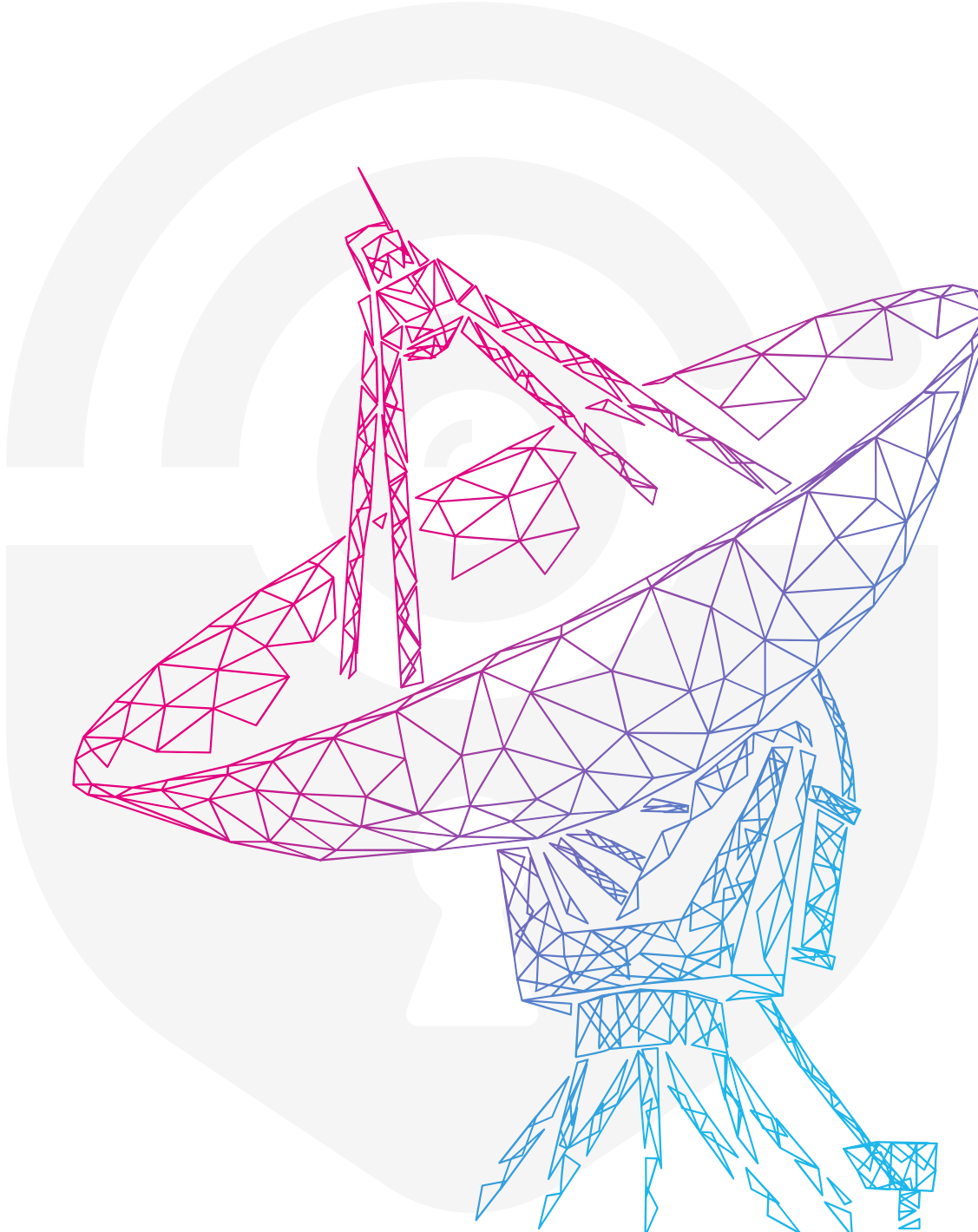
penthertz

Drones on the Air

Detecting, Reversing & Hijacking UAVs Over RF



Founder of Penthertz

- Sébastien Dudek (@FlUxIuS)
- CEO of Penthertz
  - Founded during COVID in 2020
  - Specialized in Wireless communications security
- > 15 years of experience in Software & Hardware security
  - Security researcher
  - Pentester & Red Team
  - Vulnerability researcher

Perfect mix to make Penthertz!

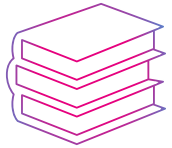


Main activities



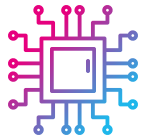
Security assessments

- Wireless communications (RFID, Wi-Fi, Mobile communication, Bluetooth, etc.)
- Embedded devices
- Backend servers
- Red Team



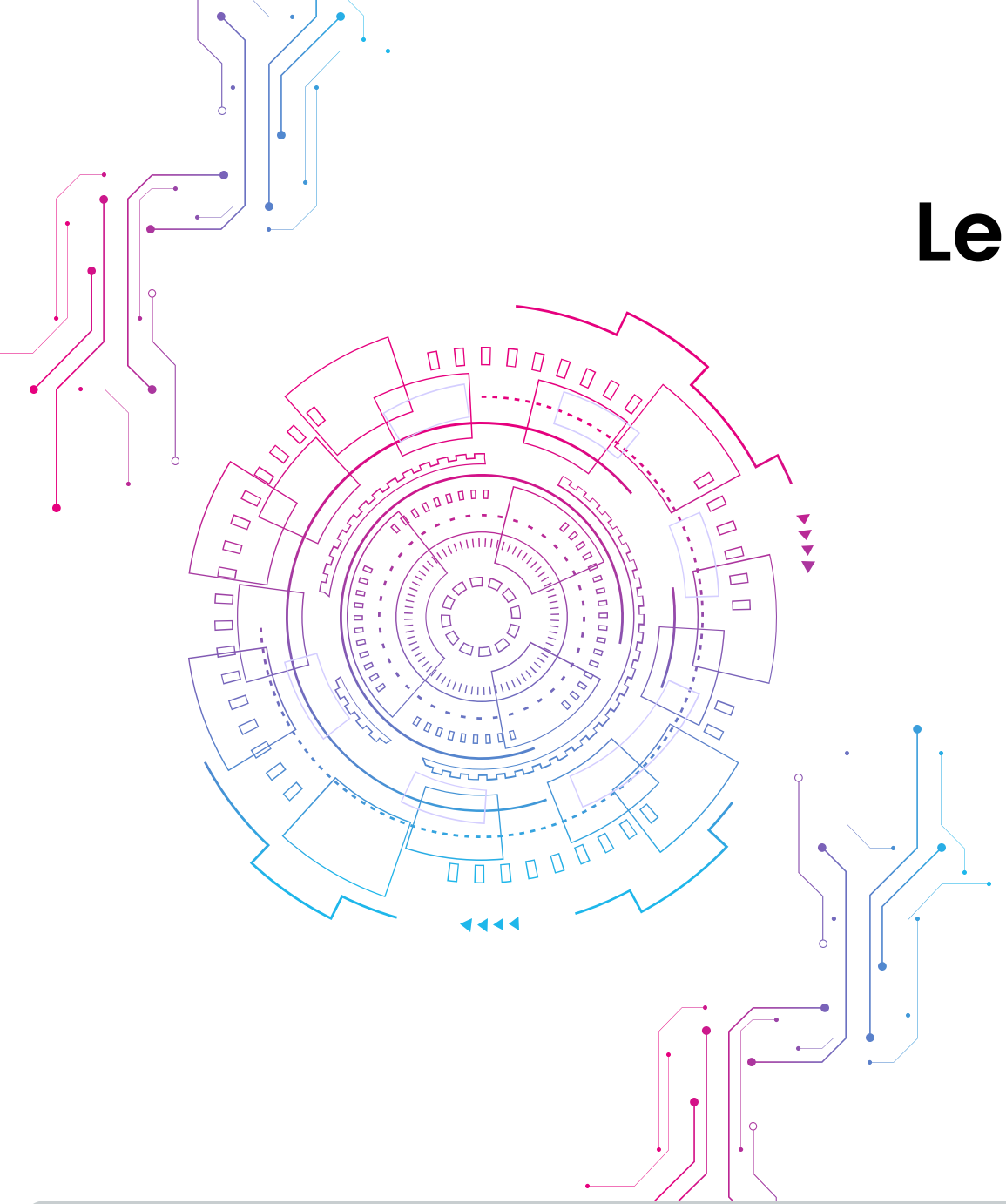
Trainings

- Software-Defined Radio Hacking
- Wi-Fi Red teaming
- RFID Hacking
- Mobile attacks (2G/3G/4G/5G)



Hardware security

- Firmware extraction
- Chip-off
- Secrets extraction
- Libraries analysis
- Vulnerability hunting



Let's talk about UAV drones

1. Context
2. Monitoring
3. Analysis
4. Attacks + Jamming
5. Forensics

Context

Drones



- 3 main domains related to our topic:

Domain	Accronyme	Example of civil, racins drones (non-exhaustive)	Military examples (non-exhaustive)
Air	UAV (Unmanned Aerial Vehicle) / UAS (Unmanned Aircraft System)	Dji Mavic/Phantom, FPV whoop, etc.	Bayraktar TB2, FPV kamikaze, etc.
Terrestrial	UGV (Unmanned Ground Vehicle)	Minesweeper robot, delivery	Ratel S, Ironclad, Lyut, etc.
Maritim	USV (Unmanned Surface Vehicle) / UUV (Unmanned Underwater Vehicle)	Coastal surveillance, bathymetry	Magura V5, Sea Baby, Toloka, etc.





Drones (2)

- RF convergence across all three domains -> All share the same dependency on radio links

Type of radio	Figthing UAV FPV	UAV MALE	Figthing UGV	UUV
RC / C2	ELRS 868/915 MHz, mostly 2.4 GHz and others...	Satellite Ku/Ka (SATCOM), LOS radio 900 MHz	ELRS / FrSky 2.4 GHz, or proprietary RC	Fiber, or acoustic
Video downlink	FPV 5.8 GHz (analogic or digital)	Ku-band satellite / LTE 4G (IP)	FPV 5.8 GHz (analogic or digital)	No live vs ROV (Remotely Operated Vehicle)
Telemetry	Generally, MAVlink over ELRS	MAVLink over IP/SATCOM	MAVLink over 900MHz/2.4 GHz radio	Acoustic protocols (JANUS, OAM), others proprietary

This session focuses on UAV FPVs

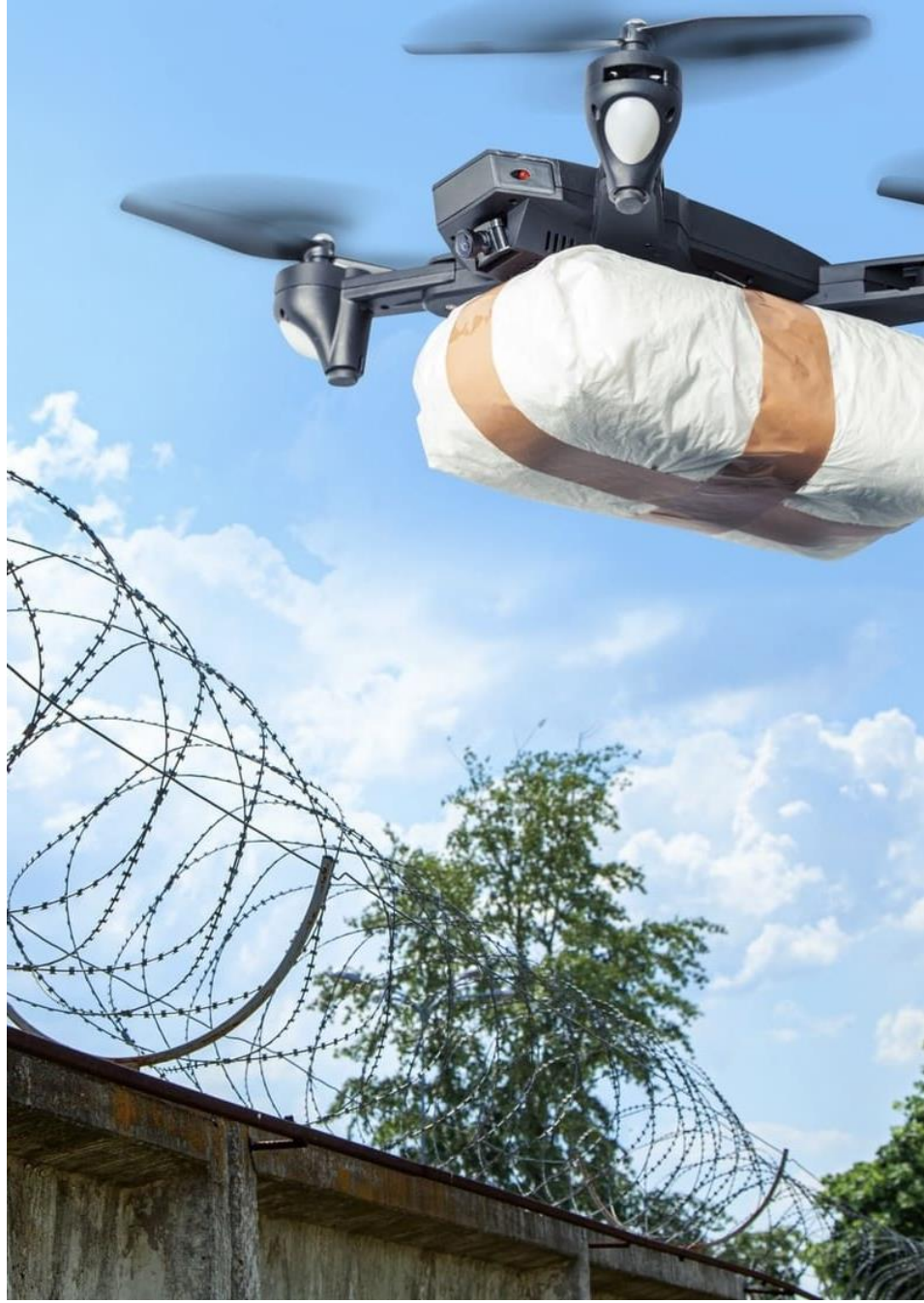
The rise of consumer drones

- Dominant civil use cases:
  - Precision agriculture: mapping, spraying, crop monitoring
  - Infrastructure inspection: HV lines, wind turbines, bridges
  - Photogrammetry & surveying: LiDAR, 3D terrain modeling
  - Last-mile delivery: Amazon Prime Air, Wing, Zipline (operational 2024)
  - Cinematography & broadcasting



The rise of consumer drones (2)

- Emerging risk surface:
  - Airport intrusions: Gatwick 2018, Heathrow 2023
  - Non-consensual surveillance & privacy violations
  - Prison contraband delivery
  - Weaponization by non-state actors



Context

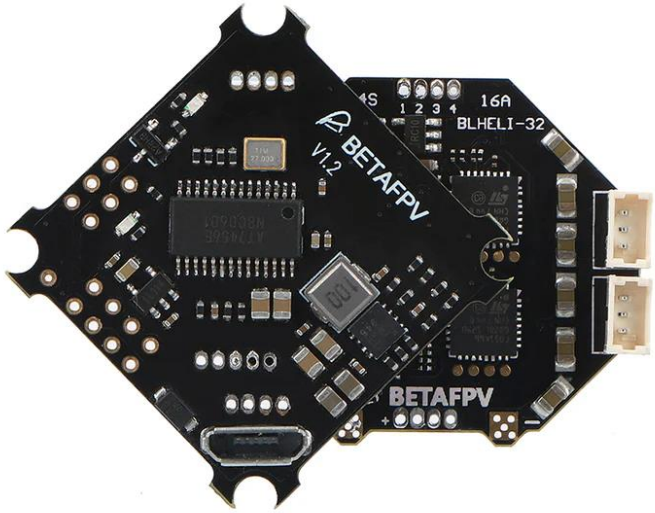
Drones as weapons: From hobby to battlefield

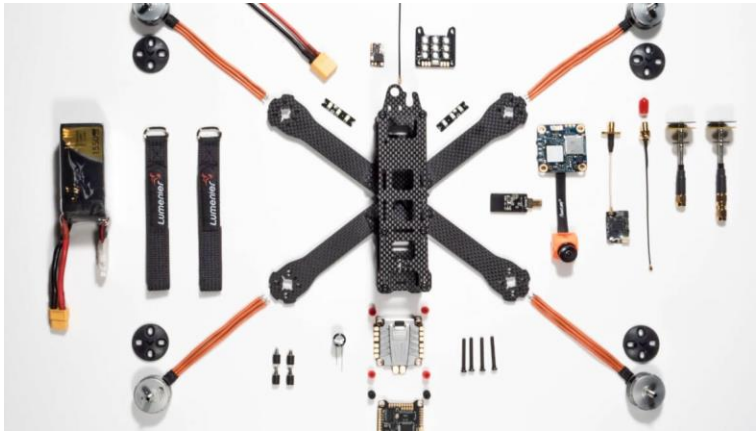
- A few dates:
  - 2016: ISIS drops grenades from DJI Phantom: first documented COTS weaponization
  - 2019: Houthi drones strike Saudi Aramco: critical infrastructure attacks at scale
  - 2022: Ukraine FPV kamikaze drones emerge: **~$300 max drone vs. ~$3M tank** -> scalable asymmetric warfare
  - 2023: First all-robot ground assault (Ratel S + FPV). USVs sink Russian warships in Black Sea
  - 2024: Coordinated multi-domain drone swarms
  - Even beyond Ukraine: the Sudan case -> Non-state actor (RSF) operating drones with 2,000 km range -> no air force needed
    - Both sides now use FPV COTS kamikaze drones -> direct Ukraine technology diffusion



Drones' BoM

Part	Cost	Notes
Plastic or carbon frame	~30€ max	
Flight Controller & ESC	~30€	
4× brushless motors	~50€	
Analog VTX 5.8 GHz	~20€	FM-NTSC, or numeric
ELRS RC receiver	~20€	Generally, 868/915/2400 MHz selectable -> we can hack
FPV camera	~20€	CMOS wide-angle
LiPo 4S 1500 mAh	~30€	





Drone warfare is no longer a state privilege -> ~90% UAV are FPV drones

Monitoring

Detection in the normal "regulated" world

- Use of OpenDroneID and RemoteID
- Cases:
  - EU: UE 2019/945 + 2019/947 -> required since 2024 for all drones (C1 category and > 250g)
  - US: FAA Part 89 -> required since 2023 for all drones > 250g
- The drone broadcast its ID continually, its location, speed, operator location via BLE or Wi-Fi*
- Implemented for DJI drones, but rarely FPV racing quad (especially custom ones)

Counter Unmanned Aerial System: Detection

- RF is the only universal signature:
  - No ADS-B, no transponder, no Remote ID on combat FPV
  - RC link + video link = always present during flight - unavoidable emission
  - Passive detection range: 1–5 km depending on hardware and protocol

Classic sensors and their hard limits

Sensor	Fatal limitation on FPV
Radar	RCS < 0.01 m² -> micro-drones below detection floor
Optical / IR	Range-limited, angle-of-view constraints, blind at night
Acoustic	Ineffective beyond 200m, masked by wind and combat noise
RF passive	Works but FHSS + frequency migration => moving target

But when RF is replaced by fiber -> EM can be alanyzed

FPV Drones analysis

FPV

- First Person View (FPV) drones
- Provide real-time video feed from onboard camera to the pilot
- Applications:
  - Racing
  - Freestyle
  - Search and rescue
  - Military



Communications

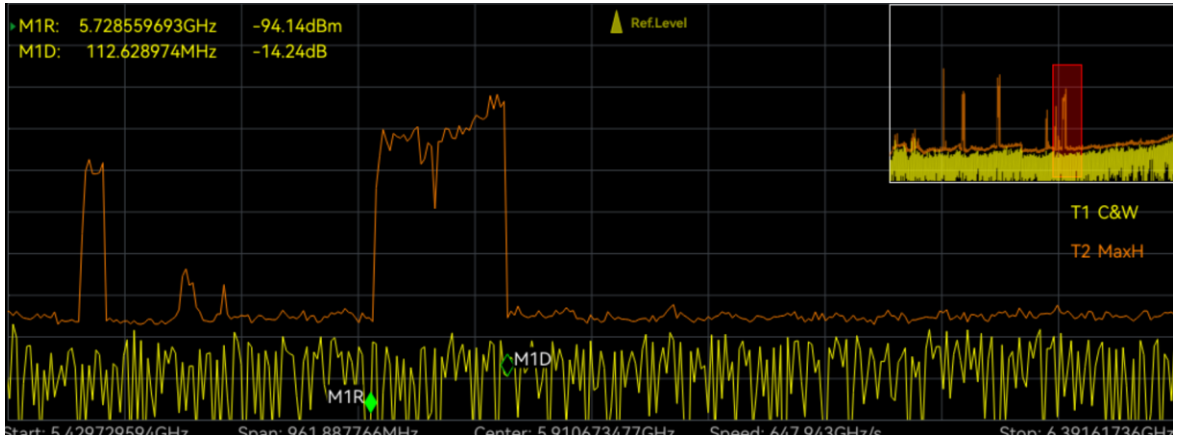
- Control Link:
  - Pilot commands to drone
  - Frequencies: 2.4 GHz, 868 MHz and 900 MHz (and more => it's possible to custom)
  - Range (1-30 Km depending on link budget)
- Video Link
  - Camera feed to goggles
  - Frequencies: 5.8 GHz generally
  - Technologies: Analog, Digital (DJI, HDZero, Walksnail, etc.)
- GPS -> depends...

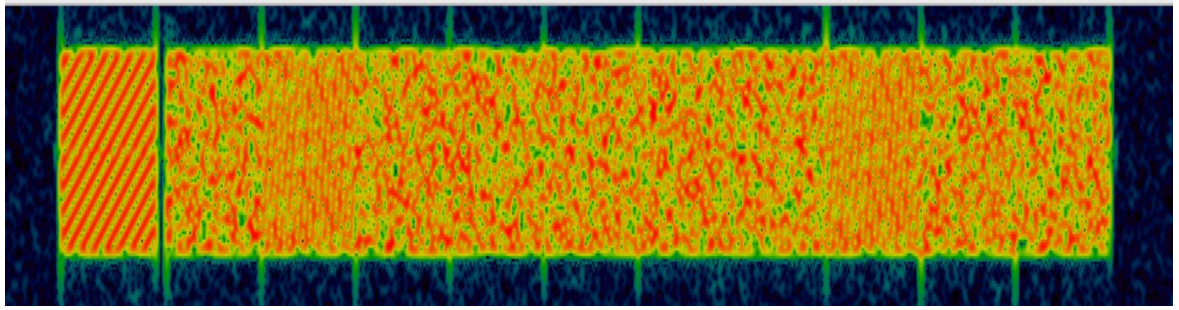
Some Control Protocols

Protocol	Frequency band	Description / Comment
ExpressLRS	915 MHz (US, Asia, Australia) /2.4 GHz (EU) but can be found also on 868/900 MHz with external module	Open-source, using LoRa PHY -> the dominant protocol
mLRS	2.4 GHz / 868 MHz (EU) / 915 MHz (US) / 433 MHz (70 cm, ham band);	Open-source, using LoRa PHY with bidirectional serial connection + full RC. Niche: far less widespread than ELRS; used mainly by the ArduPilot/PX4 community
Crossfire	868 MHz (EU, Russia) / 915MHz (USA, Asia, Australia)	Proprietary
Ghost	2.4 GHz	Low latency for racing
Tracer	2.4 GHz	Affordable and performant
FrSky	915 MHz (US, Asia, Australia) /2.4 GHz (EU)	
DJI OcuSync 2.0/3.0/4.0	2.4 GHz & 5.8 GHz	Proprietary and frames now encrypted, encrypted DroneID since 4.0

DJI OcuSync

- Different versions:
  - OcuSync 1.0: clear-text
  - OcuSync 2.0: clear-text
  - OcuSync 3.0: Partially decoded
  - OcuSyn 4.0: Ciphered -> new hash ID per session





DJI monitoring solution: Aeroscope



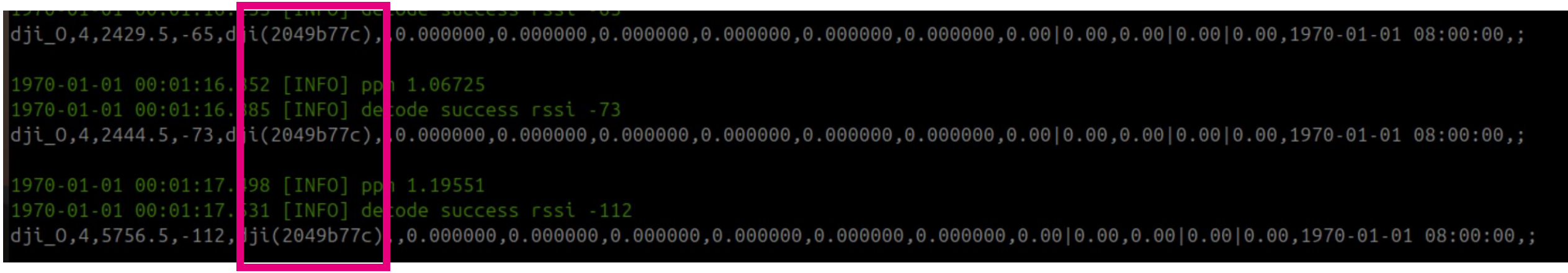
But some solutions are also available publicly ->

DJI OcuSync 4.0 detection

- Fails with previous tools -> no ID nor coordinates:


```
0u{"freq":5756.500000000000000,"device_type":"DJI Unknown","device_type_8":169,"drone_gps_time":"2009-06-15 19:16:36","app_lat":-8706.977540064057393
one_lat":-1839.480585333432600,"drone_lon":8374.005838437429702,"home_lat":3285.358751640090759,"home_lon":4737.393467138019332,"heigth":-3261.400000
000000}
0y{"freq":5776.500000000000000,"device_type":"DJI Unknown","device_type_8":151,"drone_gps_time":"1989-01-08 29:53:29","app_lat":-9819.922897102553179
rone_lat":4490.942182853672421,"drone_lon":-11352.634768210024049,"home_lat":-10661.590323892902234,"home_lon":-4287.321595343000808,"heigth":-568.70
9999999989}
```

DJI OcuSync 4.0 detection (2) -> hash ID



ExpressLRS (ELRS)

- Open-Source RC Link -> easily hackable
- Dominant in racing
- Hardware:
  - For radio: Semtech SX127x/SX128x LoRa -> very cheap and efficient
  - ESP32/STM32 for MCUs



SX1276/SX1278 used in lower ranges

- Bands: 136 – 1020 MHz
- Classic ELRS usage: 868/915/433 MHz
- Just need to setup a specific register
- But to arrive at ~1200 MHz:
  - Out of range of the VCO -> possible distortions, degraded dynrange, etc.
- Also, the perfomances are lower to SX1280 (BW, modulations, etc.)
- So, we can take the SX1280 instead and hack it!



Closer look at SX1280 used in common ELRS FPV

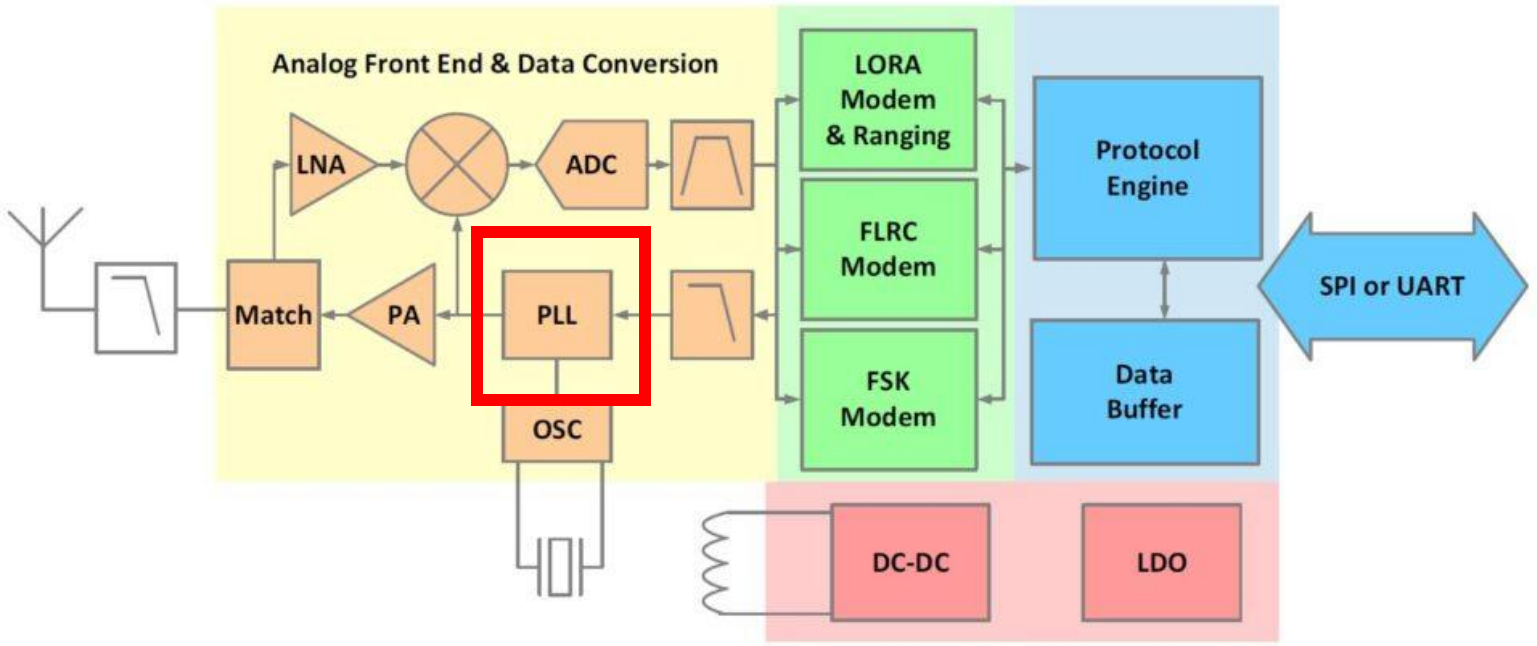


Figure A: Transceiver Block Diagram

SX1280 hack

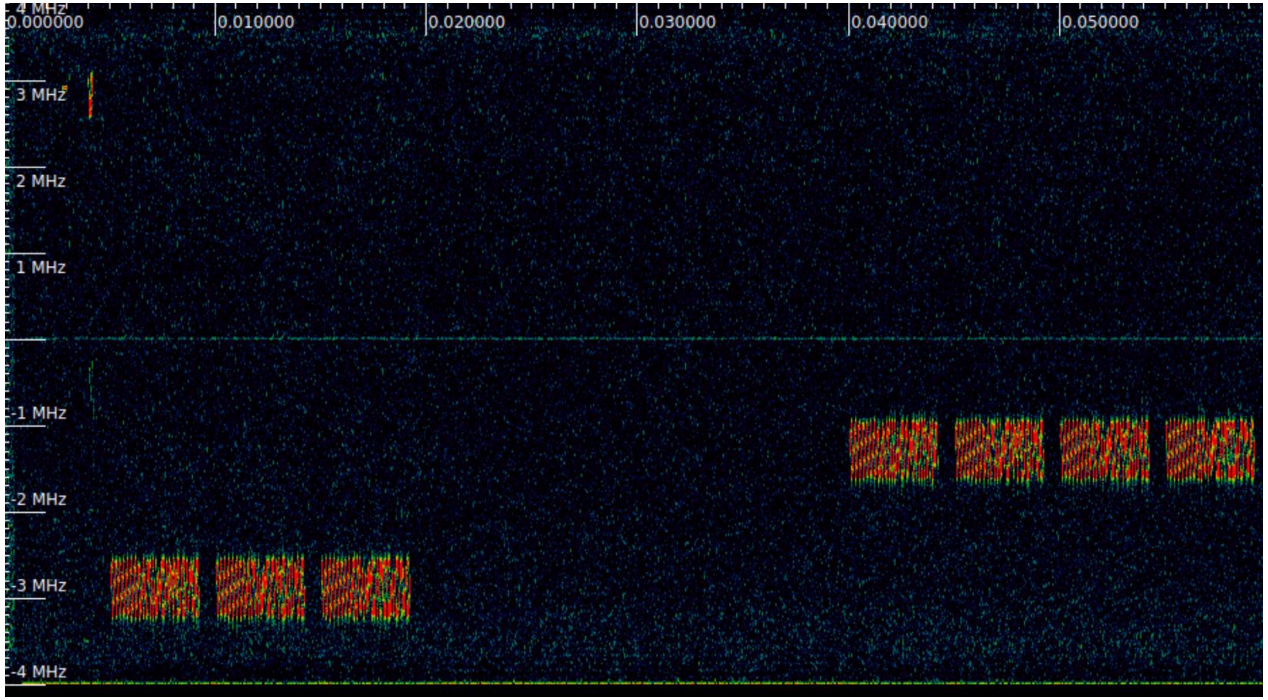
- Original crystal: 52 MHz
- Crystal swap -> 26 MHz + F_XOSC to set properly
- New local oscillator -> shifts to lower frequencies between 1200-1250 MHz
- We keep LoRa/FLRC/GFSK modulations and rates
- Could be also patched with an UP/DOWN converter -> takes space

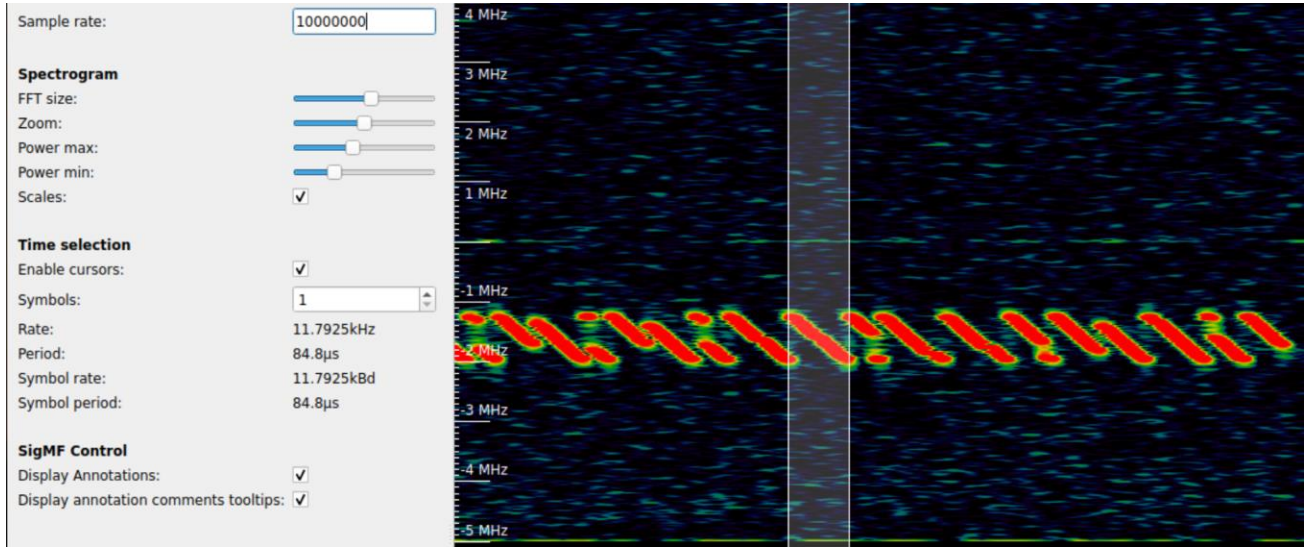
ELRS modulations

- LoRa PHY -> sending chirps -> efficient for long distances
- FLRC (Fast Long-Range Communication) -> Semtec's GFSK
  - Rare to see for cheap FPVs

ELRS LoRa

- Modulation: LoRa CSS
- Frequency: 2.4 GHz generally
- Bandwidth: 500kHz – 800 kHz
- Spreading factor: SF5 – SF10
- Packet rates:
  - 50 Hz: Long range
  - 150 Hz: Balanced
  - 250 Hz: Racing
  - 500 Hz: Ultra-low latency
  - 1000 Hz: Experimental (2.4 GHz)





Jamming

Jamming attacks, and limits

- Most jammers focus on traditional ISM bands:
  - 433 MHz
  - 868 MHz
  - 2.4 GHZ
  - 5.8 GHz
- But warfare FPV are "hacked" -> 1080-1320 MHz mostly and other bands for ELRS FPV
  - Need a real UWB Jammer, but there would always be a non-supported band in use by the drones
- It is also illegal unless having specific authorization

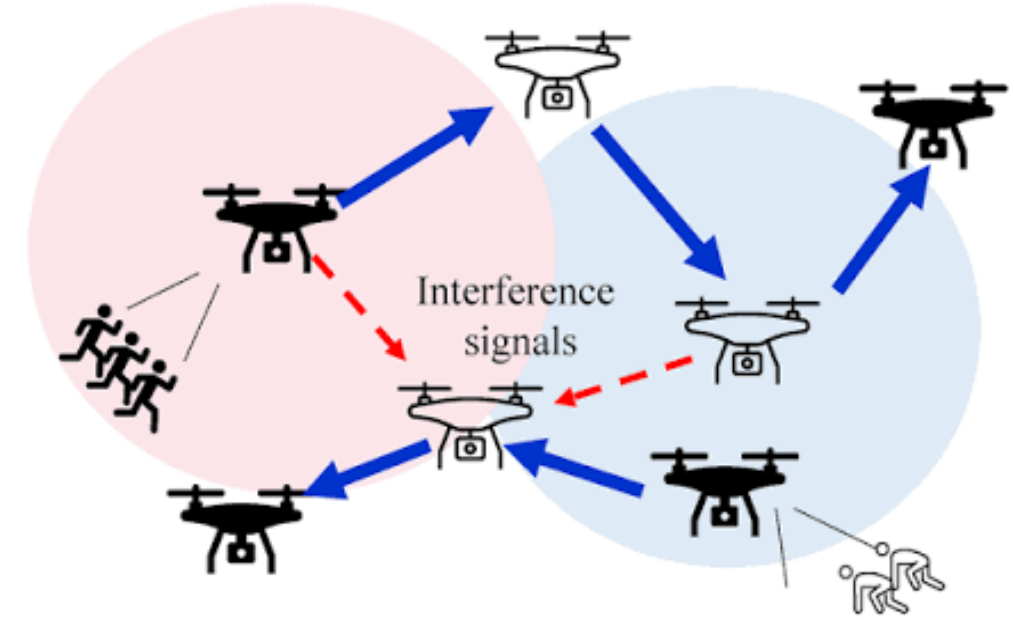
-> Some other techniques can be used (see analysis)

But what about drones using fiber?

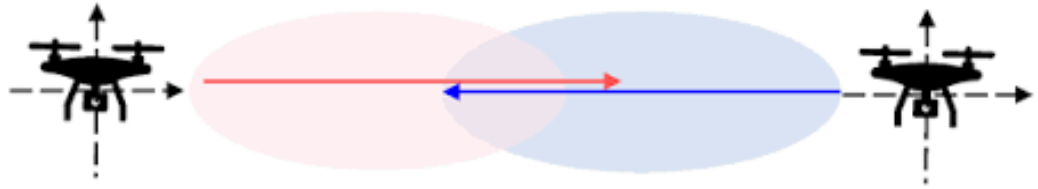


Jamming fun fact

- Drones can flight very far
  - with a powerful LNA and matching antenna
  - And/or a relay
- Jamming a relay -> affects all covered drones



(a) How to use a relay network.



(b) Relay method using directional beams.

Drones on fiber

- Optic fiber = no RF jamming :'(
- But without proper isolation -> laser dazzler sweep

(See video)



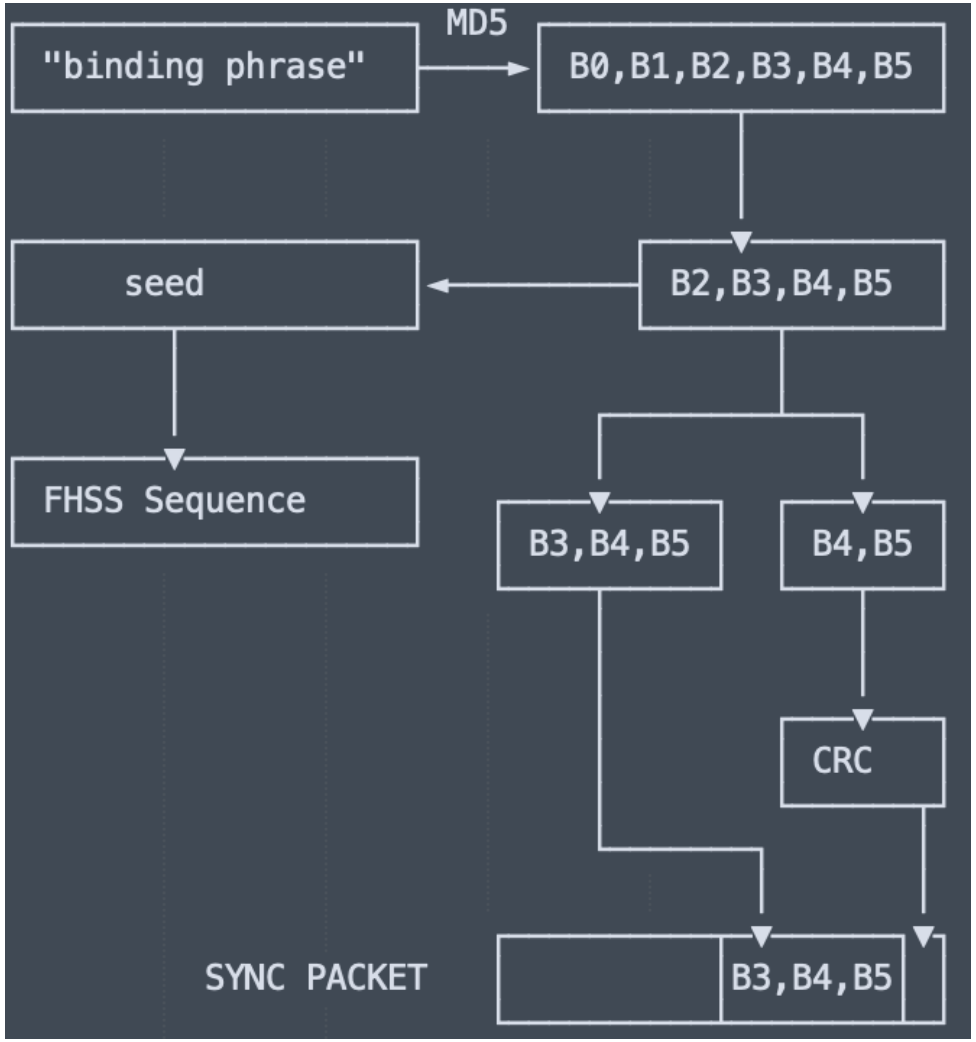
Hijacks and other attacks

ELRS "Security"

- Use of binding phrase -> generate a UID
- But only for anti-collision
- Difficult to demodulate:
  - Hopping
  - No clear specs -> need to reverse and look at sources
- Limitation:
  - No encryption
  - No authentication
  - Vulnerable to replay

ELRS binding

- Uses of "binding phrase" -> hashed in MD5 -> UID
- 6 bytes -> stored has shared UID receiver <-> transmitter
- Last 4 Bytes -> seed defining the FHSS sequence
- CRC init by 2 last bytes of UID



Source: https://www.nccgroup.com/research-blog/technical-advisory-expresslrs-vulnerabilities-allow-for-hijack-of-control-link/

RX boot sequence

1. RX powers on
2. Scans for sync packets at different packet rates
3. Locks onto TX when sync packet detected
4. Establishes FHSS sequence
5. Begins receiving command packets

ELRS team vs Security

- NCC group tried to patch the implementation to make things a bit more complicated to attack
  - https://github.com/ExpressLRS/ExpressLRS/pull/1411
- Response of the team: TL;DR "ExpressLRS is not SecureLRS"
  - But also at the end, CRC is just 14 bits -> fast to crack so no need to know the UID
  - And at the end, sync packets can be replayed

Attacking the video + demo

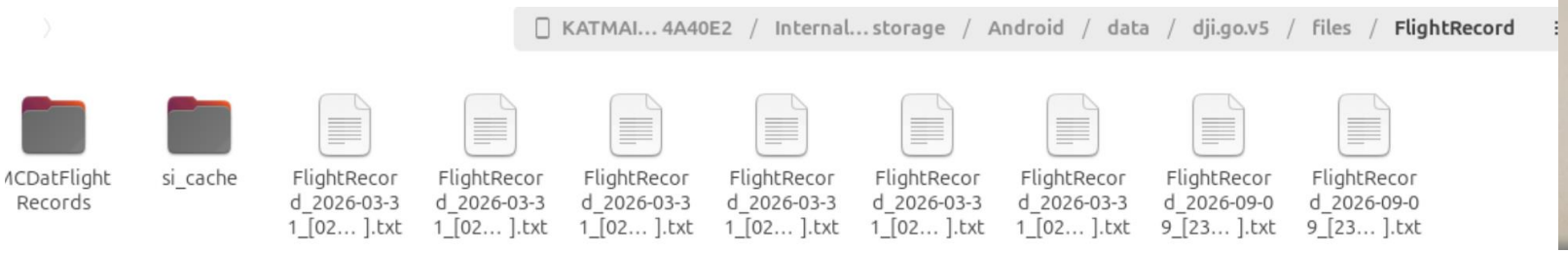
System	Type	Official band(s)	Modulation	Occupied BW	SDR / tool capture
Analog FPV (NTSC/PAL)	Analog	5.8 GHz (also 1.2/1.3, 2.4, 900 MHz legacy)	Wideband FM of composite CVBS; FM audio subcarrier (~6.0/6.5 MHz)	~17–27 MHz (channel spacing ~20–37 MHz)	WFM demod → composite baseband → NTSC/PAL decode
DJI OcuSync / O2 / O3 / O4	Digital	2.4 & 5.8 GHz (some 5.1)	Proprietary OFDM (LTE/Wi-Fi-like)	10 / 20 / 40 MHz	Wideband IQ record -> Payload AES-encrypted
HDZero (ex-SharkByte)	Digital, low-latency line-based	5.8 GHz	Proprietary PHY	~27 MHz/channel	Wideband IQ record; no public end-to-end decoder
Walksnail Avatar (Caddx/Fatshark)	Digital	5.8 GHz (2.4 on some)	Proprietary PHY	~20–27 MHz	Wideband IQ record; proprietary, no public decoder

Non-RF: Forensics

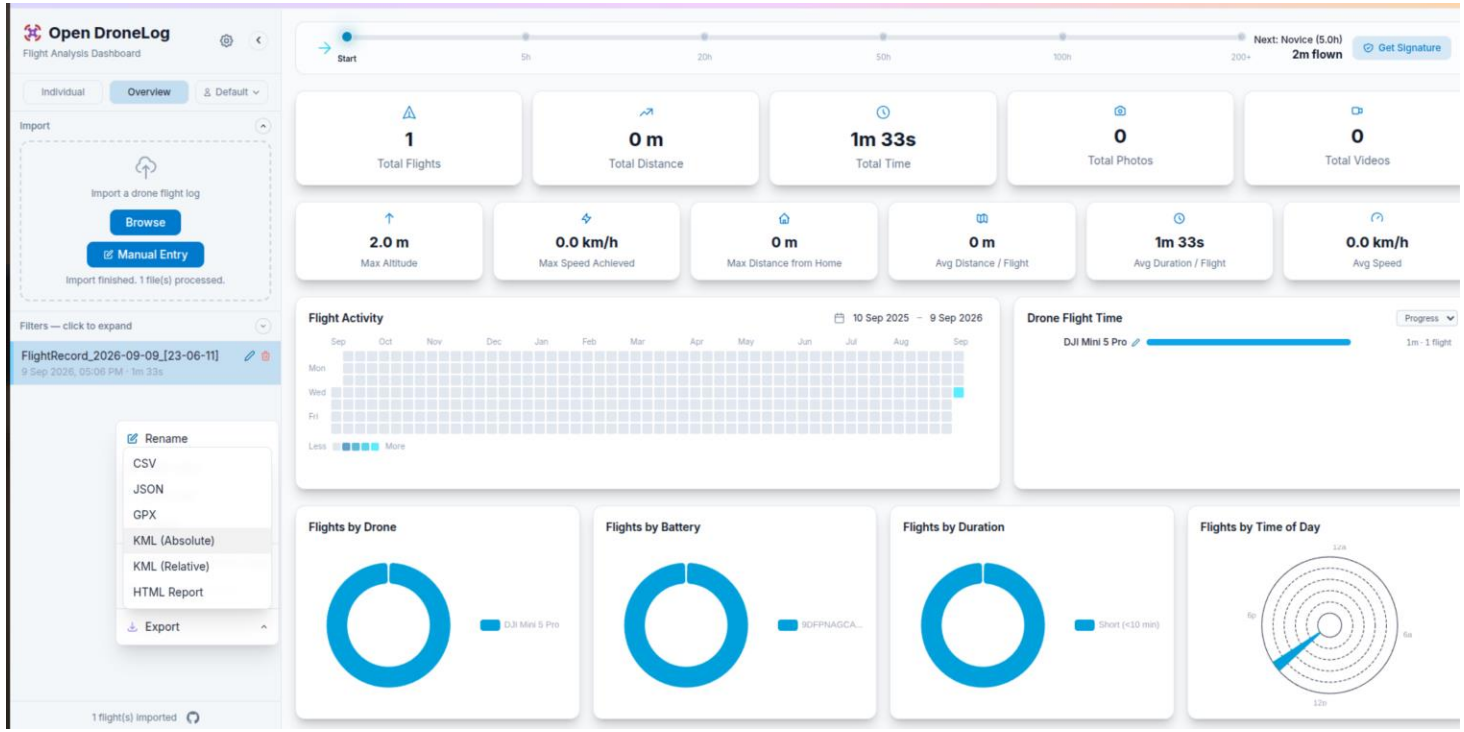
DJI drones: remote's USB

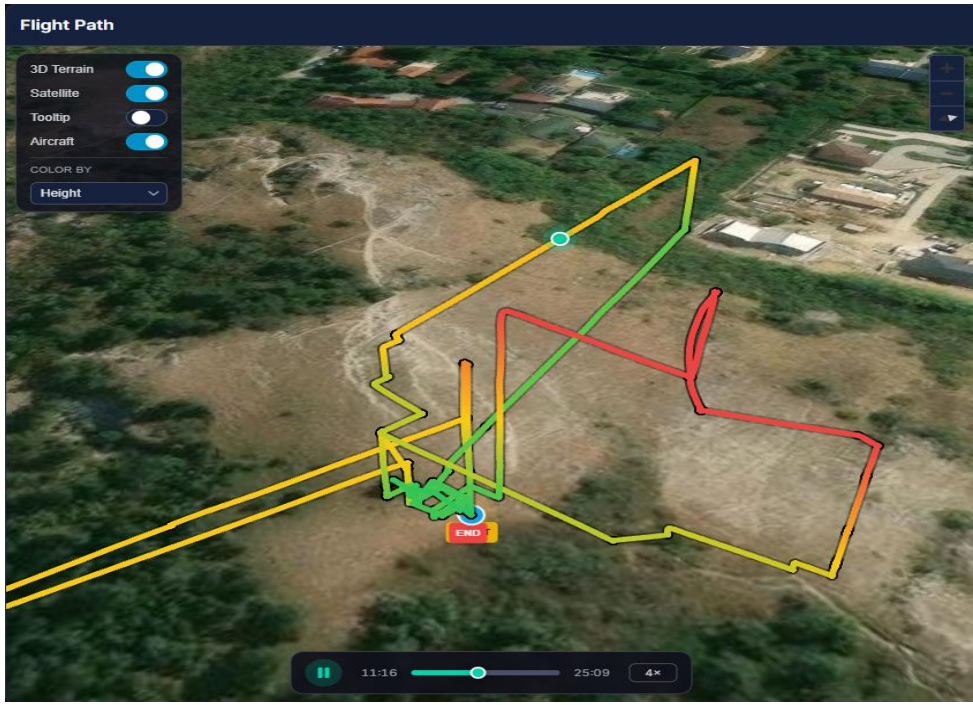
- Turn on the remote and connect into a computer -> look for FlighRecord_***.txt





Reading RC's logs



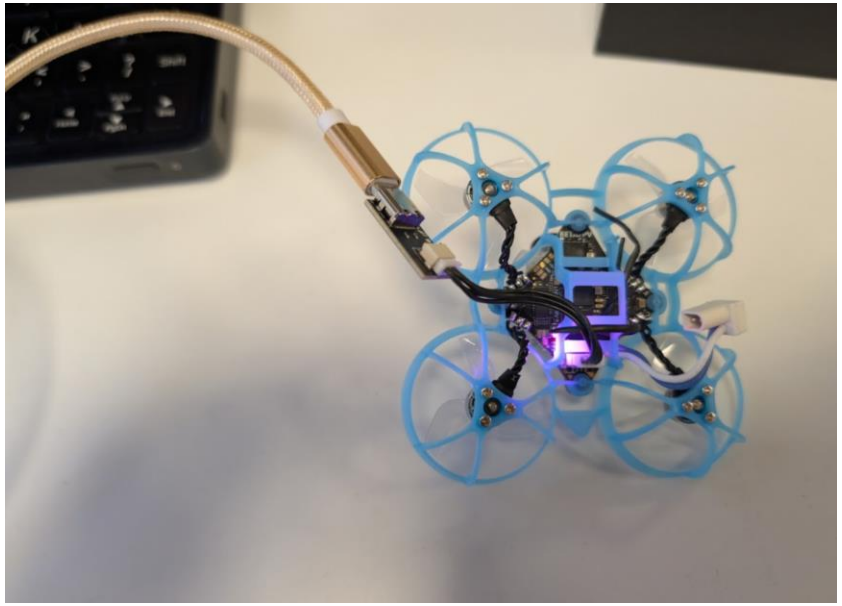


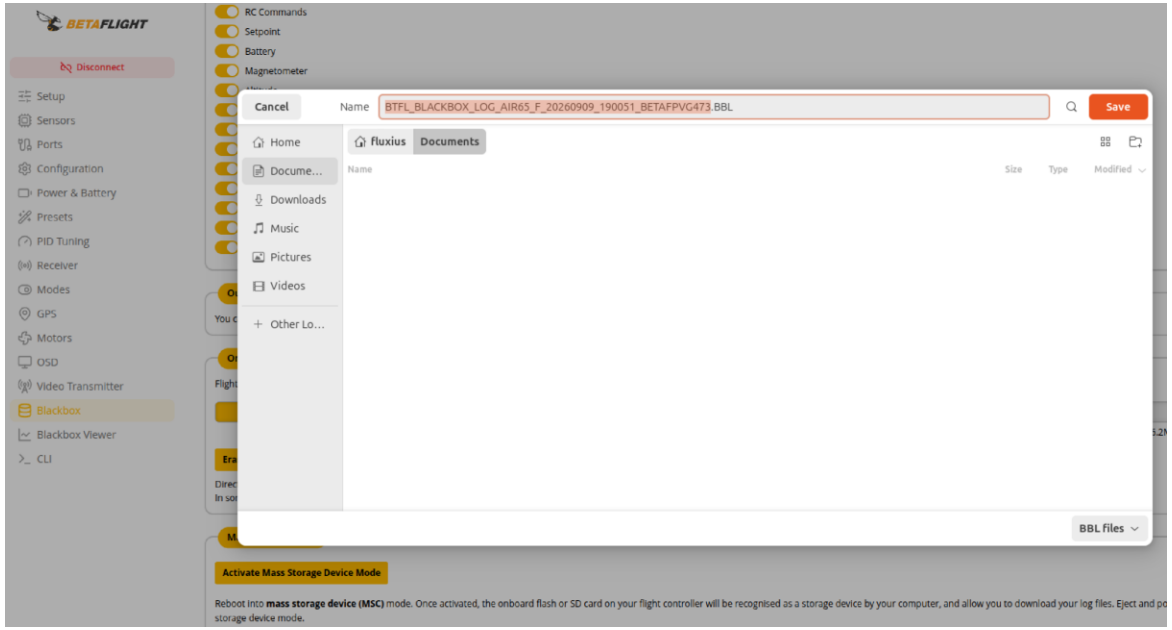
DJI drones: FC's side

- DAT files -> USB can be accessed with DJI Assitant 2
  - But will be encrypted
- On old drones -> USB access -> RCE with ADB and extract even DAT and keys
- New drones -> firmware is locked
  - Extract via JTAG or even chip-off

ELRS based drones

- Everything is in clear text
- Can be accessed in
  - UART
  - or simply with an appropriate configurator (e.g.: betaflight configurator)
- Use blackbox_decode to transform BBL -> CSV and convert to KML at the end for the nice map





Conclusion

Conclusion

- And that was just an overview...
- Drones and their remote using RF -> can be attacked and monitored
- Using fiber -> can also be spotted with sound, radar but also their EM signature and have their own jamming exposure
- C-UAS can also be accessible but needs a lot of work
  - And it's a cat and mouse game

penthertz

Thank You

Please contact us:

contact@penthertz.com

+33 1 73 13 82 77

penthertz.com

Watch us on YouTube