Spoofed MAC Address Detection with ESP 32

Justin Ngo

CMPEN 462

04.18.25

Abstract:

The purpose of this project is to develop a hybrid device capable of WiFi client tracking and detecting spoofed MAC addresses using an ESP32 microcontroller in promiscuous mode. The goal is for the ESP32 to passively listen to the nearby wireless traffic, and log detected MAC addresses from the corresponding probe requests and beacon frames. By passively listening to incoming connections, the device can build up a whitelist of valid MAC addresses and their typical signal strength to spot when a MAC address has been spoofed.

Materials:

- Arduino Nano ESP32
- Breadboard
- LEDs

Work Breakdown:

| Date | Milestone | Details |
|---|---|---|
| 04.21 | Initial Setup | Set up the Arduino environment, ESP32, and verify that the board works in promiscuous mode. |
| 04.25 | MAC Address Logging and Whitelisting | Within the IDE set up a way for the ESP32 to log and whitelist incoming connections from known sources (i.e. the phones and laptops of my roommates) |
| 04.30 | Spoofing Detection and Testing | After confirming that the ESP32 is successfully and accurately logging the incoming information from the incoming connections, begin building the capability to detect when a MAC address is being spoofed, test by modifying my own MAC address and look for changes in data |
| 05.03 | Alert and Output Formatting | Once the core functionality is working, design a way for the ESP32 to display that there was an attempt to make a connection with a spoofed MAC address and light up an LED while outputting a log event to the terminal |
| 05.07 | Report Writing | After finalizing the device, record the demonstration video and document the methodology and work for the final submission on the 7th |