INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 97-106

e-ISSN : 2583-1062

Impact Factor: 5.725

AN IOT BASED MULTI-PENTESTING TOOLKIT (MPT^2)

Kalash Jain A[1], Sachin S[2], Christ Jerold A[3]

[1,2,3]Department of Computer Science Rathinam College Of Arts And Science Coimbatore 0009, India.

DOI: https://www.doi.org/10.58257/IJPREMS33114

ABSTRACT

In recent years, the world is facing a common problem that the number of attacks is increasing day by day, as the technologies are developing increasingly. This project proposes a working model in which various sensors are incorporated to attack an organization and test the security score of the organization using IoT architecture. An Arduino microcontroller board is used to receive inputs from the sensors and then used to attack by modifying the UIDs if needed to test the security whether the network is vulnerable or not. The hardware device will continuously send the data from sensors to the network and capture for future analysis and development. The data will be monitored remotely through the Arduino IDE via the mobile application. If any vulnerability is present further decisions can be made in order to mitigate the risk and prevent it. In this, IoT is becoming a major platform for many services & applications, also using Node MCU not just as a sensor node but also a Wi-Fi controller here this paper proposes a generic attacking system as a step forward to the progress made in this department till now.

Keywords- Risk, Mitigation, Monitoring, Sensors, IoT hardware device, Attack

1. INTRODUCTION

Nowadays, the interest about IoT device for Multi - Pentesting purpose has increased a lot as it is connected over the internet and devices can be inter – connected through various IoT devices such as Node MCU, RFID, sensors … etc. It has also become important to enhance the hardware with software in order to tackle the futuristic attacks that are happening through the networks and organizations. This will help us improve the overall security as well as prevent and mitigate the risks.

Overall, the goal of security IoT is to improve the quality and efficiency of organizations security, reduce costs and enhance the compliance score. An IoT-based security system has the potential to mitigate risks and remove threats of the organization

This system would utilize Internet of Things (IoT) devices to continuously send and receive data from sensors and provide real-time data to security professionals. This would allow for earlier detection of vulnerabilities and prompt intervention, leading to improved patient outcomes. Additionally, the system could also provide security professionals to enhance and also change the hardware based on their need and choose an option for which they are testing. The aim of this project is to design and implement an IoT-based security system to enhance the quality of the network over the organization through improved monitoring and management of the networks.

1.1. Motivation

The growing use of IoT devices for multi-pen testing is indicative of how digital systems are becoming more and more interconnected. Organizations today use IoT devices like RFID, sensors, and Node MCU, which calls for hardware-software coordination to fend off future network threats. To improve overall organizational security and compliance, it is critical to strengthen security, proactively identify vulnerabilities, and minimize risks. This drive is a result of the necessity to adjust to the more complicated networks brought about by the various entry points that Internet of Things devices introduce. The proposed Internet of Things (IoT) security system aims to offer round-the-clock surveillance and facilitate instantaneous data sharing between security experts and sensors.

By taking a proactive stance, weaknesses can be identified early on, enabling timely intervention and better patient outcomes. Furthermore, because of the system's flexibility, security experts can change the hardware to meet testing specifications. The project's ultimate goal is to develop and deploy an Internet of Things (IoT)-based security system that improves network quality by means of improved monitoring and administration, meeting the changing demands of the networked digital environment.

1.2. Contribution

An IoT-based security system's value for multi-pen testing is found in its capacity to handle the complex problems that the growing IoT ecosystem presents. First off, by offering a proactive method for promptly detecting and addressing weaknesses, the system enhances security. It strengthens an organization's overall security posture by drastically lowering the probability of security breaches through early detection and constant monitoring.

Second, the hardware's versatility and modification help provide the flexibility required to counter new threats.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 97-106

e-ISSN : 2583-1062

Impact Factor: 5.725

Security experts can adjust and improve the system in accordance with certain testing specifications, guaranteeing that the security infrastructure is resilient against changing cyberthreats.

The system's ability to provide ongoing data interchange between security experts and IoT devices is another noteworthy feature. Quicker reaction times are made possible by this real-time information flow, enabling timely intervention in the event of possible security threats. This enhances patient outcomes in addition to increasing the effectiveness of security measures, particularly in industries where prompt reactions are essential.

2. PROJECT OVERVIEW

A. Scope of the project

The Internet of Things (IoT) and Security have the potential to greatly improve the IT sector by allowing for better risk analysis, threat mitigation, incident responses .

1) Custom firmware development for better use of the hardware and extend its abilities for tailor specific projects.
2) Radio Signal Analysis to decode various signals from different frequencies and wireless signals.
3) Security testing and penetration testing for analyzing and exploiting various systems, networks and wireless frequencies with various other wireless communication protocols.
4) Automation and Scripting to enhance the functionality of the tool
5) Cost Savings: By reducing the cost of the hardware and the existing system and providing it to the security team of the organizations for a reasonable cost.

3. INTERNET OF THINGS(IOT)

IoT (Internet of Things) design is the process of designing connected devices and systems for the Internet of Things. It involves defining the requirements, Overview of Proposed system selecting the components, creating the architecture, and developing the software and firmware that runs on the devices. A multi-Pentesting attacking system is an IoT-based platform that enables security professionals to monitor the compliance score and report that data to officials in real-time.

The system typically consists of a set of sensors and other hacking devices that are connected to Arduino IDE platform using wireless communication technologies such as Wi-Fi or Bluetooth. Security professionals can use the system to track

the risks and vulnerabilities of the organization and its network. If the organization finds any vulnerabilities, then it can make decisions on further patches and what should be done in order to mitigate this risk. Also, the organization can keep a track i.e., monitor its system regularly in order to overcome the risks and threats which can lead to a data breach.

The system can be useful for scanning vulnerabilities in RFIDs (Radio Frequency Identification), RFs (Radio Frequency), Wireless Communication, Bluetooth and SDR (Software defined radio) modules.

The way this can be used is the security professionals can keep the hardware with them and start to choose what kind of module they are using whether be it RFID, RF, SDR, Bluetooth or Wi-Fi Module. Once the module is selected for the attack the script will automatically start running the attack and get the data in the Arduino IDE. This data can then be used to change UIDs and other IDs to make further attacks in the future. Thus, frequencies can be managed and proper system can be developed to remove the risks over the network.

4. HARDWARE MODULES

Remote monitoring through Arduino IDE.

SDR module is used for better range and tampering all frequencies.

In proposed Arduino microcontroller is used 4. Bluetooth module is included.

HARDWARE MODULES:

- NODE MCU
- RFID
- RF
- Bluetooth Module
- SDR Module

1) Node MCU (ESP8266)

The ESP-12E module, which houses the ESP8266 chip with Tensilica Xtensa 32-bit LX106 RISC microprocessor, is included with the NodeMCU ESP8266 development board. This microprocessor runs at a flexible timepiece frequency

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 97-106

e-ISSN : 2583-1062

Impact Factor: 5.725

of 80 MHz to 160 MHz and supports RTOS. For storing data and programs, NodeMCU contains 4 MB of Flash memory and 128 KB of RAM. It is perfect for Internet of Things systems due to its powerful processing capacity, integrated Bluetooth and Wi-Fi, and deep sleep operating features. VIN leg (External Supply Leg) and Micro USB jack can be used to power NodeMCU. It has I2C, SPI, and UART interface capability.

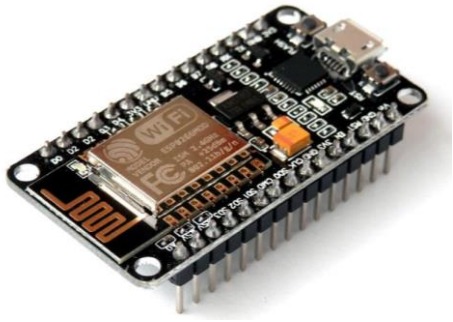

Figure 1 NODE MCU

2) RFID

Electromagnetic fields are used in radio-frequency identification to automatically detect and track markers affixed to items. A radio receiver, transmitter, and bitsy radio transponder make up an RFID system. The label transfers digital data, typically a related force number, back to the anthology when it is triggered by an electromagnetic interrogation palpitation from a nearby RFID anthology device.

Figure 2 RFID

3) RF

RF Radio Frequency detectors and communication are foundation to ultramodern day telecommunications. From having to shoot letters by bottom or boat to long distance calls by telegraph, all dispatches had a significant detention. The RF signals are entered through a software- controlled radio receiver also transmitted into the tackle to capture the data. It's used for radio dispatches including Wi- Fi, Bluetooth, cellular networks and further.

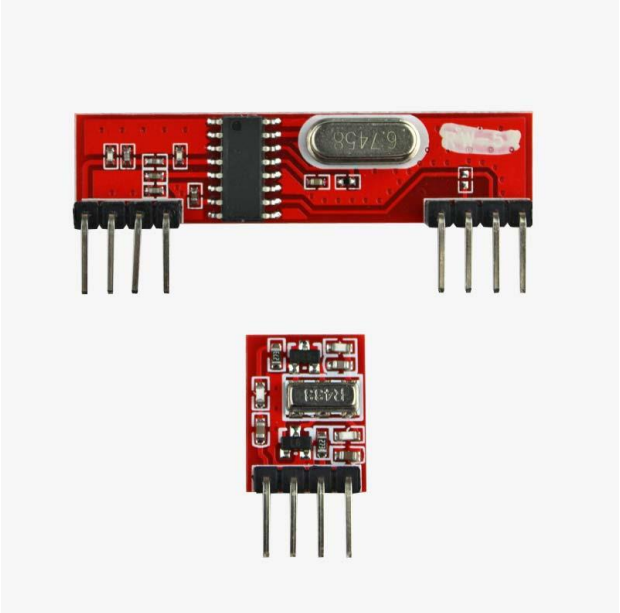

Figure 3 RF Transmitter and Receiver

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 97-106

e-ISSN : 2583-1062

Impact Factor: 5.725

4) Bluetooth Module

Bluetooth is a type of wireless technology wherein a low range frequency is used in order to communicate to send and receive data over the devices. It was first mainly developed for audio streaming but with the emergence of IoT, Bluetooth integration made it possible for tracking and monitoring for data analysis captured through IoT. It communicates by internal antennas that allow remote communication over the devices. The Bluetooth system is also known as piconets, as they rely on a master/slave system. The ability to tamper into Bluetooth can lead to data breach of sensitive information such as images, SMS … etc.

Figure 4 Bluetooth Module

5) SDR

Software Definition Resources, or SDR A communication system known as radio has been created using analog electronics. Hardware includes detectors, modulators, demodulators, amplifiers, filters, and mixers all employ it. Either an analog-to-digital converter or an embedded system is used to implement it. It serves a wide range of dynamic radio protocols in real time and is highly useful for the military and cellular phone services.

Figure 5 SDR

5. SOFTWARE MODULES

Arduino IDE

Arduino IDE is a free open source software wherein code for different hardware can be run for testing.

It is mainly used to simulate electronic items of how they work and it is best used for prototyping various components for electronic projects.

It simulates the whole project in the virtual environment and when its ready the code can be easily uploaded to the hardware efficiently optimizing the resources and managing the storage.

Also, the data can be easily monitored and preprocessed using the Arduino IDE.

6. EXISTING SYSTEM

The race to launch satellites has prompted new commercial and amateur operators, but lack of regulations and standards has led to unprotected solutions. Hacking satellite connections can significantly impact society and businesses. Research shows that cheap software-defined radios can listen and attack these connections without thorough domain knowledge. This research aims to build awareness of attack methodology against satellite connections for robust, secure communication solutions.

The increasing number of IoT devices and Bluetooth technology has led to a need for protection against malware and data theft. BlueZ's Bluetooth File Transfer Filter (BTF) can block unauthorized transfers, protecting devices like smartphones, tablets, and laptops. However, the Bluetooth worm poses a threat. A Bluetooth OBEX Proxy (BOP) is proposed to filter malicious files, preventing illegal transfers and protecting devices with various Linux distributions.

7. PESUDO CODE

1. Include necessary libraries:

a. RCSwitch for RF communication.
b. SD for SD card functionality.
c. SPI and MFRC522 for RFID communication.
d. IRLib for IR communication.

2. Define pin configurations:

a. SD_CS_PIN for SD card chip select.
b. IR_RECEIVE_PIN for IR receiver.

3. Initialize RCSwitch object for RF communication.

4. Define outputRF function:

a. Display information about received RF signal.

5. Define setupRRF function:

a. Enable RF receiver on interrupt 0 (pin #2).

6. Define loopRRF function:

a. Check if RF signal is available.
b. If available, call outputRF function with received signal details.

7. Initialize RCSwitch object for RF transmission.

8. Define setupSRF function:

a. Enable RF transmitter on pin #10.
b. Set pulse length and protocol for RF module.

9. Define loopSRF function:

a. Send a binary RF signal "000101010101000101010101" every second.

10. Initialize MFRC522 object for RFID communication.

11. Define setup_RFID function:

a. Initialize MFRC522.
b. Dump version information.

12. Define read_RFID function:

a. Reset loop if no new card is present.
b. Read card serial and dump debug info.

13. Initialize IRsendRaw object for IR transmission.

14. Define setupIRSend function:

a. Display a message.

15. Define loopIRSend function:

a. Send IR signals rawDataON and rawDataOFF with delays.

16. Define setupIRRev function:

a. Begin SD card.
b. Open the file "received_signal.txt".
c. Read lines from the file.
d. Extract raw data and send IR signal.

8. PROPOSED SYSTEM

For penetration testers, hardware aficionados, and security experts, we created the MPT^2 (Multi - Pentesting Tool kit) device. This small gadget has a lot of characteristics, such as the capacity to simulate different cards and devices for security testing, as well as radio frequency (RF) capabilities and an infrared transmitter.

RFID Emulation and Hacking: Users can test and evaluate the security of RFID systems by using the MPT^2, which

can imitate different RFID cards. RFID signals can also be recorded and replayed.

Infrared (IR) Transmitter: The device has an IR transmitter, enabling it to control and interact with IR-controlled devices such as TVs, air conditioners, and more.

Wireless hacking: The MPT can communicate with many wireless protocols, including Bluetooth and Wi-Fi, which makes it possible to test and examine these technologies' security.

Hardware Hacking and Debugging: It can be used for hardware hacking and debugging tasks because it has GPIO pins and can function as a JTAG and UART interface.

Radio hacking: The Flipper Zero is a powerful tool for examining and tampering with wireless communication because it can interact with a variety of radio frequencies.

User Interface: For user engagement, the device usually has a small display and a few buttons. Users are able to choose between various modes and functions using the interface.

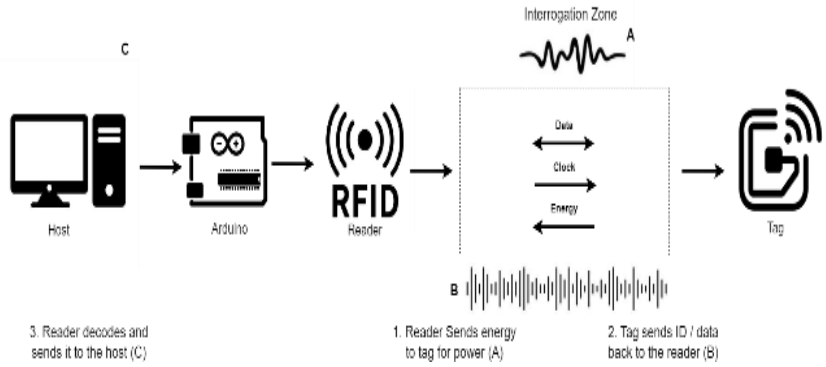

Figure 6 Architecture

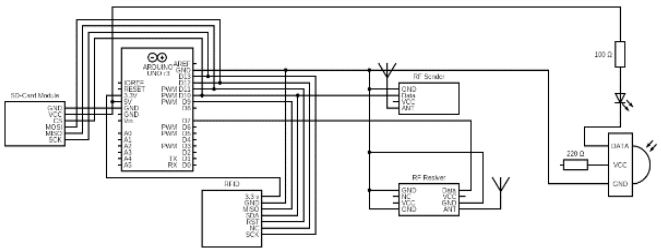

Figure 7 Circuit diagram

9. RELATED WORKS

IOT devices against Bluetooth worms with Bluetooth OBEX proxy

The Bluetooth OBEX proxy has many features wherein it works with the BlueZ's BTP (Bluetooth file transfer Filter) in order to protect Bluetooth from malwares and it is better than the traditional Bluetooth attack prevention.

AUTHOR: Fu-Hau Hsu 1, Min-Hao Wu 2,* , Yan-Ling Hwang

Year: 2023

HACKING SATELLITES WITH SOFTWARE DEFINED RADIO

In this project Reaktor Hello World satellite command and control is done via encrypted channel through SDR to attack on the ground station. They have intercepted it and spoofed the satellite signal from the ground station with a replay attack.

AUTHOR: Kimberly Lukin, Maximilian Haselberger

Year: 2021

HACKING COMMERCIAL DRONES USING NODEMCY

Drones have been discussed both in commercial as well as govt. sector and using it for privacy concerns the user. In this paper, a commercial drone was launched and attacked by using a simple basic deauthentication attack and compromising the drone for user data.

AUTHOR: Jonas Gabrielsson, Joseph Bugeja, Bahtijar Vogel

Year: 2021

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 97-106

e-ISSN : 2583-1062

Impact Factor: 5.725

THE ART OF RFID HACKING

We all use cards to make payments nowadays and also badges to gain access to certain areas. These all cards carry RFID thus having radio frequency signals. The method used is Tastic RFID Thief it is used to capture the signal from within a proximity in order to hack RFID and gain access by copying their UID. Thus getting the information and impersonating them.

AUTHOR: Kolin Nielson, Sayeed Sajal

YEAR: 2023

10. OUTPUT

Arduino IDE

It shows the output of the embedded code in ESP2866 that runned in Arduino IDE, which is used to write and upload the embedded code to the microcontroller boards. It also act as a compiler for converting the code into machine readable-format and also provides uploader for transferring the compiled code to the arduino boards. An easy-to-use interface is provided by the Arduino IDE for authoring, compiling, and uploading code to an Arduino board. It has a text editor for creating code, a compiler for turning that code into machine-readable form, and an uploader for sending that code to the Arduino board.

Here in this output, the data that is generated at the given time interval will be displayed in the IDE.

RFID

AWS Lightsail is a cloud-based virtual private server (VPS) solution provided by Amazon Web Services (AWS). It is designed to make it easy for developers, businesses, and individuals to quickly launch and manage virtual private servers, databases, and other application resources in the cloud. We can simply scale our resources up or down with AWS Lightsail as necessary to manage changes in traffic or consumption without worrying about capacity planning.

AWS Lightsail is a cost-effective solution for hosting websites and applications in the cloud. It offers a range of pre-configured plans with fixed monthly pricing, so you can easily predict your costs and avoid unexpected charges.

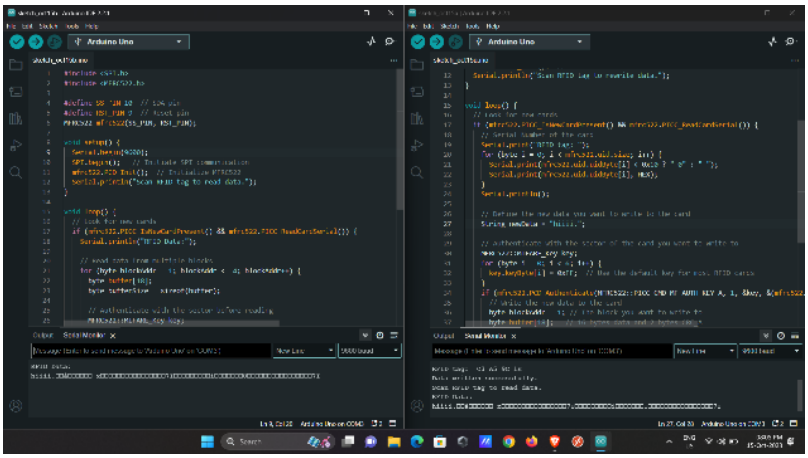

Figure 8 Output 1

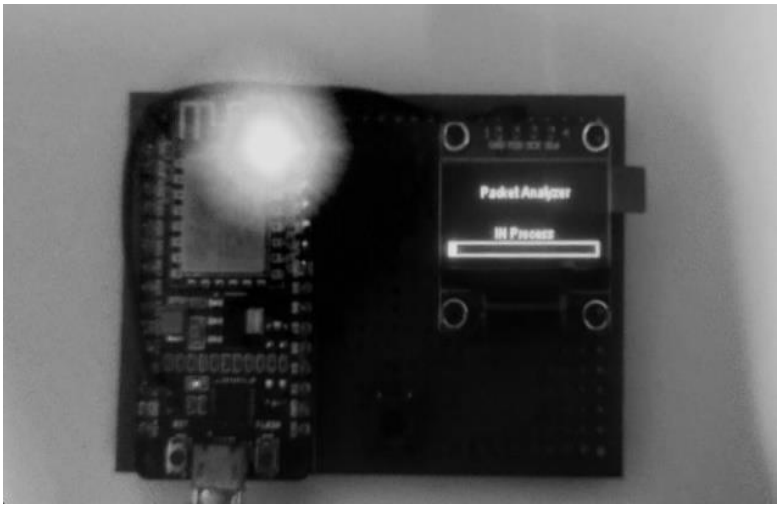

Figure 9 Output 2

11. CONCLUSION

Our project involves the integration of multiple technologies to attack and test the security of an organization. Firstly, we are using sensors to capture data from the recievers continuously. The data is then streamed to the Arduino IDE, which provides a platform for the storage and analysis of the data. This data is processed and then used for further future attacks in order to test the compliance score of the organization making it a safe way to learn ethical hacking educationally.

12. FUTURE WORK

In the future, we are in the plan to integrate AI (Artificial Intelligence) and ML (Machine Learning) in order to analyze the data efficiently and process it. This data can also then be compared with other data sets in order to make comparisons and run proper diagnostics.

Also we would like to integrate cloud so that once the testing phase is over a report can be generated and submitted to the officials in the organization through a web portal which is integrated with cloud services to get a faster efficient workflow. This report can be accessed by the security professionals and then improvise and patch the flaws in their systems.

Personalized Medicine: The system can be used to personalize medicine by collecting and analyzing patient data to develop tailored treatment plans for each individual.

Wearable Devices and Sensors: The development of new wearable devices and sensors can provide healthcare providers with even more data about a patient's health and improve the accuracy of monitoring and analysis.

Interoperability Standards: Developing and implementing interoperability standards can make it easier for different systems to communicate and exchange data, improving the overall efficiency of the Healthcare Monitoring System in IoT Cloud.

13. REFERENCES

[1] Charléty, A., Le Breton, M., Baillet, L., & Larose, E. (2023). RFID landslide monitoring: long-term outdoor signal processing and phase unwrapping. IEEE Journal of Radio Frequency Identification.

[2] Arora, L., Thakur, N., & Yadav, S. K. (2021, February). USB rubber ducky detection by using heuristic rules. In 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 156-160). IEEE.

[3] Manjunath, M., Venkatesha, G., & Dinesh, S. (2019). RF Hacking Detection using Spectrum Scanning. Perspectives in Communication, Embedded-systems and Signal-processing-PiCES, 3(1), 22-25.

[4] Kim, S. W., & Park, D. W. (2020). Hacking attack and vulnerabilities in vehicle and smart key RF communication. Journal of the Korea Institute of Information and Communication Engineering, 24(8), 1052-1057.

[5] Jiao, X., Liu, W., Mehari, M., Aslam, M., & Moerman, I. (2020, May). openwifi: a free and open-source IEEE802. 11 SDR implementation on SoC. In 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring) (pp. 1-2). IEEE.

[6] Capota, C., Halunga, S., Fratu, O., Eugen, S., & Mădălin, P. (2021, May). Security Aspects and Vulnerabilities in Authentication Process WiFi Calling–RF measurements. In 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) (pp. 1-5). IEEE.

[7] Agarwal, M. (2021, December). DES Based IDS for detection Minimal De-authentication DoS Attack in 802.11 Wi-Fi Networks. In 2021 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 143-148). IEEE.

[8] Sheth, J., & Dezfouli, B. (2019). Enhancing the energy-efficiency and timeliness of IoT communication in WiFi networks. IEEE Internet of Things Journal, 6(5), 9085-9097.

[9] Arora, L., Thakur, N., & Yadav, S. K. (2021, February). USB rubber ducky detection by using heuristic rules. In 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 156-160). IEEE.

[10] Thomas, T., Piscitelli, M., Nahar, B. A., & Baggili, I. (2021). Duck hunt: memory forensics of USB attack platforms. Forensic Science International: Digital Investigation, 37, 301190.

[11] Lukin, K., & Haselberger, M. (2020, October). Hacking Satellites With Software Defined Radio. In 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC) (pp. 1-6). IEEE.

[12] Chauvin, M., Piot, O., Boveda, S., Fauchier, L., & Defaye, P. (2023). Pacemakers and implantable cardiac defibrillators: Must we fear hackers? Cybersecurity of implantable electronic devices. Archives of Cardiovascular Diseases, 116(2), 51-53.

[13] Pereira, H., Carreira, R., Pinto, P., & Lopes, S. I. (2020, June). Hacking the RFID-based Authentication System of a University Campus on a Budget. In 2020 15th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-5). IEEE.

[14] Nevliudov, I., Yevsieiev, V., & Maksymova, S. (2022). Development of a Layout for Hacking an Industrial Computer Using the Hid Attack Method. INFORMATION SECURITY: PROBLEMS AND PROSPECTS, 58.

[15] Kawle, R., & Thakare, S. (2021, August). Designing, Analysis and Synthesis of 32-Bit Configurable Hack CPU. In 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT) (pp. 779-783). IEEE.

[16] Iavich, M., Iashvili, G., Gagnidze, A., & Odarchenko, R. (2021, September). Use of Content-Filtering Method for Hardware Vulnerabilities Identification System. In 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT) (pp. 132-136). IEEE.

[17] Hassan, K. M., & Ibrahim, S. A. (2019, April). A non-return-to-zero charge-steering flip-flop for high-speed wireline transceivers. In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) (pp. 525-529). IEEE.

[18] Singh, R., Thakkar, R., Thakkar, M., Rote, U., Patil, S., & Ingle, B. (2022, December). WiFi Deauth and Cloning using ESP8266. In 2022 5th International Conference on Advances in Science and Technology (ICAST) (pp. 1-5). IEEE.

[19] Zhu, R., Peng, W., Han, Y., & Huang, C. G. (2022). Intelligent health monitoring of machine tools using a Bayesian multibranch neural network. IEEE Sensors Journal, 22(12), 12183-12196.

[20] Fil, N., & Gurko, A. (2022, October). Method for Choosing a Set of Data Protection Tools in Computer Networks of an Environmental Monitoring System. In 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 311-314). IEEE.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 04, Issue 04, April 2024, pp: 97-106

e-ISSN : 2583-1062

Impact Factor: 5.725