Issues in Information Systems
Volume 25, Issue 2, pp. 84-95, 2024

DOI: https://doi.org/10.48009/2_iis_2024_107

Unveiling exploitation potential: a comparative analysis of flipper zero and rubber ducky

Robert Pava, *Robert Morris University, rjpst280@mail.rmu.edu*
Reese Martin, *Robert Morris University, rgmst170@mail.rmu.edu*
Sushma Mishra, *Robert Morris University, mishra@rmu.edu*

Abstract

Penetration testing is an important security control to ensure that unsolicited malware or threat vectors are not allowed access to the private network. This paper presents a comparative analysis of the Rubber Ducky and Flipper Zero devices as tools for penetration testing in physical and network security domains. The study assesses their effectiveness in simulating real-world attack scenarios, and their adaptability in different threat situations. The goal is to provide a comprehensive guide for leveraging these devices to improve organizational defenses against physical and network-based threats. This research is intended to raise awareness and facilitate informed decision-making among security professionals, policymakers, and technology enthusiasts by outlining the capabilities, benefits, and risks associated with these devices. The findings indicate that the Flipper Zero device, due to its robustness and versatility in network security, should be seriously considered as a potential security threat. The paper also identifies the implications of the study and its limitations.

Keywords: flipper zero, exploitation, rubber ducky, threat assessment, network security, security controls

Introduction

Cybersecurity has increasingly become more challenging due to the forever evolving nature of the threat vectors around the Internet. The importance of security within the workforce is driven by the vast amounts of sensitive information stored within organizational networks. Penetration testing tools like the Rubber Ducky and Flipper Zero, which can be exploited by insider threats or cybercriminals, pose significant risks to information security. This paper evaluates these devices' effectiveness, capabilities, and risks in compromising secured systems, emphasizing the urgency of regular system testing and staying informed about the latest penetration tools.

Our research goal is to compare the Rubber Ducky and Flipper Zero, highlighting their distinct methods for breaching security and the implications for organizational trust and data protection. Rubber Ducky attacks can swiftly compromise inadequately protected computers, undermining trust and security by capturing sensitive credentials and personal information. The Flipper Zero extends these threats with its multifunctional capabilities for various cyber-attacks. This paper analyzes these devices' practical applications and potential dangers on physical and network security. The outcomes of our study will inform security professionals on best practices for safeguarding networks against such advanced penetration tools, thereby mitigating risks of data breaches and unauthorized access.

The Rubber Ducky with the ability to act like a keyboard to execute payloads can compromise computers that are not fully protected in a matter of seconds. (Cannols & Ghafarian, 2017) The exploration of this device is growing rapidly with cybercriminals using tools such as this to execute scripts to collect personal information. Alongside personal information, the Rubber Ducky creates an erosion of trust in machines. The ability to gain so much information from a Rubber Ducky can be damaging to organizations through collecting keystrokes. These keystrokes can collect credentials among other identifying information about a worker or a client. The Flipper Zero creates this erosion also through "signal capture and analysis to RFID/NFC cloning, Bluetooth vulnerability assessment, network sniffing, keyless entry system assessment, physical layer attacks, device identity testing, replay attacks, and more." (Winston, 2023). These attacks, along with being able to complete tasks that relate to the Rubber Ducky, have many other features. This creates the device to act as a Swiss army knife when it comes to penetration testing tools and what it can achieve. This paper also aims to describe the overall capabilities, benefits, and risks associated with such devices with the hope that individuals can better understand and protect the networks from outside threats, data breaches, and network compromises.

The paper is structured as follows: it begins with a comprehensive literature review on the Rubber Ducky and Flipper Zero in the context of physical and network security, providing a solid foundation for our research. We then detail the methodology used in our study. The discussion section presents our findings and compares the capabilities of these devices. Finally, the paper concludes with a summary of the study and suggests potential avenues for future research in this critical area of cybersecurity.

Literature Review

One way that these devices can be looked at in pen testing is in terms of endpoint security. Endpoint security is defined as "the cybersecurity approach to defending endpoints — such as desktops, laptops, and mobile devices — from malicious activity" (Aarness, 2024). This form of security has arguably become increasingly important over the years. Users are susceptible to receiving phishing emails that contain malicious files. These files can do a number of things such as provide attackers with backdoors into information systems, get users' password information, and much, much more. Besides phishing emails, USB drives can be utilized as a method of intrusion. Through the USB port of any given computer or system, the Flipper Zero and the Rubber Ducky can execute USB attacks. These attacks often emulate keystrokes on a keyboard. This way, an attacker can gain access to sensitive information. Users of the Rubber Ducky can write Ducky script, the Rubber Ducky's custom scripts, so that keystrokes can be injected into their personal computer (Cannols & Ghafarian, 2017). These scripts can be used for a variety of purposes including changing file information, accessing websites, and downloading and executing files.

Many antivirus programs, such as Symantec Endpoint Protection, provide security on USB ports. These programs will stop a USB device from being used so that foreign scripts may not be detonated. However, the USB Rubber Ducky relies on the fact that most of these programs, and computers, do not block keyboards. The Rubber Ducky is purposefully created so that it can be seen by the computer as a keyboard and perform keystroke injections on a machine (Hak5, 2018). For example, the command 'GUI r' opens the run dialog box on a Windows machine. From here, the command 'cmd' can be run to open the command prompt. With this open, the Rubber Ducky is unrestricted in its ability to run commands that may potentially harm the user's system.

In a similar fashion, the Flipper Zero can also execute bad USB attacks. It can "emulate a USB keyboard and mouse, and can execute scripts that can control a graphical user interface—a boon for those seeking to automate tasks, another security headache for others" (Cass, 2023, p. 3). The distinct difference between

the Rubber Ducky and the Flipper Zero when it comes to executing these scripts is the method of activation. The Rubber Ducky automatically runs the script that it was programmed with once it is plugged into a computer by default. Conversely, the Flipper Zero has to manually be activated in order to detonate a script. This can be done both from the Flipper itself or through a mobile device, such as a phone. By using Bluetooth, users can connect to the Flipper Zero and control the device through their phone ("Settings," 2024). Both devices provide an ample way to pen test the USB security of computers.

In order to program bad USB attacks, users will need access to PayloadStudio from Hak5. PayloadStudio is an IDE that users can use to develop Ducky scripts ("PayloadStudio," 2023). Hak5 offers a free version and a premium version of PayloadStudio. For this paper, PayloadStudio Pro, the premium license of the application, will be utilized. The pro edition offers "access to every convenience and configuration option PayloadStudio has to offer" ("PayloadStudio," 2023). After creating a script in PayloadStudio, it can be loaded into the Rubber Ducky and Flipper Zero for the devices to perform.

Network Security

Flipper Zero and Rubber Ducky can also be used to pen test network security. Network security can be defined as "a discipline concerned with protecting networks and computer systems against threats such as hacking exploits, malware, data leakage, spam and Denial of Service (DoS) attacks, as well as ensuring trusted access through mechanisms such as IPsec or SSL" (Schneider, 2012, pp. 14-20). This is an ever-evolving space that is constantly faced by new threats.

The USB Rubber Ducky is primarily used for endpoint attacks, but it can additionally be used for network security attacks. For instance, there have been cases in which the Rubber Ducky has been used to steal and exfiltrate Wi-Fi passwords. First, "the attacker will try to get physical access into the computer to run [a] Wi-Fi password stealing program" (Harianto & Gunawan, 2019, pp. 745-752). From there, the Rubber Ducky opens the command prompt as an admin to disable the computer's firewall. This is needed so that certain commands can be ran without interruption and "to avoid the protection from the firewall to certain features, such as File Transfer Protocol (FTP)" (Harianto & Gunawan, 2019, pp. 745-752). From here, the Rubber Ducky creates a Wi-Fi directory, extracts the Wi-Fi information, executes Visual Basic (VB) scripts to compress and zip files, and sends the information to the attacker via FTP (Harianto & Gunawan, 2019, pp. 745-752). The script runs the command 'netsh wlan export profile key=clear' to extract all Wi-Fi information ever connected to the computer and exports it to Extensible Markup Language (XML) files. Then, the VB script "will create an empty zipped file and put the source folder inside the empty zipped file" (Harianto & Gunawan, 2019, pp. 745-752).

Once the file is ready, the script will open a connection to the attacker's server through FTP, and it will be uploaded using passive mode and binary transfer method. The Rubber Ducky will finalize the attack by "closing FTP connection, deleting Wi-Fi folder, deleting VB script, deleting Wi-Fi.zip, enabling [a] firewall, and closing the command prompt" (Harianto & Gunawan, 2019, pp. 745-752). This can be used to pen test network security to detect if there are measures in place to detect unnecessary FTP connections being made reaching out to external IPs. These detections can be set up with many systems such as Splunk and Symantec Endpoint Protection. Another example of attack utilizing the Rubber Ducky would be to take a user to a malicious website and have them download and run a virus. For this to occur, the Rubber Ducky would open the run dialog box, type "msedge.exe", paste in the website, and, lastly, download the file. Depending on the website, there would need to be some additional keystrokes in order to download the file or maneuver the site. For this project, we do not have any trusted websites or viruses to download onto our machine. As a result, we will need to demonstrate the Rubber Ducky performing this action, but instead by going to a legitimate site, obtaining a file, and running the file.

The Flipper Zero itself cannot connect to or interact with a network. It needs a Wi-Fi development board in order for it to interact with the internet. Out of the box, the Wi-Fi dev board allows the Flipper to wirelessly update its firmware, provide debugging with the Black Magic Probe firmware, and supply an ESP32-S2 board which allows Wi-Fi penetration testing (PMKID capturing, deauth, and more) ("WI-FI Devboard for Flipper Zero," 2021). This permits the Flipper Zero to acquire custom firmware and interact with the network. Because the Black Magic Probe is only an "in-application debugging tool for embedded microprocessors," we will be flashing Marauder onto our board ("Blackmagic," 2017).

Marauder allows Flipper Zero to connect to the network and interact with the internet. With Marauder installed, it allows the Flipper to perform attacks against a network. For example, users can "target an access point with a flood of deauthorization packets, killing active connections" (Cass, 2023, p. 3). The Flipper does this by scanning and intercepting packets from the surrounding networks. The user can choose to let it run for a while or stop it after so much scanning. From there, the Flipper compiles a list of all the network packets that it received and numbers them 1-however many networks were scanned. The user can then decide which network they would like to attack. The network does not allow any devices that are connected to it to use the network as long as the Flipper is running the attack. Another attack that can be performed with Marauder is the Rick Roll attack where "you can spoof a series of access-point names, so the list of Wi-Fi networks in your area is spammed, line by line, by the lyrics to Rick Astley's 'Never Going to Give You Up,' in an unusual version of Rickrolling" (Cass, 2023, p. 3). We performed this attack on our own network, and it worked as pictured in Figure 1:

Figure 1: Example of Rickrolling

Another attack the Flipper Zero can perform involves stealing Wi-Fi passwords (Sasquach, 2024). By using the Marauder software, users can capture the pcaps of the networks that are within the area of the Flipper. The user will first need to capture the packets of the networks around the Flipper. This allows the user to target specific networks. Then, the user needs to sniff the network using PMKID so that they can target the Wi-Fi access point and trigger a deauthentication attack toward the network. From there, pcaps need to be pulled off of the Flipper's SD card. Finally, the user can use hashcat and some custom software to extract the Wi-Fi network's password (Sasquach, 2024). Both of these devices are incredibly useful when it comes

to pen-testing as they allow cyber professionals access to methods of attack that they may not have had before.

Methodology

The data was collected by performing different attacks with the Flipper Zero and Rubber Ducky devices on a Windows 10 virtual machine. All tests were run with Windows Defender turned off. We installed the Xtreme firmware on the Flipper Zero. To install the Xtreme software, we visited https://Flipper-xtre.me/, connected the Flipper to the PC, and installed the latest version of Xtreme at the time (XFW-0053). This software helped improve the UI of the Flipper and organized some of the programs. To obtain more scripts, we loaded files from GitHub: https://github.com/skizzophrenic/Ubers-SD-Files (Skizzophrenic, 2023). These files contain different kinds of attacks (BadUSB, Bluetooth, Network, etc.) that we searched through and used for this paper. The following are a few examples of the scripts that were used in the paper:

For the first test, we used a script that was developed by us. The DuckyScript will reveal the network password that the PC is connected to and is shown below in Table 1. It should be noted that before running the script, the user must change the name to the network name in the script to the network. Prior knowledge of the network name will be required.

Table 1: The DuckyScript

```
DELAY 2000
WINDOWS r
DELAY 2000
STRING cmd
ENTER
DELAY 2000
STRING netsh wlan show profile name=<enter network
name here> key=clear
ENTER
```

The second test that was run was used with scripts from the GitHub mentioned earlier in the paper and is shown in Table 2. This plays a text version of Rick Astley's 'Never Going to Give You Up' and it will continue to play it until the command prompt is closed or the command is canceled.

Table 2: The Rickrolling

```
REM Title: Rick Roll Windows CMD
REM Author: Nando Kools | NanKooDev
REM Description: RickRoll in Windows Command
Prompt
REM Target:      Windows
REM
GUI r
DELAY 1000
STRING curl http://ascii.live/rick
ENTER
DELAY 750
ALT ENTER
```

All scripts that can be used in this paper can be provided if requested or can be found on https://github.com/skizzophrenic/Ubers-SD-Files. We also flashed the marauder software on the Wi-Fi dev board so that we can interact with the network. All executed scripts were either programmed by us or obtained via GitHub. The next section will show the results of our experiments.

Results

We are now going to present the results of our tests. Below is the physical security.

To obtain the Wi-Fi password we plugged in the Rubber Ducky with written script loaded on it. The command in Figure 2 will reveal the password of the network that the computer is connected to. For this to work, the network name needs to be known. We can also have the command listed here put the information into a text file with a > filename.txt at the end of the command.

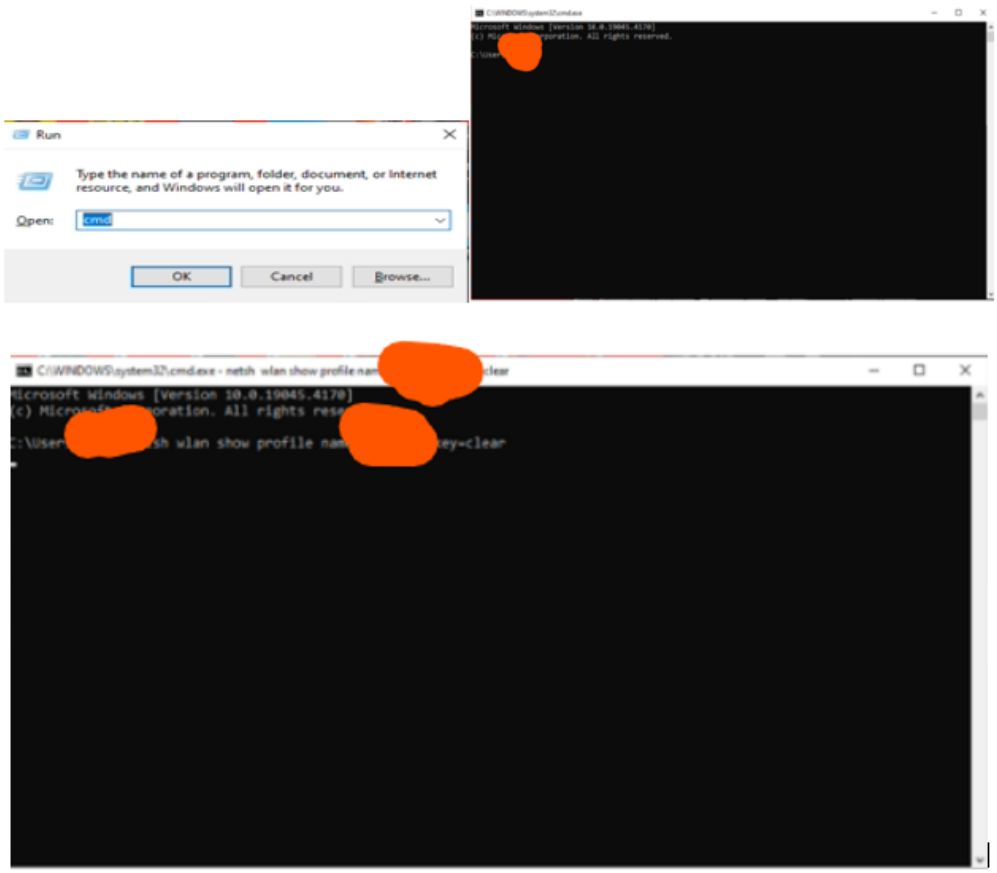

Figure 2: Obtaining Wi-Fi Password:

Executing the program runs a text "video" of *Never Gonna Give You Up* by Rick Astley and is shown in Figure 3. While this program is not harmful, it does lock the user out of the computer until they hit alt + f4 to close the command prompt.

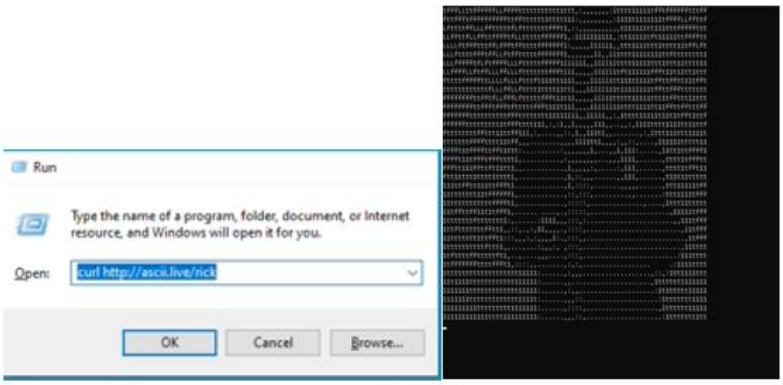

Figure 3: Executing the Program

This file locks the user out of the computer. As seen in Figure 4 the script goes to a GitHub page, downloads, and executes the file. The user needs to restart the computer, and it will go away.

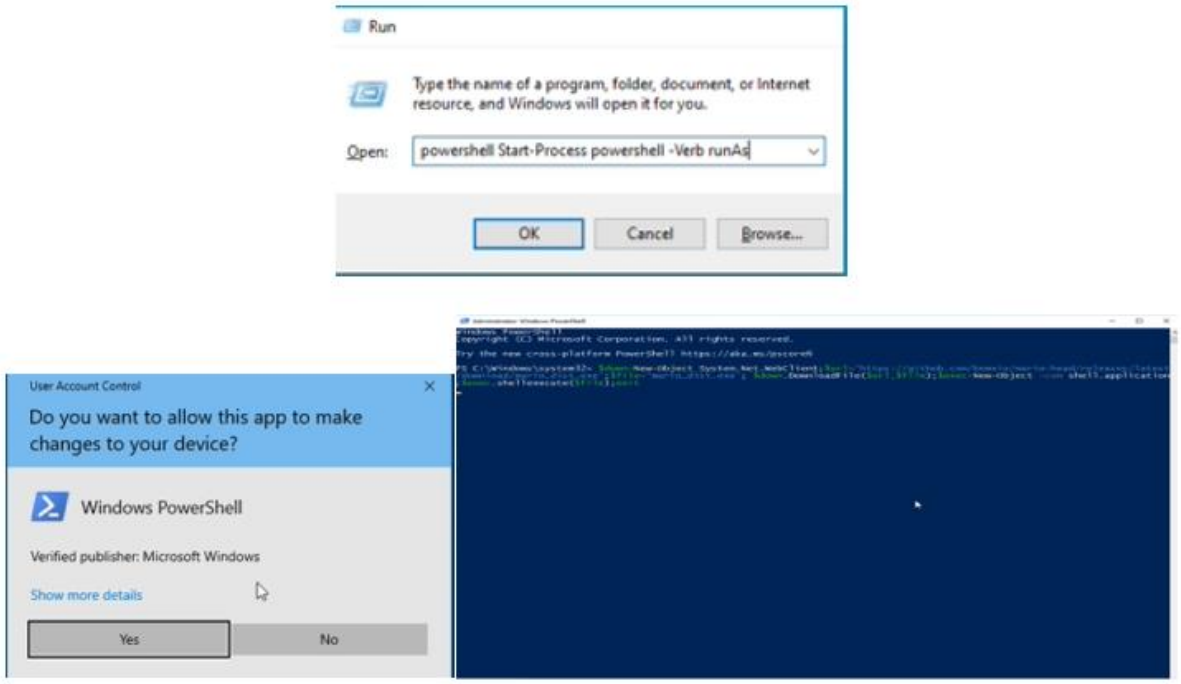

Figure 4: Download and Execute Files

Figure 5 shows that both the Rubber Ducky and Flipper Zero can create and write files. This was obtained from a GitHub for Flipper Zero but was detonated using a Rubber Ducky since it was written in Ducky Script.

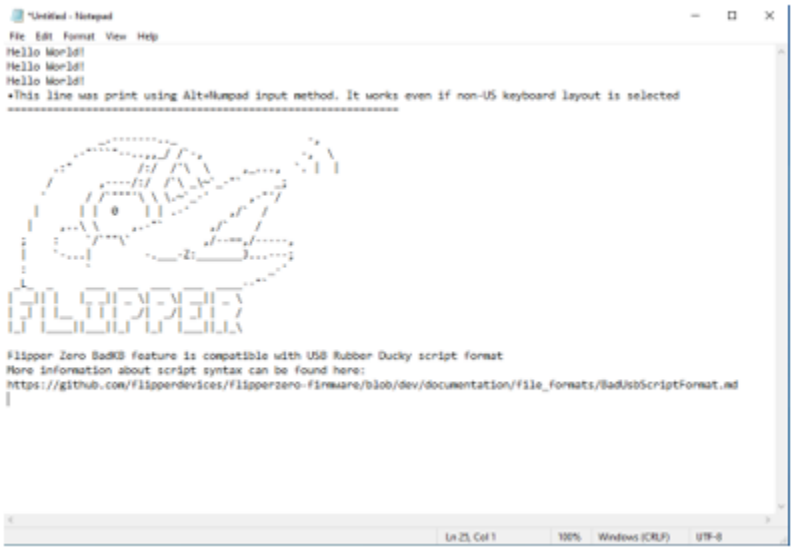

Figure 4: Download and Execute Files

This line takes the user to a fake blue screen website and goes into full screen, tricking the user into thinking that the computer has had an error. While this is not harmful, the script could have taken the user to places that were.

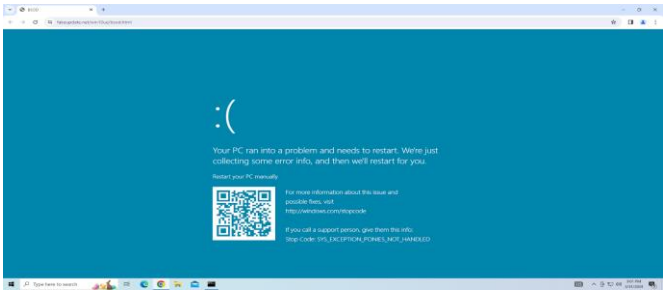

Figure 6: Goto URLs

Network Security:

We are now going to discuss the results of our network security tests. Figure 7 illustrates a Rick Roll attack spoofing a Wi-Fi network. It creates multiple fake networks to the lyrics of Rick Astley's *Never Gonna Give You Up*. This can be used to steal people's log in credentials, credit card information, and much more.

Figure 7: Spoofing Wi-Fi Networks

Figure 8 illustrates a deauthentication attack. This attack will kick the other devices that are on the network off until the Flipper stops its attack. However, we did not get this attack to work since the Wi-Fi dev board is only a 2.4 GHz band, and we do not have a 2.4 GHz band Wi-Fi network to attack.

Figure 8: Deauthentication attack:

With the Wi-Fi Dev Board, the Flipper Zero can intercept packets and mark them down in a list for the user of the Flipper to see. As a result, the Flipper can target that specific network to attack. *No picture is shown in this step to maintain privacy of networks that the Flipper had acquired.* Figure 9 shows how the Flipper can sniff raw network data. With this, users can intercept the proper handshakes to be able to get a password. From there, it generates a pcap where it will contain the password. You can then use different tools, that we did not test, to obtain Wi-Fi passwords. Table 3 presents the overview of our findings on network security.

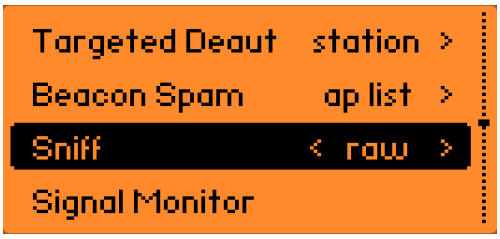

Figure 9: Scanning Raw Network Data

Table 3: Results of network security findings.

Network	Flipper Zero	Rubber Ducky
Spoofing Wi-Fi Networks	Can perform with the use of Wi-Fi dev board	Cannot perform by itself if at all. Potentially could code it and use a third-party software but this has not been tested
Deauthentication Attack	Can perform on 2.4 GHz networks with the use of Wi-Fi dev board	Cannot perform
Packet Capture	Can perform with the use of Wi-Fi dev board	Cannot perform by itself if at all. Potentially could code it and use a third-party software but this has not been tested
Scanning Raw Network Data	Can perform with the use of Wi-Fi dev board	Cannot perform by itself if at all. Potentially could code it and use a third-party software but this has not been tested

Discussion

This paper contributes by shining more light onto the Flipper Zero and Rubber Ducky. There are many other devices that perform similar attacks, such as BadUSB Cable and BadAndroid, and cyber professionals should be made aware of these tools (Do, 2023). However, even with the bad USB attacks that the Rubber Ducky provides, there are limitations of the device. This is the only functionality that it can achieve on its own. With innovations to improve the defense against bad USB attacks, the device can become obsolete.

One innovation is an implementation of a GoodUSB which provides security to the architecture that the bad USB exploits. (Jing Tian et al., 2015) This can provide the example that the Flipper Zero device can better provide pen testing tools than the Rubber Ducky. Though, working with both devices, one device can work better than the other in many areas. Even though the Flipper Zero can achieve many of the same impacts as the Rubber Ducky, it does not mean the Flipper is better than the Rubber Ducky.

For example, if a pen tester were attempting to be discreet, they would find better results with the Rubber Ducky. This is because the Flipper Zero device would need a cable to connect it to the computer, whereas the Rubber Ducky can plug straight in. Also, the size of the Flipper is much bigger than the Rubber Ducky, which would also impact the discreteness one would need. However, the Flipper surpasses the Rubber Ducky through its additional abilities. The following is a comparison of the two Penetration testing tools:

Comparison	Rubber Ducky	Flipper Zero
Method of execution	Used to execute hotplug attacks.	Developed for interaction with access control systems.
Different types of attacks	Some attacks include keystroke injection, backdoors, executing files, and packet capture.	Some attacks include emulating RFID & NFC tags, radio remotes, Bad USB iButton, and digital access key.
Physical/Network Security Capability	The ability to run in both physical security and network security settings.	The ability to run in physical security but requires additional tools to run on network security.
Limitations	Only can run USB attacks.	Can run multiple types of attacks listed above. Some attacks require more hardware or software to be used.

This study has implications for research and practice. The Flipper Zero has advantages over the Rubber Ducky when used as a network pen-testing device. While the Rubber Ducky can be more inconspicuous, having the Flipper Zero in one's possession can be more beneficial when configuring a penetration test or hacking into an organization. Raising awareness about the Flipper Zero in the field of cybersecurity will ultimately help protect networks. As of right now, we were not able to learn too much about the Flipper Zero device's benefits and what it is capable of. By continuing to study the Flipper Zero and its abilities, networks and organizations can become more secure.

Limitations

The price of the Flipper Zero and Rubber Ducky could be a big turn away for people. The Rubber Ducky is, at the time of writing this paper, $79.99 USD (Hak5, 2018). The Flipper Zero, at the time of writing this

paper, is priced at $169.00 USD ("Flipper Zero Shop," 2021). This was not a problem for us, but it is possible that these costs may discourage others. There is also the necessity of needing an expendable system or machine to perform these tests on. The two devices could cause real damage to machines that they are targeted towards. Lastly, we did not have all the resources to test every aspect of the Flipper Zero. For example, we did not have access to a physical access system to test the RFID capabilities on. The final section is the conclusion where we summarize our findings and explore future research problems.

Conclusion

The Flipper Zero and Rubber Ducky are both very powerful devices, if used for their intended purpose of pen testing. The Rubber Ducky can perform BadUSB attacks, or keystroke injections, to do a number of things. This includes obtaining Wi-Fi passwords, going to URLs, and creating files. The Flipper can do the same things, but it differs in that it can interact directly with the network and needs to be manually executed. Future research should be done to explore the new and emerging additions to these devices and custom firmware that can be installed.

References

Aarness, A. (2024, February 21). *What is endpoint security? - crowdstrike*. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/endpoint-security/

Blackmagic-Debug. (2017). *Blackmagic-Debug/Blackmagic: In Application Debugger for ARM Cortex microcontrollers*. GitHub. https://github.com/blackmagic-debug/blackmagic

Cannols, B., & Ghafarian, A. (2017). *Hacking Experiment by Using USB Rubber Ducky Scripting*. https://www.iiisci.org/journal/PDV/sci/pdfs/ZA340MX17.pdf

Cass, S. (2023). A hacker's delight > you'll either love or hate the flipper zero. *IEEE Spectrum, 60*(5), 18–20. https://doi.org/10.1109/mspec.2023.10120663

Dave Jing Tian, Adam Bates, and Kevin Butler. (2015). Defending Against Malicious USB Firmware with GoodUSB. In Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC '15). Association for Computing Machinery, New York, NY, USA, 261–270. https://doi.org/10.1145/2818000.2818040

Do, H. (2023). *Implement Rubber Duckies On Available Usb Devices And Make A Practical Test*. Theses.cz. https://theses.cz/id/m5muam/projekt.pdf?zpet=%2Fvyhledavani%2F%3Fsearch%3DIMPLEMENT%20RUBBER%20DUCKIES%20ON%20AVAILABLE%20USB%20DEVICES%20AND%20MAKE%20A%20PRACTICAL%20TEST%26start%3D1;info=1;isshlret=Implement%3BRubber%3BDuckies%3Bon%3BAvailable%3BUSB%3BDevices%3Band%3BMake%3Ba%3B

Flipper zero shop. Flipper Shop. (2021). https://shop.flipperzero.one/

Hak5. (2018). *USB rubber ducky*. https://shop.hak5.org/products/usb-rubber-ducky

Harianto, H. E., & Gunawan, D. (2019a). Wi-Fi password stealing program using USB rubber ducky. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 17*(2), 745. https://doi.org/10.12928/telkomnika.v17i2.11775

Payloadstudio. PayloadStudio - Payload Studio. (2013). https://docs.hak5.org/payload-studio/

Sasquach, T. (2024, February 11). *Flipper zero WI-FI hacking has never been easier! updated for 2024!*. YouTube. https://www.youtube.com/watch?v=nKcwJodcOTA

Schneider, D. (2012). The state of network security. *Network Security, 2012*(2), 14–20. https://doi.org/10.1016/s1353-4858(12)70016-8

Settings. Flipper Zero - Documentation. (2024). https://docs.flipper.net/basics/settings

Skizzophrenic. (2023). *Skizzophrenic/ubers-SD-files: These are all of the SD card assets you need for your flipper zero!*. GitHub. https://github.com/skizzophrenic/Ubers-SD-Files

WI-FI Devboard for flipper zero. Flipper Shop. (2021). https://shop.flipperzero.one/products/Wi-Fi-devboard

Winston, Joy. (2023). Evaluating Iot Device Security: Penetration Testing and Vulnerability Assessment with Flipper Zero. Available at SSRN: https://ssrn.com/abstract=4658141 or http://dx.doi.org/10.2139/ssrn.4658141