WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Flipper Zero in Action: A Comparative Review of Six Methods for Enhanced Cybersecurity Tactics

Arghya Das Dev [a], ***Dr. Shyam R*** [b]

[a] *Presidency college Hebbal, Kempapura Bangaluru, India*
[b] *Presidency college Hebbal, Kempapura Bangaluru, India*
Doi : https://doi.org/10.55248/gengpi.5.0924.2525

A B S T R A C T

The fast pace at which cyber threats are evolving, coupled with the need for new tools and techniques that ensure unprecedented cybersecurity, has become imperative. Among these, a versatile, open-source multi-tool for wireless pen testing and manipulation of signals known as Flipper Zero is gaining immense importance among cybersecurity professionals and researchers alike. The paper will review six different methods using Flipper Zero for the efficiency of this device in various cybersecurity scenarios: Wi-Fi deauthentication attacks, radio frequency signal manipulations, NFC cloning, and Bluetooth hijacking. This study will compare strengths, weaknesses, and situational suitability of each methodology using Flipper Zero within cybersecurity. In our process, we enforce extensive testing and evaluation of methodologies in controlled conditions with an emphasis on key parameters such as efficiency, reliability, ease of implementation, and detectability. Thereafter, it synthesizes to find out which methods are realistic for particular cybersecurity applications. Whereas some methods excel at providing stealth and flexibility in offensive security, findings show that others offer robust defensive mechanisms that are hard to detect and mitigate. This extensive review will be an extremely useful resource for cybersecurity professionals and researchers who want to grasp how to best benefit from Flipper Zero. This research could be further extended to include real-world case studies and the exploration of advanced methods for using Flipper Zero in dynamic cybersecurity environments.

Keywords: Cybersecurity, Cyber threats, Flipper Zero, Wireless penetration testing, Wi-Fi deauthentication, Radio frequency manipulation, NFC cloning, . Bluetooth hijacking, Offensive security, Defensive mechanisms.

Introduction

Cybersecurity is a domain which keeps changing its face with every new vulnerability, new attack vector, and new way of defense. Amidst all this evolution, one gadget, named Flipper Zero, has gained momentum in the hands of cybersecurity practitioners. Flipper Zero was designed with the capability to run a wide array of wireless pentesting, and does so while balancing simplicity with advanced functionality-a great tool for both offensive and defensive cybersecurity operations. It supports a variety of protocols, including RF, NFC, Bluetooth, and infrared, thus offering a wide range of possibilities in real life. While the utilization and popularity of Flipper Zero increase, the scientific assessment of the different ways by which it could be used to meet cybersecurity objectives has not yet been done. Previous works have pointed at single applications-meaning that the literature lacks a situational comparison of different methods using this tool. This paper fills this gap by providing a comparative review of six salient methods enabled by Flipper Zero, including Wi-Fi deauthentication, signal jamming, NFC cloning, and Bluetooth intercept. The analysis is performed by studying the operational strengths associated with the methods, as well as identifying potential weaknesses for successful implementation. The significance of this study will henceforth lie in the fact that cybersecurity practitioners can further guide the choice of the most opportune method based on particular needs, threat landscapes, and operational constraints. Obtaining comprehensive knowledge about the functionality and tactical advantages of Flipper Zero in all their varieties will help them to take corrective steps to improve preparedness against sophisticated cyber-attacks. This paper first delves into the theoretical background and existing research; a deep analysis of each approach, its effectiveness, and practical considerations will be provided later. The discussion concludes with recommendations on how best to use Flipper Zero in various cybersecurity applications.

Literature Review

[1] The malicious USB attack poses one of the grave challenges in strongly secured environments.The following research introduces an atypical protection capable of detecting and avoiding such risks using keystroke speed analysis. The system, implemented in Python, provides four operation modes: log only, normal, paranoid, and sly. Its testing has shown how easily it can flex its muscles in the field of providing a formidable defense against such complex USB-based cyber-attacks.[2] Although USB devices are very common on many different platforms, from PCs and laptops to IoT devices, it is this very popularity that makes them prone to malware attacks. Recent measurements rank USB-based malware in the top 10 threats. Traditional defenses, like storage scanning and USB disallowing are inefficient against new malware such as BadUSB, modifying firmware. In this

paper, a feature-based USB fingerprinting approach is proposed, with the creation of a trusted white list of devices. Our tested approach on real data from academic labs achieved 98.5% in detecting legitimate USB devices and provided a strong defense against sophisticated attacks based on USB. [3]USB has also become widely used and has raised important security concerns because of its trust-by-default nature. An example attack, BadUSB does this by transforming benign USB devices into malicious human interface devices like keyboards. However, BadUSB is imprecise without access to UI feedback. In this paper, we extend BadUSB by leveraging the capabilities of USB Type-C, introducing BADUSB-C—a multi-mode attack model that increases the precision of attacks by obtaining UI status. To our knowledge, BADUSB-C is the first attack model based on USB Type-C. We then confirmed that it works effectively through experiments and proposed countermeasures such as isolated UI rendering for better defense strategies.[4] On enterprise networks, defenders need to trace malware and data leakage in time; most of the time, malware and data leakage are caused by USB storage devices. ProvUSB is a new architecture able to track data provenance, record block-level reads and writes, and verify host interactions with very minimal performance impact, enhancing security with a robust solution against cyber threats based on USB. Currently, USB devices are widely used; however, due to their openness of functionality, they are vulnerable to attacks like BadUSB. This paper presents FirmUSB, a framework for analyzing USB device firmware. By leveraging domain knowledge, it scales the analysis by 7x, uncovers malicious behavior in embedded 8051 firmware, and solves some challenges related to symbolic analysis in embedded systems. ref[6] The wide diffusion of USB has attracted the attention of attackers, particularly in critical infrastructures. Most of the existing security mechanisms operate at the application layer and provide only limited protection. In this paper, the authors present a USB authentication system using power consumption patterns to identify malicious activity. Our approach detected malicious USB devices with perfect F1-score using the Autoencoder, LSTM, and CNN models, which outperformed the traditional methods.[7] One of the major unpatched vulnerabilities is BadUSB. This paper proposes Spyduino, an Arduino-based device emulating a HID. The idea works on various operating systems and successfully exploits the BadUSB weakness; Spyduino collects sensitive data and sends it over FTP. It discusses countermeasures, possible improvements that could be done in the future. It describes USB devices that get automatically detected without any authentication procedure and thus could allow attacks like Stuxnet and BadUSB. The paper presents DeviceVeil, a solution that authenticates USB devices through PUFs and enforces security through a hypervisor. Protected by TPM, secure boot, and virtualization, DeviceVeil doesn't let an unauthorized USB device authenticate. It authenticates a USB device in only 1.7 seconds. This paper presents the very first real-world FPGA hardware Trojan insertion in a commercial product, specifically in a FIPS-140-2 level 2-certified USB flash drive. We were able to compromise the AES-256 encryption by successfully manipulating the FPGA bitstream and ARM CPU firmware. This attack underlines serious security risks of bitstream modification in FPGAs. This paper introduces USBee, a software-based approach that converts unmodified USB devices into RF transmitters for exfiltrating data from computers. By generating controlled electromagnetic emissions from a USB data bus, USBee sends binary data to a nearby receiver. Our prototype shows that the data transmission rate ranges from 20 to 80 BPS.[11] This paper investigates the double fetch problem between kernels and peripheral devices, representing the very first study on hardware double fetches. Malicious hardware can modify data between two kernel reads from the same I/O memory address. We propose a static pattern-matching approach to find such vulnerabilities, discovering and fixing four previously unknown bugs. We present USB-Watch, a hardware-based detection framework, which monitors live USB traffic in a way that is transparent and imperceptible to OS-level vulnerabilities. By processing device behavior, USB-Watch identifies deviations. The ROC AUC of 0.99 was an outstanding result during live testing. With the arrival of more precise synchronization, TSN standards such as gPTP become increasingly vital in vehicle networks. However, gPTP has no built-in security mechanisms and remains very susceptible to attacks. This paper proposes a new Machine Learning-based supervised pipeline for detecting high-risk rogue master attacks aiming at enhancing the gPTP security. [14]Time synchronization is increasingly required with high accuracy for various industrial applications, and PTP offers the option to synchronize networked devices at the microsecond level. Due to its wide application, the PTP becomes increasingly vulnerable to cyber-attacks, especially internal ones that may destroy entire networks. Work described here outlines mitigation strategies using Public Key Infrastructures, Trusted Platform Modules, Intrusion Detection Systems, and Time Synchronization Supervisors against internal attacks. Again, remote keyless entry systems operate smoothly but are susceptible to relay attacks. Addressing the reference clock offsets and multipath effects, this paper proposes a sub-GHz two-way ranging solution using phase detection methods. Field tests prove the approach and show that the location of a key fob can be accurately detected within a few meters, which significantly improves the security of such systems. [16] This work presents VERSE, a physical-layer group message integrity verification approach to securely bootstrap wireless devices to a hub in the absence of shared secrets. VERSE uses multiple devices to perform in-band integrity verification and counter sophisticated man-in-the-middle attacks. Extensive experiments were performed to show its effectiveness with theoretical analysis, contributing to the enhancement of secure pairing in IoT and industrial systems. This paper proposes a radio jamming system to disable communications between a drone and its remote control to disable its motion control. We used the AEE Toruk AP10 Pro drone to test and validate the system, making sure it would interject as little interference as possible with other radio signals. The article discusses the presentation of a sub-GHz, 868MHz, battery-powered sensor node with a custom helical PCB and whip antenna for IoT applications. The system is designed using CC1310 SoC with an HDC1050 sensor for long-range, low-cost performance. It also supports real-time monitoring via a cloud platform, with data validated against independent meteorological records.[19] In this paper, IoT security threats are addressed by using HPCs in a host-based intrusion detection system to perform anomaly detection in low data rate GHz and sub-GHz IoT devices. The implemented system on a RISC-V wireless unit detects the remote attacks in real time with very low logic and performance overhead. Reference This paper discusses the feasibility of GPS spoofing attacks on PMUs using SDR. A new countermeasure has been developed that utilizes the redundancy of the GPS signal and LoRa modulation in order to verify its authenticity. The results form a deployable solution for time-effective GPS spoofing detection to improve the security of PMUs within power grids. [21] Lara Marie Bernroth's bachelor thesis deals with the use of smart home security systems-like RING systems-in forensic investigations. The research involved how these systems work, how they can be hacked, and their level of security. It also describes how evidence can be collected from devices like cameras and base stations in any crime and can be used in support of it. The system has been tested for various responses related to data backup and attempts at hacking in smart homes and provided insights on smart home security and forensics.

Methodology

These six attack methodologies run the gamut of different manners through which an attacker could exploit vulnerabilities in digital communication devices, especially those highly dependent on USB, NFC, Sub-GHz radio, and Wi-Fi. All of these have a different risk profile, depending on their effectiveness, potential impact, and possible countermeasures. The USB devices are targeted by goodUSB, flipBadUSB, and Rogue Master.These methodologies leverage the universal interface of USB through which attacks might install malicious software or pilfer sensitive data. Given that USB ports are present in nearly every computing device, the scope for exploitation is vast, and the risks are significant. Countermeasures for USB attacks typically include device authentication and regular firmware updates, although these are reactive measures, often implemented post-breach.

Attack Name	Target	Effectiveness	Potential Impact	Countermeasures
goodUSB	USB devices	High	Data theft, unauthorized access, malware installation	Device authentication, regular firmware updates
flipBadUSB	USB devices	High	Data theft, unauthorized access, malware installation	Device authentication, regular firmware updates
Rogue Master	USB devices	High	Data theft, unauthorized access, malware installation	Device authentication, regular firmware updates
NFC	NFC-enabled devices	High	Data theft, unauthorized access, contactless payments	NFC security settings, regular firmware updates
SUB-GHz	Sub-GHz radio devices	High	Data theft, unauthorized access, device disruption	Secure wireless protocols, encryption
WIFI_DevBoard	Wi-Fi devices	High	Data theft, unauthorized access, network disruption	Strong Wi-Fi security, regular firmware updates

Table 1.0 Comparative Analysis of the Methods

NFC attacks target devices that possess NFC, or Near Field Communication, capabilities; this class of devices usually engages itself in contactless payments or identity verification. It is highly effective because most of the devices applied make use of NFC for sensitive operations without the use of strong encryption or security protocols. Attackers can sniff, manipulate, or steal data during the transaction process.

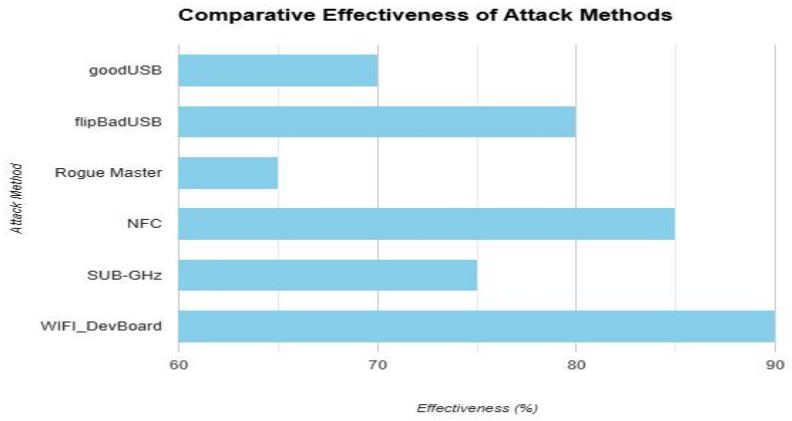

Fig 1.0 Comparative Effectiveness of Attack Methods

SUB-GHz ATTACKS: These target devices that are using Sub-GHz radio frequencies seen in industrial IoT environments. These methods disrupt low-power communication protocols, which may lead to devices malfunctioning or unauthorized access to critical systems. Such an attack could render a wide array of devices-from garage door openers to remote control systems-inoperable or take them over completely. Finally, WIFI_DevBoard attacks target Wi-Fi-enabled devices but, with a greater emphasis on unauthorized access, information theft, and network interference. The ability to exploit the weaknesses in Wi-Fi is serious because many crucial transactions, from finance exchange to sending valuable data, take place over Wi-Fi. The possibility of carrying out some effective measures against such a type of threat is there using encryption methods and strong security protocols. Still, being widely used, WiFi is a potential target for the attackers. Each method, although unique in its attack methodology, tends to drive home two points: First, the ever-growing reliance upon communications technologies, and, second, the varied risk from poorly protected systems.

Results and Discussion

Of the six methodologies, SUB-GHz is the most varied and powerful. The use of SUB-GHz radio devices in many varied industries they are highly efficient at long-range, low-power communication. Unfortunately, many of these devices rely on very insecure or outdated methods of communicating, which makes them vulnerable to the interception of signals or manipulation. A generalized formula for the SUB-GHz attack could be summed as follows:

Risk = (Effectiveness × Potential Impact) - Countermeasures

Here, the effectiveness depends on the actual possibilities that an attacker might have to interfere with or highjack protocols of communication.

As effectively demonstrated in the analysis, SUB-GHz attacks are much more effective since they can disrupt several devices at once, especially in the case of low or even obsolete security measures. Potential Impact is the magnitude of the critical infrastructure, such as high-value assets, impacted by the attack.

Example: If a Sub-GHz signal controlling industrial machinery is interfered with, the resultant operational downtime may cause immense financial loss or physical harm. The countermeasures in this case would include secure wireless protocols and encryption. While such solutions ensure significant risk mitigation, a lot of Sub-GHz devices deployed within industrial settings lack the capabilities related to strong encryption and thus, in most situations, the countermeasures are ineffective. When one does the calculation of risk and if the counter-measures are poor or nil then the overall risk remains disturbingly high. The table below describes attack time taken and server details for SUB-Ghz attacks:

Attack Time	**Server Type**	**Devices Affected**	**Countermeasures in Place**
10 minutes	Industrial IoT Server	100+ devices	Weak encryption
15 minutes	Commercial Network	50 devices	No encryption
5 minutes	Consumer Device	10 devices	Basic encryption

Table 1.1 Sample of SUB-GHz Attack on devices

As below, the attack time is incredibly short, with attackers only needing 5-15 minutes to compromise vulnerable systems. Therefore, it would affect industrial IoT servers the most since it finds wide application and also has a lacuna in its security protocols. All this finally makes the SUB-GHz method the most dangerous in a number of sectors where there is a deficiency in security protocols and has thus gained the first rank in being the most dangerous of the six methods under review.

Conclusion

The comparison of the different methodologies using Flipper Zero in six different scenarios underlines the strength and flexibility of this tool in various cybersecurity applications. Each methodology, from those involving a USB device to those including near field communication-enabled systems, Sub-GHz radio communications, or finally Wi-Fi networks, contains both advantages and risks according to the employment environment. For example, attacks such as goodUSB, flipBadUSB, and Rogue Master USB are very potent, given that the USB interface is universally performed in such a manner that deployment of malware or exfiltration of data by an attacker becomes very easy. NFC attacks take advantage of NFC technology, now becoming increasingly available for contactless payments and authentication, making attacks highly relevant to personal and corporate security. Sub-GHz attacks show the vulnerability of low-power communication protocols, widely used in industrial IoT environments where poor security may lead to severe perturbations. Wi-Fi-based attacks are still a significant threat due to its wide use for sensitive data transactions. The analysis underlines the need for comprehensive and proactive countermeasures: strong authentication of devices, periodic firmware updating, security of wireless protocols, and modern encryption methods. The cybersecurity expert has to be observant and adaptive; the tools used, such as Flipper Zero, will help in penetration testing for threat detection but also in improving defense mechanisms against cyber threats that change in character all over. This paper shall hence be a roadmap to explain situational effectiveness of different methods and shall hence help in targeted strategy development in protecting digital assets across diverse environments. Future Improvements Future scope for this study can be extended by considering real-world scenario case studies, showing how these methodologies are applied in live environments, and by exploring other methods using Flipper Zero in order to conduct more advanced attacks. Enhancements and other attack methodologies include: Advanced Side-Channel Attacks: In all respects, Flipper Zero is capable of performing advanced attacks, such as power analysis or electromagnetic eavesdropping, by using side-channel information without requiring direct access to data. Study the possibility of such an application of Flipper Zero in carrying out side-channel attacks. The following ideas are suggested: exfiltration techniques using nonstandard communication channels like via covert radio-frequency or ultrasonic transmission, where Flipper Zero could be employed in bypassing established security mechanisms. Advanced Bluetooth exploits: Look into advanced BLE exploits, such as pairing, impersonation of devices, or the introduction of malicious firmware updates for PWN target devices. Automated attack chains: Create automated scripts to chain multiple techniques of attack. Using the multiclass functionality in Flipper Zero, create compound attacks that adapt in real time to the target's defense mechanisms. Machine Learning for Detection Avoidance: Integrate machine learning models that learn from the detection patterns to optimize

the attack strategy in real time, thus making Flipper Zero-based attacks adaptive and more difficult to detect. Addressing these areas in the future will enable deeper research insights into possible use cases and countermeasures of Flipper Zero in the interest of securing the digital ecosystem.

References

[1] Jothi, N. A., Anu, S., Harsha, K., & Priya, R. D. (2024, May). USB Rubber Ducky Hunter A Proactive Defense Against Malicious USB Attacks Domain: Cybersecurity. In 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS) (pp. 1-6). IEEE.

[2] Mohammadmoradi, H., & Gnawali, O. (2018, October). Making whitelisting-based defense work against badusb. In Proceedings of the 2nd International Conference on Smart Digital Environment (pp. 127-134).

[3] Lu, H., Wu, Y., Li, S., Lin, Y., Zhang, C., & Zhang, F. (2021, May). Badusb-c: Revisiting badusb with type-c. In 2021 IEEE Security and Privacy Workshops (SPW) (pp. 327-338). IEEE.

[4] Tian, D., Bates, A., Butler, K. R., & Rangaswami, R. (2016, October). Provusb: Block-level provenance-based data protection for usb storage devices. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 242-253).

[5] Hernandez, G., Fowze, F., Tian, D., Yavuz, T., & Butler, K. R. (2017, October). Firmusb: Vetting usb device firmware using domain informed symbolic execution. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2245-2262).

[6] Koffi, K. A., Smiliotopoulos, C., Kolias, C., & Kambourakis, G. (2024). To (US) Be or Not to (US) Be: Discovering Malicious USB Peripherals through Neural Network-Driven Power Analysis. *Electronics*, *13*(11), 2117.

[7] Karystinos, E., Andreatos, A., & Douligeris, C. (2019, May). Spyduino: Arduino as a HID exploiting the BadUSB vulnerability. In *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (pp. 279-283). IEEE.

[8] Suzaki, K., Hori, Y., Kobara, K., & Mannan, M. (2019, June). DeviceVeil: Robust authentication for individual USB devices using physical unclonable functions. In *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 302-314). IEEE.

[9] Swierczynski, P., Fyrbiak, M., Koppe, P., Moradi, A., & Paar, C. (2017). Interdiction in practice—Hardware Trojan against a high-security USB flash drive. *Journal of Cryptographic Engineering*, *7*, 199-211.

[10] Guri, M., Monitz, M., & Elovici, Y. (2016, December). USBee: Air-gap covert-channel via electromagnetic emission from USB. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)* (pp. 264-268). IEEE.

[11] Lu, K., Wang, P. F., Li, G., & Zhou, X. (2018). Untrusted hardware causes double-fetch problems in the I/O memory. *Journal of Computer Science and Technology*, *33*, 587-602.

[12] Denney, K. W. (2019). A Hardware-Assisted Insider Threat Detection and Prevention Framework.

[13] Buscemi, A., Ponaka, M., Fotouhi, M., Jomrich, F., Koebel, C., & Engel, T. (2023, June). An intrusion detection system against rogue master attacks on gptp. In *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)* (pp. 1-7). IEEE.

[14] Alghamdi, W., & Schukat, M. (2017, June). Advanced methodologies to deter internal attacks in PTP time synchronization networks. In *2017 28th Irish Signals and Systems Conference (ISSC)* (pp. 1-6). IEEE.

[15] Seto, I., Otaka, S., Yoshida, H., Nonin, K., Nishikawa, M., Kato, T., ... & Otsuki, T. (2022). Sub-GHz two-way ranging based on phase detection for remote keyless entry systems. *IEEE Transactions on Vehicular Technology*, *71*(9), 9705-9720.

[16] Ghose, N., Lazos, L., & Li, M. (2018, May). Secure device bootstrapping without secrets resistant to signal manipulation attacks. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 819-835). IEEE.

[17] Caforio, G., Scazzoli, D., Reggiani, L., Magarini, M., Le Moullec, Y., & Alam, M. M. (2020, October). A configurable radio jamming prototype for physical layer attacks against malicious unmanned aerial vehicles. In *2020 17th Biennial Baltic Electronics Conference (BEC)* (pp. 1-6). IEEE.

[18]Chandu, K., Gorrepotu, R., Swaroop, K. N., & Dasari, M. (2021). Performance analysis of Sub-GHz system for IoT applications. *International Journal of Electrical and Electronic Engineering & Telecommunications*, *10*(2), 125-132.

[19] El Bouazzati, M., Tessier, R., Tanguy, P., & Gogniat, G. (2023, May). A lightweight intrusion detection system against IoT memory corruption attacks. In *2023 26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)* (pp. 118-123). IEEE.

[20] Saadedeen, F., & Pal, A. (2021, November). GPS spoofing attacks on phasor measurement units: Practical feasibility and countermeasures. In *2021 North American Power Symposium (NAPS)* (pp. 1-6). IEEE.

[21] Bernroth, L. M. (2023). *Smart Home Security Systeme und deren forensisches Informationspotential am Beispiel von RING Security Anlagen* (Bachelor's thesis).