SERMA
SAFETY & SECURITY

Le Hack Workshop
Capture the Drone

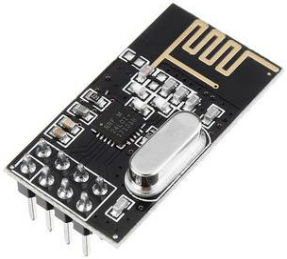
SECURE YOUR FUTURE

SOMMAIRE

INTRODUCTION

SECURE YOUR FUTURE

HARDSPLOIT

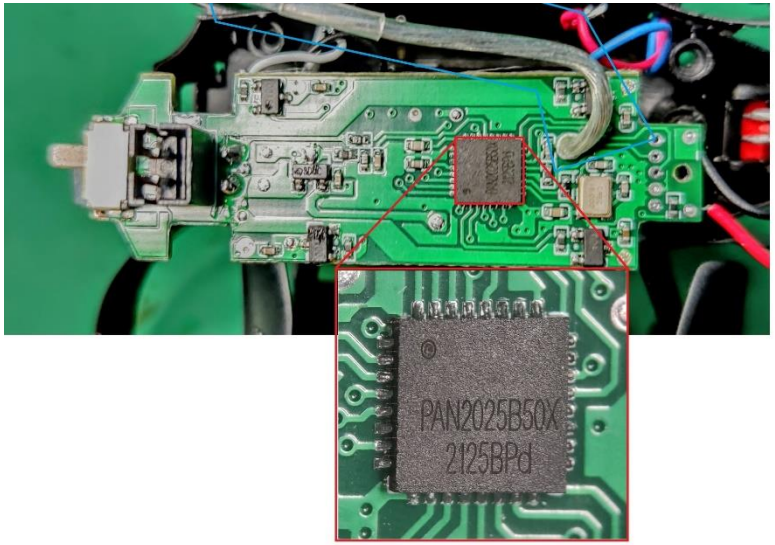


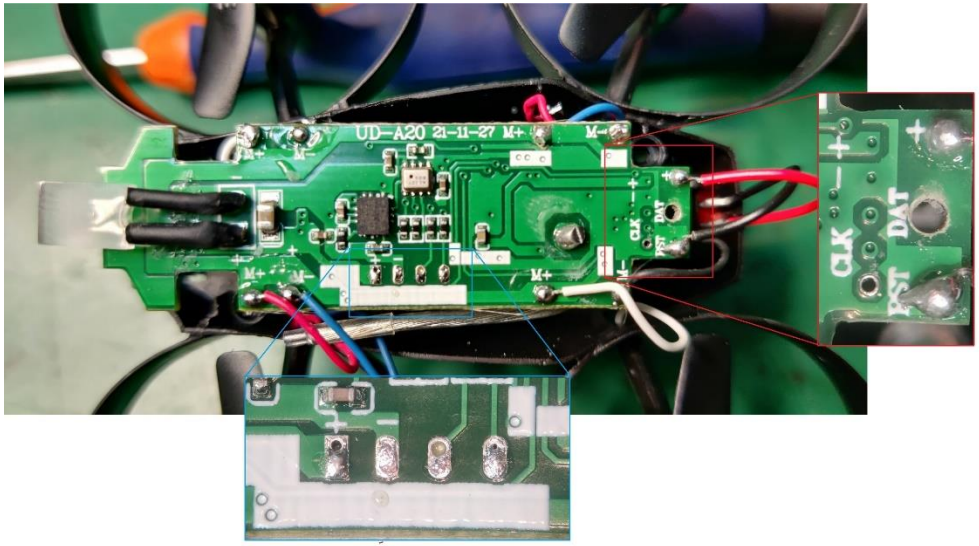
FINGERPRINTING

Where do we start ?

CHALLENGE 1 : What is the reference of the microchip of the drone and its architecture ?

CHALLENGE 2 : What communication/debug interfaces are present on the drone ?



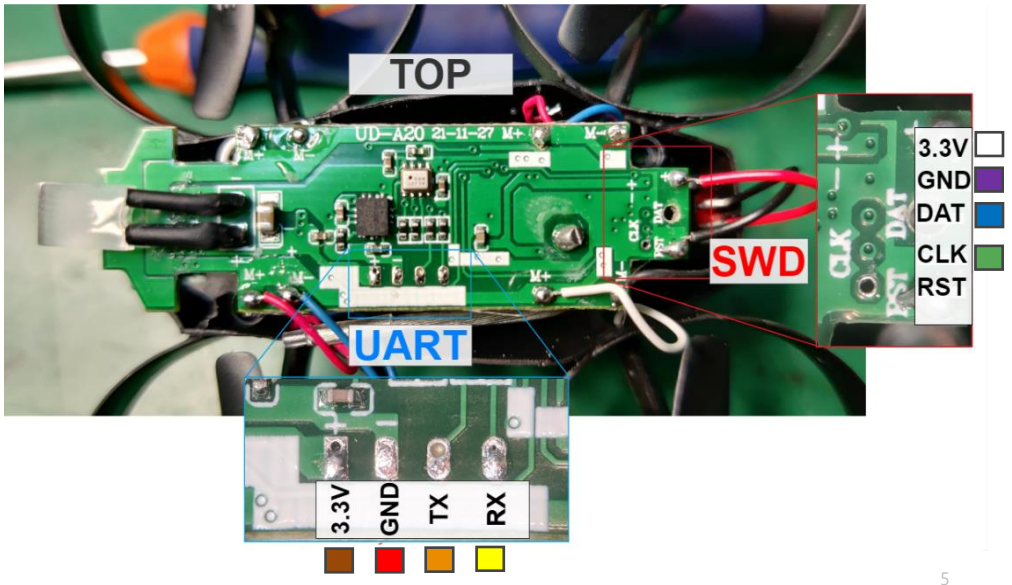


UART INTERFACE

CHALLENGE 3 : What information is leaking on UART?

GEAR

- Drone Potensic A20
- Logic analyser
- Logic 2

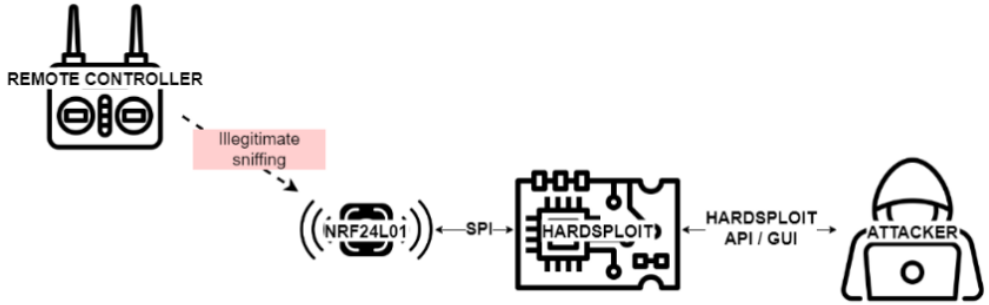


RADIO INTERFACE

CHALLENGE 4 : On which radio channels the remote is communicating ?

GEAR

- Hardsploit
- Hardsploit RF_tool_stud.py
- NRF24L01+



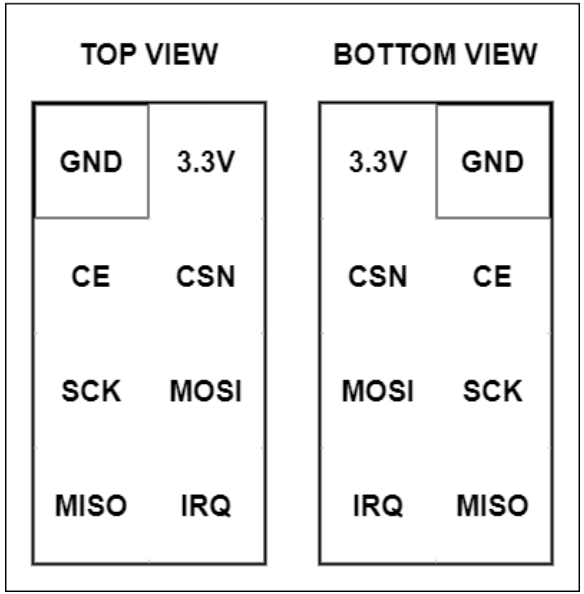
RADIO INTERFACE

CHALLENGE 4 : On which radio channels the remote is communicating ?

PINING

Hardsploit signal	Harsploit pin number	NRF signal
SPI_CLK	pin A0	SCK
SPI_CS	pin A1	CSN
SPI_MOSI	pin A2	MOSI
SPI_MISO	pin A3	MISO
SPI_PULSE	pin A4	CE

NRF24L01 pinout



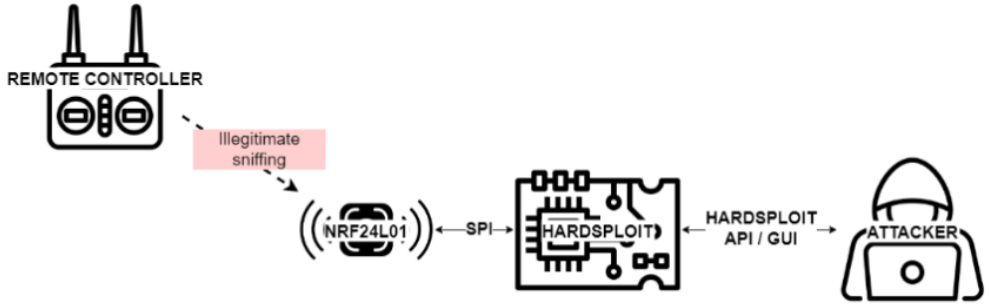
RADIO INTERFACE

CHALLENGE 5 : What is the address of trainer's controller?

CHALLENGE 6 : How does pairing work between the drone and the controller?

MATERIEL

- Hardsploit
- Hardsploit RF_tool_stud.py
- NRF24L01+

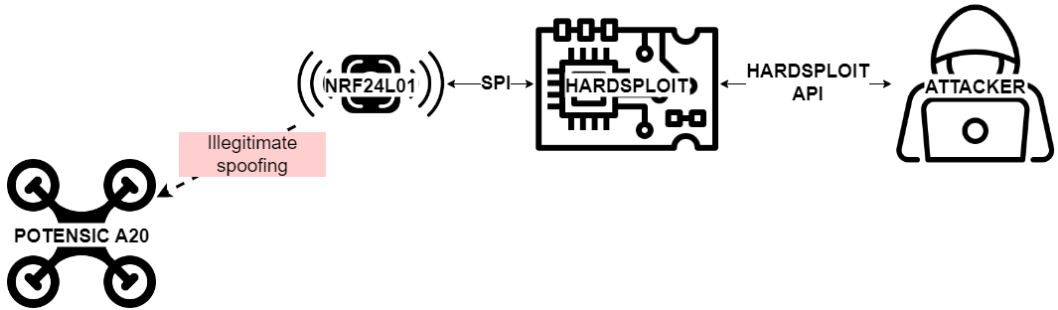


RADIO SPOOFING

CHALLENGE 7 : Find the take off command

GEAR

- Hardsploit
- Hardsploit RF_tool_stud.py
- NRF24L01+

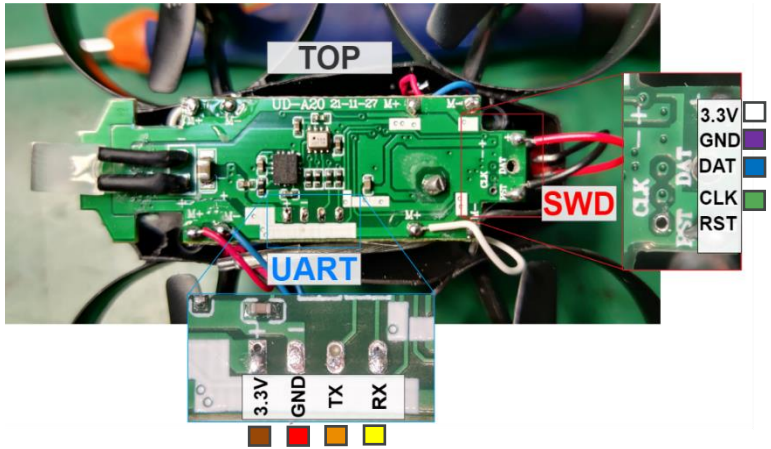


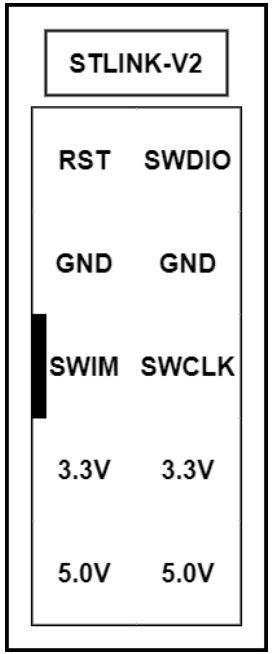
REVERSE & VULNERABILITY SEARCH

CHALLENGE 8 : Extract the firmware of the drone

MATERIEL

- Drone Potensic A20
- STLINK-V2
- OpenOCD





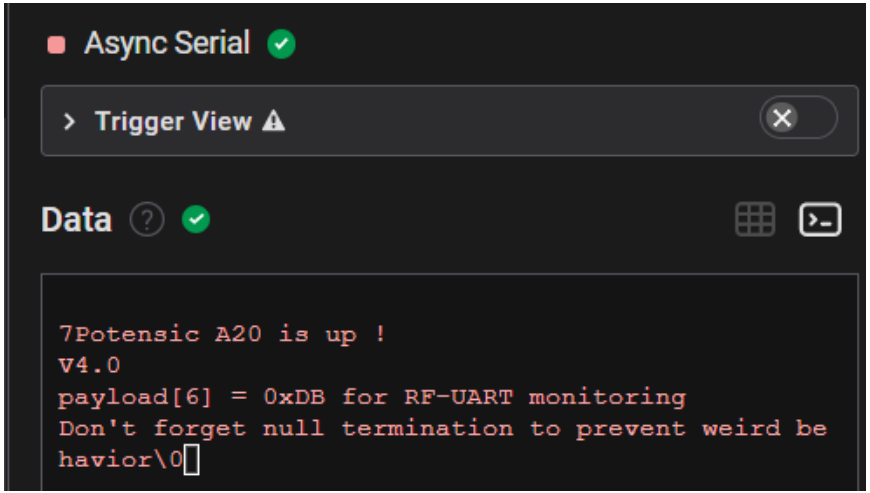
REVERSE & VULNERABILITY SEARCH

CHALLENGE 9 : Find the address of the RF-UART monitoring function

GEAR

- Drone firmware
- Ghidra
- **PAN2025B datasheet**

Several ways to do it (at least 3 !)



REVERSE & VULNERABILITY SEARCH

CHALLENGE 10 : Find the address of the vulnerable function

GEAR

- Drone firmware
- Ghidra

Think about the most classic vulnerability in C developpement

BUFFER OVERFLOW STUDY

CHALLENGE 11 : Find the address where the RF payload is first stored in RAM

CHALLENGE 12 : Find the address where the RF payload is copied in the stack

GEAR

- Potensic A20
- Hardsploit
- Hardsploit RF_tool_stud.py
- NRF24L01+
- STLINK-V2
- OpenOCD
- Gdb-multiarch

BUFFER OVERFLOW STUDY

CHALLENGE 13 : Find the address where the targeted Link Register is stored

GEAR

- Potensic A20
- Hardsploit
- Hardsploit RF_tool_stud.py
- NRF24L01+
- STLINK-V2
- OpenOCD
- Gdb-multiarch

BUFFER OVERFLOW STUDY

CHALLENGE 14 : Find the payload to perform a buffer overflow on the target function @0x6788

GEAR

- Potensic A20
- Hardsploit
- Hardsploit RF_tool_stud.py
- NRF24L01+
- STLINK-V2
- OpenOCD
- Gdb-multiarch

BUFFER OVERFLOW STUDY

CHALLENGE 15 : Manage to print “Expert overflow” on the UART

GEAR

- Potensic A20
- Hardsploit
- Hardsploit RF_tool_stud.py
- NRF24L01+
- STLINK-V2
- OpenOCD
- Gdb-multiarch
- Logic analyser
- Logic 2


THANK YOU &
HAPPY KACKING !!
SERMA
SAFETY & SECURITY

SERMA
SAFETY & SECURITY

14, rue Galilée
33600 PESSAC
05 57 26 08 88
contact-s3@serma.com

NATHALIE MONEY
DIRECTRICE COMMERCIALE
CYBERSÉCURITÉ & SAFETY
+33 (0)6 20 52 04 87
N.MONEY@SERMA.COM

FRANÇOIS-XAVIER DUPLA
RESPONSABLE COMMERCIAL
LABORATOIRE DE SÉCURITÉ
+33 (0)6 74 95 98 99
FX.DUPLA@SERMA.COM

LIONEL AGULHON
RESPONSABLE LABORATOIRE DE SÉCURITÉ
+33 (0)6 68 36 94 32
L.AGULHON@SERMA.COM

MICHEL DUFRESNE
RESPONSABLE SÛRETÉ DE FONCTIONNEMENT /
CYBERSÉCURITÉ INDUSTRIELLE ET EMBARQUÉE
+33 (0)6 72 77 59 06
M.DUFRESNE@SERMA.COM

SERVET IDRIZI
RESPONSABLE SOC/AUDIT TECHNIQUE
+33 (0)6 44 66 00 99
S.IDRIZI@SERMA.COM

SYLVAIN METAIS
RESPONSABLE INTÉGRATION / MATÉRIEL
+33 (0)6 98 28 27 62
S.METAIS@SERMA.COM

GEORGES HANNA
RESPONSABLE GOUVERNANCE RISQUE ET
CONFORMITÉ
+33 (0)6 21 52 86 65
G.HANNA@SERMA.COM

SERMA
GROUP