Anleitung zum Raspi-CyberSec-Lab

Jonas Schmitt

28. April 2025

1 Allgemeine Informationen

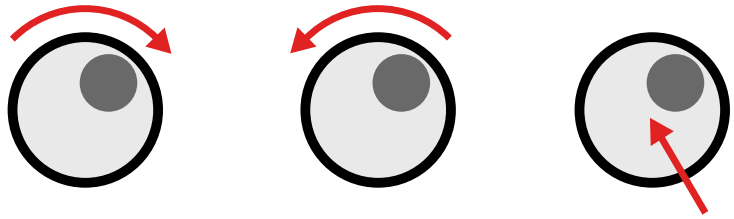
Das RaspberryPI Cybersecurity Lab (RCSL) ist eine Platform zum Testen verschiedener Cyberangriffe, das Projekt ist Teil meiner Bachelorarbeit in Elektro- und Informationstechnik an der Technischen Hochschule Nürnberg. Es hat verschiedene Funktionen um Umgebungen zu schaffen, welche für das Ausprobieren von Angriffen aus den Bereichen Wifi Netzwerke, Webseiten / -applikationen, MQTT Kommunikation und Bluetooth ausgelegt sind.

2 Benutzeranleitung

Zum Einschalten des Geräts, schließen Sie das Gerät mit dem zugehörigen Netzteil an den Strom an. Das Gerät fährt nun hoch, wobei der Bootvorgang zu sehen ist (das RaspberryPI Logo wird angezeigt). Nach erfolgreichem Bootvorgang wird das Hauptmenü angezeigt.

2.1 Navigation

Zur Navigation wird das Drehrad, wie in folgender Abbildung beschrieben, genutzt:



nach unten **nach oben** **bestätigen**

Die farbige Hinterlegung zeigt an, welcher Menüpunkt aktuell ausgewählt ist. Mit dem Drücken des Knopfes wird die Auswahl bestätigt und das Untermenü geöffnet, bzw die Aktion ausgeführt.
Zum verlassen eines Menüs wird die Option "back"gewählt.

2.2 Menü Übersicht

Dem Nutzer steht der folgende Menübaum zu Verfügung:

- **wifi** - Optionen zu Wifi Netzwerken
  - **activate** - Aktivieren eines Hotspots
    Auswahl der Netzwerkart
  - **deactivate** - Abschalten des aktiven Hotspots
  - **status** - Anzeigen der aktuellen Netzwerkeinstellungen
  - **change password** - Setzen eines neuen Passworts
    Auswahl der zu änderenden Netzwerkart
  - **monitoring** - Einschalten und Anzeigen des Netzwerkmonitoring
    on - Einschalten
    off - Ausschalten
    show log - Log anzeigen
    delete log - Log löschen
- **bluetooth** - Optionen zu Bluetooth
- **webapp** - Optionen zu Webapplikationen
  - **Juice Shop**
    on - Server Einschalten
    off - Server Ausschalten
  - **MQTT**
    on - MQTT Konversation starten
    off - MQTT Konversation beenden
- **development** - Anpassbare Optionen für Entwickler
- **power off** - Ausschalten des Geräts

3 Installation

Das Projekt wurde mit folgender Hardware umgesetzt:

- RaspberryPI 4B mit 8GB RAM
- Fenvi AX1800 USB Netzwerkkarte
- Waveshare ESP32c6 Microcontroller
- Waveshare 4.3 zoll LCD
- Drehgeber mit Druckknopf

Als Betriebssystem des RaspberryPI dient RaspberryPI OS in der light Version (nur Kommandozeile). Zum Kompilieren und Flashen des ESP32 Codes wird das ESP-IDF benötigt, dieses kann in Visual Studio Code als Erweiterung installiert werden.

Zuerst muss das Github Repository des Projekts auf den RaspberryPI geklont werden, dies kann mit folgendem Kommando erfolgen:

```
git clone https://github.com/Der-Erzfeind/Raspi-CyberSec-Lab-Project.git
```

Es wird empfohlen das Repository in das standardmäßige Nutzerverzeichnis zu klonen. Folgende Aktionen müssen im Anschluss ausgeführt werden:

- Kompilieren von main.cpp, encoder.cpp und mqtt.cpp
- Alle Skripte ausführbar machen
- Installation und Konfiguration von Mosquitto
- Installation des JuiceShops (und node.js)
- Einrichten des systemd services zum Ausführen von start.sh beim Start des Geräts
- Kompilieren und Flashen des ESP32 Codes

4 Entwicklung

Das RCSL öffnet nach dem Bootvorgang einen Hotspot, der für den Aufbau einer SSH Verbindung, wie folgend, genutzt werden kann:

1. Mit dem Hotspot verbinden,
   SSID: RPI
   Passwort: CyberSec
2. SSH Verbindung aufbauen mit **`ssh pi@10.40.0.1`**
   Passwort: admin

Im Nutzerverzeichnich befinden sich die Ordner mit den Daten zum Projekt und dem Juice Shop. In der Datei */Raspi-CyberSec-Lab-Project/Skripte/devMenu.sh* können die Entwicklungsfunktionen, welche im Menü "development"verfügbar sind, angepasst werden.