Design and Implementation of WPA2 Wi-Fi Cracking Attack

Awesh Islam, 2005054
Ha Meem, 2005055
Department of Computer Science and Engineering
Bangladesh University Of Engineering & Technology

July 25, 2025

Abstract

This report details the design, implementation, and analysis of a WPA2 Wi-Fi password cracking attack tool. The tool was developed using C/C++/Python to capture and exploit WPA2 4-way handshake packets. The attack involves triggering deauthentication frames to collect handshake data, followed by offline analysis to recover the password. We discuss the topology, attack timing, packet/frame modifications, and justify why our design should work.

1 Introduction

Wireless networks, specifically those secured by WPA2-PSK, are vulnerable to offline attacks, especially when weak passwords are used. In this project, we developed a custom tool to crack WPA2 passwords by exploiting the 4-way handshake protocol. The attack is executed through a deauthentication strategy that forces clients to reconnect, enabling the capture of critical handshake packets for offline analysis.

2 Attack Definition and Topology

2.1 Attack Overview

The attack aims to exploit the WPA2-PSK protocol's reliance on the 4-way handshake process, which is unencrypted and susceptible to offline dictionary attacks. Our custom tool intercepts this handshake after forcing a client to reconnect through a deauthentication attack. This enables us to test potential passwords using an offline brute-force method.

2.2 Network Topology

The following diagram illustrates the network topology for the attack:

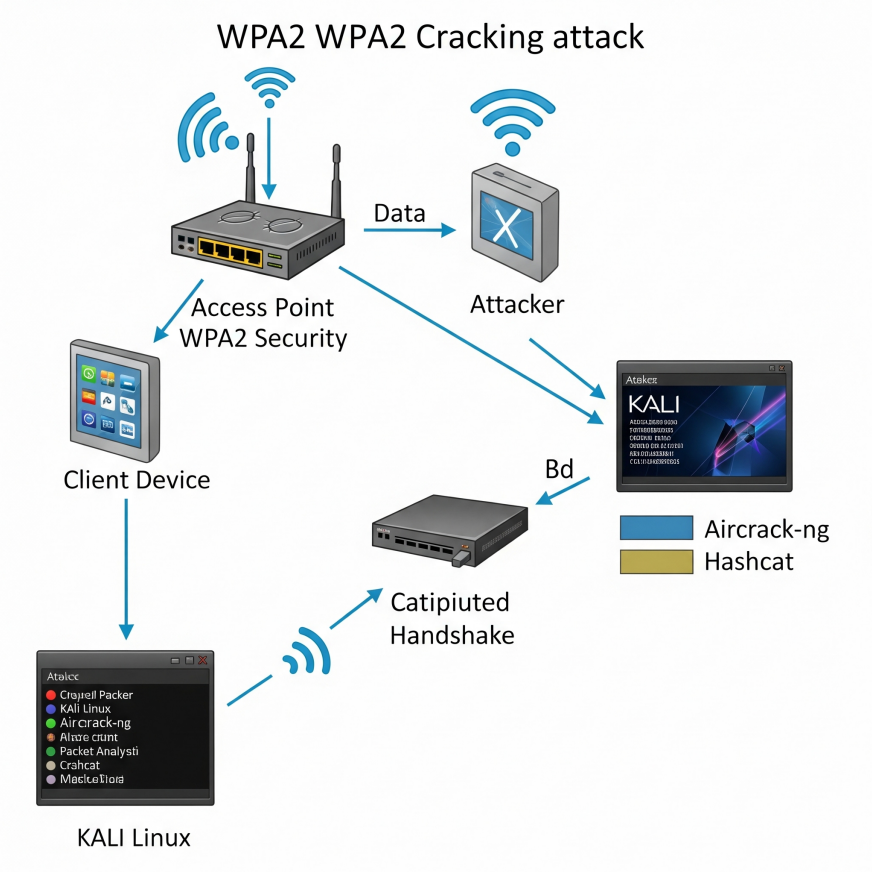

Figure 1: Attack Network Topology: Access Point (AP), Client, Attacker (Monitor Mode)

3 Timing Diagrams

3.1 Original WPA2 4-Way Handshake

The original WPA2 handshake sequence involves:

- **Step 1:** The AP sends an ANonce (random number) to the client.
- **Step 2:** The client generates an SNonce and sends it to the AP.
- **Step 3:** Both the AP and client exchange a Message Integrity Code (MIC) for verification.
- **Step 4:** The AP sends a GTK (Group Temporal Key) to the client, completing the handshake.

This process securely establishes encryption keys.

3.2 Attack Timing Diagram

The attack consists of:

- **Step 1:** Attacker sends deauthentication packets to the client, forcing it to disconnect.
- **Step 2:** The client reconnects, initiating a new handshake.
- **Step 3:** Attacker captures the 4-way handshake.
- **Step 4:** The attacker performs offline brute-force or dictionary attacks to determine the PSK.

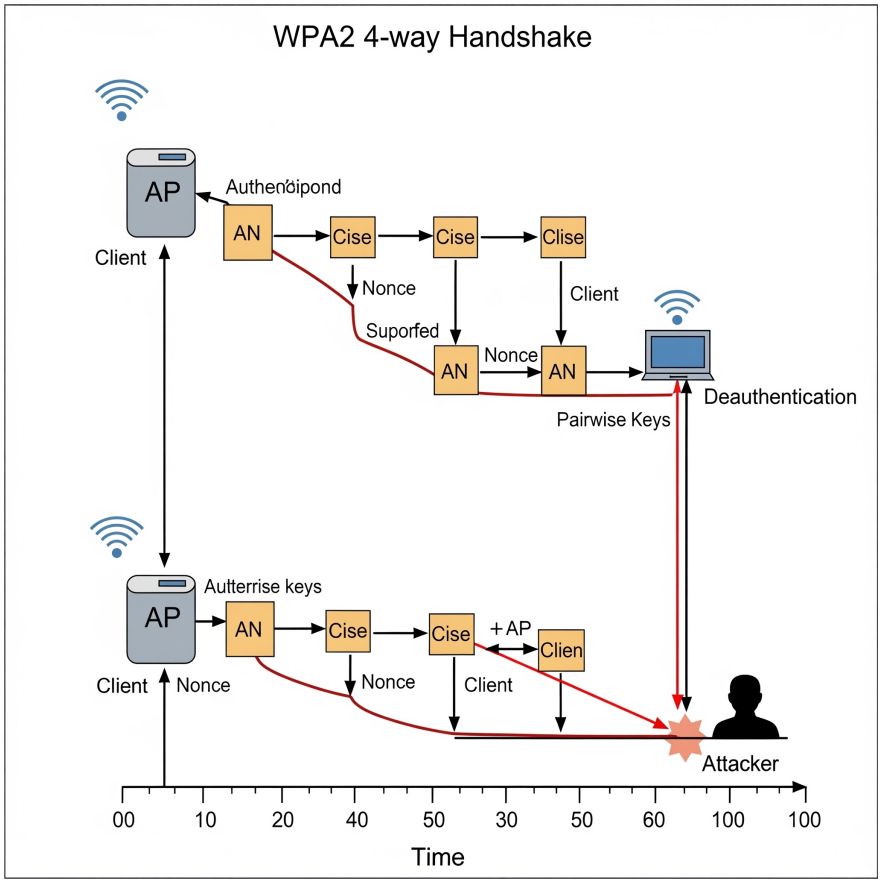

Figure 2: Timing Diagram: WPA2 4-Way Handshake and Attack Process

4 Packet and Frame Details

4.1 Deauthentication Frame Structure

The deauthentication packet is a management frame designed to disconnect the client from the AP:

- **Type/Subtype:** 0x00 (Management/Deauth)
- **Destination Address:** Victim's MAC address

- **Source Address:** Spoofed AP MAC address
- **Reason Code:** 7 (Class 3 frame from nonassociated station)

These values ensure the client disconnects and reconnects, triggering the 4-way handshake.

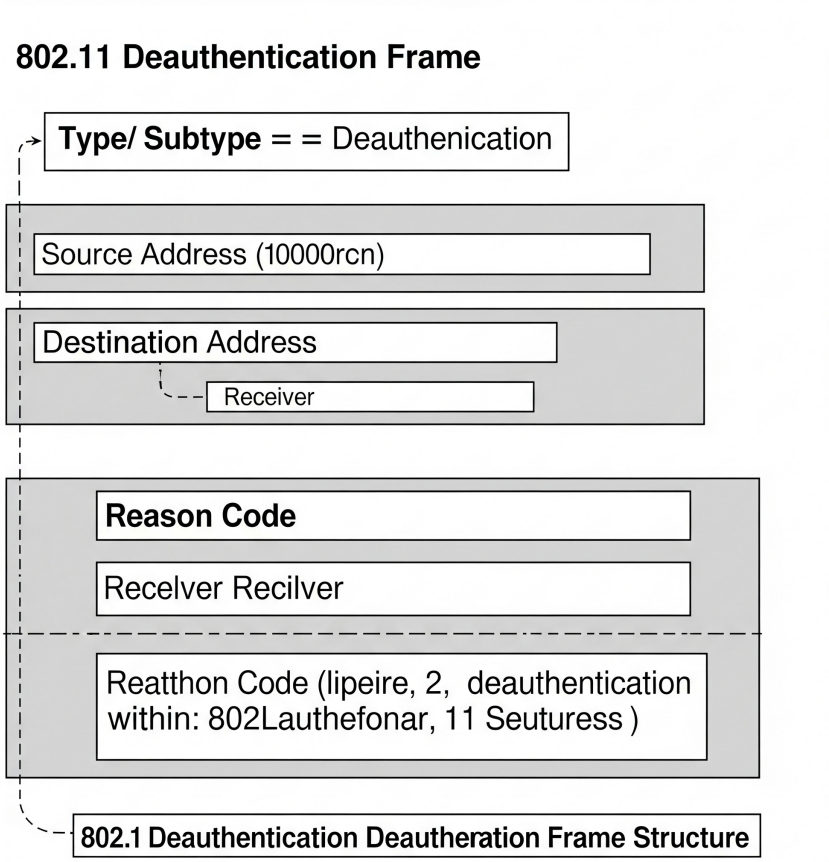

Figure 3: Deauthentication Frame Structure

4.2 Handshake Capture

The handshake packets contain:

- **ANonce/SNonce:** Random nonces generated by the AP and client.
- **MIC:** Message Integrity Code used to validate the handshake.
- **MAC Addresses:** Identifiers for the AP and client.

These elements are captured during the reconnection, allowing the attacker to attempt offline cracking.

5 Attack Justification

We believe this design works due to the following reasons:

- **Unencrypted Handshake:** The 4-way handshake is sent in plaintext, making it accessible for packet capture.
- **Offline Attack:** All required cryptographic material is contained in the handshake, allowing offline cracking without network detection.
- **Weak Passwords:** Many WPA2 networks use weak passwords, making dictionary and brute-force attacks feasible.
- **Client Trust:** The client trusts deauthentication frames from any source, allowing the attacker to forcibly disconnect and trigger a new handshake.

These factors ensure the feasibility and effectiveness of the attack.

6 Conclusion

This report outlines the design and implementation of a WPA2 Wi-Fi cracking attack tool. By leveraging a deauthentication strategy, we capture critical handshake data and perform offline analysis to recover the PSK. Our approach highlights the vulnerabilities in WPA2, particularly the reliance on weak passwords and unencrypted handshake messages.