



Nico Schiller

@74ck_0

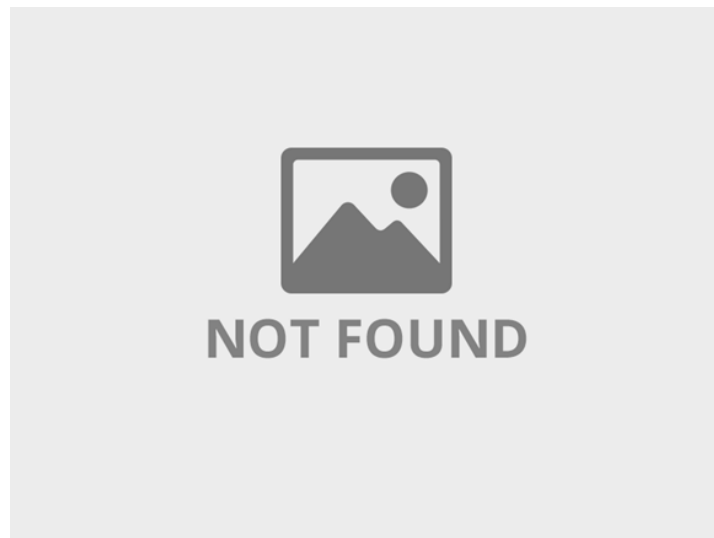
22-04-2022

12:40

This is what DJI's Drone-ID packets look like. every drone broadcasts this data all the time. we managed to receive + decode the packets over the air. no encryption. (we saw some confusion around that before)

@merlinchlosta

1/n



Drone-ID sends high-accuracy GPS positions of drone, pilot, and "home point" (where the drone returns to). the packets are sent basically every second, revealing the full flight path. along with GPS, it discloses drone type and serial number.

2/n

we didn't require "DJI Aeroscope" for this: a cheap SDR is sufficient.

our receiver is a proof-of-concept with super low range of ~5m — nothing to compare with the Aeroscope range of 20km+. but it shows that there is no encryption whatsoever.

2/n

encryption isn't "missing" really: Drone-ID is considered a safety feature for consumer drones, compromising on pilot location privacy. next year, all drones sold in EU and US require remote identification through WiFi + BT.

3/n

consumer drones broadcast GPS data, now and in the foreseeable future. but we think AWARENESS for this feature (and the data sent) is incredibly important.

4/4

Tivitiko - The most beautiful shape of tweets!

Continue to read: <https://tivitiko.herokuapp.com/thread/IL4knF.html>