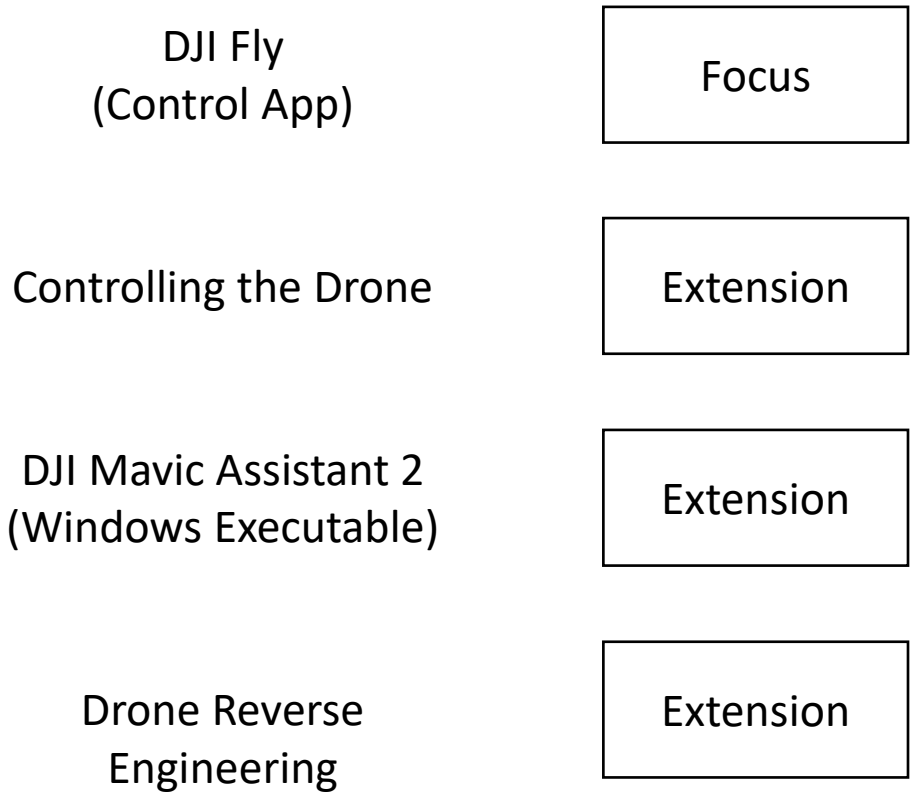
DJI Hacking

deadbeat

Aims of this Project

- To learn about the process of reverse engineering a consumer device.
- To conduct effective research around a target.

Discovery


DJI Fly
(Control App)
Focus
Controlling the Drone
Extension
DJI Mavic Assistant 2
(Windows Executable)
Extension
Drone Reverse
Engineering
Extension

DJI Fly – The Basics

- The Mavic Air 2 is controlled through the DJI Fly app (more on control later).

- The old application for control called DJI GO was compromised and I wanted to see it this was possible for the DJI Fly App (again more on this later).

- Therefore the first task is to analyse the DJI Fly APK.

DJI Fly – Reverse Engineering (1)

(Downloaded on an Android 10 device)

- First step is to reverse engineer the APK, DJI don’t make this easy…
- Most of the application is downloaded directly from the app store, other “stuff” is downloaded on first boot.
- Once unpacked, there is a LOT of files, most of which are binaries; others are specifically designed not to be read by cheeky westerns (me).

DJI Fly – Reverse Engineering (2)

- These files have been heavily encoded and are written in either Mandarin or Korean (according to Google Translate)
- Even once “translated” they seem to heavily encoded further.
- Next steps…

DJI GO Exploitation

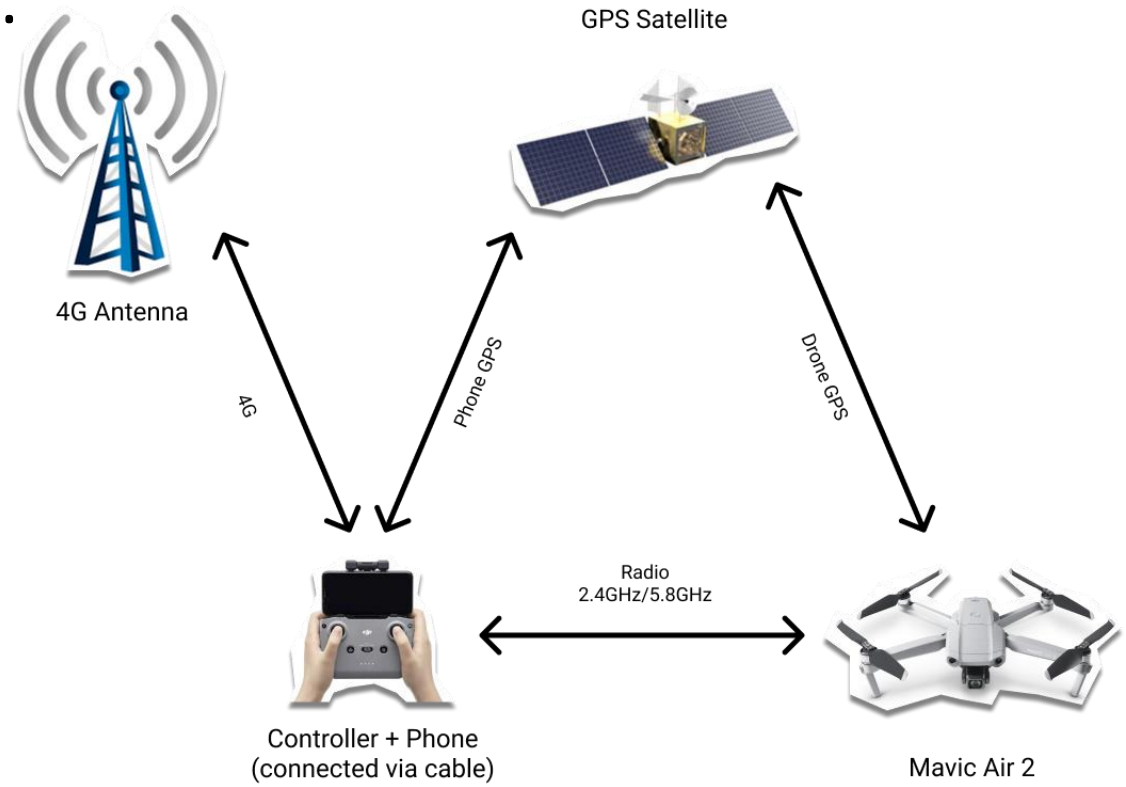
- DJI GO is another control app used to control other drones in the DJI lineup, not used in newer models due to successful reverse engineering.

- Individuals managed to *acquire* the encryption keys for DJI GO package encryption and were able to edit the source code of the application.

- With the source code they were able to remove **all** safety limits on the drone, including; maximum speed in all 6 axes, maximum height, turn on and off the propellers mid-flight at will etc. etc.[1]

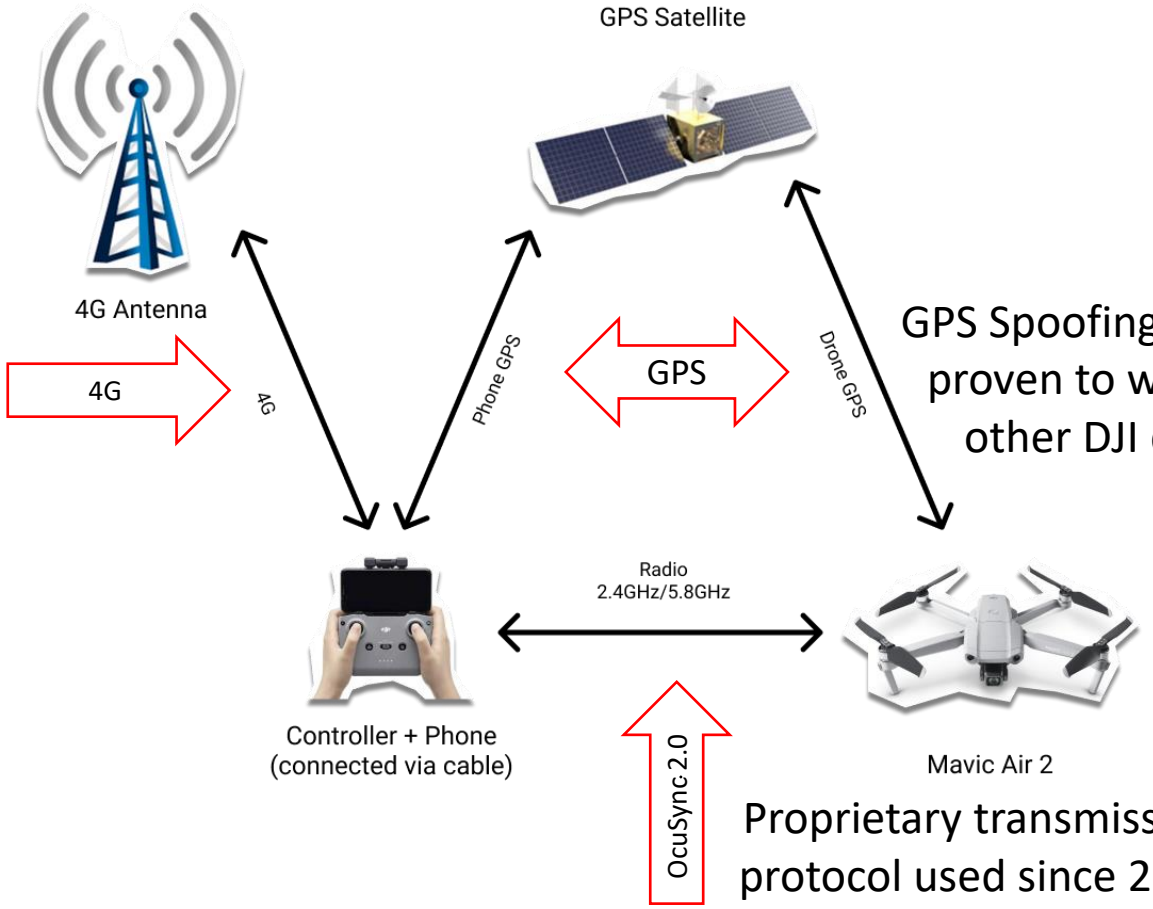
Controlling the Drone – The Basics

Various models are controlled in different ways, the Mavic Air 2 is controlled like so:



Controlling the Drone – Possible Attack Vectors

High effort, but could allow you to MITM firmware updates, steal private keys etc.

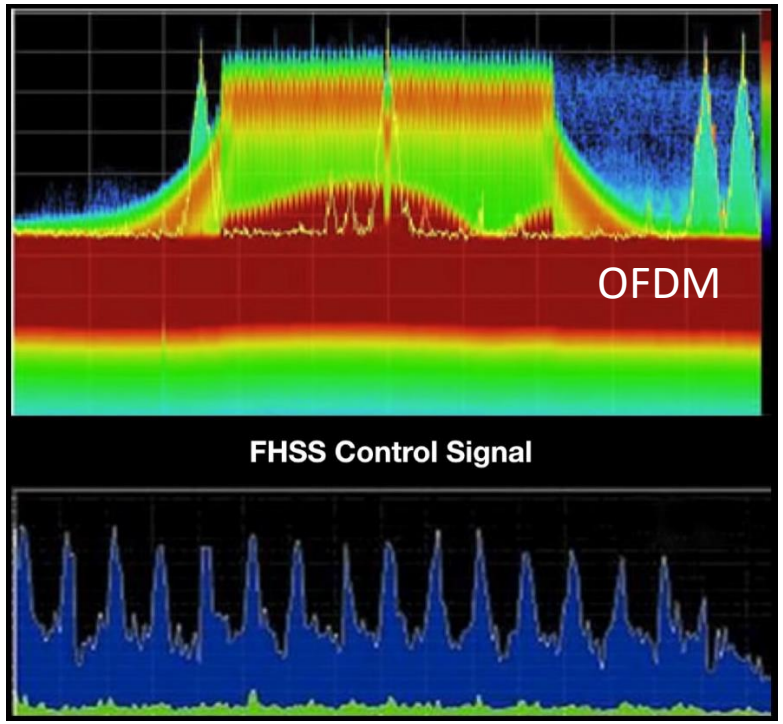


GPS Spoofing has been proven to work with other DJI drones

Proprietary transmission protocol used since 2018

Controlling the Drone – OcuSync 2.0 (1)

- OcuSync 2.0 is DJI's proprietary radio standard combining different standards to achieve the intended functionality. [2]



Video-carrier, prefers 5.8GHz with automatic band switching. Supports DES and AES.

Always 2.4GHz, somewhat resistant to jamming.

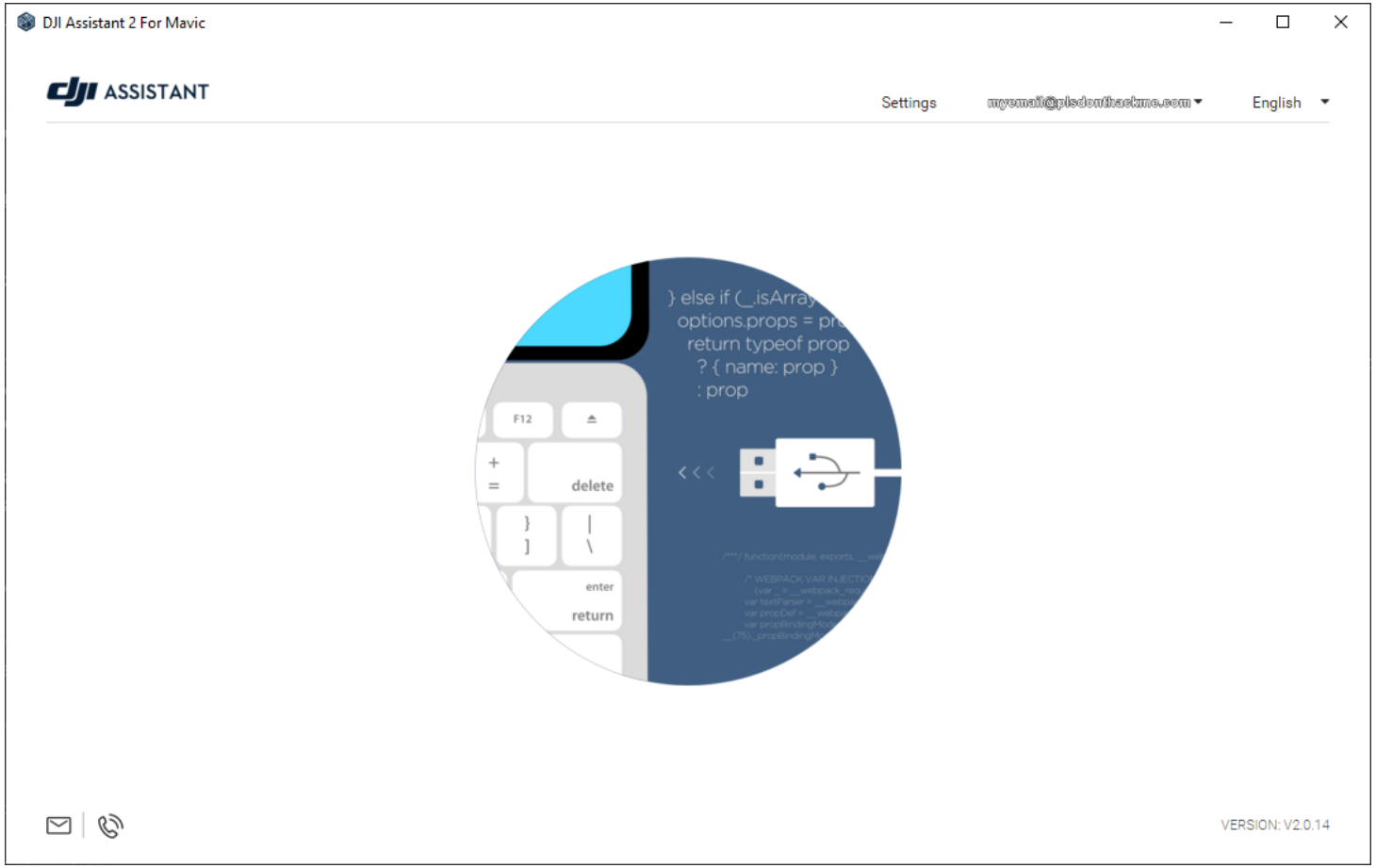
- OcuSync 2.0 is an SDR-defined solution, which presents an interesting attack vector.

Controlling the Drone – OcuSync 2.0 (2)

- Unable to intercept or exploit this due to inexperience working with radio and lack of SDR equipment.

- Next steps…

DJI Mavic Assistant 2



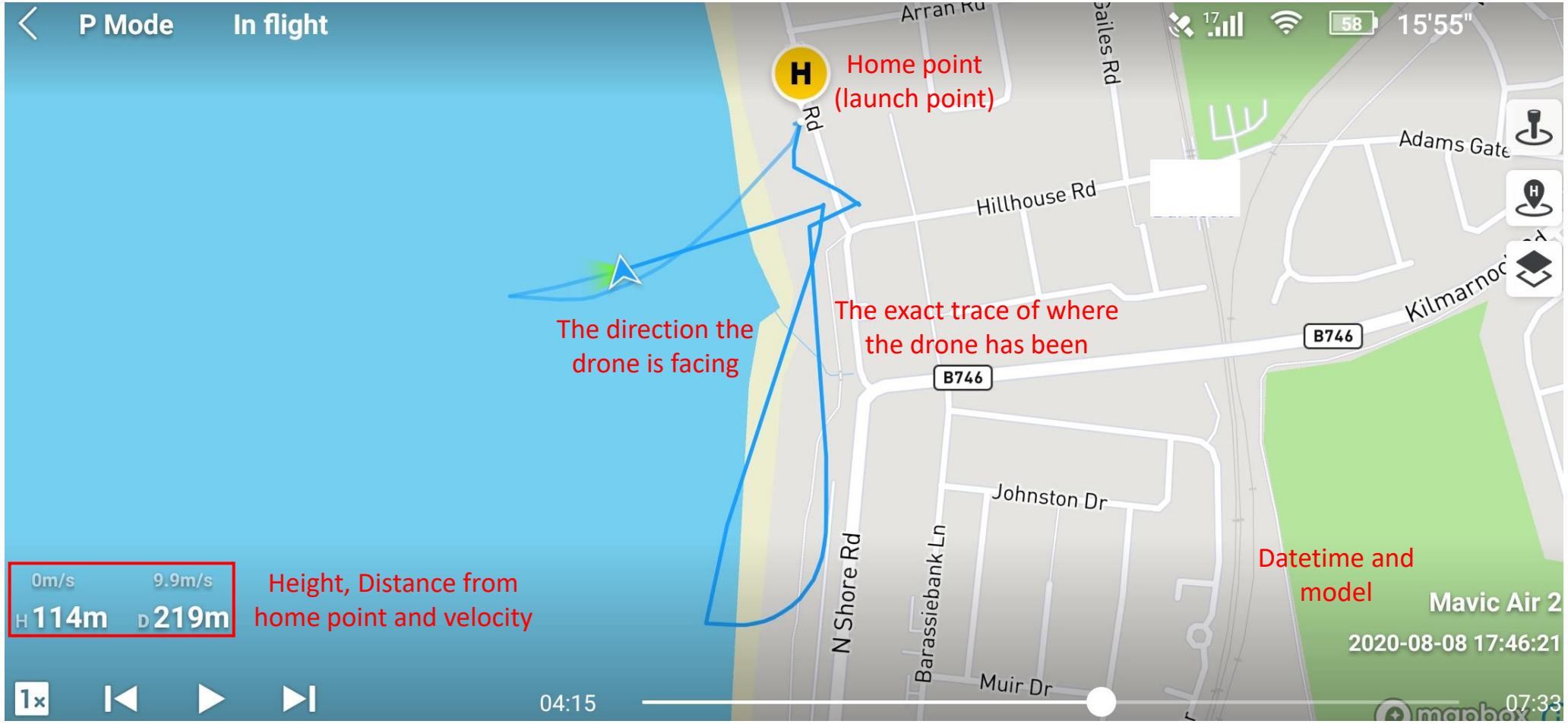
DJI Mavic Assistant 2

- Mavic Assistant 2 used to allow extensive viewing and modification of drone configuration. (Still achievable if you use old firmware and application) [3] However, the Mavic Air 2 lacks this feature.

- Mavic Assistant 2 can allow you to view flight logs[4] but newer drones like the Mavic Air 2, only the DJI Fly (app) logs are unencrypted.

- These provide a **juicy** opportunity for intelligence gathering.

~~Mavic Assistant 2~~DJI Fly – Logs (1)



~~Mavic Assistant 2~~DJI Fly – Logs (2)

- These obviously provide a crazy amount of information; pattern analysis could allow sensitive locations (e.g. home addresses) to be leaked.

- Other models have other unencrypted logs that provide crazy detail about diagnostic data, which may allow further exploitation of those systems.

Drone Reverse Engineering – Hardware (1)

- External Connectors
  - SD Card
  - USB-C

- Internal Connectors
  - From my rudimentary analysis of the board, I couldn’t find any debug connectors BUT previous DJI models have had usable debug connectors in production models.

Drone Reverse Engineering – Hardware (2)

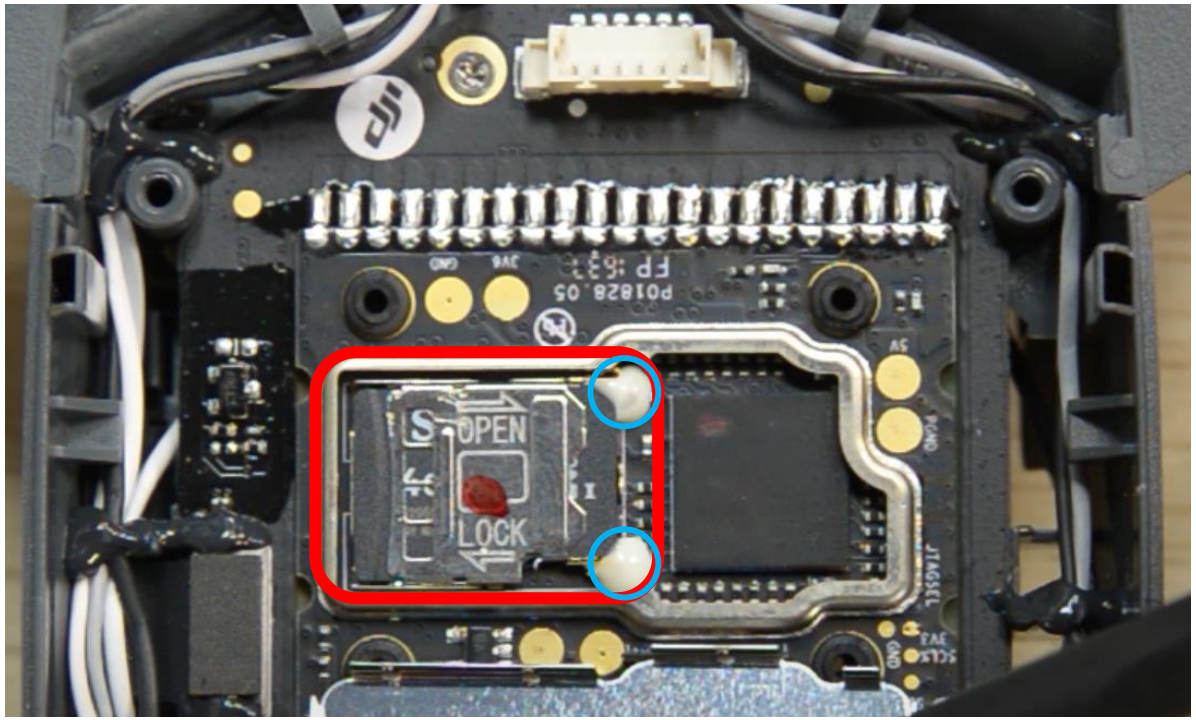
- Two PCBs in the drone

- Motherboard
  - Unknown ARM64 based processor
  - Ambarella H6 processor (ARM)[5]
  - SKHynix RAM[5]
  - Samsung 8GB internal memory[5]

- GPS Board
  - GPS
  - Motor power delivery and data

Drone Reverse Engineering – Previous Models

- Mavic Pro (pictured) had a glued in SD card functioning as a “black box” for the drone.



Discovery

DJI Fly (Control App) → Reverse Engineer App → DJI Go Exploitation

Controlling the Drone → Hijack Using SDR

DJI Mavic Assistant 2 (Windows Executable) → Reverse Engineer

Drone Reverse Engineering → Hardware → Previous Models

Append(ish)

Ethics, the Law and Resources

Ethics (1)

- Drone usage in the UK is regulated by the CAA. All research involved in this presentation was done within the law and CAA guidance on good drone practice.
  - Further information can be found at: https://register-drones.caa.co.uk/drone-code
- Appropriate permission was obtained when flying in restricted areas.
  - Interestingly, “Government” spec drones have no geofencing…[7]
- DJI has an active bug bounty program and (mostly) encourage finding exploits in their products.
  - Further information can be found at: https://security.dji.com/

Ethics (2)

- DJI is a Chinese company and it brings similar baggage as other high-profile cases such as TikTok (from ByteDance).

- Security researchers recently, have found that DJI updated their control apps without user consent, however, DJI refutes this.[6][7]

- Avoiding the politics, China has the National Intelligence Law (2017) which compels Chinese companies to divulge information to the Chinese government without the need for a warrant.[8][9]

- I’ve learnt a lot, and I would do things differently if I did it again.

- And I’ve still got a lot to learn!

Resources

1. https://dji.retroroms.info/howto/start
2. http://djibestdrones.com/dji-ocusync-2-0/
3. https://greyarro.ws/t/how-to-change-flight-parameters-on-a-dji-mavic-pro-phantom-4-and-inspire-2/930
4. https://mavicpilots.com/threads/mavic-flight-log-retrieval-and-analysis-guide.78627/
5. https://www.youtube.com/watch?v=9Uy9QNidi1U
6. https://www.synacktiv.com/en/publications/dji-android-go-4-application-security-analysis.html (Researcher Article)
7. https://www.dji.com/uk/newsroom/news/dji-statement-on-further-misleading-claims-about-app-security (DJI Rebuttal)
8. https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense
9. https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws

https://creativeelectron.com/dji-mavic-air-2-drone-teardown/ - Slides 20,21 (Drone X-Rays)

https://youtu.be/GJUDqxf0c8k?t=82 – Slide 22 (Mavic Pro “Black Box)

fin

please fin-ack

If you do, I'll ack :)