COMP6841 Project

Z5286111

Wenqian Zhang

Introduction

This is fishing wifi modelled on UNSW's wifi and running on raspberry pi, can do some operations on other hardware through Grovepi+.

Code

Github link:

https://github.com/Jamesxwq/COMP6841_proj

Video

The video of these two links is the same, but Youtube will have a higher definition.

Flipgrid link:

https://flipgrid.com/s/4XwfRhBxYBLC

YouTube link:

https://www.youtube.com/watch?v=wCiVEr4_N0E

Setup

`curl -kL dexterindustries.com/update_grovepi | bash` to setup Grovepi+

`sudo python3 frist_time_setup.py` to setup the project

Tested environment

- raspberrypi v5.10.103(buster)

  (It can also run on Bullseye, which is the latest system version of Raspberry Pi, but since Grovepi+ cannot be installed on Bulleye, only the fishing function (`python3 setup_wifi.py`) can be enabled in this version, and hardware connection cannot be performed.)

- Python v3.7.3
- hostapd v2.8
- lighttpd v1.4.53
- Dnsmasq v2.80

Hardware

- Raspberry Pi 4 Model B 4GB
- Grovepi+
- Grove - Button(P)
- Grove - Switch(P)
- Grove - LCD RGB backlight v4
- Grove - Rotary Angle Sensor

Ability

- Redirect newly connect user to a Captive Portal
- There is a screen that can display some menu options, and select some actions.
- Attacker will have direct access to this information by simple operations after inserting a USB drive
- Phishing can be easily turned on/off.
- The screen changes colours through RGB cycling.
- Screen can be easily closed or opened with a switch

Functionalities introduction

menu

- **push button to turn on/off Phishing:**

  Fishing can be easily turned on and off, turn on/off Phishing will take about 30 seconds because Raspberry Pi needs to be restarted.

- **Num connecting:**

  View the total number of devices connected to this hotspot in real—time

- **Num zid received:**

  View the total number of Zid and passwords that have been received in real-time

- **Get data:**

  Insert the USB device into the USB port on the side, and push the button to use this option to write the obtained zid and password to the USB device. If the USB device cannot be written or the USB device is not detected, the screen will display "no device", if The number of zid and password that have been obtained is 0, the screen will display "No data", if the writing is successful, it will display "success", data.txt and data.json will be written to the USB device, and the USB device will be ejected safely.

- **Clear Acquired Data:**

  Delete all zid and password that have been acquired, The screen displays "success" if the cleanup is successful, and "error, no data" if there is currently no data

- **poweroff ? :**

  Basic function, shutdown

File introduction

- **frist_time_setup.py:**

  For first time setup, install hostapd, dnsmasq and lighttpd, and add main.py to boot, also turn on the phishing

- **hardware.py:**

  For reading sensor data, like button, knob, switch.

- **helper.py:**

  Some helper functions, including running command line commands and writing to rc.local

- **main.py:**

  The main file for this project, the implementation of the menu and also the use of multithreading to run the backend of the Login page.

- **phase_out_wifi.py:**

  Turn off phishing by changing all changed files to what they were before and reboot.

- **rgbscreen.py:**

  Control the color and text displayed on the screen.

- **server.py:**

  The backend of the login page to accepts the submitted table by the frontend and stores the data.

- **setup_wifi.py:**

  Enabling fishing is the core of the entire project. Change the settings of interfaces, hostapd, dnsmasq and lighttpd to enable fishing. The function of each step is mentioned in the comments of this file.

- **wifi_connect_detile.py:**

  Get the current number of device connected this hot spot, the currently number of acquired zid and password, and the current phishing status.

What I learned

(I never learned about phishing and the Raspberry Pi before, Actually, I bought Raspberry Pi at the beginning of this semester.)

- Basic understanding on Rospberry Pi.
- Basic understanding on Phsihing WIFI/Hotspot.
- Operations of Rospberry Pi.
- Practices into Embedded Programming.
- Fundemental Principal of Online Phising.

Reference

File: rgbscreen.py

grovepi official github library

https://github.com/DexterInd/GrovePi/blob/master/Software/Python/grove_rgb_lcd/grove_rgb_lcd.py