# **Software Design Document (SDD)**

## **Project Title: Wi-Fi WPA2 Key Extractor GUI**

### **1. Introduction**

**Purpose:** This document provides a detailed software design for the Wi-Fi WPA2 Key Extractor GUI tool. The purpose of this application is to allow ethical hackers, penetration testers, and cybersecurity enthusiasts to automate WPA2 handshake capture and key extraction with a modern, user-friendly graphical interface.

**Scope:** The tool enables users to scan for available Wi-Fi networks, automatically select the best client for deauthentication, capture WPA2 handshakes, and attempt password cracking. It includes a GUI built using PyQt5 and relies on existing Linux utilities like airmon-ng, airodump-ng, aireplay-ng, and aircrack-ng.

**Intended Audience:**

* Cybersecurity students
* Penetration testers
* Red team professionals

### **2. System Overview**

The application is a Python-based GUI tool that integrates Linux terminal utilities with PyQt5 to perform WPA2 cracking workflows in an interactive, animated format.

**3. Functional Requirements**

* **Scan Networks:** List available Wi-Fi SSIDs, BSSIDs, and Channels using nmcli.
* **Capture Handshake:** Initiate monitor mode and capture WPA2 handshakes with airodump-ng.
* **Deauthenticate Client:** Automatically find the strongest client and send deauth packets using aireplay-ng.
* **Crack Key:** Use aircrack-ng to brute-force the key with a predefined wordlist.
* **Restore Wi-Fi:** Disable monitor mode and restart network services.

### **4. Non-Functional Requirements**

* Cross-platform compatibility with Debian-based Linux distributions
* Requires root access for packet injection and monitoring
* Responsive GUI with multithreading to prevent freezing
* Must run in Python 3.6+

### **5. Architecture Design**

**Technology Stack:**

* **Language:** Python 3
* **GUI Framework:** PyQt5
* **System Tools:** airmon-ng, airodump-ng, aireplay-ng, aircrack-ng, nmcli

**Modules:**

* GUI (Main Window, Buttons, Labels, List)
* Wi-Fi Scanner Module
* Deauthentication Module
* Handshake Capture Module
* Cracking Module
* Wi-Fi Restore Module

### **6. User Interface Design**

* **Window Title:** Wi-Fi WPA2 Key Extractor
* **List Widget:** Displays SSID, BSSID, and Channel
* **Progress Bar:** Shows status of scanning/attack/crack
* **Status Label:** Text status of current operation
* **Buttons:**
  + Scan Networks
  + Start Attack
  + Restore Wi-Fi

### **7. Data Flow**

1. User clicks **Scan** → Calls nmcli → Parses results → Populates list
2. User selects network → Clicks **Start Attack**
3. Tool starts monitor mode, launches airodump, finds best client, runs aireplay
4. Captures .cap file and uses aircrack-ng to crack
5. Displays result and allows Wi-Fi restoration

### **8. Security Considerations**

* Tool must be run with root privileges (use sudo)
* Logs are not saved to disk (to avoid accidental leakage)
* Intended strictly for educational/authorized testing only

### **9. Limitations**

* Only supports external Wi-Fi adapters capable of monitor mode
* Wordlist-based cracking may fail if the password is not in the list
* Works only on Linux systems

### **10. Future Enhancements**

* Add support for Hashcat (GPU cracking)
* Live packet viewer panel
* Configurable wordlist path
* Support for saving handshakes for later cracking

### **11. Appendix**

**Dependencies:**

* Python 3
* PyQt5
* aircrack-ng suite

**Run Instructions:**

sudo apt install python3-pyqt5 aircrack-ng

python3 wpa2\_gui.py

**Author:** Laxmish Saini  
 **Last Updated:** March 31, 2025