Drone Hacking Basics

Intro to UAS Architectures, Attack Vectors and RF Hacking

Matt Koskela

June 15, 2017

Outline

Drone Architectures

RF Basics

Information Gathering

RF Hacking Tools

Exploits & Demos

Q&A

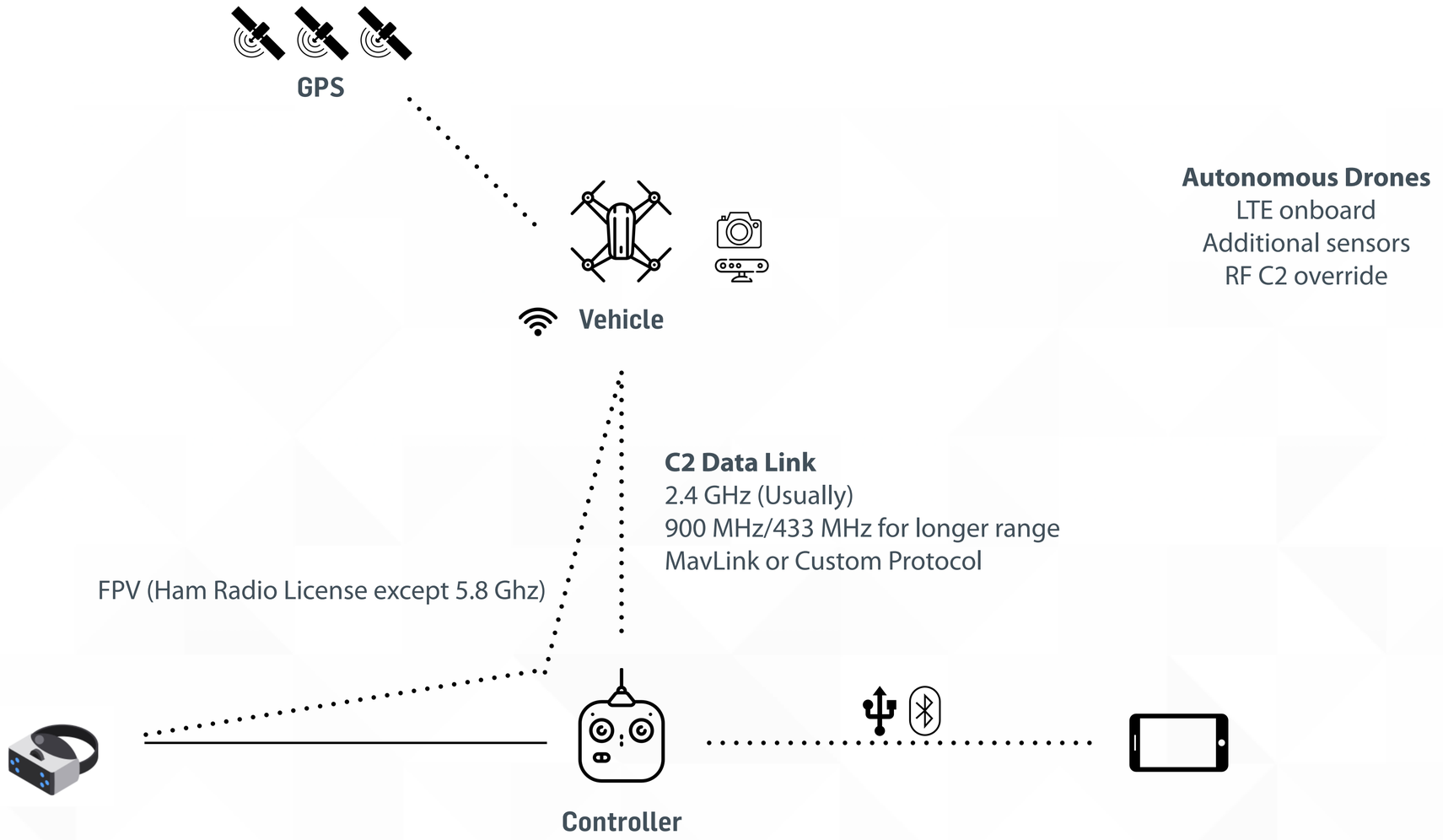
Why?

Wright's Law
Security will not get better until tools for practical exploration of the attack surface are made available.
(Progress increases with experience)

Drone Architectures

Potential Attack Vectors

Drone Architecture Overview



Attack Vectors

C2 Spoofing
Cheers CX-10
Remotely inject commands

Video Intercept
Syma X5SW
Remotely take photos and view live video

WiFi Deauth
Parrot Bebop
Hi-jack possible

GPS Jamming
DJI, Parrot, 3DR, Yuneec, etc
Breaks RTH
Breaks Waypoint & Autonomous Missions

GPS Interference (Aluminum Foil)
DJI
Disables No Fly Zones

Telnet into Drone
Parrot
Able to completely pwn
Run scripts, upload/download video library

Magnetic Field
DJI
No take off due to recalibration

Replay Attacks
Unknown
Record and replay commands remotely

Furious farmer blasts drone out of sky with shotgun for flying over stately country home

An inhabitant of the stately home had clearly had enough of drone pilots trying to sneak a peak at the property

RF Basics

Frequencies, Modulation, Frequency Hopping and Whitening

Frequencies

Primarily ISM Bands

The **industrial, scientific and medical (ISM)** radio bands are radio bands (portions of the radio spectrum) reserved internationally for the use of radio frequency (RF) energy for industrial, scientific and medical purposes other than telecommunications.

Most FPV goggles are either not on ISM or high powered and need license.

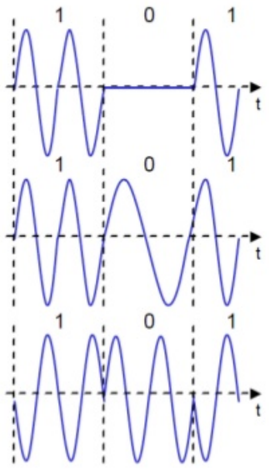
Frequency range		Type	Center frequency	Availability	Licensed users
6.765 MHz	6.795 MHz	A	6.78 MHz	Subject to local acceptance	FIXED SERVICE & Mobile service
13.553 MHz	13.567 MHz	B	13.56 MHz	Worldwide	FIXED & Mobile services except Aeronautical mobile (R) service
26.957 MHz	27.283 MHz	B	27.12 MHz	Worldwide	FIXED & MOBILE SERVICE except Aeronautical mobile service, CB Radio
40.66 MHz	40.7 MHz	B	40.68 MHz	Worldwide	Fixed, Mobile services & Earth exploration-satellite service
433.05 MHz	434.79 MHz	A	433.92 MHz	only in Region 1, subject to local acceptance	AMATEUR SERVICE & RADIOLOCATION SERVICE, additional apply the provisions of footnc
902 MHz	928 MHz	B	915 MHz	Region 2 only (with some exceptions)	FIXED, Mobile except aeronautical mobile & Radiolocation service; in Region 2 additional Ama
2.4 GHz	2.5 GHz	B	2.45 GHz	Worldwide	FIXED, MOBILE, RADIOLOCATION, Amateur & Amateur-satellite service
5.725 GHz	5.875 GHz	B	5.8 GHz	Worldwide	FIXED-SATELLITE, RADIOLOCATION, MOBILE, Amateur & Amateur-satellite service
24 GHz	24.25 GHz	B	24.125 GHz	Worldwide	AMATEUR, AMATEUR-SATELLITE, RADIOLOCATION & Earth exploration-satellite service (a
61 GHz	61.5 GHz	A	61.25 GHz	Subject to local acceptance	FIXED, INTER-SATELLITE, MOBILE & RADIOLOCATION SERVICE
122 GHz	123 GHz	A	122.5 GHz	Subject to local acceptance	EARTH EXPLORATION-SATELLITE (passive), FIXED, INTER-SATELLITE, MOBILE, SPACE service
244 GHz	246 GHz	A	245 GHz	Subject to local acceptance	RADIOLOCATION, RADIO ASTRONOMY, Amateur & Amateur-satellite service

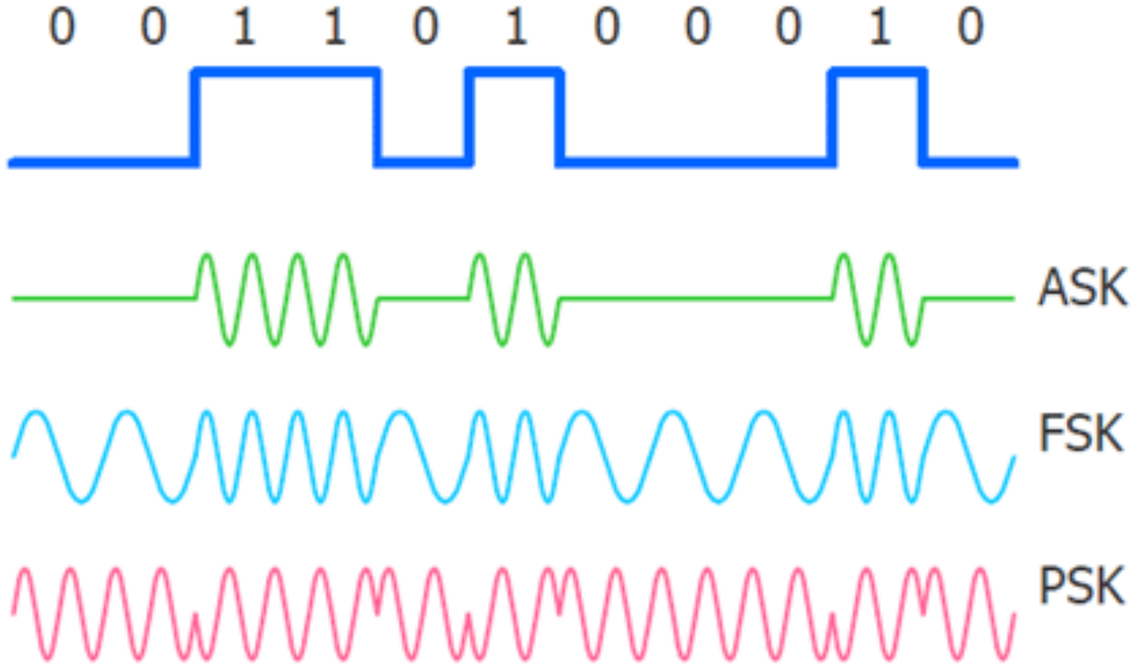
Frequency	Wavelength	Designation	Abbreviation[6]
3–30 Hz	10^5–10^4 km	Extremely low frequency	ELF
30–300 Hz	10^4–10^3 km	Super low frequency	SLF
300–3000 Hz	10^3–100 km	Ultra low frequency	ULF
3–30 kHz	100–10 km	Very low frequency	VLF
30–300 kHz	10–1 km	Low frequency	LF
300 kHz – 3 MHz	1 km – 100 m	Medium frequency	MF
3–30 MHz	100–10 m	High frequency	HF
30–300 MHz	10–1 m	Very high frequency	VHF
300 MHz – 3 GHz	1 m – 10 cm	Ultra high frequency	UHF
3–30 GHz	10–1 cm	Super high frequency	SHF
30–300 GHz	1 cm – 1 mm	Extremely high frequency	EHF
300 GHz – 3 THz	1 mm – 0.1 mm	Tremendously high frequency	THF

Modulation

Digital modulation techniques

- Amplitude Shift Keying (ASK):
  - change amplitude with each symbol – frequency constant
  - low bandwidth requirements
  - very susceptible to interference
- Frequency Shift Keying (FSK):
  - change frequency with each symbol
  - needs larger bandwidth
- Phase Shift Keying (PSK):
  - Change phase with each symbol
  - More complex
  - robust against interference

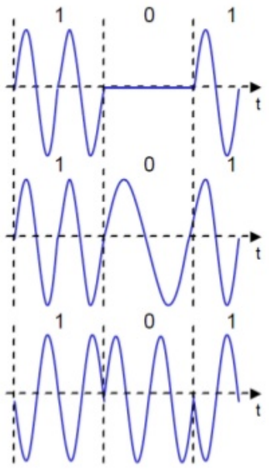




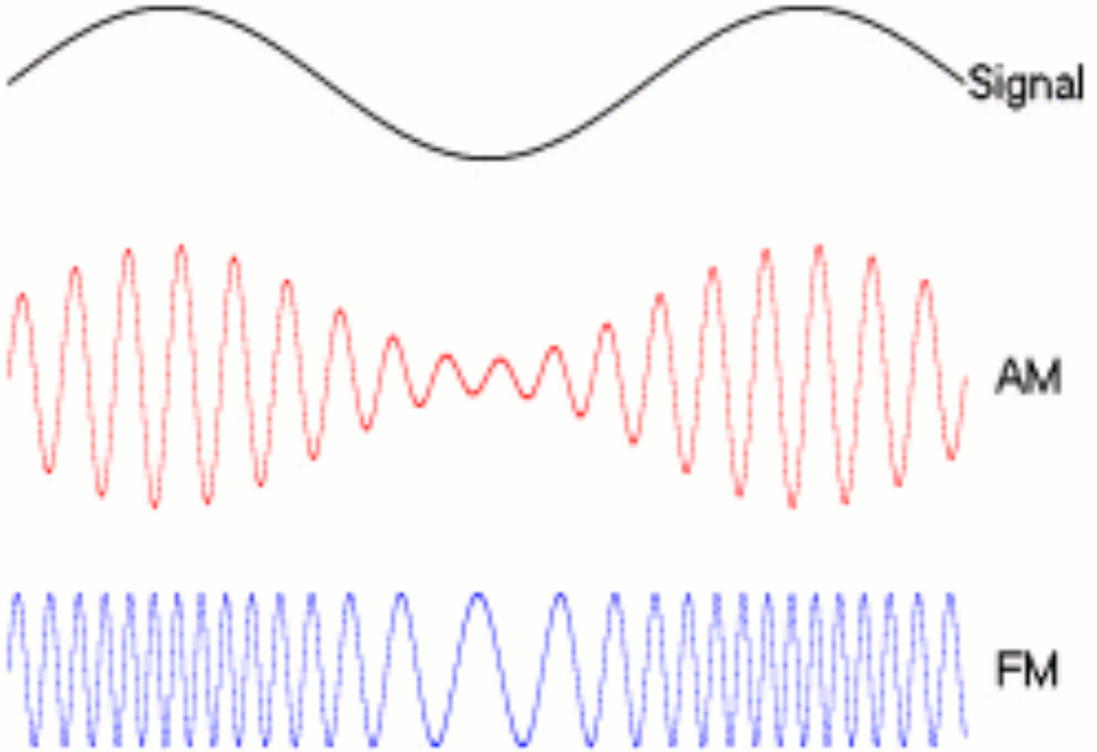
Modulation

Digital modulation techniques

- Amplitude Shift Keying (ASK):
  - change amplitude with each symbol – frequency constant
  - low bandwidth requirements
  - very susceptible to interference
- Frequency Shift Keying (FSK):
  - change frequency with each symbol
  - needs larger bandwidth
- Phase Shift Keying (PSK):
  - Change phase with each symbol
  - More complex
  - robust against interference

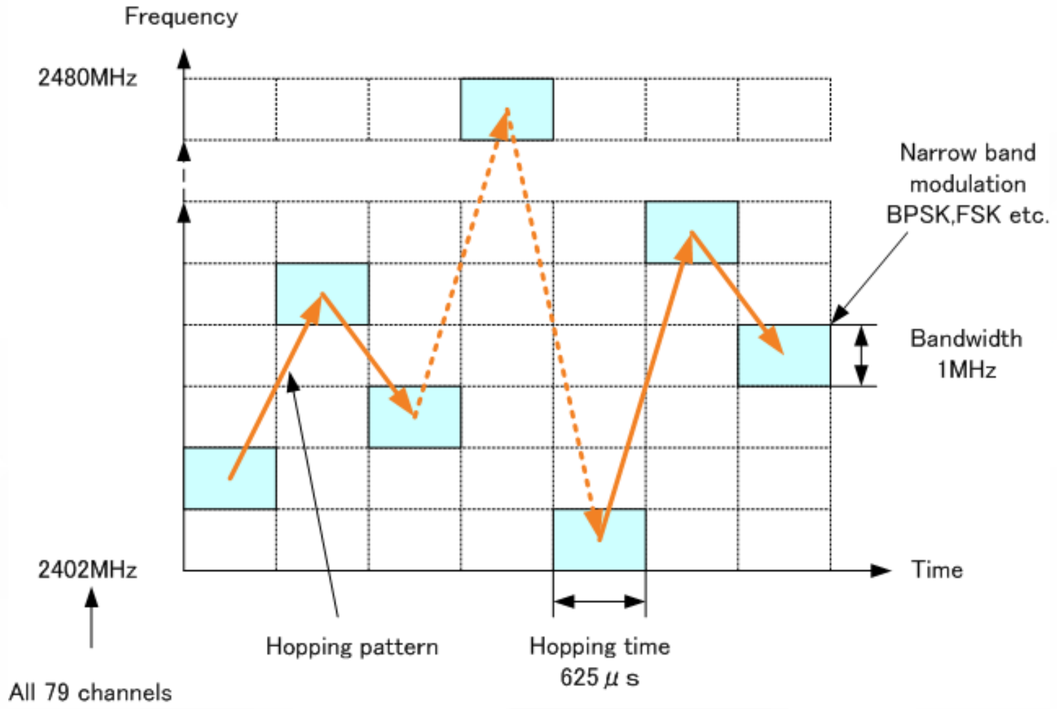


AM vs FM Radio



Frequency Hopping

Various patterns
Various rates (Bluetooth is 1600Hz!)



Information Gathering

Information Gathering

FCC ID

Examine Hardware

Prior Art

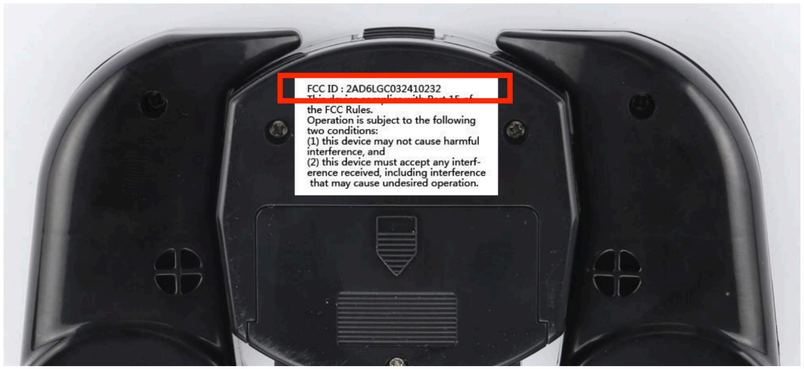
Patents

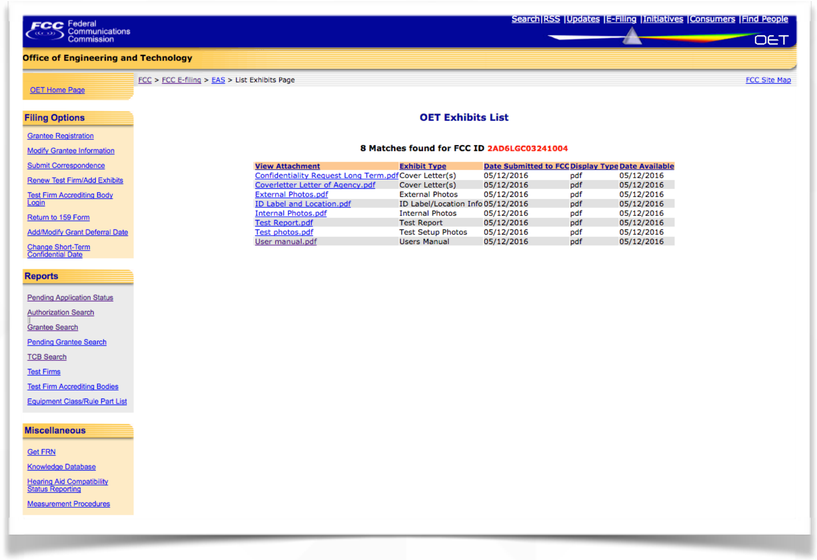
Sniff Packets

Google!

FCC Papers

http://fcc.io/2AD6LGC03241004





FCC Federal Communications Commission — Search | RSS | Updates | E-Filing | Initiatives | Consumers | Find People — OET

Office of Engineering and Technology

FCC > FCC E-filing > EAS > List Exhibits Page — FCC Site Map

OET Home Page

Filing Options

- Grantee Registration
- Modify Grantee Information
- Submit Correspondence
- Renew Test Firm/Add Exhibits
- Test Firm Accrediting Body Login
- Return to 159 Form
- Add/Modify Grant Deferral Date
- Change Short-Term Confidential Date

Reports

- Pending Application Status
- Authorization Search
- Grantee Search
- Pending Grantee Search
- TCB Search
- Test Firms
- Test Firm Accrediting Bodies
- Equipment Class/Rule Part List

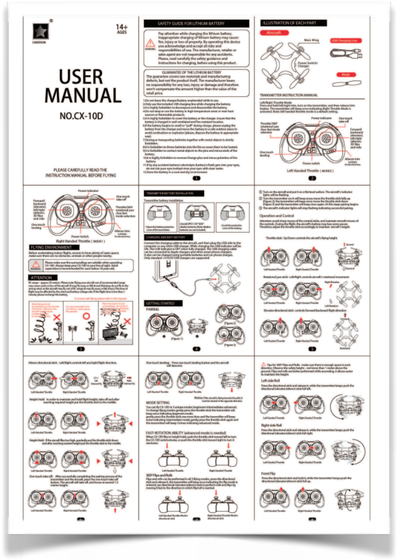
Miscellaneous

- Get FRN
- Knowledge Database
- Hearing Aid Compatibility Status Reporting
- Measurement Procedures

OET Exhibits List

8 Matches found for FCC ID 2AD6LGC03241004

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
Confidentiality Request Long Term.pdf	Cover Letter(s)	05/12/2016	pdf	05/12/2016
Coverletter Letter of Agency.pdf	Cover Letter(s)	05/12/2016	pdf	05/12/2016
External Photos.pdf	External Photos	05/12/2016	pdf	05/12/2016
ID Label and Location.pdf	ID Label/Location Info	05/12/2016	pdf	05/12/2016
Internal Photos.pdf	Internal Photos	05/12/2016	pdf	05/12/2016
Test Report.pdf	Test Report	05/12/2016	pdf	05/12/2016
Test photos.pdf	Test Setup Photos	05/12/2016	pdf	05/12/2016
User manual.pdf	Users Manual	05/12/2016	pdf	05/12/2016

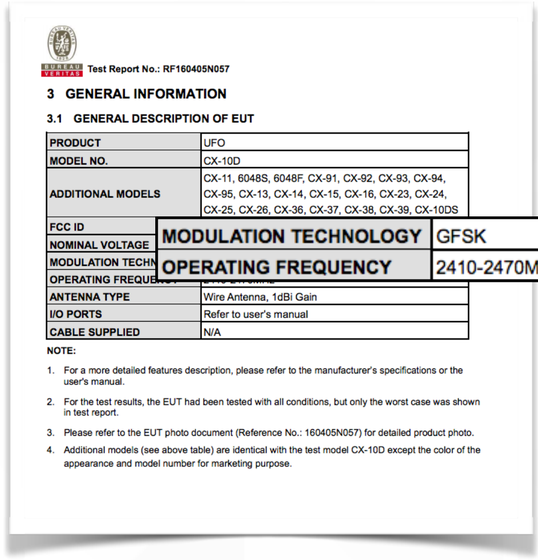


14+ AGES

USER MANUAL

NO.CX-10D

PLEASE CAREFULLY READ THE INSTRUCTION MANUAL BEFORE FLYING



BUREAU VERITAS — Test Report No.: RF160405N057

3 GENERAL INFORMATION

3.1 GENERAL DESCRIPTION OF EUT

PRODUCT	UFO
MODEL NO.	CX-10D
ADDITIONAL MODELS	CX-11, 6048S, 6048F, CX-91, CX-92, CX-93, CX-94, CX-95, CX-13, CX-14, CX-15, CX-16, CX-23, CX-24, CX-25, CX-26, CX-36, CX-37, CX-38, CX-39, CX-10DS
FCC ID	
NOMINAL VOLTAGE	
MODULATION TECHN	
OPERATING FREQUEN	
ANTENNA TYPE	Wire Antenna, 1dBi Gain
I/O PORTS	Refer to user's manual
CABLE SUPPLIED	N/A

MODULATION TECHNOLOGY	GFSK
OPERATING FREQUENCY	2410-2470MHz

NOTE:

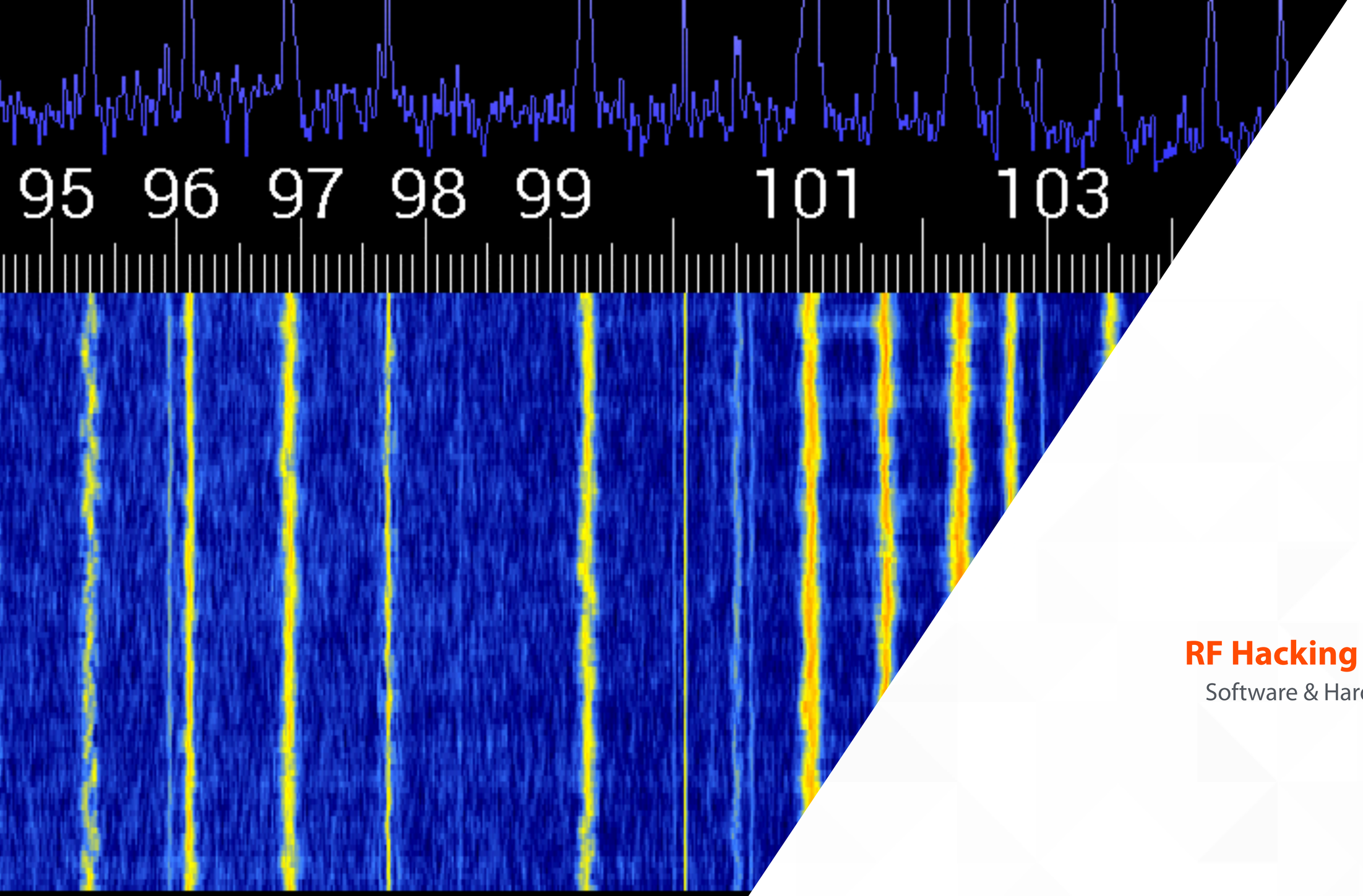
1. For a more detailed features description, please refer to the manufacturer's specifications or the user's manual.
2. For the test results, the EUT had been tested with all conditions, but only the worst case was shown in test report.
3. Please refer to the EUT photo document (Reference No.: 160405N057) for detailed product photo.
4. Additional models (see above table) are identical with the test model CX-10D except the color of the appearance and model number for marketing purpose.

Products & Companies

DroneDefender
Anti-Drone Shoulder Rifle

DeDrone
DroneTracker, Jammers, Sensors

Gryphon Sensors
Radar, Optical, Acoustic, Passive RF

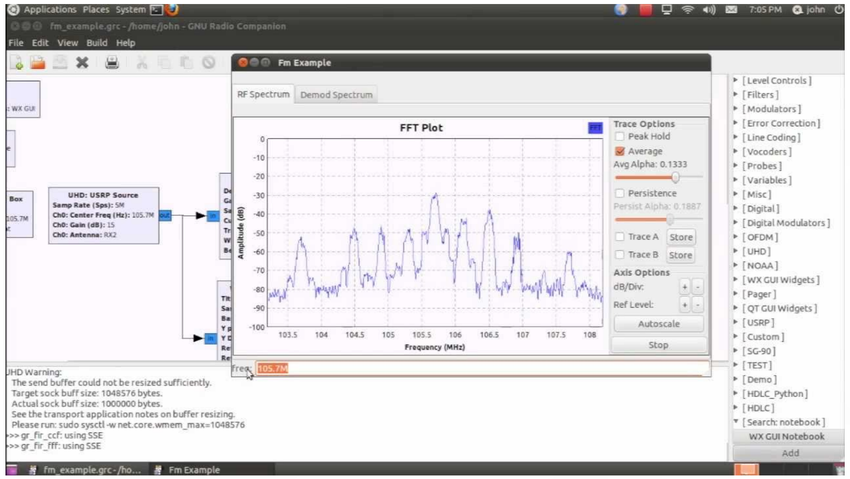


RF Hacking Tools

Software & Hardware

GNU Radio

Open Source Toolkit for Software Radio
Drag and Drop Component Workflow
Powerful & Flexible
Builds a Python Script
Steep Learning Curve



RTL_FM

Simple Command Line Tool

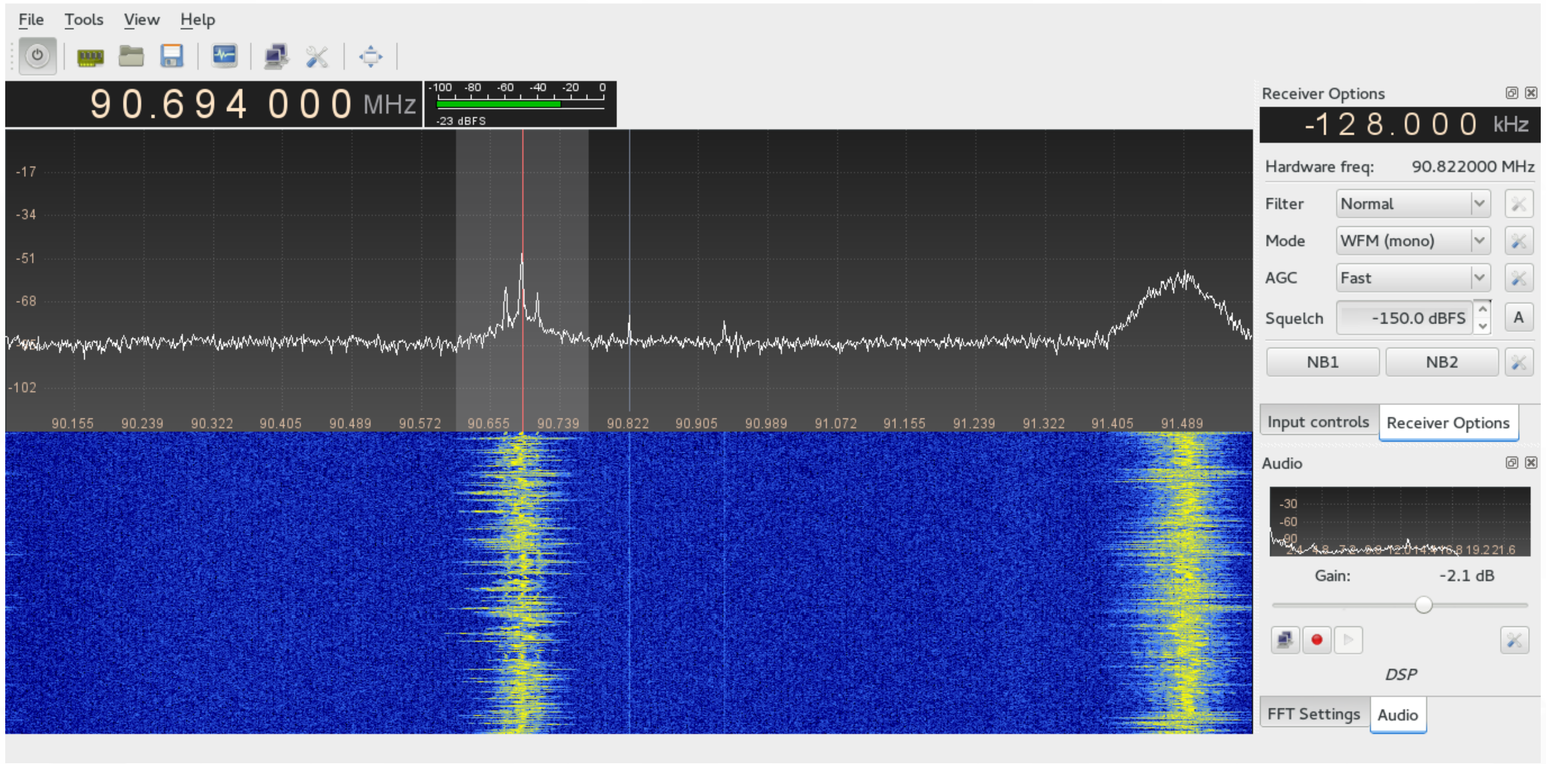
FM Demo:

```
rtl_fm -M wbfm -f 89.1M | play -r 32k -t raw -e s -b 16 -c 1 -V1 -
```

Demo: Explore and Listen to FM Radio

GQRX

Software Defined Radio Receiver
Powered by GNU Radio
Supports tons of Radios
Great Spectrum Analyzer



Demo: HackRF One w/ gqrx on favorite radio station or 2415-17

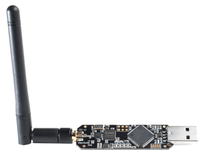
Software Defined Radios

and "Developer Platforms"

RTL_SDR
$30
13 - 1864 MHz* (Receive Only)

HackRF One
$300
10 MHz to 6 GHz (Transmit & Receive)

Ellisys Explorer 400-STD-LE
$30,000
Capture & decode all Bluetooth channels at once



Ubertooth One
$130
2.4GHz (Transmit & Receive)

Yardstick One
$100
< 1 GHz (Transmit & Receive)
IM Me (OpenSesame)

CrazyRadio PA (or any nRF24LU1+ chip)
$30
2.4 GHz (Transmit & Receive)
MouseJack

and many others…

Exploits & Demos

Video Intercept

WiFi Access Point

SYMA X5SW

Android App Reverse Engineering

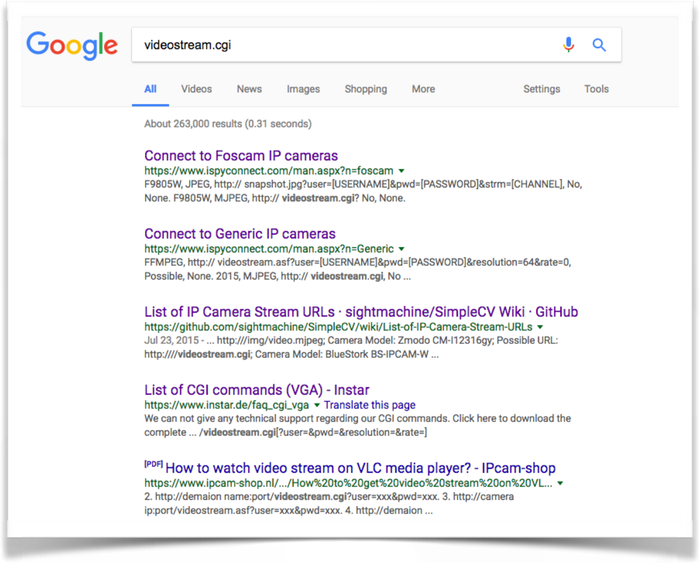
apktool
Simple Command Line Tool

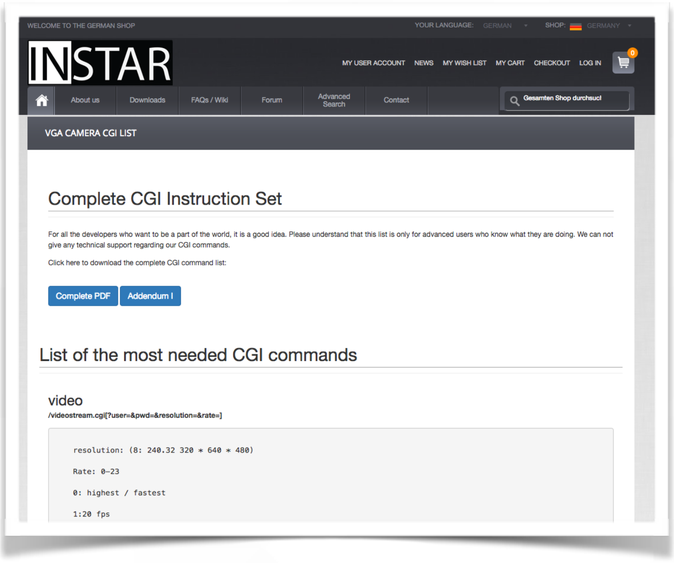
Demo:

```
apktool d name-of-the-app.apk
```

Reference to:

```
http://192.169.1.1:80/videostream.cgi&user=admin&pwd=
```





GPS Spoofing & Jamming

Image Source: Wired

US Border Patrol Drones Hacked by Drug Cartels

Don’t do this without permission - its super illegal

Civilian GPS Overview
Not encrypted or authenticated
Never intended for safety and security-critical applications

How does GPS Work?
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
4 satellites required, at minimum, for 3d positioning

Device	GPS Test Generator
Cost	$25
Range	20m

Replay Attack

hackrf_transfer

Listen and Transfer Tool for HackRF Radio

Listen

```
hackrf_transfer -r 390_data.raw -f 39000000
```

Replay

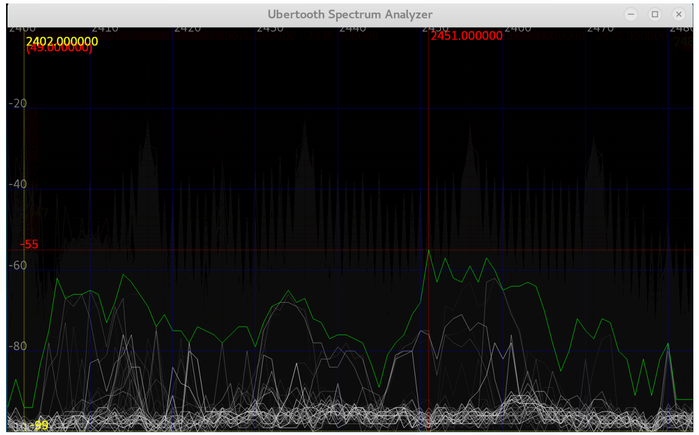
```
hackrf_transfer -t 390_data.raw -f 39000000
```

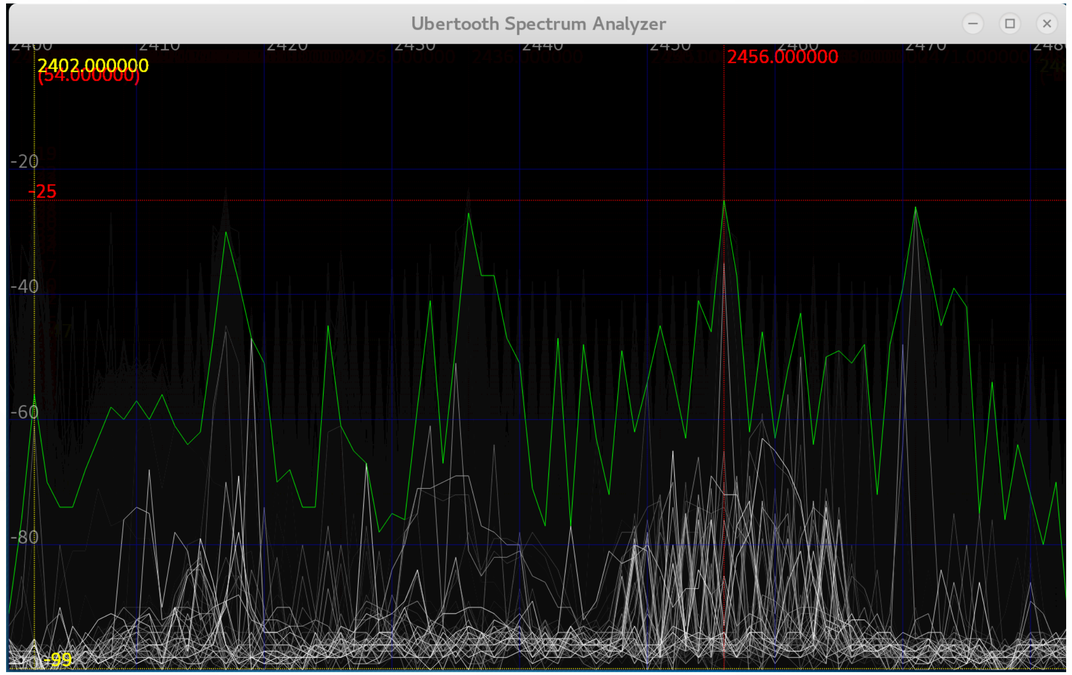
Decode Controller

Cheers CX-10

Sturdy Palm Tree
Translate raw 2.4 Ghz to actual commands

Drone Duel Demo
Inject fake packets w/ nRF24LU1+
Flashed w/ MouseJack





Frequency Hopping

Sync Channel: 2402 MHz
Channel 1: 2417 MHz
Channel 2: 2436 MHz
Channel 3: 2456 MHz
Channel 4: 2471 MHz

Special Thanks

Further Reading and Related Projects

Dominic Spill and Michael Ossman (Great Scott Gadgets)
#ubertooth
https://greatscottgadgets.com/
https://github.com/dominicgs/sturdy-palm-tree

Samy Kamkar
https://github.com/samyk/skyjack
https://github.com/samyk/opensesame
https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/

Marc Newlin
https://github.com/BastilleResearch/mousejack

Jared Ablon
https://www.airmap.com/security-drone-of-things/

https://pastebin.com/6GwatPdj
https://github.com/miek/gr-hubsan
https://www.youtube.com/watch?v=5CzURm7OpAA
http://blog.ptsecurity.com/2016/06/phd-vi-how-they-stole-our-drone.html
https://medium.com/@swalters/drones-hacking-is-becoming-childs-play-b56843342e36
https://medium.com/@swalters/how-to-set-up-a-drone-vulnerability-testing-lab-db8f7c762663
https://www.reddit.com/r/HowToHack/comments/4512il/how_to_hack_ip_camera_in_toy_drone/
https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809
https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Aaron-Luo-Drones-Hijacking-Multi-Dimensional-Attack-Vectors-And-Countermeasures-UPDATED.pdf

Questions?

Matt Koskela
mattkoskela@gmail.com
Twitter: @matt_koskela
Slides: mattkoskela.com/tech/drone-hacking-basics