

Mainstreaming Hacking:

The Ethical and Security Implications of Consumer-Grade Cyber Tools

Christopher Torres

University of Arizona

CYBV 498: Senior Capstone – Defense & Forensics

Professor Paul Wagner

09/17/2024

Abstract

Consumer grade hacking tools, such as the Flipper Zero have called into question current cybersecurity posturing, presenting both challenges and opportunities. This paper will examine the ethical, security and legal implications of these tools, which were once confined to cybersecurity professionals but are now marketed to the general public. Through a literature review, lab analysis, and discussion of real world case studies, this paper will explore the capabilities of tools such as the Flipper Zero in penetration testing, vulnerability assessments and the potential for misuse. The findings of the lab will highlight the dual use aspect of these tools, underscoring the need for more awareness on the part of both users and regulators. While devices can serve as valuable educational resources, their accessibility has raised ethical concerns about unauthorized exploitation, especially within corporate environments. Recommendations will be provided in this paper for organizations to adopt proactive measures to mitigate the potential risks posed by these tools and will provide information to ensure that they are used ethically and responsibly.

Table of Contents

The Role of Commercial Hacking Tools in Cybersecurity..... 5

Literature Review..... 6

Recommendations 8

Proliferation and Accessibility 8

Security Implications for Corporations 11

Legal and Ethical Issues 15

Lab Analysis: Exploring the Flipper Zero and Wi-Fi Dev Board 18

Lab Takeaways..... 27

The Educational Value of Consumer-Grade Hacking Tools 28

Conclusion..... 29

Bibliography 31

Table of Figures

Figure 1 19

Figure 2 20

Figure 3 20

Figure 4 21

Figure 5 22

Figure 6 23

Figure 7 24

Figure 8	24
Figure 9	25
Figure 10	26
Figure 11	26

The Role of Commercial Hacking Tools in Cybersecurity

The rise of commercial hacking tools has transformed the cybersecurity landscape. Tools and capabilities that were once in the domain of professional penetration testers and security experts are now being mass-marketed for commercial use to a much broader audience.

Commercial hacking tools have become widely marketed and purportedly used for both ethical and malicious purposes. The ease of use and “script kiddie” aspect of these tools has caused borderline panic within conversations surrounding cybersecurity. Their capabilities are often debated as either a malicious actor's ultimate multitool or a toy for wannabe hackers that offers no real threat. Countries like Brazil, Israel, and now possibly Canada have banned a relatively new device called the Flipper Zero due to concerns surrounding its unethical usage among hackers.

While the capabilities of the Flipper Zero include Wi-Fi jamming, RFID cloning, NFC reading, signal emulation, and even remote exploitation of IoT devices, conducting these attacks is somewhat complicated. A basic understanding of technology, networking, and possibly additional hardware is still necessary. Tools like the Flipper Zero and others are marketed as “plug and play,” which often leads people to believe they possess more capabilities than they actually do; while simultaneously making experienced penetration testers or tinkerers feel they have purchased a lackluster product when they could’ve achieved the same results from a homemade device powered by a cheap raspberry pi or any laptop.

The emergence of marketed, user-friendly hacking tools introduces new ethical and legal challenges by empowering novice users to knowingly or unknowingly exploit vulnerabilities, complicating corporate defenses, forensic investigations, and the attribution of cyberattacks. The ease of acquiring and operating these tools presents significant challenges for corporate security

defenses and forensic investigations. Companies can now face attacks from individuals with minimal training who are equipped with hardware capable of executing a variety of attacks. The user-friendliness of these tools complicates the attribution of cyberattacks, as they lack identifying data, making it difficult to trace malicious activities back to specific actors. The introduction of these tools has effectively created a new “script kiddie” adjacent culture, relying on hardware, where amateur hackers can easily launch attacks.

This paper will address the growing concerns that commercial hacking tools are changing the cybersecurity field. These tools offer both benefits and risks while providing impressive capabilities for novice users. I will explore the dual impact of these tools on corporate security postures and examine their actual effectiveness relative to how they are marketed. Additionally, I will discuss the broader ethical and legal implications of widely available hacking tools and the conversations regarding the lack of regulatory oversight.

Literature Review

Unveiling Exploitation Potential: A Comparative Analysis of Flipper Zero and Rubber Ducky

Unveiling Exploitation Potential: A Comparative Analysis of Flipper Zero and Rubber Ducky, dives into a comparative analysis of two hacking tools, the Flipper Zero and the Rubber Ducky. Both devices are being used for penetration testing purposes; however, the versatility of the Flipper Zero is noted. The publication remarks on the various tasks the Flipper Zero can undergo, such as signal capture, RFID cloning and Wi-Fi attacks. This allows it to offer a broader range of capability than the Rubber Ducky, which relies on USB-based attacks. The publication emphasizes the differences between these tools and that although they are useful for

penetration testing, the misuse by potential malicious actors can pose a significant risk to network and physical security.

Analysis of Network Security in LAN and Wi-Fi at Dishub Kominfo Banyuasin

Analysis of Network Security in LAN and Wi-Fi at Dishub Kominfo Banyuasin, showcases vulnerabilities in local and wireless network environments. The research in the publication focuses on penetration testing within and government office, using techniques such as network sniffing and social engineering to expose vulnerabilities. The publication encourages the importance of adhering to the National Institute of Standard and Technology (NIST) guidelines to secure networks to protect against unauthorized access. The findings of the publication reveal significant gaps in network defenses, relevant to not only government agencies, but also organizations reliant on local and wireless infrastructures.

Evaluating IoT Device Security: Penetration Testing and Vulnerability Assessment with Flipper Zero

Evaluating IoT Device Security: Penetration Testing and Vulnerability Assessment with Flipper Zero, explores the usage of the Flipper Zero in relation to assessing the security of Internet of Things (IoT) devices. As the proliferation of IoT devices continues to rise, so do the security challenges presented by unknown variables. The Flipper Zero is a tool that is known for finding vulnerabilities within IoT's, particularly through techniques such as Bluetooth vulnerability assessments and RFID cloning. This publication highlights the increased risks associated with IoT's and it calls for the continuation of security assessments and proactive defense strategies.

Recommendations

The publications all emphasize the importance of regulatory oversight, whether that be from corporate awareness or proactive defense against hacking tools like the Flipper Zero; however, one critical area left unexplored by these studies is the role of risk management and mitigation practices designed for organizations facing threats from potential amateur hackers using these tools. While the publications offer valuable insights into vulnerabilities that the Flipper Zero can find and exploit, they lack a comprehensive dialogue on how organizations can implement security strategies to manage the increasing threat landscape posed by consumer-grade hacking tools.

In addition to addressing vulnerabilities found and exploited by consumer-grade hacking tools, organizations should focus on integrating risk assessments that prioritize threats based on potential business impact. Social engineering and training employees to raise awareness of consumer hacking tools and incorporating monitoring for abnormal network activities can indicate usage of tools such as the Flipper Zero (that of which has little to no identifying data).

Expanding on this gap that was not addressed in the publications, this paper will discuss how organizations can incorporate threat intelligence and security measures that can be used to detect emerging hacking tools. This approach would provide a more actionable strategy to protect their networks against growing threats.

Proliferation and Accessibility

Purpose-built consumer hacking tools have gained a lot of notoriety and attention in recent years. Capabilities from tools such as the Flipper Zero, Hack RF and Rubber Fucky, once considered niche and used primarily by security professionals, are now under scrutiny due to

their increased availability to the general public. These tools are often marketed as being multi functional, capable of tasks like signal interception, network testing and penetration. However, the unregulated sale and availability of these devices have sounded the alarm of world governments about potential malicious usage. Websites such as Hak5, Amazon (with the exception of the Flipper Zero) and other general e-commerce stores have made consumer hacking tools easier than ever to acquire. Some argue that the accessibility of these devices eliminates a traditional barrier to hacking, technical knowledge.

Beyond the accessibility of these devices, the online environment surrounding these tools strengthens their potential usability. Basic platforms like YouTube, Reddit and Discord (both official and unofficial channels) are focal points for tutorials and community-driven support. For example, a new Flipper Zero owner can find numerous step by step guides on setting up attacks such as starting a rogue access point, to steal credentials or Wi-Fi deauthentication attacks. These guides lower the technical barrier of entry for these attacks and can make novice users much more confident in their abilities.

Part of the appeal of these tools and the free information surrounding them is the approachable design of not only the devices themselves, but also the auxiliary modules users can buy along with the platforms they are consuming informational content from. For example, the Flipper Zero markets itself as a “Swiss Army knife for hackers” (Although it used to be “Hack the Planet” but they changed it due to the bad optics after being banned in some countries). The device features a dolphin mascot and a user interface that feels more like a toy than a professional tool. Comparably, older penetration testing devices typically often required some knowledge of coding or general tech knowledge in order to operate effectively. Today’s

consumer-grade hacking tools only really require how to troubleshoot by researching on the internet in order to execute, what used to be considered, complex tasks.

The proliferation of these hacking tools has sparked debates among cybersecurity experts, as their dual use nature allows for both legitimate security research and potentially harmful activities. For example, the Flipper Zero has been described by Stephen Cass of IEEE Xplore (a research database and digital library for Computer Science and Engineering), as "an open-source hacking tool of exceptional polish and functionality," capable of cloning RFID cards, manipulating wireless signals, and more. While it serves legitimate purposes, its ease of access and versatility have raised concerns about misuse (IEEE Staff, 2023). Consumer hacking tools like the Flipper Zero are often crowd funded. The development of these devices through platforms like Kickstarter ensure a grass roots approach of progression. They also offer educational content as the project is developed to their backers or potential buyers when the product goes live. Grass roots crowdfunding legitimizes the sale to the general public, without the rigorous scrutiny of a traditional development. For example, the Flipper Zero received significant attention by raising over \$4.8 million from almost 38,000 on Kickstarter, showcasing its appeal to a broad audience (Flipper Devices, 2020). Many of the demos on the Kickstarter page include clips of the device being used in a way that may seem unethical such as using the IR to interact with monitors or barrier gate arms for cars. On one hand, these tools serve as a resource for cybersecurity professionals, educators and hobbyists interested in ethical hacking and penetration testing. On the other hand, the accessibility of these tools can be utilized by malicious actors or individuals with a limited understanding of ethical boundaries. Many posts on social media and forums often showcase users bypassing security measures or exploiting vulnerabilities with these types of devices (which many are frequently inaccurate or blatantly

false depicting capability of the device), often boasting about their exploits. This has raised ethical concerns, as the line between legitimate use and abuse becomes increasingly blurred.

Despite the argued capabilities of these hacking tools, they remain largely unregulated in most countries, including the United States. Their legality often hinges on intent rather than possession, making enforcement and attribution difficult. For example, when a user employs the Flipper Zero and its Wi-Fi development board to test the security of their own Wi-Fi network, they are acting within legal bounds. However, if the same device is used to conduct a penetration test on a neighbor's network, the user would be violating laws, most notably the Computer Fraud and Abuse Act (CFAA), a federal law in the United States. This regulatory gap underscores the challenges posed by the wide availability and onset usage of these hacking tools, as law enforcement and law makers struggle to address their misuse without stifling legitimate and ethical usage.

Security Implications for Corporations

Consumer-grade hacking tools, such as the Flipper Zero can pose significant security challenges for corporations, if used correctly. These devices can exploit vulnerabilities in corporate environments by providing novice malicious actors with more advanced capabilities.

Corporations now face threats from unskilled attackers, often referred to as “script kiddies,” as well as from more moderate to highly skilled attackers. The same way in which a script kiddie would typically utilize prebuilt code for a specific purpose, without the knowledge on how and why the code was written, they can also use consumer hacking tools in order to achieve a specific purpose without understanding what the device is really doing. Additionally,

consumer grade hacking tools can challenge traditional corporate security measures by targeting sub-GHz. The Flipper Zero is capable of this and can intercept and manipulate signals from physical access controls such as RFID enabled employee badges or smart locks, granted, the range is limited and you need to be close to save the signal to emulate it. Physical security systems are often overlooked. Addressing potential threats requires an integrated approach where cybersecurity teams collaborate with physical security departments to assess and mitigate risks from tools capable of exploiting physical vulnerabilities with tools that are capable of doing so.

John Gunn (2024), a CEO and expert in next-generation multi-factor authentication, stated:

The democratization of cyberattacks, fueled by the availability of easy-to-use hacking tools and the rise of the gig economy, presents significant challenges for cybersecurity. Untrained individuals now have the capability to launch sophisticated attacks, increasing the volume and complexity of threats faced by organizations. Addressing these challenges requires an upgrade to current defense technologies, most importantly legacy MFA. By adopting these strategies, we can mitigate the risks and protect against the evolving landscape of cyber threats. (para. 17)

A statement from an expert like this underscores the number of potential adversaries targeting organizations and highlights the vulnerabilities in outdated systems like legacy multi-factor authentication (MFA). Legacy MFA would typically be considered weaker or outdated if it solely uses methods such as SMS based authentication or static one-time passwords that do not cycle or reset. These are more vulnerable to attacks such as phishing, interception of passwords through a rogue access point or even man on the middle attacks.

Newer MFA leverages more robust methods and often combines two or more. These methods can include Push notifications, biometric authentication, a security key in the form of hardware and even time sensitive passwords. Tools like the Flipper Zero can clone Near Field Communication (NFC) cards or even spoof Wi-Fi networks if it has the dev board for the General Purpose Input Output (GPIO) ports, but they can't bypass hardware keys or push based authentication tied to secure sessions. This would largely negate phishing based attacks (along with some form of social engineering for a corporate employee), as these MFA methods are generated and time sensitive. Some authentication methods can even tie authentication to a specific domain, which means that rogue portals wouldn't be effective. Biometric and hardware tokens that generate unique codes per session or for a specific window of time make stolen tokens useless. Script kiddies that rely on consumer hacking tools typically lack the knowledge or sophistication it takes to break into these modern MFA systems, which demand advanced techniques like hardware exploitation or very elaborate and professional phishing campaigns.

Internet of Things (IoT) devices are becoming increasingly integrated into corporate networks, exacerbating risks that can potentially be exploited. Many IoT devices lack robust security protocols, making them a prime target for exploitation. A Duke Law and Technology Review (2018) article highlighted that IoT devices can act as entry points into corporate systems, noting the difficulty of prosecuting malicious actors due to attribution challenges in such cases. For example, the 2016 Dyn attack disrupted large portions of the internet by weaponizing poorly secured IoT devices, underscoring the need for corporate vigilance in securing all connected endpoints on their network (Beale & Berris, 2018).

Exploitation of vulnerabilities caused by consumer hacking tools can also result in severe financial and operational repercussions for businesses. For example, the use of deepfake

technology, another open source tool, has led to multi million dollar scams. CNN reported that scammers used AI to impersonate a company's CFO and other staff in order to transfer funds, ultimately securing the scammers \$25.6 million. (2024) This incident underscores the increasing complexity and variety of threats corporations must defend against and illustrates how far behind current corporate defenses really are. Additionally, consumer hacking tools can be used to conduct reconnaissance on corporate networks by gathering sensitive data. For example, the Flipper Zero can detect sub GHz radio frequencies, RFID systems and other protocols commonly used in corporate security. Modules can be used and connected to the GPIO ports that can then extend the physical range of its capabilities. Adrian Kingsley-Hughes, an internationally published technology author and journalist, notes that while tools like the Flipper Zero can have legitimate applications, their misuse highlights the gaps that currently exist in corporate security measures (2024).

Attribution remains one of the most significant challenges for corporations dealing with threats enabled by consumer hacking tools. The lack of identifying data makes tracing the attacks back to their source somewhat difficult. Denial attacks and rogue access points that the Flipper Zero can conduct are difficult too, as both of these kinds of attacks do not require the attacker to even be connected to the network in order to attack it. Moreover, the reactive nature of the legal and regulatory framework surrounding cybersecurity often leaves corporations vulnerable. Laws such as the Computer Fraud and Abuse Act (CFAA), focus on penalizing post-incident actions rather than proactively addressing threats posed by consumer hacking tools. The Duke Law and Technology review (2018) mentioned earlier also stated that there is a necessity for stronger regulatory standards and international cooperation in order to manage emerging threats effectively.

To mitigate these risks, corporations should adopt modern methodologies. Utilizing modern MFA systems, implementing Zero Trust architectures (a “never trust always verify” approach to network security) and continuously monitoring IoT devices. Additionally, employee training should drive home recognizing social engineering tactics, deepfakes and other emerging threats. The CNN reporting (2024) mentioned earlier that resulted in a \$25.6 million dollar loss demonstrates the importance of verifying requests through secondary channels. Corporations should also commit to taking ethical hacking initiatives, using consumer hacking tools to identify and patch vulnerabilities via a penetration testing team before malicious actors can exploit them. This approach not only enhances security, but also engrains a proactive rather than reactive stance when addressing potential threats.

Legal and Ethical Issues

Due to the vast number of laws and regulations in each country, there is a lack of a cohesive, unified stance on how and what needs to be controlled in regard to consumer hacking tools. As a result, the legal landscape remains reactive and fragmented. The federal law mentioned earlier, the Computer Fraud and Abuse Act (CFAA) is designed to prosecute unauthorized access and hacking activities. However, post-incident, laws such as the CFAA struggle because they are reactive in nature. The Flipper Zero's capability to interact with a wide variety of wireless signals further complicates attribution. Unlike traditional hacking tools that leave digital footprints, such as IP addresses or identifiable payloads, the Flipper Zero operates as a piece of hardware, which inherently makes tracing the source of malicious activity more difficult. Post incident, even if the device is recovered, it will contain no logs or records of the actions performed unless the user has explicitly configured logging features via the Command Line Interface (CLI). Even then, the logs are stored on a microSD card, and if this card is

removed, the logs are inaccessible, further hindering law enforcement's ability to attribute the attack to a specific individual (Flipper Zero Documentation, 2024).

The ethical implications of using consumer hacking tools are as equally complex as the legal ones. While these devices can empower users to test their own systems and learn about cybersecurity, their misuse can pose significant risk. What some called the “democratization” of hacking, has led to questions surrounding the ethical responsibilities of manufacturers, users and regulators. Manufacturers of devices like the Flipper Zero often walk a fine line in their marketing. They used to lean heavily into the gray hat marketing aspect of their device, having an attitude of plausible deniability towards the device’s potential misuse. Dr.Joy Winston James, at the University of Technology Bahrain (2024), points out that while tools like the Flipper Zero offer significant value in penetration testing and vulnerability assessments, they also expose critical flaws in IoT security, highlighting the need for stricter ethical guidelines in their production and use. The ethical responsibility of these companies extends beyond mere disclaimers; it involves actively working to prevent misuse, such as implementing safeguards or requiring certifications for advanced features.

From a novice user’s perspective, ethical dilemmas can appear when consumer hacking tools are used in ways that, while technically legal, may still potentially harm others. For example, scanning a neighbor’s unsecured network without permission to demonstrate vulnerabilities may lead to unintended consequences, such as privacy violations. Actions like these, even if performed with good intentions, can undermine trust and may provoke legal repercussions.

Being able to strike a balance between fostering education and ensuring security should be the primary goal for most regulatory entities. Overregulation could hinder development of

essential cybersecurity tools and discourage ethical hacking practices for both professionals and hobbyists. Moreover, unclear or poor foundational starting points that regulatory entities typically start from, can often add more chaos to an already sporadic sphere that is regulating technology. A report from the Bina Darma University (2015), argues for a more proactive regulatory framework that emphasizes compliance with established security standards, such as those set by the National Institute of Standards and Technology (NIST), a U.S. based organization that develops guidelines to improve cybersecurity practices globally. NIST's standards provide a foundation for securing networks and devices, including recommendation for vulnerability management by keeping up to date with the Common Vulnerabilities and Exposures (CVE) database and penetration testing protocols, offering a structured way to address the risks associated with consumer hacking tools.

The Canadian Minister of Innovation, Science, and Industry François-Philippe Champagne, even called for the Flipper Zero to be banned (similar to other countries such as Brazil and Israel) citing its alleged rampant use in car thefts (Canadian Broadcasting Corporation [CBC], 2024). Restricting access to tools that can be used for legitimate purposes, such as security testing and educational applications, can potentially risk stifling innovation and limit resources available for ethical hackers. Banning devices have the potential to drive the development and distribution of similar tools into less regulated or even black market channels.

The vast majority of private open source content surrounding tools like the Flipper Zero are aimed at raising awareness about the ethical use of these tools. By fostering a culture of responsibility among users and being honest about the devices capability, the sphere of influence in which these devices reside can be one in which the risks are mitigated without governments resorting to outright bans.

The legal and ethical challenges surrounding consumer grade hacking tools are representative of the broader challenges that are starting to exist in cybersecurity. As the proliferation of tools like the Flipper Zero become more apparent, and people's interest grows, so will the necessity for more advanced security posturing from corporations. Oftentimes, the capability of these tools can be over exaggerated and crucial steps in the cyber kill chain are overlooked such as the recon phase, which can make or break a successful execution. The growing concerns surrounding consumer hacking tools and the dialogue they have established will undoubtedly lead to more advanced proactive security posturing that will be a net positive for cybersecurity.

Lab Analysis: Exploring the Flipper Zero and Wi-Fi Dev Board

The lab focused on evaluating the Flipper Zero and its Wi-Fi development board in the context of network penetration testing and signal emulation capabilities. The process began by accessing the QFlipper desktop application, where the latest version of the firmware was installed, and the micro SD card required for the device to run was formatted. The Flipper Zero is designed to support various applications from them directly, as well as third parties. One of the tools, called Marauder, which includes both "Evil Portal" and "Death" attacks was selected for testing. However, attempts to use these tools were unsuccessful. The device was incapable of conducting basic access point scans or basic broadcasting. Research revealed that to unlock the device's full functionality, the Flipper Zero needed to be "jailbroken", which requires the official firmware to be overwritten by a third party firmware.

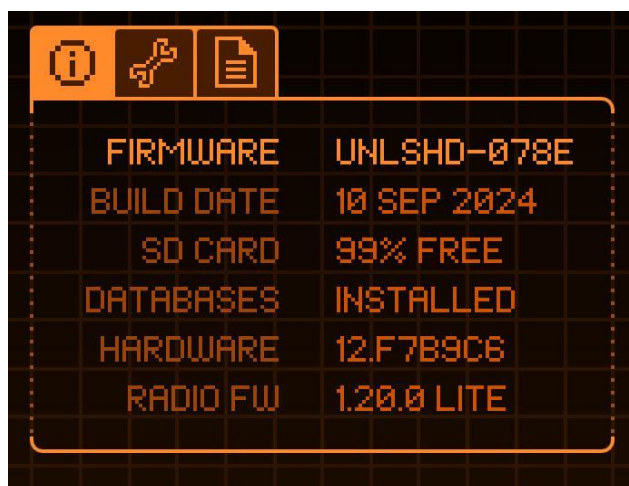


Figure 1

The image above shows a successful installation of the Flipper Unleashed firmware.

Various open source firmware options are available, but the Flipper Unleashed firmware was chosen for the lab from a GitHub repository due to its frequent updates. Even after installing this firmware, both the Evil Portal and the scans for access points to prepare for a Deauth failed to function at all. Further troubleshooting led to the discovery of a GitHub repository for Evil Portal attacks, which required the manual navigation and installation of files to the compatible ports. Upon successful installation, the Evil Portal attack could be tested.

The Evil Portal attack creates a fake, unencrypted Wi-Fi access point labeled “Free Google WiFi” by default, simulating a public access point. When a victim connects to the network, they are redirected to a phishing page that mimics common login portals. Attackers can modify these pages using HTML, allowing them to impersonate trusted organizations, such as healthcare providers or airlines. The credentials entered by victims are then saved to the Flipper’s micro SD card. This attack showcased how dangerous unsecured networks are and also

depicts a useful tool for ethical hacking when auditing employee awareness or rogue access points.

```
html set  
all set  
starting ap Google Free WiFi  
ap ip address: 192.168.4.1  
web server up
```

Figure 2

The image above shows a successful Evil Portal Execution.

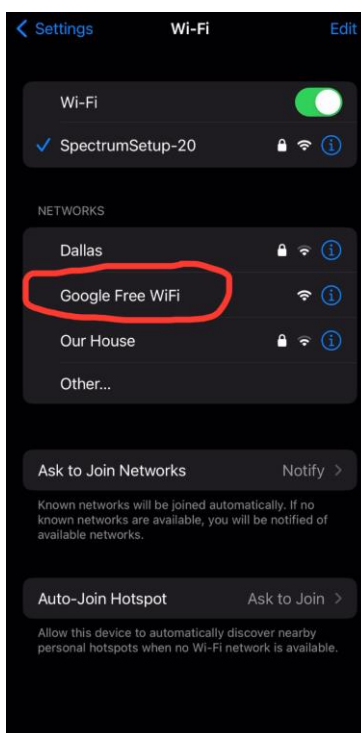


Figure 3

The image above shows how the rogue access point can appear on iOS.

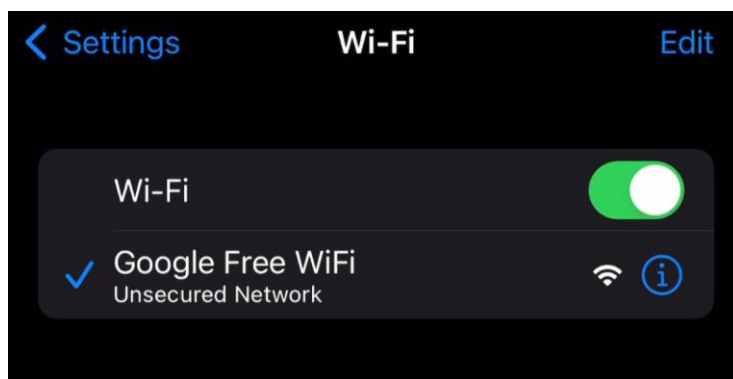


Figure 4

The image above shows that when the device is connected, that it is in fact, an unsecured/unencrypted network.

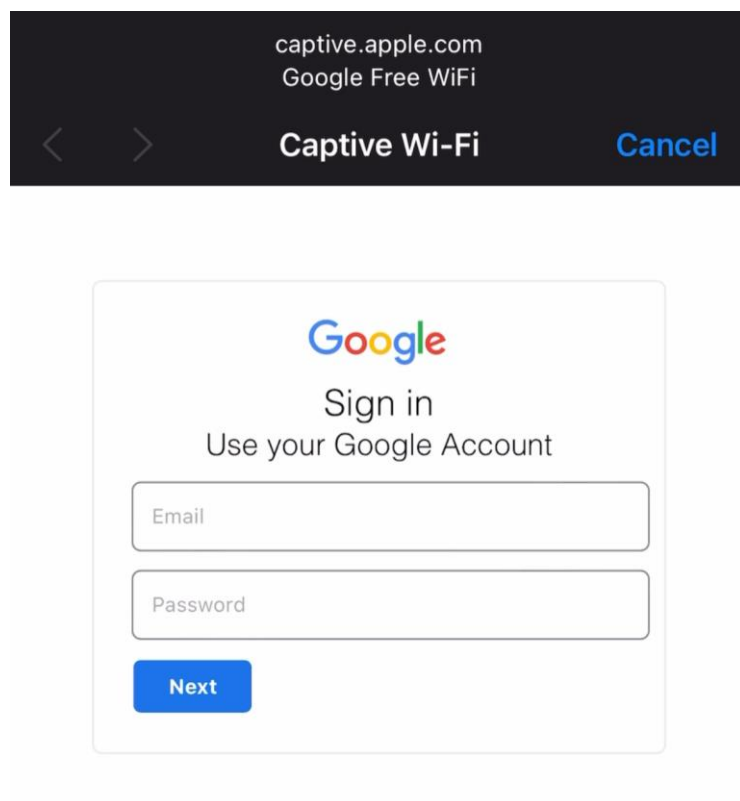
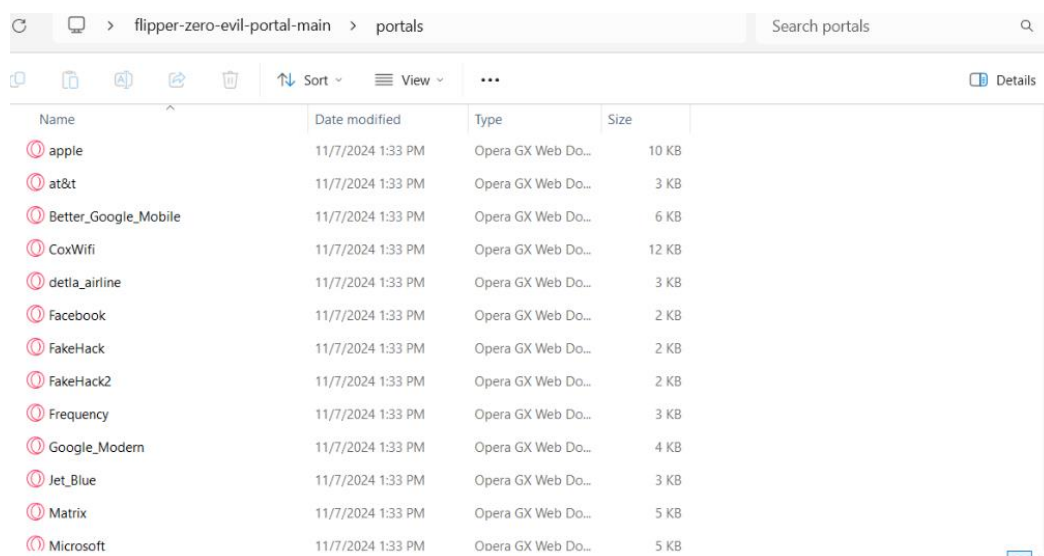


Figure 5

This image shows how the default Google portal appears in iOS.



Name	Date modified	Type	Size
apple	11/7/2024 1:33 PM	Opera GX Web Do...	10 KB
at&t	11/7/2024 1:33 PM	Opera GX Web Do...	3 KB
Better_Google_Mobile	11/7/2024 1:33 PM	Opera GX Web Do...	6 KB
CoxWifi	11/7/2024 1:33 PM	Opera GX Web Do...	12 KB
detla_airline	11/7/2024 1:33 PM	Opera GX Web Do...	3 KB
Facebook	11/7/2024 1:33 PM	Opera GX Web Do...	2 KB
FakeHack	11/7/2024 1:33 PM	Opera GX Web Do...	2 KB
FakeHack2	11/7/2024 1:33 PM	Opera GX Web Do...	2 KB
Frequency	11/7/2024 1:33 PM	Opera GX Web Do...	3 KB
Google_Modern	11/7/2024 1:33 PM	Opera GX Web Do...	4 KB
Jet_Blue	11/7/2024 1:33 PM	Opera GX Web Do...	3 KB
Matrix	11/7/2024 1:33 PM	Opera GX Web Do...	5 KB
Microsoft	11/7/2024 1:33 PM	Ooera GX Web Do...	5 KB

Figure 6

This image shows some of the list of HTML's available from the repository.

For the Wi-Fi deauthentication attack, the Wi-Fi dev board was reflashed using the Marauder firmware, which enabled the Flipper Zero to scan 2.4GHz networks. Devices operating on 5GHz networks and proprietary wireless protocols could not be targeted by this attack. This limitation underscored the importance of the reconnaissance phase of the cyber kill chain, where identifying network information and configuring devices accordingly become critical. Without proper prior knowledge and preparation, consumer hacking tools can fail to deliver any results. After configuring the capture settings, the Flipper Zero was used to scan for access points and capture packets, which were then saved in Packet Capture (PCAP) files to further analyze using a desktop application called Wireshark.

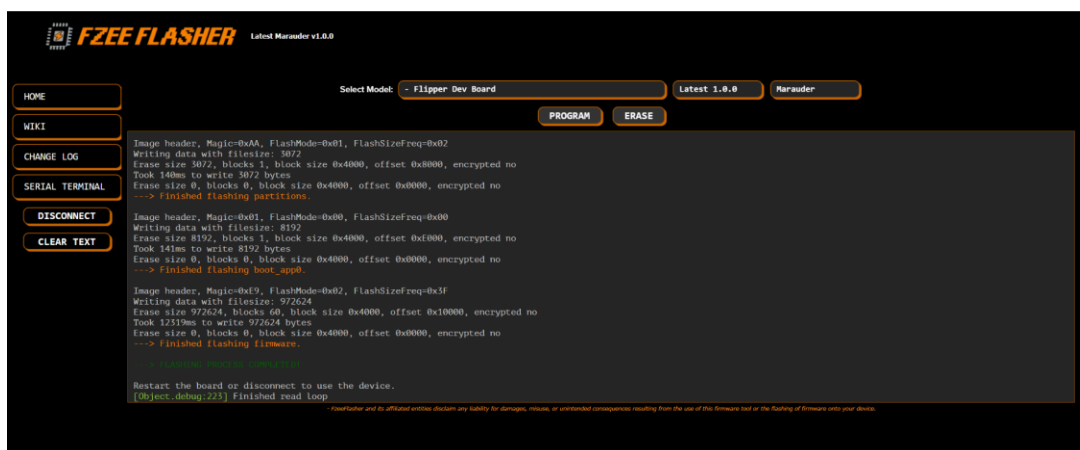


Figure 7

This image shows how the Wi-Fi dev board was flashed before the Death.

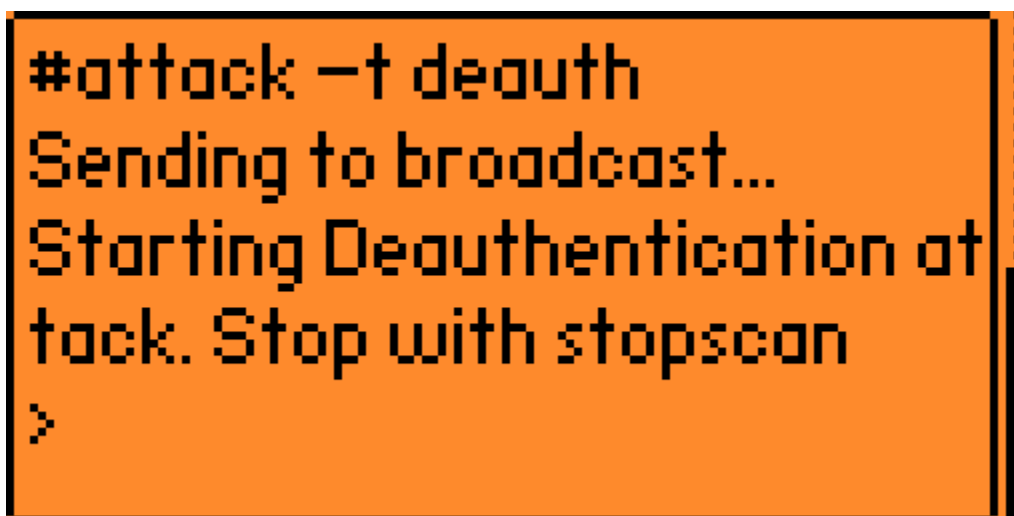


Figure 8

This image shows a successful Death attack execution

Wireshark was employed to filter Extensible Authentication Protocol Over LAN (EAPOL) packets, specifically identifying possible four way handshakes, which could potentially be used to crack WPA2 encryption via tools like Hashcat. In this case, the target network's SSID was public, so further decryption was unnecessary. While WPA3 networks offer

stronger protection, they can still be cracked under certain conditions. The deauthentication attack was effective only against devices operating on 2.4GHz networks, such as smartphones and tablets. Devices using proprietary protocols, like security cameras and smart TVs, remained unaffected, illustrating the limitations of the attack when targeting hybrid, dual-band networks.

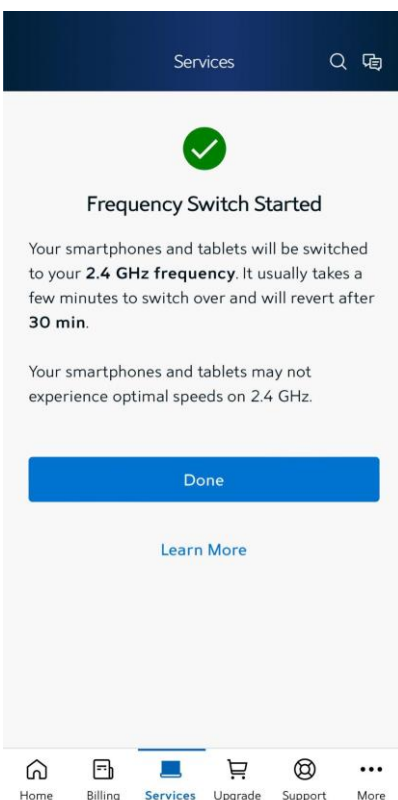


Figure 9

This image shows how the 2.4 GHz option can only be switched for smartphones and tablets.

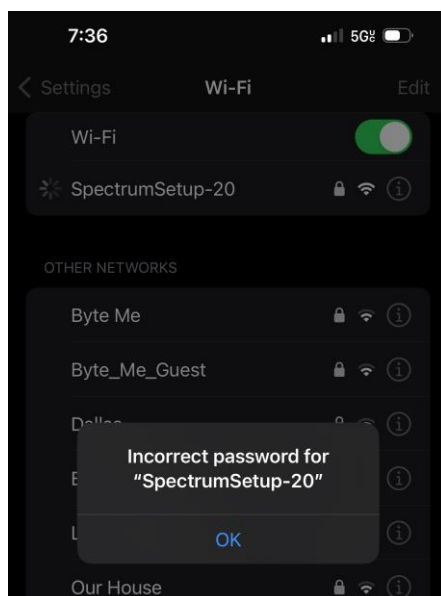


Figure 10

This image shows what the victim sees after a successful death on iOS.

sniffpmkid_0.pcap						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
wlan.ssid == "SpectrumSetup-20" eapol						
No.	Time	Source	Destination	Protocol	Length	Info
390	8.315591	Ring_b3:d4:ab	SagemcomBroa_28:6e:...	802.11	58	Probe Request, SN=491, FN=0, Flags=....., SSID="SpectrumSetup-20"
391	8.316165	SagemcomBroa_28:6e:...	Ring_b3:d4:ab	802.11	211	Probe Response, SN=3174, FN=0, Flags=....., BI=100, SSID="SpectrumSetup-20"
393	8.317309	Ring_b3:d4:ab	SagemcomBroa_28:6e:...	802.11	133	Association Request, SN=493, FN=0, Flags=....., SSID="SpectrumSetup-20"
395	8.318552	SagemcomBroa_28:6e:...	Ring_b3:d4:ab	EAPOL	137	Key (Message 1 of 4)
396	8.319153	Ring_b3:d7:b2	Broadcast	802.11	86	Probe Request, SN=437, FN=0, Flags=....., SSID="SpectrumSetup-20"
397	8.331112	Ring_47:be:c9	Broadcast	802.11	100	Probe Request, SN=1819, FN=0, Flags=....., SSID="SpectrumSetup-20"
398	8.335782	SagemcomBroa_28:6e:...	Ring_47:be:c9	802.11	211	Probe Response, SN=3195, FN=0, Flags=....., BI=100, SSID="SpectrumSetup-20"
399	8.338925	Ring_b3:d7:b2	SagemcomBroa_28:6e:...	802.11	58	Probe Request, SN=441, FN=0, Flags=....., SSID="SpectrumSetup-20"
401	8.397000	SagemcomBroa_28:6e:...	Broadcast	802.11	217	Beacon frame, SN=3197, FN=0, Flags=....., BI=100, SSID="SpectrumSetup-20"
404	8.559060	Ring_b3:d7:b2	SagemcomBroa_28:6e:...	802.11	133	Association Request, SN=443, FN=0, Flags=....., SSID="SpectrumSetup-20"
406	8.560309	SagemcomBroa_28:6e:...	Ring_b3:d7:b2	EAPOL	137	Key (Message 1 of 4)
407	8.560976	Ring_b3:d7:b2	SagemcomBroa_28:6e:...	EAPOL	159	Key (Message 2 of 4)
409	8.562673	SagemcomBroa_28:6e:...	Ring_b3:d7:b2	EAPOL	193	Key (Message 3 of 4)
416	8.602004	SagemcomBroa_28:6e:...	Broadcast	802.11	217	Beacon frame, SN=3212, FN=0, Flags=....., BI=100, SSID="SpectrumSetup-20"
422	8.817999	Ring_36:c9:5d	Broadcast	802.11	132	Probe Request, SN=1605, FN=0, Flags=....., SSID="SpectrumSetup-20"
424	8.819999	SagemcomBroa_28:6e:...	Broadcast	802.11	217	Beacon frame, SN=3219, FN=0, Flags=....., BI=100, SSID="SpectrumSetup-20"
426	8.821756	SagemcomBroa_28:6e:...	Ring_36:c9:5d	802.11	211	Probe Response, SN=3225, FN=0, Flags=....., BI=100, SSID="SpectrumSetup-20"
428	8.824050	SagemcomBroa_28:6e:...	Ring_36:c9:5d	802.11	211	Probe Response, SN=3225, FN=0, Flags=....., BI=100, SSID="SpectrumSetup-20"
429	8.826798	SagemcomBroa_28:6e:...	Ring_36:c9:5d	802.11	211	Probe Response, SN=3225, FN=0, Flags=....., BI=100, SSID="SpectrumSetup-20"
430	8.829227	SagemcomBroa_28:6e:...	Ring_36:c9:5d	802.11	211	Probe Response, SN=3225, FN=0, Flags=....., BI=100, SSID="SpectrumSetup-20"
431	8.831619	SagemcomBroa_28:6e:...	Ring_36:c9:5d	802.11	211	Probe Response, SN=3225, FN=0, Flags=....., BI=100, SSID="SpectrumSetup-20"
436	9.148751	SagemcomBroa_28:6e:...	Resideo_df:dc:bc	EAPOL	137	Key (Message 1 of 4)
437	9.150002	SagemcomBroa_28:6e:...	Broadcast	802.11	217	Beacon frame, SN=3228, FN=0, Flags=....., BI=100, SSID="SpectrumSetup-20"
438	9.150673	Resideo_df:dc:bc	SagemcomBroa_28:6e:...	EAPOL	159	Key (Message 2 of 4)
439	9.151269	Ring_b3:d4:ab	SagemcomBroa_28:6e:...	802.11	58	Probe Request, SN=505, FN=0, Flags=....., SSID="SpectrumSetup-20"

Figure 11

This image shows the captured 4 way handshake in the event that WPA2 or 3 encryption will need to be cracked using a tool such as Hashcat.

The Flipper Zero's ability to emulate remote control signals was also tested using a garage door opener. While the device successfully detected the frequency of the remote, it could not emulate the signal due to the use of rolling codes, which prevent replay attacks by generating a unique code for each signal. A workaround for this limitation involves interrupting the power to the garage door opener, capturing a fresh signal upon reset, and then replaying it. This method requires repeating this action to generate a new code each time. This limitation also applies to modern car key fobs, which similarly use rolling codes to secure vehicles. Contrary to concerns raised in Canada as discussed earlier, about the Flipper Zero's potential for vehicle theft, the device cannot be used to break into vehicles using these systems.

Lab Takeaways

The technical limitations of the Flipper Zero and its Wi-Fi dev board are limited to 2.4GHz networks, which restrict their effectiveness on hybrid networks. Additionally, proprietary systems and modern encryption protocols like WPA3 significantly mitigate the risk of successful attacks and breaking of encryption. Features like Evil Portal reveal the importance of user education regarding public Wi-Fi safety and the dangers of connecting to unencrypted/unsecure networks. The reliance on rolling codes in devices like garage doors and car locks illustrates how far behind consumer hacking tools that are marketed as plug and play, really are. The ethical implications for the good that consumer hacking tools can provide for novice users and hobbyists should be acknowledged in order to counter exaggerated fears that can have real world consequences. Tools like the Flipper Zero are dual use in nature and have potential for both legitimate cybersecurity testing and unethical misuse. While technical challenges and robust security protocols limit the scope of certain attacks, these devices serve as a reminder of the need for fostering responsible usage and that if any regulation does emerge, it

needs to come from an informed foundation. The findings of this lab emphasize that banning such tools may not address the root cause of misuse but rather hinder the development of ethical cybersecurity practices.

The Educational Value of Consumer-Grade Hacking Tools

The rise of consumer-grade hacking tools like the Flipper Zero has sparked global debates about their impact on the cybersecurity landscape. While concerns about their misuse are valid, these tools ultimately represent a net positive in fostering an ethical hacking culture with a population that is competent in cybersecurity awareness. The playful and approachable design of devices like the Flipper Zero has lowered the barrier of entry for individuals curious about penetration testing and security research and has undoubtedly ushered in a new populace of people that would not have been interested otherwise. Importantly, as shown in the lab portion of this paper, the effectiveness of these tools still hinges on prior knowledge. Without a foundational understanding of networking, signal protocols or security principles, their use is limited to a surface level, shallow experimentation, which is why so many call the Flipper a toy rather than a professional tool. Even with an advanced understanding, the Flipper Zero's capabilities remain constrained. Tasks like Wi-Fi attacks or signal emulation require additional hardware and preparation, and most of its functions can already be replicated using a standard laptop with the appropriate software and auxiliary equipment. The Flipper Zero and similar tools are not inherently groundbreaking in terms of capability but are significant in terms of the cultural and education value. Moreover, the playful design, along with community driven support behind tools like the Flipper Zero have demystified hacking for many individuals. By introducing concepts such as signal analysis, brute forcing and network vulnerabilities in an

approachable way, these tools are helping cultivate a culture of curiosity rather than malicious actions.

As new cybersecurity threats continue to emerge, the proliferation of hacking knowledge can strengthen defenses rather than weaken them. These tools can inspire new generations of hackers to approach cybersecurity with curiosity and integrity, and can serve as a stepping stone towards a more informed and advanced population that will have confident abilities in cybersecurity.

Conclusion

This paper explored the dual use nature of tools like the Flipper Zero, highlighting the educational value for aspiring cybersecurity professionals while acknowledging the potential for malicious usage. Through a review of existing literature, documents and a detailed lab analysis, the findings revealed that these tools and the culture surrounding them often overpromise their capabilities but still pose a notable risk due to their accessibility and ease of use.

The security implications for corporations and regulatory bodies are clear; there is a reasonable need for more comprehensive security measures and education to counteract the risk and overregulation of these tools. Organizations need to prioritize proactive defenses and modernize to incorporate MFA practices. Simultaneously, the ethical use of these tools should be encouraged.

Ultimately, the growing prevalence of these devices demands a nuanced approach to cybersecurity, that regulators seem to struggle to address. As these tools and the culture surrounding them continue to evolve, they will also continue to challenge what is seen as a

typical threat vector, pushing both individuals and organizations to adopt more resilient security postures and procure a more informed and prepared community.

References

Canadian Broadcasting Corporation. (2024). *Canada moves to ban hacking devices over auto theft concerns*. <https://www.cbc.ca>

Flipper Zero Documentation. (n.d.). Sub-GHz – Read signals. Flipper Zero. Retrieved December 5, 2024, from <https://docs.flipper.net/sub-ghz/read>

Flipper Devices. (2020). *Flipper Zero – Multitool for hackers* [Kickstarter campaign].

Kickstarter.

<https://www.kickstarter.com/projects/flipper-devices/flipper-zero-tamagochi-for-hackers>

IEEE Staff. (2023, April 26). The Flipper Zero: A hacker's delight. IEEE Spectrum.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10120663>

Bibliography

Gunn, J. (2024). The Democratization of Cyberattacks: How Billions of Unskilled Would-be Hackers Can Now Attack Your Organization.

<https://thehackernews.com/expert-insights/2024/06/the-democratization-of-cyberattacks-how.html>

Analysis: John Gunn, a CEO and expert in next-generation multi-factor authentication (MFA), shows how AI and consumer hacking tools are democratizing cyberattacks, creating a new “script kiddie” type threat. This article explains how unskilled individuals can now easily participate in (what used to be) more experienced cybercriminal activities, driven by Ransomware-as-a-Service (RaaS) and the gig economy. It emphasizes the vulnerabilities of legacy MFA systems and calls for modern security upgrades to address these growing threats.

Beale, S. S., & Berris, P. (2018). Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses. Duke Law & Technology Review.

<https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1319&context=dltr>

Analysis: This article explores the growing risks associated with the Internet of Things (IoT), focusing on how vulnerabilities in IoT devices expose them to hacking. The authors provide case studies like the 2016 Dyn attack and analyzes the current legal framework, particularly the Computer Fraud and Abuse Act (CFAA). They argue that

while hacking is illegal under current laws, prosecution is difficult due to attribution challenges because of IoT's and a nature of having a reactive legal structure. The article also discusses potential solutions, including regulation, international standards and ethical considerations of hacking back.

Arntz, P. (2024). Canada revisits decision to ban Flipper Zero. Malwarebytes.

<https://www.malwarebytes.com/blog/news/2024/03/canada-revisits-decision-to-ban-flipper-zero>

Analysis: This article by Arntz explores the Canadian government's reconsideration of banning the Flipper Zero device due to its potential use in car theft. It discusses the capabilities of the Flipper Zero, its implications for security vulnerabilities, and the broader context of consumer-grade hacking tools. Arntz emphasizes the need for regulatory measures while highlighting the lack of confirmed thefts using the device, offering a perspective on the challenges of managing emerging technologies in cybersecurity and how lawmakers really don't understand the capabilities of what they want to regulate.

Hackread. (2024). Employee Duped by AI-Generated CFO in \$25.6M Deepfake Scam.

Hackread.

<https://hackread.com/employee-duped-ai-generated-cfo-deepfake-scam/>

Analysis: This article details a significant deepfake scam that led to a \$25.6 million loss for a multinational company's Hong Kong branch. It highlights the increasing sophistication of deepfake technology, and the risks associated with its use in financial fraud. The piece emphasizes the need for enhanced employee training to recognize such scams, reflecting the broader challenges posed by emerging cybercrime tactics in both corporate and legal frameworks. This is relative to my paper, as most AI services are open source, though not marketed for this purpose.

Chen, H., & Magramo, K. (2024, February 4). Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'. CNN.

<https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>

Analysis: Scammers use AI to fraud a company of \$25.6m by pretending to be the company's CFO and other staff during a video call. This is relevant to show how open source tools are being used but more importantly, how important recon is for the cyber kill chain, which is what consumer hacking tools excel in.

Kingsley-Hughes, A. (2024). Flipper Zero: 'Can you really hack Wi-Fi networks?' and other questions answered. ZDNET.

<https://www.zdnet.com/home-and-office/flipper-zero-can-you-really-hack-wi-fi-networks-and-other-questions-answered/>

Analysis: This article provides an overview of the Flipper Zero. Kingsley-Hughes discusses the device's capabilities, including its ability to explore RFID and radio protocols, while also emphasizing the importance of ethical use. The article clarifies misconceptions surrounding the Flipper Zero's hacking potential, particularly regarding social media claims, and positions it as a valuable educational tool for those interested in learning about networking and hardware. Overall, it serves as a guide for understanding the practical applications and limitations of the Flipper Zero in cybersecurity contexts.

Starks, T. (2023). Yes, ChatGPT can write malicious code — but not well. The Washington Post.

<https://www.washingtonpost.com/politics/2023/01/26/yes-chatgpt-can-write-malware-code-not-well/>

Analysis: This article explores the cybersecurity implications of using AI tools like ChatGPT for malicious purposes. Tim Starks summarizes findings from a Recorded Future report, which indicates that while cybercriminals are beginning to leverage ChatGPT for activities such as malware creation and phishing schemes, the effectiveness and sophistication of the outputs are currently limited. The article highlights the necessity for users to have a foundational understanding of cybersecurity to utilize AI effectively.

Ikeda, Scott. (2019). “Juice Jacking” at Public USB Charging Stations? Los Angeles County DA’s Office Issues Warning, but How Real Is the Threat? CPO Magazine.

<https://www.cpomagazine.com/cyber-security/juice-jacking-at-public-usb-charging-stations-los-angeles-county-das-office-issues-warning-but-how-real-is-the-threat/>

Analysis: Scott Ikeda explores the warning issued by the Los Angeles County District Attorney's Office about "juice jacking," a threat involving data skimming and malware deployment through public USB charging stations. The article highlights the rarity of actual juice jacking incidents while discussing the potential risks associated with public charging. Ikeda emphasizes the limitations of such attacks and suggests alternative precautions users can take, providing a balanced perspective on the real and perceived dangers of using public USB charging facilities.

Zhu, Y., Zheng, H., Zhao, B., Liu, M., Chen, Y., & Li, Z. (2020). Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors. Accepted for the Network and Distributed Systems Security (NDSS) Symposium.

<https://news.uchicago.edu/story/how-hackers-could-use-wi-fi-track-you-inside-your-home>

Analysis: This study by researchers from the University of Chicago and the University of California, Santa Barbara, explores the vulnerabilities of smart devices connected to Wi-Fi networks. It reveals how attackers can utilize inexpensive Wi-Fi receivers to passively monitor and detect motion inside buildings without detection, raising significant concerns for both privacy and physical security. The authors propose potential defenses, such as the implementation of cover signals to obfuscate true device activity, highlighting the

urgent need for improved security measures in the growing landscape of Internet of Things (IoT) devices.

Johncox, C. (2023). Videos: Organized crews smash glass, use jammers to break into high-end Metro Detroit homes. WDIV ClickOnDetroit.

<https://www.clickondetroit.com/news/local/2023/12/07/videos-organized-crews-smash-glass-use-jammers-to-break-into-high-end-metro-detroit-homes/>

Analysis: Cassidy Johncox, a senior news editor, reports on a series of high-end home burglaries in Metro Detroit carried out by organized crime crews from Chile. The article highlights the use of tools, such as Wi-Fi jammers, to bypass security systems, and details the ongoing efforts by local and federal authorities to track and apprehend the criminals. This source provides a current example of how organized crime exploits consumer grade technology to commit burglaries across the U.S., offering insights into security vulnerabilities in homes.

Rose, J. (2024). Feds Want to Ban the World's Cutest Hacking Device. Experts Say It's a 'Scapegoat.' VICE.

<https://www.vice.com/en/article/flipper-zero-ban-canada-hacking-car-thefts/>

Analysis: Janus Rose, a journalist for VICE, explores the controversy surrounding the Canadian government's proposal to ban the Flipper Zero. The article critiques the government's lack of evidence linking the device to car thefts and highlights expert

opinions that the ban targets a tool often used for legitimate cybersecurity testing. This piece emphasizes the potential harms to cybersecurity research if the ban is implemented and positions the Flipper Zero as a scapegoat for vulnerabilities in car keyless entry systems.

Pava, R., Martin, R., & Mishra, S. (2024). Unveiling exploitation potential: A comparative analysis of Flipper Zero and Rubber Ducky. *Issues in Information Systems*, 25(2), 84-95.

https://www.researchgate.net/publication/384606341_Issues_in_Information_Systems_Unveiling_exploitation_potential_a_comparative_analysis_of_flipper_zero_and_rubber_ducky

Analysis: This article compares the penetration testing capabilities of the Flipper Zero and Rubber Ducky. It highlights their use in physical and network security, emphasizing the broader risks posed by these consumer-grade hacking tools in compromising secured systems. It underscores the versatility of Flipper Zero while warning about its potential misuse.

Kunang, Y. N., Wijaya, R. P. E., & Widyanto. (2015). Analysis of network security of local area network (LAN) and WiFi in Dishub Kominfo Banyuasin. *Proceedings of the 4th International Conference on Information Technology and Business Applications (ICIBA)*.

https://www.researchgate.net/publication/303788222_Analysis_of_Network_Security_of_Local_Area_Network_LAN_and_WiFi_in_Dishub_Kominfo_Banyuasin

Analysis: This paper explores network vulnerabilities within the LAN and Wi-Fi systems of a government office, using various testing techniques. The study reveals critical

security weaknesses and emphasizes the importance of compliance with NIST standards in securing organizational networks.

James, J. W. (2024). Evaluating IoT device security: Penetration testing and vulnerability assessment with Flipper Zero. Preprint, SSRN.

<https://ssrn.com/abstract=4658141>

Analysis: This review discusses the role of the Flipper Zero in IoT device penetration testing and security assessments. It categorizes IoT vulnerabilities and provides recommendations for improving device security, emphasizing the need for continuous monitoring and ethical hacking practices to safeguard against growing threats in IoT environments.