Drone Security and the Mysterious Case of DJI's DroneID

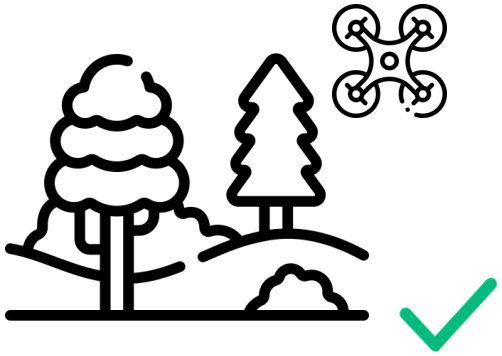
Nico Schiller, Merlin Chlosta, Moritz Schloegel, Nils Bars, Thorsten Eisenhofer,
Tobias Scharnowski, Felix Domke, Lea Schönherr, Thorsten Holz

NDSS'23

Presentor : Suhwan Jeong

Introduction

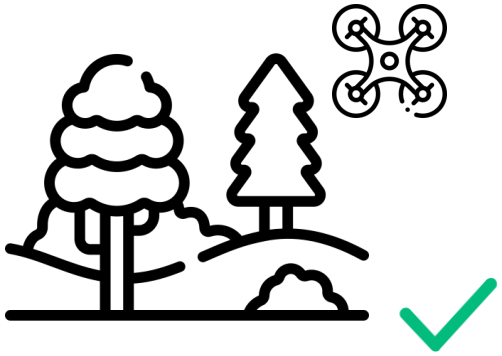
- Consumer Drones



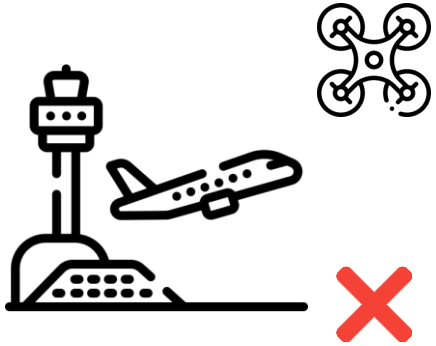
- Mainstream product
- High popularity

Introduction

- Consumer Drones



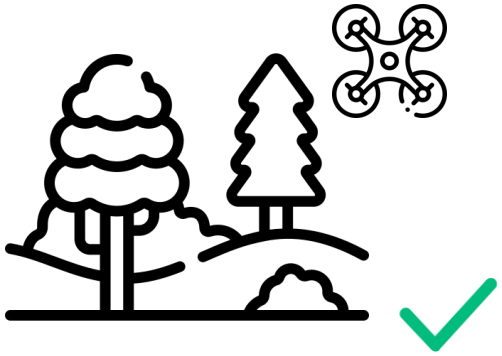
- Mainstream product
- High popularity



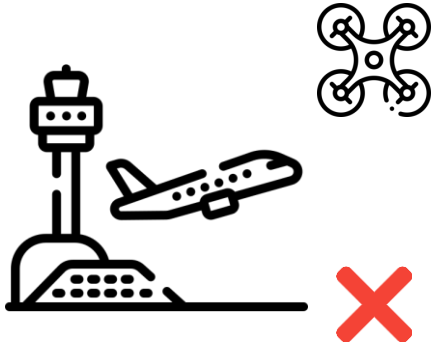
- Disturb air traffic
- Expensive shutdowns

Introduction

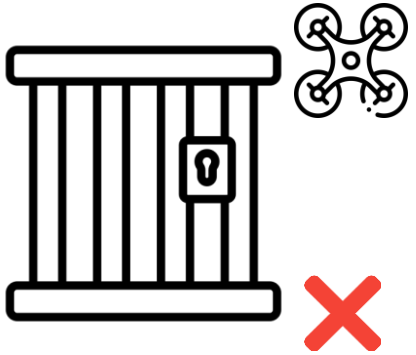
- Consumer Drones



- Mainstream product
- High popularity



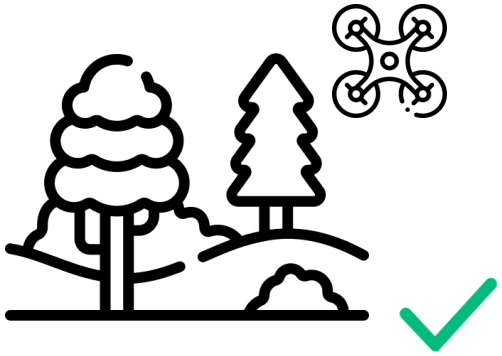
- Disturb air traffic
- Expensive shutdowns



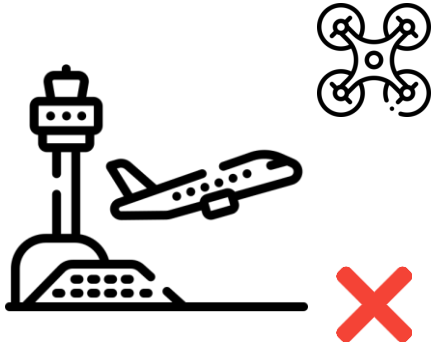
- Smuggling
- Bypass physical barrier

Introduction

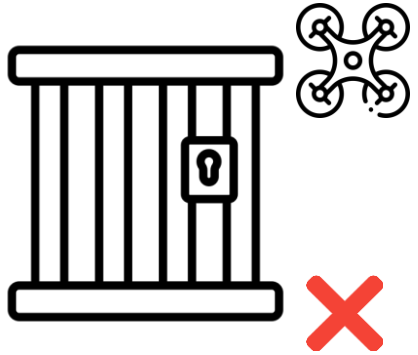
- Consumer Drones



- Mainstream product
- High popularity



- Disturb air traffic
- Expensive shutdowns

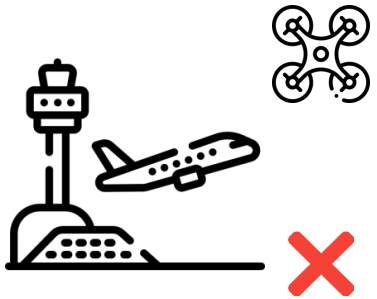


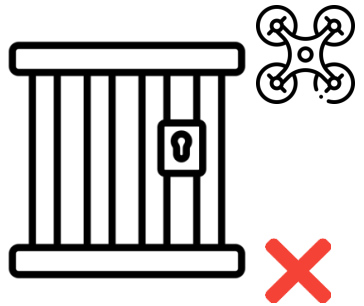
- Smuggling
- Bypass physical barrier

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

Introduction

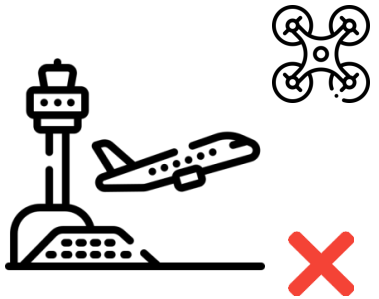
Vendors know these problems!

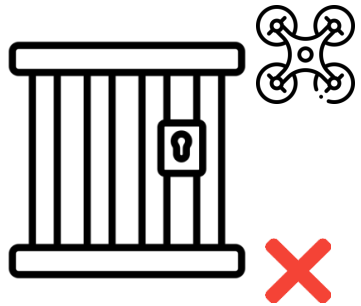




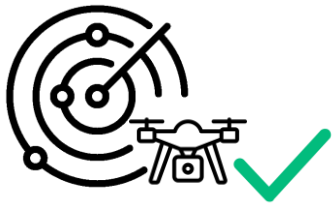
Introduction

Vendors know these problems!



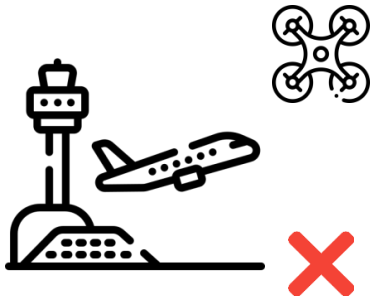


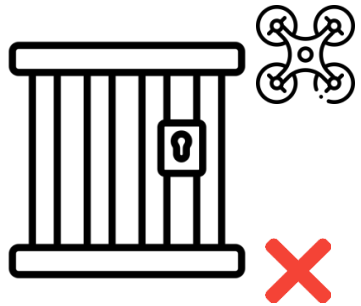
Position tracking
DJI Aeroscope



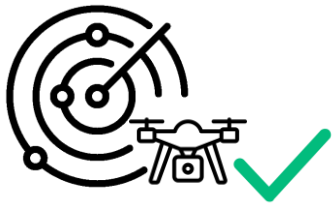
Introduction

Vendors know these problems!

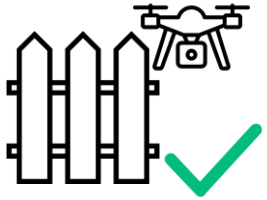




Position tracking
DJI Aeroscope

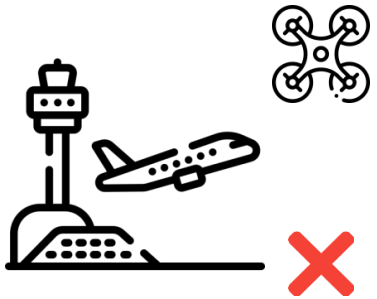


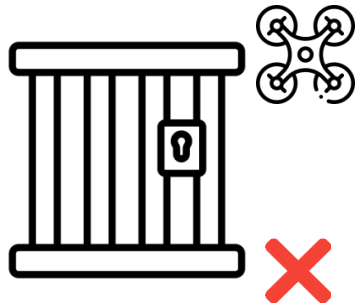
Software limits
Geofencing



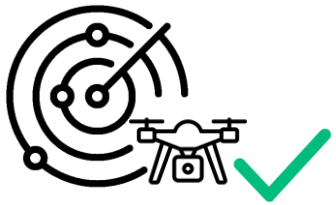
Introduction

Vendors know these problems!

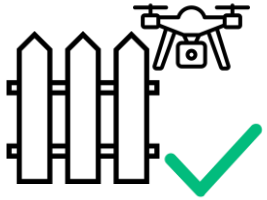




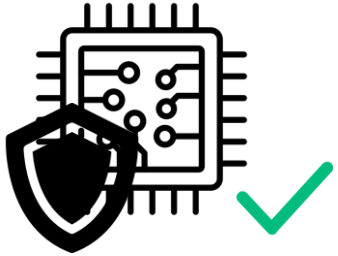
Position tracking
DJI Aeroscope



Software limits
Geofencing

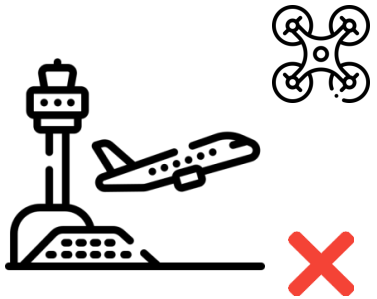


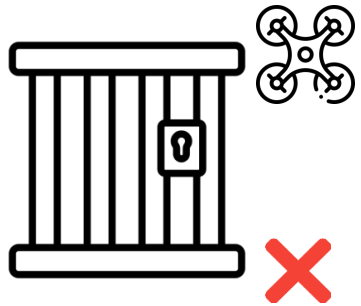
Hardware protection
No debug interfaces



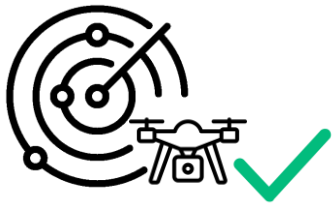
Introduction

Vendors know these problems!

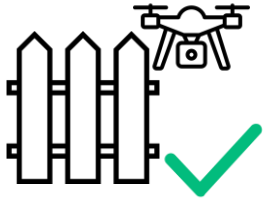




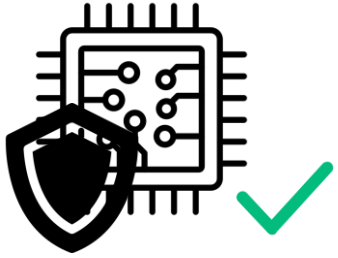
Position tracking
DJI Aeroscope



Software limits
Geofencing



Hardware protection
No debug interfaces



Are these countermeasures sufficiently implemented?

Target

- DJI Drones
  - Market share (94% Consumer)

Target

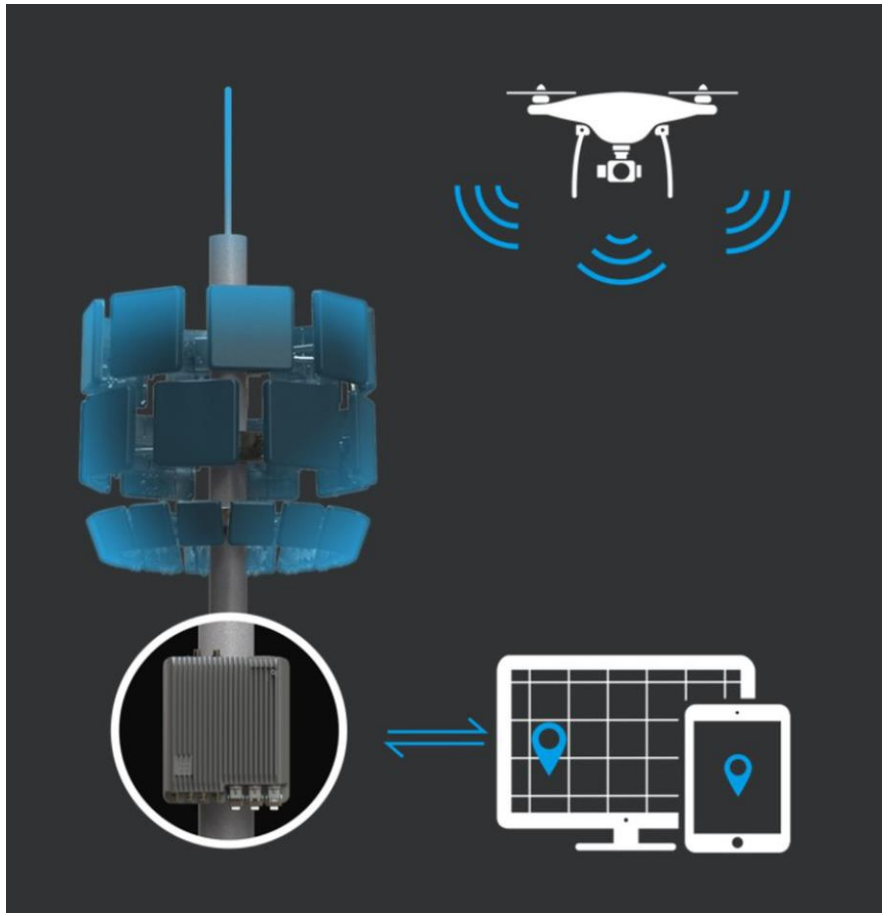
- DJI Drones
  - Market share (94% Consumer)
  - They take security seriously
    - Whitepaper
    - Bug bounty program

Target

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

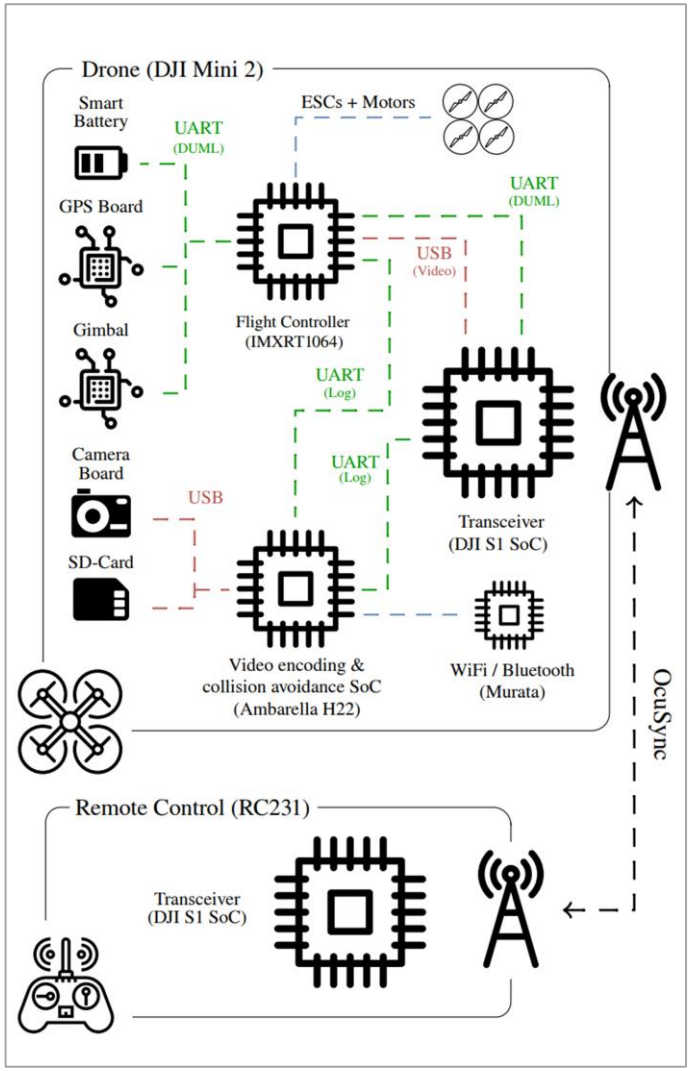
Inconsistent statements

- DroneID is encrypted?
  - N drones
  - M Aeroscopes
  - Aeroscope : $5,000

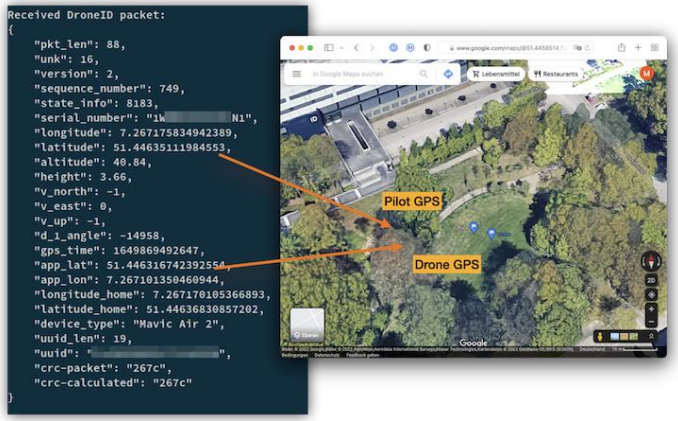


Schematic Overview

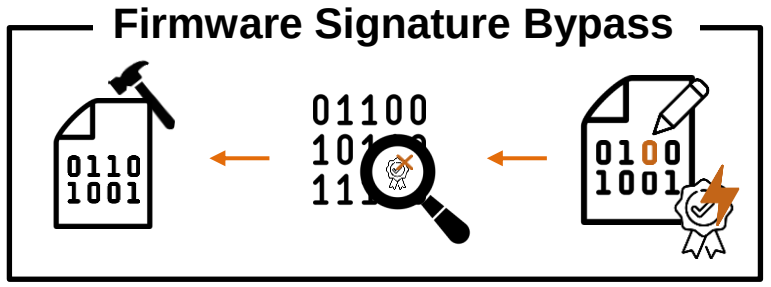
- Target
  - DJI S1 SoC
    - Bootloader
    - AP (Application Processor)
    - CP (Communication Processor)



Research Flow



Drone and pilot's location tracking



Firmware signature verification bypass

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
#16	UI change	flight controller	change drone name[d]	—	—	✓	Mavic Air 2, Mini 2

Vulnerability detection via fuzzing

Wireless Analysis

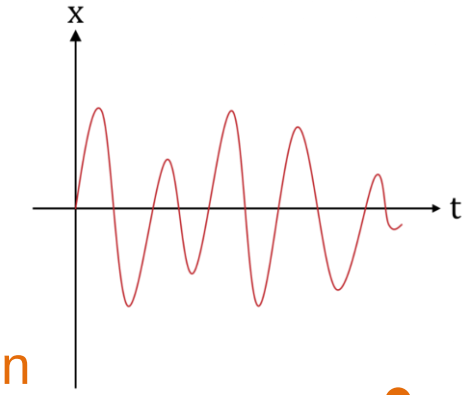
Static Analysis

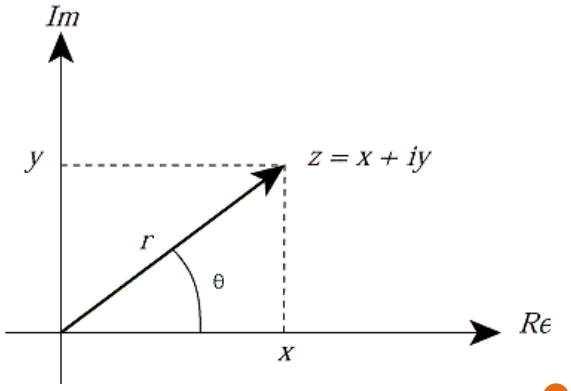
Dynamic Analysis

1. Wireless Analysis

Background

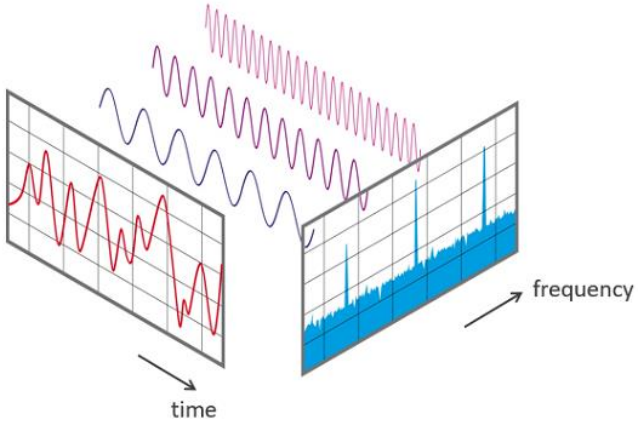
- modulation & demodulation

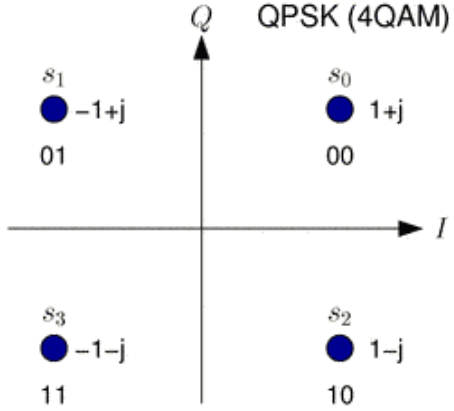




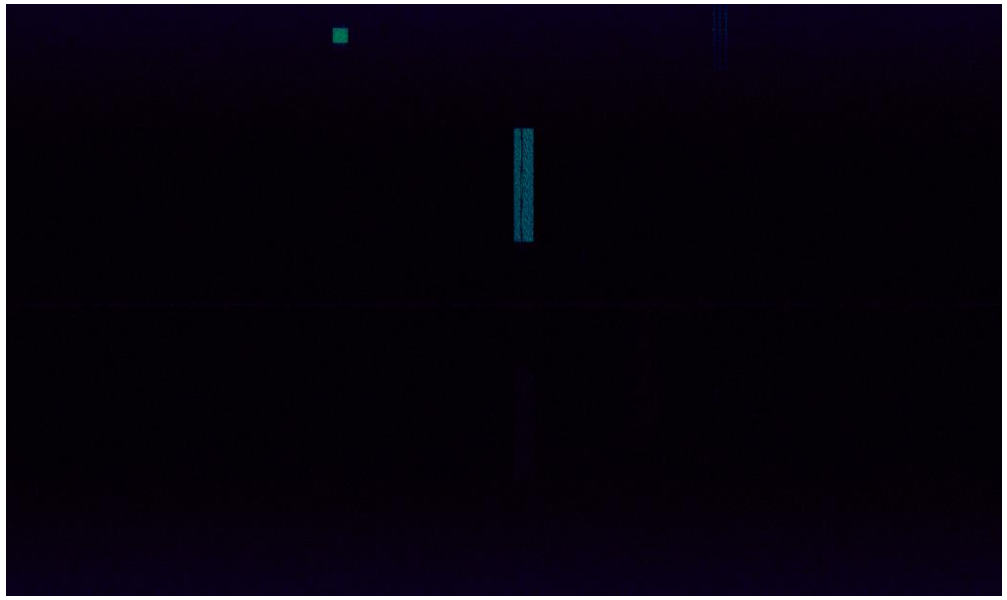
modulation — Demodulation

Fourier transformation — Euler's formula — mapping





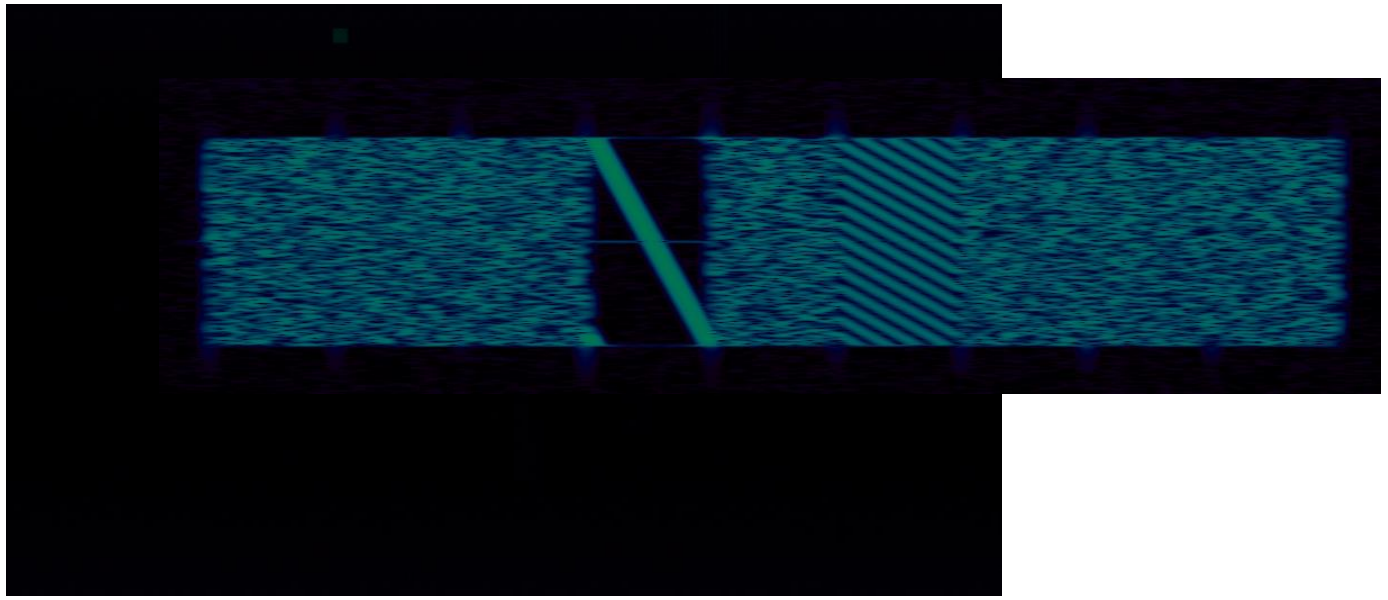
1. Wireless Analysis



Capture Raw Signal Data

1. Wireless Analysis

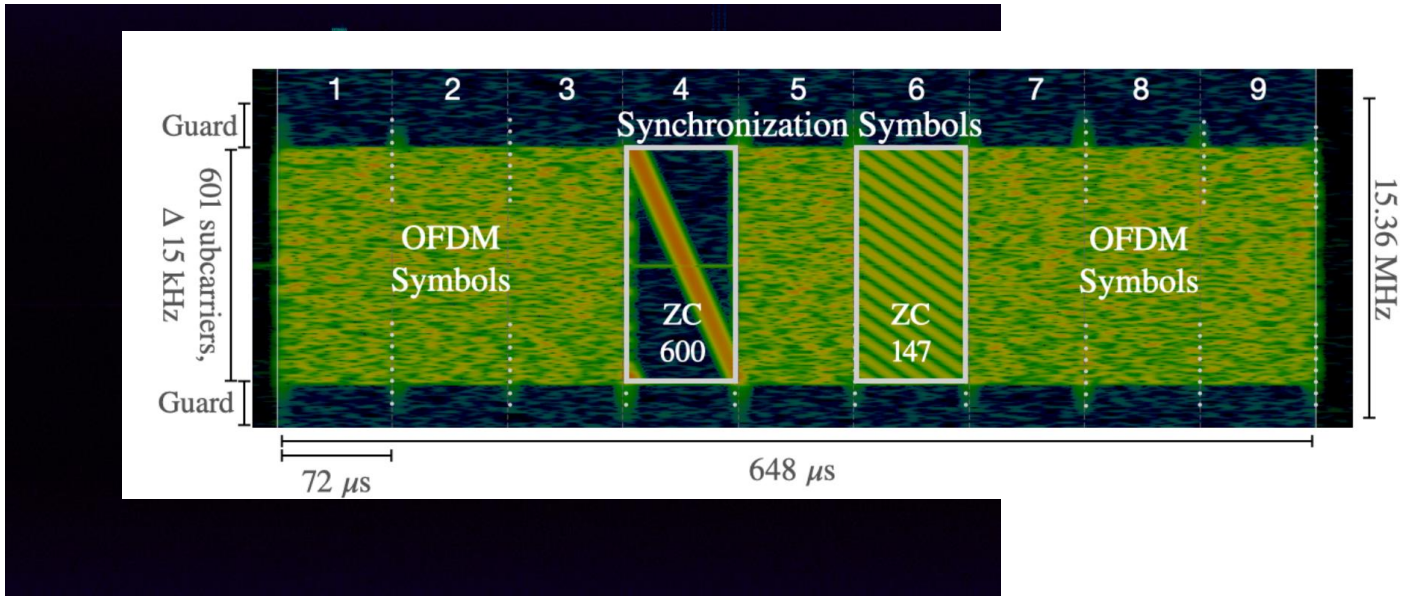
1. Wireless Analysis



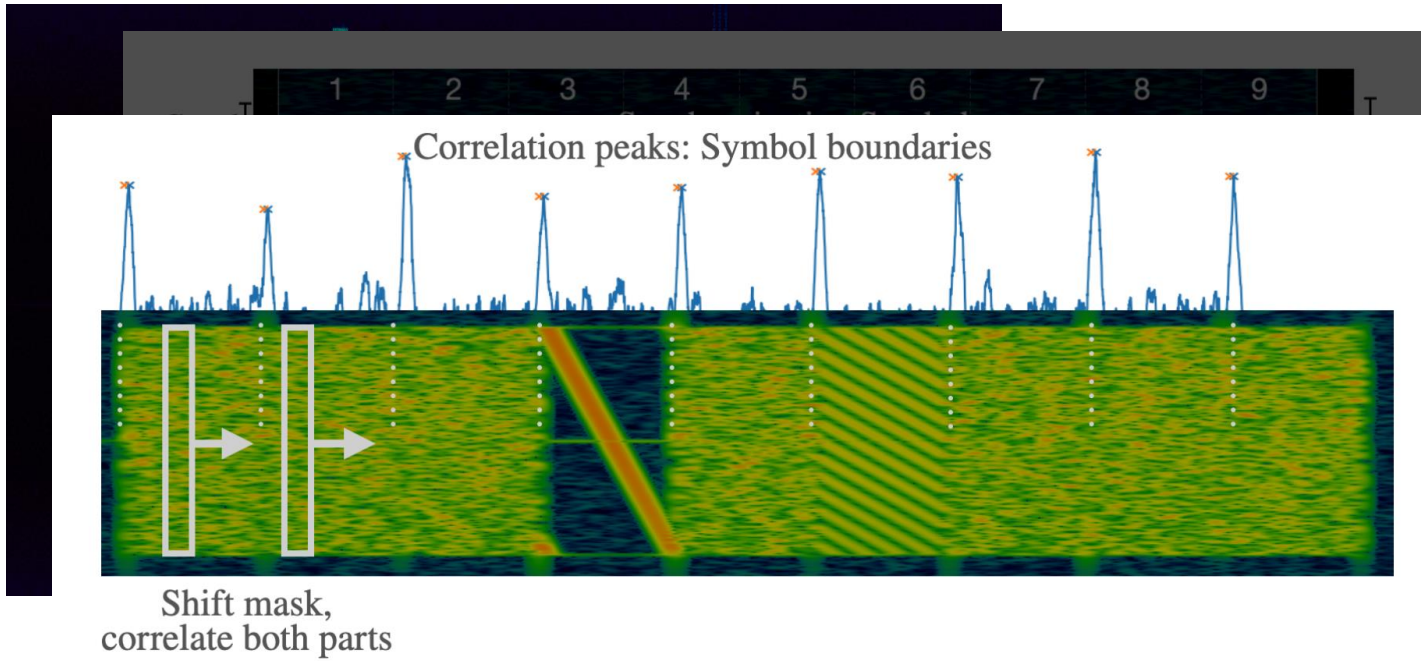
Capture Raw Signal Data

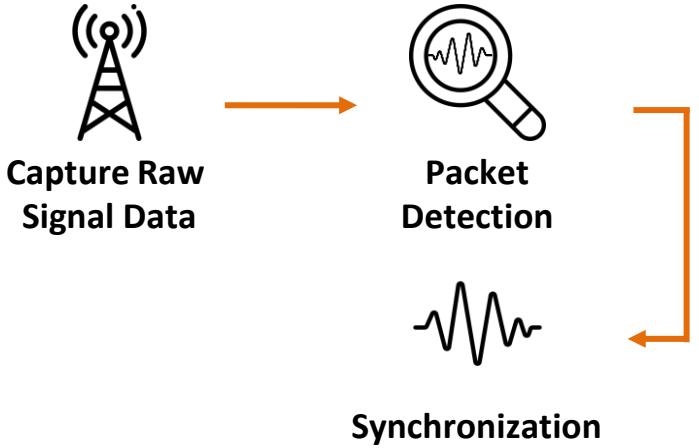
Packet Detection

1. Wireless Analysis

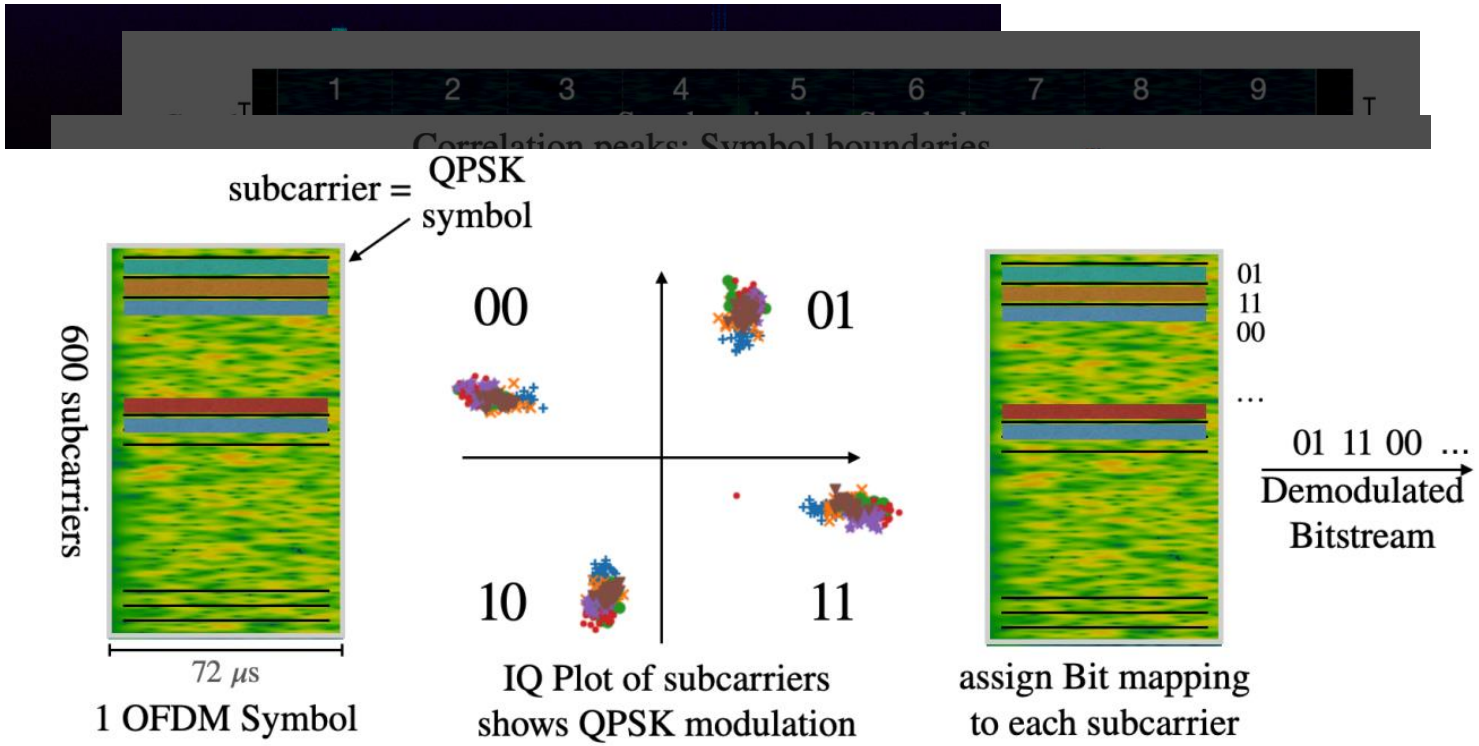


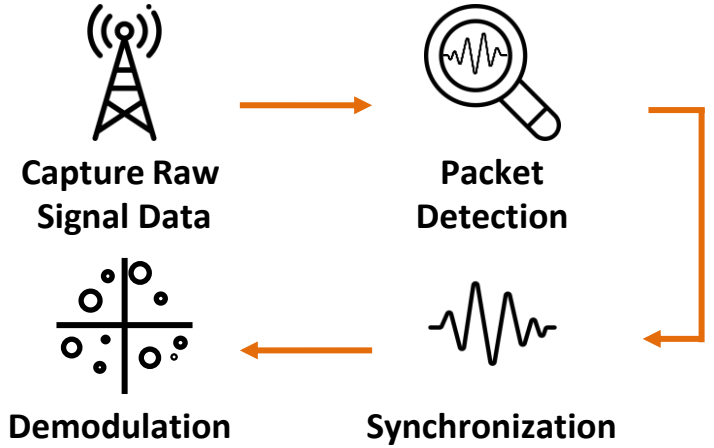
1. Wireless Analysis



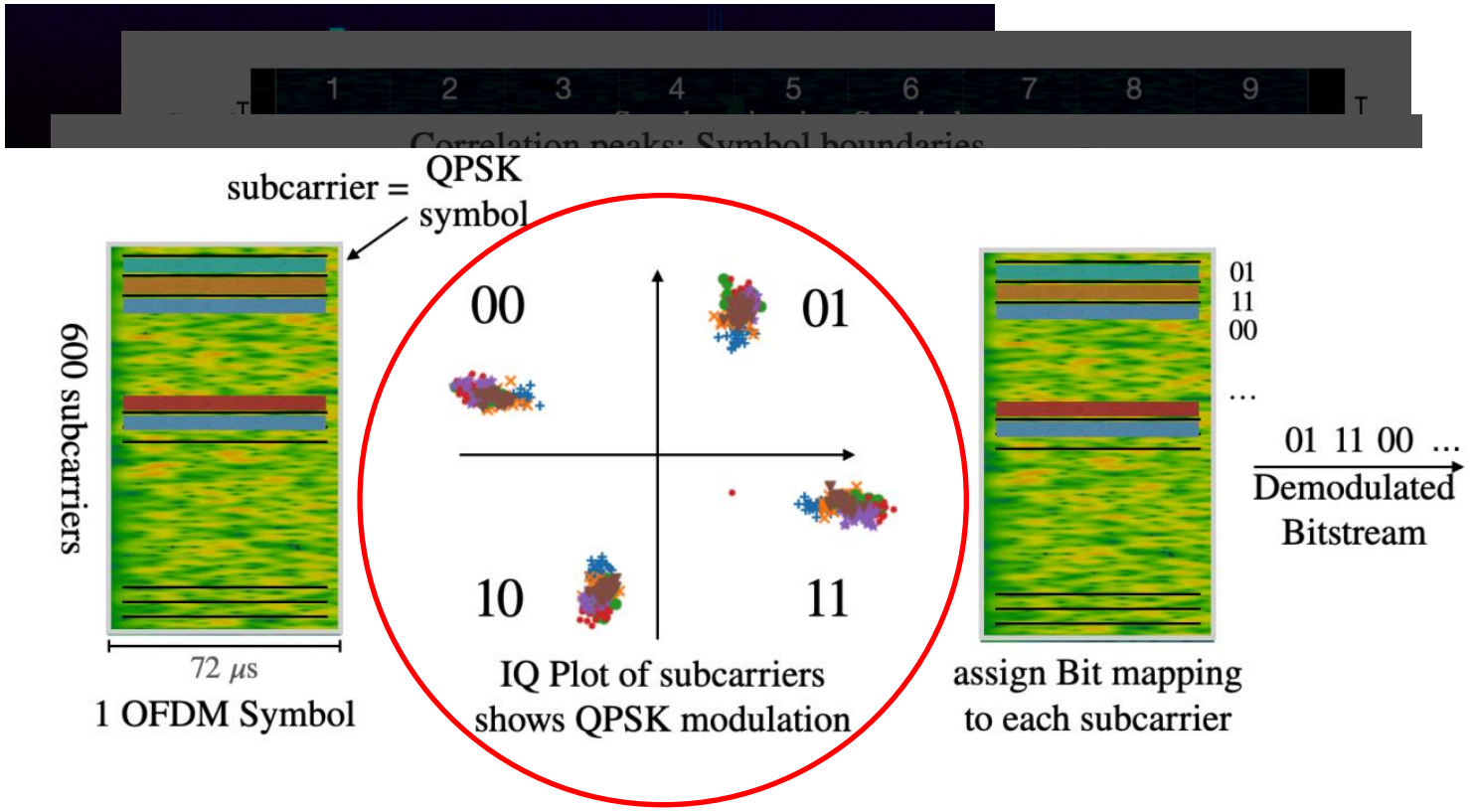


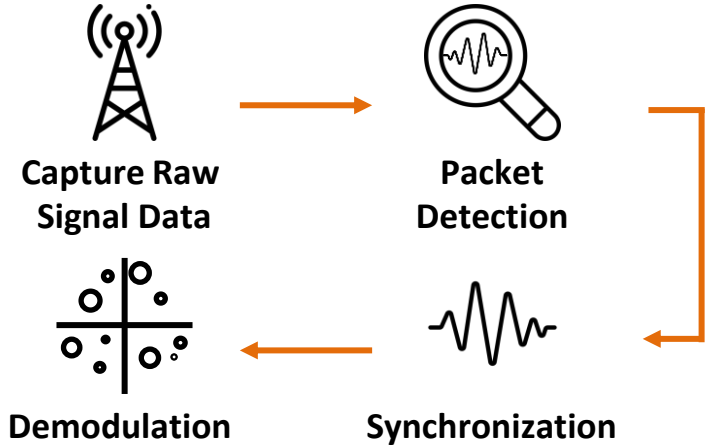
1. Wireless Analysis





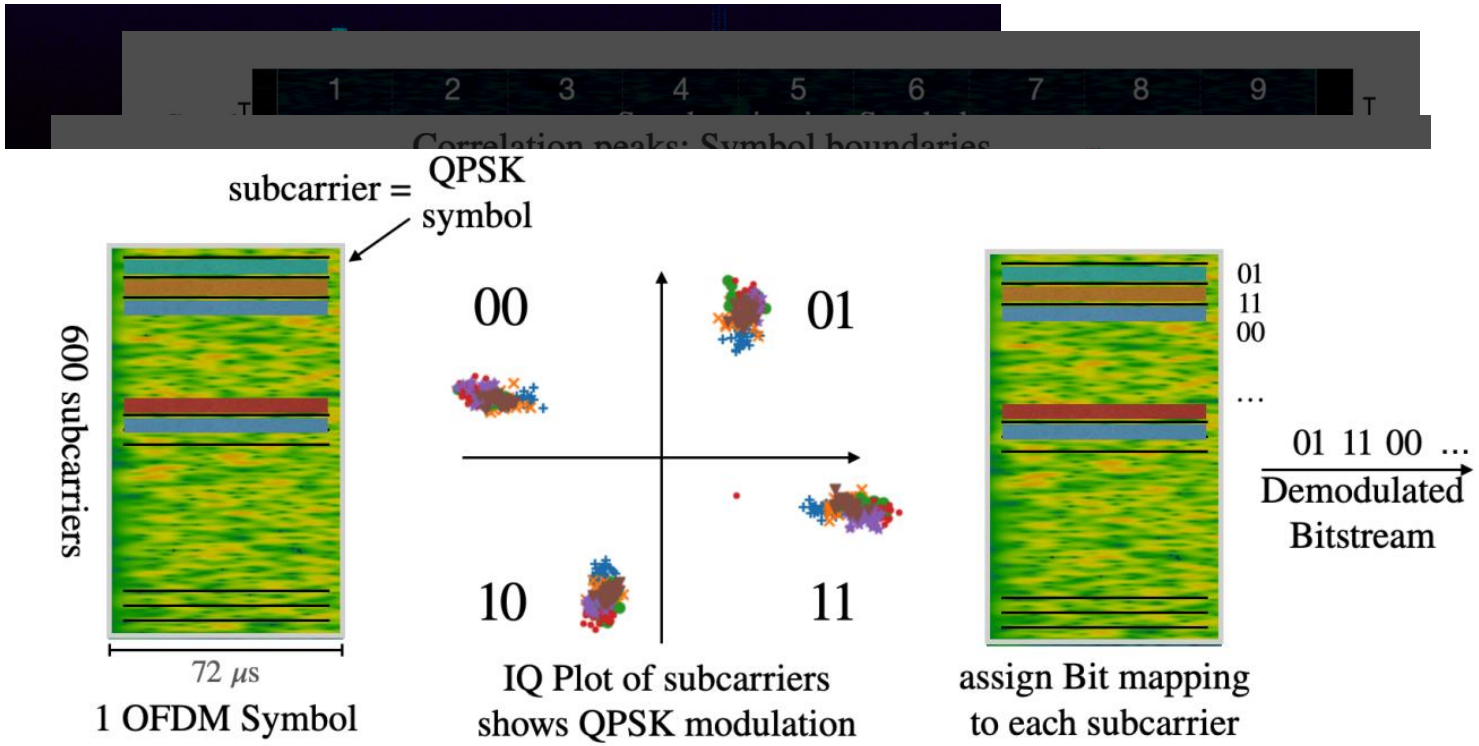
1. Wireless Analysis

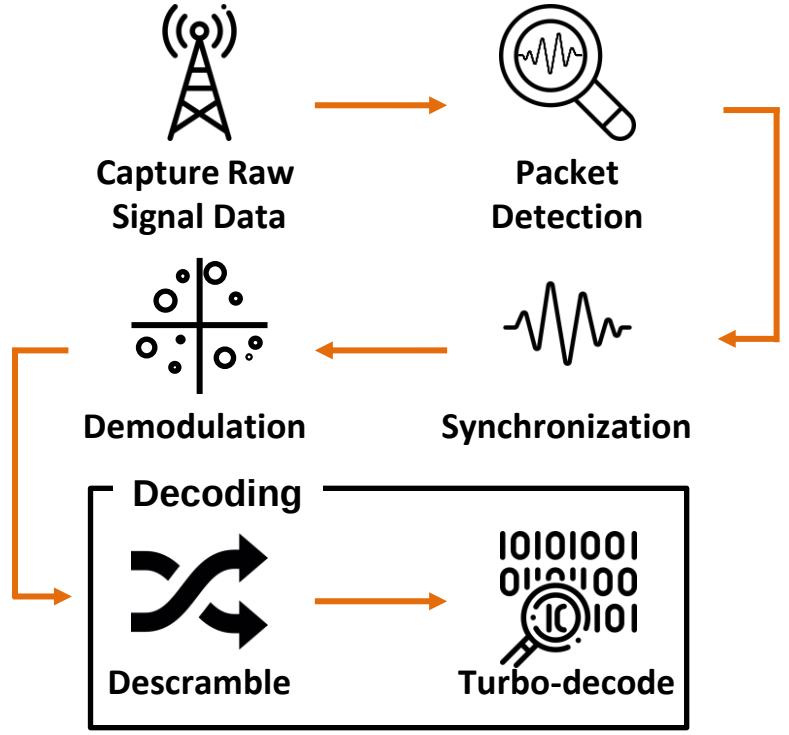




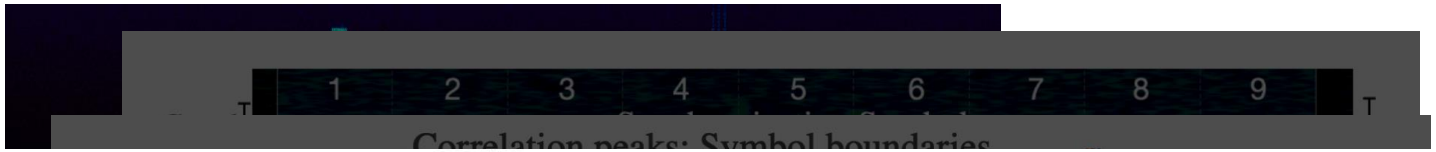
SysSec System Security Lab

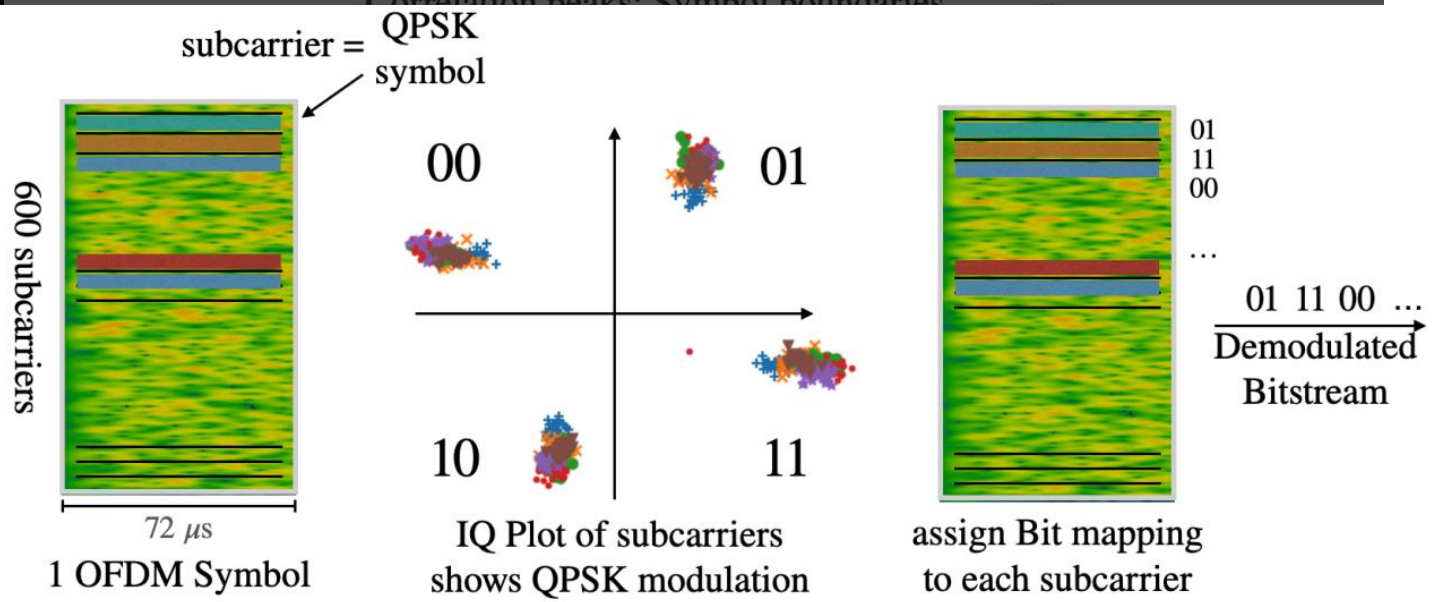
1. Wireless Analysis

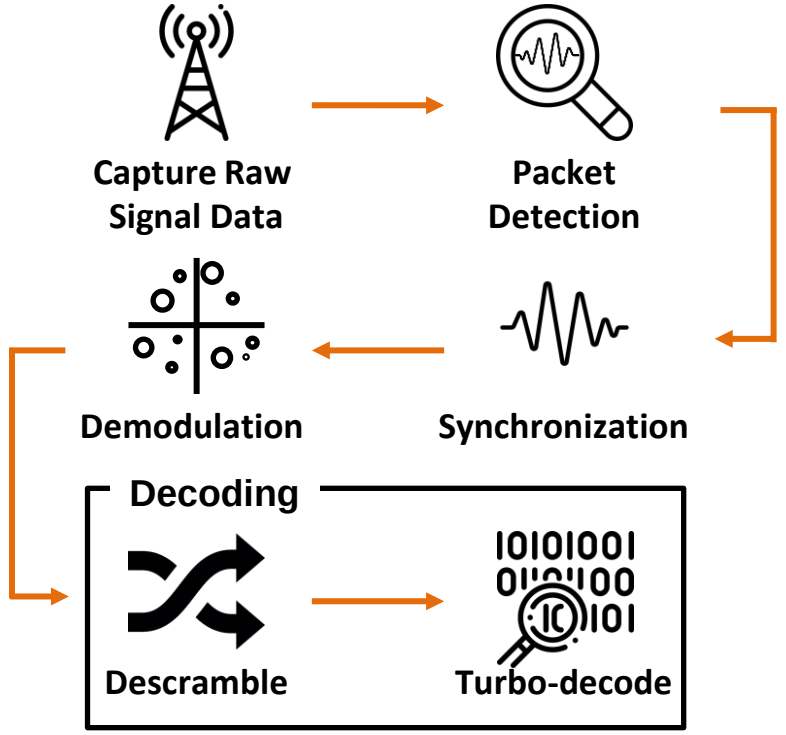




1. Wireless Analysis

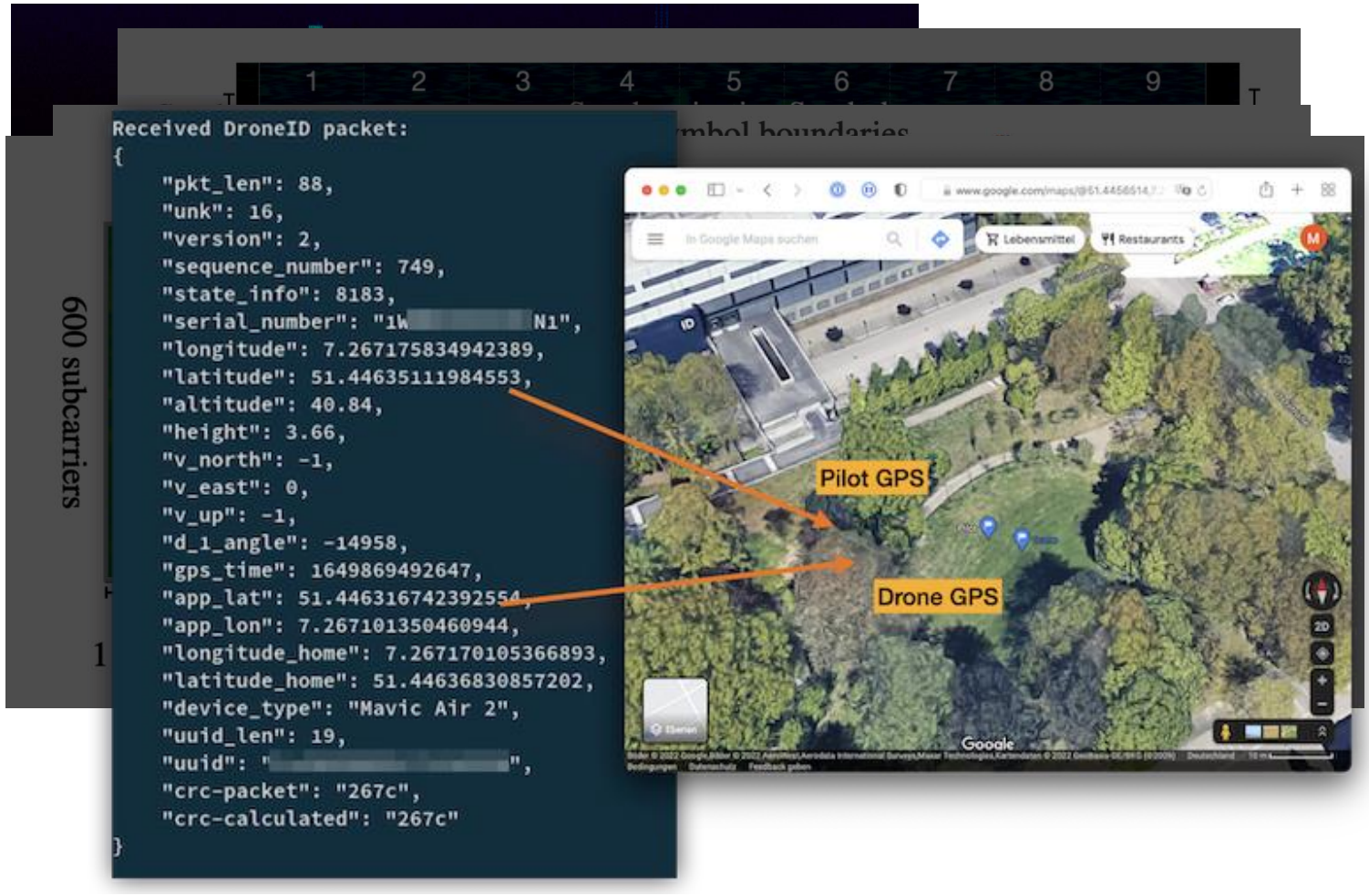


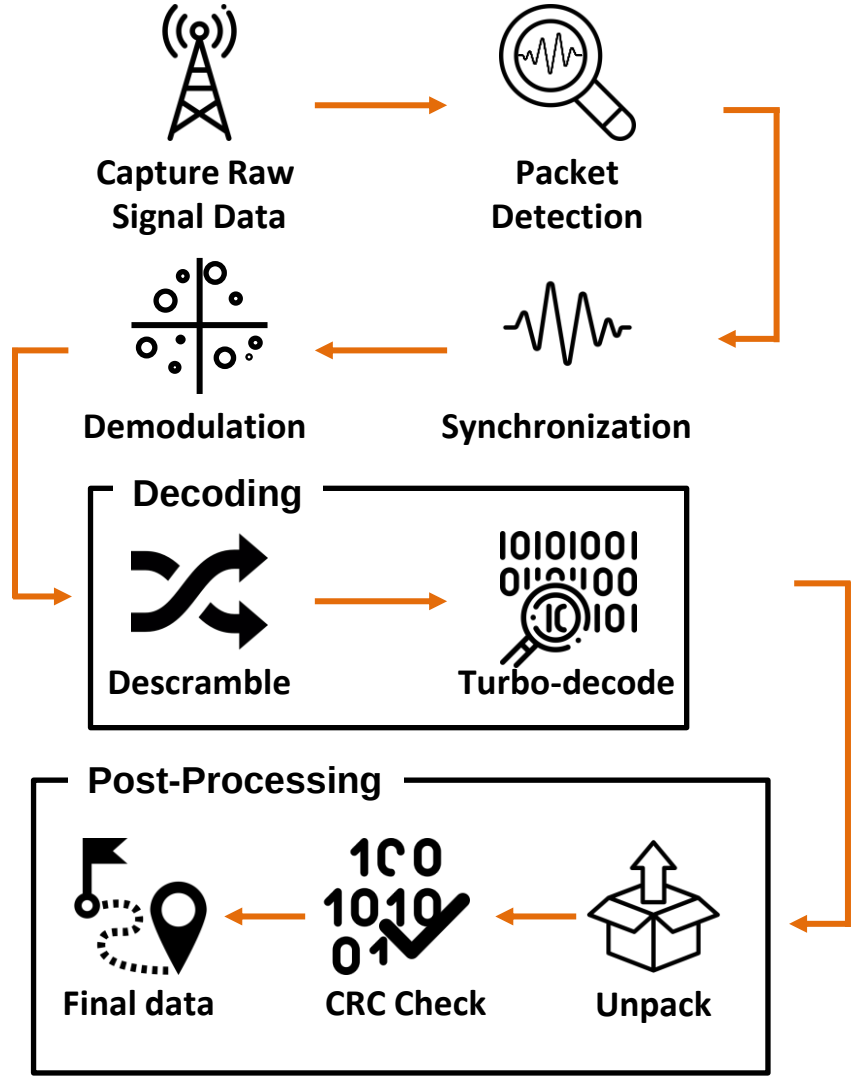




[Seed]
0x12345678

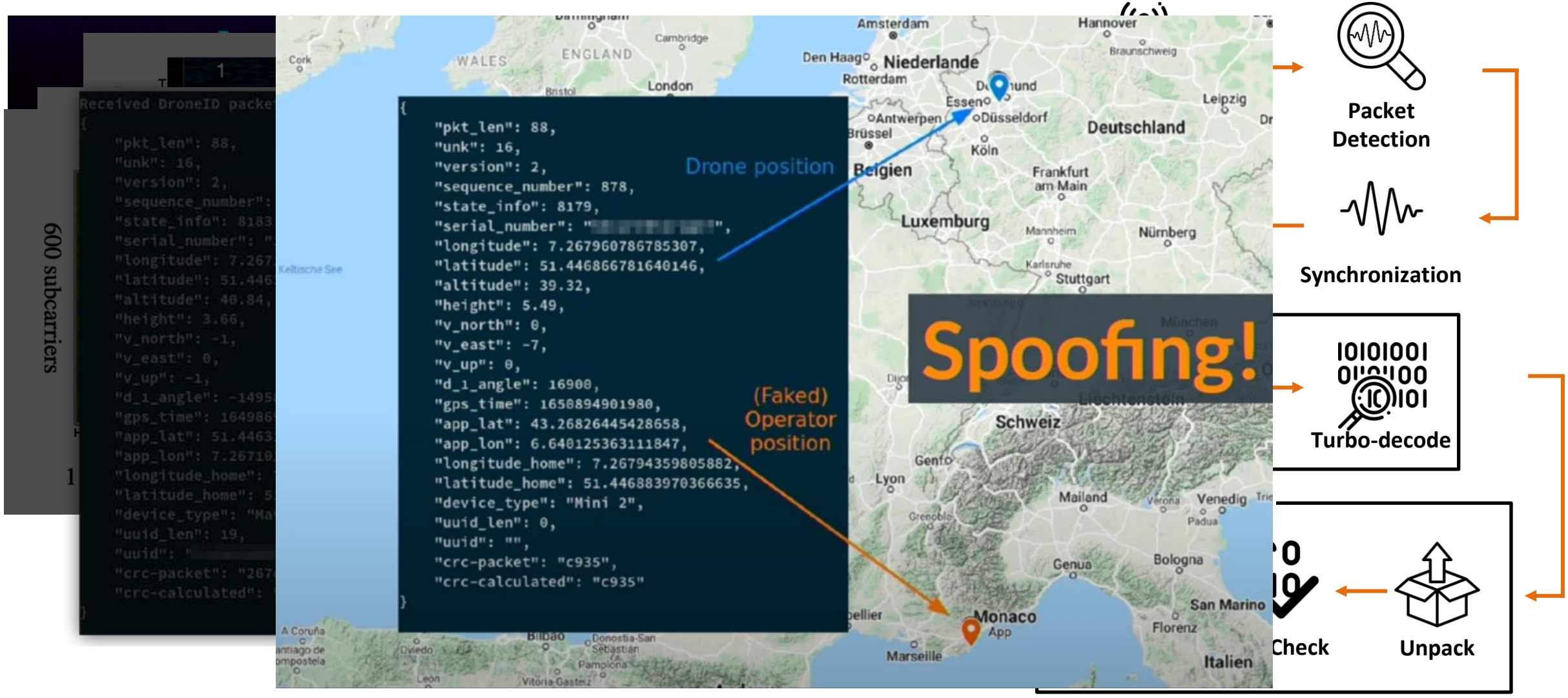
1. Wireless Analysis





SysSec System Security Lab

1. Wireless Analysis

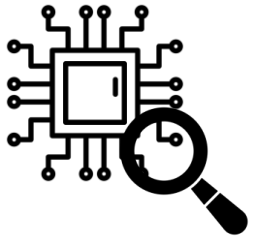


1. Wireless Analysis

- DroneID
  - decodable
  - can be spoofed / disabled

2. Static Analysis

2. Static Analysis



Analyze
PCB

2. Static Analysis

Analyze
PCB

Found
Boot Screen
(UART)!

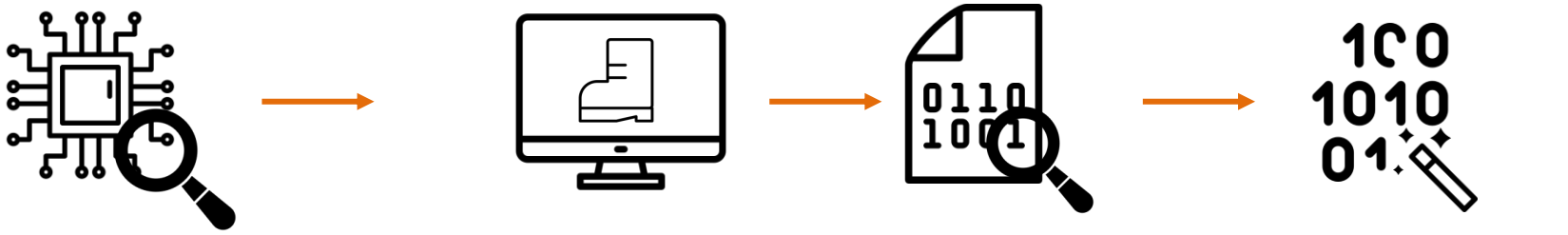
2. Static Analysis

Analyze PCB

Found Boot Screen (UART)!

Check Bootloader Firmware

2. Static Analysis



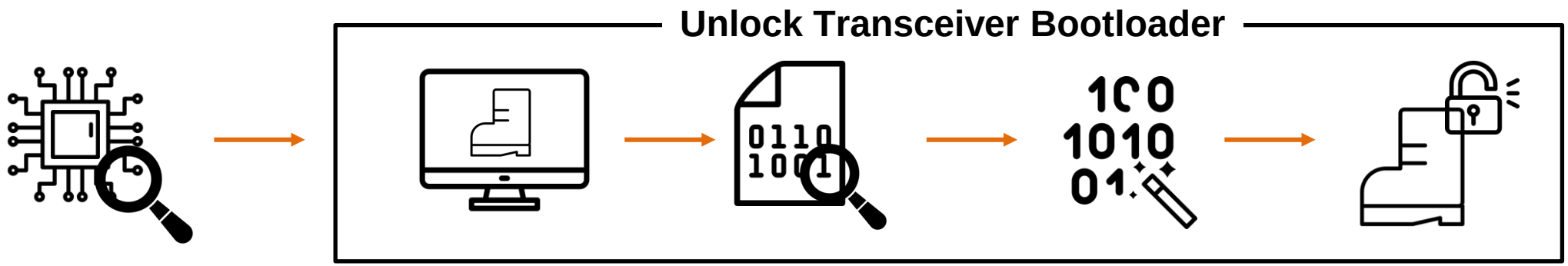
Analyze PCB

Found Boot Screen (UART)!

Check Bootloader Firmware

Three Magic Values to Unlock Bootloader?!

2. Static Analysis



Analyze PCB

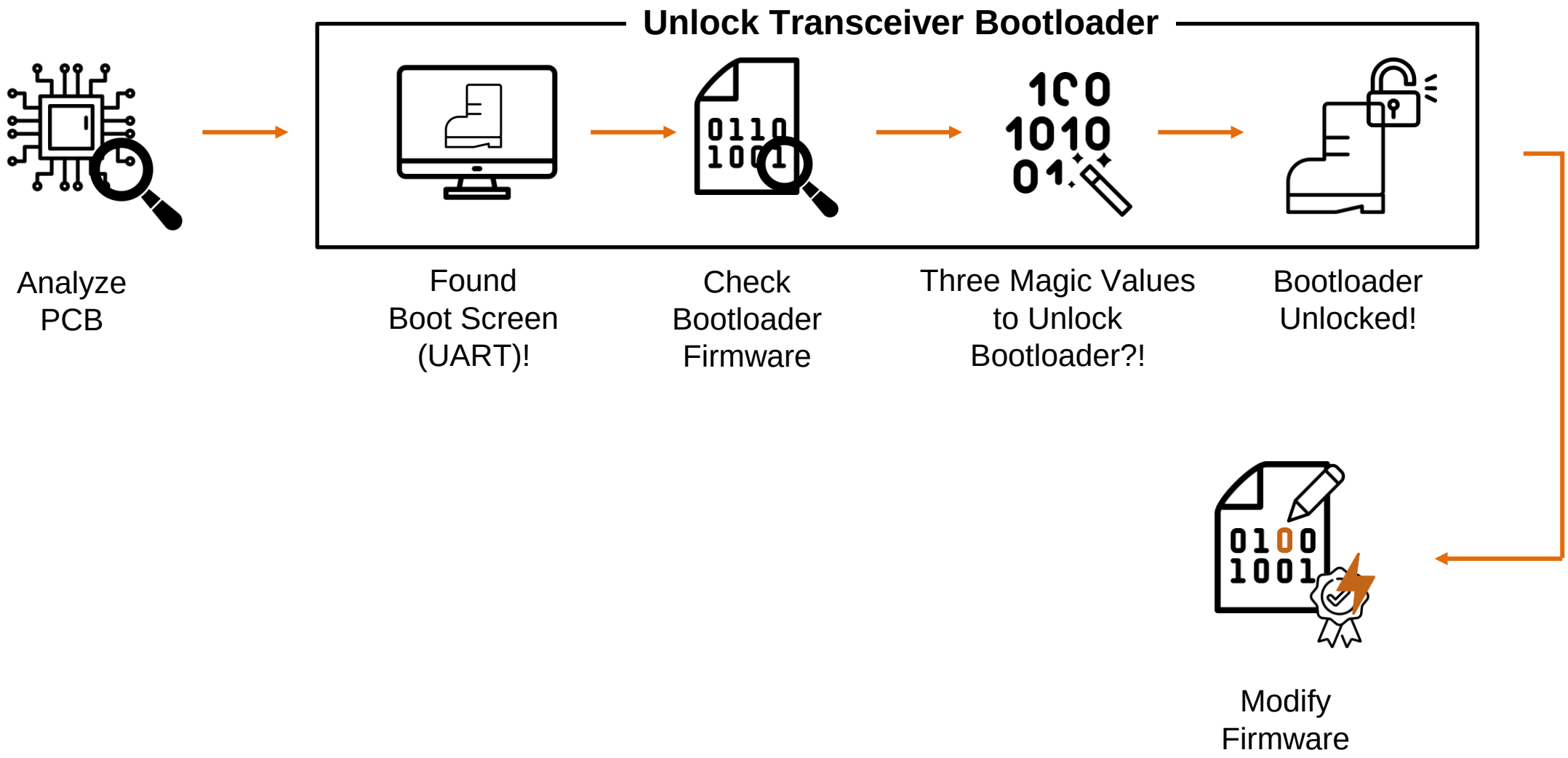
Found Boot Screen (UART)!

Check Bootloader Firmware

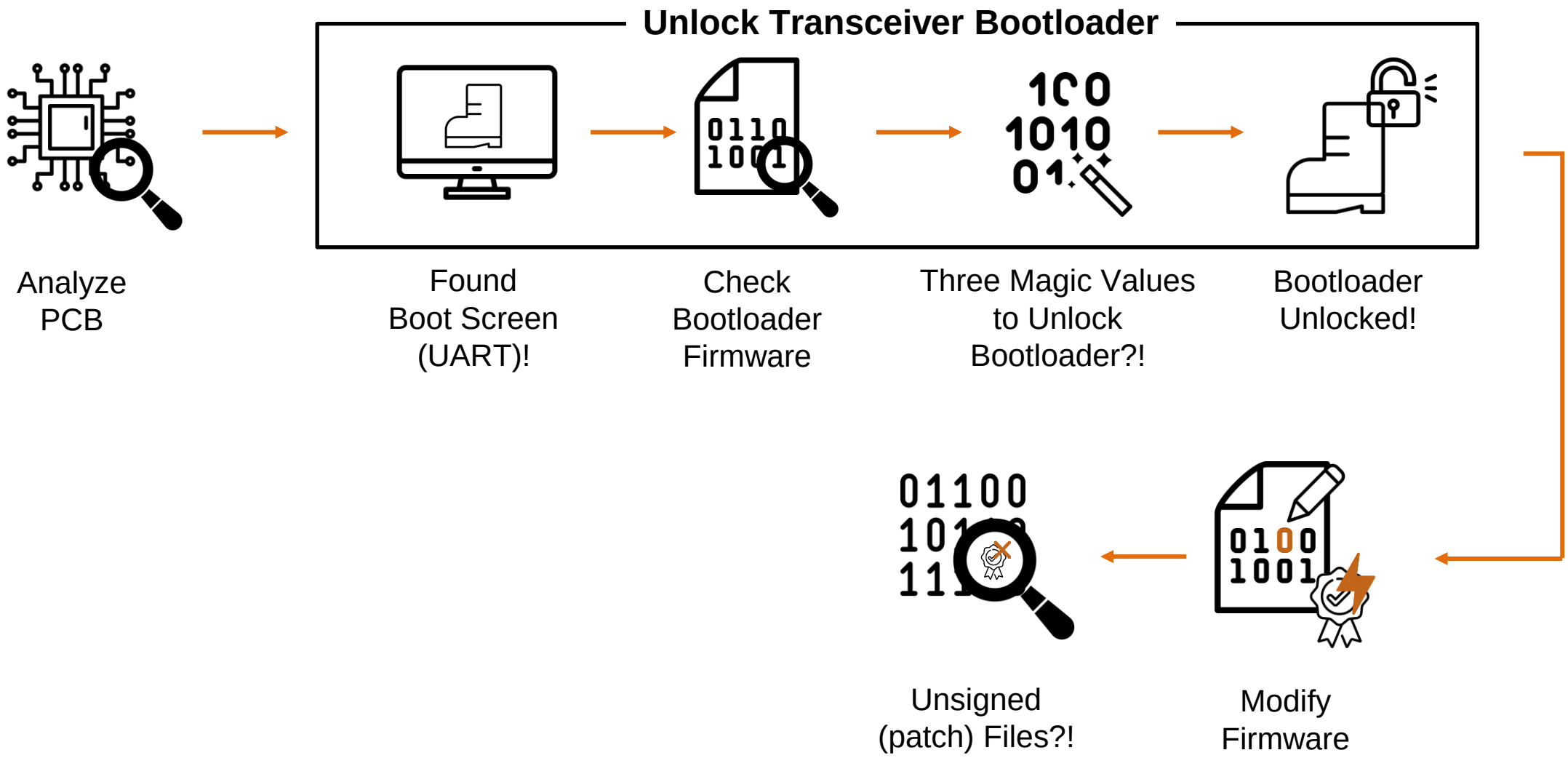
Three Magic Values to Unlock Bootloader?!

Bootloader Unlocked!

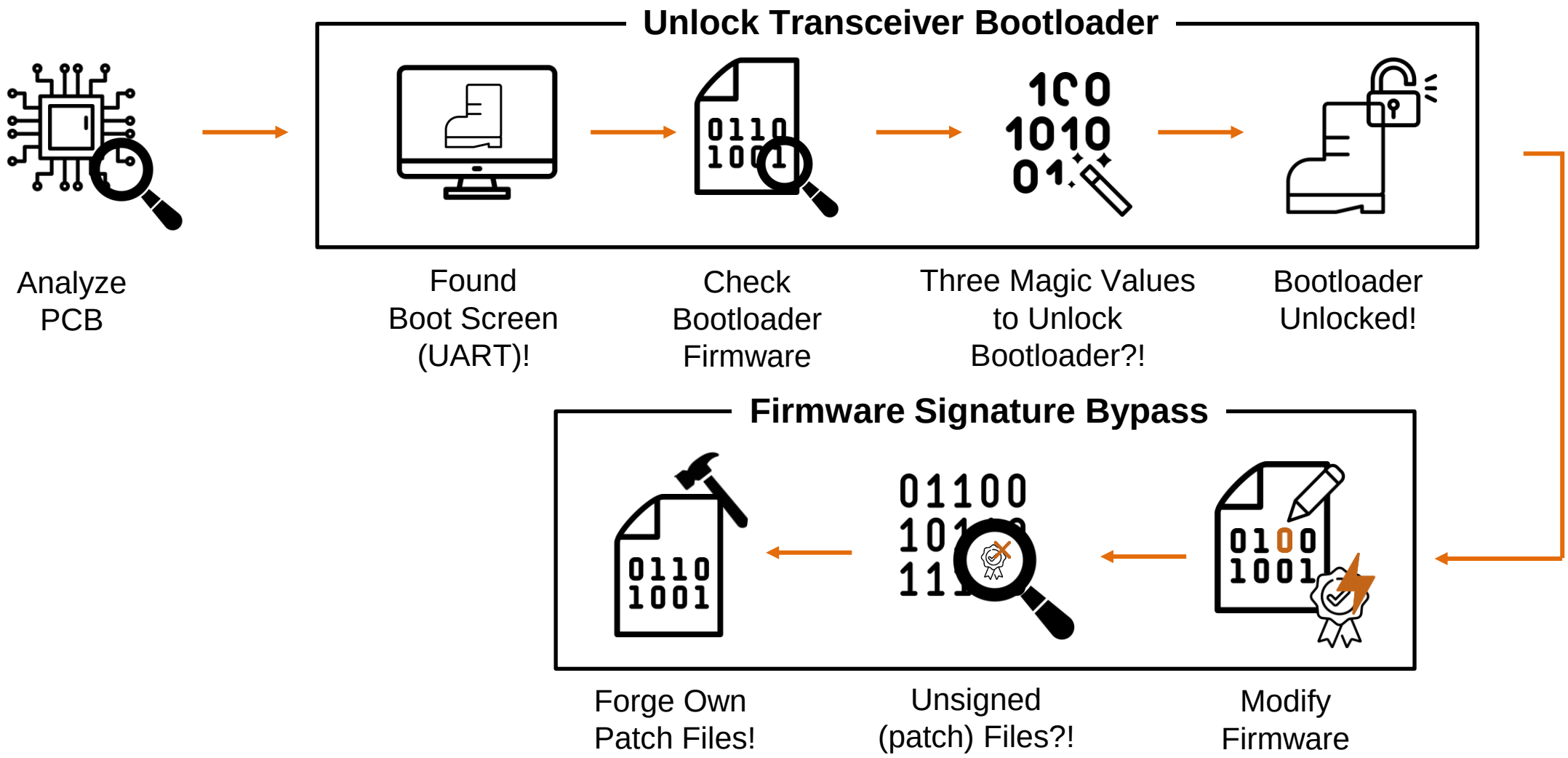
2. Static Analysis



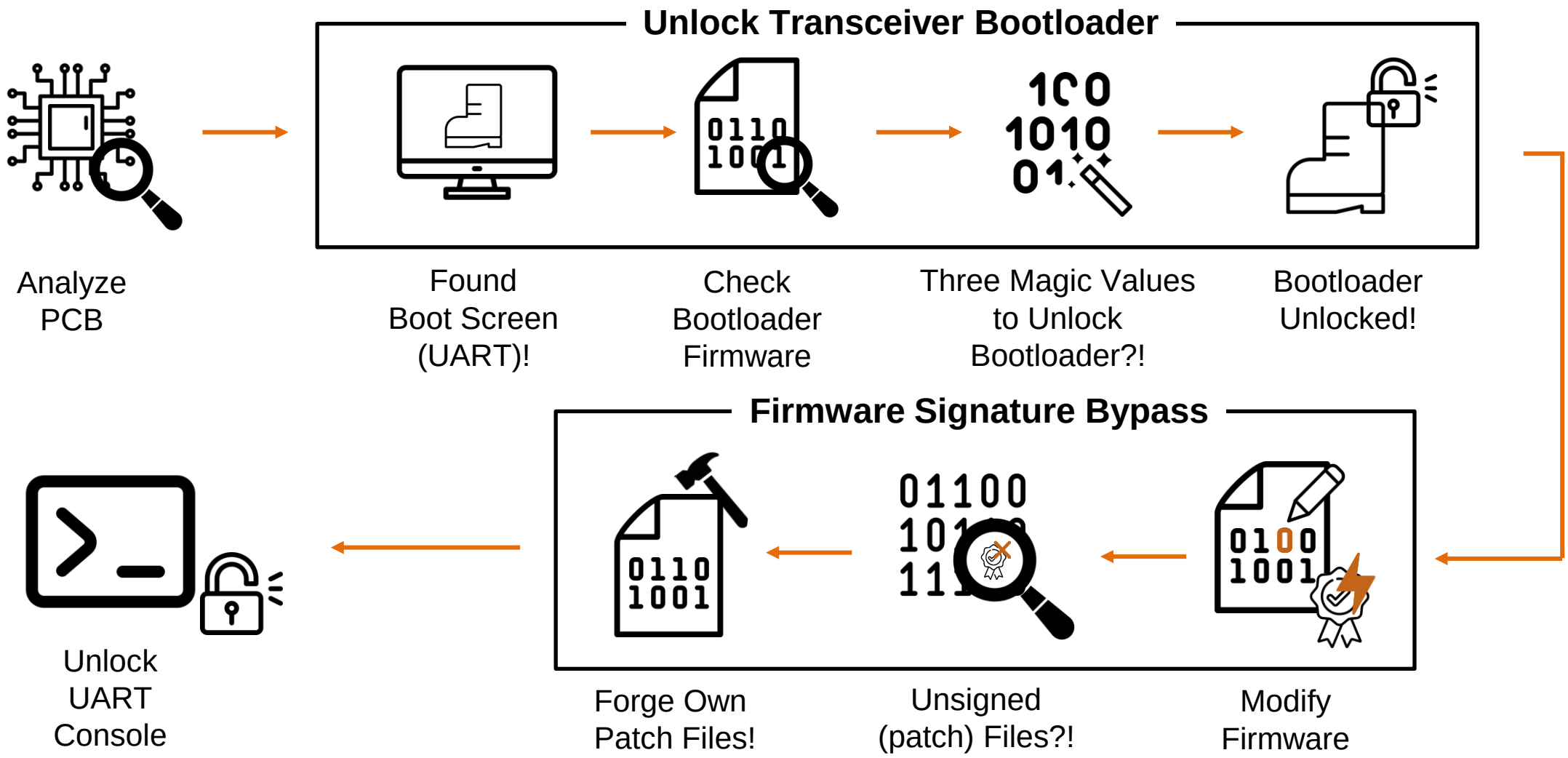
2. Static Analysis



2. Static Analysis



2. Static Analysis



2. Static Analysis

- Firmware signature bypass
- UART console

3. Dynamic Analysis

3. Dynamic Analysis

- How to Fuzz Real Drones?

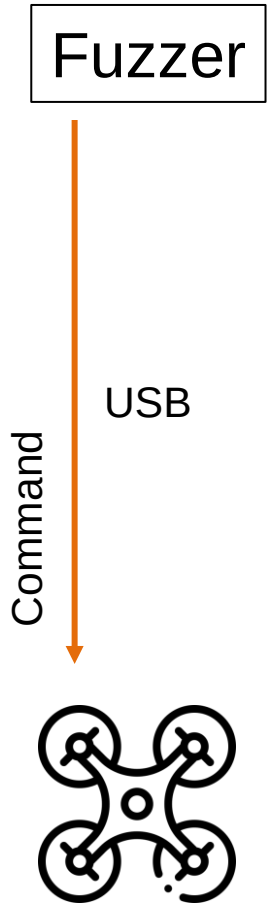
3. Dynamic Analysis

- How to Fuzz Real Drones?
  - Prerequisites
    - A drone and fuzzer

Fuzzer

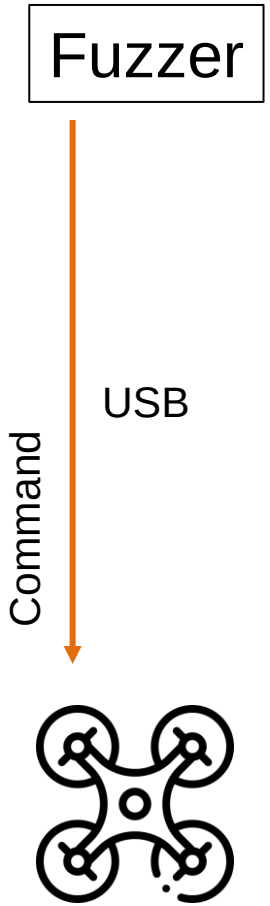
3. Dynamic Analysis

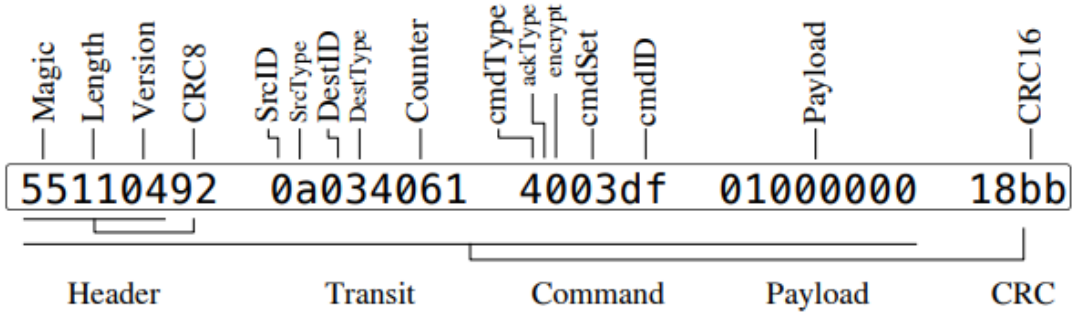
- How to Fuzz Real Drones?
  - Prerequisites
    - A drone and fuzzer



3. Dynamic Analysis

- How to Fuzz Real Drones?
  - Prerequisites
    - A drone and fuzzer
    - Protocol knowledge

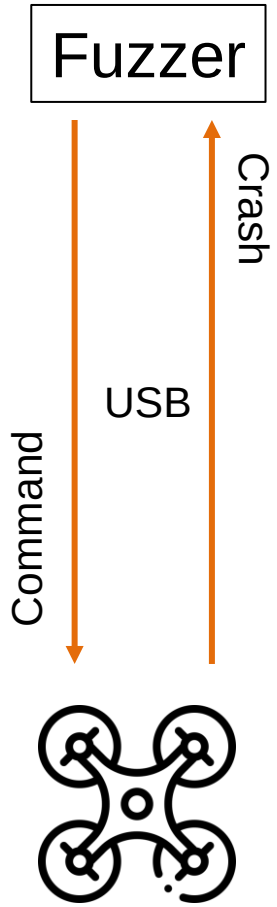




DUML protocol

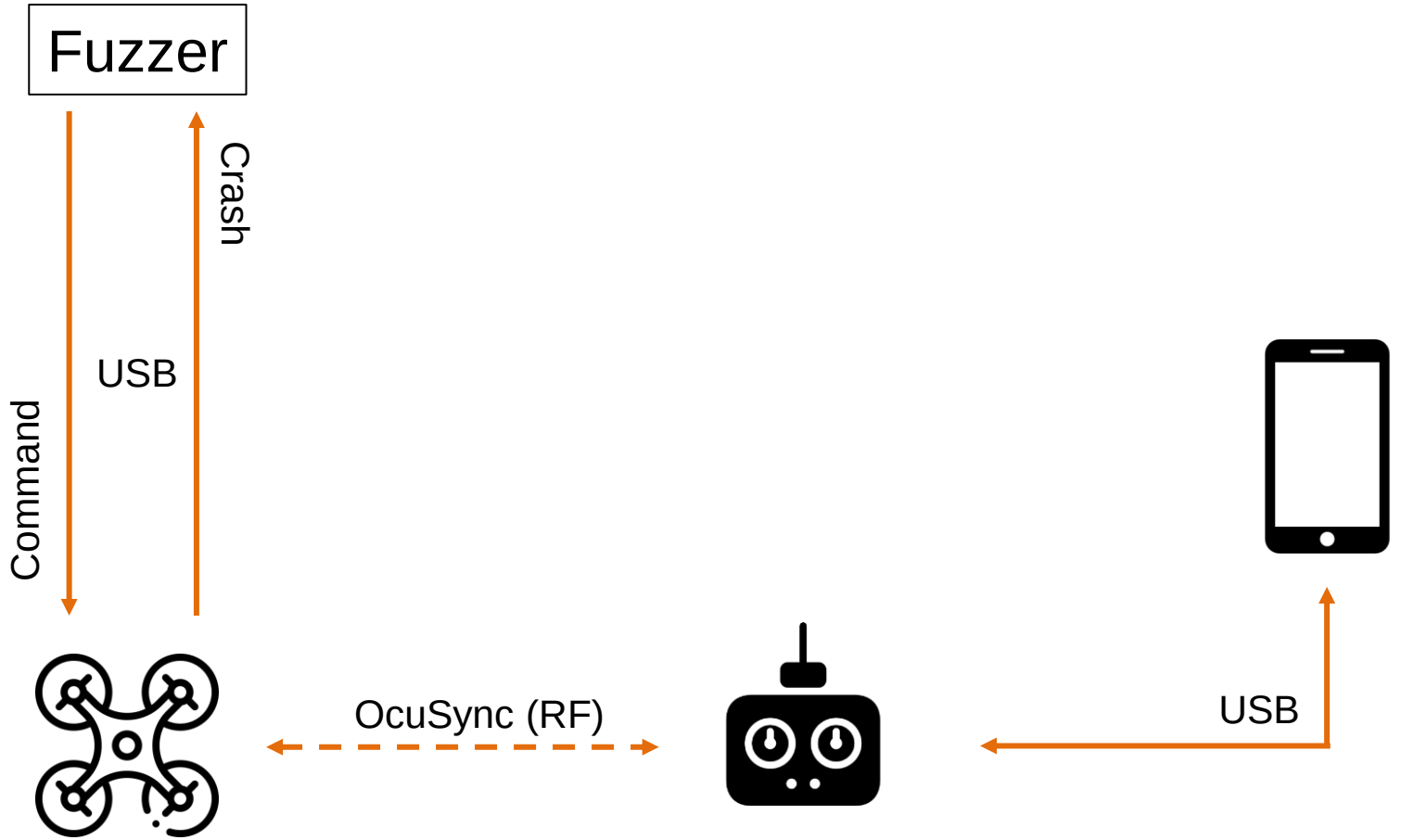
3. Dynamic Analysis

- How to Fuzz Real Drones?
  - Prerequisites
    - A drone and fuzzer
    - Protocol knowledge
    - Bug oracle



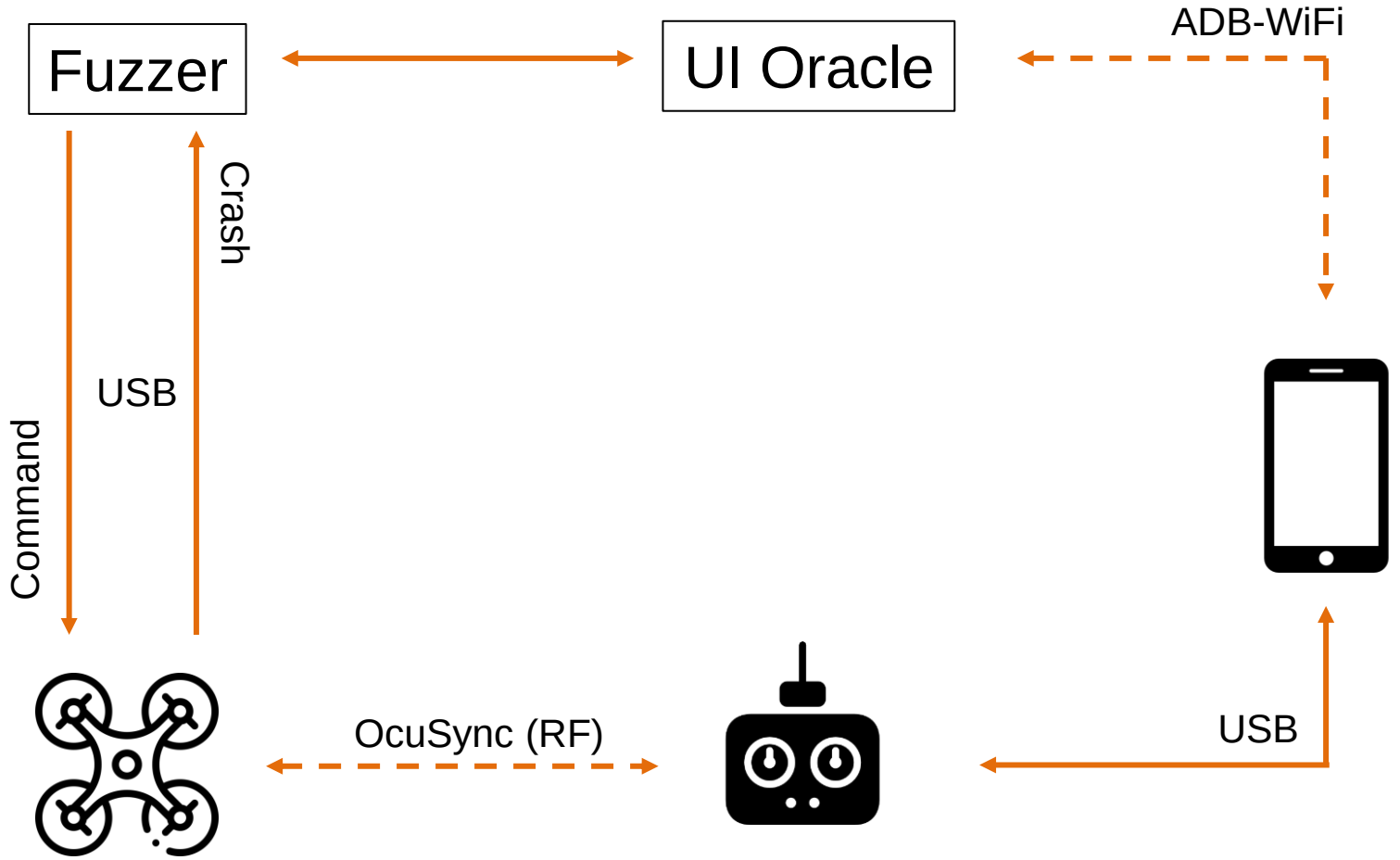
3. Dynamic Analysis

- How to Fuzz Real Drones?
  - Prerequisites
    - A drone and fuzzer
    - Protocol knowledge
    - Bug oracle



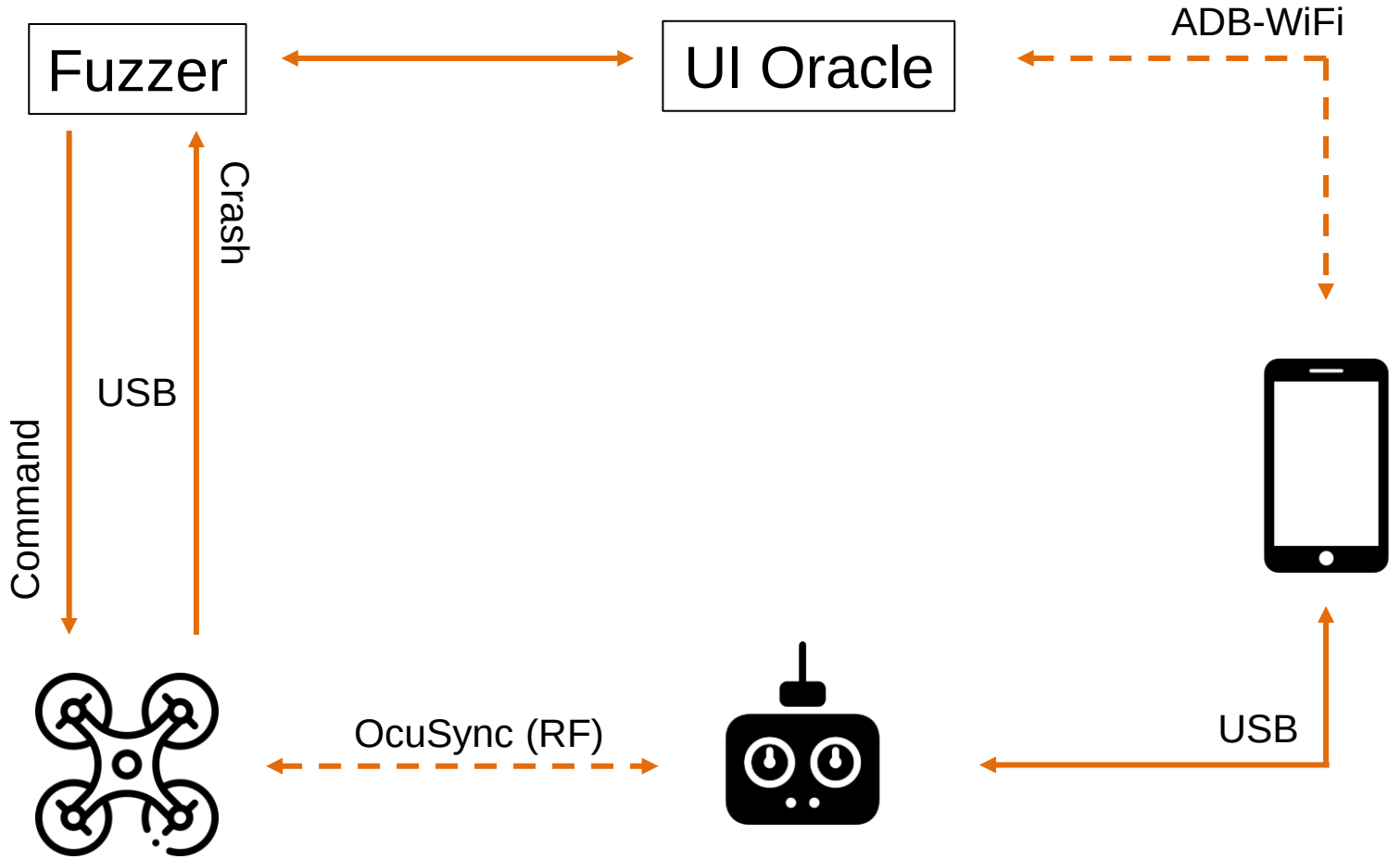
3. Dynamic Analysis

- How to Fuzz Real Drones?
  - Prerequisites
    - A drone and fuzzer
    - Protocol knowledge
    - Bug oracle



3. Dynamic Analysis

- How to Fuzz Real Drones?
  - Prerequisites
    - A drone and fuzzer
    - Protocol knowledge
    - Bug oracle



Reproducible bugs!

3. Dynamic Analysis

- Fuzzing result

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

3. Dynamic Analysis

- Fuzzing result

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

3. Dynamic Analysis

- Fuzzing result

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

3. Dynamic Analysis

- Fuzzing result

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

Summary

Summary

- Position tracking
  - DroneID is decodable
  - DroneID can be spoofed / disabled
- Hardware protection
  - Debugging interfaces can be enabled
  - Firmware signature verification is bypassed
- Fuzzing
  - 15 vulnerabilities (3 x low, 12 x medium)

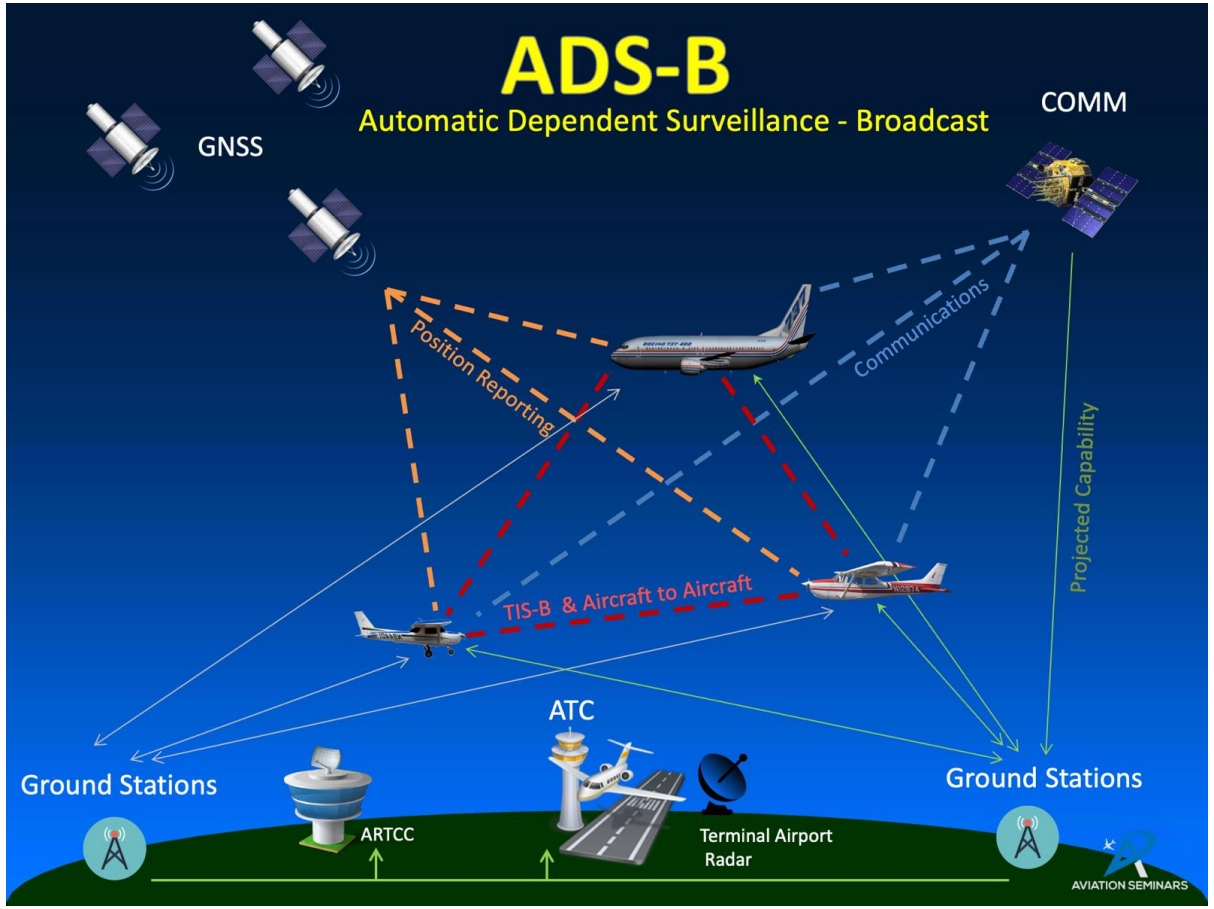
RUB-SysSec/DroneSecurity

Conclusion

- DroneID is still unencrypted
- This paper discovered several information of unknown protocol and it is very meaningful approach.

Related Work - previous

- ADS-B



Related Work - previous

- Security Analysis of FHSS-type Drone Controller(WISA ’15)

Coverage #	Partial hopping sequence	Length
1 (Ch1∼Ch9)	7, 1, 6, 5, 4, 9, 3, 8, 2, 7, 1, 6, 5, 4, 3, 2, 1, 9, 8, 7, 6, 5, 4, 9, 3, 8, 2	27
2 (Ch1∼Ch17)	7, 1, 12, 6, 11, 5, 10, 4, 9, 3, 8, 2, 7, 1, 6, 17, 5, 16, 4, 15, 3, 14, 2, 13, 1, 12, 17, 11, 16, 10, 15, 9, 14, 8, 13, 7, 12, 6, 17, 11, 5, 16, 10, 4, 15, 9, 3, 14, 8, 2, 13	51
3 (Ch9∼Ch25)	12, 23, 11, 22, 10, 21, 9, 20, 25, 19, 24, 18, 23, 17, 22, 16, 21, 15, 20, 14, 25, 19, 13, 24, 18, 12, 23, 17, 11, 22, 16, 10, 21, 15, 9, 20, 14, 19, 13, 18, 12, 17, 11, 16, 10, 15, 9, 14, 25, 13, 24	51
4 (Ch17∼Ch33)	26, 31, 25, 30, 24, 29, 23, 28, 22, 33, 27, 21, 32, 26, 20, 31, 25, 19, 30, 24, 18, 29, 23, 17, 28, 22, 27, 21, 26, 20, 25, 19, 24, 18, 23, 17, 22, 33, 21, 32, 20, 31, 19, 30, 18, 29, 17, 28, 33, 27, 32	51
5 (Ch25∼Ch41)	41, 29, 40, 28, 39, 27, 38, 26, 37, 25, 36, 41, 35, 40, 34, 39, 33, 38, 32, 37, 31, 36, 30, 41, 35, 29, 40, 34, 28, 39, 33, 27, 38, 32, 26, 37, 31, 25, 36, 30, 35, 29, 34, 28, 33, 27, 32, 26, 31, 25, 30	51
6 (Ch33∼Ch47)	44, 43, 42, 47, 41, 46, 40, 45, 39, 44, 38, 43, 37, 42, 36, 47, 41, 35, 46, 40, 34, 45, 39, 33, 44, 38, 43, 37, 42, 36, 41, 35, 40, 34, 39, 33, 38, 37, 36, 47, 35, 46, 34, 45, 33	45
7 (Ch39∼Ch47)	44, 43, 42, 47, 41, 46, 40, 45, 39, 44, 43, 42, 47, 41, 46, 40, 45, 39, 44, 43, 42, 41, 40, 39, 47, 46, 45	27

Table 1: Extracted partial sequences for each coverage

Combined partial periods	7, 1, 36, 30, 24, 12, 6, 47, 35, 29, 23, 11, 5, 46, 34, 28, 22, 10, 4, 45, 33, 27, 21, 9, 3, 44, 32, 26, 20, 8, 2, 43, 31, 25, 19, 7, 1, 42, 30, 24, 18, 6, 47, 41, 29, 23, 17, 5, 46, 40, 28, 22, 16, 4, 45, 39, 27, 21, 15, 3, 44, 38, 26, 20, 14, 2, 43, 37, 25, 19, 13, 1, 42, 36, 24, 18, 12, 47, 41, 35, 23, 17, 11, 46, 40, 34, 22, 16, 10, 45, 39, 33, 21, 15, 9, 44, 38, 32, 20, 14, 8, 43, 37, 31, 19, 13, 7, 42, 36, 30, 18, 12, 6, 41, 35, 29, 17, 11, 5, 40, 34, 28, 16, 10, 4, 39, 33, 27, 15, 9, 3, 38, 32, 26, 14, 8, 2, 37, 31, 25, 13 (Length = 47×3 =141)

Table 2: Acquired total hopping sequence

Further Work

- Signal analysis
  - Ocusync
- Debugging Interface
  - Enhance it and make the debugger

Best questions

- When unencrypted DroneID is encrypted and sent, does the overhead for processing real-time sensitive information such as location information increase? (Kwangmin Kim)

Best questions

- Similar with traditional IoT device fuzzing, can’t we emulate the firmware in to desired system to perform fuzzing? (Dongok Kim)

Best questions

- Is it possible to use TEE to reduce attack vectors in drone software? Is it beneficial to use? If you say no, what is the problem with using TEE? (Hobin Kim)