Wi-Fi Security Demonstrator: Deauthentication & Evil Twin Attack using NodeMCU

Project Report

Institution: BR TECHGEEKS

Name: Keshav Gupta

Objective

To demonstrate the vulnerabilities of IEEE 802.11 wireless networks through controlled Deauthentication and Evil Twin attacks, and to propose countermeasures for securing Wi-Fi networks against such threats. The demonstration is performed on a test network to ensure legality and ethical standards.

Introduction / Theory

Wireless networks are widely used but are susceptible to various security threats due to weaknesses in the underlying protocols. This project focuses on demonstrating two well-known attack types:

1. Deauthentication Attack:
- This attack exploits the unencrypted nature of the deauthentication management frame in IEEE 802.11.
- By sending forged deauthentication packets, a client can be forcibly disconnected from a target access point.

2. Evil Twin Attack:
- This attack involves creating a fake access point (AP) with the same SSID as a legitimate AP.
- Victims unknowingly connect to the fake AP, enabling the attacker to intercept or manipulate data.

These attack simulations are conducted for educational purposes to raise awareness about wireless security and to present mitigation strategies.

Hardware & Software Requirements

Hardware

- NodeMCU (ESP8266)
- Breadboard & Jumper wires

- Power source (USB cable)
- Test router & test devices (mobile/laptop)

Software

- Arduino IDE
- ESP8266 board package installed
- Libraries: ESP8266WiFi.h, DNSServer.h (for Evil Twin portal)
- Web browser for control panel
- Wireshark / Airodump-ng (for detection demonstration)

Working / Implementation Steps

1. Deauthentication Attack Module:

- The ESP8266 sends forged deauthentication frames to clients connected to the target SSID (in this case, the test network 'Excitel 2.4').
- As a result, devices get disconnected.

2. Evil Twin Module:

- The ESP8266 creates a fake AP named 'EvilTwinAP', imitating the legitimate network SSID.
- Optionally, a captive portal can be used to mimic a login page.

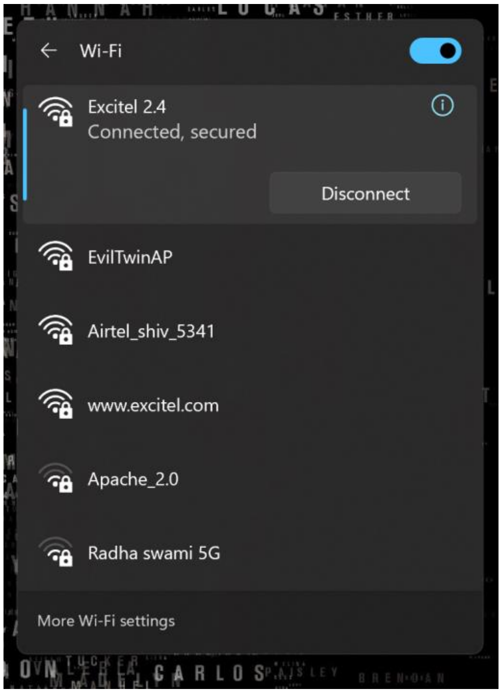
3. Detection & Prevention Demonstration:

- Using Wireshark/Airodump-ng to identify packet anomalies during the attack.
- Show preventive measures like WPA3 encryption, MAC filtering, disabling WPS, etc.

Setup and Demonstration

The setup involves flashing the NodeMCU with firmware that supports both Deauthentication and Evil Twin attacks. A control panel is accessed via a web browser to select the target network and execute the desired action.

1. Screenshot of the NodeMCU Wi-Fi list showing 'EvilTwinAP' created by the device.



Excitel 2.4
Connected, secured

EvilTwinAP

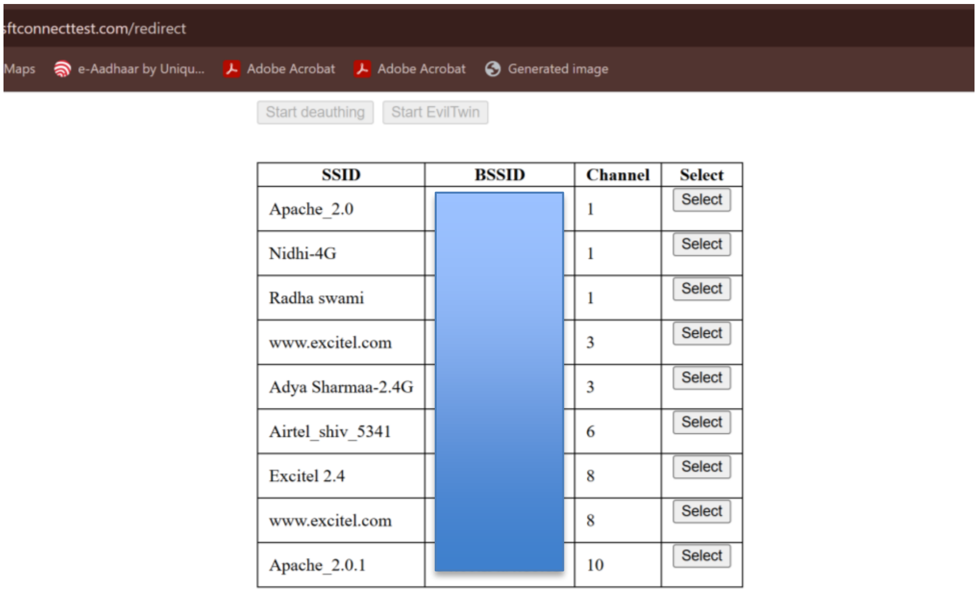
Airtel_shiv_5341

www.excitel.com

Apache_2.0

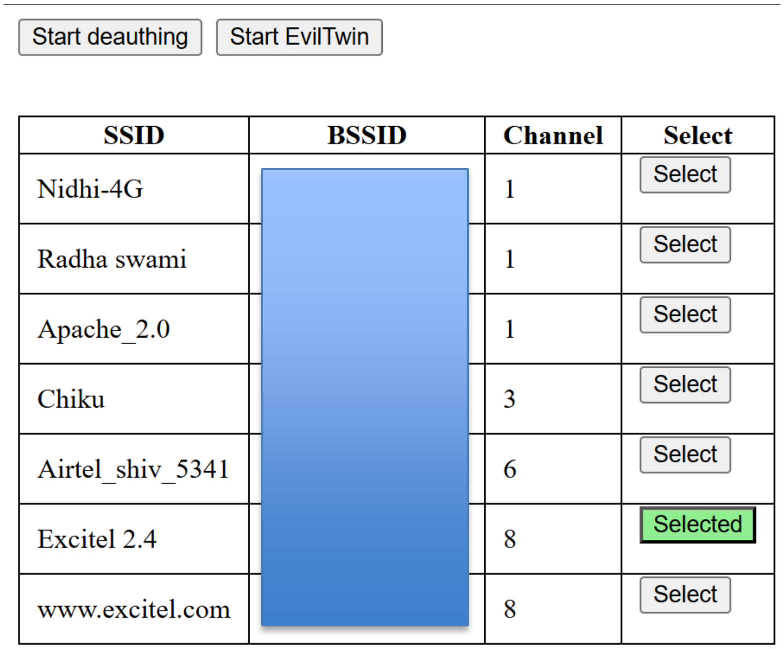
Radha swami 5G

2. Screenshot of the control panel/interface page from where the attack is launched.



SSID	BSSID	Channel	Select
Apache_2.0	[redacted]	1	Select
Nidhi-4G	[redacted]	1	Select
Radha swami	[redacted]	1	Select
www.excitel.com	[redacted]	3	Select
Adya Sharmaa-2.4G	[redacted]	3	Select
Airtel_shiv_5341	[redacted]	6	Select
Excitel 2.4	[redacted]	8	Select
www.excitel.com	[redacted]	8	Select
Apache_2.0.1	[redacted]	10	Select

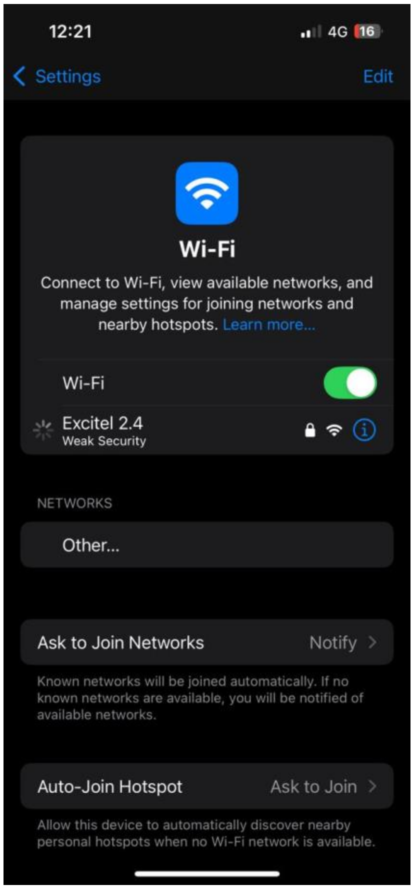
3. Screenshot showing 'Excitel 2.4' (personal test Wi-Fi) as the target in the interface.



SSID	BSSID	Channel	Select
Nidhi-4G	[redacted]	1	Select
Radha swami	[redacted]	1	Select
Apache_2.0	[redacted]	1	Select
Chiku	[redacted]	3	Select
Airtel_shiv_5341	[redacted]	6	Select
Excitel 2.4	[redacted]	8	Selected
www.excitel.com	[redacted]	8	Select

4. Screenshot of the another device being disconnected which are connected to Excitel 2.4

#Deauth Attack Successful



Wi-Fi

Connect to Wi-Fi, view available networks, and manage settings for joining networks and nearby hotspots. Learn more...

Wi-Fi

Excitel 2.4
Weak Security

NETWORKS

Other...

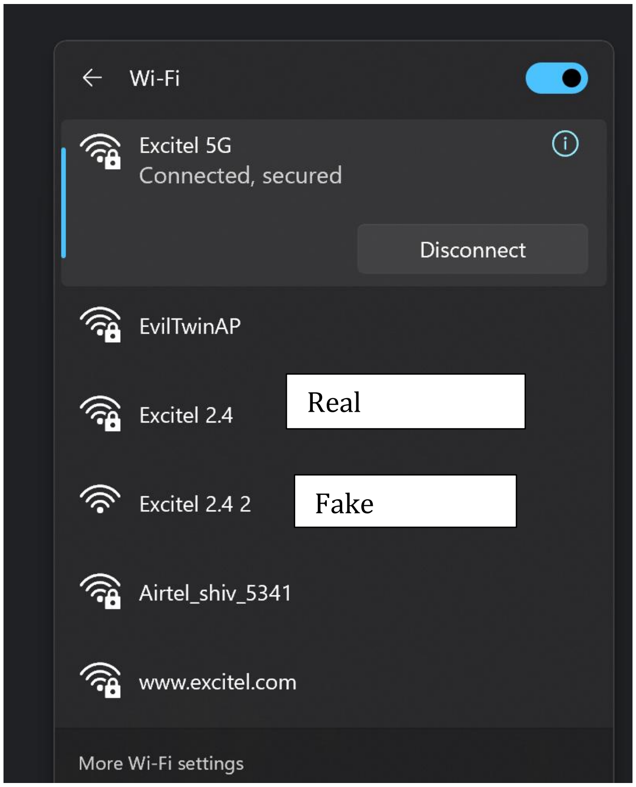
Ask to Join Networks — Notify

Known networks will be joined automatically. If no known networks are available, you will be notified of available networks.

Auto-Join Hotspot — Ask to Join

Allow this device to automatically discover nearby personal hotspots when no Wi-Fi network is available.

5) Screenshot of performing EvilTwin Attack on Excitel 2.4



## In this setup, a deauthentication (deauth) attack is executed on the legitimate Wi-Fi network, forcing connected clients to disconnect. As a result, when a user attempts to reconnect, they will be unable to join the original network due to continuous deauthentication. Instead, they are presented with a malicious access point (Evil Twin) configured to replicate the legitimate network's SSID. Once the user connects to this fake network and enters the Wi-Fi password into the authentication prompt, the credentials are captured by the attacker, providing unauthorized access to the legitimate network.

Code Overview

The Arduino code uses the ESP8266WiFi library to control the wireless interface of the NodeMCU. For Deauthentication, it crafts and sends forged 802.11 frames. For the Evil Twin, it sets up an AP with a specified SSID and optionally runs a DNS server to redirect traffic to a local captive portal page.

Security Recommendations

1. Use WPA3 encryption wherever possible.
2. Disable WPS to prevent brute force attacks.
3. Regularly update router firmware to patch vulnerabilities.
4. Monitor network for unusual traffic patterns.
5. Educate users about not connecting to unknown Wi-Fi networks.

Conclusion

This project successfully demonstrates two common Wi-Fi attacks using affordable hardware. By carrying out these tests in a controlled environment, it highlights the ease with which such attacks can be performed and stresses the importance of proper security configurations. The knowledge gained from this project can be applied to strengthen wireless network defenses.