Flipper Zero: Capabilities, Risks, and Mitigations

Christopher May

College of Humanities and Computing, Limestone University

CS 470: Capstone

Dr. Jane Watkins

March 30, 2025

Flipper Zero: Capabilities, Risks, and Mitigations

Cybersecurity is one of the most volatile industries to the constant and increasing growth of new technologies developed from year to year. It is common for workers in the field to restructure and re-secure their infrastructure to make sure their systems maintain the necessary security due to the release of new technology that renders their previous security measures irrelevant and ineffective. One of the new tools to demonstrate this need is the Flipper Zero. This paper investigates Flipper Zero's features (Flipper Devices Inc., n.d.), security risks (Johnson, 2024), how it works, its accessories (ZDNET, n.d.), and how it compares to similar preexisting tools. The goal is to inform those involved in cybersecurity about this emerging threat and how to protect your systems. The Flipper Zero has great potential as an educational tool for penetration testing, but also presents big risks like unauthorized access, data stealing, and exploitation. Its accessibility and low barrier for entry make it a device that can cause serious vulnerabilities to security if the cybersecurity industry does not properly analyze its abilities and adapt to this threat. While its base tools are impressive, the real problem comes with how easily it can be expanded with accessories using the General-Purpose Input/Output (GPIO) pins. This device doesn't just run scripts or copy NFC signals and re-emit them seamlessly. It can also be used to mirror, create, or takedown networks; sniff packets being transmitted wirelessly; bypass security on electric safes; or even mimic an HID that can change system settings, open backdoors, retrieve data, or initiate reverse shells. This paper argues that the Flipper Zero's versatility, affordability, and low skill requirement make it a uniquely dangerous device in the modern cybersecurity landscape, one that requires both public awareness and technical mitigation to counter.

Flipper Zero is a small, portable cybersecurity tool that runs on open-source firmware and has hardware that can be customized. It has a small screen, navigation buttons, and wireless modules like NFC, RFID, infrared, and Sub-1GHz. It also has a USB connection to send or receive data. All of this is sold openly online for a one-time payment of $170 (Flipper Devices Inc., n.d.). The Flipper has grown popular on sites like GitHub, Reddit, and Discord, where people upload and share custom scripts and firmware (Johnson, 2024). These unmoderated changes grow the Flipper's capabilities far beyond what is marketed. One of the most common uses is to impersonate a keyboard or mouse with BadUSB. This allows an attacker to plug the device into someone's computer and automatically run code or scripts. It could install malware, open backdoors, or start a reverse shell, all in just a few seconds. This is way faster than doing the same thing manually. Another feature is RFID cloning. An attacker can copy wireless signals from keycards or badges just by getting close to them. For example, putting a Flipper near someone's wallet for a few seconds might be enough to steal access to a building. There are also tools like "RFID fuzzing", which crash or confuse scanners by sending unexpected signals. The GPIO pins (General Purpose Input/Output) on the Flipper allow people to connect other devices or tools. This is where things get even more serious. It's not just copying signals or running scripts. It can be used to attack wireless networks, sniff data being sent through the air, or even pretend to be a USB device that changes system settings.

With all of these capabilities, one might be asking themselves, "Why haven't I seen these before?" And the answer is these tools have existed for decades, only separated into different devices. One common example is the Rubber Ducky (Hak5, n.d.), a device the size of a thumb drive with USB C and A connections that emulate pre-programmed keystrokes at high speed. This has been the standard tool for BadUSB attacks that inject malicious commands when

plugged into a target machine (Bishop, 2022). However, while it might be faster and smaller, the Rubber Ducky comes with no wireless capabilities, no interface, lacks expansion, and is around $45. Another similar device is the WiFi Pineapple (Hak5, n.d.), which is known for its powerful Wi-Fi auditing, professional-grade tools, and browser interface. This device is used primarily for penetration testing and identifying vulnerabilities in network security. While this device is more powerful, it is much bigger, costs around $300, and has a much steeper learning curve. When the Flipper Zero was released, it quickly became the best of both worlds. Powerful, but while remaining a lower barrier for entry.

The Flipper Zero is a double-edged sword. It holds extreme power and can be used for good, but also for bad. Its combination of low price point and low knowledge barrier make it a great starter tool for those looking to get into cybersecurity and data protection. Anyone can buy one online, and tutorials are everywhere (Johnson, 2024). One does not have to be an experienced hacker to use it, they only must have the desire and persistence to learn. This creates a lot of risk for businesses and regular people. Someone could walk by a stranger on the street with a Flipper in their pocket and steal their RFID signal, or they could plug it into an unattended computer and install malware in seconds (ZDNET, n.d.). On the other hand, they could perform device configuration and penetration testing to help secure their networks. Either way, updates and scripts are easy to install and execute, putting the power into the hands of the public.

Protecting against devices like the Flipper Zero means doing two main things: educating people and improving technical defenses. Education is the first step. People need to know not to leave phones and laptops alone in public. RFID badges should be stored in protective sleeves, and companies should warn employees about new devices like this (Johnson, 2024). On the tech side, using NFC encryption, turning off unused USB ports, and requiring two-factor

authentication helps. Organizations should also do regular security audits and stay updated on tools being used in the field, even ones sold as educational toys.

The Flipper Zero is a versatile and accessible tool that blurs the line between ethical testing and malicious exploitation. Its affordability, compact design, and open-source extensibility make it a powerful asset for security professionals, and a dangerous weapon in the wrong hands. As demonstrated in this report, the device consolidates functions once limited to expensive, specialized tools, and lowers the barrier for entry into cybersecurity operations. While this paper only scratches the surface of its potential, it is clear that the Flipper Zero represents a growing concern for system administrators, businesses, and end users alike. Proactive education and defensive strategies are essential to stay ahead of emerging threats like this one.

References

Johnson, S. (2024, December 17). *Everything you can do with a flipper zero, from perfectly legal to slightly shady*. Lifehacker. https://lifehacker.com/everything-flipper-zero-can-and-cant-do

Flipper Zero - portable multi-tool device for geeks. FLIPPER. (n.d.). https://flipperzero.one/

Now Android and windows devices aren't safe from Flipper Zero either. ZDNET. (n.d.). https://www.zdnet.com/article/now-android-and-windows-devices-arent-safe-from-flipper-zero-either/

Hak5. (n.d.). *WiFi Pineapple*. Hak5. https://shop.hak5.org/products/wifi-pineapple

Hak5. (n.d.). *USB Rubber Ducky*. Hak5. https://shop.hak5.org/products/usb-rubber-ducky

Bishop, S. (2022, August 15). *The new USB Rubber Ducky is more dangerous than ever*. The Verge. https://www.theverge.com/23308394/usb-rubber-ducky-review-hack5-defcon-duckyscript