WIFI JAMMER AND HACKING
IT5611-EMBEDDED SYSTEM AND IOT LABORATORY
DEPARTMENT OF INFORMATION TECHNOLOGY | MIT CAMPUS :: ANNA UNIVERSITY, CHENNAI

MENTOR:UMAMAHESWARI

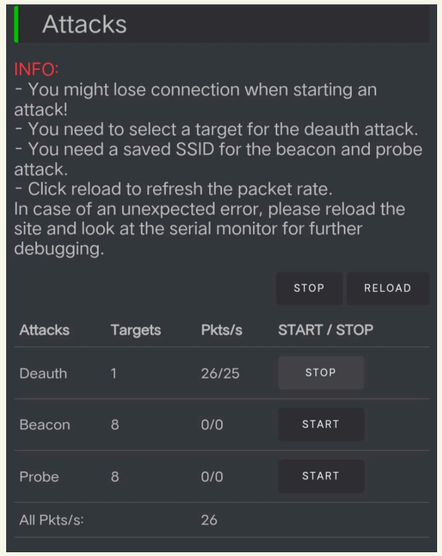
2021506068	RAJ KUMAR A D
2021506069	RAMESH KANNA S
2021506307	PREMKUMAR M

TEAM MEMBERS

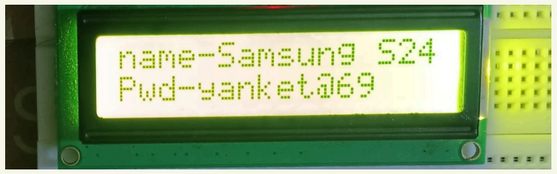
OBJECTIVES

- Develop a WiFi jammer using one NodeMCU device to disrupt wireless network connections within a specified range.
- Implement a functionality on the second NodeMCU device to create multiple fake WiFi networks, enticing nearby devices to connect.
- Utilize I2C communication to transfer hacked WiFi passwords from the NodeMCU device to an LCD display for visualization.
- Enhance security awareness by demonstrating the vulnerabilities of WiFi networks and the importance of securing them against potential threats.

CONNECTION AND SETUP



RESULT

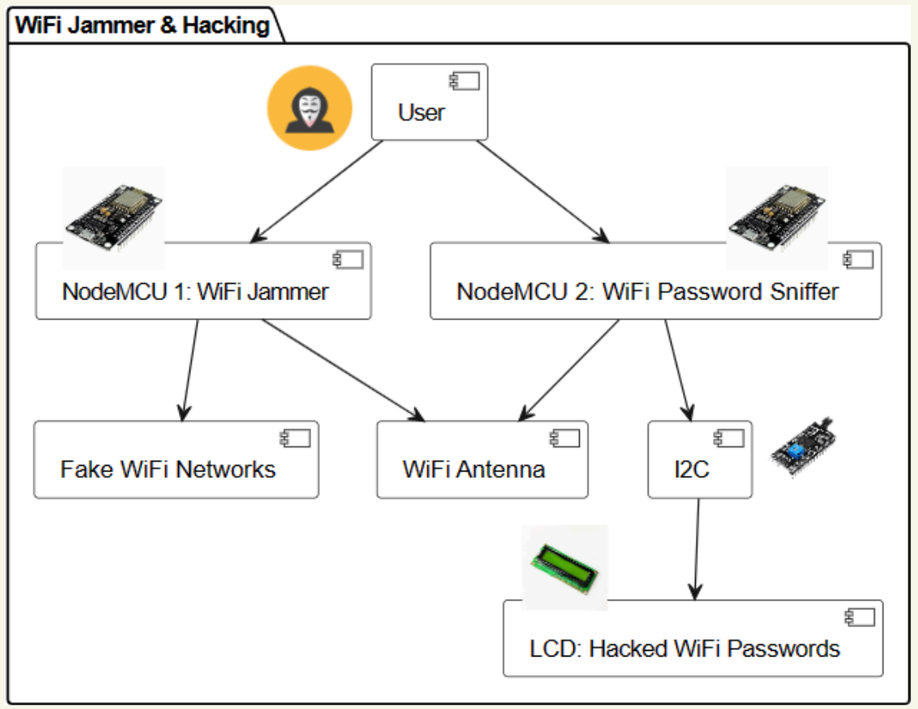


- Develop a WiFi jammer and hacking system using two NodeMCU boards to disrupt and intercept WiFi signals, with one NodeMCU dedicated to jamming and creating fake WiFi networks, and the other NodeMCU focused on capturing passwords.
- Implement an LCD display with I2C interface to visualize the hacked WiFi passwords in real-time, providing a user-friendly interface for monitoring and managing the intercepted data.

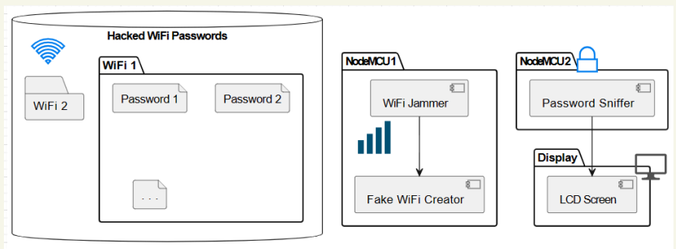
REQUIREMENTS

- **NodeMCU ESP8266**
- **LCD Display Module**
- **I2C Interface**
- **Power Supply**
- **USB Cables**
- **Arduino IDE**

OVERALL ARCHITECTURE



PROCESS



CONCLUSION

- The implementation of the WiFi jammer and hacking system demonstrates the feasibility of using NodeMCU boards for disrupting and intercepting WiFi signals effectively.
- The integration of an LCD display with I2C interface enhances the usability and accessibility of the system by providing real-time visualization of hacked WiFi passwords.

FUTURE SCOPE

- Further enhance the capabilities of the WiFi jammer and hacking system by incorporating advanced signal processing techniques to improve signal jamming effectiveness and password interception accuracy.
- Explore the possibility of integrating machine learning algorithms for automated password recognition and classification, enabling the system to identify and prioritize high-value WiFi passwords for more targeted attacks.