Wireless Network Attacks with Flipper Zero

Ayyaz Akhtar
Department of Cybersecurity
New York University
New York, USA
aia7143@nyu.edu

***Abstract*—The research aims to look at Flipper Zero as a threat actor and identify mitigations for wireless attacks against home networks. The methods for this study used the GIPO module to use a Wi-Fi board to conduct Beacon Spam, Spoofing, De-authentication, and Evil Portal. Hardening a home network from these attacks requires technical skills to enable VLAN network segmentations. The results show that segmented networks will provide some protection and mitigations of critical components of a home network.**

Keywords—Wireless network attacks, De-authentication, Spoofing, Jamming, Beacon Spam, Evil Portal, Denial of Service

I. Introduction

The problem domain will focus on surveying, exploiting, and hardening wireless networks. Integrating technology with the electromagnetic spectrum has changed the fabric of society. Complicated engineering tasks can now be untethered and transposed from remote locations.

Wireless network attacks are rapidly evolving, and the hardware to initiate these attacks is becoming inexpensive and easy to acquire. The Flipper Zero can be mistaken for a Tamagotchi [1] or Pocket Pikachu; however, this gadget is a powerful wireless pen-testing device that can be used as a learning tool or wreak havoc with various attacks under its toolkit.

Typically, home networks broadcast all devices on a single Local Area Network (LAN) and use the default configurations. Guided mediums (wired) generally are more secure than unguided mediums (wireless) [2]. With a basic setup, home networks are vulnerable to a malicious neighbor who wants to use your Wi-Fi to download illegal content or a prankster who wants to cause an inconvenience by jamming or spoofing networks.

IoT devices on the 2.4 GHz wireless network pose the most significant risk on a network due to a lack of patch management support, encryption libraries, and observability. In a default network configuration with a shared broadcast, these hosts are assumed to be trusted and will be targets that can be used to snoop, spoof, pivot, and escalate to other parts of the network.

The related research provides context and examples to work off and has some mitigation strategies that are more difficult to set up for a home network. The main difference of the research in the paper is that it highlights that network segmentation is a critical component in protecting home networks and is more feasible to set up.

In section 2, some information on related research will overlap with the attacks performed in this study. Section 3 will provide details on how this study will be conducted on a home network. In section 4, the hypothesis about the experiment is explained with mitigation metrics. In section 5, the paper will provide conclusions and next steps.

II. Related Research

A. A Hacker's Delight > You'll Either Love or Hate the Flipper Zero

The article by Cass [1] provides an overview of the Flipper Zero and its capabilities. This pen-testing tool will be used as the leading threat actor for the experiments conducted in this research. Wi-Fi attacks are briefly mentioned as a concept, whereas the research conducted in this paper will perform the attacks.

B. Denial of Service Attacks in Wireless Networks: The Case of Jammers

The study by Pelechrinis et al. [2] goes into different types of jamming techniques and mitigations. The authors highlight the best strategies for jamming attacks that are energy efficient and have a low detection level for denial of service. The mitigations in this paper refer to frequency hopping and spatial retreats, whereas this paper will use segmentation of wireless networks.

C. ETGuard: Detecting D2D attacks using wireless Evil Twins

The research conducted by Jain et al. [3] focuses on evil twin attacks against Android mobile phones. In addition, the paper references a software solution called Evil Twin Guard to notify mobile users when an SSID is cloned and not join the network. The research in this paper will be different in that it focuses on entire 2.4GHz networks and hosts being attacked by a flipper zero.

D. Detecting and Localizing Wireless Spoofing Attacks

The review on spoofing attacks written by Chen et al. [4] focuses on identifying and detecting spoofing attacks. The scope includes 802.11 (Wi-Fi) and 802.51.4 (Zigbee) wireless networks. The content of this paper will focus strictly on 2.4 GHz home wireless networks.

E. Secure routing in wireless sensor networks: attacks and countermeasures

The research conducted by Karlof et al. [5] goes into depth about network attacks on sensors. The mitigations

recommended focusing on encryption, authentication, and bidirectional link verification. This study in this paper focuses on network segmentation to mitigate wireless network attacks on hosts and the 2.4 GHz network.

III. Motivating Example

For this research, an advanced home network will be the attack target for multiple wireless network attacks directed from a Flipper Zero. In addition, wireless network attacks will be run against this network to identify metrics and mitigations.

A. Network

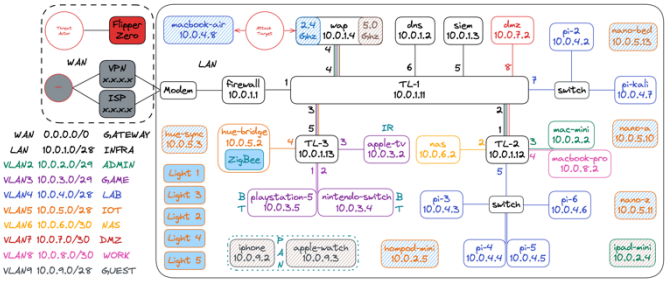

Fig. 1. Physical and Logical network diagram of a home network

B. Elements

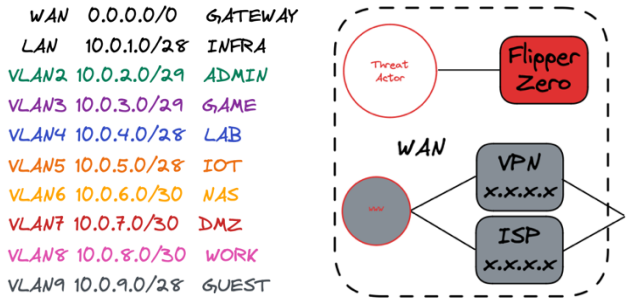

Fig. 2. 10 Segmented networks on the LAN and threat actors from WAN

Fig. 3. Attack targets will be hosts and the 2.4 GHz wireless network.

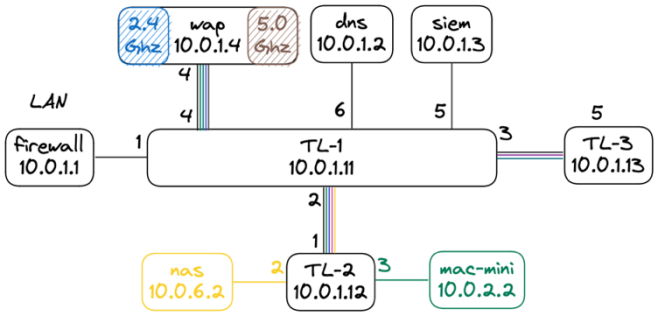

Fig. 4. Network - Infrastructure, Administrator, Network Attachment Storage

C. Threats

TABLE I. Threat Model

ID	Statements	Element	STRIDE
T-01	A threat actor with access to the WLAN can beacon spam which leads to an overload of SSIDs resulting in reduced availability of infrastructure wireless networks.	Infrastructure	Spoofing
T-02	A threat actor with control of a SSID name can trick users into an Evil Twin/Portal which leads to stealing credentials, resulting in reduced confidentially of wireless hosts on the network.	Hosts	Tampering
T-03	A threat actor with access to the network can delete log entries which leads to data loss on auditing, resulting in reduced integrity of the Network Attached Storage network.	Network Attached Storage	Repudiation
T-04	A threat actor with access to the WLAN can de-auth hosts which leads to sniffing re-auth handshake, resulting in reduced confidentially of Infrastructure wireless networks.	Infrastructure	Information Disclosure
T-05	A threat actor with access to the WLAN can probe the WLAN which leads to denial of service, resulting in reduced availability of the infrastructure wireless networks.	Infrastructure	Denial of Service
T-06	A threat actor with access to the network can laterally traverse network which leads to complete ownership, resulting in reduced Integrity of the Administrator network.	Administrator	Elevation of Privilege

IV. Hypothesis and Empirical Evidence

This study plans to show a segmented network can provide mitigations to protect a home network from multiple wireless network attacks. The threat model table will identify mitigation metrics to show that a properly segmented network can withstand attacks from an unguided medium.

Below define the constraints and test results of the threats.

TABLE II. What We Are Working On

ID	Description
WWAWO-01	Target 2.4 GHz wireless networks.
WWAWO-02	Leverage Flipper Zero GPIO Wi-Fi attacks.
WWAWO-03	Wireless attacks will run for 3-5 minutes.
WWAWO-04	Attacked WiFi networks should be available and in use.

TABLE III. What Could Go Wrong

ID	Description
WCGW-01	The firewall segmentation configuration and ACL rules can be relied on.
WCGW-02	The Flipper Zero will perform targeted attacks on a single WLAN.

TABLE IV. MITIGATIONS

ID	*Mitigation*	*Threat*	*Success*
M-01	Filter beacon spam wireless address from useable connections.	Spoofing	No
M-02	Prevent credentials from being stolen.	Tampering	No
M-03	Audit wireless network attacks.	Repudiation	Yes
M-04	The network can keep information in an encrypted channel.	Information Disclosure	No
M-05	Core networks will be available for use.	Denial of Service	Yes
M-06	Prevent lateral movements within the networks.	Elevation of Privilege	Yes

V. CONCLUSIONS AND FUTURE WORK

The conclusion of the results shows that the Flipper Zero was able to successfully attack the segmented wireless network by Spoofing and Tampering. Spoofing demonstrated that if the SSIDs are sorted alphabetical than availability of networks will no longer show as the top list of usable networks. Tampering from an evil portal attack can compromise credentials if the user is tricked into a similar network SSID. The Information Disclosure and Denial of Service attacks were partially successful. Information disclosure only happened when the user fell for a Evil portal attack off the network and Denial of Service only happen to segmented Wireless network. The segmented networks were able to successfully mitigates Repudiation and Elevation of Privilege threats.

The following steps would be to research if the Flipper Zero can do chained attacks to compromise networks. As of right now, attacks are independent and done in sequence. Additional software tooling on the device will enable this functionality which will require support from the open-source community and security researchers.

REFERENCES

[1] S. Cass, "A Hacker's Delight > You'll Either Love or Hate the Flipper Zero," in IEEE Spectrum, vol. 60, no. 5, pp. 18-20, May 2023, doi: 10.1109/MSPEC.2023.10120663.

[2] K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," in IEEE Communications Surveys & Tutorials, vol. 13, no. 2, pp. 245-257, Second Quarter 2011, doi: 10.1109/SURV.2011.041110.00022.

[3] V. Jain, V. Laxmi, M. S. Gaur, and M. Mosbah, "ETGuard: Detecting D2D attacks using wireless Evil Twins," Computers & Security, vol. 83, pp. 389-405, 2019, doi: 10.1016/j.cose.2019.02.014.

[4] Y. Chen, W. Trappe and R. P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, San Diego, CA, USA, 2007, pp. 193-202, doi: 10.1109/SAHCN.2007.4292831.

[5] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks, vol. 1, no. 2-3, pp. 293-315, 2003, doi: 10.1016/S1570-8705(03)00008-8.

https://stream.nyu.edu/media/Wireless%20Network%20Attacks%20with%20Flipper%20Zero/1_wxura313