Flipper Zero Demonstrations

CS27, Professor Akbarfam
Ethan Kanyid: ethan.kanyid@wsu.edu

ABSTRACT. This project explores, in a responsible and controlled way, how a small gadget like the Flipper Zero can interact with the many invisible signals that surround society. Wireless communication is highly advantageous when the rules and regulations surrounding it are obeyed, but this project will bring to light the minimal effort it takes to hijack these pervasive signals. These signals range from radio and infrared to NFC and other short-range transmissions. The Flipper Zero comes with some of the capabilities to interact with these signals without modification, but for some of these demonstrations, additional hardware, firmware, and software will be needed – although there are many vendors and forums that will offer these services free of charge. The goal is not to teach attacks but to show how everyday wireless communications can be intercepted or tricked with a simple tool. The outcome of this is that people will be more aware of the invisible risks in homes, offices, and public spaces.

I. INTRODUCTION

Wireless signals are invisible packets of information transferred through radio waves, infrared beams, NFC, or Bluetooth pulses. Many of these waves are similar, but they have certain ranges and frequencies that have been coined to them, which creates a sense of these different wireless signals. Though many do not understand how these waves work, a little bit of hardware and a pinch of technical experience can unlock the door to interacting with these waves. This is where the Flipper Zero comes in. The Flipper Zero is a pocket-sized, consumer-friendly gadget that can read, emulate, and test many of these signals, making it useful for hobbyists and security researchers. Used responsibly, it helps reveal weak spots in everyday gadgets so owners can improve security. Used unresponsibly? Well, that is what we hope to protect against with these experiments.

II. BACKGROUND

Physical communication was the foundation of communication for a long while. In ages past it was letters; in nearer history, there were computers and cables. With the development of these interconnecting devices, the internet was born. With this rapid expansion, a new medium of communication was needed: wireless. Wireless communication was not new to the stage for it had existed in radio programs and other telecommunications already. Yet, the spectrum on which these signals exist needed to be controlled *[3]*. This spectrum is called the electromagnetic spectrum, and it has been adapted for communication through standardization by several organizations. The Institute of Electrical and Electronics Engineers (IEEE) defines the use of Wi-Fi (IEEE 802.11) and Bluetooth/ZigBee (IEEE 802.15). These are radio frequencies – as are cellular, SubGHZ, RFID, and NFC. These other standards of communication are defined by other organizations such as 3GPP (cellular) and ISO (RFID/NFC). Notably, SubGHz and Infrared are less regulated.

As well, some background into these technologies can be useful since there is so much overlap. SubGHz is any frequency less than 1000 MHz on the electromagnetic spectrum. These are longer waves that can travel further. RFID (Radio Frequency Identification) and NFC (Near Field Communication) are also SubGHz but are set apart for localized communication such as key cards or tracker tags. Higher on the spectrum is Bluetooth 2.4GHz, which is for a personal area network. Next is Wi-Fi, which uses 2.4GHz and 5GHz, which is useful for local households and common areas – referred to as a Local Area Network (LAN). Cellular is even higher where it can get up to 24GHz for high-speed communication (mmWave). Lastly, infrared which is just below the visible light spectrum at 300GHz – 400THz.

These signals benefit humanity tremendously, but they can also be naively used. The Flipper Zero will be able to show that through this project.

III. RELATED WORK

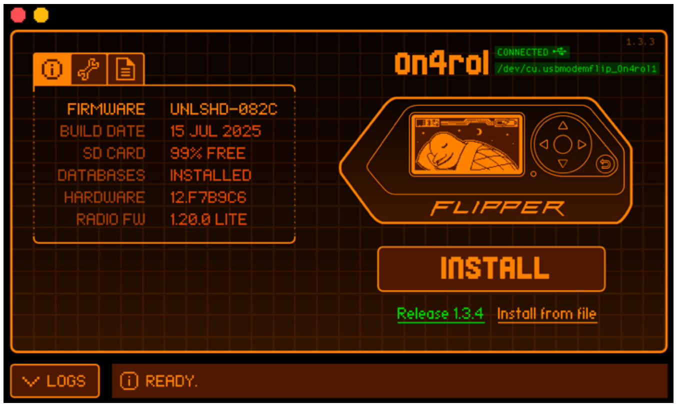
The Flipper Zero is shipped with a firmware called the 'OFW', which stands for original firmware *[2]*. Yet, that is not the only firmware – as the name implies. There are other common firmwares such as RogueMaster, Unleashed, and Xtreme. These firmwares add additional capabilities to the Flipper Zero that it cannot be sold with because it would be in violation of regulations. Some of these attacks that will be demonstrated can be accomplished with the OFW firmware, but some require a custom firmware. It is not illegal to modify the Flipper Zero, but some of the activities done with it can be against the law, so caution is highly recommended.

IV. SYSTEM DESIGN / METHODOLOGY

Several Flipper Zero demonstrations will be done in this project. These will be on Bluetooth, WiFi, RFID/NFC, Infared, and Sub GHz. Cellular will not be included because it is outside the range of capabilities of the Flipper Zero. The Flipper Zero will use the Unleashed firmware with several custom apps installed. This Includes Wi-Fi marauder, BLE spam, and SubGHz remote. As well, additional hardware will be used to unlock the capabilities of the Wi-Fi spectrum. This hardware is an ESP-32 board with Wi-Fi capabilities. It will use a custom marauder firmware on the board as well to unlock its capabilities. The first demonstrations will be benign uses of the Flipper Zero, which can be done without the custom firmware: Infrared remote and SubGHz remote. After that, it will be shown how the Flipper Zero can be used to capture NFC credit card information. Next, an attack will be performed on Bluetooth devices in the form of a Bluetooth Low Energy Spam (BLE Spam). Lastly, an evil portal server can be deployed to capture login credentials.

V. IMPLEMENTATION / EXPERIMENT SETUP

The Flipper Zero was modified with the Unleashed custom firmware *[1]*. This was done through the qflipper app on MacOS. Next, the flipper app was also use on IOS to download additional apps. These apps were the BLE Spam, SubGHz remote, and Wi-Fi marauder. The next step was installing the custom firmware on the Wi-Fi ESP-32 devboard. This involved connecting the board to MacOS again and using an online flasher to write to the board. Once the apps and firmwares were all customized, the devices were connected, and the demonstrations were carried out.



FIRMWARE	UNLSHD-082C
BUILD DATE	15 JUL 2025
SD CARD	99% FREE
DATABASES	INSTALLED
HARDWARE	12.F7B9C6
RADIO FW	1.20.0 LITE

On4rol CONNECTED

/dev/cu.usbmodemflip_On4rol1

READY.

Figure 1. QFlipper UI with Unleashed Firmware

VI. PRELIMINARY RESULTS OR PROGRESS

The demonstrations that have been carried out so far are the SubGHz remote and Infrared remote. These results have proved to be successful by capturing and replicating signals. These signals are stored on the Flipper Zero for further use too. As well, the NFC card reader has proven partially successful as well, although it is not able to capture all the information yet. The BLE Spam is also underway. The app was successfully loaded and launched on the Flipper Zero, but it has not been measured how successful it has been at denying service through fraudulent Bluetooth requests. Lastly, the Wi-Fi marauder attack has been partially implemented. An evil portal has been developed, but its full capabilities are still limited. More experimenting needs to be done to test the full effect of the attack.

VII. DISCUSSION / NEXT STEPS

The next step of the project is to measure the effects of these demonstrations. It is necessary to find quantifiable measurements to define the full usability of the Flipper Zero. As well, it will be imperative to document the process and verify the legitimacy of each step.

VIII. CONCLUSION

This project has shown that the Flipper Zero, especially when paired with custom firmware and additional hardware, can interact with and exploit various wireless signals such as SubGHz, infrared, NFC, Bluetooth, and Wi-Fi. While some demonstrations were simple and harmless, others revealed how easily these signals can be intercepted or misused. These findings highlight the need for increased awareness about the vulnerabilities in everyday wireless communication. The goal was not to promote misuse, but to educate users and encourage better security practices. Moving forward, further testing and quantifiable analysis will help assess the full impact of these tools.

REFERENCES

[1] DarkFlippers, “unleashed-firmware,” GitHub repository. [Online]. Available: https://github.com/DarkFlippers/unleashed-firmware. [Accessed: Oct. 9, 2025].

[2] Flipper Zero, “Flipper Zero — Multi-tool for pentesters and geeks,” FlipperZero.one. [Online]. Available: https://flipperzero.one. [Accessed: Oct. 9, 2025].

[3] IEEE, “IEEE — The Institute of Electrical and Electronics Engineers,” IEEE.org. [Online]. Available: https://www.ieee.org. [Accessed: Oct. 9, 2025].