Sunday, 24 March 2019

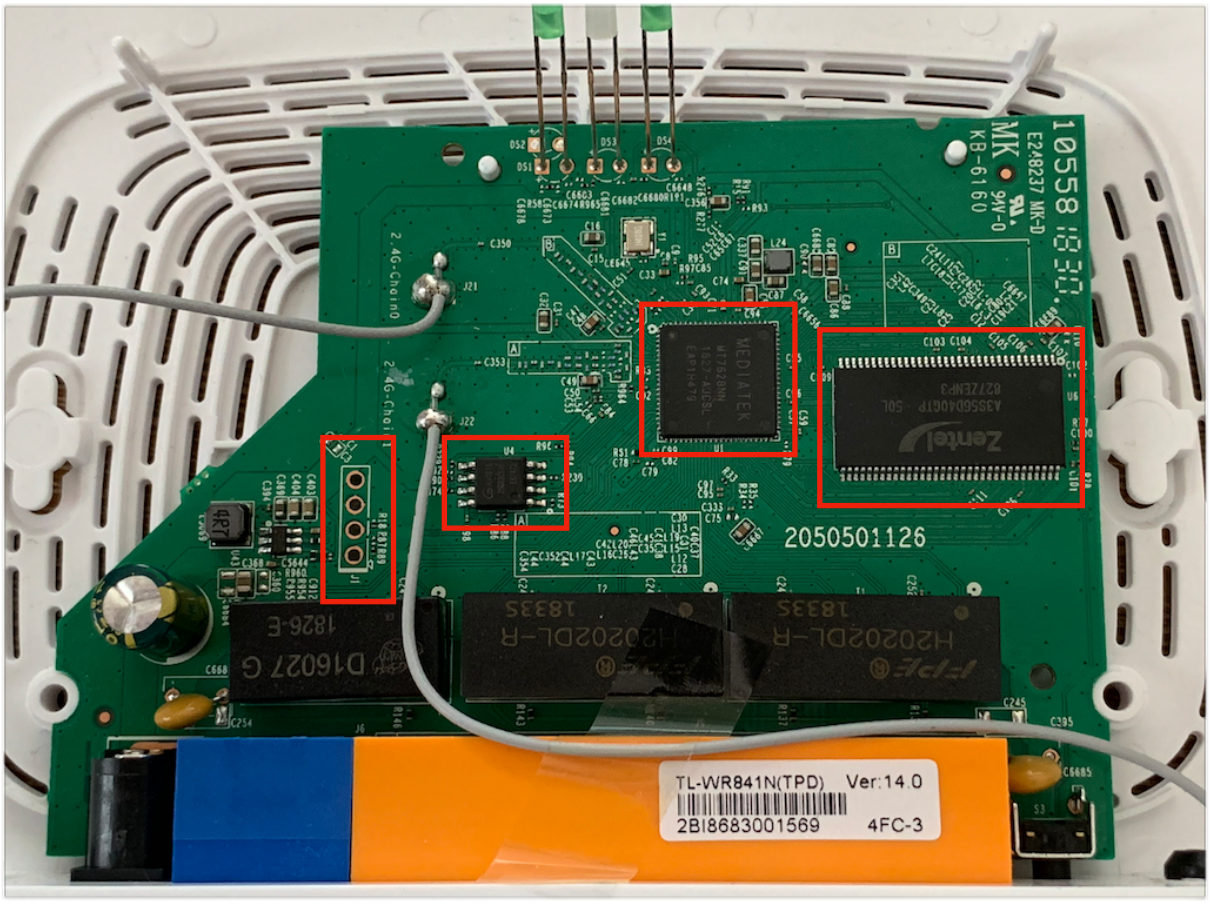
Hardware Hacking 101

BSides Munich 2019 Workshop

Exercise 1 - Inspect the Router

One fo the initial reconnaissance activity for hardware hacking is the visual inspection of the PCB. It helps to understand how the hardware was designed, what components are used and how they communicate with each other. In this exercise the task is to identify core components of the target router TP-Link TL-WR841N v14.

Task 1 - The picture below presents PCB of TP-Link TL-WR841N. Name the components in circle and try to identify the models of them.



Component #	Name	Vendor	Purpose
1			
2			
3			
4			

Exercise 2 - UART

This exercises is about connecting to the target's UART port and see if we get any data.

Task 1 - Identify pins of the UART

Pin #	Label (Rx, Tx, Vcc, GND)	Hydrabus #	How did you identify the UART label?
1			
2			
3			
4			

Task 2 - Connect target device to Hydrabus and configure UART settings

Config parameter	Value	How did you identify this value?
Device: (UART1 / UART2)		
Speed:		
Parity:		
Stop bits:		

Task 3 - Read entire boot log to a file and identify interesting information.

Question	Answer
Which Bootloader and version is used?	
What is the kernel version?	
What is the partition type?	
How many partitions are configured?	
What are addresses for each of the partitions?	
On which memory address is MAC stored and which partition is it?	
What is the MAC address value?	
Where is SSH password stored?	

Task 4 - At this stage you should have some access to the device.

Can you identify the admin password for the SSH connection?

Were you able to login to the device over the SSH?

Exercise 3 - NOR Flash dumping

Task 1 - Connect Hydrabus to NOR Flash

What is the NOR Flash series number:

What is the Voltage value:

! Be careful to use proper voltage level !

Pin #	SPI Symbol	Hydrabus Pin
1		
2		
3		
4		
5		
6		
7		
8		

Task 2 - Ensure that you connected the Hydrabus properly by reading the readID of the NOR Flash and reading some data.

Question	Answer
What is the SPI readID command?	
What is the the readID value?	
What is the hydrabus command to readID?	
What are the first 8 bytes of data in the address 0x3F0000	

Task 3 - At this point, the connection to the NOR Flash works and we are ready to dump entire firmware. Use a script dump_flash.py in a course folder to dump data. Be careful, there is information missing in the beginning of the script that need to be set by you.

Note: It is required to reset the board via RESET button between attempts.

What is the MD5 checksum of the image:

Task 4 - Verify that the image has been properly dumped. Use binwalk tool to see if it recognises firmware structures and extract it.

What is the filesystem?
Did you manage to extract the filesystem?

Task 5 - Extract the configuration file

From the boot log recall the address where the config file is stored. Extract the config file with dd.

What is the WPA2 WiFi password:
Can you connect to the WiFi network with that password?

What is the admin password:
Can you connect to the router web with that password?

Exercise 4 - NAND Flash

Task 1 - Find the datasheet for your NAND Flash chip.

Task 2 - In the folder NAND/Logic there are 3 pictures of the Logic Analyser capture of some NAND commands and outputs. Using datasheet for the NAND Flash chip try to understand what is the communication.

Task 3 - Connect Hydrabus to the NAND Flash using either the NAND adapter or HydraFlash.

Task 4 - Use DumpFlash utility to dump the NAND Flash firmware. (https://github.com/hydrabus/DumpFlash-Hydrabus)

Task 5 - Try to write to NAND chip. You can use read_write_nand.py as a template and a starting point.
