University of Wah

Department of Computer Science

BS Cyber Security

Network Security

Project Report

Title: SPECTRUM-2.4G

Submitted to: Sir Inzmamul Haq

Group Members:

Muhammad Azfar Waqas (UW-23-CY-BS-013)

Ibrar Ul Hassan Shami (UW-23-CY-BS-018)

Hassan Iftikhar (UW-23-CY-BS-002)

Section: BS-CYS-5N

Table of Contents

1 Introduction:

Wireless communication technologies such as **Wi-Fi and Bluetooth Low Energy (BLE)** operating in the **2.4 GHz spectrum** are widely used in modern environments including smart homes, IoT systems, and mobile devices. Despite their convenience, these technologies are vulnerable to various network-level attacks that can compromise availability, confidentiality, and user trust.

This project focuses on the **analysis and demonstration of wireless security threats** targeting both **Wi-Fi and BLE networks** using an ESP32-based platform. The framework demonstrates how attackers exploit weak configurations and protocol limitations through **controlled simulations**, while also highlighting defensive and mitigation strategies.

The project is designed strictly for **educational and security awareness purposes**, emphasizing ethical testing and defensive network security principles.

---

2 Problem Statement:

Many users deploy Wi-Fi and BLE-enabled devices without understanding the security implications of these technologies. Weak authentication mechanisms, poor network monitoring, and lack of encryption awareness make such systems vulnerable to **denial-of-service, impersonation, and social engineering attacks**

Additionally, BLE devices often lack proper authentication and verification mechanisms, making them susceptible to **device spoofing and impersonation attacks**. There is a need for an educational framework that demonstrates these threats in a controlled environment to improve network security awareness.

---

3 Project Objectives:

The main objectives of this project are:

- To analyze common **Wi-Fi and BLE security threats** in the 2.4 GHz band
- To demonstrate Wi-Fi attacks such as:
  - ✓ Wi-Fi clone spam networks
  - ✓ Evil portal (captive portal impersonation)
  - ✓ Deauthentication and denial-of-service flooding
- To demonstrate BLE attacks such as:
  - ✓ Spoofed BLE device advertisements
  - ✓ Impersonation of trusted BLE peripherals
- To study the impact of these attacks on users and network availability
- To promote ethical hacking and defensive security awareness

---

4 Scope of the Project:

This project covers:

- Analysis of **Wi-Fi-based attacks**:
  - ✓ Fake Wi-Fi access points (Wi-Fi clone spam)
  - ✓ Evil portal demonstrations
  - ✓ Deauthentication and death-flood–style availability attacks
- Analysis of **BLE-based attacks**:
  - ✓ BLE device spoofing
  - ✓ Fake BLE beacon and device broadcasting
- Testing performed **only on authorized test networks and devices**
- Educational demonstrations within a laboratory environment

The project **does not target real-world networks** and strictly adheres to ethical and legal boundaries.

---

5 Tools & Technologies Used:

Tools & Technologies	Purpose
ESP32 DevKit (WROOM-32U)	Wi-Fi & BLE monitoring and simulation
Arduino IDE	Firmware development
IEEE 802.11 b/g/n	Wi-Fi protocol analysis
Bluetooth Low Energy (BLE)	BLE device advertising and analysis
Test Access Points	Controlled Wi-Fi environment
Test BLE Devices	BLE spoofing demonstrations
Laptop / PC	Logging, monitoring, and analysis

---

6 Methodologies:

The project follows a **controlled attack simulation methodology** to demonstrate wireless network vulnerabilities for educational and research purposes.

Threat Identification:

The following wireless threats are studied and demonstrated:

- **Wi-Fi Threats:**
  - ✓ Deauthentication attacks (availability disruption)
  - ✓ Fake access points (Wi-Fi clone spam)
  - ✓ Evil portal / captive portal impersonation
  - ✓ Flood-based denial-of-service attacks
- **BLE Threats:**
  - ✓ BLE device spoofing
  - ✓ Fake BLE advertisement broadcasting
  - ✓ Impersonation of trusted BLE devices

- **Identifies Assets:**
  - ✓ Network availability
  - ✓ User trust
  - ✓ Wireless device identity

---

7 Attack Implementation:

- The ESP32 is configured to operate in **Wi-Fi and BLE attack modes**
- Wireless packets are generated to:
  - ✓ Disrupt Wi-Fi connectivity
  - ✓ Broadcast fake Wi-Fi networks
  - ✓ Simulate evil portal behavior
  - ✓ Advertise spoofed BLE devices
- Attack modules are executed **only against test networks and devices** created for experimentation

---

8 Controlled Testing:

- All attacks are performed in an **isolated laboratory environment**
- Testing is limited to:
  - ✓ Personal access points
  - ✓ Authorized test devices
- The impact of each attack is observed in terms of:
  - ✓ Network availability loss
  - ✓ User confusion or misdirection
  - ✓ Device impersonation visibility

---

9 Expected Outcomes:

The expected outcomes of this project include:

- Successful demonstration of **Wi-Fi attacks** such as:
  - ✓ Deauthentication attacks
  - ✓ Wi-Fi clone spam networks
  - ✓ Evil portal (captive portal impersonation)
  - ✓ Flood-based denial-of-service attacks
- Successful demonstration of **BLE-based attacks**, including:
  - ✓ Spoofed BLE device advertisements
  - ✓ Impersonation of trusted BLE devices
- Practical understanding of how **wireless attacks affect network availability and user trust**
- Improved knowledge of **real-world wireless attack vectors** targeting the 2.4 GHz spectrum

---

10 Significance of the Project:

This project is significant as it provides a **hands-on demonstration of wireless network attacks** that are commonly discussed in theory but rarely visualized by students. By simulating real-world attack scenarios using low-cost hardware, the project helps bridge the gap between **theoretical network security concepts and practical attack behavior**.

The project emphasizes the importance of understanding **offensive techniques** in order to design stronger defensive strategies. It highlights how Wi-Fi and BLE technologies, despite being widely adopted, remain vulnerable to **availability, impersonation, and social engineering attacks**.

This work is particularly valuable for cybersecurity students, as it strengthens their understanding of **wireless threat models**, ethical hacking boundaries, and the real impact of network-level attacks.

---

11 Conclusion:

This project presents a controlled and ethical framework for demonstrating **Wi-Fi and BLE attack techniques** operating in the 2.4 GHz frequency band. By using an ESP32-based platform, the project provides a practical demonstration of how wireless networks and devices can be disrupted or impersonated when security measures are weak or improperly configured.

The project reinforces the importance of wireless security awareness and highlights the need for proper configuration, monitoring, and user education. While the system focuses on attack simulation only, the analysis of attack behavior contributes to a deeper understanding of how such threats can be mitigated in real-world environments.

Overall, the project successfully meets its objective of enhancing practical knowledge in **network security and wireless attack analysis**.

---

12 References:

1. IEEE Standards Association. (2021). *IEEE 802.11 Wireless LAN Standards*.
2. Bluetooth SIG. (2022). *Bluetooth Low Energy Security Overview*.
3. Espressif Systems. (2023). *ESP32 Technical Reference Manual*.
4. NIST. (2012). *Guidelines for Securing Wireless Local Area Networks (WLANs)* (SP 800-153).
