ISSN: 2473-4901
v10 n6232

Teaching Case

Exploring Signals Hacking with Flipper Zero (FZ)

Tre' Vega
ov9820@uncw.edu

Robert Velez
rjv7649@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Congdon School
University of North Carolina Wilmington
Wilmington, NC 28403 USA

Hook

"In the eighteenth century, we knew how everything was done; but here I rise through the air; I listen to voices in America; I see men flying – but how it's done I can't even begin to wonder. So my belief in magic returns" (Woolf, 1928, p. 300).

Abstract

This teaching case provides engaging exposure to the popular hardware device *Flipper Zero*™ in an introduction to signals hacking. In this study, students are encouraged to think more deliberately about the electromagnetic spectrum (EMS) and the central role it plays in transmitting data among the myriad of devices in our modern digital world.

Keywords: Flipper Zero, Teaching Case, Electromagnetic Spectrum

1. INTRODUCTION

The electromagnetic spectrum (EMS) plays a critical and largely hidden role in our modern world. Harnessing the EMS makes it possible for us to listen to FM radio, heat food in a microwave, send/receive text messages, remotely unlock our car doors, and much more. The EMS is so seamlessly integrated into our digital lives and so poorly understood that it can seem like magic, validating the saying that, "Any sufficiently advanced technology is indistinguishable from magic" (Clarke, 1958/1973, p. 21).

Becoming comfortably naïve about EMS "magic" seems like something society can ill afford, as is illustrated by the surprising risk of leaving a car fob near an external wall (Figure 1).

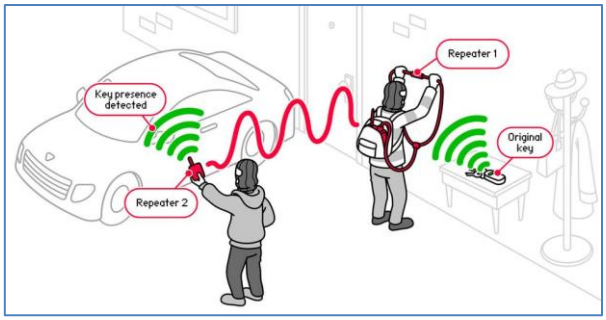

Figure 1: How car thieves can exploit a car fob through a wall (Zhovner et al., 2024)

ISSN: 2473-4901
v10 n6232

Flipper Zero™

The Flipper Zero™ (FZ), a multi-functional portable hacking tool currently available for $169 (Shop Flipper, 2024), has drawn significant interest. Originally conceived as a versatile device for security researchers, hobbyists, and hackers, the FZ has garnered widespread attention due to its extensive capabilities and user-friendly design.

Figure 2: The Flipper Zero™ – note the MicroSD card slot and USB-C port.

The FZ separates itself from traditional hacking tools through its combination of a wide array of different functionalities, including radio frequency (RF) communication, infrared (IR) control, and universal asynchronous receiver-transmitter (UART) interfacing. These features enable users to interact with a broad range of electronic devices, from radio frequency identification (RFID) tags to smart home systems, highlighting the tool's potential for both legitimate security testing and potential misuse.

> Flipper Zero's sub-1 GHz module is capable of receiving signals at all frequencies in the 300-348 MHz, 387-464 MHz, and 779-928 MHz operational bands. However, **Flipper Zero transmits signals only at frequencies that are allowed for civilian use**. (Flipper Zero Documentation, n.d., Sub-GHz section, Frequencies subsection, para. 1)

This teaching case offers an opportunity to engage with the FZ and, by extension, understand something about the importance of the EMS.

WARNING: IT IS POSSIBLE TO USE THE FZ FOR POTENTIALLY ILLEGAL OR UNETHICAL ACTIVITIES; BE CAREFUL HOW YOU USE IT.

The FZ recently made headlines when it came to the attention of members of the Canadian government, who consider it sufficiently dangerous to discuss potentially banning it (Comeau, 2024).

2. OVERVIEW

This exercise was created to provide exposure to the EMS generally and the FZ hardware device specifically. While many students are likely to have heard of the EMS and have a basic understanding or awareness of it, there is probably much more that can be learned. For example, students are often surprised to realize that since the part of the EMS (Figure 3) we call visible light can be seen with our eyes, that part of our body can be considered a type of antenna tuned to a particular frequency range (400-790 THz) in the EMS. And that if we had the ability to turn a dial in our heads to tune into different frequency ranges, we might be able to "see" radio waves or the waves bouncing around the inside of a microwave oven.

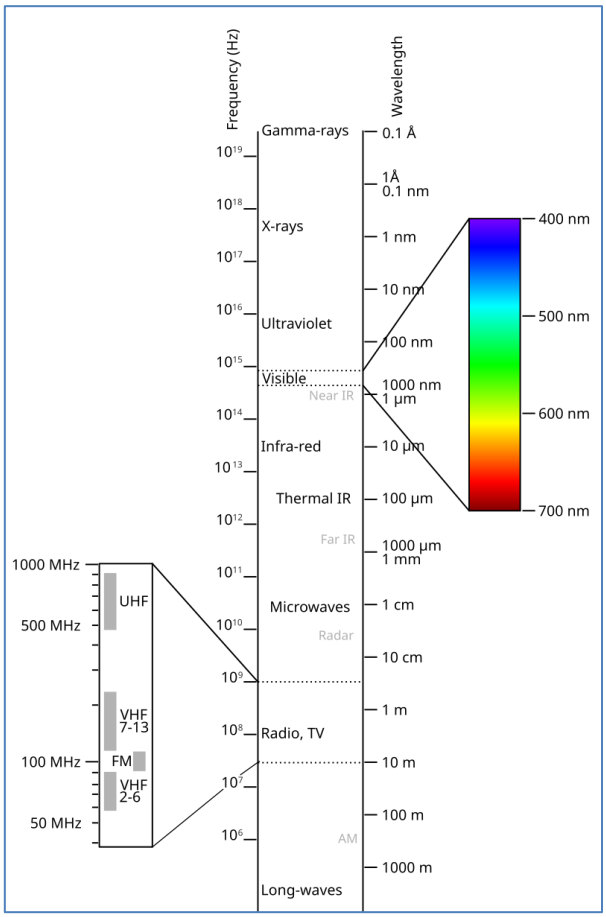

Figure 3: Frequency range of the EMS (Electromagnetic Spectrum, 2024)

ISSN: 2473-4901
v10 n6232

3. CASE COMPONENTS

There are quite a few experiments that can potentially be done with the FZ. In this paper, we describe five:

- Conduct warwalking
- Brute force TV signal
- Mimic a particular TV signal
- Emulate an access card
- Copy a garage door opener

Experiment 1 – Conduct Warwalking
This experiment provides a nice introduction to both the FZ and some of the signals that are often bouncing around the area in which we live and work. Warwalking involves moving through an area using the FZ to discover wireless signals and identifying devices broadcasting within the sub-1 GHz frequency bands via the FZ's built-in module (https://docs.flipper.net/sub-ghz#kfpN7). Steps include:

1. Power on the FZ. Go to Main Menu – Sub-GHz – Frequency Analyzer.
2. The FZ will scan within the 300-348, 387-464, and 779-928 MHz bands.
3. Begin walking around, preferably in a more public area; signals found while using the frequency analyzer will be displayed on the screen as in Figure 5.
4. Once a signal is found, try capturing the signal. Go to Main Menu – Sub-GHz – Read RAW (Figure 6).
5. Using the received signal strength indication (RSSI) functionality available with Read RAW and by looking around for electronic devices, try and determine from where the signal is emanating.

Maintain a log of the different frequencies encountered. For each frequency, use the Read RAW function to capture the signal and try to identify the source.

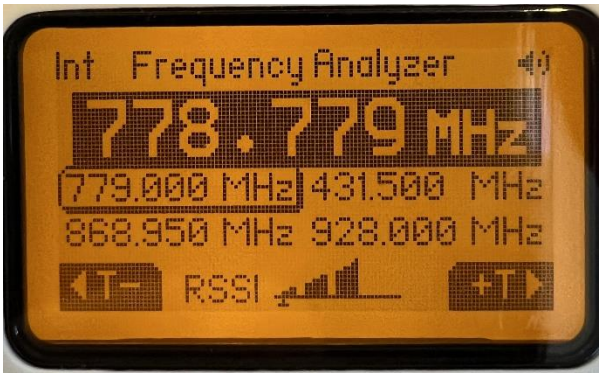

Figure 5: Result of warwalking with the FZ

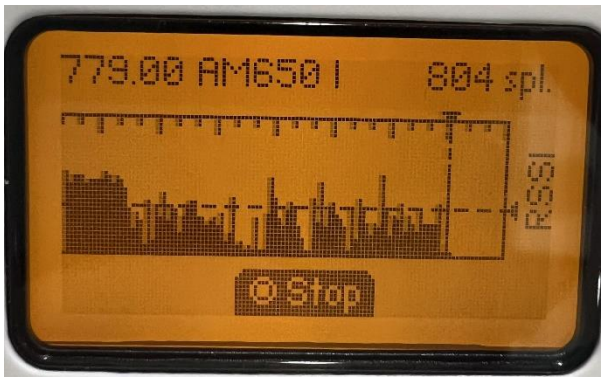

Figure 6: Scanning (raw read) of a particular frequency identified while warwalking.

Experiment 2 – Brute Force TV Signal
In addition to the sub-1 GHz antenna, the FZ has an infrared (IR) module (https://docs.flipper.net/infrared#FOaB8). As shipped, the FZ has a dictionary file that contains hundreds of different infrared remote-control protocols. Find and examine the contents of the *tv.ir* file (Figure 7).

```
#
name: Power
type: parsed
protocol: NEC
address: 08 00 00 00
command: 05 00 00 00
#
name: Vol_up
type: parsed
protocol: NEC
address: 08 00 00 00
command: 00 00 00 00
#
name: Vol_dn
type: parsed
protocol: NEC
address: 08 00 00 00
command: 01 00 00 00
#
```

Figure 7: Sample of IR protocols

ISSN: 2473-4901
v10 n6232

Attempt to power on a TV using the FZ as the remote (Figures 8 & 9). Try to navigate the FZ menu using your intuition or consult the online documentation. If you cannot figure it out, ask your instructor for hints about the steps to take.

Log the make/model of the TV that was successfully turned on and try to identify from the *tv.ir* file which protocol command set worked.

Figure 8: Using the TV remote brute force feature.

Figure 9: Successfully brute force powering on three of the same TVs at the same time.

Experiment 3 – Mimic a Particular TV Signal

In addition to operating as a universal remote and brute-forcing commands, the FZ can also detect specific IR signals. After identifying a frequency, the FZ can scan it to identify specific protocols used by the scanned TV remote and emulate that signal (Figures 10 & 11).

Attempt to capture the signal from a TV remote (or any device remote like an air conditioner, ceiling fan, etc.) and use that signal to control the TV rather than using a brute-force approach, as in Experiment 2. Once again, navigate the FZ menu using your intuition or consult the online documentation. If you cannot figure it out, ask your instructor for hints about the steps to take.

Figure 10: Scanning and identifying a particular TV remote control.

Figure 11: Using a particular TV remote protocol to control the TV.

Log the make/model of the TV (or other device) for which a signal was captured, saved, and used successfully to power on a device.

ISSN: 2473-4901
v10 n6232

Experiment 4 – Emulate a Smart Card

WARNING: IT IS POSSIBLE TO USE THE FZ FOR POTENTIALLY ILLEGAL OR UNETHICAL ACTIVITIES; BE CAREFUL HOW YOU USE IT

Never copy an access card without explicit permission. Ensure that such a copy does not remain on the FZ. Failing to protect access credentials could result in the use of those credentials for unauthorized access, exposing all those in the chain of access to legal and/or disciplinary action.

In addition to the sub-1 GHz and IR modules, the FZ has a dual-band RFID antenna (https://docs.flipper.net/rfid#ctlrU) that supports low-frequency (125kHz) and high-frequency (13.56 MHz) RFID technology. For this experiment, explore extending FZ capabilities with an app to read and emulate RFID smart cards.

One way to do this is to download and install qFlipper (Figure 12), a desktop application for updating the FZ firmware via a computer, (https://flipperzero.one/update - available for Windows, macOS, or Linux) to extend the FZ capabilities with the PicoPass app. Once installed, use the FZ's RFID reader to allow the scan and capture of RFID data (Figures 13 & 14). Then, test the FZ's ability to emulate the data by attempting to use the FZ in place of the original card (e.g., to use a common area copier/printer or unlock a door/access a secure area – Figures 15 & 16).

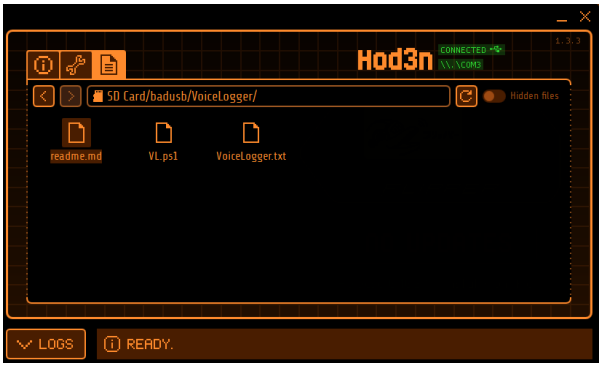

Figure 12: qFlipper PC Menu

How close does the FZ need to be to the smart card to capture the data?
Try reading the card when both the FZ and card are flat on the same surface and when the FZ is above the smart card.

Can a smart card in someone's pocket be read by the FZ when standing behind or beside them?

Many wallet manufacturers now offer RFID-blocking models or sleeves. If one is available, try reading a smart card through one of these wallets (Figure 17).

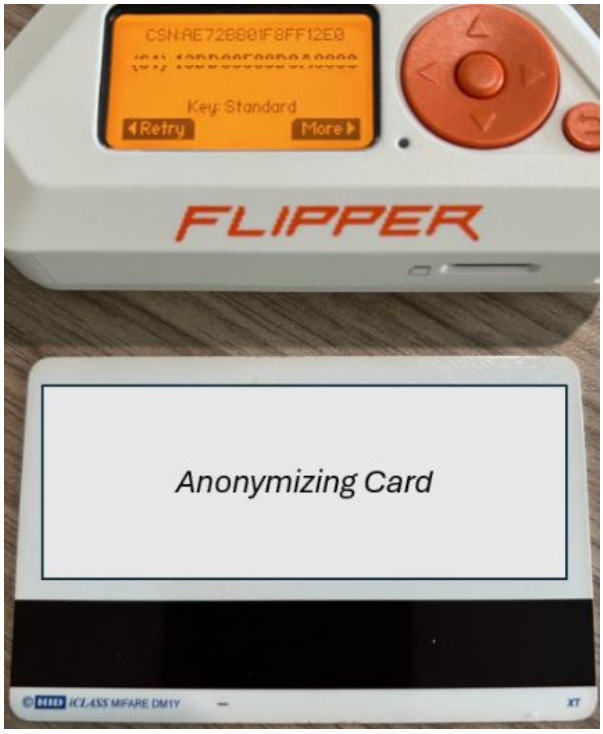

Figure 13: Reading a smart card.

Figure 14: Vertical distance at which reading smart card was possible.

Smart card technology can seem just as magical as the EMS to many people. How exactly does smart card RFID technology work? How are smart cards constructed to harness the power of the EMS?

ISSN: 2473-4901
v10 n6232

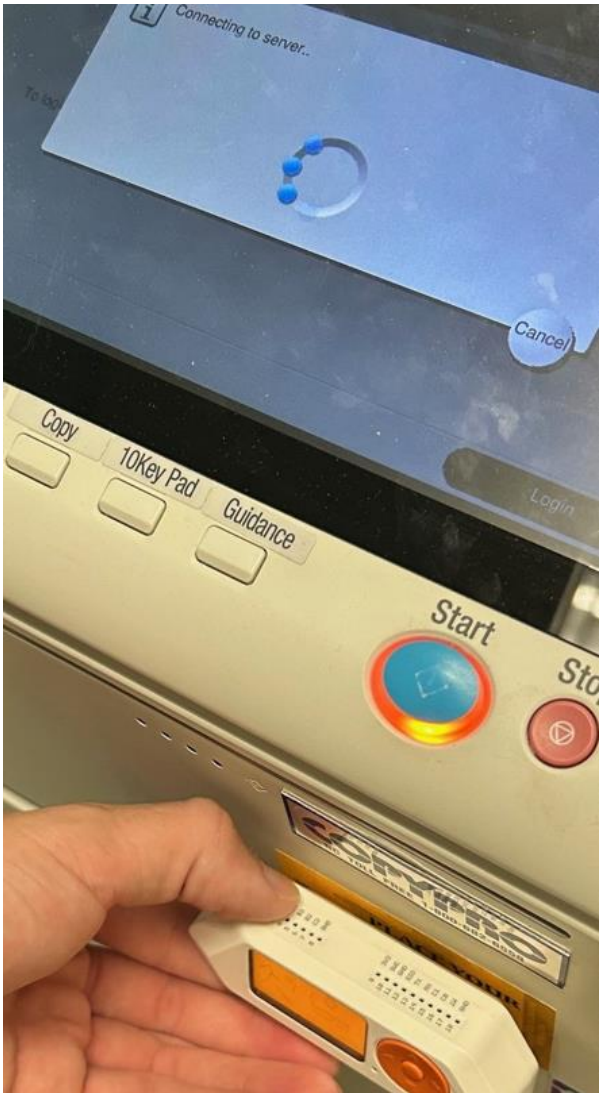

Figure 15: Emulating smart card to access copier/printer.

Experiment 5 – Copy a Garage Door Opener

The idea of this final experiment is to become more aware of some of the realities of EMS management. The National Telecommunications and Information Administration (NTIA) within the US Department of Commerce is responsible for managing the federal government's use of the EMS. On the NTIA's website (https://www.ntia.gov/category/spectrum-management) are posted the words, "Spectrum Management – Protecting a Vital, Limited Resource" (National Telecommunications and Information Administration, n.d.). Because uncoordinated use of any frequency in the EMS can cause interference and thus impact the efficient use of technologies reliant on EMS, it must be managed.

Figure 16: Emulating a smart card to gain access to a locked room.

Figure 17: RFID blocking wallet successfully protects smart card.

This experiment, in part, shows how the FZ creators try to abide by the rules and laws

ISSN: 2473-4901
v10 n6232

established for the management of the EMS. Try to figure out how to capture a garage door opener frequency (Figure 18) and then attempt to replay it (Figure 19).

There are various rules, regulations, and laws that govern the use of the EMS by civil authorities, the military, and civilians. The official FZ documentation provides a bit of information about what frequencies are approved for civilian use in the US. Can you discover what they are?

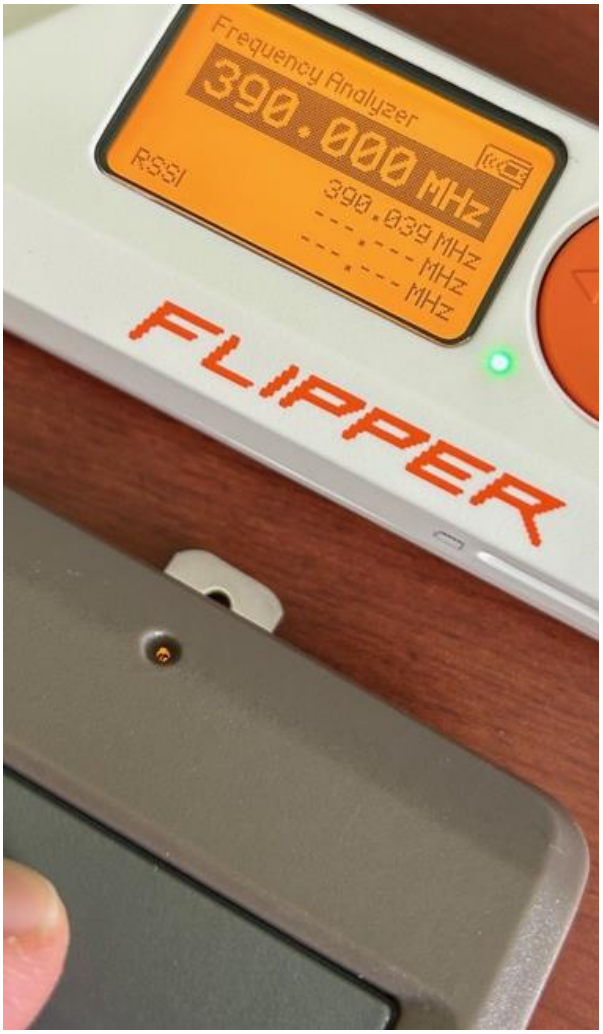

Figure 18: Discover garage door frequency

6. CONCLUSION

This teaching case with accompanying experiments should provide an improved awareness and understanding of the EMS. Also, it should provide a practical appreciation for some of the security risks associated with technologies that use the EMS, some of the capabilities of the Flipper Zero, and some of the challenges in managing the EMS. In addition to technical aspects of signal detection, analysis, and replication, it should also help participants gain insight into the ethical considerations and real-world implications of using the EMS. The Flipper Zero is a versatile educational tool offering hands-on experience in a wide range of wireless security topics. Students should find this hands-on approach to learning about EMS engaging and fun.

Figure 19: Garage door signal cannot be broadcast

7. REFERENCES

Clarke, A.C. (1958/1973). Profiles of the Future, An Inquiry into the Limits of the Possible, revised edition. Harper & Row. https://archive.org/details/profilesoffuture0000clar/page/20/mode/2up

Comeau, J-S. (2024 February 2). Government of Canada hosts National Summit on Combatting Auto Theft. https://www.canada.ca/en/public-safety-canada/news/2024/02/government-of-canada-hosts-national-summit-on-combatting-auto-theft.html

Electromagnetic spectrum. (2024, May 20). In Wikipedia. https://commons.wikimedia.org/wiki/File:Electromagnetic-Spectrum.svg

Flipper Zero Documentation. (n.d.). Retrieved August 9, 2024, from https://docs.flipper.net/

Hacksmith Industries. (2014, February 12). *What's Inside A Thin Prox Card?* YouTube. https://youtu.be/CGzfljFnWhU?si=GEtgvMOCRjRBFsZ3&t=59

National Telecommunications and Information Administration. (n.d.). Retrieved August 13, 2024, from https://www.ntia.gov/category/spectrum-management

Shop Flipper (2024). https://shop.flipperzero.one/?srsltid=AfmBOoqR_OMc6cPhlOlcHu6ouaWatKPlO1Q_ezt_MbgZ_qb4DTCG7vnk

ISSN: 2473-4901
v10 n6232

Woolf, V. (1928). *Orlando a Biography*. Harcourt, Brace and Company. https://archive.org/details/orlandobiography0000virg/page/300/mode/2up

Zhovner, P., Zakharov, A., & Nadyrshin, R. (2024, March 19). Our Response to the Canadian Government. https://blog.flipper.net/response-to-canadian-government/