

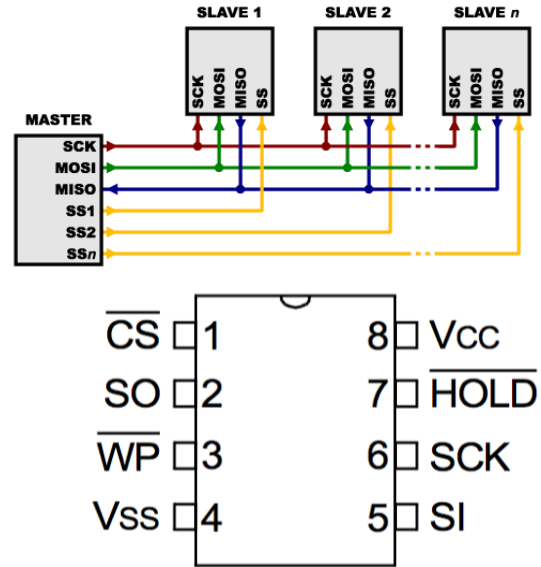
Attacking Hardware

SPI

Introduction to SPI Protocol

SPI Protocol

- It stands for serial peripheral interface.
- Developed by Motorola
- Four wire Synchronous Protocol
 - MOSI (Master Output, Slave Input),
 - MISO (Master Input, Slave Output)
 - SS/CS (Slave Select/Chip Select)
 - SCLK (Serial Clock).
 - It's faster than asynchronous serial.
 - CS line decides which device to communicate with.



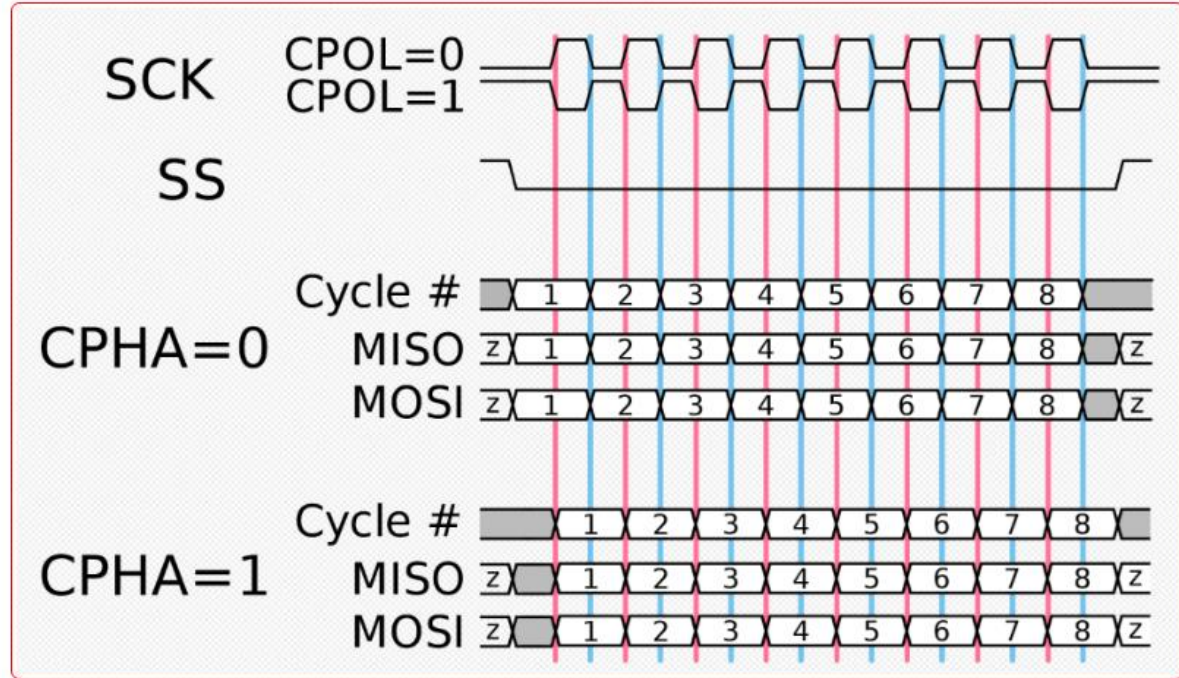
SPI Protocol

- Full-duplex
- Master slave architecture
- Single master multiple slaves
- Modes of SPI - Mode 0, Mode 1, Mode 2, Mode 3

SPI Modes	Clock Polarity (CPOL/CKP)	Clock Phase (CPHA/CKE)
Mode 0	0	0
Mode 1	0	1
Mode 2	1	0
Mode 3	1	1

Source - Wikipedia

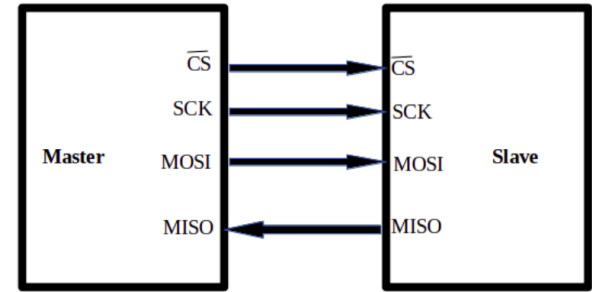
SPI Protocol



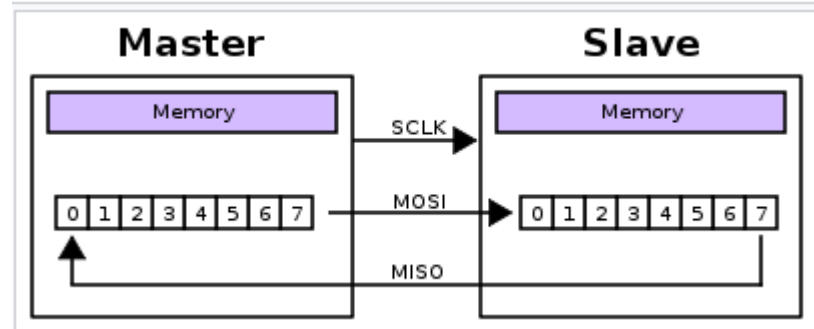
Source - Wikipedia

SPI Protocol

- Master selects the slave device
- Master sends the clock signal
- Master sends the data/command on the MOSI line
- Slave sends the data/response on the MISO line



Source - Wikipedia



SPI - Possible Attacks

- Signal sniffing
- Signal tampering
- Data extraction
- Data manipulation

SPI - Tools/Framework

- EXPLIoT Nano - <https://explot.io/products/explot-nano>
- Bus Pirate - http://dangerousprototypes.com/docs/Bus_Pirate
- Shikra - <https://int3.cc/products/the-shikra>
- CH341A - <https://www.onetransistor.eu/2017/08/ch341a-mini-programmer-schematic.html>
- EXPLIoT Framework - https://gitlab.com/explot_framework/explot
- Flashrom - <https://github.com/flashrom/flashrom>
- Pyspiflash - <https://github.com/eblot/pyspiflash>
- Logic Analyzer
- RaspberryPi or Beaglebone can also be used.

Labs

Read and Write – for 25lc256

- Chip Datasheet:
 - <course-dir>/labs/device-spi-lab-1

FIGURE 2-1: READ SEQUENCE

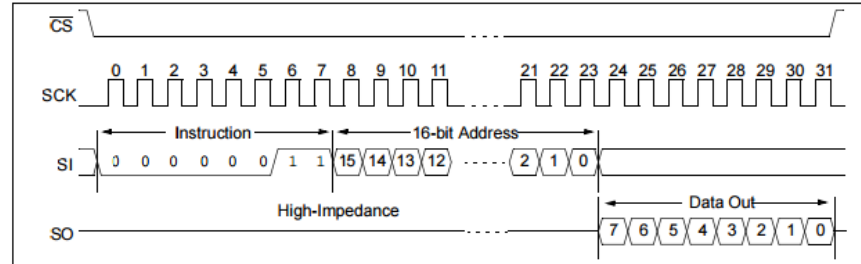
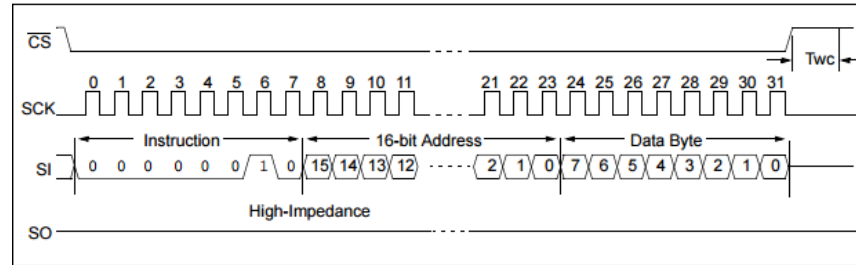


FIGURE 2-2: BYTE WRITE SEQUENCE



Lab 1 – SPI chip recon

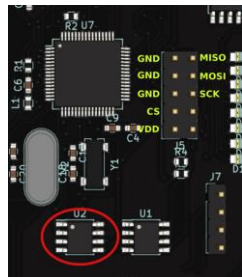
- Objective: To perform reconnaissance on Microchip 25LC256 EEPROM using datasheet
- Location: <course-dir>/labs/device-spi-lab-1
 - Datasheet can be found in this directory
- Steps
 - Identify the size
 - Identify the clock frequency
 - Identify the Pin specifications
 - Identify Clock polarity and phase (CPOL and CPHA)
 - Identify SPI Read/Write/Write enable commands



© Premier Farnell
Copying of image is prohibited

SPI Lab 2 – SPI communication sniffing to bypass authentication

- Objective: SPI communication sniffing using Logic analyzer to
- The DIVA board has two memory chips
- The circled one is SPI memory
- It's a dual in-line package (DIP)
- Connect the board using the USB wire
- Connect the saleae logic analysers pins with MOSI ,MISO and SCK on the board. Gnd of saleae logic analyser will go to Gnd of DIVA.
- Connect the board using the USB wire
- Open your serial monitor with baud rate 9600



SPI Lab 2

- On the Logic software, click on analysers and set as SPI with correct channel, click on the double arrow and set speed as 24MS/s
- Click on Start and go back to the serial monitor
- Press 3 (for SPI challenge) and a random password
- Go back to logic software and click on stop



SPI Lab 2

```
diva>3
Welcome to SPI sniffing Lab

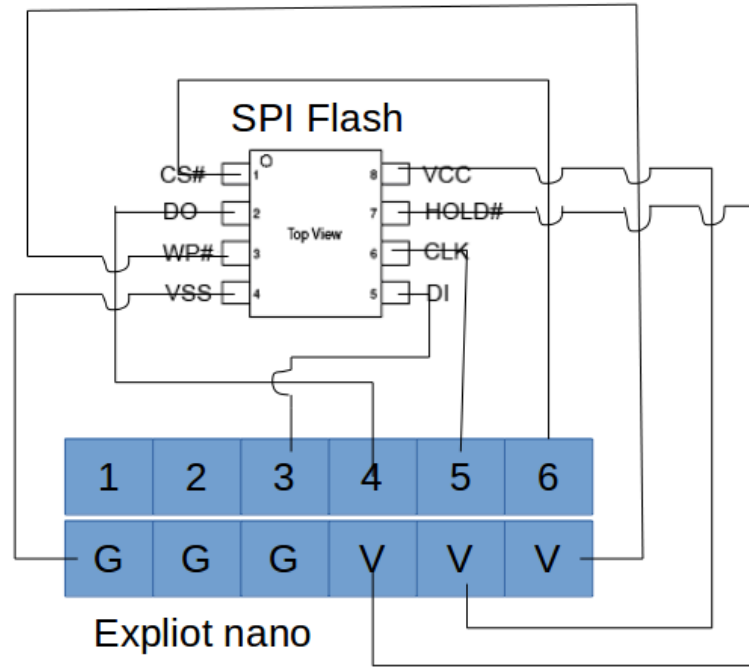
In this Lab you will sniff a SPI transaction

Please login
Enter the password
diva>>*****
Access Denied :(
diva>
```

SPI Lab 3 – Dumping SPI Flash memory

- ObjectiveL To use Expiot nano to extract the firmware from an Flash memory
 - STEPS:
 - SOIC Package is soldered into a adapter
 - Connect the expiot nano to the spi flash memory as shown in the next slide
 - Use flashrom to dump the content of the flash memory.
- “flashrom -p ft2232_spi:type=2232H -c MX25L6405 -r /tmp/camera_dump.bin “

SPI Lab 3



References

<https://www.elprocus.com/communication-protocols/>

<http://www.i2c-bus.org/repeated-start-condition/>

<http://www.i2c-bus.org/i2c-primer/how-i2c-hardware-works/>

<https://electricimp.com/docs/resources/spi/>

<https://learn.sparkfun.com/tutorials/serial-peripheral-interface-spi>

The End