



Hacking a Professional Drone

Nils Rodday

rodday@arcor.de

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

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



The UAV

Attacks

Live Demonstration

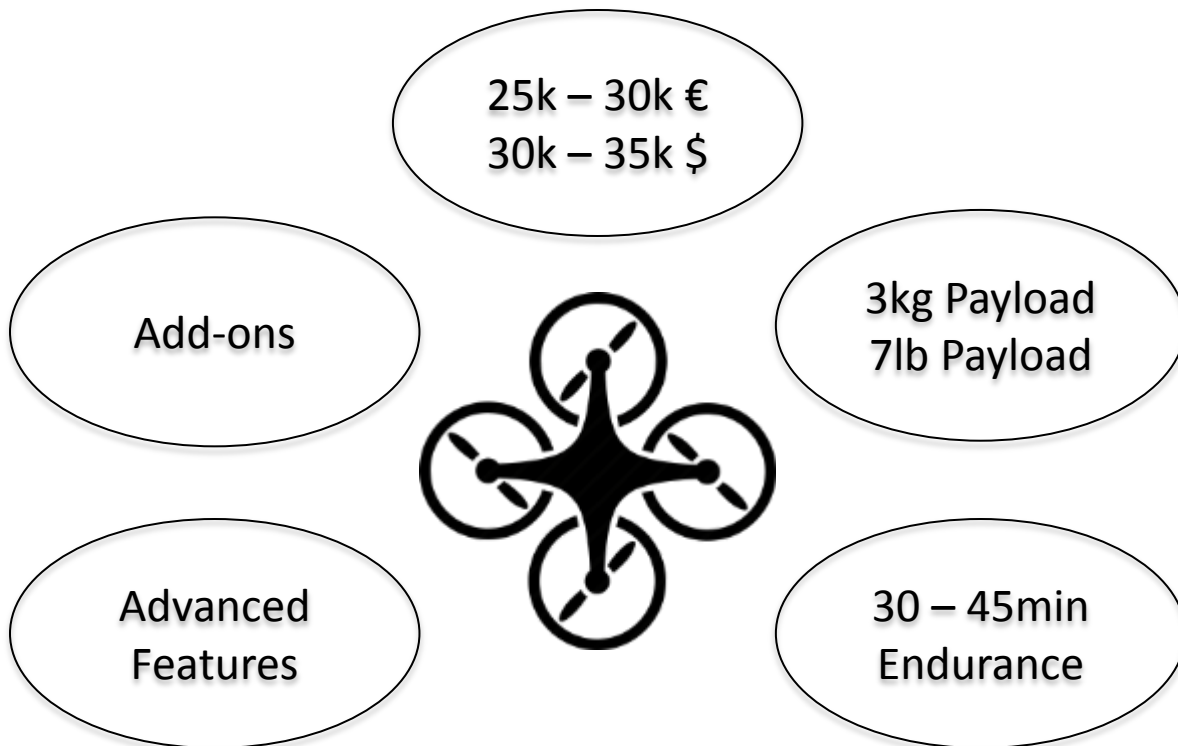
Remediation

Impact

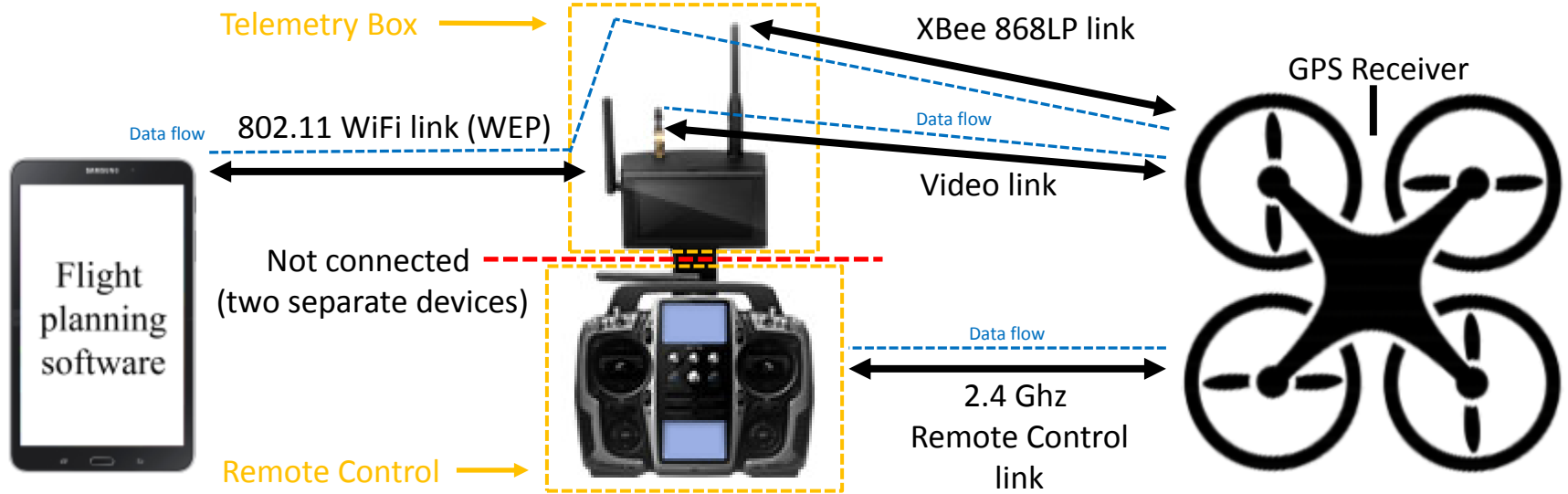
Lessons Learned

Q&A

The UAV – Specifications

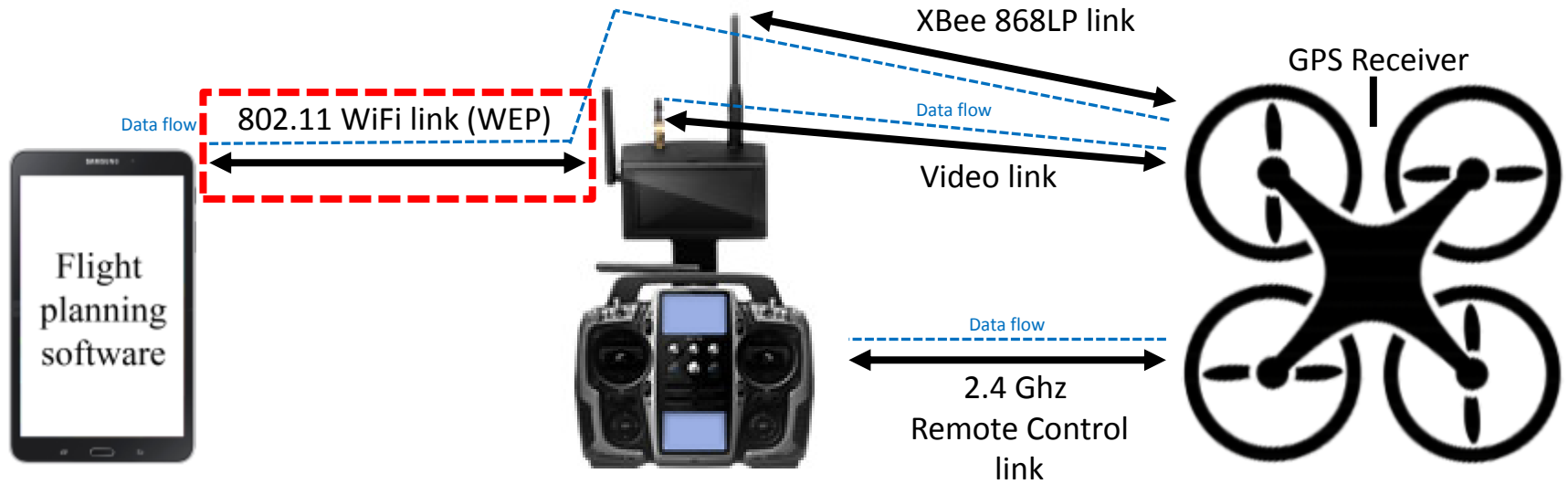


The UAV

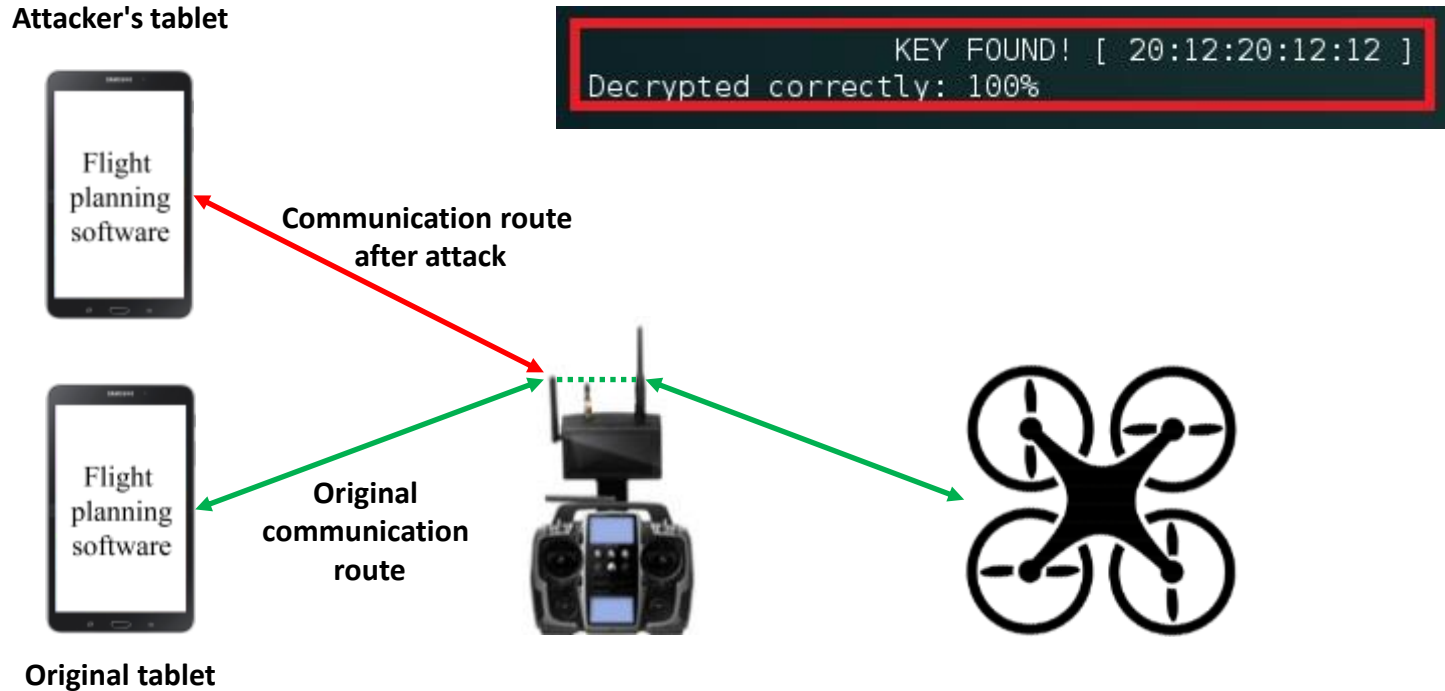


©IEEE

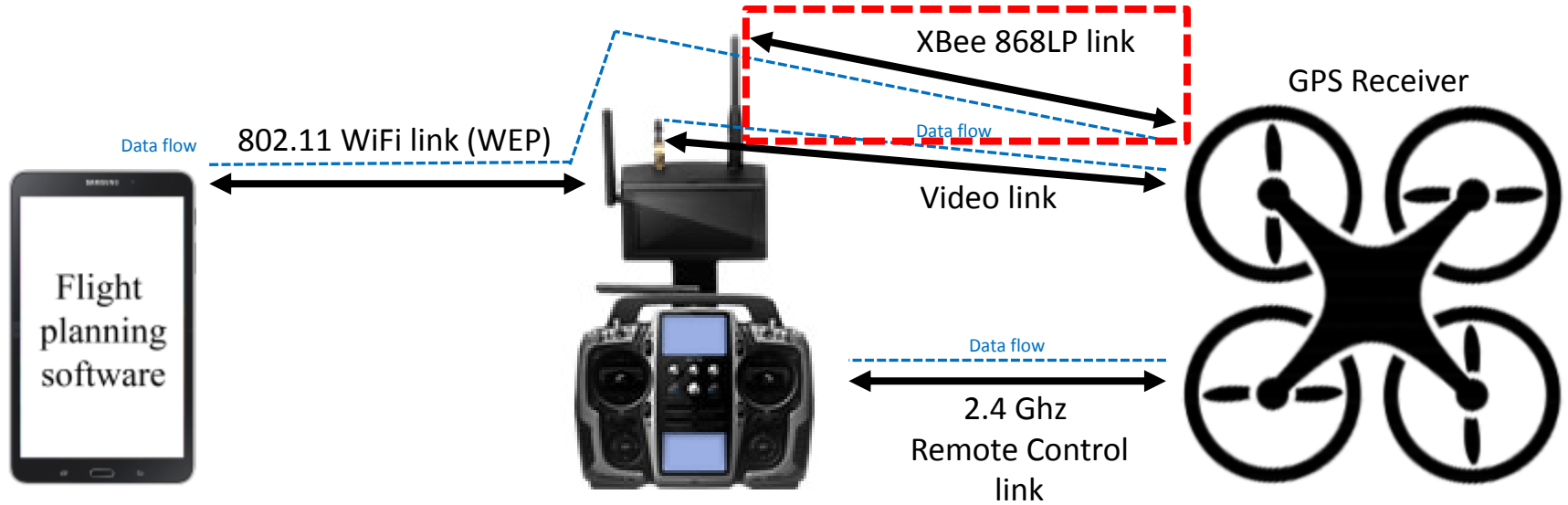
The UAV – Wifi focus



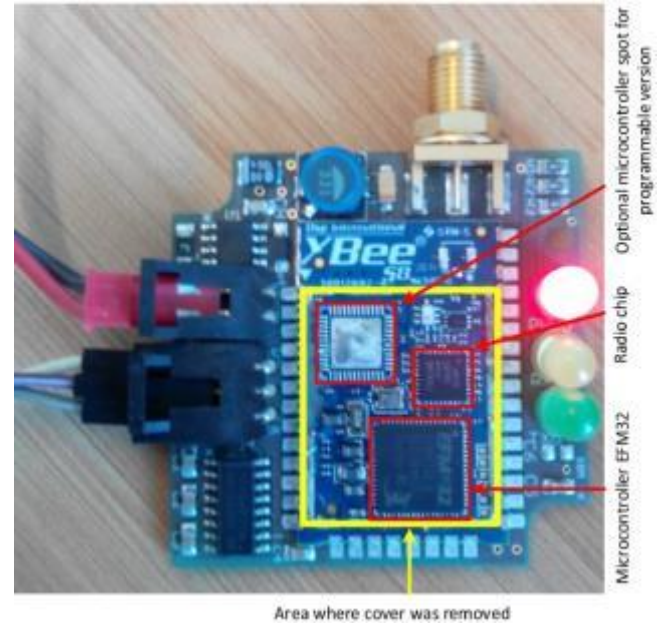
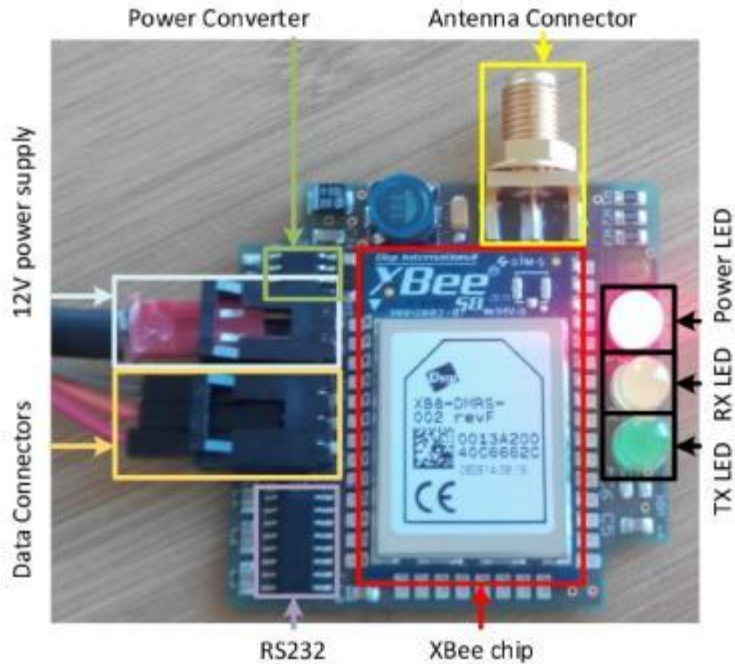
The UAV – Wifi attack



The UAV – XBee focus



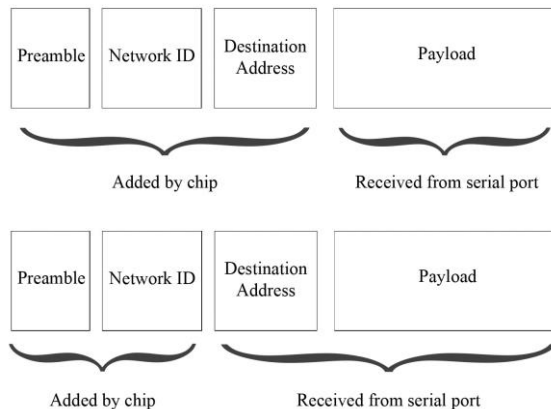
XBee – Chips





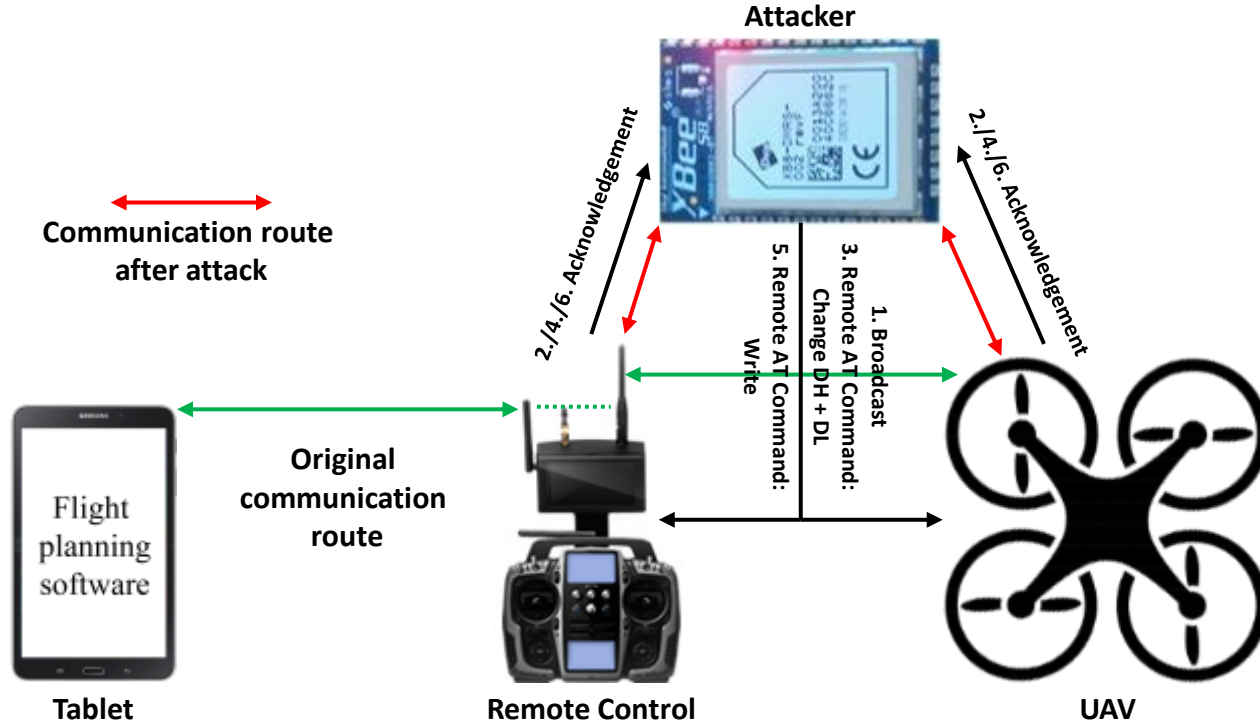
XBee – Reading the manual...

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



It's not a bug, it's a feature 😊

XBee – Man-in-the-Middle Attack

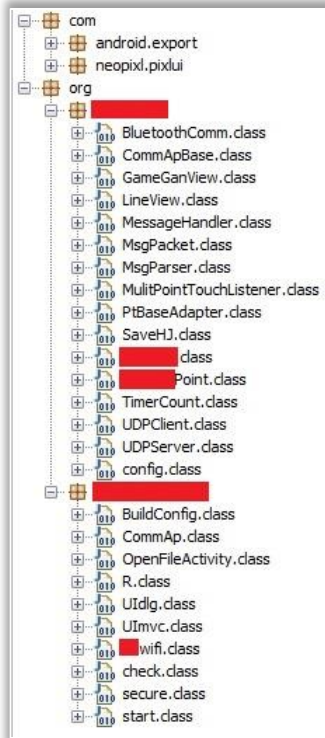


What's next?

We can read/send data on the XBee channel.

But what does that data stream mean?

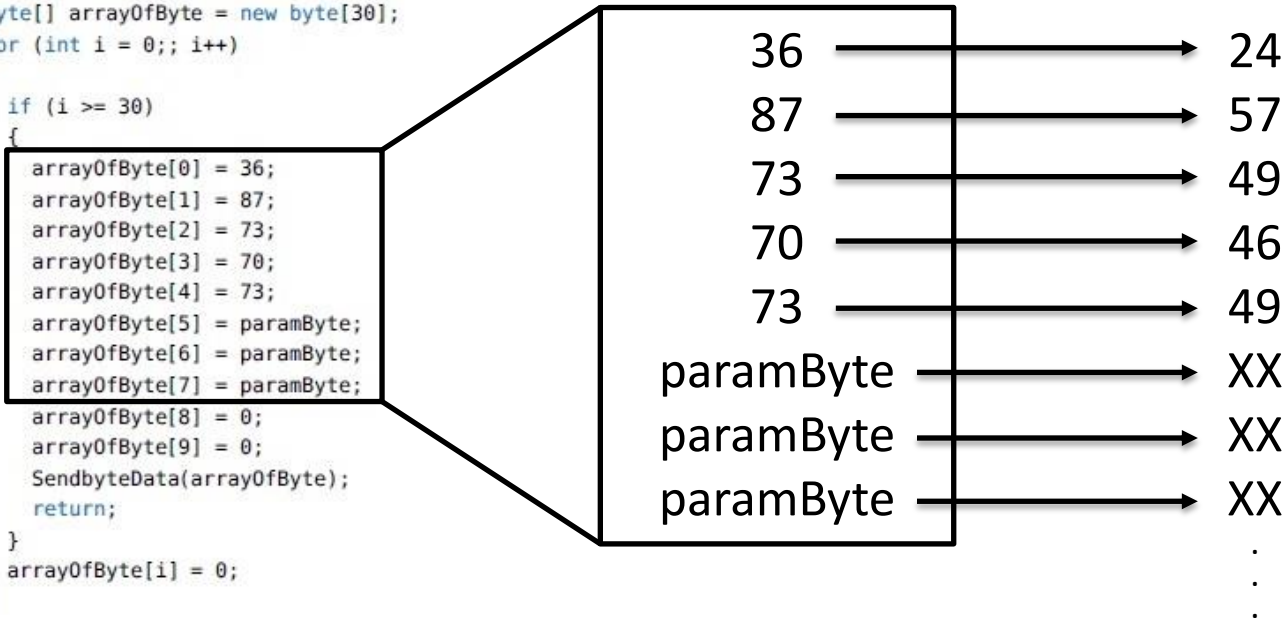
Decompilation of Android APK



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



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)








black hat[®]
ASIA 2016

Demonstration

Remediation – XBee Onboard Encryption

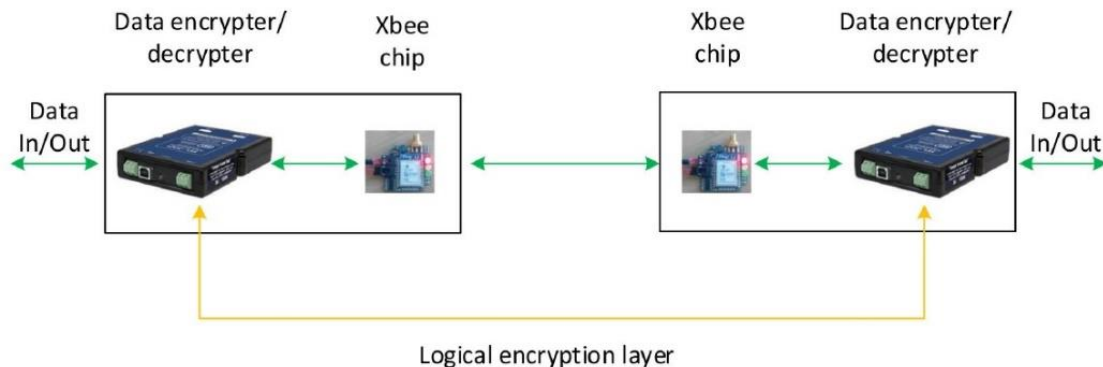
▼ Security

Change Security Parameters

 EE Encryption Enable	Disabled [0]	 
 KY AES Encryption Key	<input type="text"/>	 

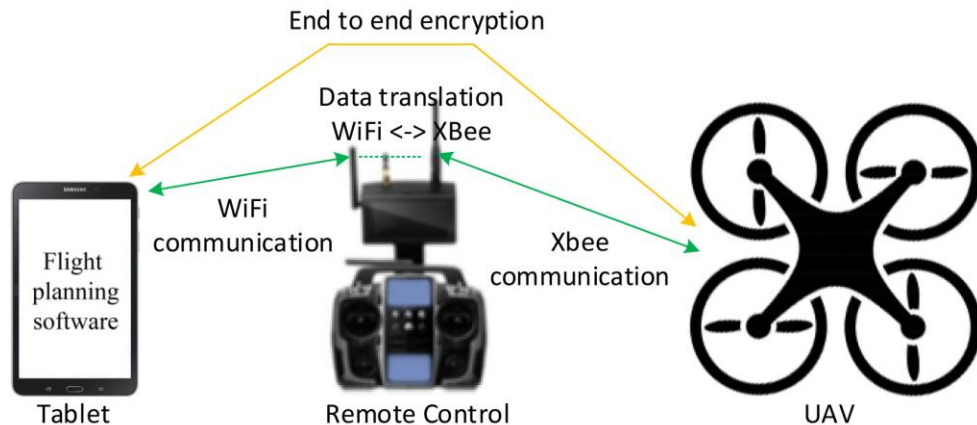
- Secures Data ONLY on the XBee channel
- Prevents Remote-AT-Commands
- Mitigates Man-in-the-Middle

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.



Prof. Dr. Aiko Pras

Dr. Ricardo de O. Schmidt



Ruud Verbij

Matthieu Paques

Atul Kumar

Annika Dahms

Nils Rodday



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



rodday@arcor.de



Hacking a Professional Drone

Nils Rodday

rodday@arcor.de

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

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	Magnetic Compass - Horizontal Alignment
24 57 49 46 49 69 69 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	Upload Waypoint Data
(01 6D 0C 63 42 80 21 8B BF 0F 27 00 00 FF FF 5A 00 EB 00 00 00 00 00 00)	(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 confirmation (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 35 35 35	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 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 24 57 49 46 49 8C 8C 8C 00 00 00 00 00 00 24 00 00 00 00 00 00 24 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 9C	Preset PTZLock
24 57 49 46 49 D2 D2 D2	Video Recording Start/Stop
24 57 49 46 49 90 90 90	Stadicans Alignment
24 57 49 46 49 91 91 91	Capture Roll
24 57 49 46 49 92 92 92	Capture Pitch

- Slide 5 & 12: Photo credit to: 978-1-5090-0223-8/16/\$31.00 © 2016 IEEE