ZYNC

Portable WiFi Vulnerability Scanner

Problem Statement

Many people connect to WiFi networks without knowing if they're safe. Public or weakly protected networks can expose users to hacking and data theft. This project aims to build a small, portable device using an ESP32 that scans nearby WiFi networks and checks for basic security issues like open access or weak encryption. The goal is to help everyday users quickly see if a network is safe before connecting — no technical knowledge needed.

Proposed Solution

The proposed solution is a portable WiFi security scanner built using an ESP32 microcontroller, an OLED display, and a set of control buttons. The device will scan for nearby WiFi networks and display key information such as the network name (SSID), signal strength, encryption type (e.g., Open, WEP, WPA), and a basic risk level. By analyzing this data, the device will identify potentially insecure networks and visually alert the user. The goal is to make WiFi security assessment simple, fast, and accessible — especially for non-technical users who may not know how to identify a risky connection. The system will run entirely on the embedded hardware and be powered by a battery, making it portable and easy to carry.

To enhance usability and data accessibility, the device will also support Bluetooth communication with an Android application. The app will allow users to:

- View live scan results sent from the ESP32
- Log historical scans with timestamps
- Export scan data in formats like CSV or JSON

This integration provides users with a more detailed and interactive interface while retaining the standalone functionality of the hardware device. It bridges IoT with mobile technology to deliver a more robust and user-friendly cybersecurity tool.

Expected Output / Demonstrable Features

During the final demo, the device will power on and automatically scan for nearby WiFi networks. The OLED screen will display key details for each detected network, such as:

- SSID (WiFi name)
- Signal strength (RSSI)
- Encryption type (Open, WEP, WPA, WPA2)
- Security status (e.g., Secure, Weak, or Insecure)

Users will be able to navigate through the list of networks using physical buttons on the device. The system will clearly highlight potentially unsafe networks—such as open networks or those using outdated encryption—through visual alerts. No internet connection or pre-configuration will be required for the hardware to function.

In addition, the project includes a companion Android application that connects to the device via Bluetooth. During the demo, the app will:

- Receive live scan data from the ESP32 in real-time
- Display a detailed list of WiFi networks with risk indicators
- Log previous scans locally within the app
- Allow users to export scan data (e.g., in CSV format) for further analysis
- Optionally use device location to tag scan logs with GPS coordinates (if permitted)

This complete system—both hardware and software—will demonstrate a working prototype that enables users to assess WiFi network security easily, with both a physical display and a user-friendly mobile interface.

Technology Stack

Front-End : Flutter(Dart)

Back-End : FastAPI

Database : PostgreSQL

DevOps & CI/CD **:** Git, Github

Cloud Platforms & Hosting : Render

AI / Machine Learning / Data Science : Python

Generative AI & LLM APIs : Gemini API

Visualization & BI Tools : Streamlit

APIs & Integration : REST API, Postman, JSON