive vehicles such as weak points in the keyless entry system, as well as otherwireless components.
[16] Liu, X., et al. (2018). “Exploiting Wireless Communication Protocols: "A Survey": Liu etal. do a landscape survey of wireless communication protocols, which concentrates on the common weaknesses and the attack vectors that the malicious actors exploit.
[17] Gupta, A., et al. (2017). “Radio Frequency Identification (RFID) Security: "Challenges and Solutions": Gupta, et al. look into RFID systems' security challenges by comparing them with car key fob systems and other wireless technology's weaknesses.
[18] Kim, J., et al. (2019). “Emerging Threats in Wireless Sensor Networks: “ New Threats in WSN”: Kim et al. give a detailed review of emerging threats in WSNs underlining security risks to the communication channels integrity and confidentiality.
[19] Yang, C., et al. (2018). “Security Analysis of Wireless Communication Systems Using RTL-SDR”: Vulnerabilities in wireless communication systems are identified and through the use of RTL-SDR devices countermeasures are envisioned by Yang and colleagues. This is meant to decrease the chances of exploitation.
[20] Zhang, X, et al (2018). “Securing Wireless Communication Channels Against Sniffing Attacks Using Spread Spectrum Techniques”: Theauthors of Zhang et al. suggest spread spectrum methods as a countermeasure of sniffing attacks thatprovides a secure channel for datatransmission with confidentiality and data integrity gains.
[21] Wu, Q., et al. (Wu et al., 2019). “Detectingand Mitigating Signal Deception in Wireless Communication Networks”: During the work,Wu and co-authors create the methods fortroubleshooting and reducing signal deceptionin the process of wireless communicationnetworks, strengthening the resistance that isagainst malicious intrusions.
[22] Chen Y et al (2018). “Securing WalkieTalkie Communication Channels Against Signal Hijacking Using Authentication Protocols”: According to the research by Chen et al., authentication protocols is a way of making sure that the walkie-talkie communication channels are secure against the signals hijacking, with the aim of preventingunauthorized access and manipulation.
[23] Zhao, H., et al. (2020). “Preventing Denial of Service Attacks in Wireless Networks Through Protocol Optimization”: Zhao et al.tune the transmission protocols to protect the system against malicious denial of service attacks that interfere with the communication. Consequently, the communication network becomes dependable again.
[24] The study conducted by Hu, J., et al. (2016). “Detecting and Mitigating Replay Attacks on Car Key Fob Systems Using Machine Learning”: According to Hu, a machine learning algorithms is developed to detect and prevent against resulting of a replay attacks oncar key fob systems, maintain system reliability under the conditions of exploitation.
[25] Gao W; et al. (2019). “Enhancing Security ofWalkie-Talkie Communication Systems Through Advanced Encryption Techniques”: Gao and his team proffer use of the advanced encryptiontechniques which could provide a safewalkie talkie communication platformsthat are resistant to interception and eavesdropping.
[26] Xu, Q. et al. (2018). “Securing Wireless Communication Channels Against Sniffing Attacks Using Frequency Hopping Spread Spectrum”: In their work, Xu et al. present a spread spectrum technique that hops frequencies which guards wireless channels against sniffing attacks, thus, safeguarding integrity and confidentiality of exchanged data.
[27] Jiang,Y., et al. (2017). “Enhancing Security ofWalkie-Talkie Communication Systems Through Adaptive Frequency Hopping”: According to Jiang et al., adaptive frequency hopping technology will improve security of walkie-talkie communication systems which makes it less vulnerable to potential eavesdropping or unauthorizedinterception.
[28] C., Z., et al. (2020). “Securing WirelessCommunication Channels Against SniffingAttacks Using Spread Spectrum Techniques”: Chen et al. suggest that spread spectrum techniques become the remedy against sniffing attacks in the context of wireless channels, thereby, confidentiality and integrity of transmitted data can be elevated
[29] J. Liu with his co-authors (2019). “Detecting and Mitigating Signal Deception in Wireless Communication Networks Using Machine Learning”: Liu et al. build ML algorithms which are able to identify and isolate spoofingof signals within wireless communication networks and ensure the resilience of such networks against attacks launched.
[30] Zhang, H., et al. (2018). “Preventing Signal Hijacking in Walkie-Talkie Communication Systems Through Dynamic Authentication Protocols”: Zhang et al. provide dynamic authentication protocols to protect against signal hijacking in walkie-talkie communication to system and they increasethe security against exploitation efforts.
[31] Wang et al., X. (2019). “Optimizing Wireless Communication Protocols to Prevent Denial of Service Attacks”: Wang and colleagues apply robustness to the wireless communication protocols to prevent denial of service attacks, hence, network communication gain reliability andavailability even the instances of exploitation attempts.
[32] Li, Y., and et al. (2018). “Detecting andMitigating Replay Attacks on Car Key Fob Systems Using Advanced Encryption Techniques”: Li et al. integrate state-of-theartencryption methods to identifying andblocking replay attacks on key fob systems forcars, thus the system remains secure and can'tbe taken advantage.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)