CLIPPERZERO: A Noval device for Ethical Hacking

Khushi Raj Srivastava[1], Soham Sarkar[2] , Singh Rakeshkumar Vinay[3]
Satya Pal Singh[4]
[1234] IIMT COLLEGE OF Engineering
[1234]IIMT College of Engineering, Gretaer Noida, UP, Indias rakeshsinghrkss88@gamil.com

Abstract ClipperZero is an innovative, DIY device designed for RF signal analysis, empowering users to explore, learn, and secure the landscape of wireless communication. It integrates seamlessly with a mobile application, enabling intuitive control, real-time tracking, and efficient data storage.

Our development process emphasizes rigorous testing and methodological evaluation under controlled conditions, focusing on key parameters such as efficiency, reliability, ease of implementation, and detectability.

This paper delves into the security landscape of widely used communication protocols, including Bluetooth and Wi-Fi. It also presents a comprehensive review of modern mobile forensic investigation tools—spanning both open-source platforms and commercial solutions.

INTRODUCTION

At its core, ClipperZERO provides powerful features for detecting, analyzing, storing, and replaying RF signals, enabling users to investigate how everyday wireless devices operate. This includes systems like keyless car entry, garage door openers, remote switches, and other unlicensed RFcontrolled devices. The device allows users to capture these signals and understand the principles of modulation, frequency use, and signal behavior in practical applications. What sets ClipperZERO apart is its dual focus on both RF and Wi-Fi technologies. In addition to RF signal analysis, ClipperZERO is capable of Wi-Fi signal monitoring and controlled attack simulations, making it a valuable tool for cybersecurity training, ethical hacking, and penetration testing. With features such as de-authentication attacks, handshake captures, signal sniffing, and packet injection, ClipperZERO allows users to simulate real-world attack scenarios in controlled environments. This hands-on approach provides deep insight into common wireless vulnerabilities and teaches users how to detect, prevent, and mitigate such threats.

ClipperZERO is supported by a dedicated mobile application that enhances its portability and functionality. Through the app, users can view captured signals, manage data, and even initiate replay or scanning actions remotely, making the device ideal for field use and educational demonstrations.

A signal analyzer—it's a gateway for education, exploration, and ethical hacking in both the RF and Wi-Fi domains Designed with security researchers, developers, students, and wireless hobbyists in mind, ClipperZERO serves as a that surround us. Whether you're aiming to understand how a key fob unlocks your car or how attackers might exploit an unsecured Wi-Fi network, ClipperZERO provides the tools and the knowledge framework needed to dive deeper into wireless communication and contribute to building more secure systems.

In summary, ClipperZERO is not just. It transforms complex wireless technology into an accessible, interactive experience, enabling users to learn by doing and to innovate by understanding

RESULTS AND DISCUSSION

1. LITERATURE REVIEW:

1. Capabilities and Applications: clipperZero combines several features into a small, compact package. This aspect helps users to effectively communicate with the variety of wireless protocols that includes infrared, RFID, Sub-GHz, & RFID. It is useful for security assessments and penetration testing because of its versatility, which enables operations like signal collection, replay assaults, and device emulation.

2.Versatile and Programmable: The clipperZero is a programmable hardware platform that enables users to customize its features and increase its capabilities through custom software. it has a versatile architecture that can be tailored to a range of requirements, from straightforward jobs like managing appliances to more intricate security tests.

3. Educational Integration: The device has been incorporated into educational settings to teach students about the electromagnetic spectrum and signal hacking. By using clipperZero, students gain hands-on experience in understanding wireless communications and the security implications associated with them.

4. RF Hacking Laboratories: In academic researches, Clipperzero has been used in conjuction with other tools such as HackRF . One to create hands-on laborartories focusing on Rf security. These laboratories give students practical experencies with signal analysis ,protocol reverse engineering, and active attack stratergies.

5. Ethical Considerations: The risk of misuse emphasizes the significance of responsible use and respect to legal frameworks when using such gadgets. Clipperzero provides significant capabilities for vulnerability testing ,but it also poses ethical considerations.

4. RF Hacking Laboratories: In academic research, Flipper Zero has been utilized alongside other tools like HackRF One to develop hands-on laboratories focused on RF security. These labs provide students with practical experience in signal analysis, protocol reverse engineering, and active attack techniques.

5. Ethical Considerations: The risk of misuse emphasizes the significance of responsible use and respect to legal frameworks when using such gadgets. Clipperzero provides significant capabilities for vulnerability testing, but it also poses ethical considerations.

6.Open-Source and Open-Hardware: The development tools, schematics and firmware source code are accessible to the general public. This encourages a community of developers that work on different firmware projects and create unique applications to enhance the device's usefulness and capabilities.

METHODOLOGY:

1.DATA COLLECTION: Academic papers, conference proceedings, technical reports, and internet resources around Flipper Zero and related technologies are some of the sources of the data.
Analysis: Integrate results to determine the clipper Zero's primary features, restrictions, and possible hazards**.**

2.DATA PREPARATION: Cleaning: Removal of duplicates, correcting missing or inconsistent values Normalization: Standardizing data formats (like images resized to uniform dimensions**)**

3. DESIGNING:

A. Components Used: ○ Microcontroller: ESP32 for core processing, Bluetooth integration, and GPIO control.

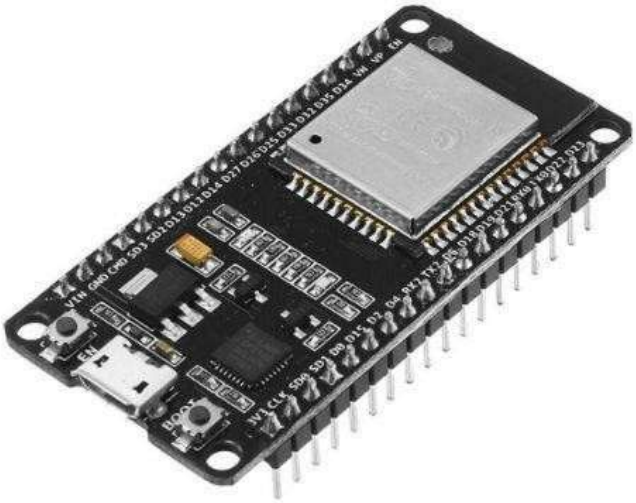
B. RF Modules: 433 MHz transmitter and receiver for RF signal capture and emission.

C. Power Source: USB or battery for powering the ESP32.

D.ESP32 Development Board: This versatile microcontroller serves as the "brain" of ClipperZERO, handling signal processing, Bluetooth communication, and control functions.

E. 433 MHz RF Transmitter and Receiver Modules: These modules are essential for capturing and emitting RF signals. They operate on the commonly used 433 MHz frequency, making them suitable for devices like remotes, IoT sensors, and other low-power RF applications.

F. Bluetooth Module: Integrated with the ESP32, the Bluetooth module allows for seamless communication between ClipperZERO and the mobile application.



G. Power Supply: A battery or USB power source can be used to power ClipperZERO, depending on your preference for portability. your preference for portability.

Software Utilized

A. **Arduino IDE:** This technology is utilized for uploading as well as developing the firmware to the ESP32. It provides an intuitive environment for programming microcontrollers and supports libraries essential for handling RF signals and Bluetooth communication.

B. **Mobile Application**: This app will serve as the control interface for ClipperZERO, allowing you to command the device, view captured signals, and initiate signal replay. The app can be developed using platforms like MIT App Inventor or Bluetooth serial apps, depending on the desired functionality.

4. TESTING:

Test Environment Setup Hardware: ESP32WROOM-32 module, laptops and smartphones (STA devices), Wi-Fi routers (APs)

Software: De-authentication-capable custom ESP-IDF firmware

Network setup: a separate lab Wi-Fi network with MAC addresses and known login credentials.

2. Broadcast De-authentication Method
Success Rate: ~70–85% of devices were disconnected during tests.

3. Rogue AP De-authentication Method Success Rate: 90–100% when client actively communicated with the AP

Reliability: High—STAs consistently responded to rogue AP due to 802.11-compliant behavior

Drawback: No effect if client did not attempt to connect

Detection: Triggered some client-side security alerts (on newer OS versions)

4. Combined Method (Broadcast + Rogue AP) Effectiveness: Best results—95–100% de-authentication rate

Latency: Reduced average disconnect time to under 1 second

Coverage: Successfully affected both active and idle clients

Use Case: Ideal for handshake capture and PMKID attacks

5. Safety & Stability
System Recovery: Cleanup functions restored normal AP operations without requiring reboots

False Positives: None observed in targetlimited tests

Error Rate: <1% across 100+ repeated test cycles

6. Limitations Observed
Device Immunity: Devices with WPA3 or advanced management frame protection were not affected

Legal Restrictions: Experiments have to be conducted only in controlled settings.

RESULT:

1. Develop a low-cost, user-friendly RF signal analyzer capable of detecting and replaying sub-GHz signals.
2. Implement signal processing and data storage features to enable real-time RF signal capture and manipulation. **3.** Create a mobile application for easy user interaction, storage, and analysis of captured signals. Encourage ethical use and awareness of RF technology's role in security and IoT systems
4. Objective is to understand the potential risks associated with using the Flipper Zero for malicious purposes and to develop strategies for mitigating these risks.
5. The study might concentrate on particular topics, such locating weak encryption keys, examining signal patterns for possible man-in-the-middle attacks, or investigating the Flipper Zero's capacity to mimic or spoof genuine devices.

FUTURE SCOPE:

1. Implement signal processing and data storage features to enable real-time RF signal capture and manipulation.

2. low-cost, user-friendly RF signal analyzer capable of detecting and replaying sub-GHz signals.
3. mobile app interference for enhanced accessibility and user control.
4. signal capture storage and proccessing 433MHZ frequency range.
5. RF signal analysis and replay for educational and security reseach application.

CONCLUSION:

Develop a low-cost, user-friendly RF signal analyzer capable of detecting and replaying sub-GHz signals**.** In order to enable the real-time RF signal capture as well as manipulation, implementation of signal processing and data storage is necessary. Create a mobile application for easy user interaction, storage, and analysis of captured signals. Encourage ethical use and awareness of RF technology's role in security and IoT systems. Objective is to understand the potential risks associated with using the Flipper Zero for malicious purposes and to develop strategies for mitigating these risks.
The study might concentrate on particular topics, such locating weak encryption keys, examining signal patterns for possible man-in-the-middle attacks, or investigating the Flipper Zero's capacity to mimic or spoof genuine devices.

REFERENCES.

[1] Alhalafi, N., & Veeraraghavan, P. (2019). Privacy and security challenges and solutions in IOT: A review. In IOP conference series: Earth and environmental science (Vol. 322, No. 1, pp. 012013). IOP Publishing.

[2] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10– 28.E., H. (2020).

[3] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146–164.

[4] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access, 7, 82721–82743.

[5] Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: A survey. Information Systems Frontiers, 17(2), 243–259.

[6] Waraga, O. A., Bettayeb, M., Nasir, Q., & Talib, M. A. (2020). Design and implementation of automated IoT security testbed. Computers & Security, 88, 101648

[7] Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: A review. In 2012 international conference on computer science and electronics engineering (Vol. 3, pp. 648–651). IEEE.

[8] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The Internet Society (ISOC), 80, 1–50

[9] Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges", *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp.

[10] Vestermark, T. 2015. Rtl_433 chuango.c source file. Updated 20 September 2023. Web page. Available at: https://github.com/merbanan/rtl_433/blob/master/src/devices/chuango.c [Accessed 22 July 2024].

[11] Youngblood, G. 2002. A software-defined radio for the masses, part 1. PDF document. Available at: https://www.arrl.org/files/file/Technology/tis/info/pdf/020708qex013.pdf [Accessed 3 January 2024].