CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

RUHR UNIVERSITÄT BOCHUM RUB

Drone Security and the Mysterious Case of DJI's DroneID

Network and Distributed System Security (NDSS) Symposium
San Diego, 2023

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

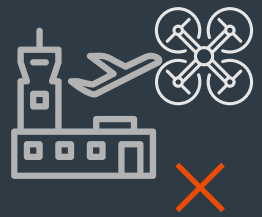
*Ruhr University Bochum
†CISPA Helmholtz Center for Information Security
‡Independent

Consumer Drones

- Mainstream product
- High popularity

Consumer Drones

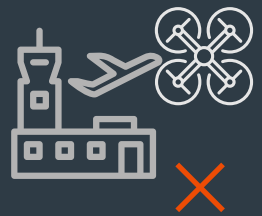
- Mainstream product
- High popularity



- Disturb air traffic
- Expensive shutdowns

Consumer Drones

- Mainstream product
- High popularity

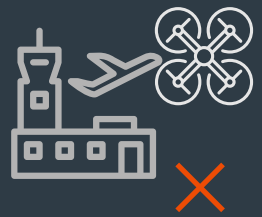


- Disturb air traffic
- Expensive shutdowns

- Smuggling
- Bypass physical barriers

Consumer Drones

- Mainstream product
- High popularity

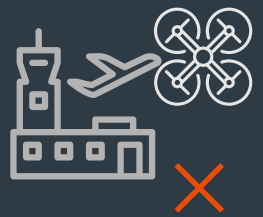


- Disturb air traffic
- Expensive shutdowns

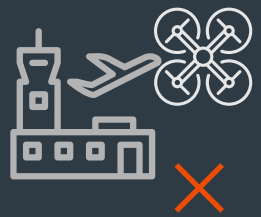
- Smuggling
- Bypass physical barriers

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

Vendors know these problems!



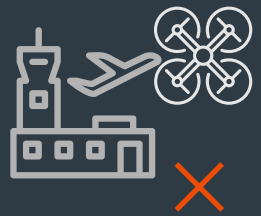
Vendors know these problems!



Position tracking

DJI Aeroscope

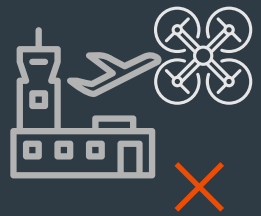
Vendors know these problems!



Position tracking
DJI Aeroscope

Software limits
Geofencing

Vendors know these problems!

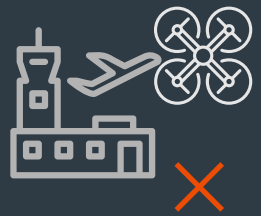


Position tracking
DJI Aeroscope

Software limits
Geofencing

Hardware protection
No debug interfaces

Vendors know these problems!



Position tracking
DJI Aeroscope

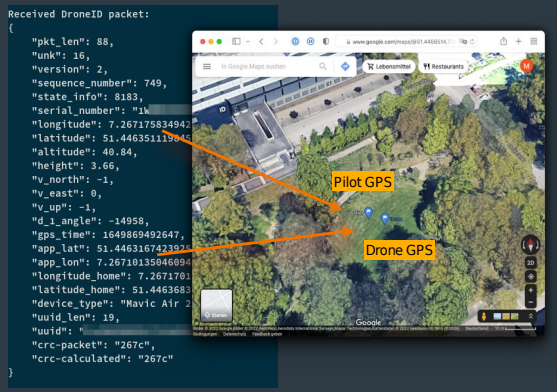
Software limits
Geofencing

Hardware protection
No debug interfaces

Are these countermeasures sufficiently implemented?

How to dissect complex systems?

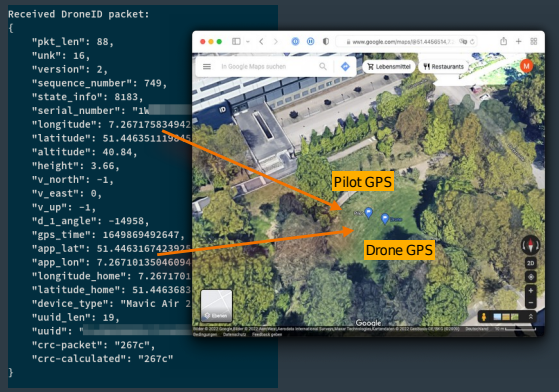
How to dissect complex systems?

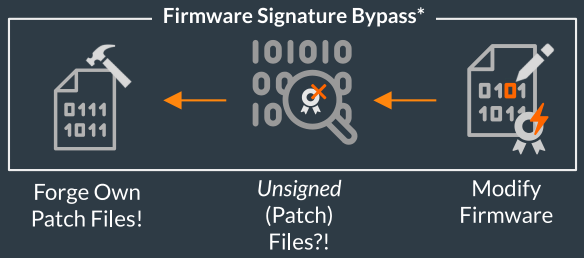


Drone and pilot’s location tracking

Wireless Analysis

How to dissect complex systems?





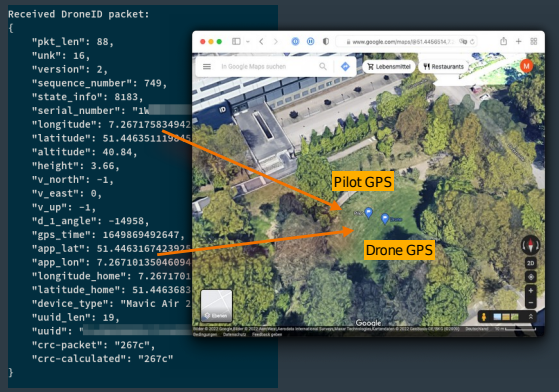
Drone and pilot's location tracking

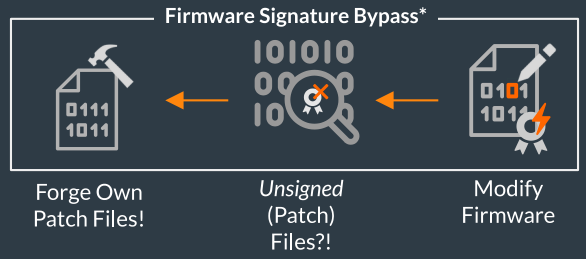
Firmware signature verification bypass

Wireless Analysis

Static Analysis

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

Our focus: DJI drones

Photo: Copyright dji.com

Our focus: DJI drones

- Market share (94% Consumer)

Our focus: DJI drones

- Market share (94% Consumer)
- They take security seriously
  - Whitepaper
  - Bug bounty program

Photo: Copyright dji.com

Our focus: DJI drones

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

Wireless Physical Layer

The Mysterious Case of DJI's DroneID

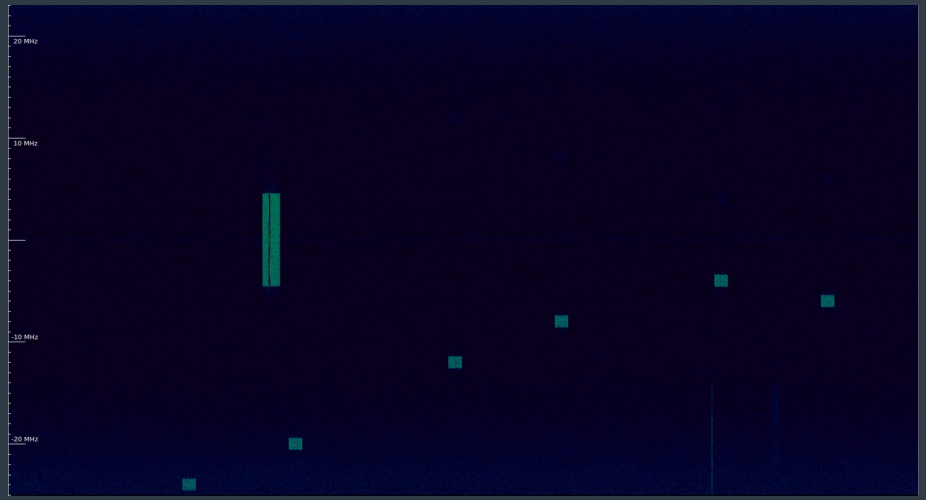
Static Analysis

Hands on the Drone

Dynamic Analysis

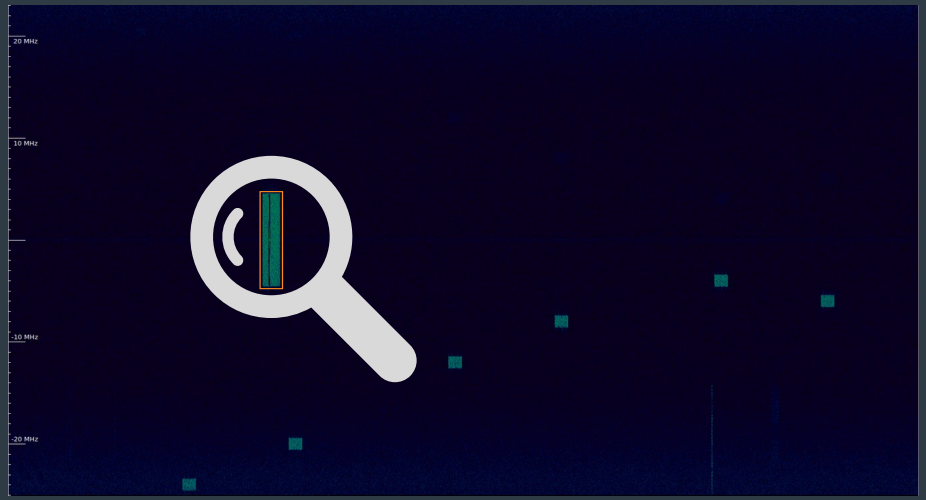
Fuzzing Drones for Pain and Profit

Listening on the Wireless Physical Layer ...



Capture Raw
Signal Data

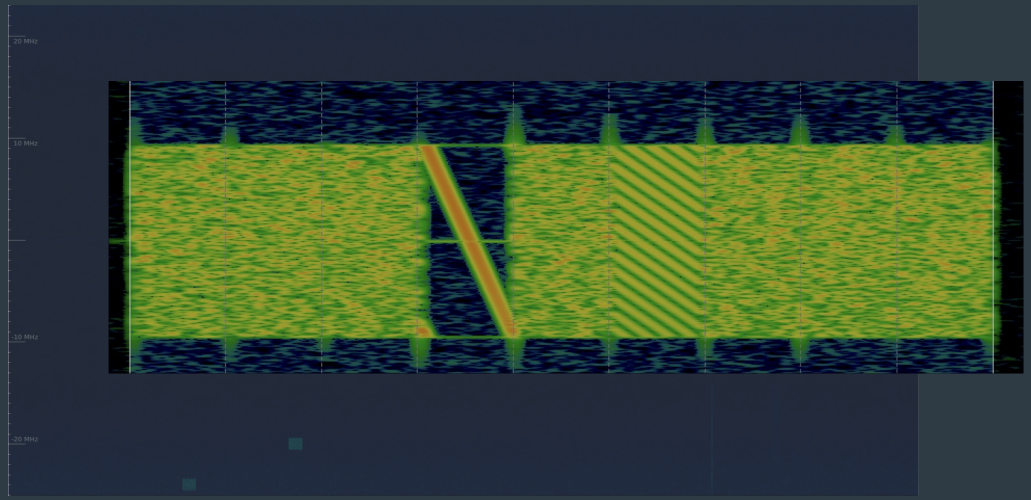
Listening on the Wireless Physical Layer ...



Capture Raw Signal Data

Packet Detection

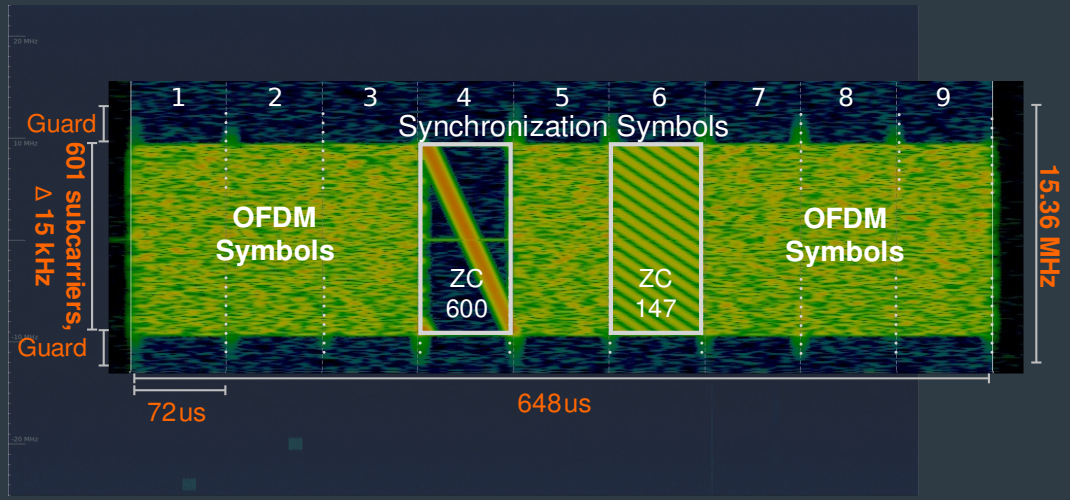
Listening on the Wireless Physical Layer ...



Capture Raw Signal Data

Packet Detection

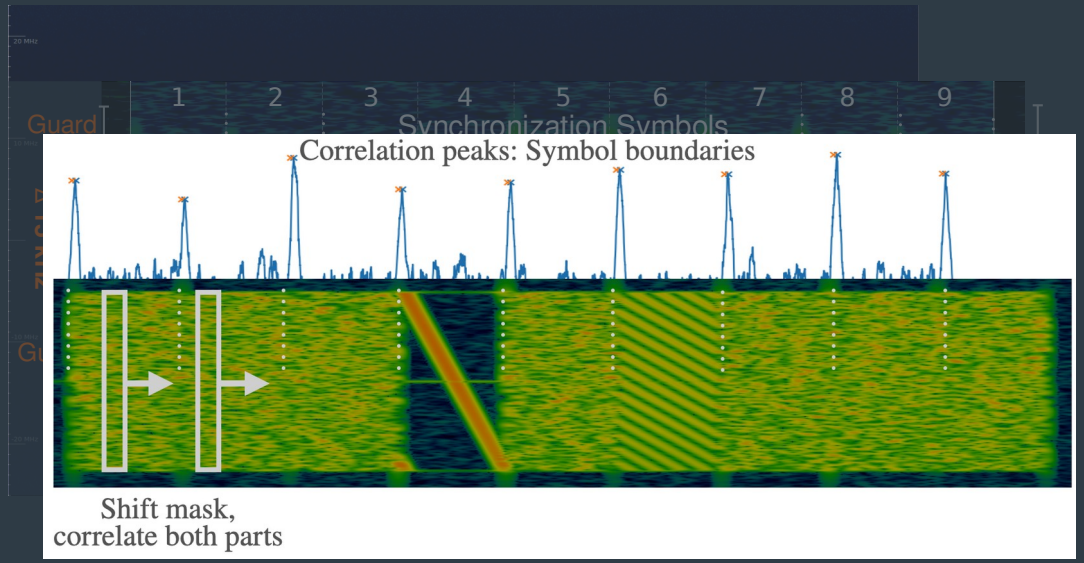
Listening on the Wireless Physical Layer ...

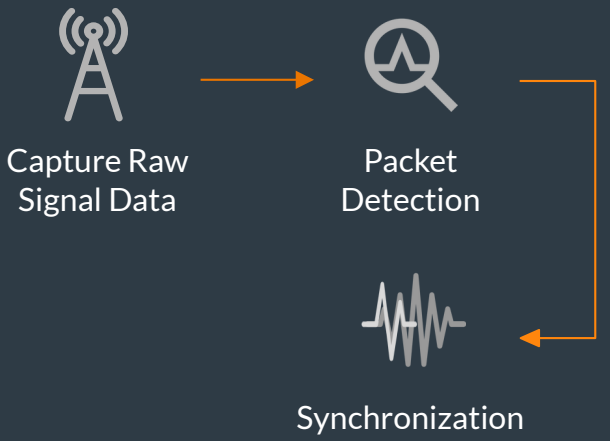


Capture Raw Signal Data

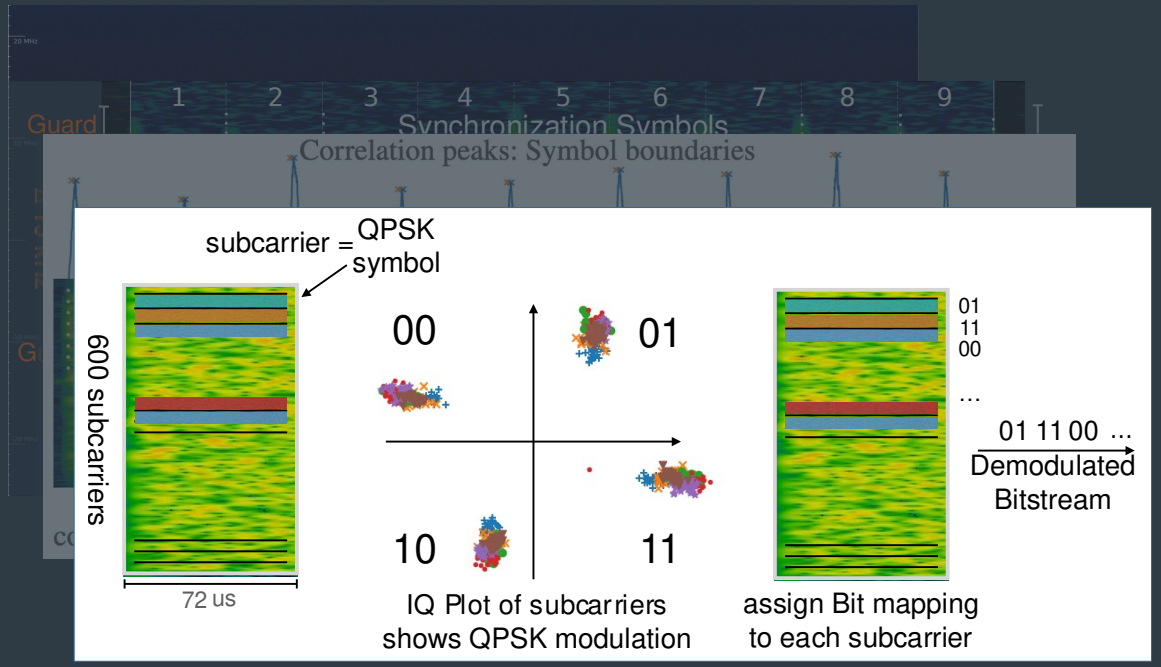
Packet Detection

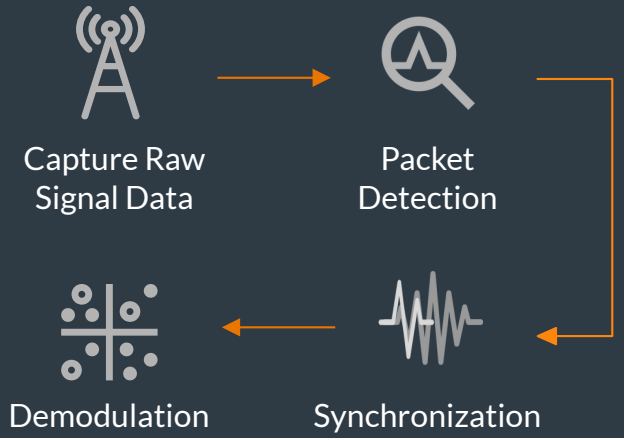
Listening on the Wireless Physical Layer ...



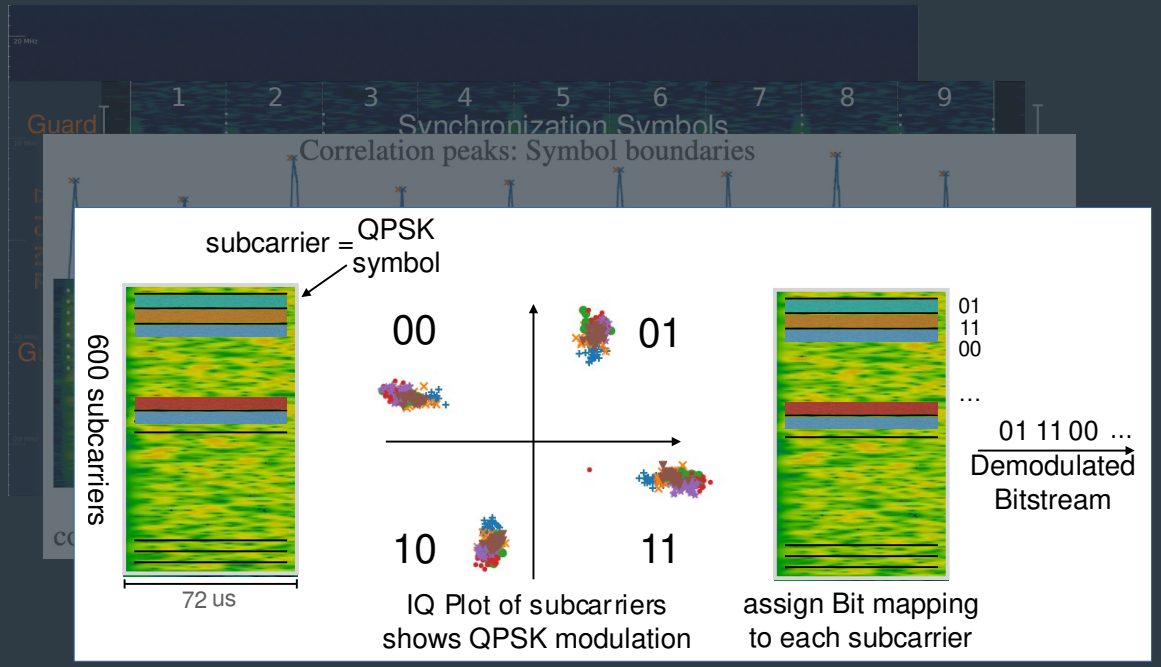


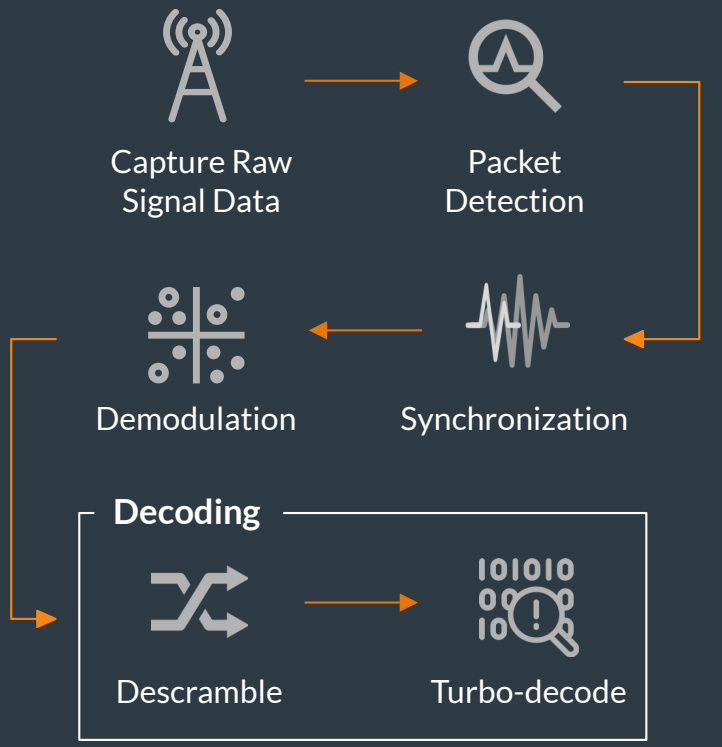
Listening on the Wireless Physical Layer ...



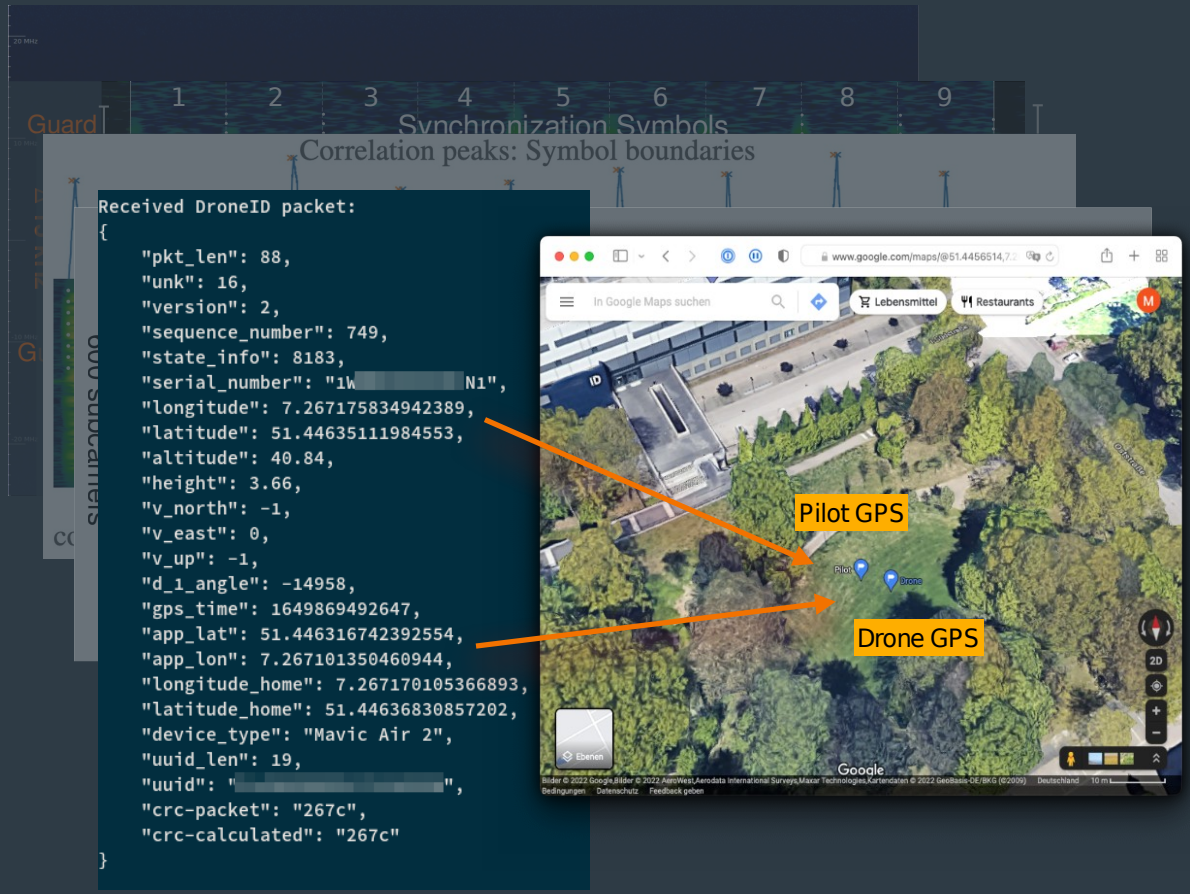


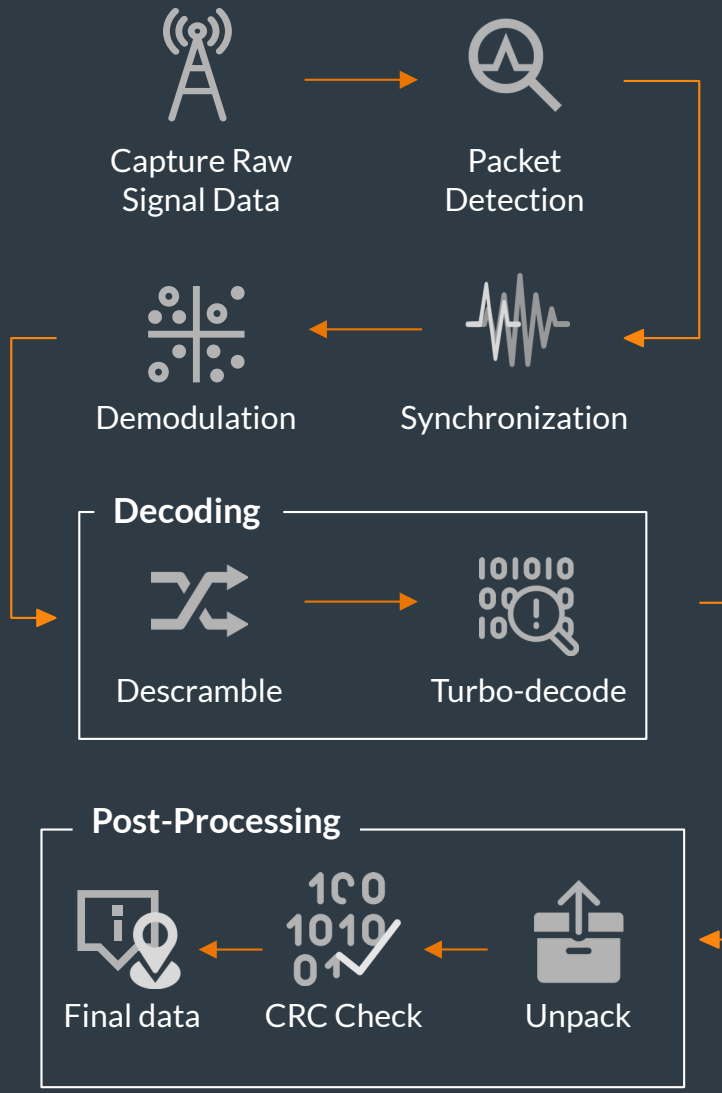
Listening on the Wireless Physical Layer …



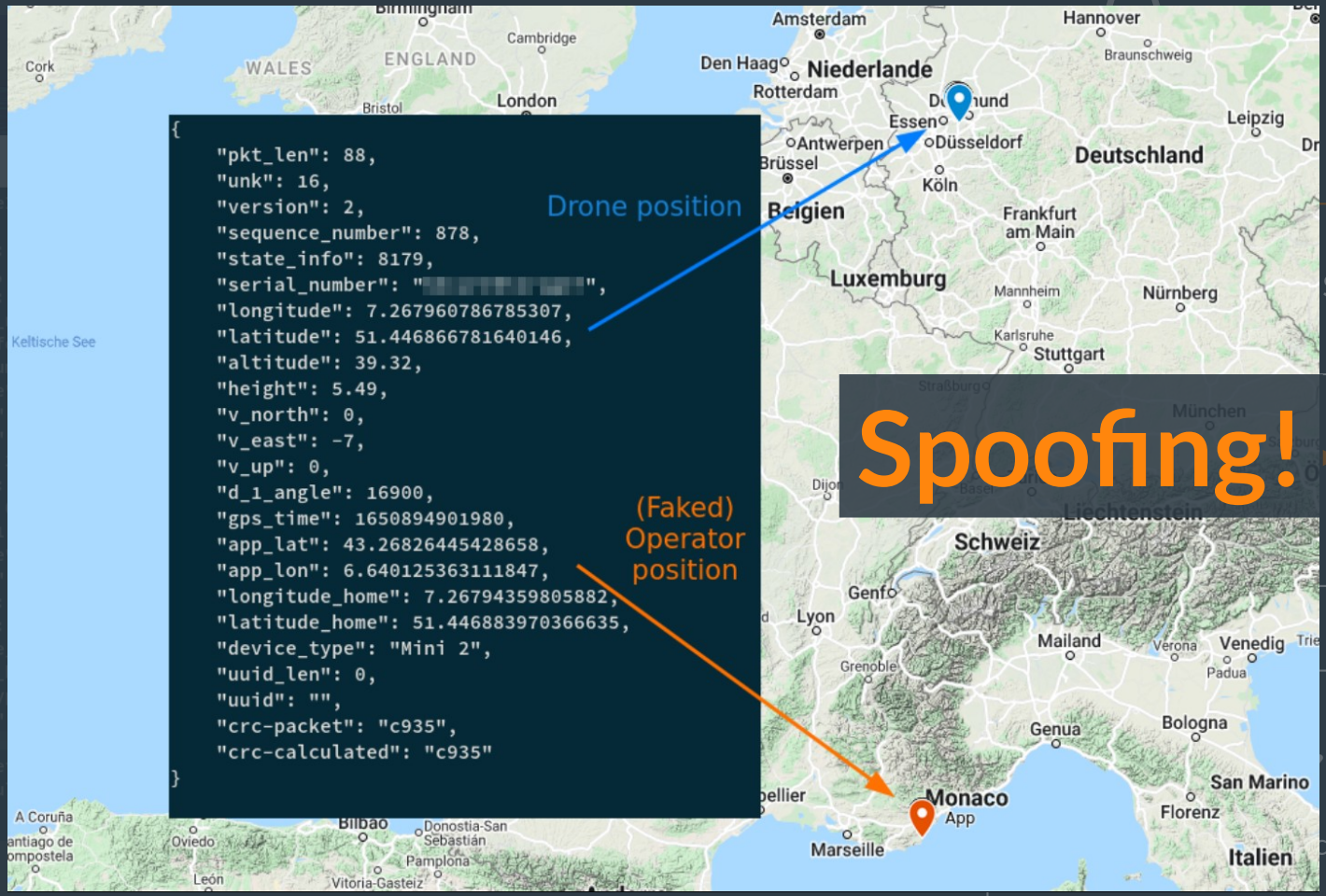


Listening on the Wireless Physical Layer ...





Listening on the Wireless Physical Layer ...



Wireless Physical Layer

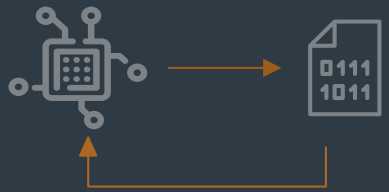
The Mysterious Case of DJI's DroneID

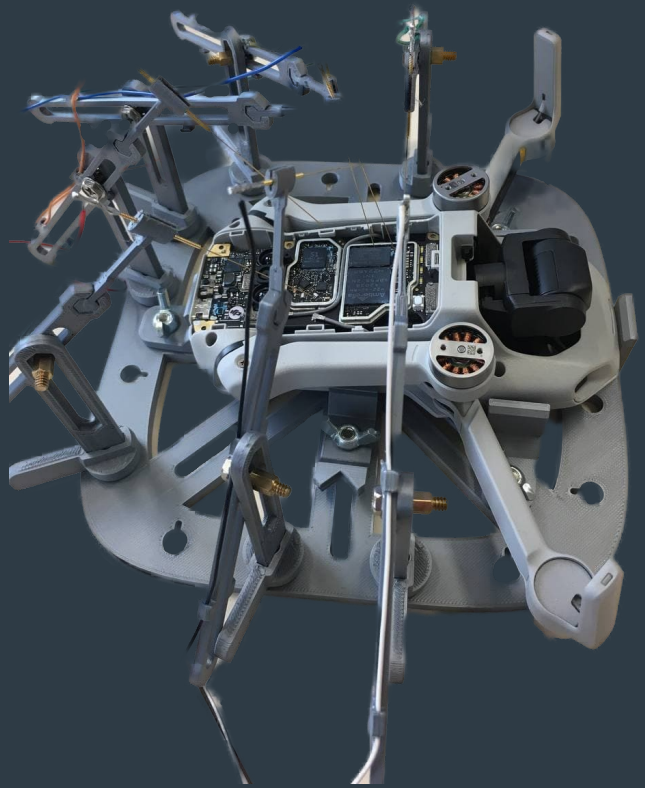
Static Analysis

Hands on the Drone

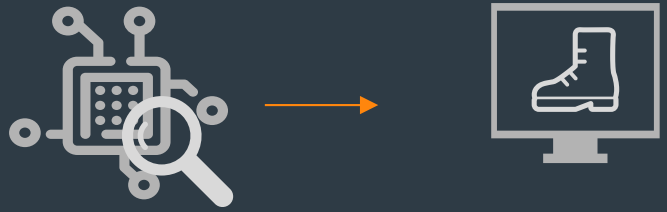
Dynamic Analysis

Fuzzing Drones for Pain and Profit





Analyze
PCB



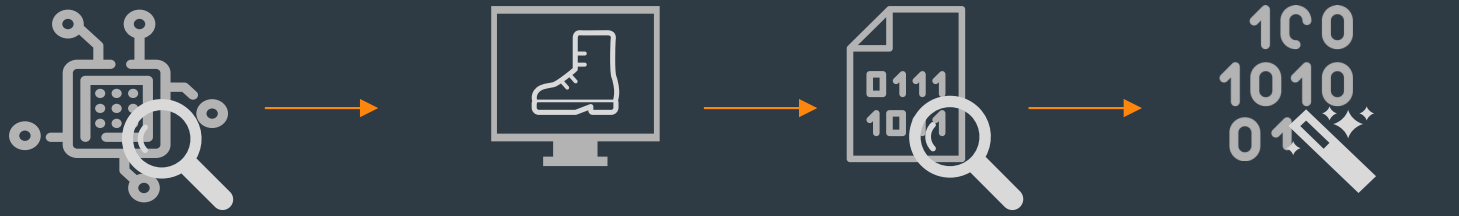
Analyze
PCB

Found
Boot Screen
(UART)!

Analyze PCB

Found Boot Screen (UART)!

Check Bootloader Firmware

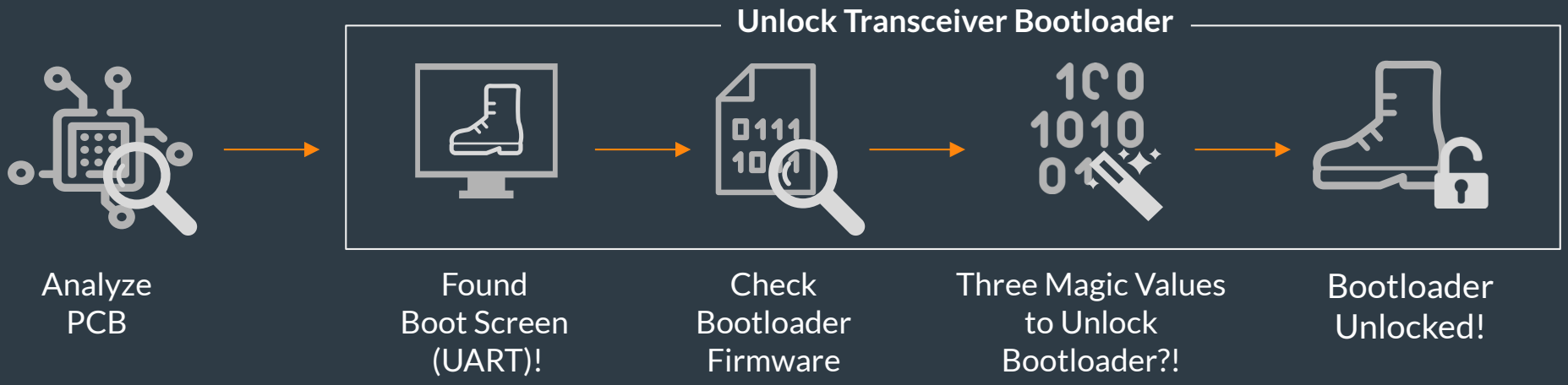


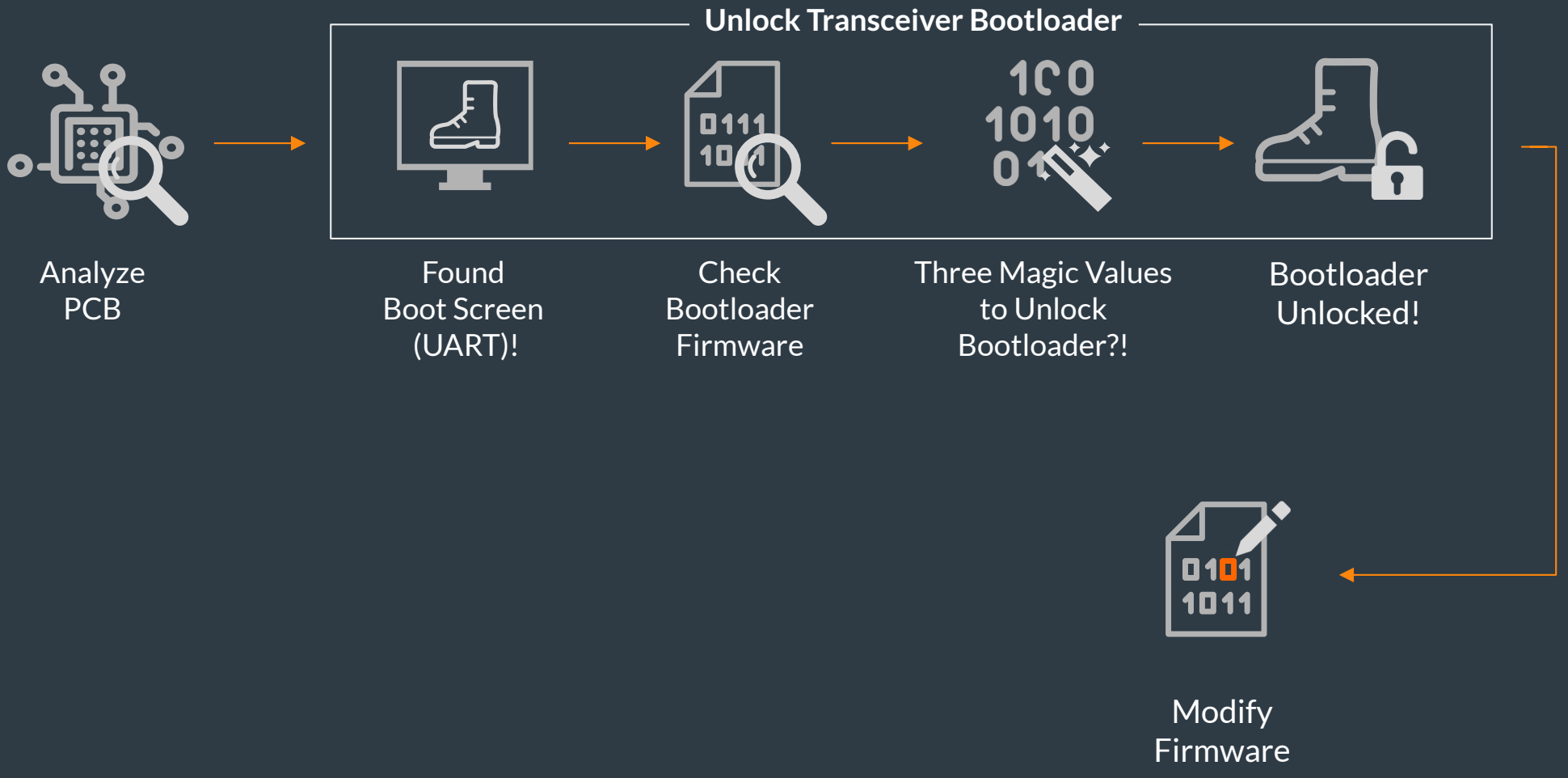
Analyze PCB

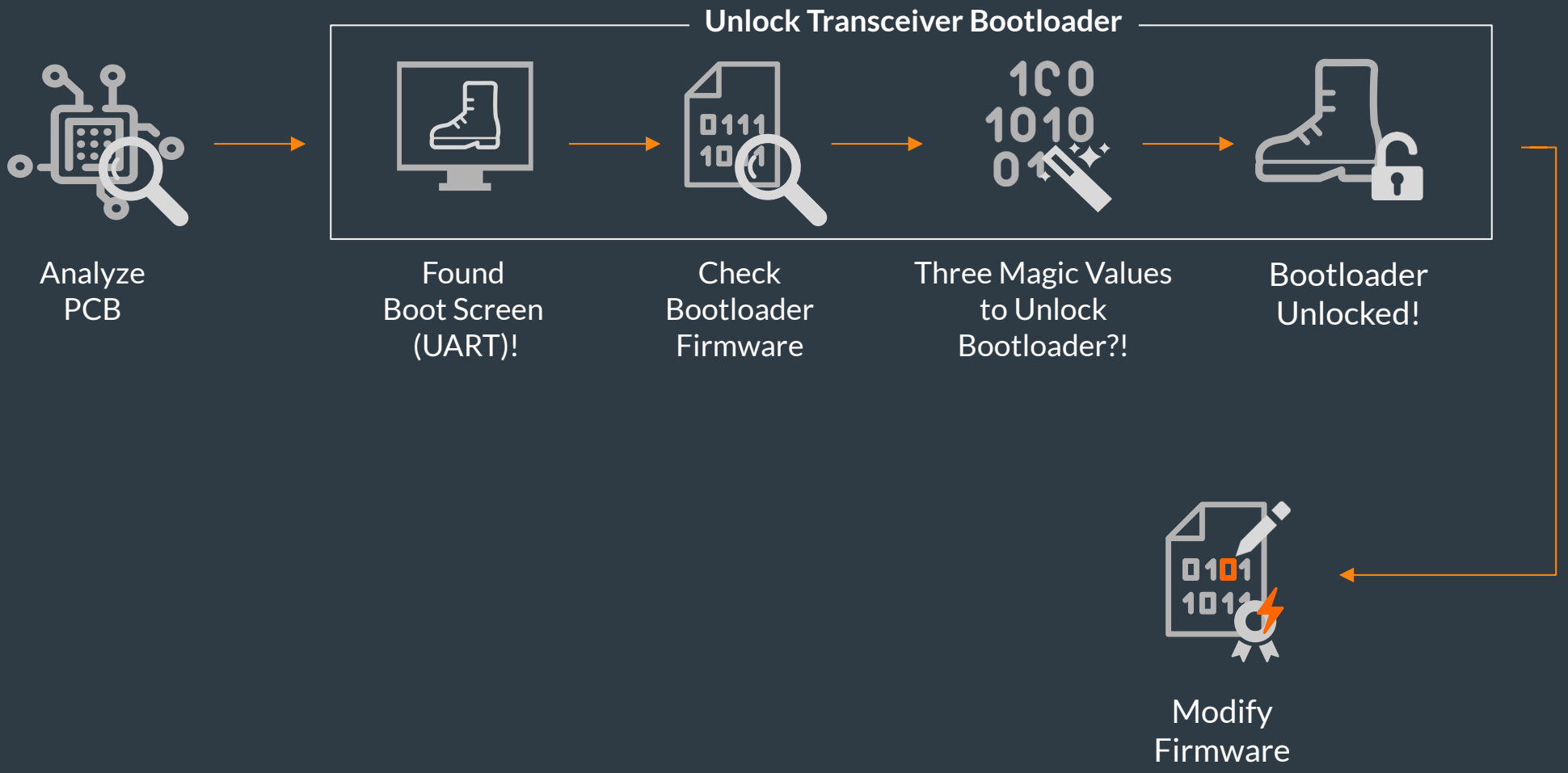
Found Boot Screen (UART)!

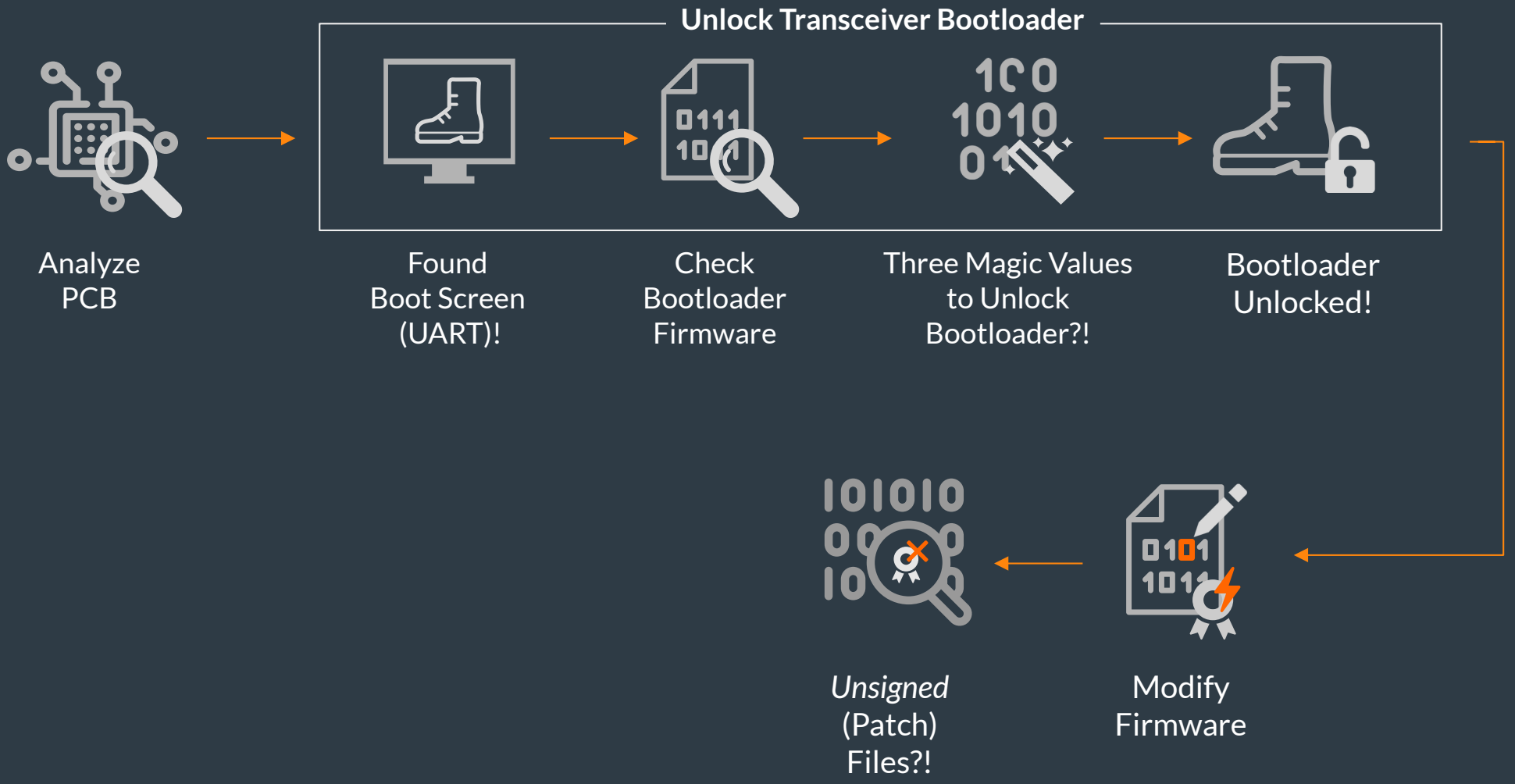
Check Bootloader Firmware

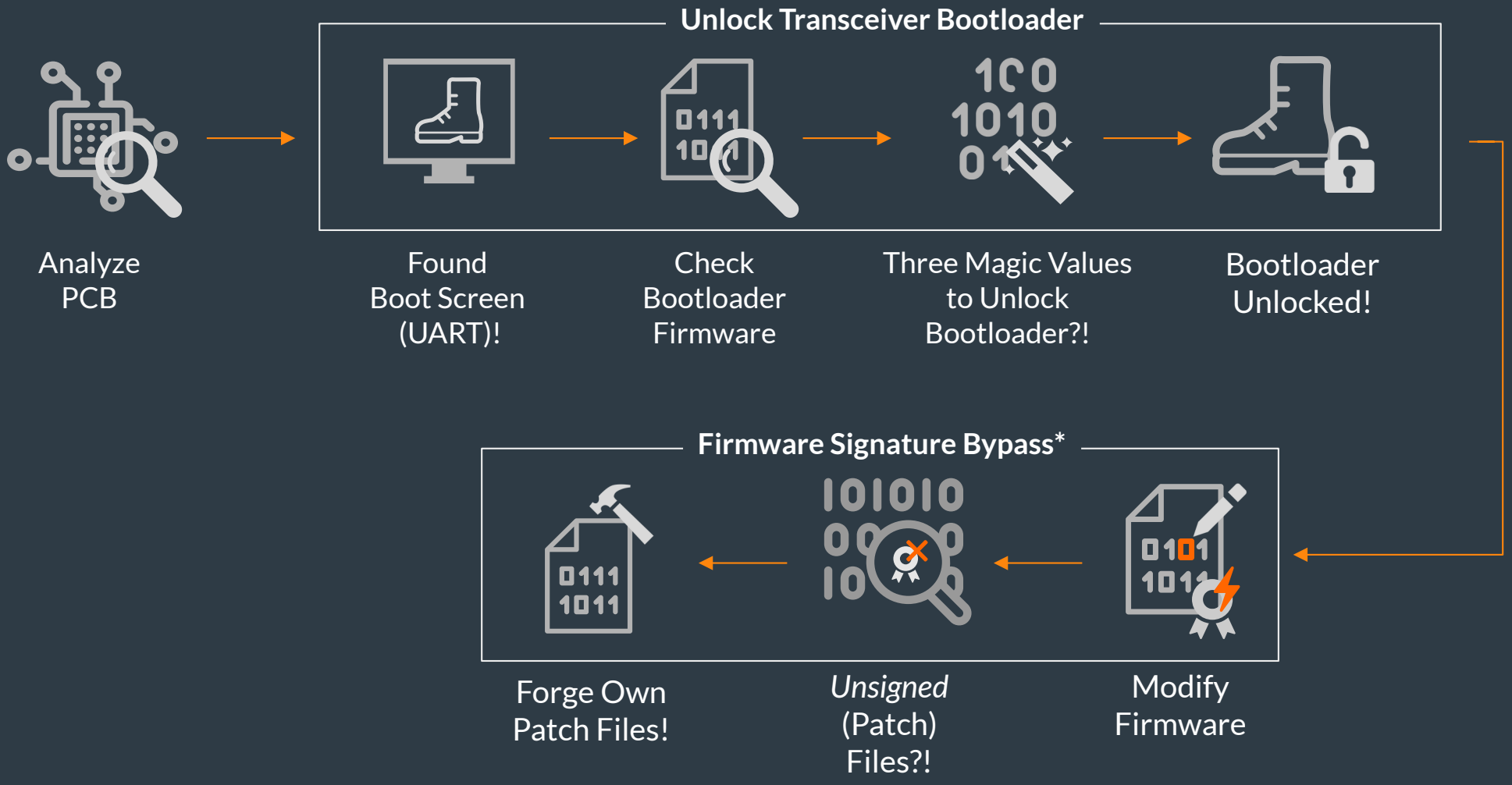
Three Magic Values to Unlock Bootloader?!


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

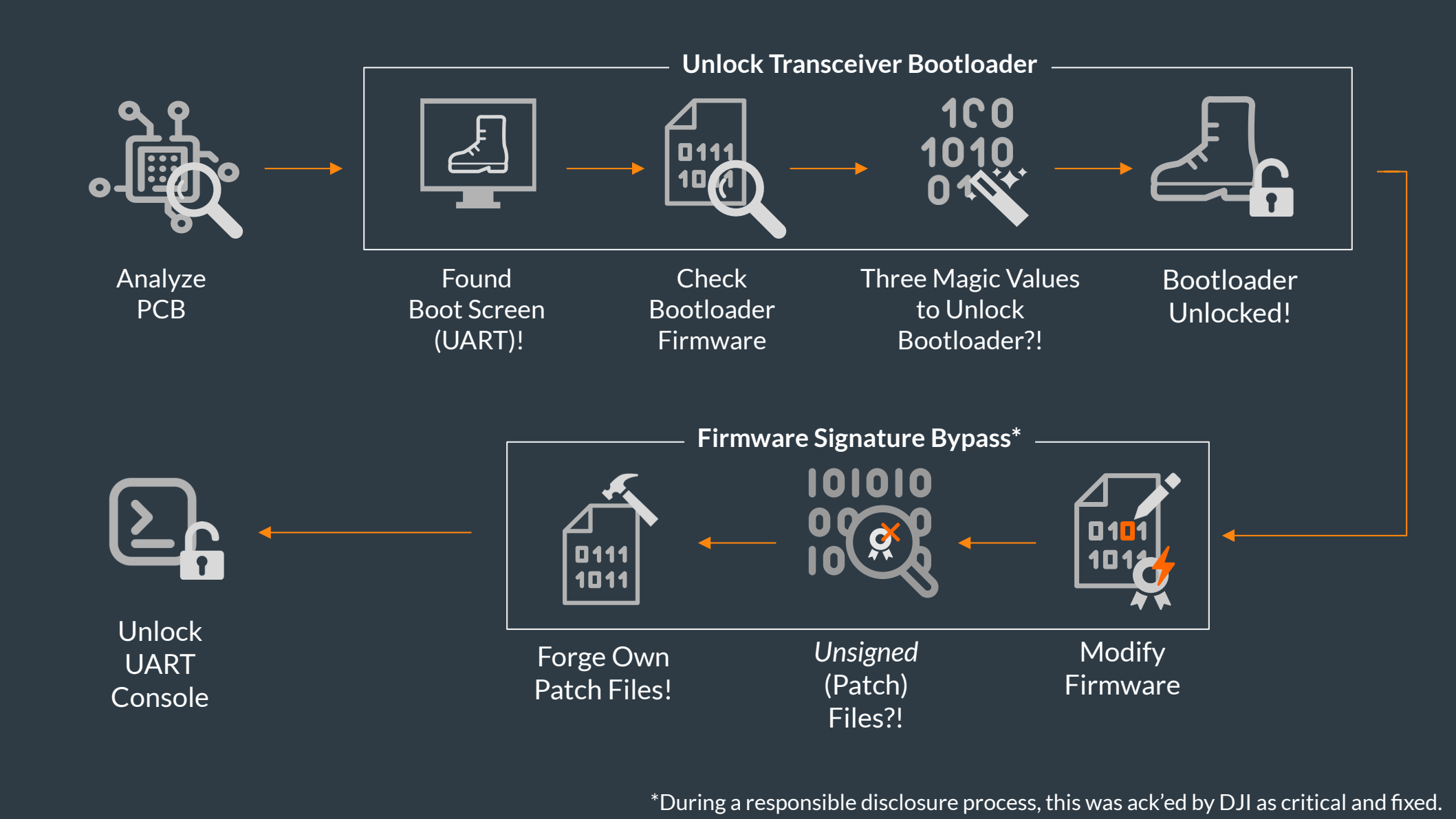

Unlock Transceiver Bootloader
Analyze PCB
Found Boot Screen (UART)!
Check Bootloader Firmware
Three Magic Values to Unlock Bootloader?!
Bootloader Unlocked!
Modify Firmware


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?!



*During a responsible disclosure process, this was ack'ed by DJI as critical and fixed.



*During a responsible disclosure process, this was ack'ed by DJI as critical and fixed.

Wireless Physical Layer

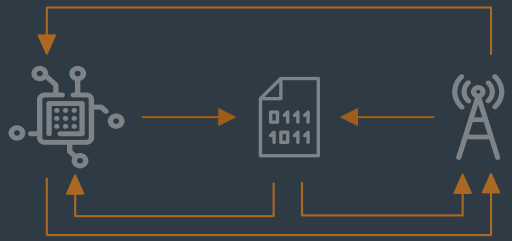
The Mysterious Case of DJI's DroneID

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
- Protocol knowledge

How to Fuzz R*eal* Drones?

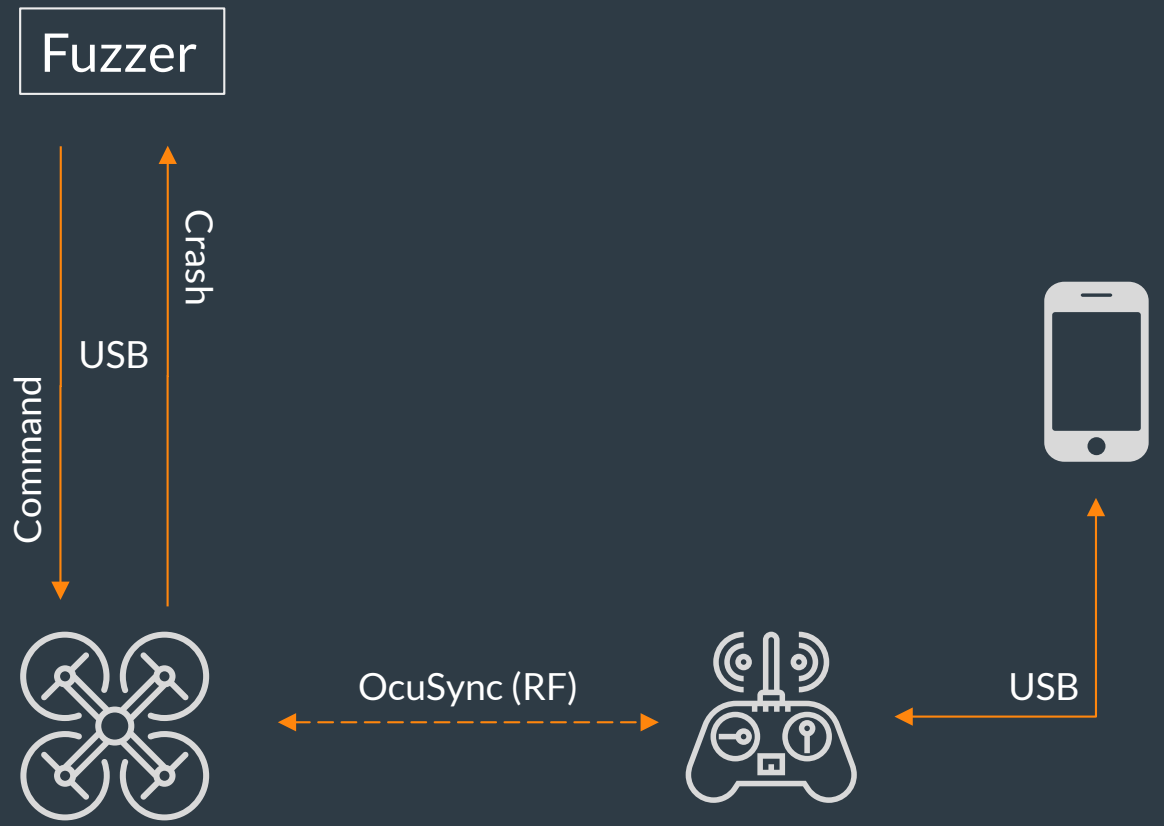
Prerequisites:

- A drone and fuzzer
- Protocol knowledge
- Bug oracle

How to Fuzz R*eal* Drones?

Prerequisites:

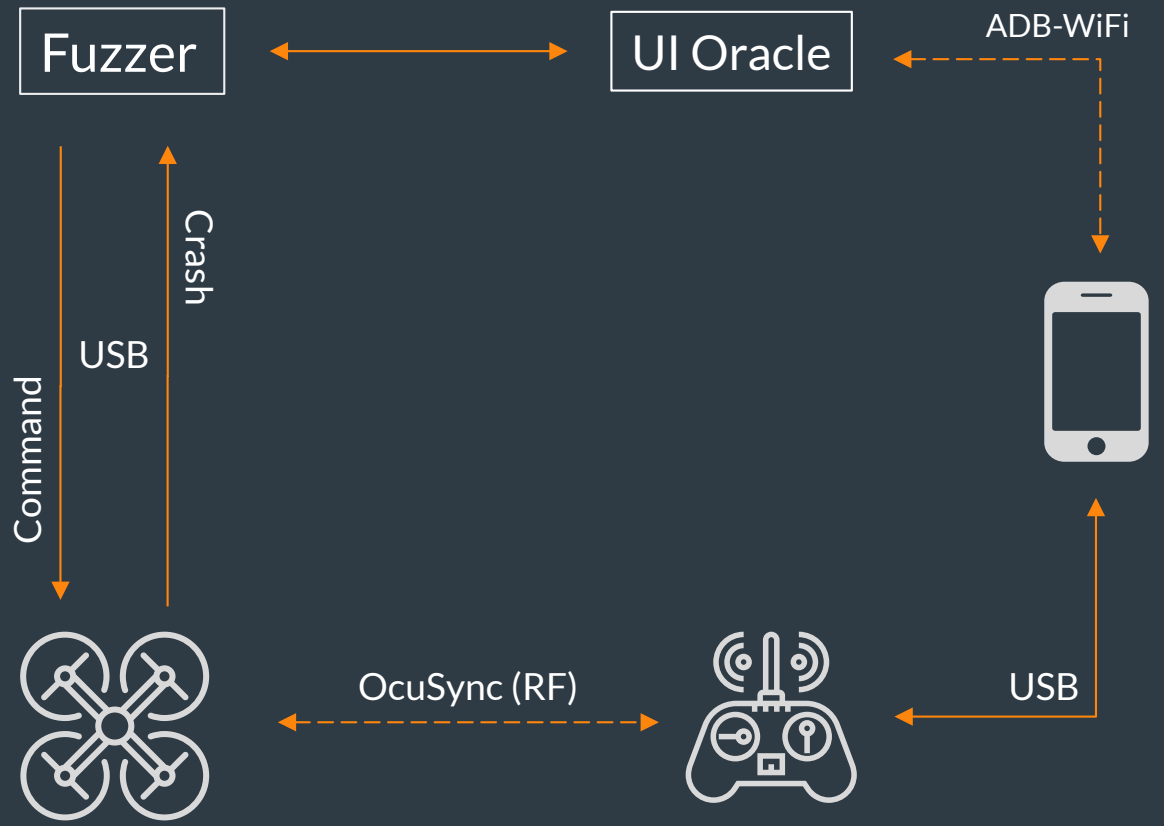
- A drone and fuzzer
- Protocol knowledge
- Bug oracle



How to Fuzz R*eal* Drones?

Prerequisites:

- A drone and fuzzer
- Protocol knowledge
- Bug oracle

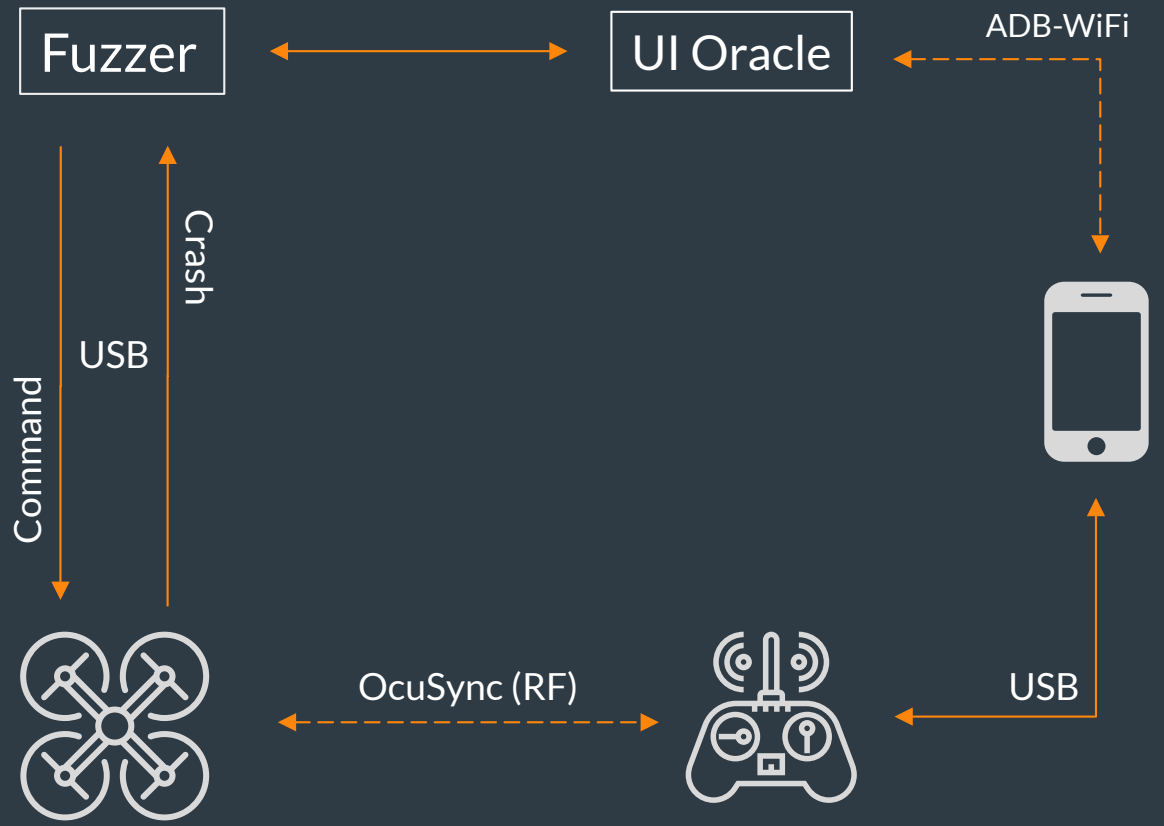


How to Fuzz R*eal* Drones?

Prerequisites:

- A drone and fuzzer
- Protocol knowledge
- Bug oracle

Reproducible bugs!



Does fuzzing work?

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

*Following responsible disclosure, DJI fixed these bugs.

Does fuzzing work?

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

*Following responsible disclosure, DJI fixed these bugs.

Does fuzzing work?

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

*Following responsible disclosure, DJI fixed these bugs.

Does fuzzing work?

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

*Following responsible disclosure, DJI fixed these bugs.

Summary of Findings

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

Position tracking

Summary of Findings

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

- Debugging interfaces enabled
- Firmware signature verification bypassed

Position tracking 

Hardware protection 

Summary of Findings

- 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 

Takeaways

Takeaways

- Countermeasures are not sufficent

Takeaways

- Countermeasures are not sufficent
- Hard to secure real world devices since they are *complex*

Takeaways

- Countermeasures are not sufficent
- Hard to secure real world devices since they are *complex*
- Requires holistic approaches to analyze real world devices

Takeaways

- Countermeasures are not sufficent
- Hard to secure real world devices since they are *complex*
- Requires holistic approaches to analyze real world devices

RUB-SysSec/DroneSecurity

74ck_0

Takeaways

- Countermeasures are not sufficent
- Hard to secure real world devices since they are *complex*
- Requires holistic approaches to analyze real world devices

RUB-SysSec/DroneSecurity

74ck_0

Questions?