Hardware

CC5325 - Taller de Hacking Competitivo
Diego Vargas

Contenidos

- Introducción a Hardware
- Reversing de *firmware*
- Comunicación serial
- Logic 1 y 2

Introducción a Hardware

¿Qué son los problemas de Hardware?

- No es Hardware Hacking
- No se necesita hardware especial

- Análisis de *firmware*
- Decodificación de comunicación serial e inalámbrica
- Explotación de vulnerabilidades de hardware

Aplicaciones Prácticas

Las técnicas que veremos aquí son aplicables a ciertos casos de Hardware Hacking. Un uso común es forzar una comunicación serial con el dispositivo, mediante una interfaz expuesta, para hacer un dump del *firmware*, y así encontrar vulnerabilidades.

Reversing de *firmware*

¿Qué es el *firmware*?

Wikipedia

> El firmware o soporte lógico inalterable es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. [...] En resumen, un firmware es un software que maneja físicamente al hardware.

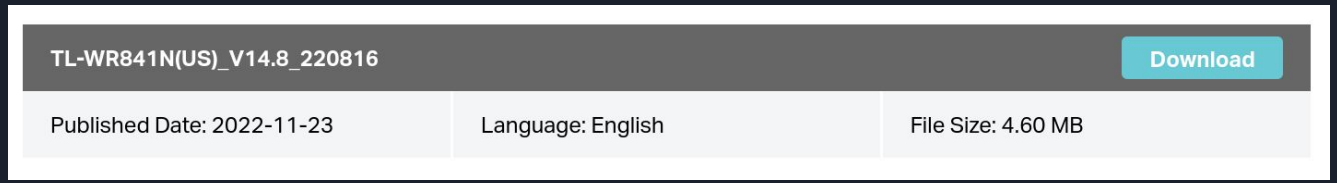
Ejemplos de *firmware*

- **BIOS**: Basic Input Output System
- **UEFI**: Unified Extensible Firmware Interface
- Open Firmware
- U-Boot/SquashFS

Caso de Estudio

Analizaremos el *firmware* de un router de TP-Link

https://www.tp-link.com/us/home-networking/wifi-router/tl-wr841n/

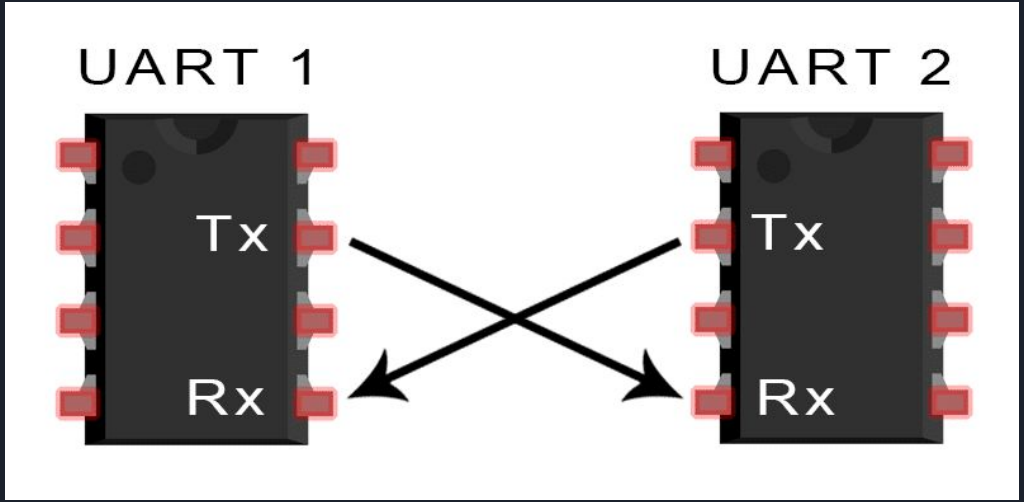


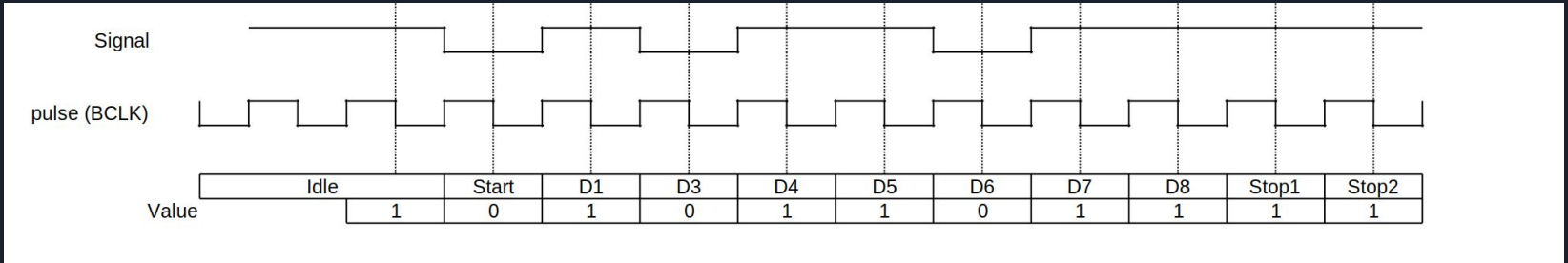
Comunicación Serial

Protocolos de Comunicación Serial

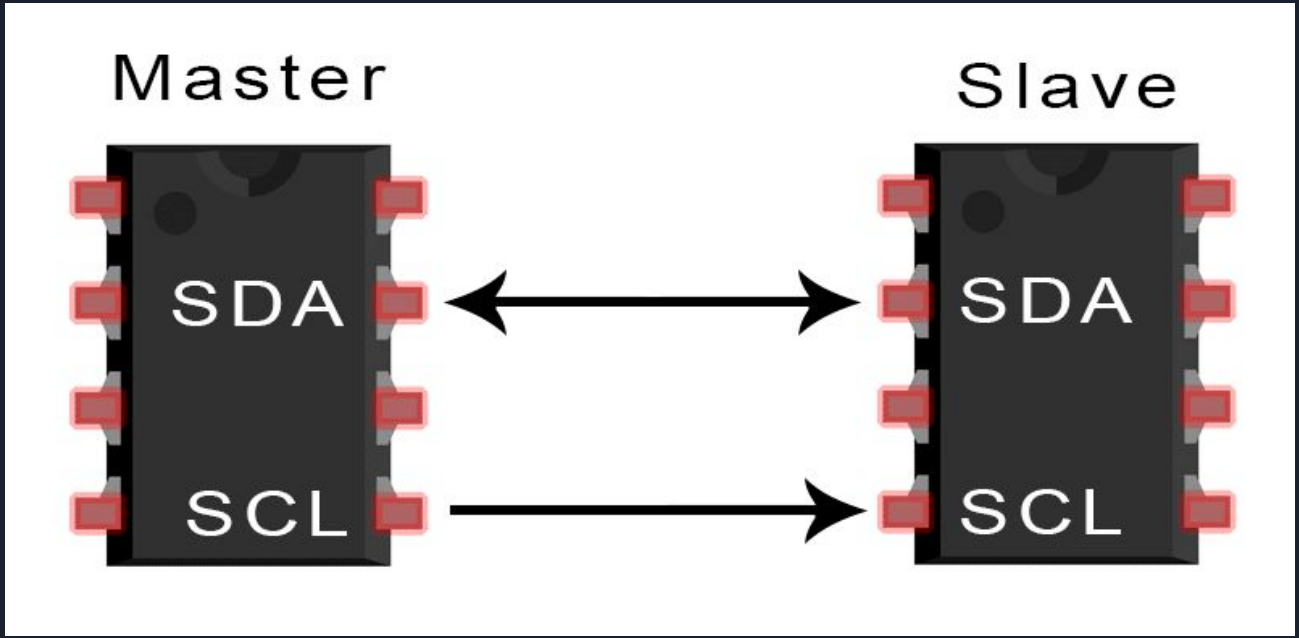
- UART: *Universal Asynchronous Receiver Transmitter*
- I2C: *Inter-Integrated Circuit*
- SPI: *Serial Peripheral Interface*

UART

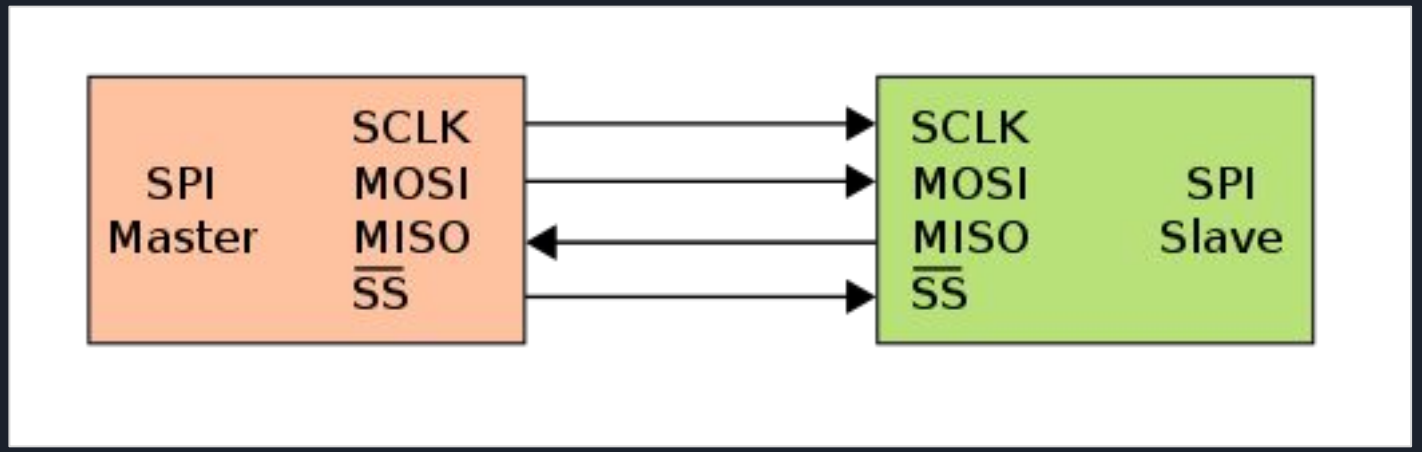

UART 1
UART 2
Tx
Rx
Tx
Rx


Signal
pulse (BCLK)
Idle
Start
D1
D3
D4
D5
D6
D7
D8
Stop1
Stop2
Value
1
0
1
0
1
1
0
1
1
1
1

I2C



SPI



Logic 1 y 2

Saleae

- Logic 1: https://support.saleae.com/logic-software/legacy-software/older-software-releases

- Logic 2: https://www.saleae.com/downloads/