Offensive and Defensive Wi-fi/Bluetooth PEN-Tool

Project Proposal

A report submitted to

Department of Electrical and Information Engineering

Faculty of Engineering

University of Ruhuna

On 25nd of April 2025

In partial completion of the module

EE6304 - Embedded Systems Design

Contents

1 INTRODUCTION

1.1 PROBLEM STATEMENT

In today's mutual connected world, wireless networks such as Wi-Fi and Bluetooth are integral parts of equipment ranging from smartphones to IOT systems. However, these networks are susceptible to various cyber security hazards, including de-authentication attacks, evil access points and unauthorized device tracking. Ethical penetration testing is necessary to identify and reduce these weaknesses, yet many existing equipment is either heavy, expensive or limited in their ability to assess both offensive and defensive. In addition, consumer-grade hardware like ESP32 often suffers from signal noise and limited range, which reduces effectiveness in diverse environments.

The project proposes a compact and portable device based on ESP32 microcontroller, an aggressive and defensive Wi-Fi/Bluetooth pen-tool. The device will increase the strength of the signal and reduce noise interference, as well as adapted to customize wireless scanning and testing capabilities, equipped with a TFT touch display with pencil. The device will provide an intuitive interface for moral penetration testing and sniffing packets, enabling users to more effectively assess and secure the wireless network.

1.2 OBJECTIVE

To design and implement a secure, portable Wi-Fi/Bluetooth penetration testing tool with the highly capable for noisy and high traffic networks by enhancing signal strength. ESP 32 bases firmware to conduct offensive and defensive wireless security assessments with improved signal reliability and user-friendly operation.

1.3 PROJECT SCOPE

This project focuses on creating a compact, user-friendly penetration test tool for Wi-Fi and Bluetooth networks using a microcontroller. Customized code enhances the device signal range and clarity, efficiency. A user involving the TFT touch Screen will improve the interface. Operating in the network to maximize security, the tool is designed for moral penetration testing applications.

The proposed device will support the following functionalities:

- Wi-Fi network scanning and analysis: Finding details such as SSID, channel, RSSI and encryption type for network reconnaissance, access points (APs) and client devices.
- Bluetooth device Discovery: To evaluate Bluetooth security configuration, identifies nearby Bluetooth devices, including names, addresses and signal power.
- Rough AP Simulation: To imitate network answers to client and unauthorized APS, this transmits fake SSID to simulate rough access points.
- Packet Sniffing and Logging: This will capture Wi-Fi packets, frames in PCAP format, saved to an SD card, to offline vulnerability analysis.
- TFT Touch Screen-based user interface: Scan results for intuitive researcher, showing system prompts and menu options.
- GUI interface: enables users to select tasks, scroll through results, and start actions through user -friendly inspection.
- Enhanced Signal Strength: The use of external antennas is supposed to improve the range of search and reduce noise in a crowded wireless environment.
- Offline Monitoring: Stores captured packets in PCAP format for offline analysis (e.g., with Wireshark).

Although this device is designed to be secure and practical, there are several constraints as well.

- Control over the selected authorized network for pen testing: The device operates, with the devices having MAC addresses for the penetration testing through Wi-Fi/Bluetooth-based remote control, enhancing security but with remote configuration.
- Range: Depends on antenna quality (Specially, inbuilt antenna), the measuring signals strength and noise will vary with the network environment (typically 50-100 meters with internal antenna).
- De-authentication Attacks: Due to ESP32-IDF restrictions, cannot send de-auth frames limiting certain Wi-Fi attack simulations.
- No Cloud Integration: The system avoids cloud connectivity to prevent remote attacks, restricting features like real-time data sharing.

2 SPECIFICATIONS

The final product is expected to fulfil the following specifications.

2.1 Network Through Real Time Operations.

1. Wi-Fi Network Analysis:

- Access point scan: detects SSIDs, channels, RSSI and encryption types (e.g., WEP, WPA2).
- Station Scanning: Identifies connected client devices, helping to detect rough devices.
- Channel analyzer: View Wi-Fi channel activity to identify congestion or anomalies.
- Packet sniffing: Capture PCAP Wi-Fi packages for offline analysis, revealing non-encrypted traffic or weaknesses in protocol.

2. Discovery of the Bluetooth device:

- Classic Bluetooth Scanning: List nearby devices with names, addresses, and signal forces.
- BLE Scanning: Detects low -energy Bluetooth energy devices, common in IoT, to evaluate pairing or firmware vulnerabilities.

3. Rough Access Point Simulation:

- Broadcasting fake AP: Creates fake SSIDs to test customer self-connection behaviors or network monitoring systems.
- Use case: Identify vulnerable devices to connecting to unqualified APS.

4. Floods of the SSID:

- Flood attack simulation: transmits several false SSIDS to stress-test network scanners or client devices.
- Usage: Evaluate the effectiveness of the intrusive detection system (IDS) against the flood of AP.

5. Some offensive attacks for pen test:

- Portable control: uses evil port attacks for ethical operations.
- Data portability: Stores logs on the Zero Flipper SD card.

6. Menu Navigation Via TFT Touch screen with Pencil.

The interface will support actions such as:

- Navigating through stored account entries
- Separate pen testing for Bluetooth and Wi-Fi
- Data frame monitoring
- Overall user-friendly interface with touch pencil

2.2 Offline Operation

The device will function entirely offline for monitor and analyze PCAP file on SD card.

- PCAP Storage: Saves captured packets to SD card for detailed analysis with tools like Wireshark.
- Scan Logs: Records scan results for reporting and documentation.

3 BLOCK DIAGRAM

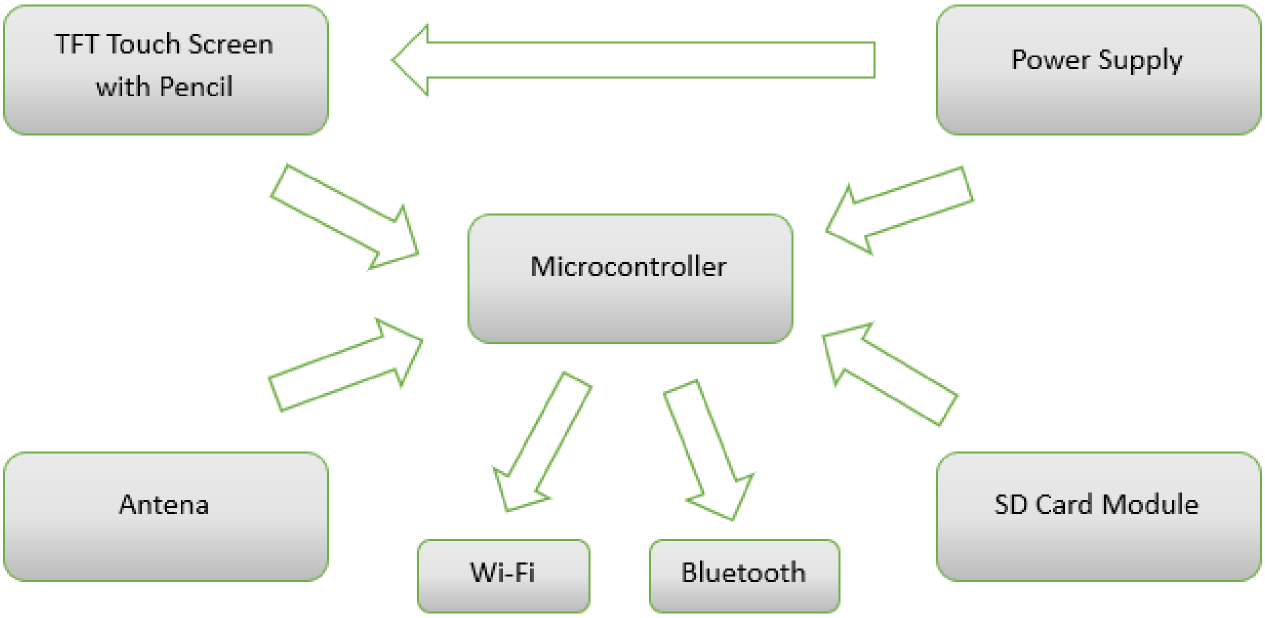

Figure 3.1: Block Diagram of the Proposed USB-Based Secure Authentication Dongle

3.1 Block Descriptions

1. Microcontroller

This microcontroller is designed for wireless penetration test, with integrated Wi-Fi and Bluetooth capabilities. It runs a customized code for Wi-Fi and Bluetooth scanning, disease AP simulation and sniffing packets. The system uses inputs from TFT touch-screen or buttons to navigate menus, select scanning modes, or start actions such as SSID broadcasting. TFT display shows output scan results, system status and menu options. The system interfaces with the SD-card module to protect the captures occupied in PCAP format for the Offline Format analysis.

2. TFT Touch Screen

The TFT with the pencil serves as the primary user interface to communicate with the touch-screen system. It displays real-time system information, including scan results, system status, menu options, and packet capture or starting actions like fake SSID transmission. The pencil enables a specific interaction, which makes the field more user -friendly for field operations.

3. The external power supply

Provides the electrical power needed to operate a power supply block system, ensuring that all components work reliably during penetration test tasks. It can be applied as a USB interface, battery or external power bank potential 5V for peripherals such as SD-card module.

4. Antenna (optional)

The antenna block represents an external antenna attached to the microcontroller, a major customization to increase the power of the signal and reduce the noise. By replacing that onboard PCB antenna, its U.FL. Connects to the microcontroller via the connector. External antennas increase the range and sensitivity of Wi-Fi/Bluetooth scanning, improving the investigation of distant points access points and devices.

5. Wi-Fi

The Wi-Fi block represents the integrated Wi-Fi functions in the microcontroller, enlarged by the external antenna. It enables the device's main penetration test features, such as scanning, packet sniffing, disease AP simulation and device discovery.

6. Bluetooth

Bluetooth supports the penetration test of Bluetooth devices, receiving details such as device names, Mac addresses and signal power.

7. SD card module

SD-card module offers non-existing storage for capture data and configurations, which are essential for the offline flame analysis and operational flexibility. It stores Wi-Fi packets in PCAP format for offline analysis, preserves configuration files, ensures the view of data in the power cycle, and allows users to collect data in the field and analyze it later.

4 EXPECTED OUTCOMES

- Security Vulnerability and weakness identification: widespread reports on Wi-Fi and Bluetooth weaknesses, including poor encryption, disease devices and misunderstood APs.
- Network Hardening: Recommendations for protecting wireless environment, such as self-connecting features.
- Tool Development: Customized code for microcontroller with specific functional operation requirements.
- Team skill growth: experience with wireless security test and embedded development.