Wi-Fi Deauthentication Bot: A Security Analysis Tool for Wireless Networks

B subhash
Reddysubash2620012@gmail.com
Girish V
gv5524442@gmail.com
Akash M
Akashm970s@gmail.com
Shekar U S
sureshut2@gmail.com

Abstract

Wi-Fi networks are widely used for providing wireless internet connectivity in both private and public environments. However, these networks are vulnerable to various security threats, with deauthentication attacks being one of the most common methods used to disrupt wireless communication. This paper introduces a Wi-Fi deauthentication bot, which is a tool designed to automate the process of conducting deauthentication attacks on a given Wi-Fi network. We explore the underlying principles of deauthentication attacks, demonstrate how they can be performed using automated tools, and discuss potential countermeasures that can help mitigate the impact of such attacks on modern wireless networks.

Keywords

Wi-Fi, deauthentication attack, wireless network security, bot, cybersecurity, network vulnerability

Introduction

Wireless networks, especially Wi-Fi, have become ubiquitous due to their convenience and ease of access. However, these networks are often targeted by attackers seeking to exploit vulnerabilities in network protocols. One of the most common methods for disrupting the normal operation of a Wi-Fi network is the deauthentication attack**.** The attack exploits a flaw in the IEEE 802.11 protocol, which is the foundation of most Wi-Fi communications, to force a client to disconnect from the network.

A deauthentication attack is typically launched by sending forged deauthentication frames to the target device, convincing it that the connection has been forcibly terminated. This may lead to denial of service (DoS), a disruption of the network, or even allow an attacker to intercept or spoof traffic if combined with other techniques. This paper aims to provide an overview of how a deauthentication bot can be developed and used to assess the robustness of wireless network security.

Background

IEEE 802.11 Protocol

The IEEE 802.11 standard governs the operation of Wi-Fi networks. It specifies the mechanism for wireless communication between a client device and an access point (AP). Each Wi-Fi communication session involves a series of management frames, which include authentication, association, and deauthentication frames. The deauthentication frame is used by the AP or client to terminate a session.

Deauthentication Attack

The deauthentication attack works by exploiting the lack of authentication for management frames in the 802.11 protocol. An attacker can send deauthentication frames to a client device, impersonating the AP and instructing the client to disconnect. Since the frames are not encrypted or authenticated, they can be easily forged by an attacker within the range of the wireless network. The attacker can execute this attack repeatedly, causing persistent disruptions to the network.

Use of Bots in Network Security

Bots have been used in various forms in network security, from automating penetration testing tasks to orchestrating large-scale distributed denial-of-service (DDoS) attacks. A Wi- Fi deauthentication bot automates the process of sending deauthentication frames to target devices, making it easier for a security professional to perform a simulated attack. This tool can be used to assess the resilience of Wi-Fi networks against deauthentication attacks.

Design and Implementation of the Deauthentication Bot

Requirements

The bot requires the following components:

- **Wireless Network Interface Card (NIC)**: A compatible NIC capable of packet injection (e.g., those based on the Atheros chipset).
- **Software Framework**: The bot can be implemented using Python with libraries such as Scapy or Aircrack-ng for crafting and sending deauthentication frames.
- **Target Information**: The MAC addresses of the target AP and the associated clients.

3.2 Architecture

The bot operates in the following stages:

1. **Scan for Networks**: The bot scans the surrounding environment for available Wi-Fi networks and identifies the target network (i.e., the AP to attack).
2. **Identify Clients**: Once the target network is identified, the bot scans for associated clients (devices connected to the AP).
3. **Send Deauthentication Frames**: The bot continuously sends forged deauthentication frames to both the AP and the client devices, forcing disconnections.
4. **Monitor Impact**: The bot monitors the results of the attack, such as whether devices disconnect or fail to reconnect automatically.

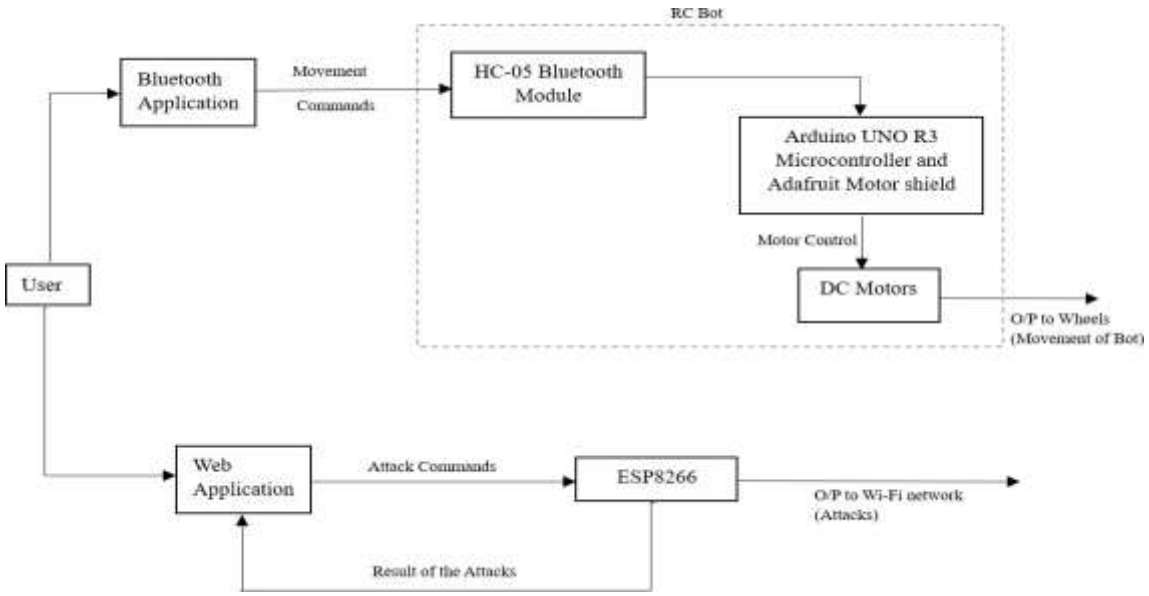
Code Snippet for Deauthentication Attack

python C

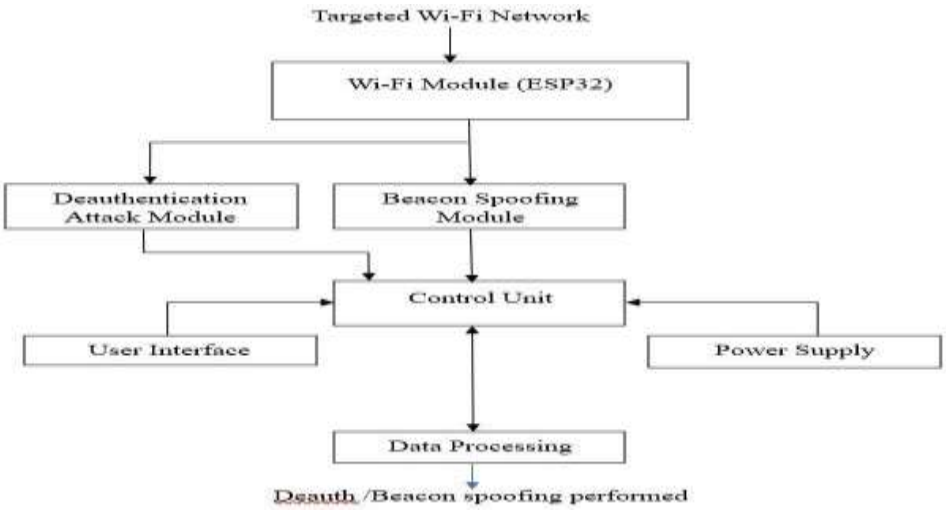
```
from scapy.all import *

# Define target AP and client MAC addresses target_ap_mac = "XX:XX:XX:XX:XX:XX" target_client_mac = "YY:YY:YY:YY:YY:YY"

# Send deauthentication packets
def deauth_attack(target_ap, target_client):
packet = RadioTap()/Dot11(addr1=target_client, addr2=target_ap, addr3=target_ap)/Dot11Deauth()
    sendp(packet, iface="wlan0mon", count=100, inter=0.1)

# Perform the attack deauth_attack(target_ap_mac, target_client_mac)
```

In the above code snippet, the bot uses the **Scapy** library to craft deauthentication frames and sends them to the target client. The deauthentication frames are repeatedly transmitted to disrupt the connection.

Block diagram



- **Flow Chart of Portable WiFi Deauthentication Bot for Security Testing**



Security Implications

While the deauthentication attack can be useful for testing Wi-Fi network security, it also poses significant risks if used maliciously. Attackers can leverage these bots to disrupt Wi-Fi networks, potentially causing loss of service for legitimate users and opening opportunities for further attacks such as man-in-the-middle (MITM) or credential harvesting.

To mitigate such risks, it is essential for network administrators to:

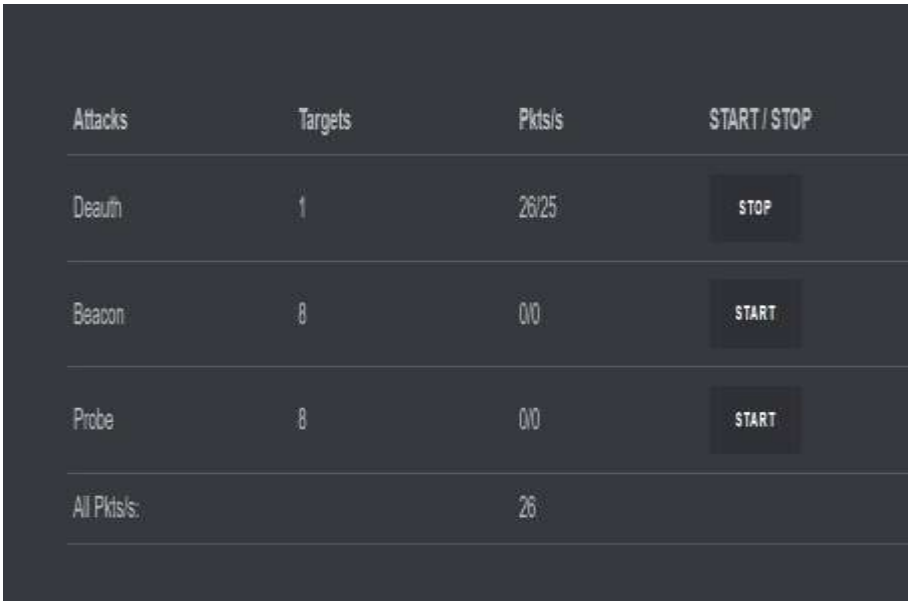
- Enable **WPA3** encryption, which provides stronger protections against certain types of attacks.
- Implement **802.11w** management frame protection, which authenticates and encrypts management frames, reducing the effectiveness of deauthentication attacks.
- Use **Intrusion Detection Systems (IDS)** to detect unusual behavior or repeated deauthentication frames.

Countermeasures and Prevention

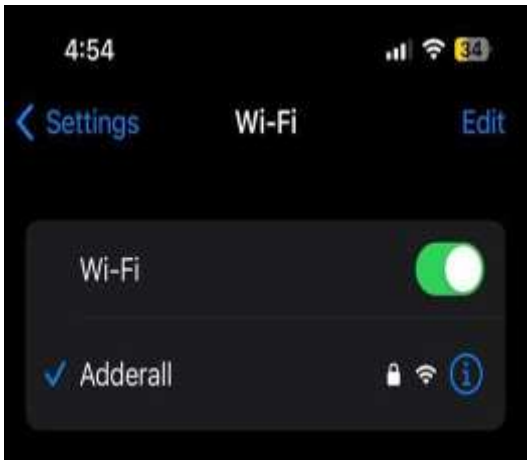
The primary defense against deauthentication attacks is the use of **802.11w** (Management Frame Protection), which secures management frames, including deauthentication messages. This prevents attackers from forging deauthentication frames. Additionally, using a combination of **WPA3 encryption** and **network monitoring tools** can help mitigate the impact of such attacks.

Result Analysis

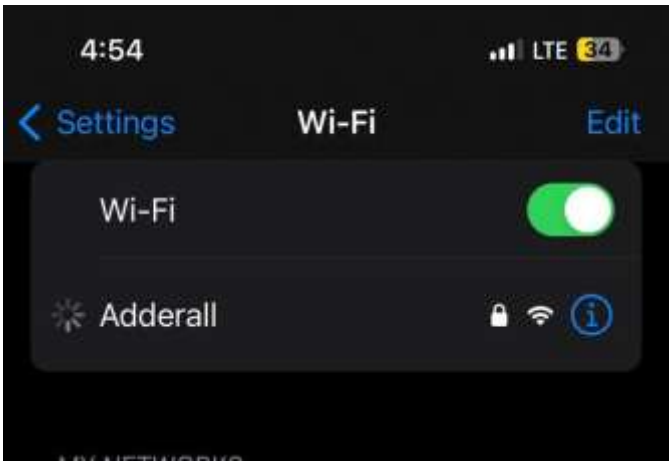
Web Page depicting various types of attacks



- **Deauther Attack:**

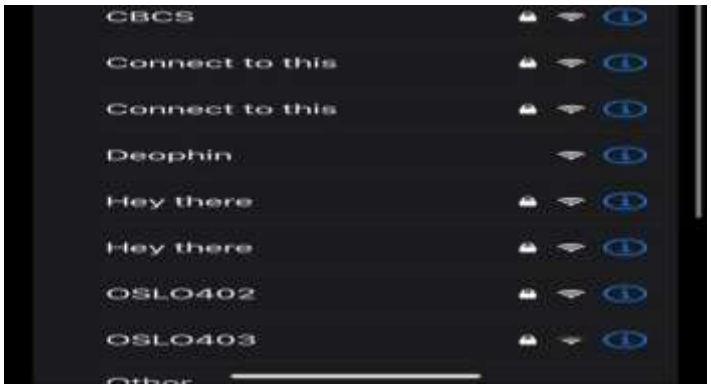


BEFORE ATTACK



AFTER ATTACK

FAKE Wi-Fi NETWORKS HAVE BEEN CREATED



References

[1] D. Eastlake, "IEEE 802.11 Management Frame Protection," IEEE Standard 802.11w, 2017.

[2] L. Zhang, A. S. Tanenbaum, and D. W. Lee, "Security in Wireless Networks," *Journal of Network and Computer Applications*, vol. 72, pp. 16-30, 2016.

[3] D. H. Grisham, "Deauthentication Attacks on Wireless Networks," *International Journal of Information Security*, vol. 13, no. 2, pp. 235-246, 2018.

[4] J. Hernandez, "Penetration Testing with Wi-Fi Tools: A Practical Guide," *Springer*, 2019.

[5] Aircrack-ng Project, "Aircrack-ng: A Wi-Fi Security Toolset," [Online]. Available: https://www.aircrack-ng.org. [Accessed: Nov. 2024].