PwnPower

WORKSHOP

Offensive Appliances

PwnPower Workshop

Introduction

Welcome to the PwnPower Workshop! Today, we will transform smart wall plugs into Wifi hacking implant by:

- learning UART operations with microcontrollers
- Connecting to MCUs via UART pads
- Flashing new firmware to ESP32-based hardware

Equipment

- Smart Wall outlet
- ESP32-C3 microcontroller with unprotected UART

PwnPower Workshop

Capabilities

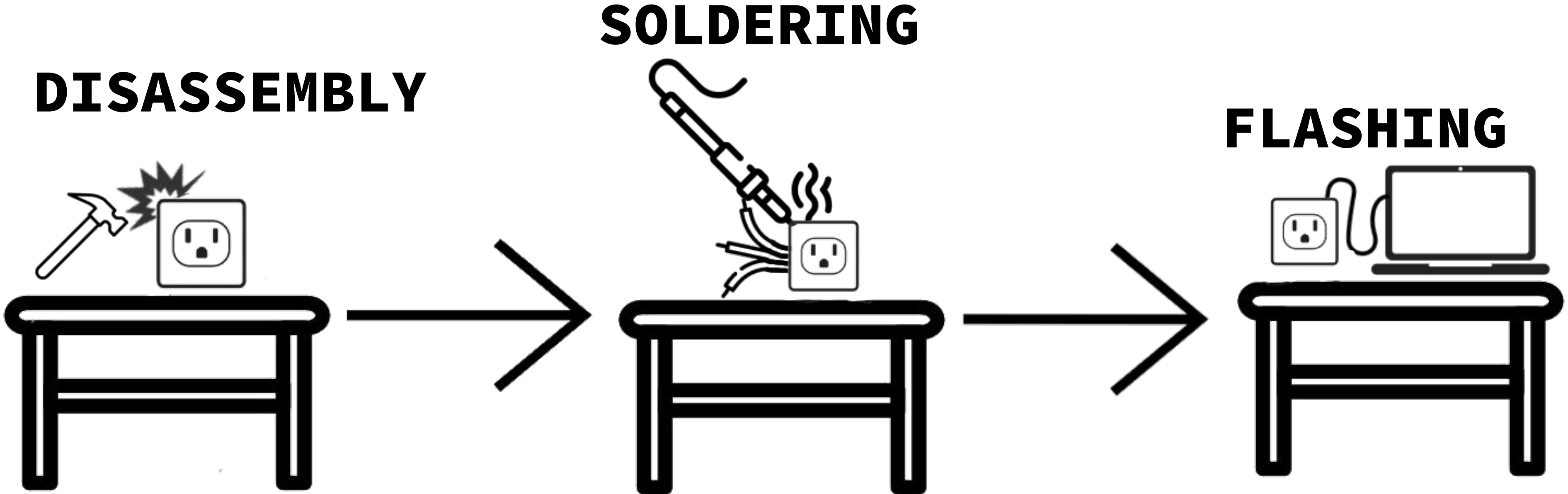
The new firmware features Wi-Fi Pentesting cabilies while also maintaining the functionality of the smart plug itself. This firmware features tools such as,

- Deauthentication
- Packet Capturing
- WPA/PMKID handshake capturing

How this works.

Overview

This workshop has been set up to run in different stages, each station for each step for the workshop.



DISASSEMBLY

SOLDERING

FLASHING

Station 1 (DISASSEMBLY)

Overview

1. Disablembe plastic housing.
2. Remove PCB from plastic housing.
3. Locate main PCB.
4. Remove ESP-C3 chip from main PCB.

Station 2 (Soldering/Wiring)

Overview

1. Add a small amount of solder to exposed pads.
2. Prepare wires for soldering.
3. Solder wires to exposed pads.
4. Create a small jumper to connect wires.

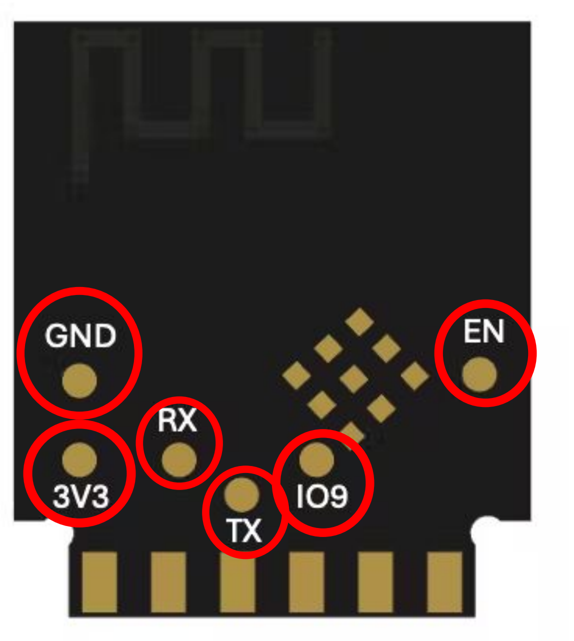
Station 2 (Soldering/Wiring)

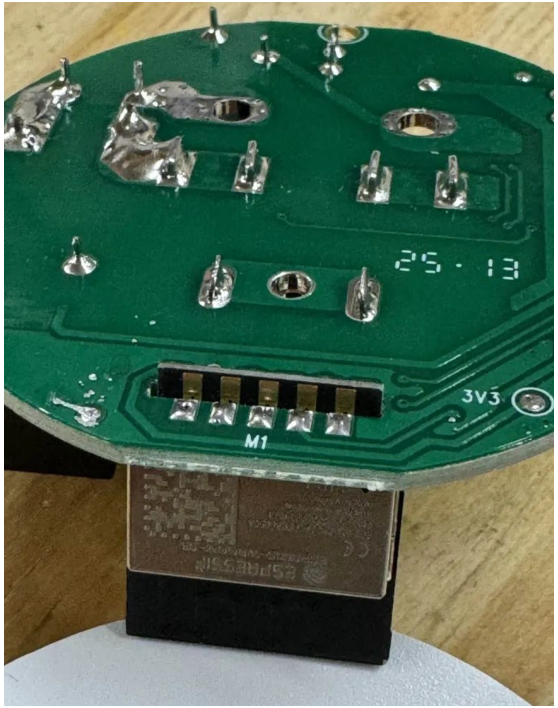
Extend – ESP32C3

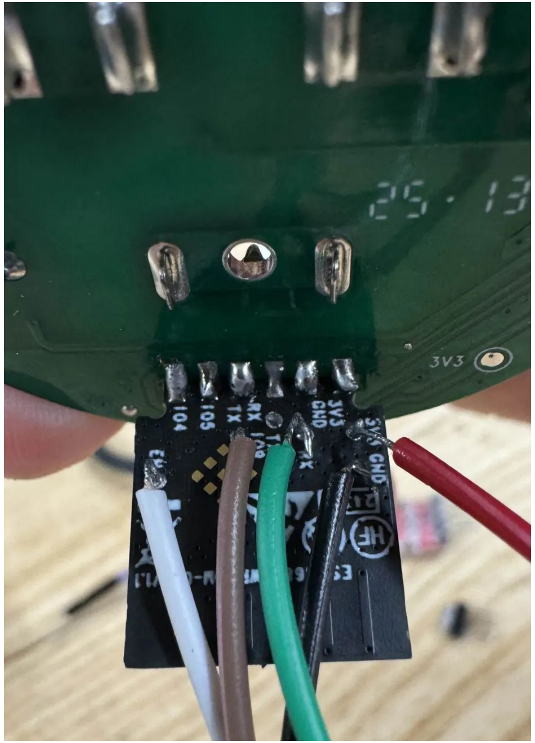
1. Ensure UART Connection
2. Flash new firmware
3. Remove jumper wire
4. Insert into main board ensuring pads align

Station 2 (Soldering/Wiring)

Extended







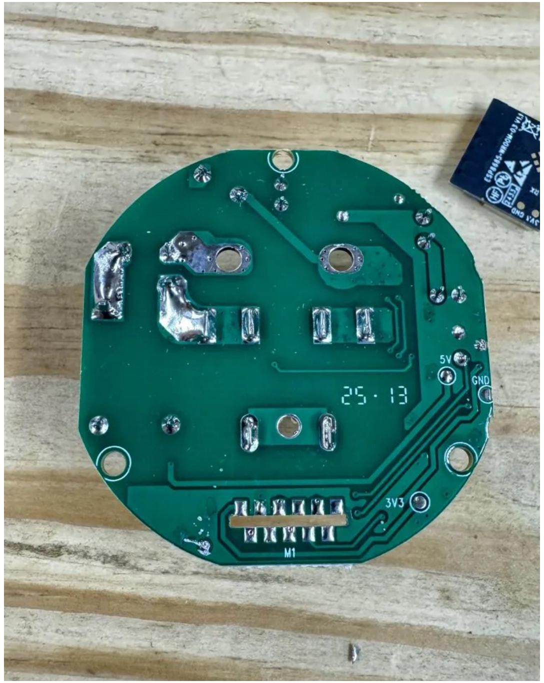
Station 2 (Soldering/Wiring)

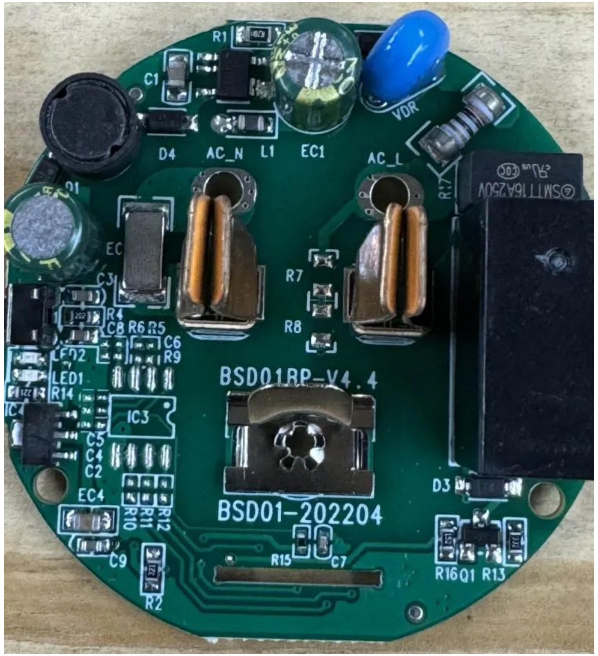
Extend - Main Board

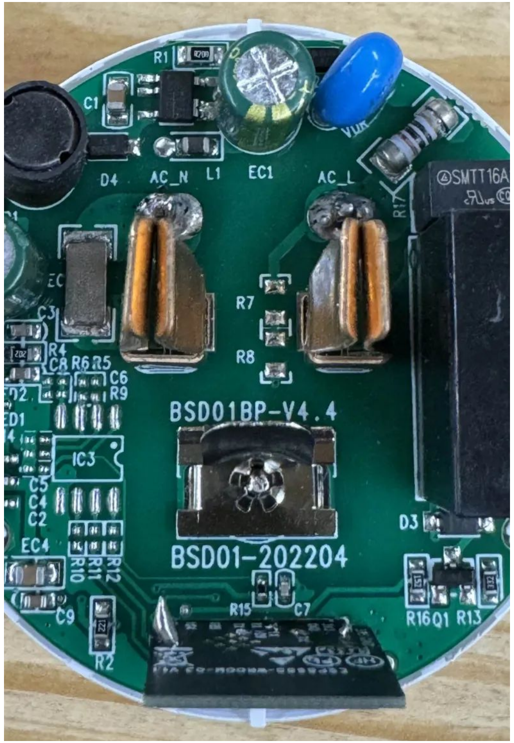
1. Solder ESP32-C3 to pads on main board
2. Insert 3 Prong mains connector
3. Solder Pins through main board

Station 2 (Soldering/Wiring)

Extended







Station 3 (Flashing)

Wiring

Ensure that your wiring is correct,

the 3.3v bridge should have the extra wire connected to 3.3v on the UART

the GND bridge should have the extra wire connected to GND on the UART

TX should be connected to RX and RX should be connected to TX

MORE INFO

https://github.com/hak5peaks/PENDING

FIRMWARE STILL IN PROGRESS

Instagram: omg.peaks
Github: Hak5peaks
Tiktok: Hak5peaks
Discord: Hak5peaks

Offensive Appliances