From Curiosity to Connectivity: Hacking into Wi-Fi Routers

IN CYBER FORUM
NORTH AMERICA

Using my Flipper Zero Friend !

Adrien Lasalle – Pentester

@alrikrr @adrien-lasalle @alrikrr

EN/FR

IN CYBER FORUM
NORTH AMERICA

SPEAKER

Adrien LASALLE

Pentester

Bradley & Rollins' Red Team

Personal Blog : alrikrr.github.io

- Github: @AlrikRr
- LinkedIn: @adrien-lasalle

Let's connect !

CC ISC2 | TCM SECURITY CERTIFIED Practical Network Penetration Tester PNPT | eJPT | CERTIFIED RED TEAM SPECIALIST CRTS CYBERWARFARE LABS

@FICAmNord

@fic-north-america

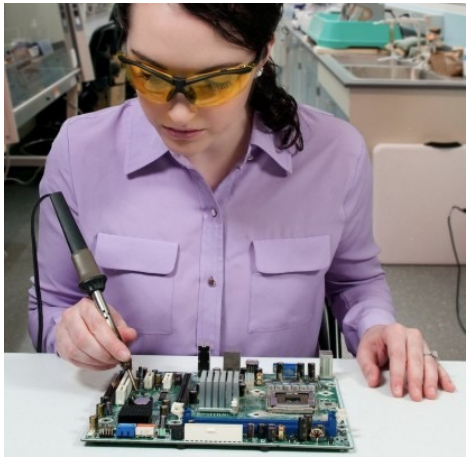
EN/FR

IN CYBER FORUM
NORTH AMERICA

Disclaimer 1

Disclaimer Electricity

Always be cautious when working with electricity and ensure you follow recommended safety protocols. Mishandling electricity can be hazardous, and it's crucial to prioritize safety at all times. Take necessary precautions so you won't damage yourself or the device you are using.



IN CYBER FORUM
NORTH AMERICA

Disclaimer 2

Disclaimer Hardware Hacking

Hardware hacking is a subject often mired in controversy and legal complexities. In many instances, tampering with a device's hardware without the owner's explicit consent is considered unlawful. Such actions like opening the device to alter its components and manipulating firmware or BIOS settings.
There are instances where hardware hacking is not only permissible but actively endorsed with the help of bug bounty programs established by many manufacturers. These programs incentivize individuals to discover and disclose vulnerabilities in their products, offering rewards for their efforts.

AGENDA

1. How it started ?
2. Hardware Hacking - Basic
3. UART
4. Let's Jump !
5. Flipper Zero
6. Setup Your Lab
7. Looking for Goodies

IN CYBER FORUM
NORTH AMERICA

IN CYBER FORUM
NORTH AMERICA

How it started ?

IN CYBER FORUM
NORTH AMERICA

Wandering on

Flashback Team

@FlashbackTeam 55 k abonnés 10 vidéos

We are a group of hackers who find and exploit vulnerabilities in hardware ...

twitter.com/FlashbackPwn et 1 autre lien

@FICAmNord

@fic-north-america

EN/FR

IN CYBER FORUM

NORTH AMERICA

Hardware Hacking - Basic

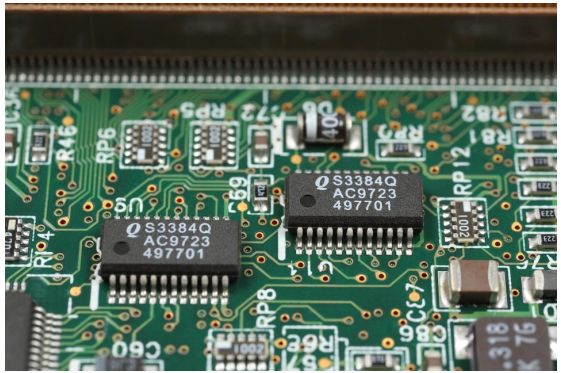
Adrien Lasalle - 2023

IN CYBER FORUM
NORTH AMERICA

Security you said ?

Challenges for embedded devices:

- Physical access == Game Over
- Lack of updates
- Cheap Components
- Battery & Encryption
- No Hardware Updates



@FICAmNord

@fic-north-america

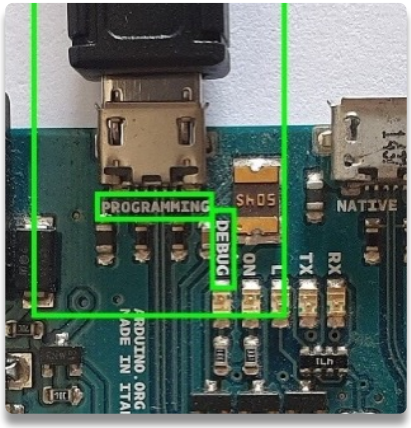
EN/FR

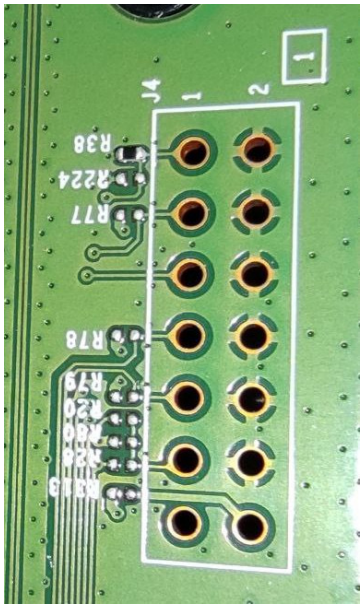
IN CYBER FORUM
NORTH AMERICA

Debug ports

Challenges

- Used for debugging during development process
- Most of the time left without “protection”
- Easy to recognize
- Root shell most of the time





EN/FR

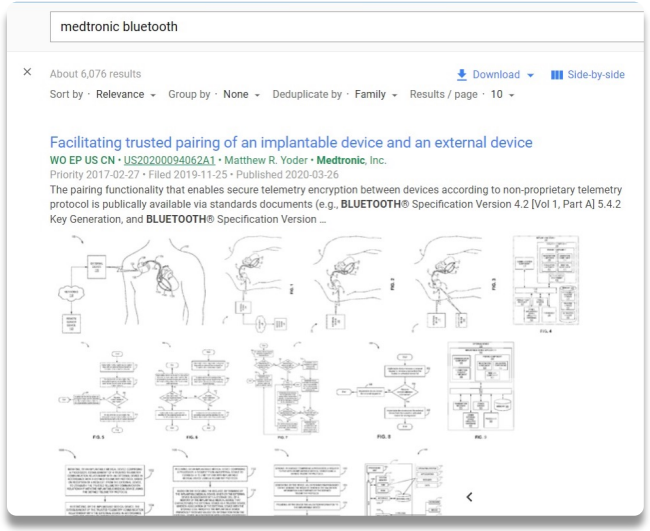
@FICAmNord

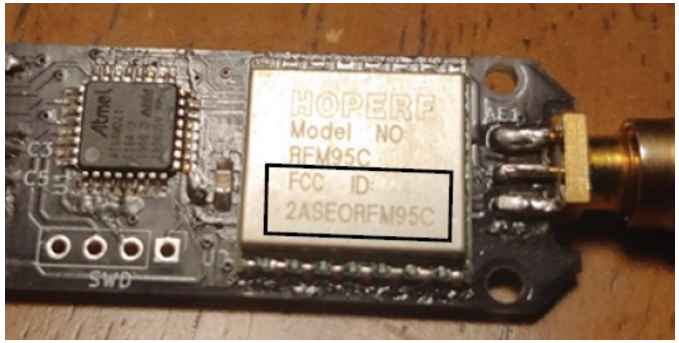
@fic-north-america

IN CYBER FORUM
NORTH AMERICA

Vulnerability Research

Some Tips
- Google Dorking
- FCC ID
- Online documentation
- Customer Reviews
- OSINT on Dev Team





LinkedIn

EN/FR

@FICAmNord
@fic-north-america

IN CYBER FORUM

NORTH AMERICA

UART

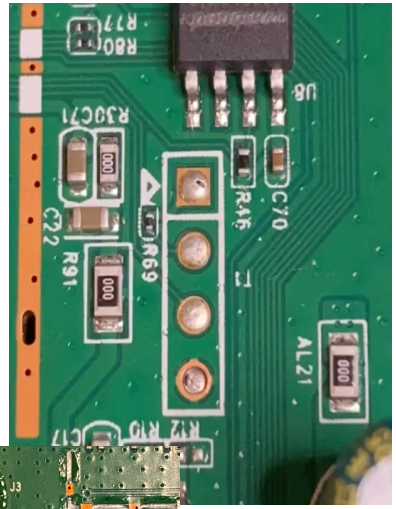
Adrien Lasalle - 2023

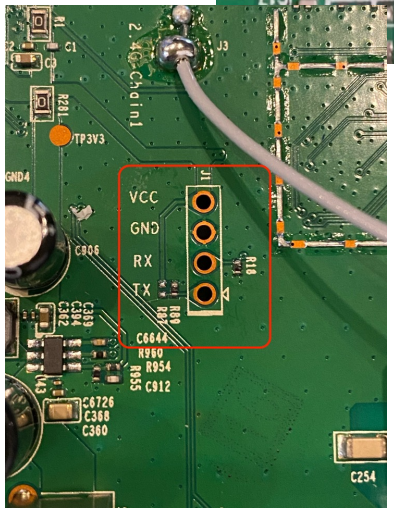
IN CYBER FORUM
NORTH AMERICA

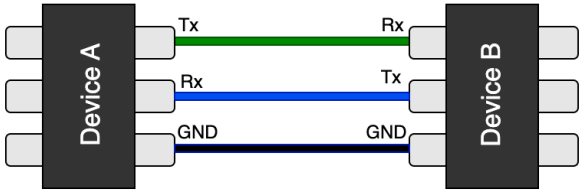
Wiki & 4 PINs

How to recognize UART ?
- 4 Pins next to each others
- Text indicators sometimes
- Already solder pin if you are very lucky

What are the PINS ?
- VCC which is the voltage of the device (3.3 or 5 v)
- GND which is the ground
- RX which is the pin that receive data
- TX which is the pin that send data







@FICAmNord
@fic-north-america

EN/FR

IN CYBER FORUM
NORTH AMERICA

Baudrate

Baudrate can be understood as the transmission speed of the device. There is a certain standard, and the most crucial aspect is to find the right one to accurately translate the bytes sent and received by the UART protocol.

Transmission speed				Real transmission speed	
Bauds	Bit/s	Bit duration	Speed	Speed	Byte duration
50 Bd	50 bits/s	20.000 ms	6.25 bytes/s	5 bytes/s	200.000 ms
75 Bd	75 bits/s	13.333 ms	9.375 bytes/s	7.5 bytes/s	133.333 ms
110 Bd	110 bits/s	9.091 ms	13.75 bytes/s	11 bytes/s	90.909 ms
134 Bd	134 bits/s	7.463 ms	16.75 bytes/s	13.4 bytes/s	74.627 ms
150 Bd	150 bits/s	6.667 ms	18.75 bytes/s	15 bytes/s	66.667 ms
200 Bd	200 bits/s	5.000 ms	25 bytes/s	20 bytes/s	50.000 ms
300 Bd	300 bits/s	3.333 ms	37.5 bytes/s	30 bytes/s	33.333 ms
600 Bd	600 bits/s	1.667 ms	75 bytes/s	60 bytes/s	16.667 ms
1200 Bd	1200 bits/s	833.333 µs	150 bytes/s	120 bytes/s	8.333 ms
1800 Bd	1800 bits/s	555.556 µs	225 bytes/s	180 bytes/s	5.556 ms
2400 Bd	2400 bits/s	416.667 µs	300 bytes/s	240 bytes/s	4.167 ms
4800 Bd	4800 bits/s	208.333 µs	600 bytes/s	480 bytes/s	2.083 ms
9600 Bd	**9600 bits/s**	**104.167 µs**	**1200 bytes/s**	**960 bytes/s**	**1.042 ms**
19200 Bd	19200 bits/s	52.083 µs	2400 bytes/s	1920 bytes/s	520.833 µs
28800 Bd	28800 bits/s	34.722 µs	3600 bytes/s	2880 bytes/s	347.222 µs
38400 Bd	38400 bits/s	26.042 µs	4800 bytes/s	3840 bytes/s	260.417 µs
57600 Bd	57600 bits/s	17.361 µs	7200 bytes/s	5760 bytes/s	173.611 µs
76800 Bd	76800 bits/s	13.021 µs	9600 bytes/s	7680 bytes/s	130.208 µs
115200 Bd	**115200 bits/s**	**8.681 µs**	**14400 bytes/s**	**11520 bytes/s**	**86.806 µs**
230400 Bd	230400 bits/s	4.340 µs	28800 bytes/s	23040 bytes/s	43.403 µs
460800 Bd	460800 bits/s	2.170 µs	57600 bytes/s	46080 bytes/s	21.701 µs
576000 Bd	576000 bits/s	1.736 µs	72000 bytes/s	57600 bytes/s	17.361 µs
921600 Bd	921600 bits/s	1.085 µs	115200 bytes/s	92160 bytes/s	10.851 µs

Source: https://lucidar.me/

IN CYBER FORUM
NORTH AMERICA

Finding the PINS

GND
- Continuity mode with multimeter

IN CYBER FORUM
NORTH AMERICA

Finding the PINS

VCC
- Power the device and check 3.3v or 5v without cuts

Tx
- Power the device and check 3.3v or 5v variation due to boot messages

IN CYBER FORUM

NORTH AMERICA

Let's jump, what do I need ?

IN CYBER FORUM
NORTH AMERICA

Find the good device

Device Information
- TP-Link AC750 (End of Life)
- Model Archer C20
- Wi-Fi 2.4GHz and 5GHz

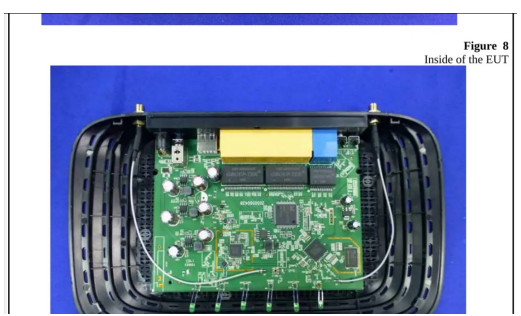


Figure 8
Inside of the EUT

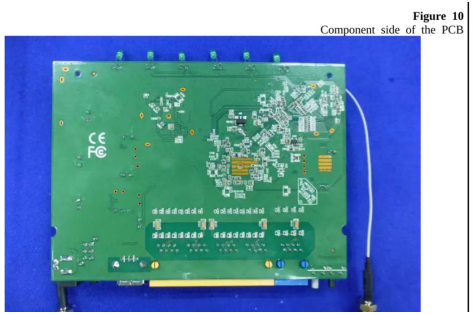


Figure 10
Component side of the PCB

https://fccid.io/TE7C2/Internal-Photos/C2-Int-Photo-2296493

EN/FR

IN CYBER FORUM
NORTH AMERICA

Basic Tools

@FICAmNord

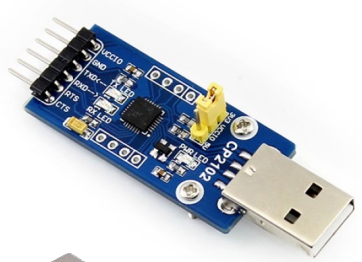
@fic-north-america

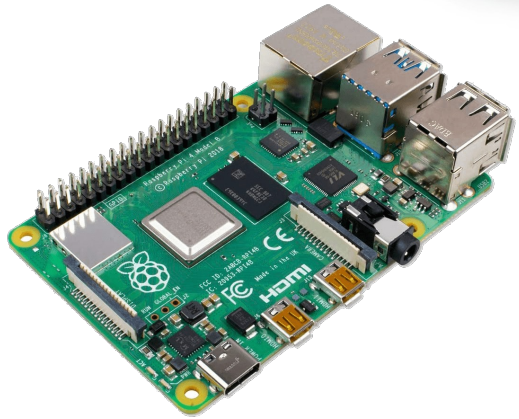
EN/FR

IN CYBER FORUM
NORTH AMERICA

USB to UART Bridge

- USB to UART
- Raspberry Pi (Don’t forget edit config.txt)
- Flipper Zero GPIO Menu





IN CYBER FORUM

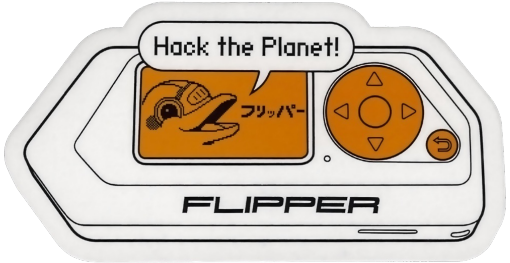
NORTH AMERICA

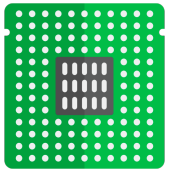
Flipper Zero Presentation

Adrien Lasalle - 2023

IN CYBER FORUM
NORTH AMERICA

Flipper Zero





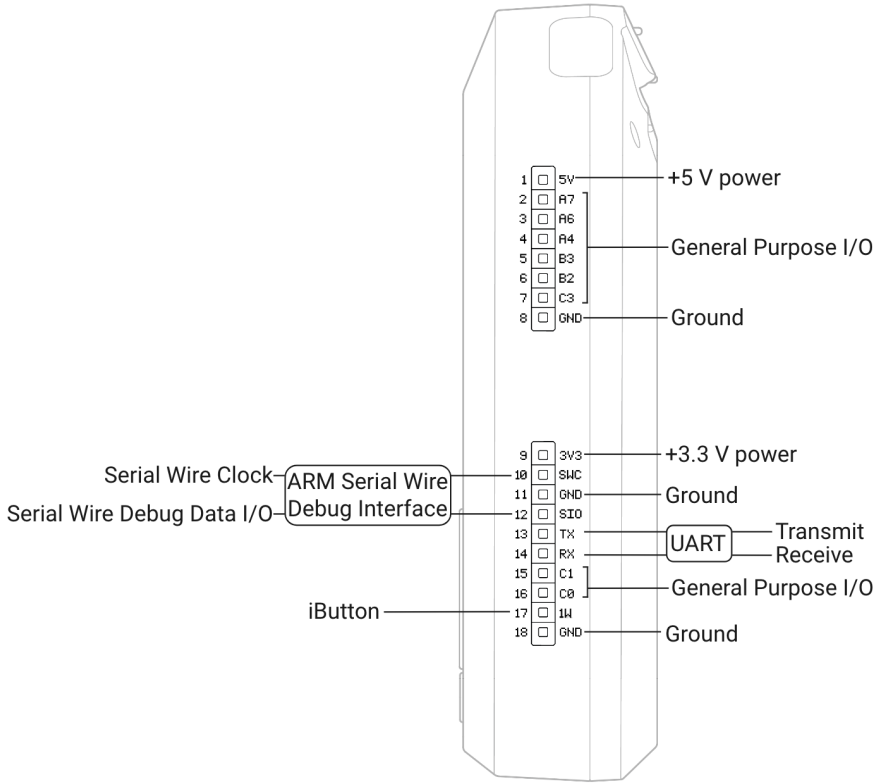
@FICAmNord

@fic-north-america

EN/FR

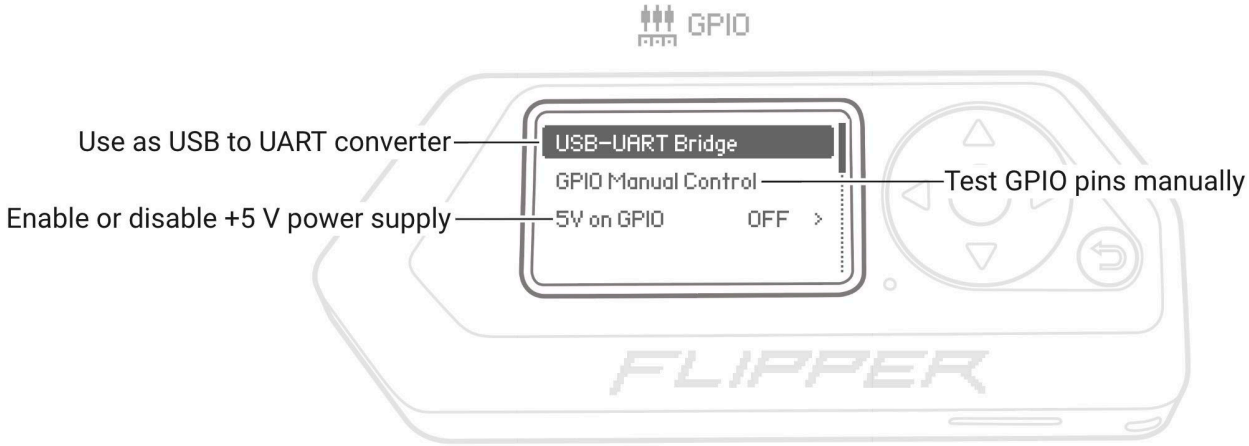
IN CYBER FORUM
NORTH AMERICA

Flipper Zero



IN CYBER FORUM
NORTH AMERICA

Flipper Zero



IN CYBER FORUM

NORTH AMERICA

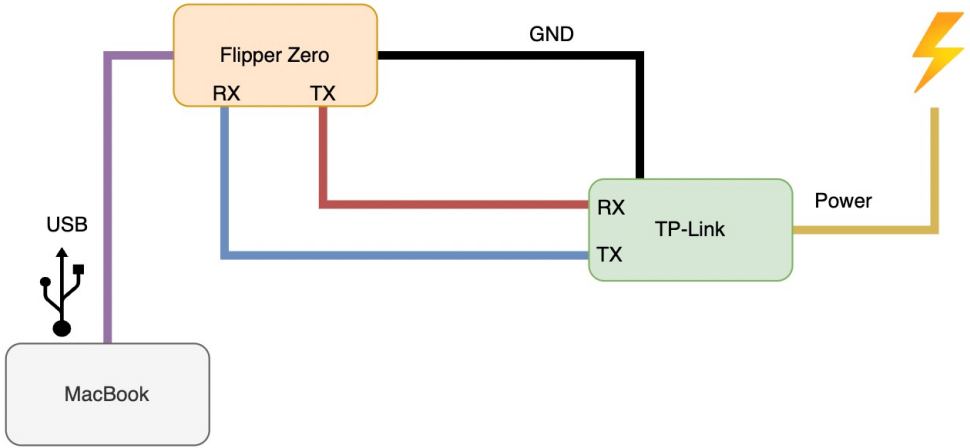
Setup your Lab

IN CYBER FORUM
NORTH AMERICA

Plug the right PINS

Flipper Zero Pin Number

- Tx 13
- Rx 14
- GND 11 or 18

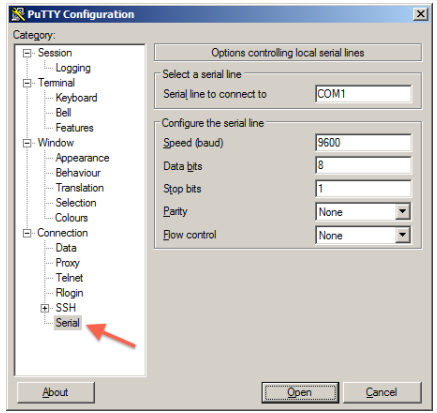


IN CYBER FORUM
NORTH AMERICA

Install the tools

```
brew install tio
```

```
sudo apt install tio
```



PuTTY

IN CYBER FORUM

NORTH AMERICA

Find the Baudrate

@FICAmNord

@fic-north-america

EN/FR

IN CYBER FORUM

NORTH AMERICA

Find the Baudrate

@FICAmNord

@fic-north-america

EN/FR

IN CYBER FORUM

NORTH AMERICA

Boot !

@FICAmNord

@fic-north-america

EN/FR

IN CYBER FORUM

NORTH AMERICA

Looking for goodies

Adrien Lasalle - 2023

IN CYBER FORUM
NORTH AMERICA

Read-Only

- Limited Binary Set
- Can’t edit configuration files
- Can’t upload new binaries

```
~ # echo 0 > test
/bin/sh: can't create test: Read-only file system
```

```
~ # ls bin
umount   sed      ping6    netstat  ls       grep     df       chmod    ash
sleep    rm       ping     mount    login    echo     date     cat
sh       ps       pidof    mkdir    kill     dmesg    cp       busybox
~ # ls sbin
vconfig         rmmod           mii_mgr_cl45    insmod          halt
switch          reboot          mii_mgr         init            getty
route           poweroff        lsmod           ifconfig        config-mii.sh
```

IN CYBER FORUM
NORTH AMERICA

Web Server Files

- Looking for vulnerability
- Understand how the web interface works
- No secrets ?

```
~ # ls web
qr.htm              js                  help                css
mainFrame.htm       index.htm           frame               MenuRpm.htm
main                img                 domain-redirect.htm
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
        "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<script language="javascript" type="text/javascript">var url=window.location.href;if(url.indexOf("tplinklogin.net
")>=0){url=url.replace("tplinklogin.net","tplinkwifi.net");window.location=url};</script>
<head>
        <link rel="Stylesheet" href="./css/main.css" type="text/css" />
        <script src="./js/language.js" type="text/javascript"></script>
        <script src="./js/oid_str.js" type="text/javascript"></script>
        <script src="./js/oid_str_coex.js" type="text/javascript"></script>
        <script src="./js/str.js" type="text/javascript"></script>
        <script src="./js/help.js" type="text/javascript"></script>
        <script src="./js/err.js" type="text/javascript"></script>
        <script src="./js/root.js" type="text/javascript"></script>
        <script src="./js/cryptoJS.min.js" type="text/javascript"></script>
        <script src="./js/encrypt.js" type="text/javascript"></script>
        <script src="./js/tpEncrypt.js" type="text/javascript"></script>
        <script src="./js/lib.js" type="text/javascript"></script>
        <link rel="Shortcut Icon" href="./img/login/favicon.ico" type="image/jpeg" />
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

        <meta http-equiv="cache-control" content="no-cache" />
</head>
```

IN CYBER FORUM
NORTH AMERICA

Admin Password

```
~ # cat /etc/passwd
admin:$1$$iC.dUsGpxNNJGeOm1dFio/:0:0:root:/:/bin/sh
dropbear:x:500:500:dropbear:/var/dropbear:/bin/sh
nobody:*:0:0:nobody:/:/bin/sh
```

```
→  VM-SHARED john passwd
Created directory: /home/adrien/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 ASIMD 4×2])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234             (admin)
1g 0:00:00:00 DONE 2/3 (2022-09-30 15:27) 3.030g/s 15845p/s 15845c/s 15845C/s 123456..green
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

@FICAmNord

@fic-north-america

EN/FR

IN CYBER FORUM
NORTH AMERICA

SSID Password

```
/var/Wireless/RT2860AP # cat RT2860AP.dat | grep "SSID"
NoForwardingBTNBSSID=0
SSID1=SecureNet
SSID2=TP-Link_Guest_E7FB
SSID3=
SSID4=
HideSSID=0;0;1;1
/var/Wireless/RT2860AP # cat RT2860AP.dat | grep "WPA"
AuthMode=WPA2PSK;OPEN
WPAPSK1=1234ABCD*
WPAPSK2=
WPAPSK3=
WPAPSK4=
ApCliWPAPSK=
```

Thank you !

Download the slides

- https://github.com/AlrikRr/Talks

References

- Check README.md

Bring your Flipper Zero at Bradley & Rollins (434)

for a Live Demo