Drone Security and the Mysterious Case of DJI's DroneID

Nico Schiller*, Merlin Chlosta†, Moritz Schloegel*, Nils Bars*,
Thorsten Eisenhofer*, Tobias Scharnowski*, Felix Domke‡,
Lea Schönherr†, and Thorsten Holz†

A

Presented by Donghyo Bang

Introduction

- Mainstream product
- High popularity

Introduction

- Mainstream product
- High popularity

- Disturb air traffic
- Expensive shutdowns

Introduction

- Mainstream product
- High popularity

- Disturb air traffic
- Expensive shutdowns

- Smuggling
- Bypass physical barriers

Introduction

- Mainstream product
- High popularity

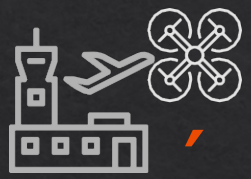
- Disturb air traffic
- Expensive shutdowns

- Smuggling
- Bypass physical barriers

Low entry barrier for air mobility in a *traditionally heavily* regulated sector!

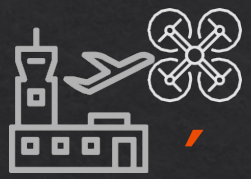
Introduction

Vendors know these problems!



Introduction

Vendors know these problems!

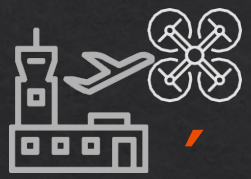


Position tracking

DJI Aeroscope

Introduction

Vendors know these problems!

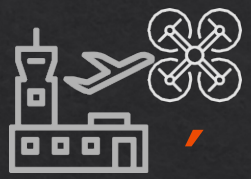


Position tracking
DJI Aeroscope

Software limits
Geofencing

Introduction

Vendors know these problems!



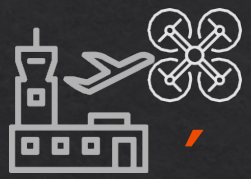
Position tracking
DJI Aeroscope

Software limits
Geofencing

Hardware protection
No debug interfaces

Introduction

Vendors know these problems!



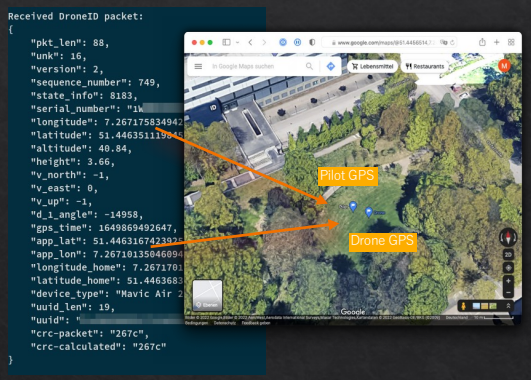
Position tracking
DJI Aeroscope

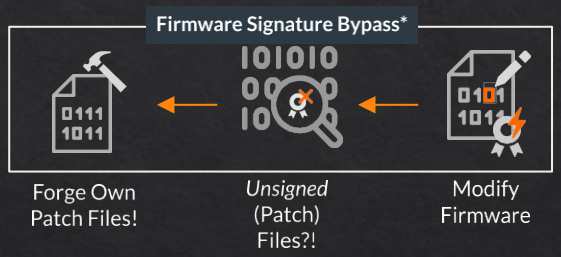
Software limits
Geofencing

Hardware protection
No debug interfaces

Are these countermeasures sufficiently implemented?

How to dissect complex systems?





ID	Oracle	Component	Observable Behavior	Classification	Severity	Remote	Vulnerable Devices
#1	ADB check	`dji_sys` binary	ADB started (root access)	arbitrary code exec	mid	✗	Mini 2
#2	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#3	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#4	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#5	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#6	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#7	crash	flight controller	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#8	crash	flight controller	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#9	crash	unknown	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#10	crash	unknown	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#11	crash	unknown	critical error (drone reboot)	denial of service	low	✓	Mini 2
#12	crash	unknown	critical error (drone reboot)	denial of service	low	✓	Mini 2
#13	crash	flight controller	critical error (drone reboot)	denial of service	low	✓	Mavic Air 2
#14	UI change	WiFi chip	change SSID	arbitrary code exec	mid	✓	Mini 2, Mavic 3
#15	UI change	flight controller	change serial number	identity spoofing	mid	✓	Mini 2

Drone and pilot's location tracking

Firmware signature verification bypass

Vulnerability detection via fuzzing

Wireless Analysis

Static Analysis

Dynamic Analysis

Why DJI Drones?

- Market share (94% Consumer)
- They take security seriously
  - Whitepaper
  - Bug bounty program
- Inconsistent statements about transmitted signals

Photo: Copyright dji.com

Introduction

TECH / DRONES / POLICY

DJI insisted drone-tracking AeroScope signals were encrypted – now it admits they aren't / The packets are in the air for anyone to grab

By Sean Hollister, a senior editor and founding member of The Verge who covers gadgets, games, and toys. He spent 15 years editing the likes of CNET, Gizmodo, and Engadget.

Apr 29, 2022, 4:34 AM GMT+9

Wireless Physical Layer

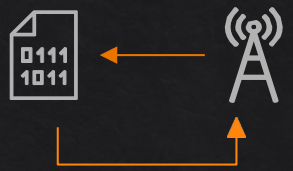
The Mysterious Case of DJI's DroneID

Static Analysis

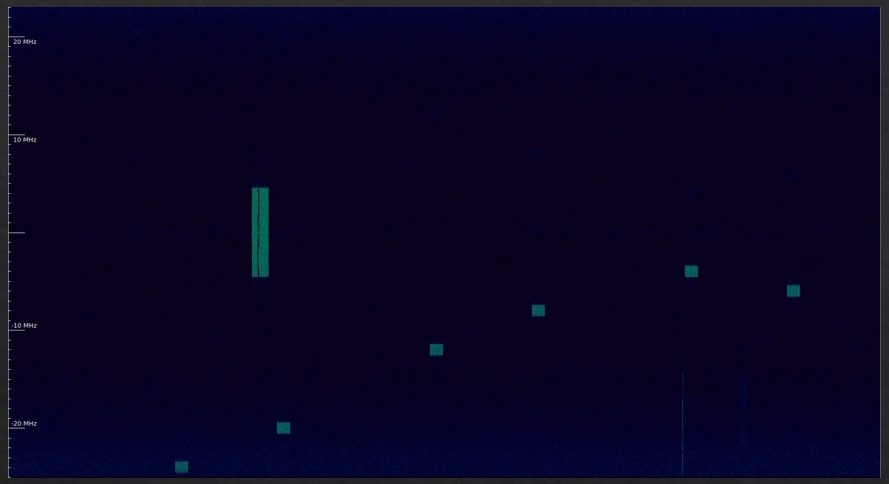
Hands on the Drone

Dynamic Analysis

Fuzzing Drones for Pain and Profit

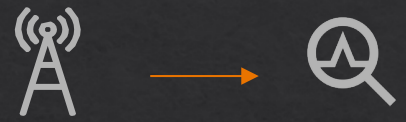


Listening on the Wireless Physical Layer …



Capture Raw
Signal Data

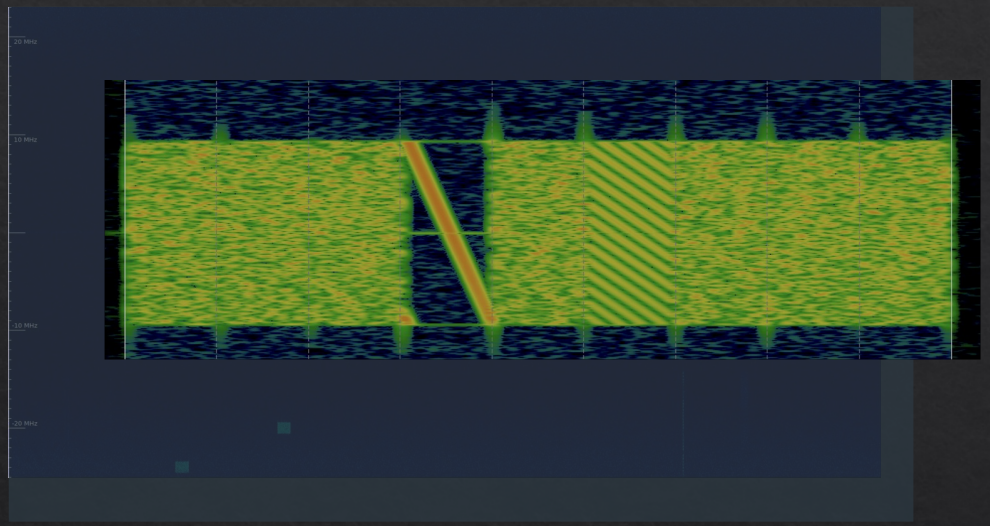
Listening on the Wireless Physical Layer …

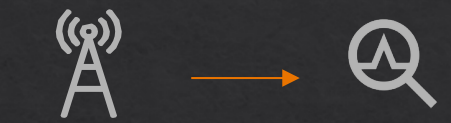


Capture Raw Signal Data

Packet Detection

Listening on the Wireless Physical Layer …

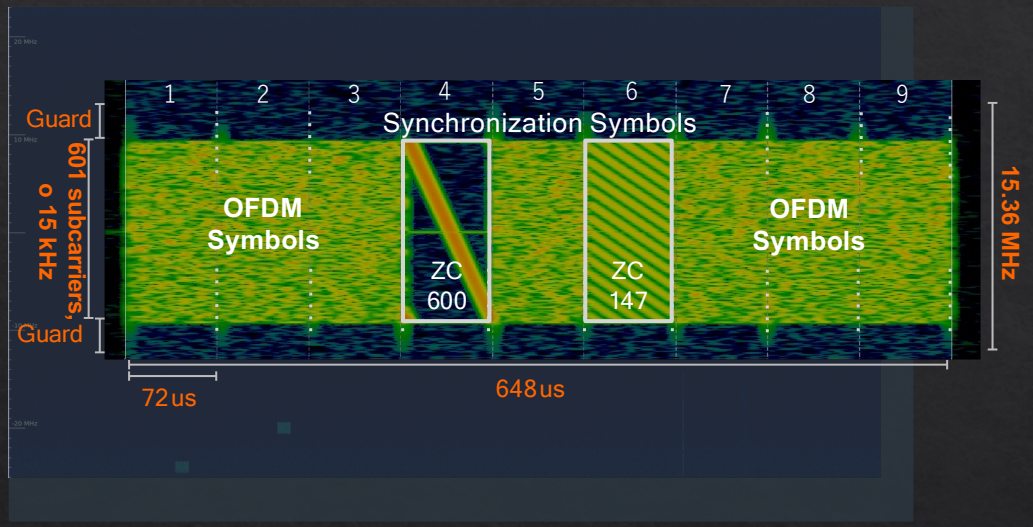


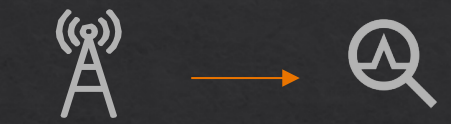


Capture Raw Signal Data

Packet Detection

Listening on the Wireless Physical Layer …

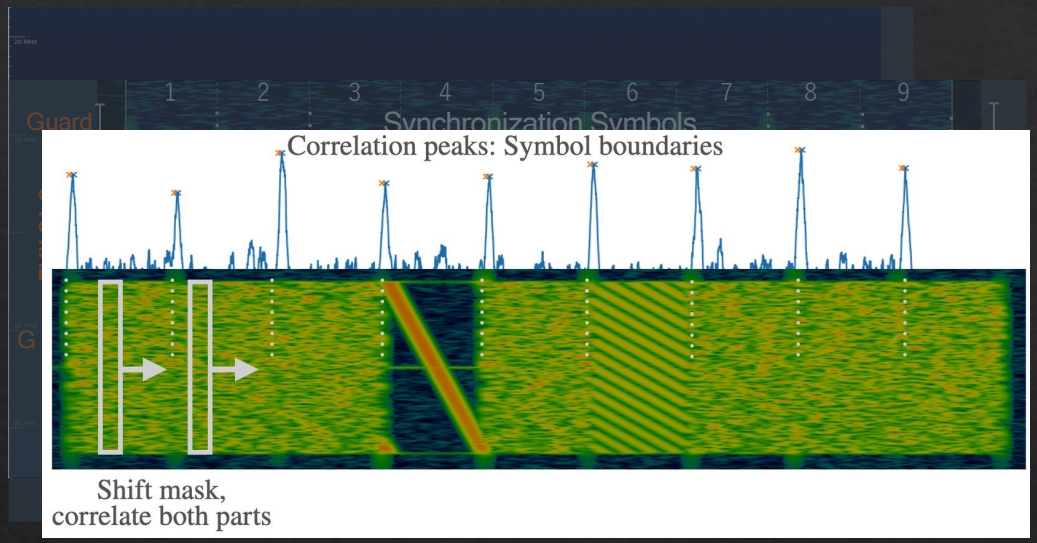


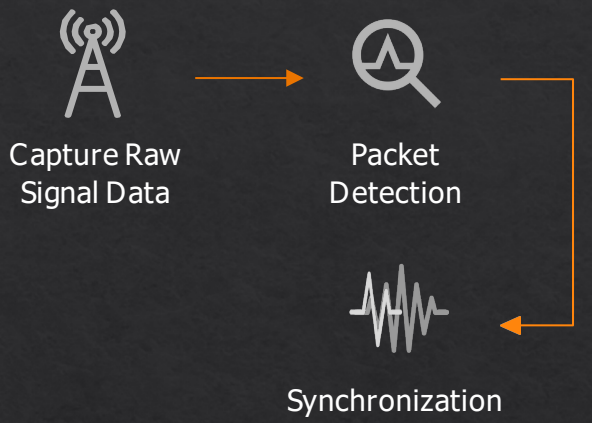


Capture Raw Signal Data

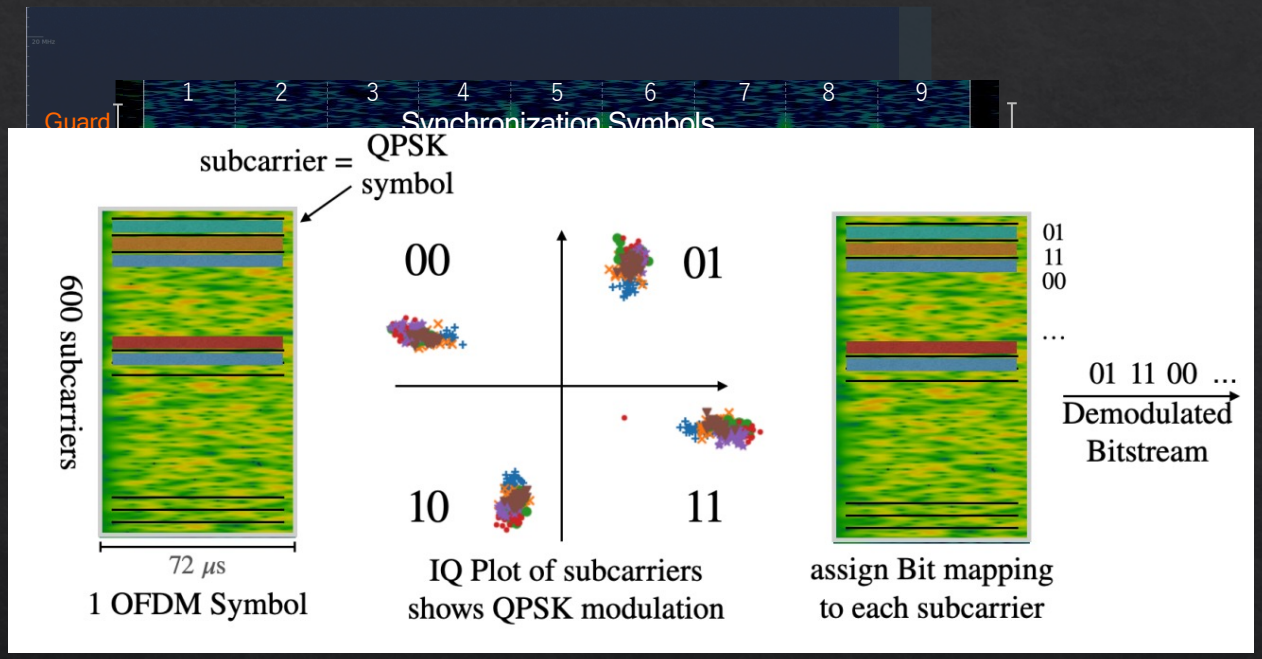
Packet Detection

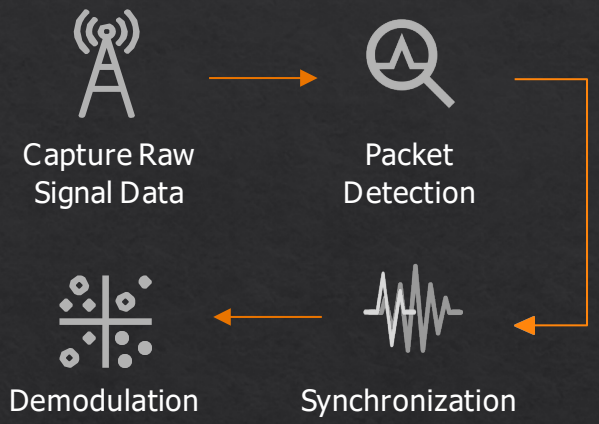
Listening on the Wireless Physical Layer …



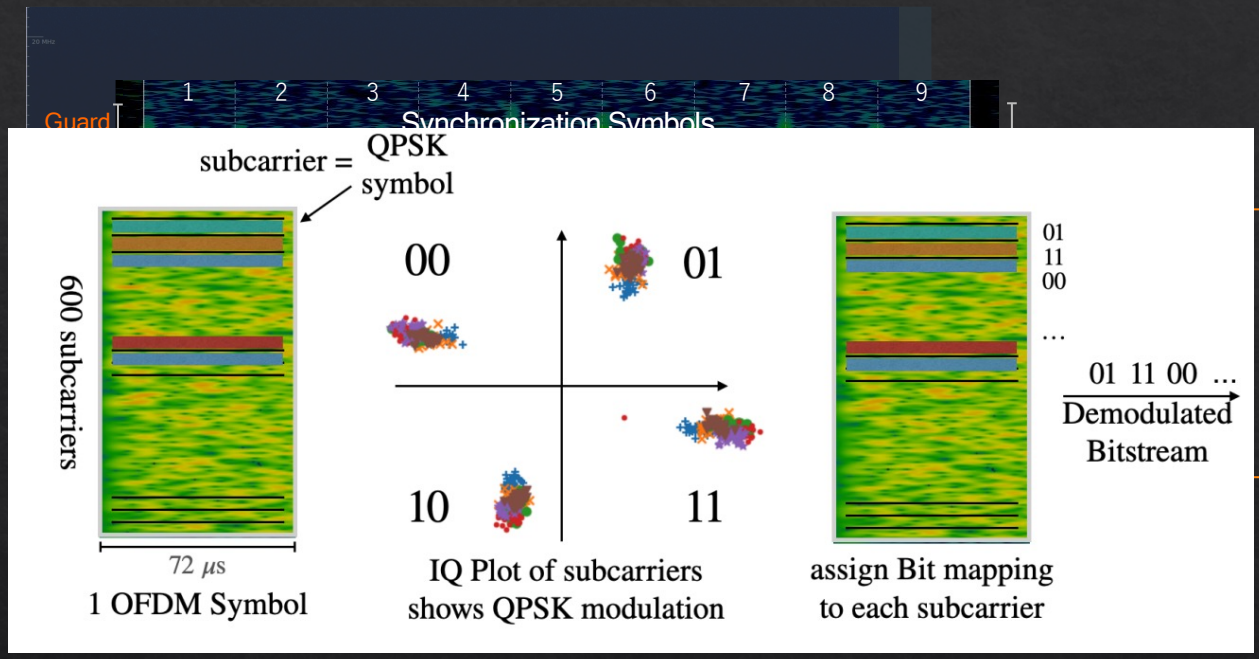


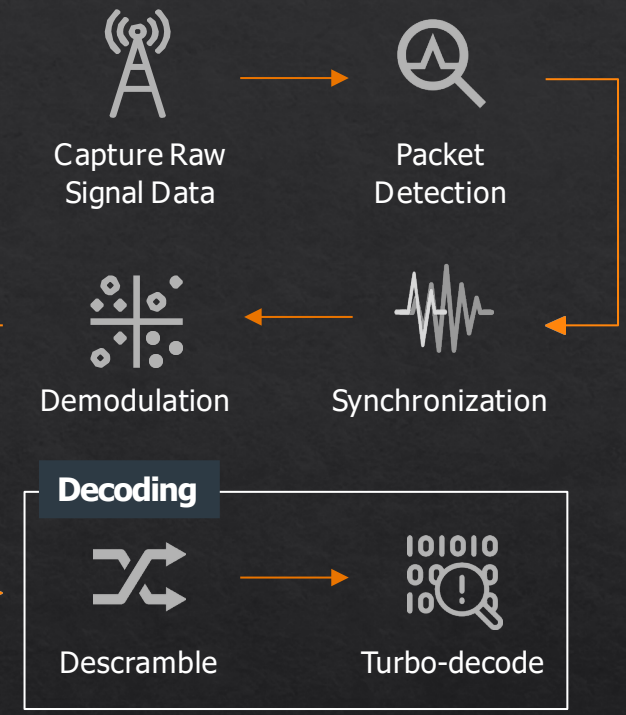
Listening on the Wireless Physical Layer …





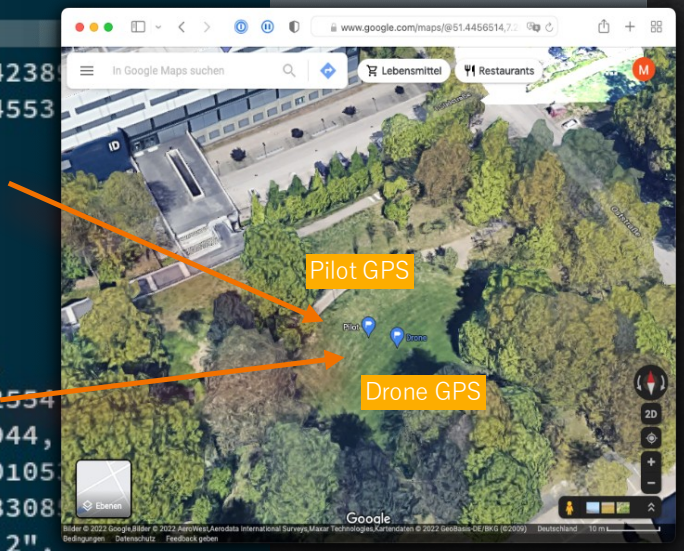
Listening on the Wireless Physical Layer …

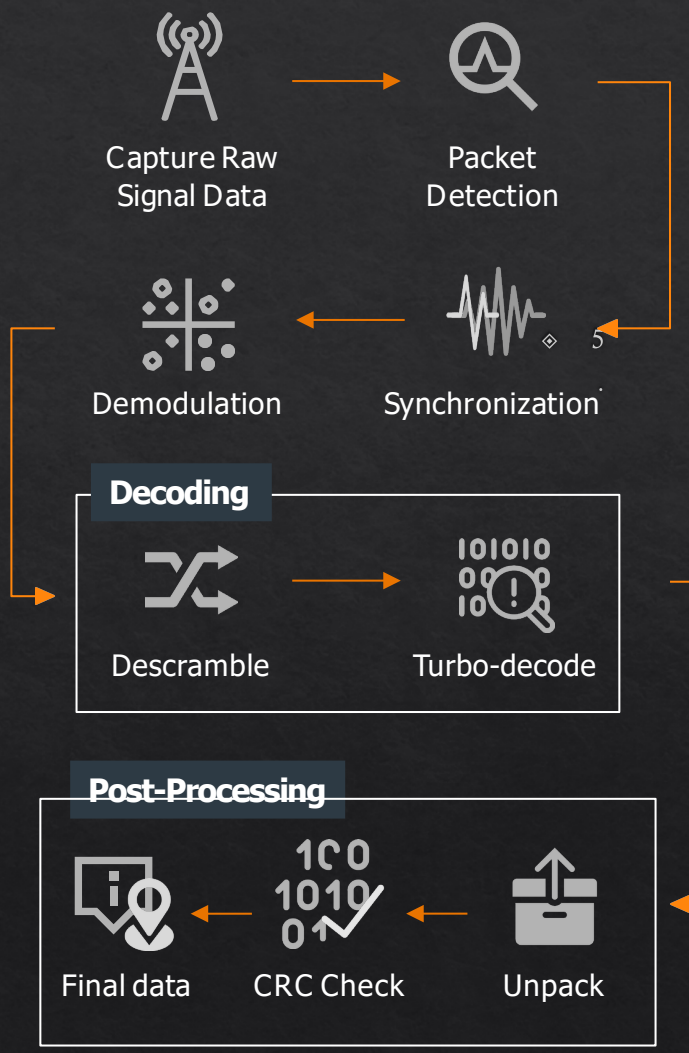




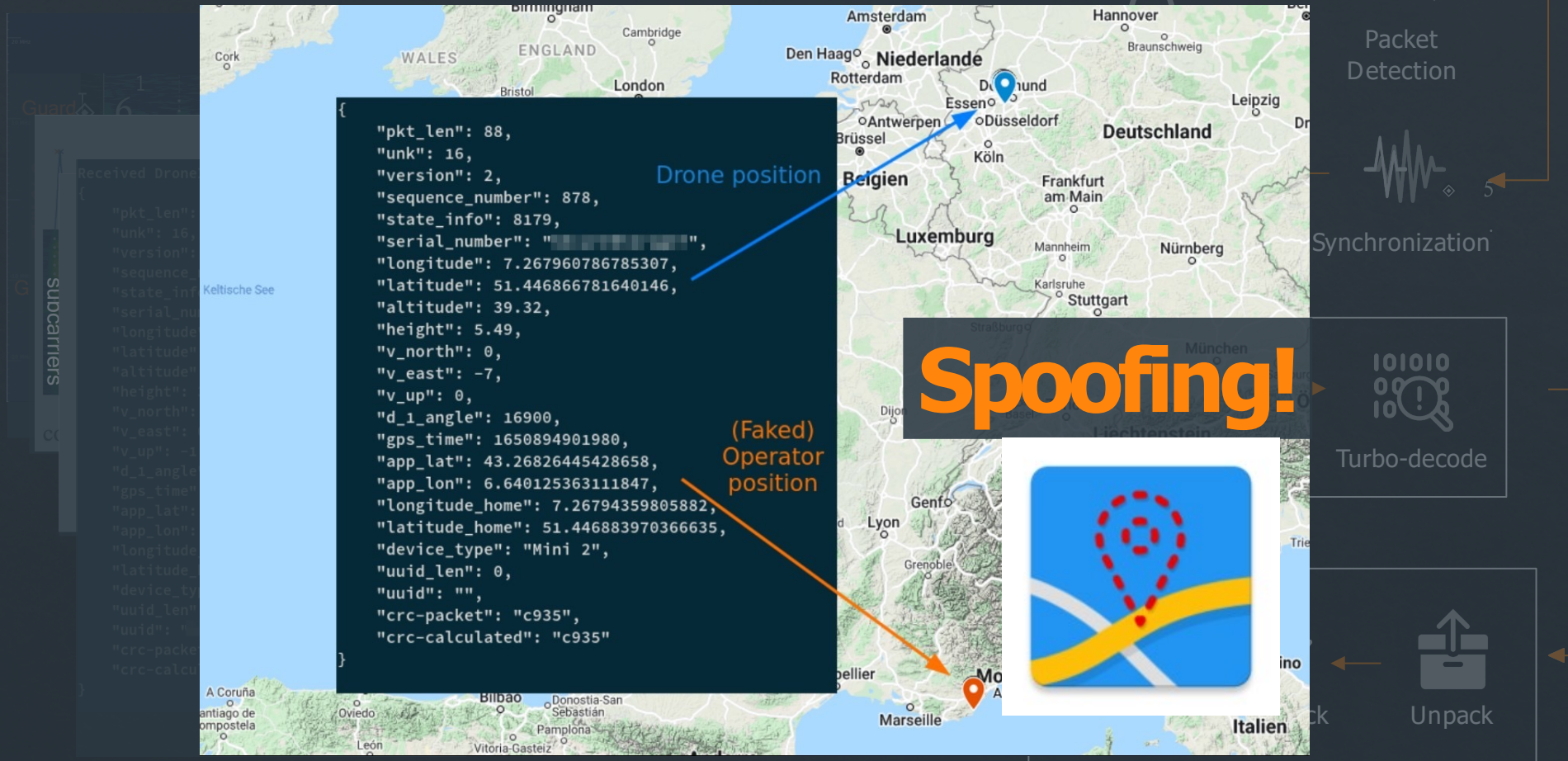
Listening on the Wireless Physical Layer ...


```
Received DroneID packet:
{
    "pkt_len": 88,
    "unk": 16,
    "version": 2,
    "sequence_number": 749,
    "state_info": 8183,
    "serial_number": "1W
    "longitude": 7.26717583494238
    "latitude": 51.44635111984553
    "altitude": 40.84,
    "height": 3.66,
    "v_north": -1,
    "v_east": 0,
    "v_up": -1,
    "d_1_angle": -14958,
    "gps_time": 1649869492647,
    "app_lat": 51.446316742392554
    "app_lon": 7.267101350460944,
    "longitude_home": 7.267170105
    "latitude_home": 51.446368308
    "device_type": "Mavic Air 2",
    "uuid_len": 19,
    "uuid": "                    ",
    "crc-packet": "267c",
    "crc-calculated": "267c"
}
```



Listening on the Wireless Physical Layer …



Wireless Physical Layer

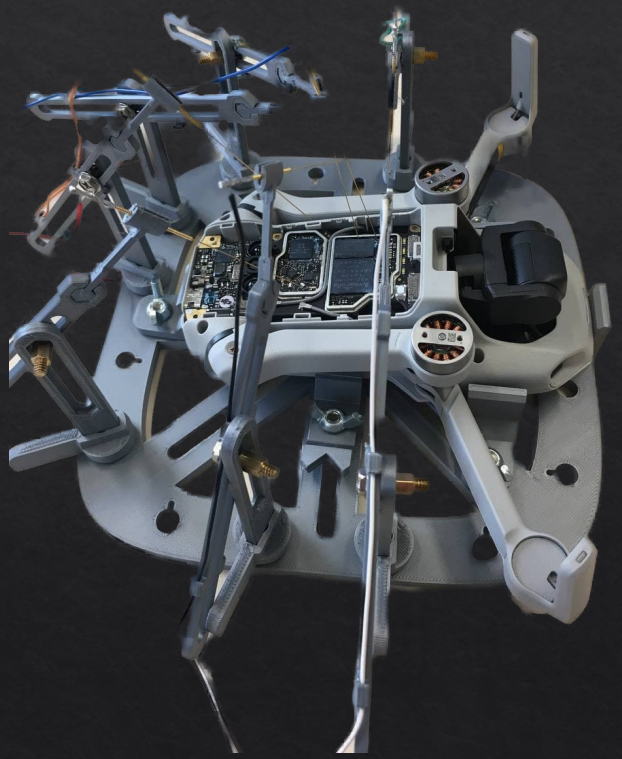
The Mysterious Case of DJI's DroneID

Static Analysis

Hands on the Drone

Dynamic Analysis

Fuzzing Drones for Pain and Profit



Analyze
PCB

Analyze
PCB

Found
Boot Screen
(UART)!

Analyze PCB

Found Boot Screen (UART)!

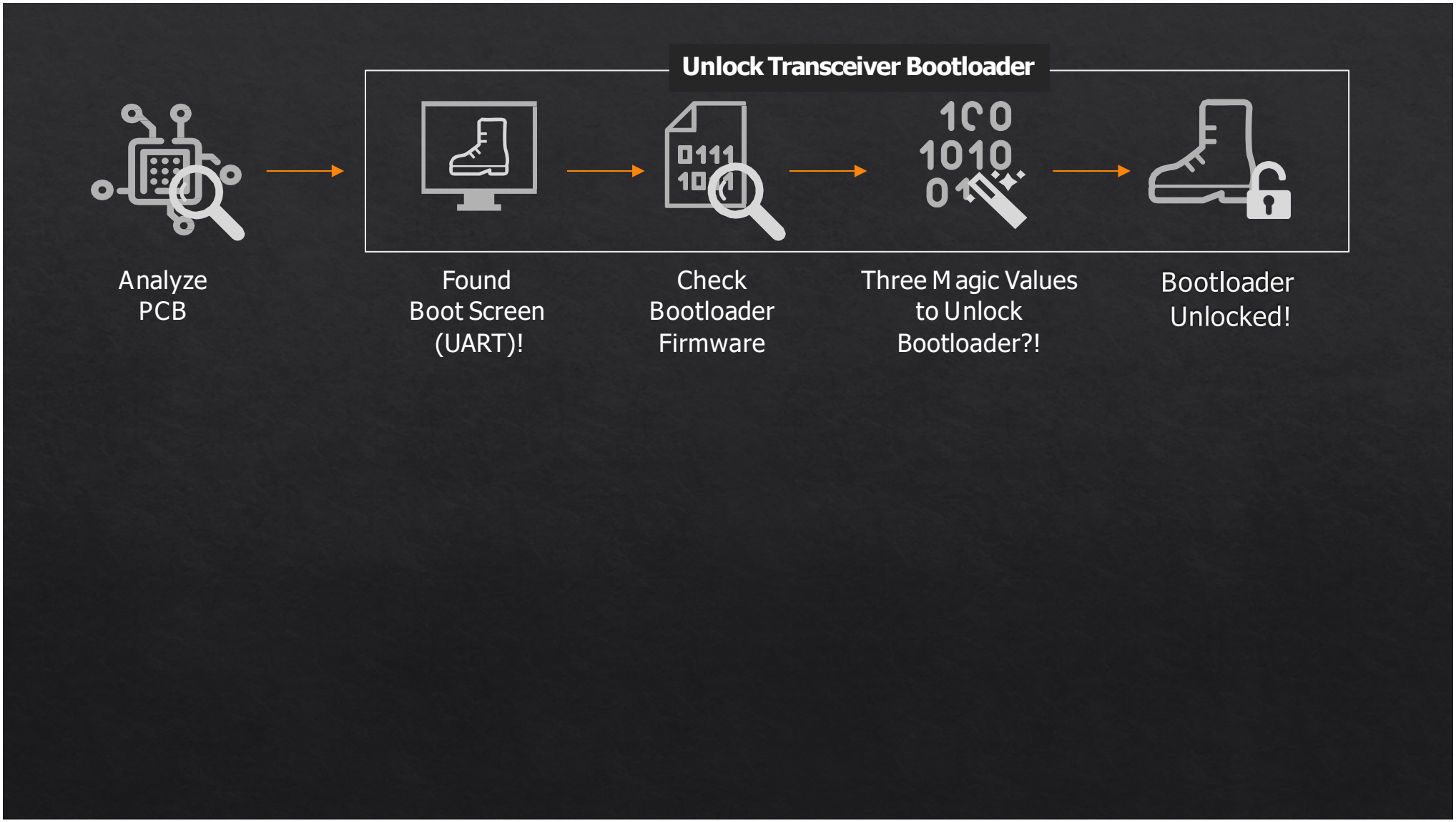
Check Bootloader Firmware

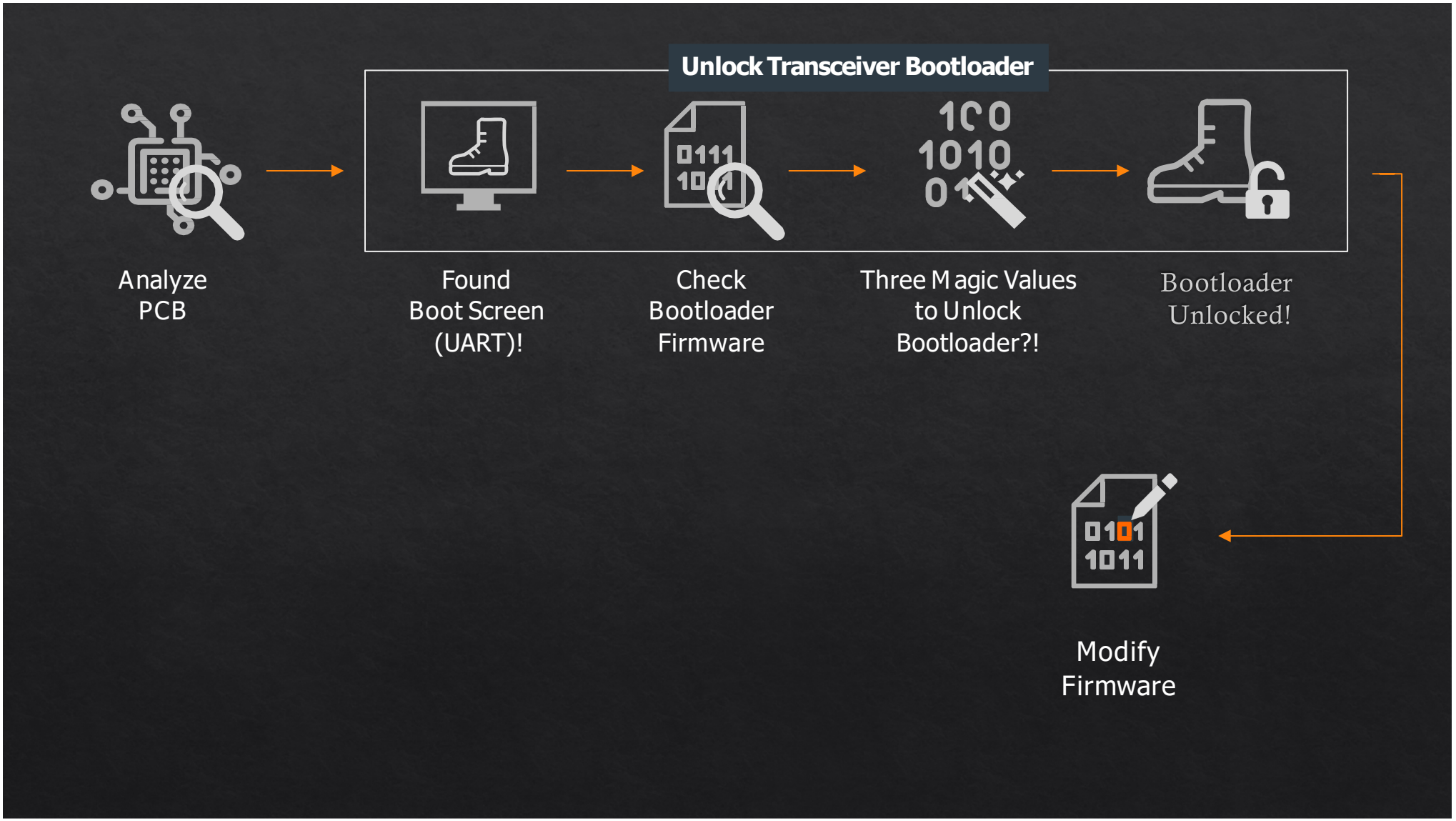
Analyze PCB

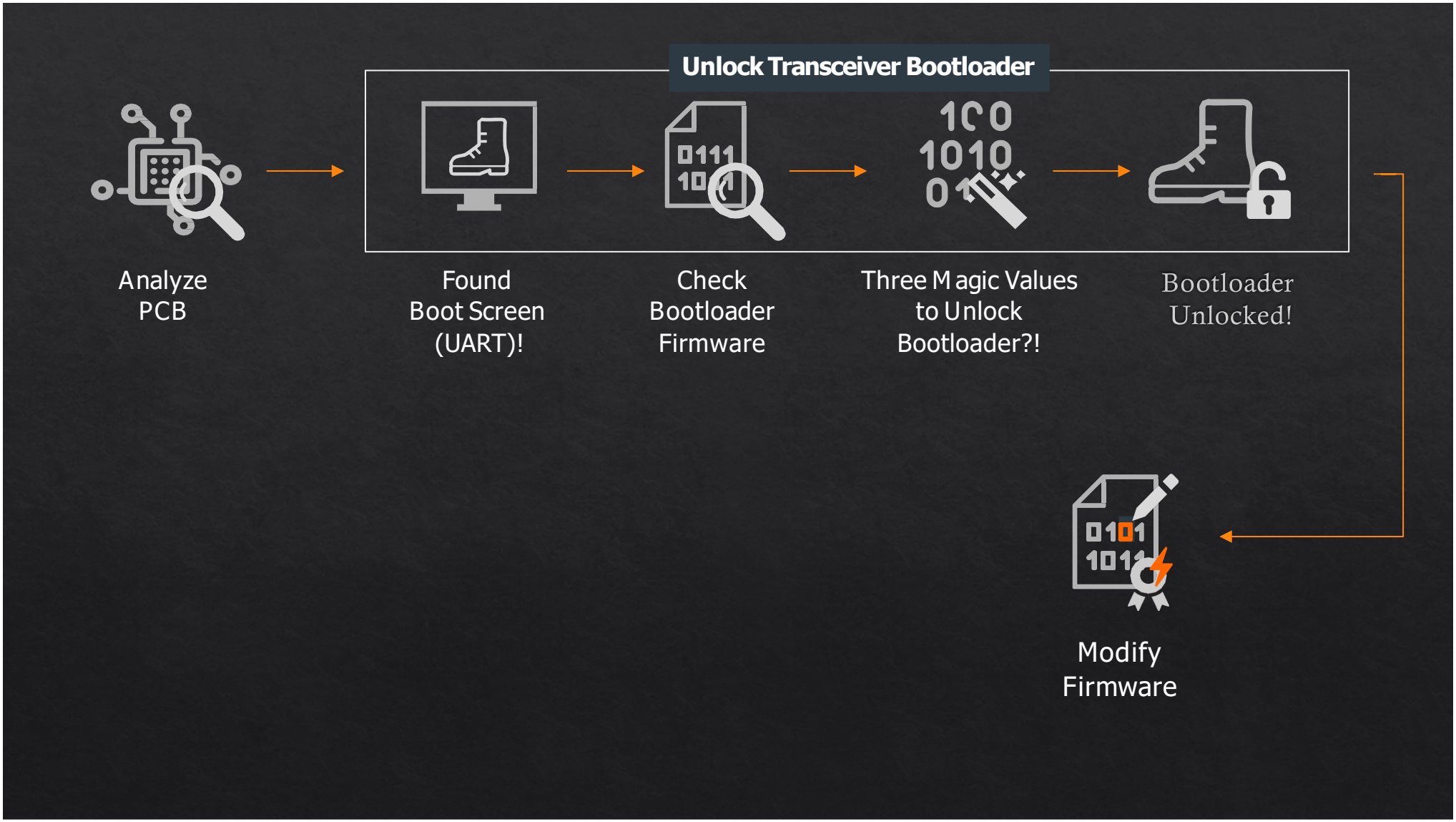
Found Boot Screen (UART)!

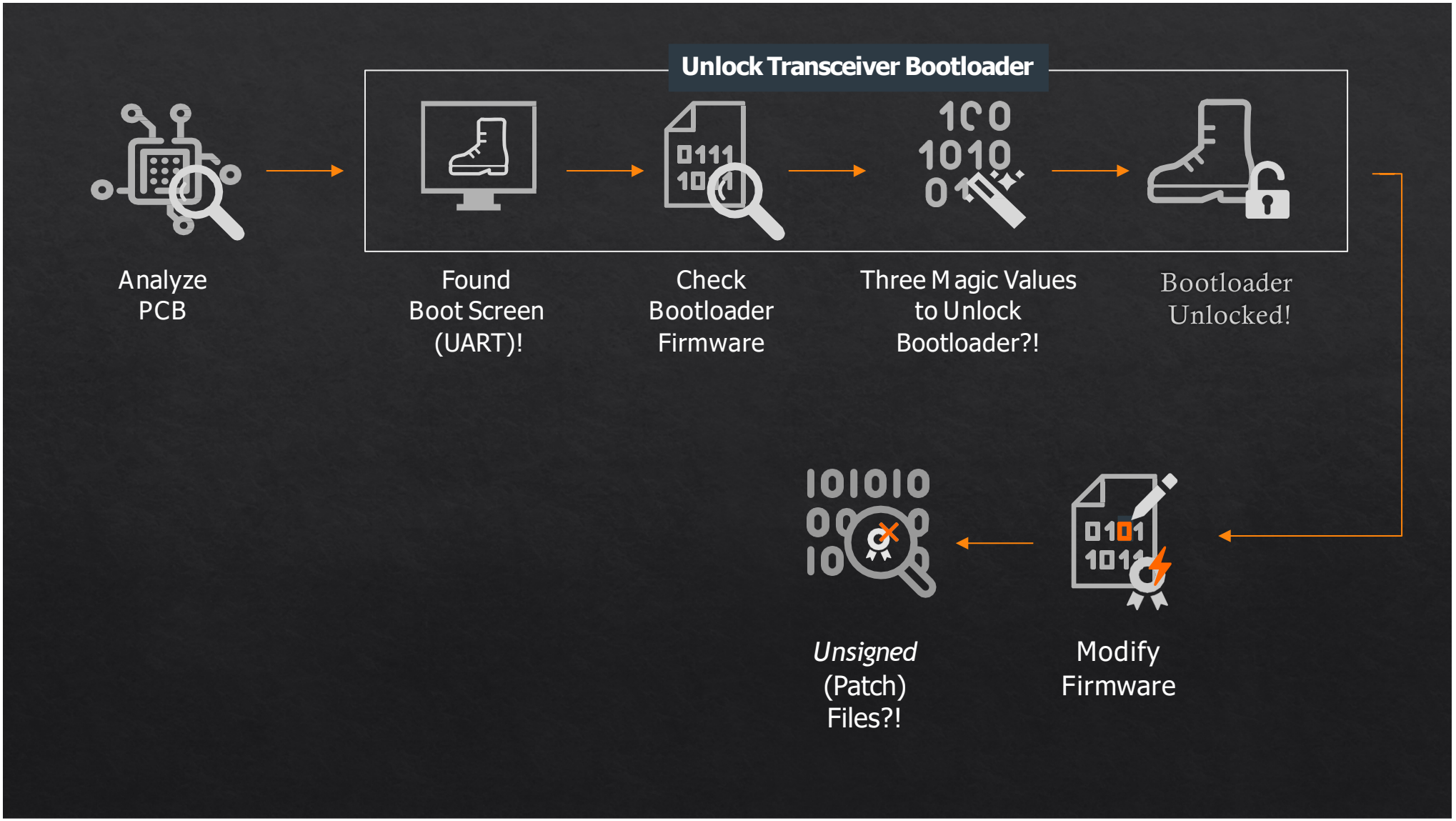
Check Bootloader Firmware

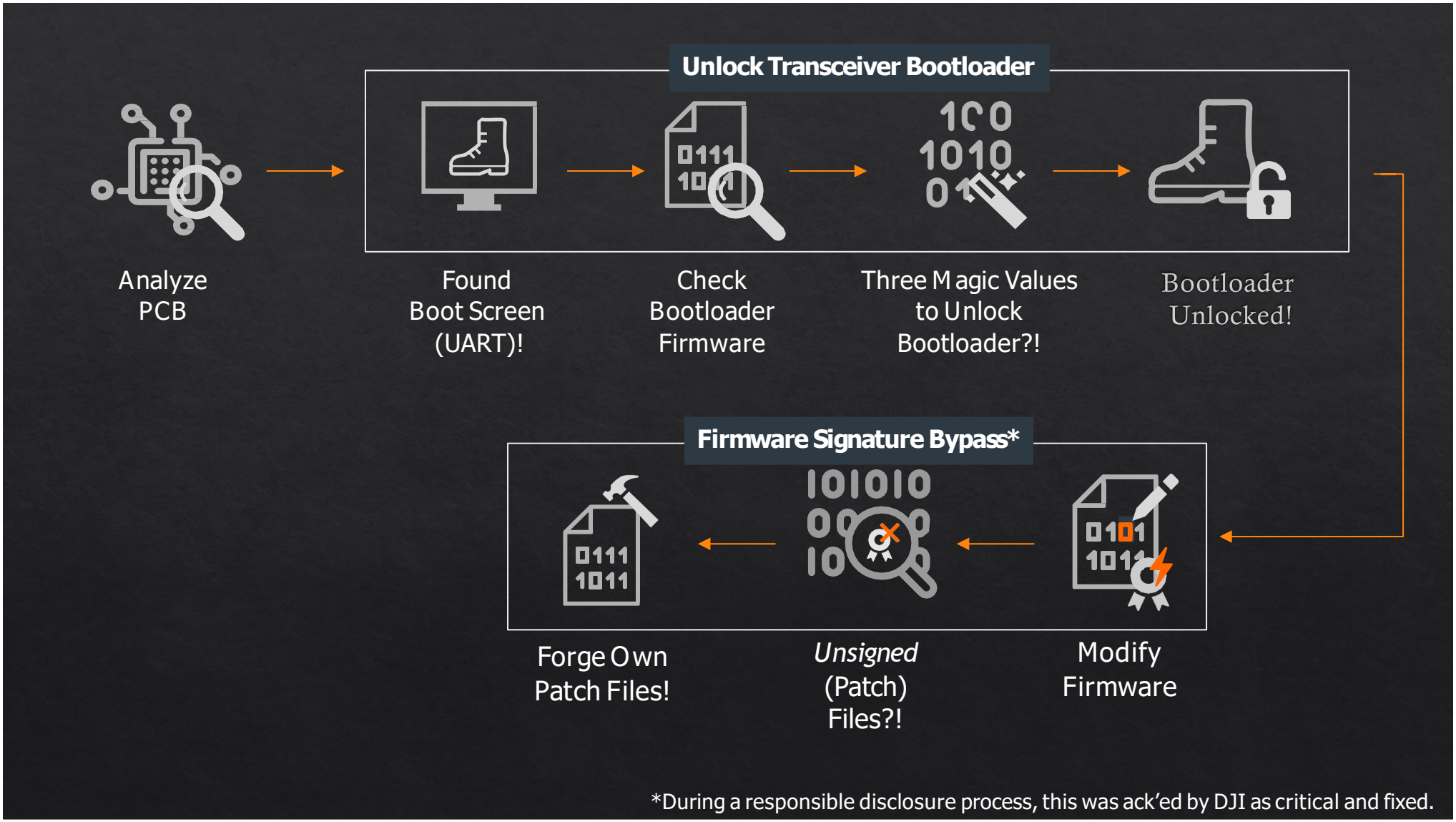
Three Magic Values to Unlock Bootloader?!

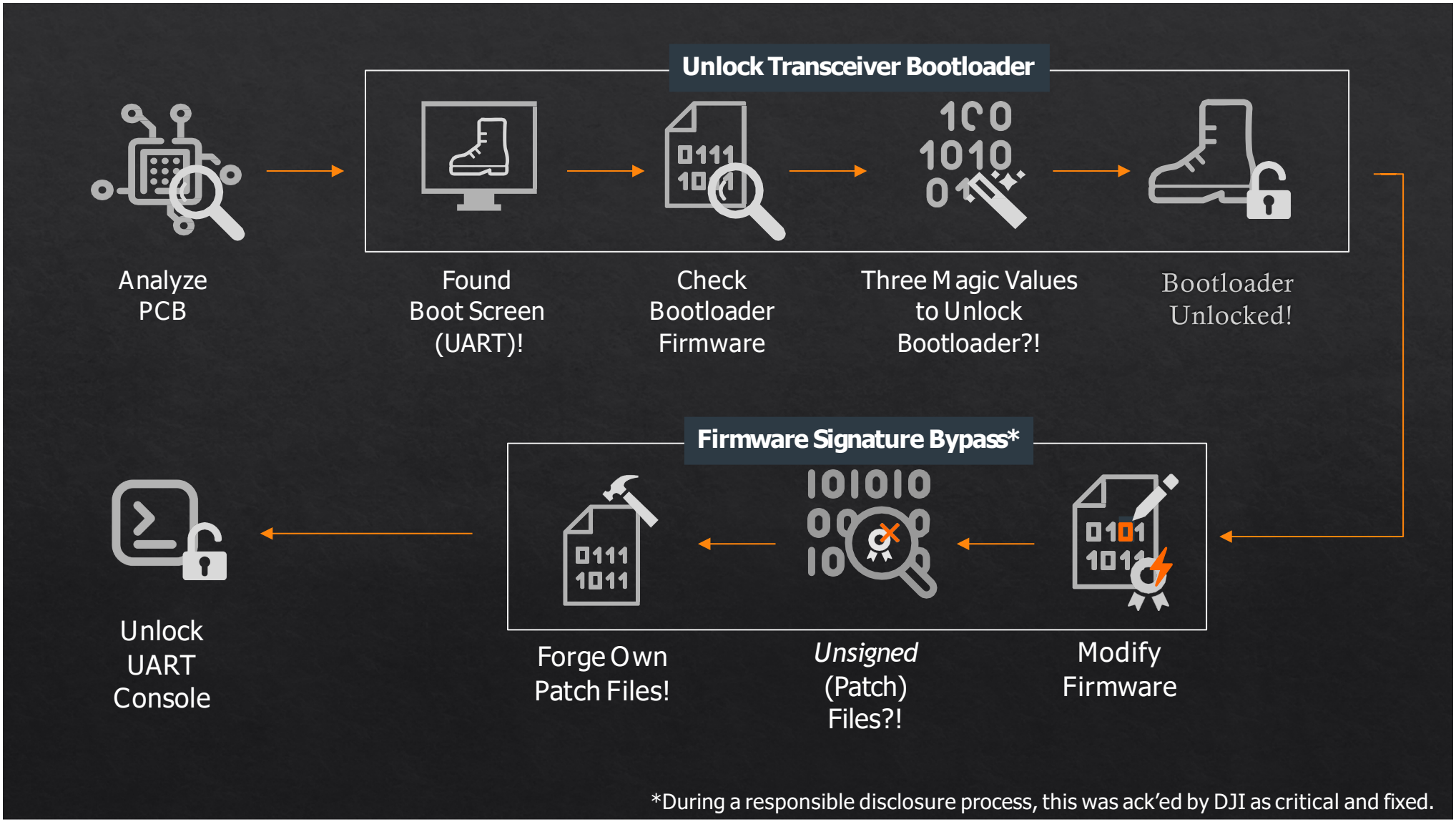

Unlock Transceiver Bootloader
Analyze PCB
Found Boot Screen (UART)!
Check Bootloader Firmware
Three Magic Values to Unlock Bootloader?!
Bootloader Unlocked!


Unlock Transceiver Bootloader
Analyze PCB
Found Boot Screen (UART)!
Check Bootloader Firmware
Three Magic Values to Unlock Bootloader?!
Bootloader Unlocked!
Modify Firmware


Unlock Transceiver Bootloader
Analyze PCB
Found Boot Screen (UART)!
Check Bootloader Firmware
Three Magic Values to Unlock Bootloader?!
Bootloader Unlocked!
Modify Firmware


Unlock Transceiver Bootloader
Analyze PCB
Found Boot Screen (UART)!
Check Bootloader Firmware
Three Magic Values to Unlock Bootloader?!
Bootloader Unlocked!
Modify Firmware
Unsigned (Patch) Files?!


Unlock Transceiver Bootloader
Analyze PCB
Found Boot Screen (UART)!
Check Bootloader Firmware
Three Magic Values to Unlock Bootloader?!
Bootloader Unlocked!
Firmware Signature Bypass*
Forge Own Patch Files!
Unsigned (Patch) Files?!
Modify Firmware
*During a responsible disclosure process, this was ack'ed by DJI as critical and fixed.


Unlock Transceiver Bootloader
Analyze PCB
Found Boot Screen (UART)!
Check Bootloader Firmware
Three Magic Values to Unlock Bootloader?!
Bootloader Unlocked!
Firmware Signature Bypass*
Unlock UART Console
Forge Own Patch Files!
Unsigned (Patch) Files?!
Modify Firmware
*During a responsible disclosure process, this was ack'ed by DJI as critical and fixed.

Wireless Physical Layer

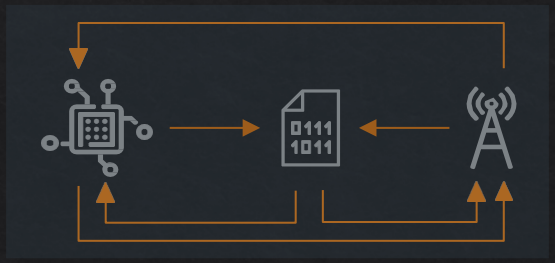
The Mysterious Case of DJI's DroneID

Static Analysis

Hands on the Drone

Dynamic Analysis

Fuzzing Drones for Pain and Profit



How to Fuzz R*eal* Drones?

How to Fuzz R*eal* Drones?

Fuzzer

Prerequisites:

- A drone and fuzzer

How to Fuzz R*eal* Drones?

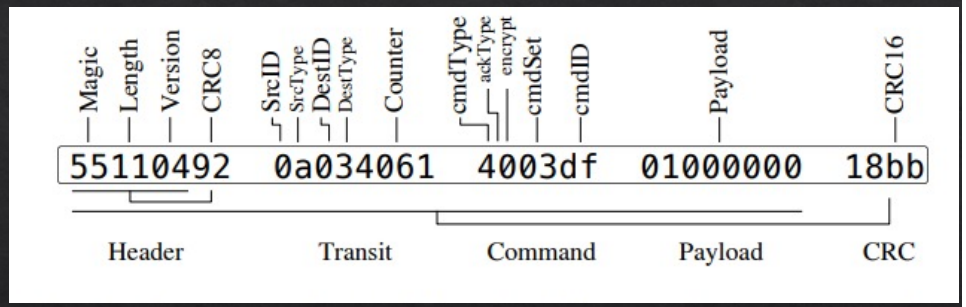
Prerequisites:

- A drone and fuzzer

How to Fuzz R*eal* Drones?

Prerequisites:

- A drone and fuzzer
- Protocol knowledge



DUML protocol

How to Fuzz *Real* Drones?

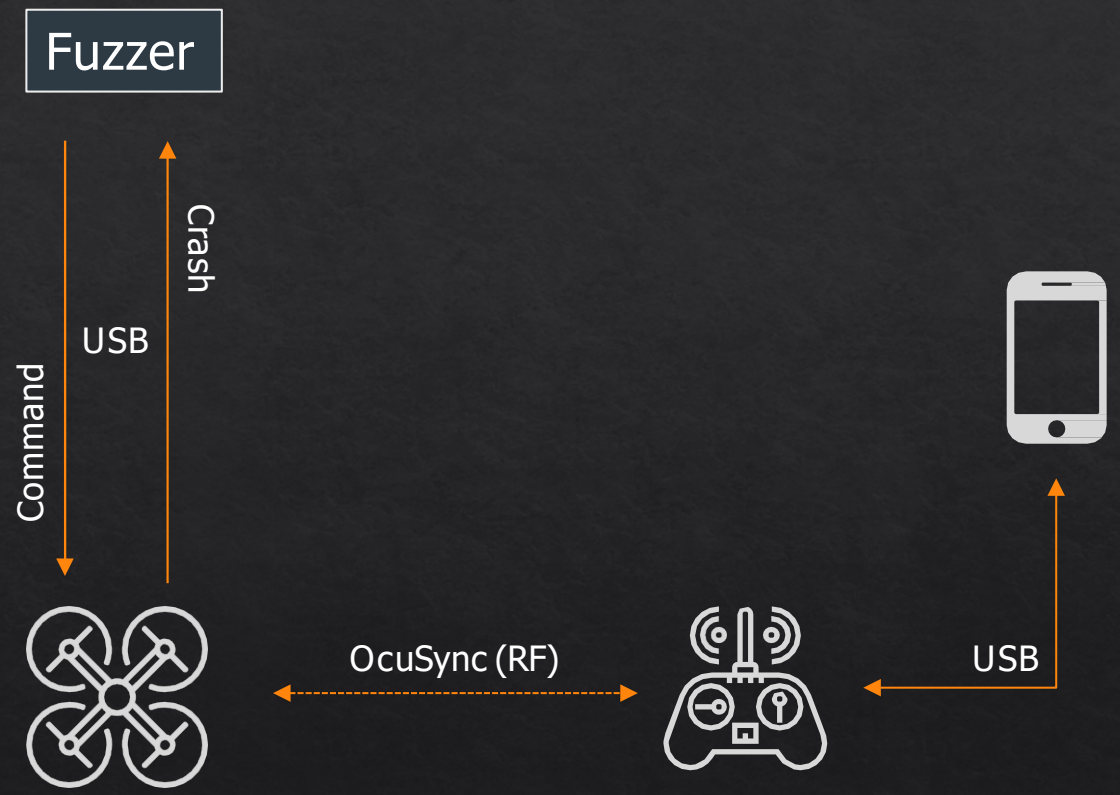
Prerequisites:

- A drone and fuzzer
- Protocol knowledge
- Bug oracle

How to Fuzz *Real* Drones?

Prerequisites:

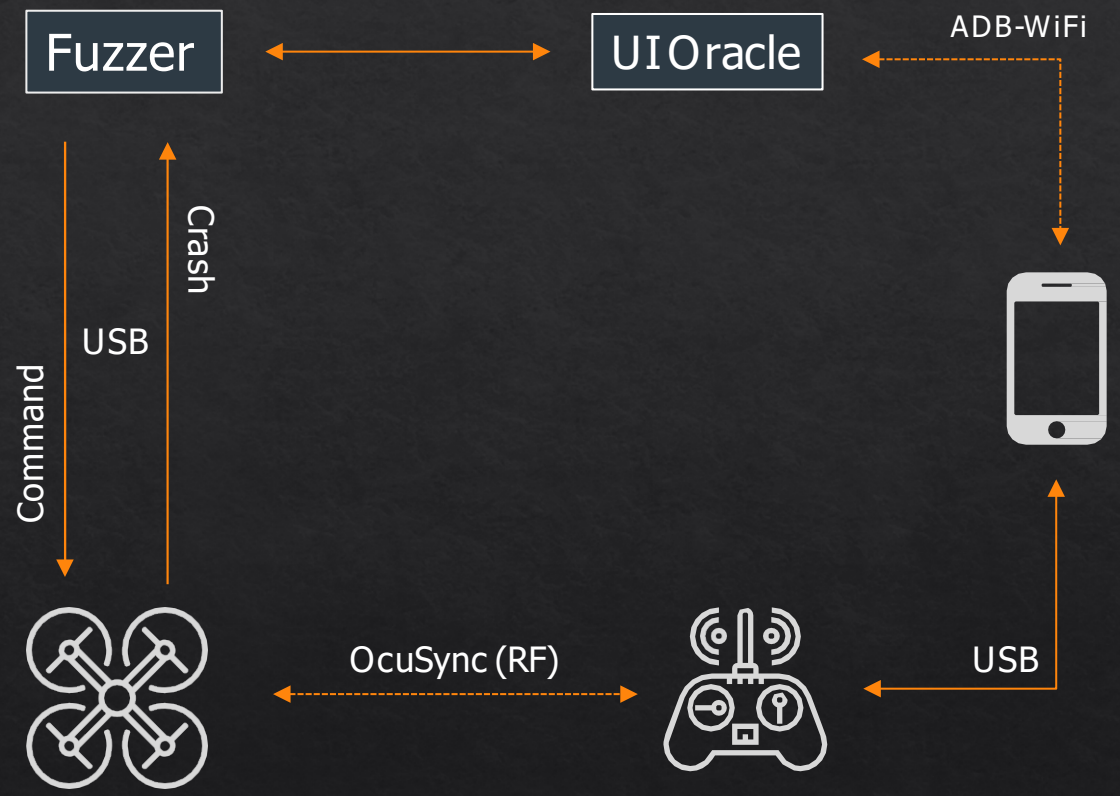
- A drone and fuzzer
- Protocol knowledge
- Bug oracle



How to Fuzz *Real* Drones?

Prerequisites:

- A drone and fuzzer
- Protocol knowledge
- Bug oracle

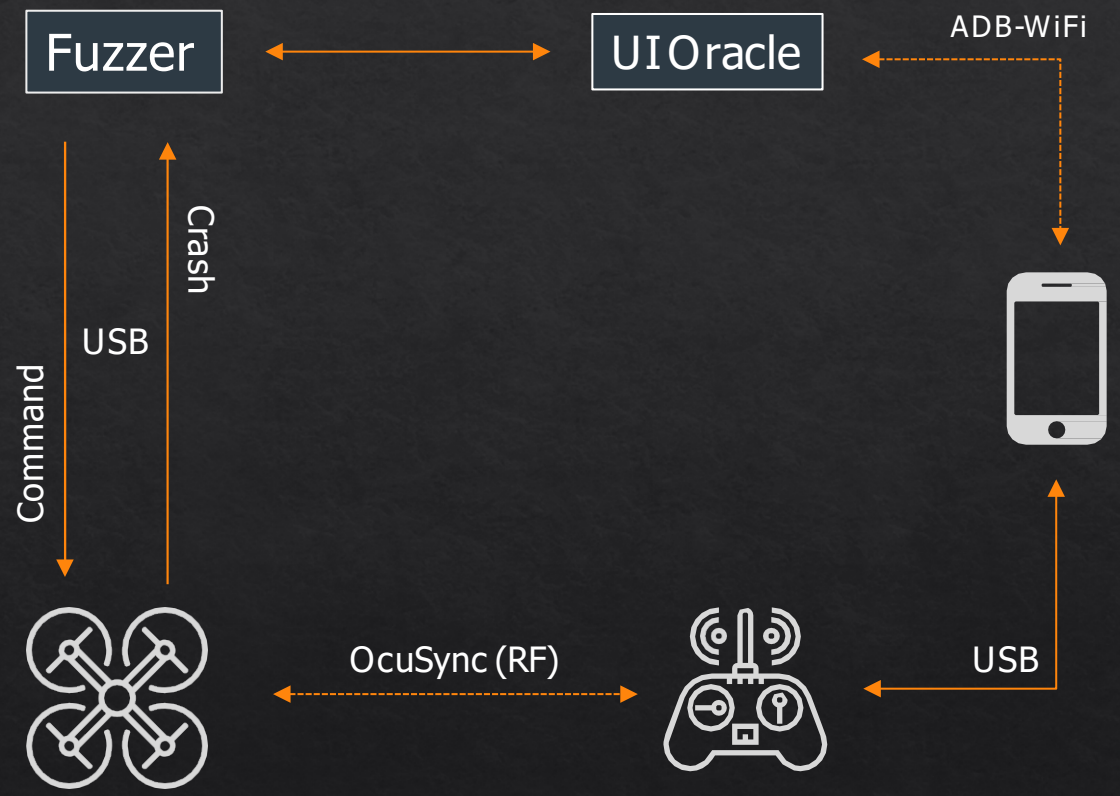


How to Fuzz *Real* Drones?

Prerequisites:

- A drone and fuzzer
- Protocol knowledge
- Bug oracle

Reproducible bugs!



Did fuzzing work?

ID	Oracle	Component	Observable Behavior	Classification[a]	Severity[a]	Remote[b]	Vulnerable Devices
#1	ADB check	`dji_sys` binary	ADB started (root access)	arbitrary code exec	mid	✗	Mini 2
#2	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#3	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#4	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#5	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#6	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#7	crash	flight controller	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#8	crash	flight controller	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#9	crash	unknown[c]	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#10	crash	unknown[c]	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#11	crash	unknown[c]	critical error (drone reboot)	denial of service	low	✓	Mini 2
#12	crash	unknown[c]	critical error (drone reboot)	denial of service	low	✓	Mini 2
#13	crash	flight controller	critical error (drone reboot)	denial of service	low	✓	Mavic Air 2
#14	UI change	WiFi chip	change SSID	arbitrary code exec	mid	✓	Mini 2, Mavic 3
#15	UI change	flight controller	change serial number	identity spoofing	mid	✓	Mini 2

*Following responsible disclosure, DJI fixed these bugs.

Did fuzzing work?

ID	Oracle	Component	Observable Behavior	Classification[a]	Severity[a]	Remote[b]	Vulnerable Devices
#1	ADB check	`dji_sys` binary	ADB started (root access)	arbitrary code exec	mid	✗	Mini 2
#2	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#3	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#4	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#5	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#6	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#7	crash	flight controller	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#8	crash	flight controller	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#9	crash	unknown[c]	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#10	crash	unknown[c]	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#11	crash	unknown[c]	critical error (drone reboot)	denial of service	low	✓	Mini 2
#12	crash	unknown[c]	critical error (drone reboot)	denial of service	low	✓	Mini 2
#13	crash	flight controller	critical error (drone reboot)	denial of service	low	✓	Mavic Air 2
#14	UI change	WiFi chip	change SSID	arbitrary code exec	mid	✓	Mini 2, Mavic 3
#15	UI change	flight controller	change serial number	identity spoofing	mid	✓	Mini 2

*Following responsible disclosure, DJI fixed these bugs.

Did fuzzing work?

ID	Oracle	Component	Observable Behavior	Classification[a]	Severity[a]	Remote[b]	Vulnerable Devices
#1	ADB check	`dji_sys` binary	ADB started (root access)	arbitrary code exec	mid	✗	Mini 2
#2	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#3	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#4	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#5	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#6	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#7	crash	flight controller	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#8	crash	flight controller	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#9	crash	unknown[c]	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#10	crash	unknown[c]	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#11	crash	unknown[c]	critical error (drone reboot)	denial of service	low	✓	Mini 2
#12	crash	unknown[c]	critical error (drone reboot)	denial of service	low	✓	Mini 2
#13	crash	flight controller	critical error (drone reboot)	denial of service	low	✓	Mavic Air 2
#14	UI change	WiFi chip	change SSID	arbitrary code exec	mid	✓	Mini 2, Mavic 3
#15	UI change	flight controller	change serial number	identity spoofing	mid	✓	Mini 2

*Following responsible disclosure, DJI fixed these bugs.

Did fuzzing work?

ID	Oracle	Component	Observable Behavior	Classification[a]	Severity[a]	Remote[b]	Vulnerable Devices
#1	ADB check	`dji_sys` binary	ADB started (root access)	arbitrary code exec	mid	✗	Mini 2
#2	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#3	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#4	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#5	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#6	crash	flight controller	critical error (drone reboot)	buffer overflow	mid	✓	Mavic Air 2
#7	crash	flight controller	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#8	crash	flight controller	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#9	crash	unknown[c]	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#10	crash	unknown[c]	critical error (drone reboot)	denial of service	mid	✓	Mini 2
#11	crash	unknown[c]	critical error (drone reboot)	denial of service	low	✓	Mini 2
#12	crash	unknown[c]	critical error (drone reboot)	denial of service	low	✓	Mini 2
#13	crash	flight controller	critical error (drone reboot)	denial of service	low	✓	Mavic Air 2
#14	UI change	WiFi chip	change SSID	arbitrary code exec	mid	✓	Mini 2, Mavic 3
#15	UI change	flight controller	change serial number	identity spoofing	mid	✓	Mini 2

*Following responsible disclosure, DJI fixed these bugs.

Conclusion

- DroneID decodable
  - Tool available
- DroneID can be spoofed / disabled

Position tracking

Conclusion

- DroneID decodable
  - Tool available
- DroneID can be spoofed / disabled

- Debugging interfaces enabled
- Firmware signature verification bypassed

Position tracking 

Hardware protection 

Conclusion

- DroneID decodable
  - Tool available
- DroneID can be spoofed / disabled

- Debugging interfaces enabled
- Firmware signature verification bypassed

- Fuzzing
  - 15 vulnerabilities (3 x low, 12 x medium)

Position tracking 

Hardware protection 

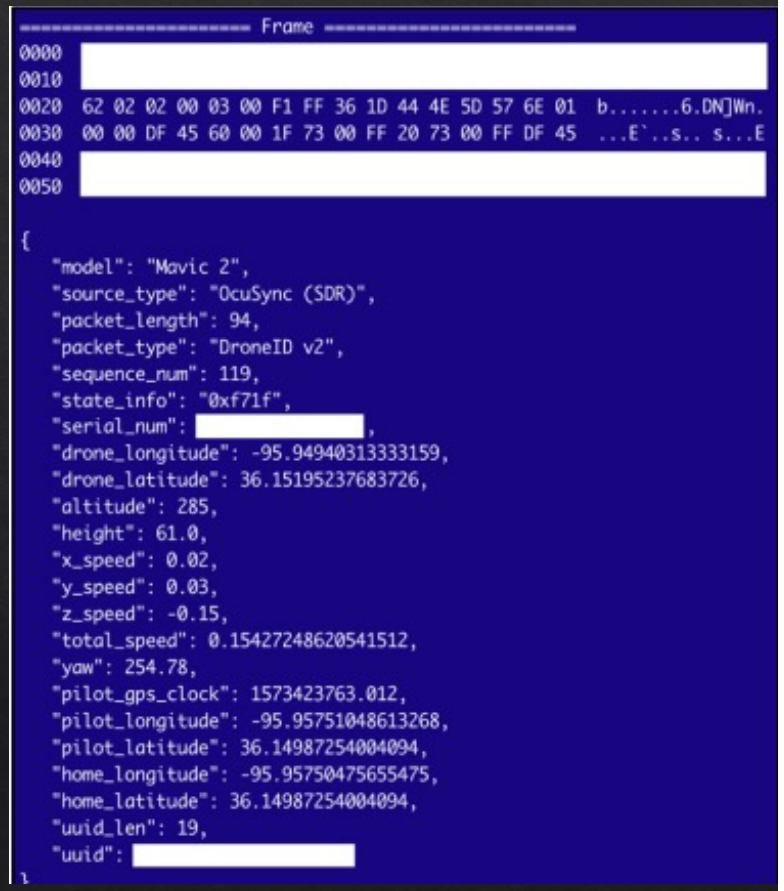
Software limits 

Future Work

- Active Attacker without Physical Access
- Data integrity
- Applicability to Other Vendors

Related Work

- T. T. synacktiv.com, “DJI Android GO 4 application security analysis, 2020
- F. Trujano, B. Chan, and R. R. May, “Security Analysis of DJI Phantom 3 Standard,” Massachusetts Institute of Technology, Tech. Rep., 2016.
- V. Dey, V. Pudi, A. Chattopadhyay, and Y. Elovici, “Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study,” 2018
- Conner Bender, “DJI drone IDs are not encrypted”, 2022



TECH

DJI drones, Ukraine, and Russia – what we know about AeroScope

Why DJI's drones are a hot-button issue in the Ukraine-Russia war

By **Sean Hollister**, a senior editor and founding member of The Verge who covers gadgets, games, and toys. He spent 15 years editing the likes of CNET, Gizmodo, and Engadget.

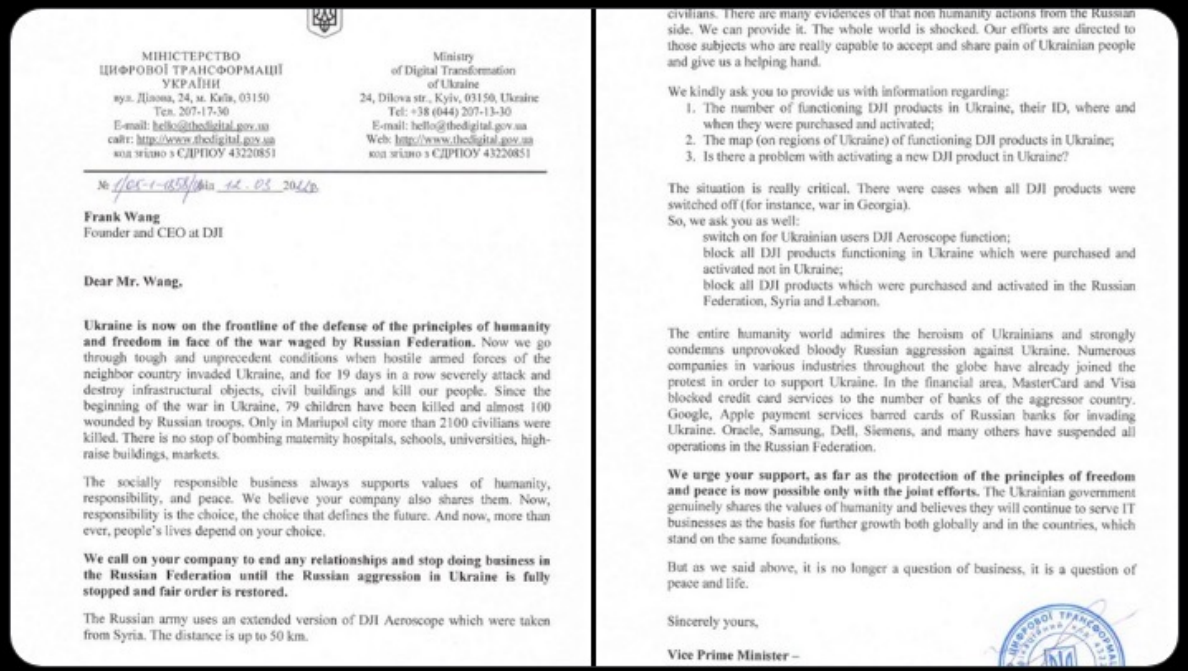
Mar 23, 2022, 7:00 PM GMT+9

Photography by Vjeran Pavic / Treatment by Alex Castro / The Verge

Mykhailo Fedorov
@FedorovMykhailo

In 21 days of the war, russian troops has already killed 100 Ukrainian children. they are using DJI products in order to navigate their missile. @DJIGlobal are you sure you want to be a partner in these murders? Block your products that are helping russia to kill the Ukrainians!

게시물 번역하기



МІНІСТЕРСТВО
ЦИФРОВОЇ ТРАНСФОРМАЦІЇ
УКРАЇНИ
вул. Ділова, 24, м. Київ, 03150
Тел. 207-17-30
E-mail: hello@thedigital.gov.ua
сайт: http://www.thedigital.gov.ua
код згідно з СДРПОУ 43220851

Ministry
of Digital Transformation
of Ukraine
24, Dilova str., Kyiv, 03150, Ukraine
Tel: +38 (044) 207-13-30
E-mail: hello@thedigital.gov.ua
Web: http://www.thedigital.gov.ua
код згідно з СДРПОУ 43220851

№ 1/05-1-853/dia 12.03 2022р.

Frank Wang
Founder and CEO at DJI

Dear Mr. Wang,

Ukraine is now on the frontline of the defense of the principles of humanity and freedom in face of the war waged by Russian Federation. Now we go through tough and unprecedent conditions when hostile armed forces of the neighbor country invaded Ukraine, and for 19 days in a row severely attack and destroy infrastructural objects, civil buildings and kill our people. Since the beginning of the war in Ukraine, 79 children have been killed and almost 100 wounded by Russian troops. Only in Mariupol city more than 2100 civilians were killed. There is no stop of bombing maternity hospitals, schools, universities, high-raise buildings, markets.

The socially responsible business always supports values of humanity, responsibility, and peace. We believe your company also shares them. Now, responsibility is the choice, the choice that defines the future. And now, more than ever, people's lives depend on your choice.

We call on your company to end any relationships and stop doing business in the Russian Federation until the Russian aggression in Ukraine is fully stopped and fair order is restored.

The Russian army uses an extended version of DJI Aeroscope which were taken from Syria. The distance is up to 50 km.

civilians. There are many evidences of that non humanity actions from the Russian side. We can provide it. The whole world is shocked. Our efforts are directed to those subjects who are really capable to accept and share pain of Ukrainian people and give us a helping hand.

We kindly ask you to provide us with information regarding:

1. The number of functioning DJI products in Ukraine, their ID, where and when they were purchased and activated;
2. The map (on regions of Ukraine) of functioning DJI products in Ukraine;
3. Is there a problem with activating a new DJI product in Ukraine?

The situation is really critical. There were cases when all DJI products were switched off (for instance, war in Georgia).
So, we ask you as well:

switch on for Ukrainian users DJI Aeroscope function;
block all DJI products functioning in Ukraine which were purchased and activated not in Ukraine;
block all DJI products which were purchased and activated in the Russian Federation, Syria and Lebanon.

The entire humanity world admires the heroism of Ukrainians and strongly condemns unprovoked bloody Russian aggression against Ukraine. Numerous companies in various industries throughout the globe have already joined the protest in order to support Ukraine. In the financial area, MasterCard and Visa blocked credit card services to the number of banks of the aggressor country. Google, Apple payment services barred cards of Russian banks for invading Ukraine. Oracle, Samsung, Dell, Siemens, and many others have suspended all operations in the Russian Federation.

We urge your support, as far as the protection of the principles of freedom and peace is now possible only with the joint efforts. The Ukrainian government genuinely shares the values of humanity and believes they will continue to serve IT businesses as the basis for further growth both globally and in the countries, which stand on the same foundations.

But as we said above, it is no longer a question of business, it is a question of peace and life.

Sincerely yours,

Vice Prime Minister –

Will DJI?

Will DJI?

Over four hundred companies have withdrawn from Russia in protest. Will DJI?

No.

"For 15 years, DJI has tried our best to stay out of geopolitics," says Lisberg.

Great Qs

- From a security perspective, "Security by Obscurity" is considered far from secure. However, generally speaking, when a significant amount of information is exposed, it also becomes easier for attackers to analyze the system. In this regard, is it always beneficial for companies like DJI to publish white papers regularly?

- Are there techniques to interfere with an attacker's spectrum analysis, such as having a drone emit random values across multiple frequencies simultaneously while transmitting meaningful data only on specific hopping frequencies?

- Would this research be useful for finding vulnerabilities on other manufacturers as the UI was specially developped for this?

Even Better Qs

- Taeha Kim:

- Eliminating all vulnerabilities in a product is largely impractical. Consequently, companies often make compromises, relying on the obscurity of protocols, system architecture, and other elements to some extent when releasing products. But to what degree should this compromise be made, and what standards should it fulfill?

- Sihun Yang

- What are the potential risks of attackers gaining control of geofencing restrictions through DUML vulnerabilities?

- Younghyo Kang

- To defend against attackers, adding a reasonable delay between input signals during fuzzing attempts on black-box devices can be effective in increasing the time required for an attacker to conduct their analysis. As long as this delay does not interfere with normal operations, it can help slow down brute-force or systematic fuzzing efforts, making it more time-consuming for the attacker to identify vulnerabilities