RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: HTA-W02

RF Exploitation: IoT/OT Hacking with SDR

Himanshu Mehta

Senior Threat Analysis Engineer
Symantec
mehta.himanshu21@gmail.com
@LionHeartRoxx

Harshit Agrawal

Security Researcher
MIT Academy of Engineering, Pune
harshit.nic@gmail.com
@harshitnic

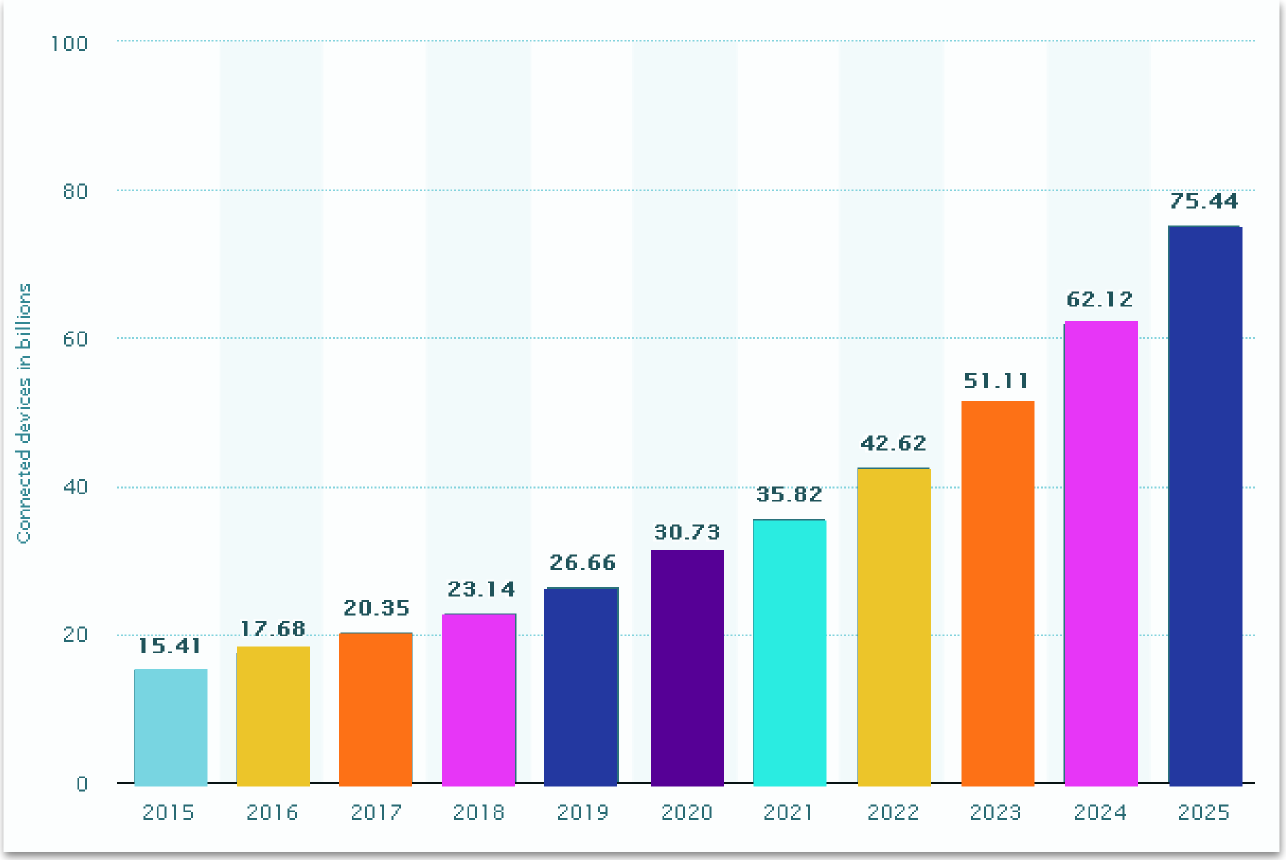
Agenda:

- Evolving radio technology landscape
- Security applications of Software Defined Radio
- What makes securing RF communications unique
- Case studies: Car RKE, Dallas Siren Hack
- Top wireless Vulnerabilities
- Privacy, Rules and Regulations for RF

IoT :

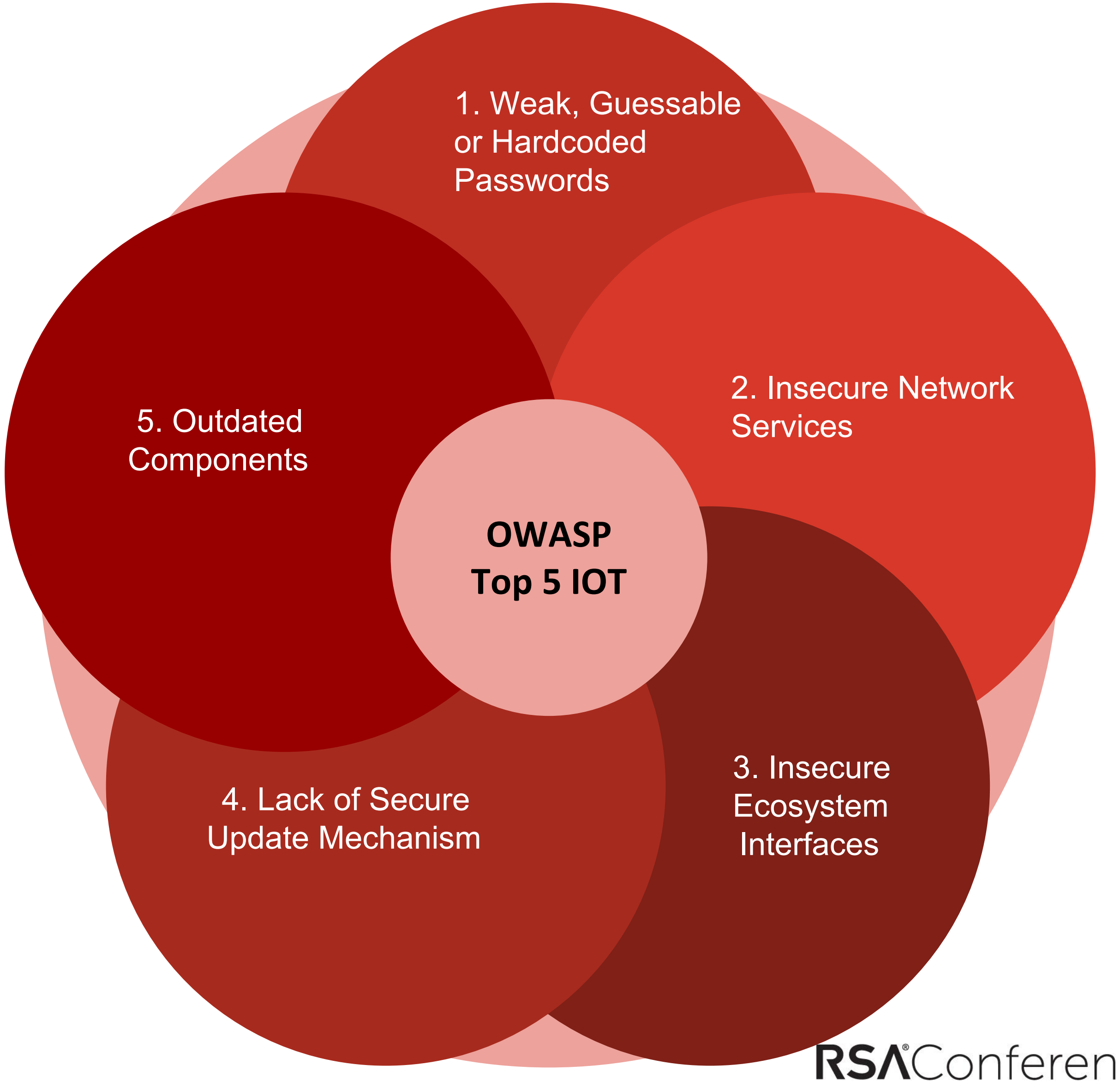
- This statistic shows the number of connected devices (Internet of Things; IoT) worldwide from 2015 to 2025.

- For 2020, the installed base of Internet of Things devices is forecast to grow to almost 31 billion worldwide.



Evolving IoT/OT landscape:

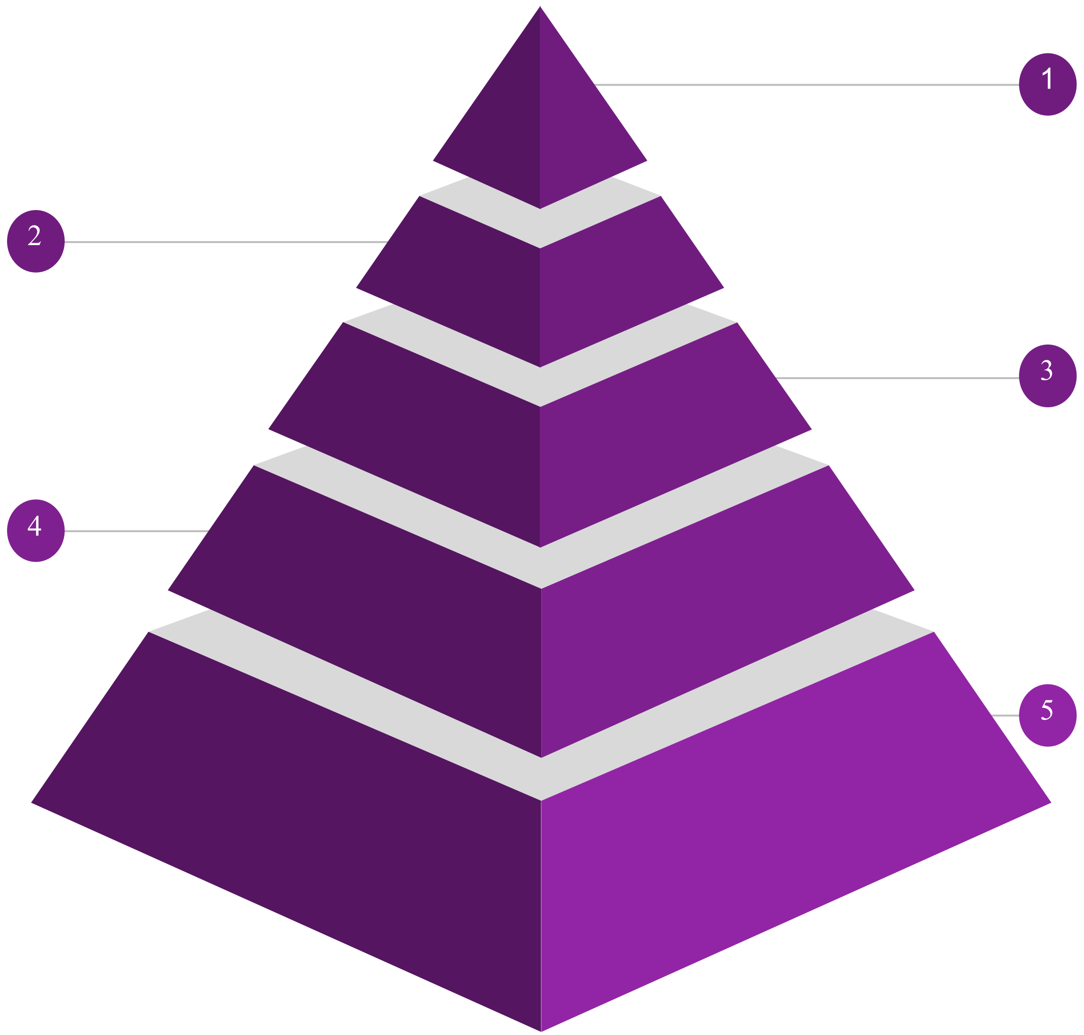
The combined markets of the Internet of Things (IoT) will grow to about $520B in 2021, more than double the $235B spent in 2017.



OWASP Top 5 IOT

1. Weak, Guessable or Hardcoded Passwords
2. Insecure Network Services
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanism
5. Outdated Components

Internet of things threat model



Controlling Device

Smartphone, tablets and other smart devices can control all types of "things"

Cloud Service

Cloud services provide the repository and access control between the "things" and its controller.

Global Network

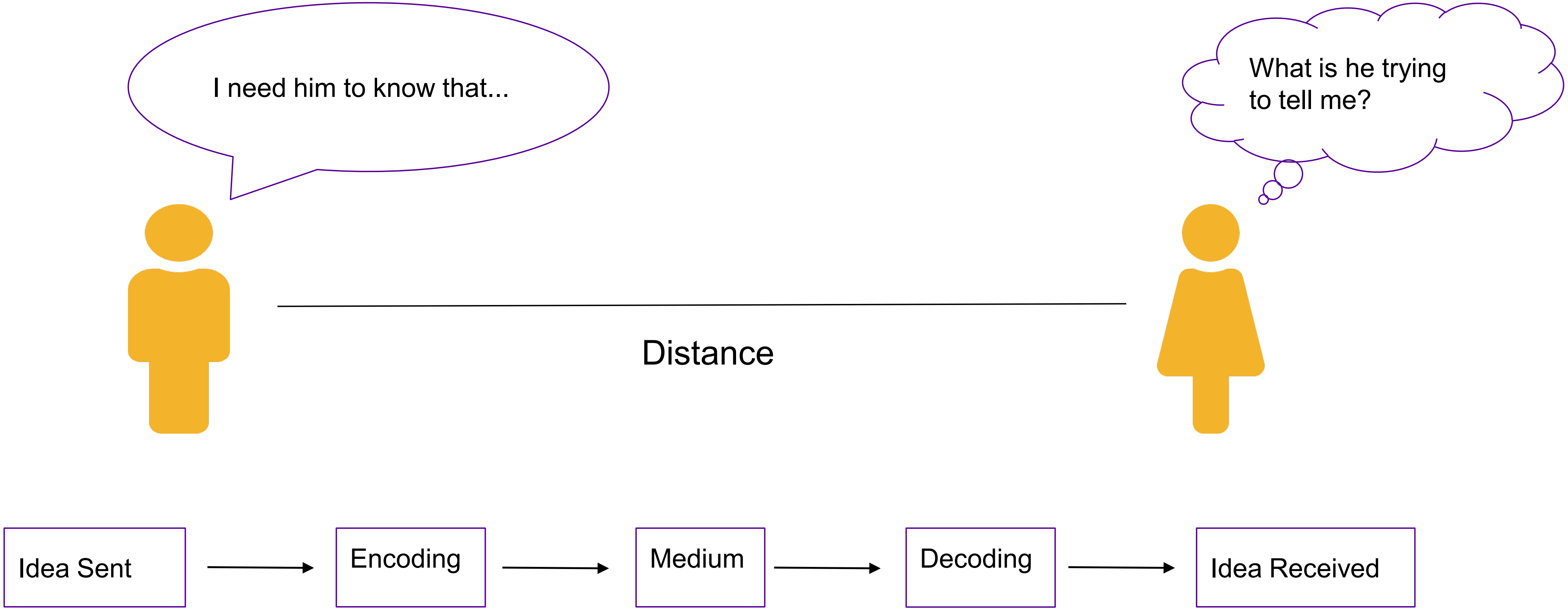
Most "things" connected to the Internet, except for power grids or classified government systems

Local Network

This may be a controller area network (CAN) in connected cars, a local network in homes, etc

Things

"Things" can be remotely controlled or viewed, and they can send telemetry for analysis.



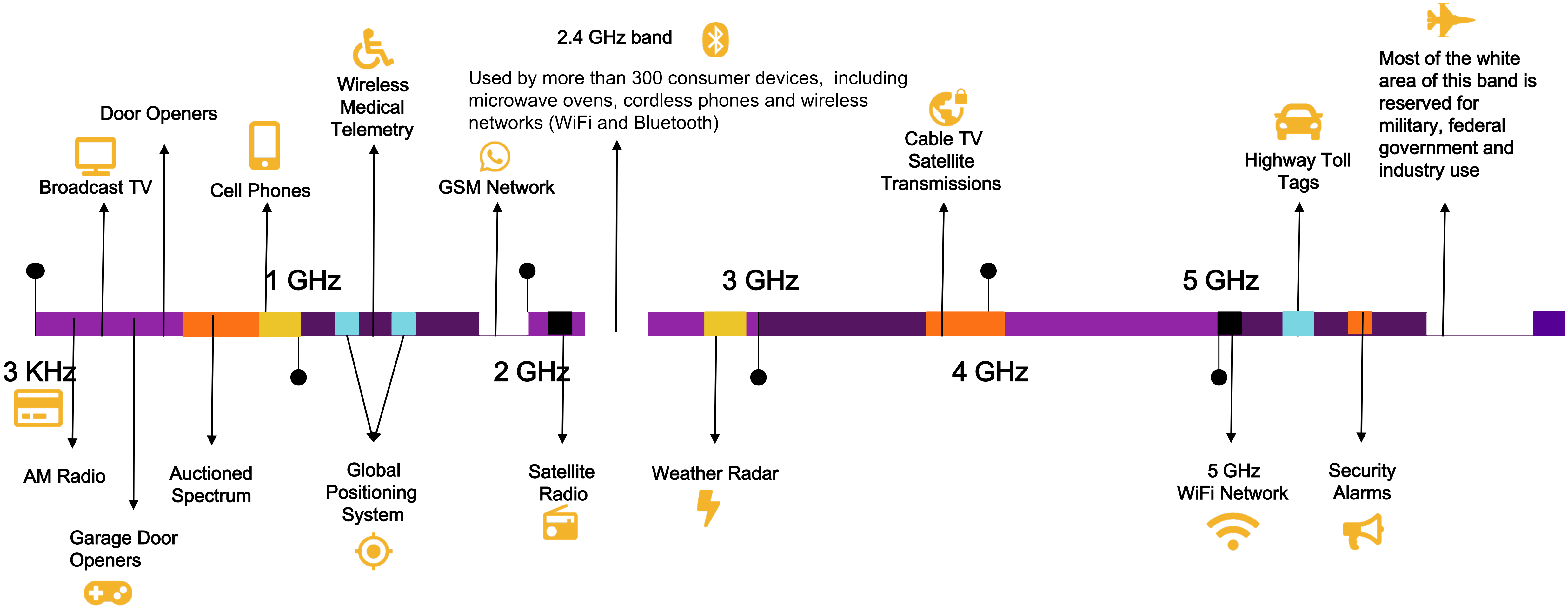
I need him to know that...

What is he trying to tell me?

Distance

Idea Sent → Encoding → Medium → Decoding → Idea Received

Inside the radio wave spectrum?

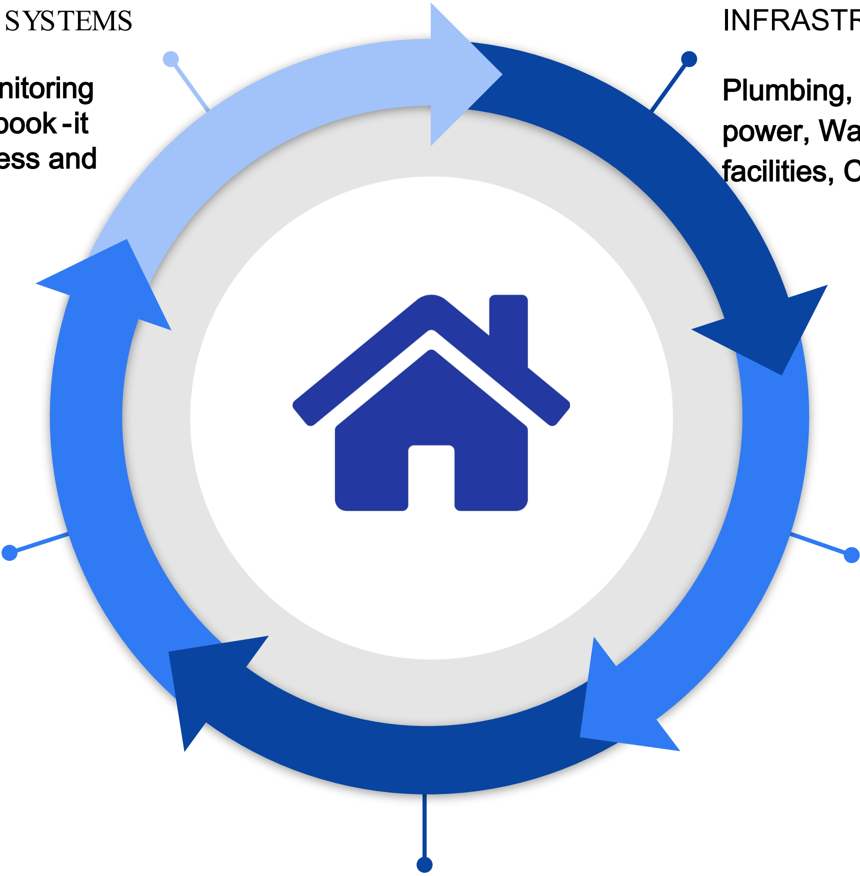

2.4 GHz band
Used by more than 300 consumer devices, including microwave ovens, cordless phones and wireless networks (WiFi and Bluetooth)
Door Openers
Broadcast TV
Cell Phones
Wireless Medical Telemetry
GSM Network
Cable TV Satellite Transmissions
Highway Toll Tags
Most of the white area of this band is reserved for military, federal government and industry use
1 GHz
3 GHz
5 GHz
3 KHz
2 GHz
4 GHz
AM Radio
Garage Door Openers
Auctioned Spectrum
Global Positioning System
Satellite Radio
Weather Radar
5 GHz WiFi Network
Security Alarms

Why Focus on RF Security?

- Current Scenario of RF and IoT Security is same as Web Security back in 90s.

Why Focus on RF Security?

IoT Components for Smart Building



COMBINED SYSTEMS

Energy usage monitoring system, Hoteling book -it system Card access and security system

INFRASTRUCTURE

Plumbing, Windows, Back-up power, Waste control, Parking facilities, Communication

SENSING

CCTV, IP video, Air quality, Water flow, Air temp, Light, Door, Smoke/fire

ACTUATING

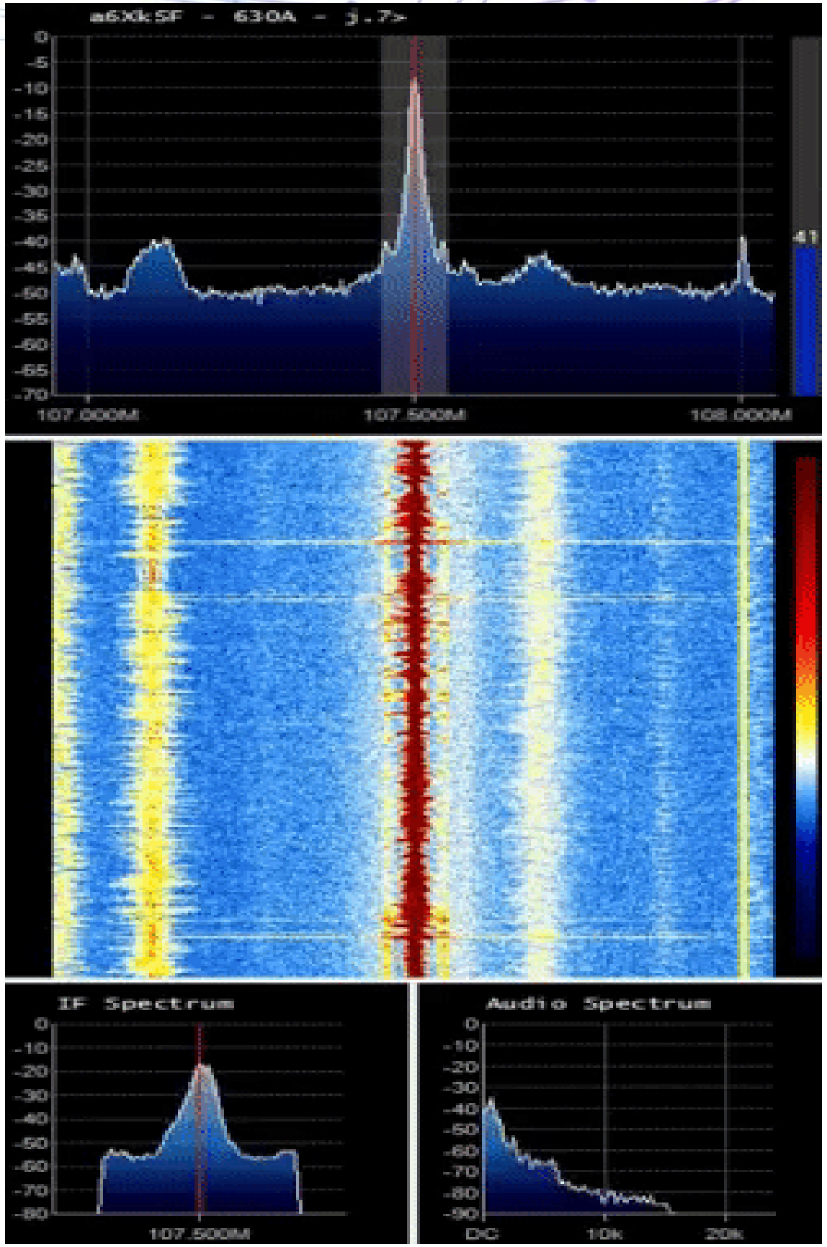
Door access, Elevator, Heater/AC, Fire alarms, Irrigation system

COMPUTING

Processors/data stores: - Databases, Servers, Cloud services, Edge devices

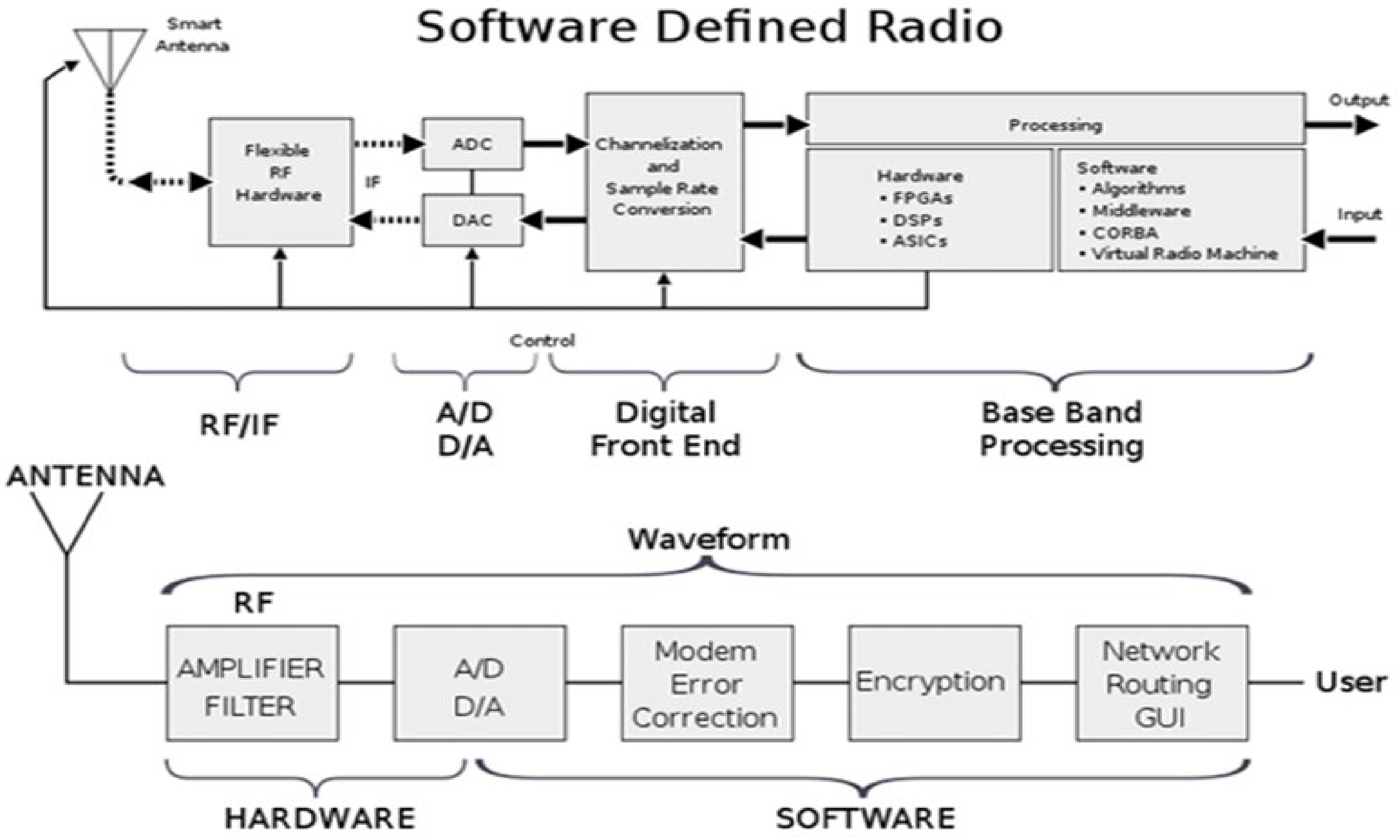
PHY LAYER

- Lowest layer in communication stack
- In wired protocols: voltage, timing, and wiring defining 1s and 0s
- In wireless: patterns of energy being sent over RF medium



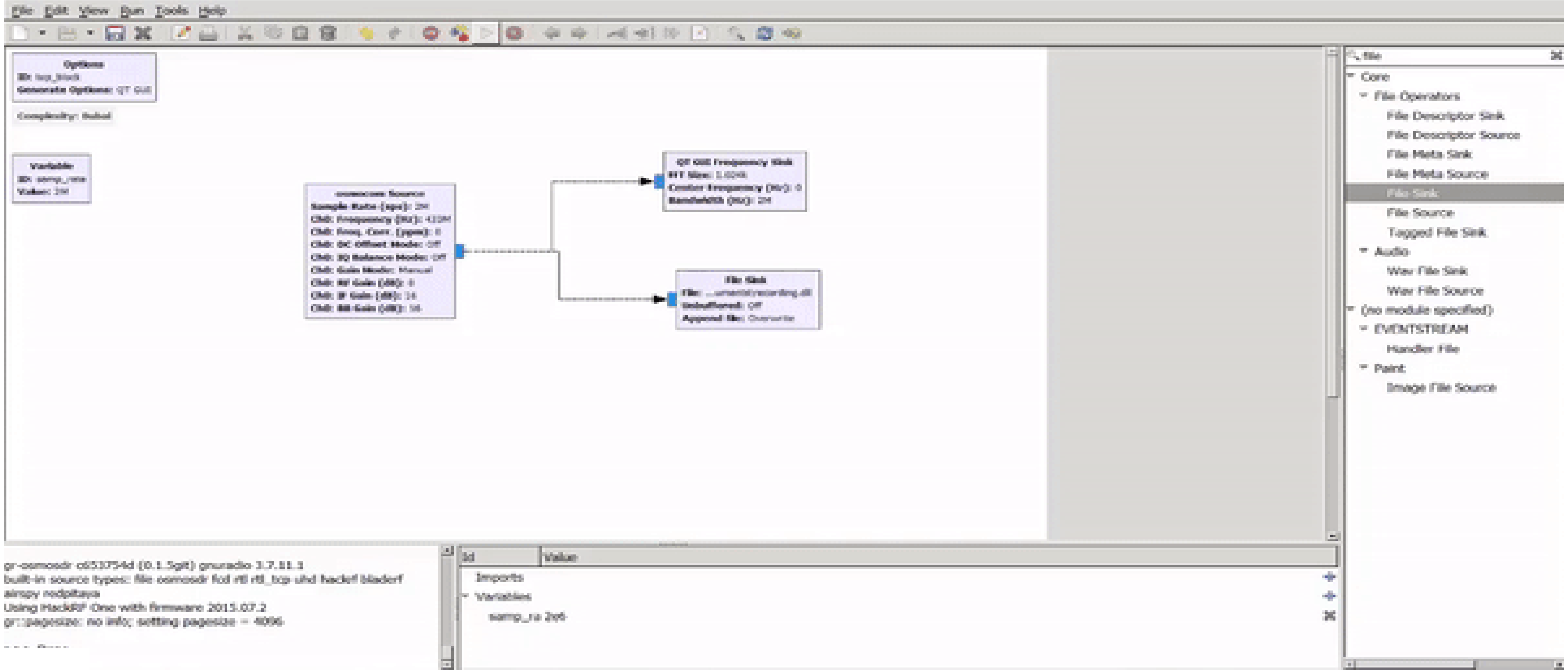
So what is SDR?

- Using Software to replace most of Hardware for implementation of Radio Networking
- Shuttles RF I/Q samples to DSP or host
- Captures raw radio spectrum



GNU Radio

- GNU Radio is a framework that enables users to design, simulate, and deploy highly capable real-world radio systems.



Options
ID: top_block
Generate Options: QT GUI

Complexity: Basic

Variable
ID: samp_rate
Value: 2M

osmocom Source
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 433M
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 0
Ch0: IF Gain (dB): 16
Ch0: BB Gain (dB): 16

QT GUI Frequency Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 2M

File Sink
File: ...amentity/recording.dt
Unbuffered: Off
Append file: Overwrite

```
gr-osmosdr c653754d (0.1.5git) gnuradio 3.7.11.1
built-in source types: file osmosdr fcd rtl rtl_tcp uhd hackrf bladerf
airspy redpitaya
Using HackRF One with firmware 2015.07.2
gr::pagesize: no info; setting pagesize = 4096
```

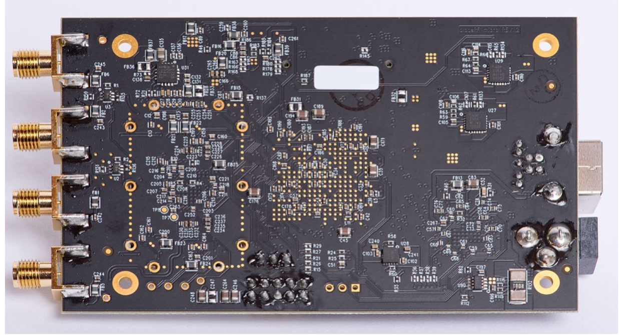
Id	Value
Imports	
Variables	
samp_ra	2e6

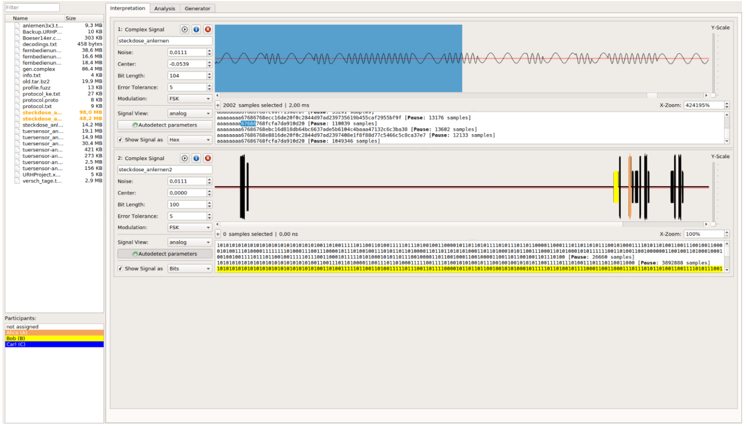
Hardwares and Softwares:

RTL-SDR.COM
QUICKSTART SETUP GUIDE: RTL-SDR.COM/QSG
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO+BIAS T+HF
V3

GNURadio

Audacity®





Name	Size
anlernen3x3.t...	9,3 MB
Backup.URHP...	10 KB
Boeser14er.c...	303 KB
decodings.txt	458 bytes
fernbedienun...	38,6 MB
fernbedienun...	16,6 MB
fernbedienun...	18,4 MB
gen.complex	86,4 MB
info.txt	4 KB
old.tar.bz2	19,9 MB
profile.fuzz	13 KB
protocol_ke.txt	27 KB
protocol.proto	8 KB
protocol.txt	9 KB
steckdose_a...	98,0 MB
steckdose_a...	48,2 MB
steckdose_anl...	14,2 MB
tuersensor_an...	19,1 MB
tuersensor_an...	14,9 MB
tuersensor_an...	30,4 MB
tuersensor-an...	421 KB
tuersensor-an...	273 KB
tuersensor-an...	2,5 MB
tuersensor-an...	156 KB
URHProject.x...	5 KB
versch_tage.t...	2,9 MB

Participants:
- not assigned
- Alice (A)
- Bob (B)
- Carl (C)

1: Complex Signal
steckdose_anlernen
Noise: 0,0111
Center: -0,0539
Bit Length: 104
Error Tolerance: 5
Modulation: FSK
Signal View: analog
☑ Show Signal as Hex
2002 samples selected | 2,00 ms
X-Zoom: 424195%

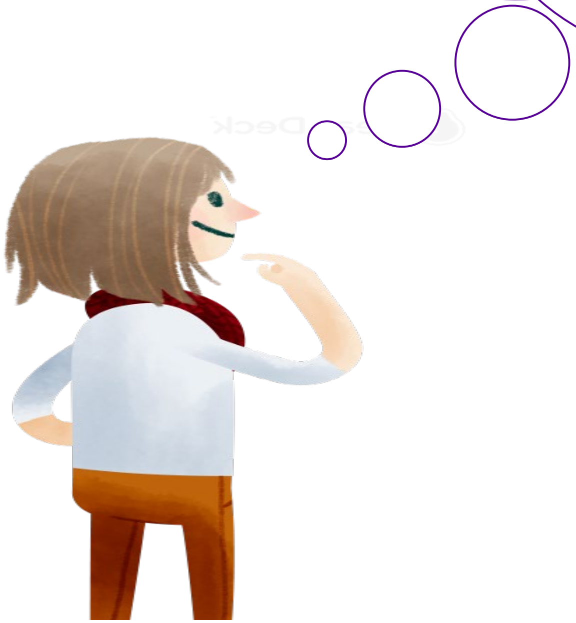
```
aaaaaaaa67686768ecc16de20f0c2844d97ad239735619b455caf2955bf9f [Pause: 13176 samples]
aaaaaaaa67686768fcfa7da910d20 [Pause: 110039 samples]
aaaaaaaa67686768ebc16d818db64bc6637ade5b6104c4baaa47132c6c3ba38 [Pause: 13602 samples]
aaaaaaaa67686768e8816de20f0c2844d97ad2397408e1f8f88d77c5466c5c8ca37e7 [Pause: 12133 samples]
aaaaaaaa67686768fcfa7da910d20 [Pause: 1049346 samples]
```

2: Complex Signal
steckdose_anlernen2
Noise: 0,0111
Center: 0,0000
Bit Length: 100
Error Tolerance: 5
Modulation: FSK
Signal View: analog
☑ Show Signal as Bits
0 samples selected | 0,00 ns
X-Zoom: 100%

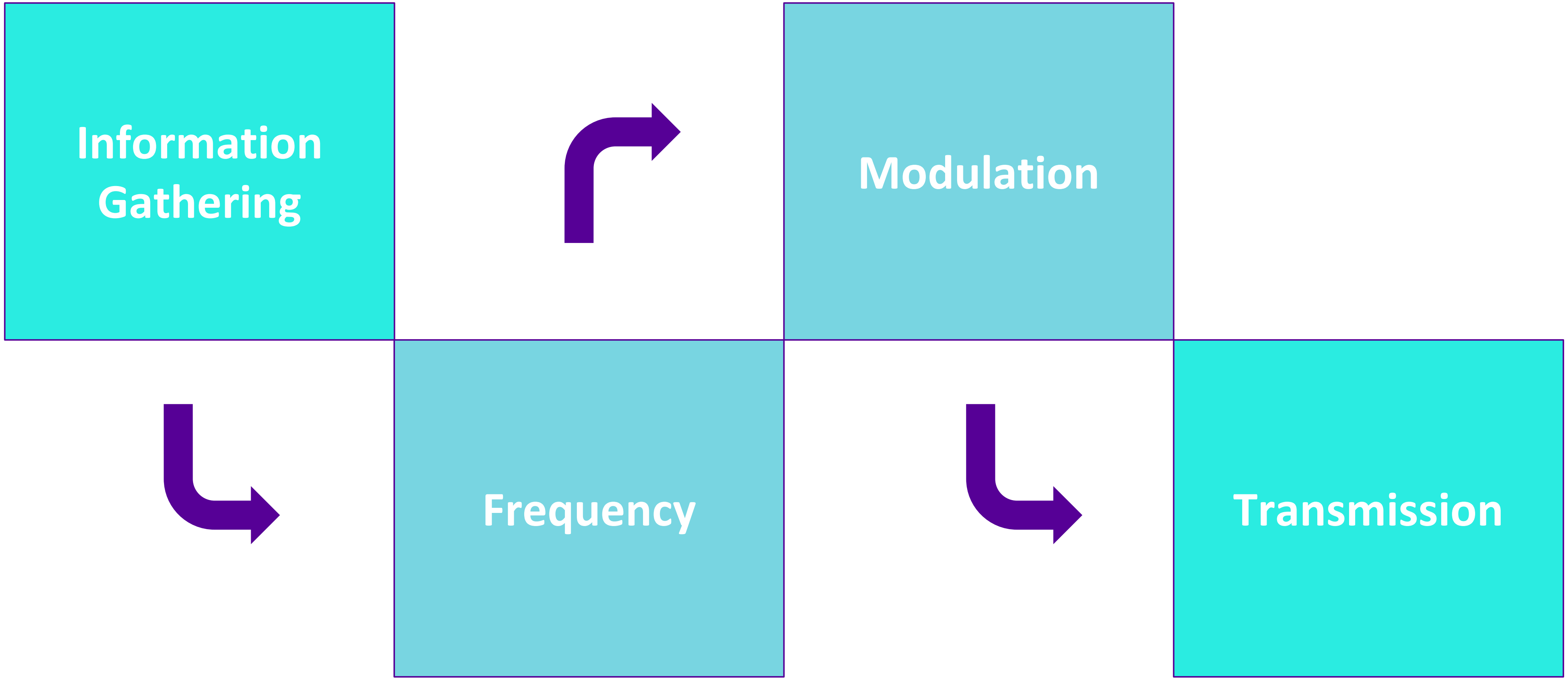
```
1010101010101010101010101010101010101001101001111101100110100111111011101001001100001011011010111101011101101100001100011101101101011100101000111101011010011001110010011000
01010011101000011111111010001110011100001011101001001110101101101000011011011010101000110110100010101100111000110101000101011111100110100110010000001100100110100010001
00100100111101110110010011111011100110001011111010100010101101110010000110110010001100100001100110110010011011110100 [Pause: 26660 samples]
10101010101010101010101010101010101001100111011010000110011101101000011111001111010010101001011100100100101010110011110111010011101110110011000 [Pause: 3892888 samples]
1010101010101010101010101010101010100110100111110110011010011111101110011011110000101101101100100101010001011111011010010111100011001100011101110101101001100111101011100
```

Initial Profiling of our device

- What does our device do in normal operation?
- How do they connect?
- Determining the frequency?



Phases of RF Attacks:



Information Gathering

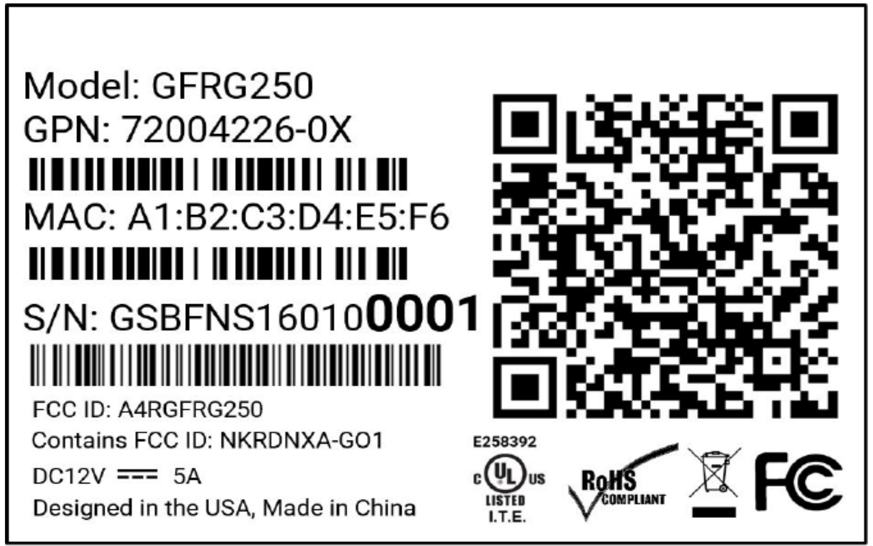
Frequency

Modulation

Transmission

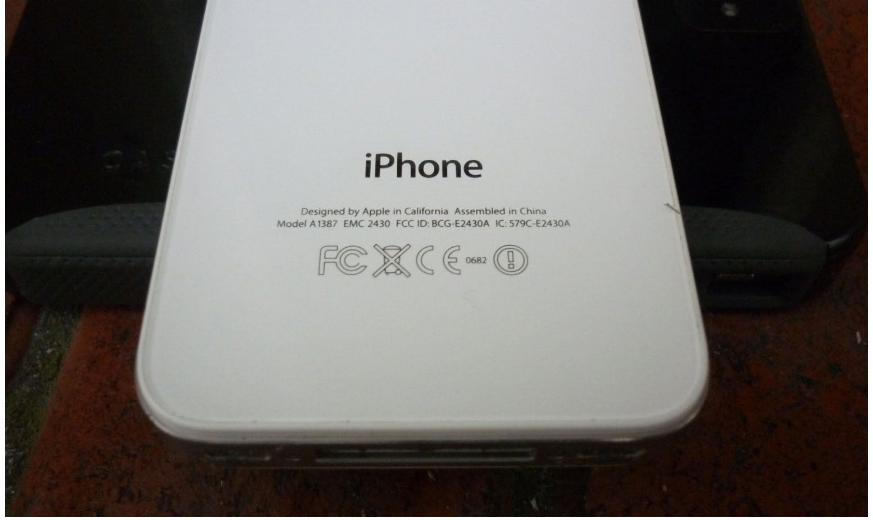
Information Gathering:

- A good starting point – if you have some luck –search for the FCC ID:
- https://www.fcc.gov/general/fcc-id-search-page
- Demo: https://fccid.io/Y8PFJ17-1



Model: GFRG250
GPN: 72004226-0X
MAC: A1:B2:C3:D4:E5:F6
S/N: GSBFNS16010**0001**
FCC ID: A4RGFRG250
Contains FCC ID: NKRDNXA-GO1
DC12V ⎓ 5A
Designed in the USA, Made in China

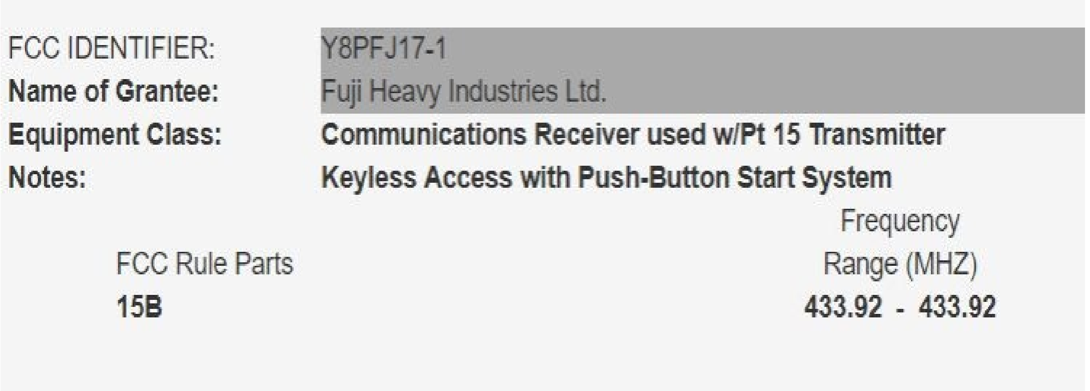
E258392
c UL us
LISTED
I.T.E.
RoHS
COMPLIANT
FC



iPhone
Designed by Apple in California Assembled in China
Model A1387 EMC 2430 FCC ID: BCG-E2430A IC: 579C-E2430A
FC
0682

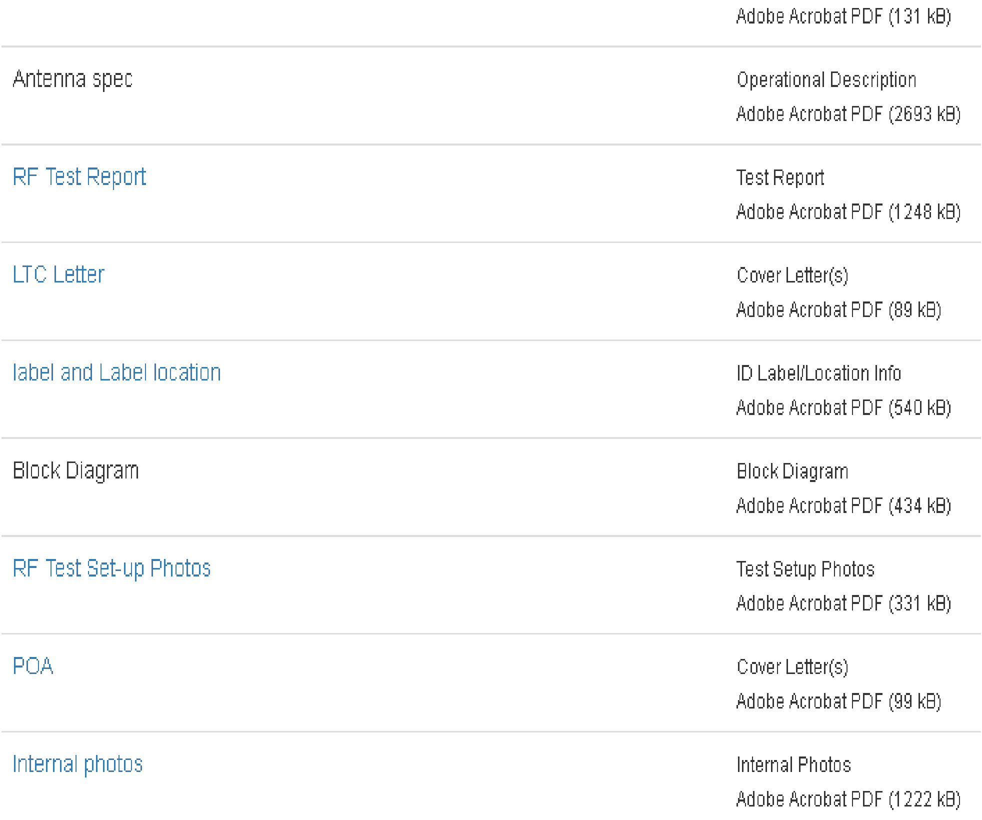
Information Extracted from FCC

- FCC also publishes internal images, external images, user manuals, and test results for wireless devices.



FCC IDENTIFIER:	Y8PFJ17-1
Name of Grantee:	Fuji Heavy Industries Ltd.
Equipment Class:	**Communications Receiver used w/Pt 15 Transmitter**
Notes:	**Keyless Access with Push-Button Start System**

FCC Rule Parts	Frequency Range (MHZ)
15B	**433.92 - 433.92**

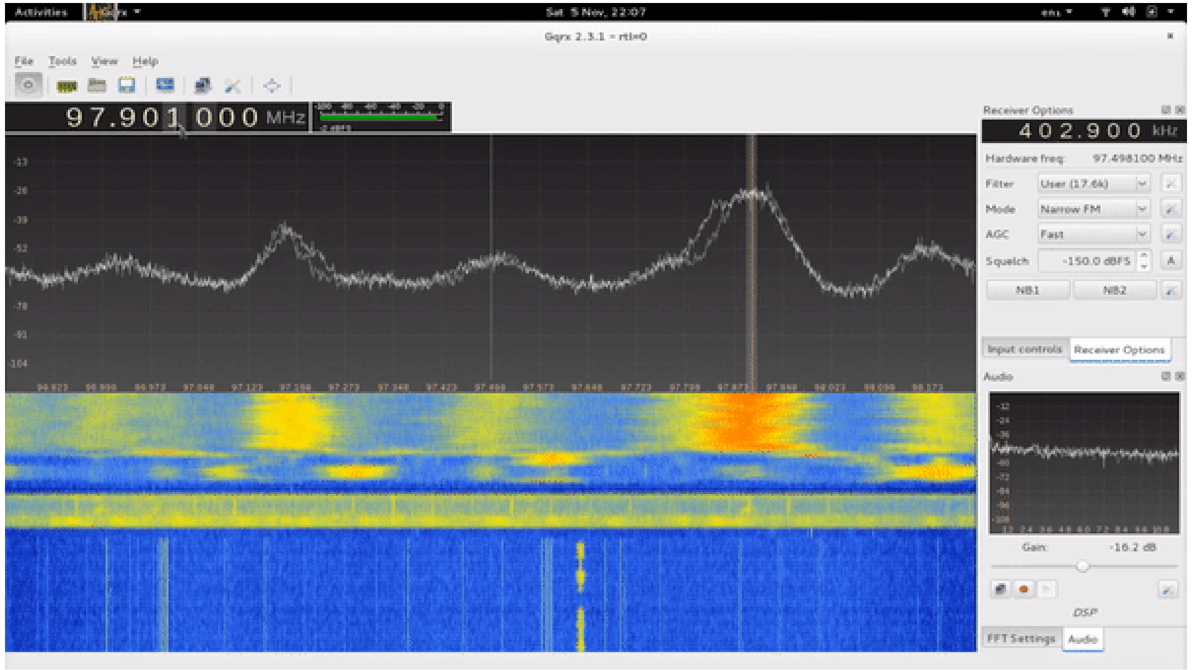


	Adobe Acrobat PDF (131 kB)
Antenna spec	Operational Description Adobe Acrobat PDF (2693 kB)
RF Test Report	Test Report Adobe Acrobat PDF (1248 kB)
LTC Letter	Cover Letter(s) Adobe Acrobat PDF (89 kB)
label and Label location	ID Label/Location Info Adobe Acrobat PDF (540 kB)
Block Diagram	Block Diagram Adobe Acrobat PDF (434 kB)
RF Test Set-up Photos	Test Setup Photos Adobe Acrobat PDF (331 kB)
POA	Cover Letter(s) Adobe Acrobat PDF (99 kB)
Internal photos	Internal Photos Adobe Acrobat PDF (1222 kB)

Frequency:

Use a Spectrum Analyzer (GQRX)

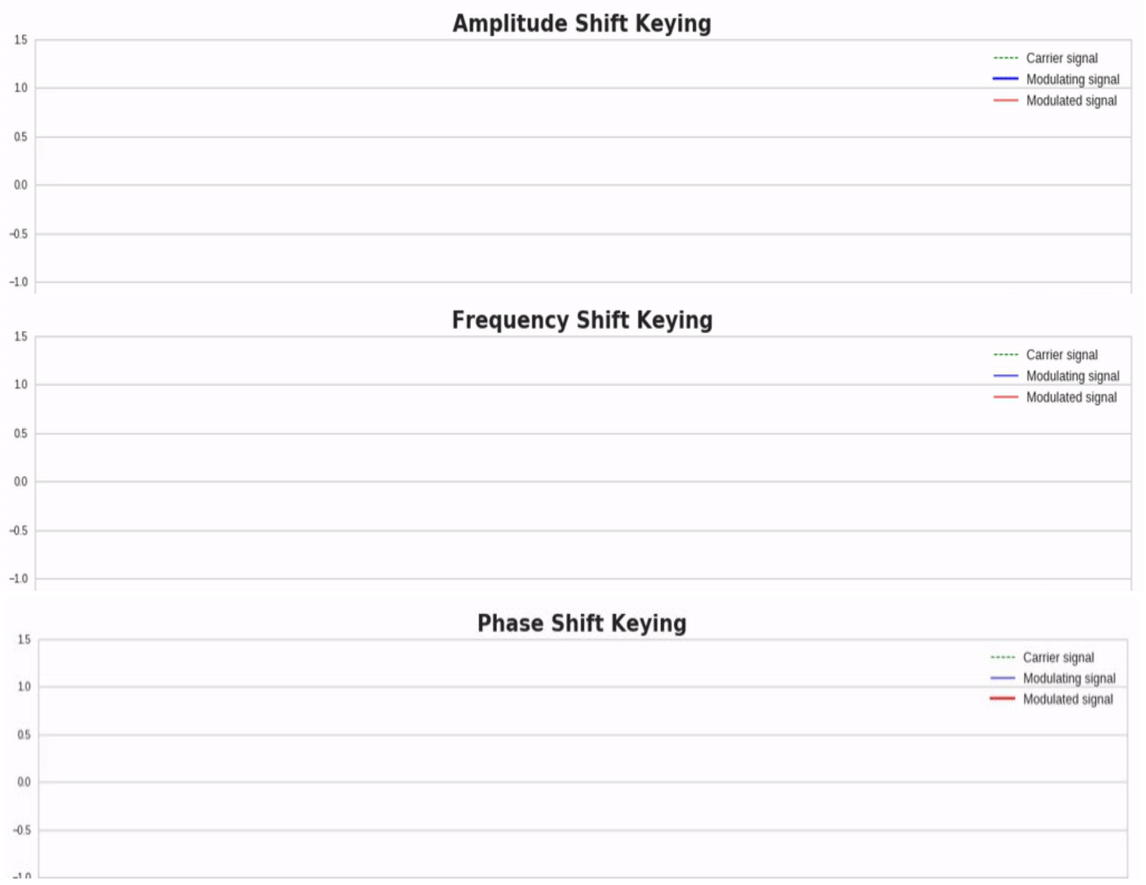
- FFT plot and waterfall
- Record and Playback
- Special FM mode for NOAA APT
- Basic Remote Control through TCP



402.900 kHz
Hardware freq: 97.498100 MHz
Filter: User (17.6k)
Mode: Narrow FM
AGC: Fast
Squelch: -150.0 dBFS
NB1 NB2

Modulation:

- Modulation is like hiding a code inside a carrier wave
- Representing digital data as variations in the carrier wave.



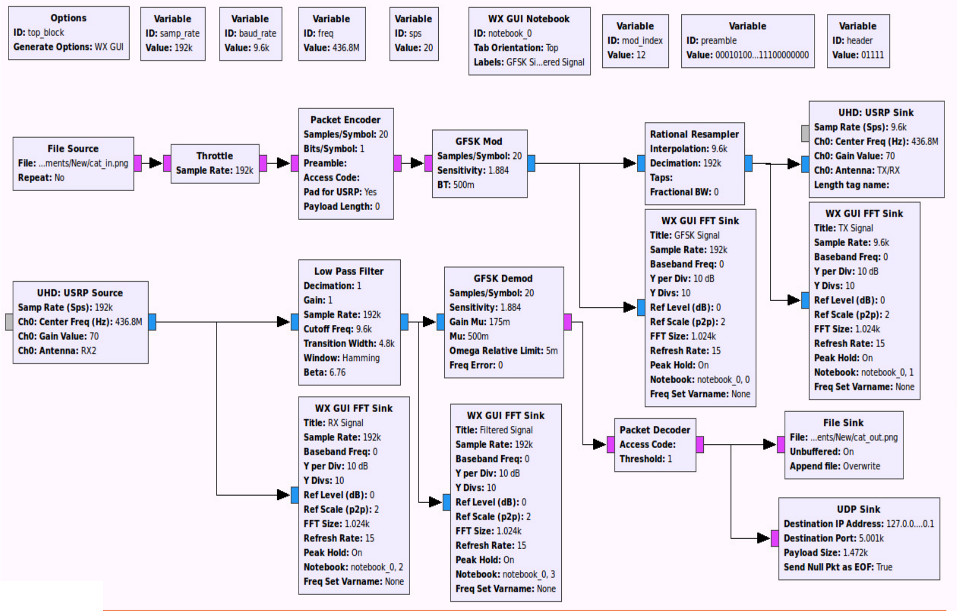
Source:Attify Inc

Transmission:

- Generate the message from above extracted details (Frequency, Modulation, Bitrate, Sync word, Preamble...)

Option 1:- Use a flow graph

Option 2: Command Line RF tool



Options
ID: top_block
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 192k

Variable
ID: baud_rate
Value: 9.6k

Variable
ID: freq
Value: 436.8M

Variable
ID: sps
Value: 20

WX GUI Notebook
ID: notebook_0
Tab Orientation: Top
Labels: GFSK Si...ered Signal

Variable
ID: mod_index
Value: 12

Variable
ID: preamble
Value: 00010100...11100000000

Variable
ID: header
Value: 01111

File Source
File: ...ments/New/cat_in.png
Repeat: No

Throttle
Sample Rate: 192k

Packet Encoder
Samples/Symbol: 20
Bits/Symbol: 1
Preamble:
Access Code:
Pad for USRP: Yes
Payload Length: 0

GFSK Mod
Samples/Symbol: 20
Sensitivity: 1.884
BT: 500m

Rational Resampler
Interpolation: 9.6k
Decimation: 192k
Taps:
Fractional BW: 0

UHD: USRP Sink
Samp Rate (Sps): 9.6k
Ch0: Center Freq (Hz): 436.8M
Ch0: Gain Value: 70
Ch0: Antenna: TX/RX
Length tag name:

WX GUI FFT Sink
Title: GFSK Signal
Sample Rate: 192k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Peak Hold: On
Notebook: notebook_0, 0
Freq Set Varname: None

WX GUI FFT Sink
Title: TX Signal
Sample Rate: 9.6k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Peak Hold: On
Notebook: notebook_0, 1
Freq Set Varname: None

UHD: USRP Source
Samp Rate (Sps): 192k
Ch0: Center Freq (Hz): 436.8M
Ch0: Gain Value: 70
Ch0: Antenna: RX2

Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 192k
Cutoff Freq: 9.6k
Transition Width: 4.8k
Window: Hamming
Beta: 6.76

GFSK Demod
Samples/Symbol: 20
Sensitivity: 1.884
Gain Mu: 175m
Mu: 500m
Omega Relative Limit: 5m
Freq Error: 0

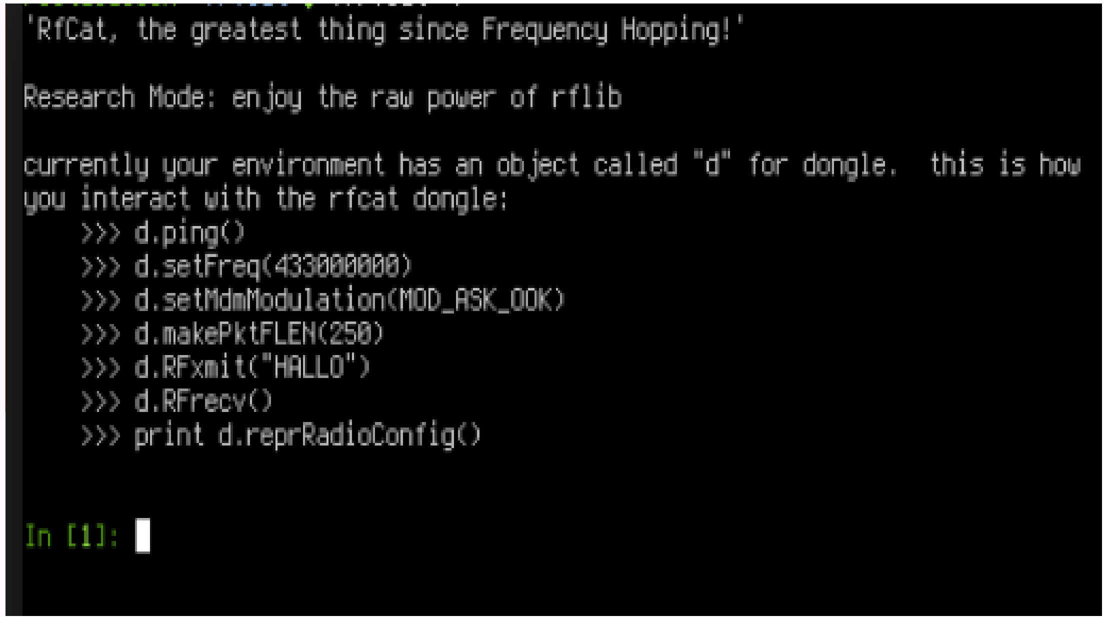
WX GUI FFT Sink
Title: RX Signal
Sample Rate: 192k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Peak Hold: On
Notebook: notebook_0, 2
Freq Set Varname: None

WX GUI FFT Sink
Title: Filtered Signal
Sample Rate: 192k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Peak Hold: On
Notebook: notebook_0, 3
Freq Set Varname: None

Packet Decoder
Access Code:
Threshold: 1

File Sink
File: ...ents/New/cat_out.png
Unbuffered: On
Append file: Overwrite

UDP Sink
Destination IP Address: 127.0.0....0.1
Destination Port: 5.001k
Payload Size: 1.472k
Send Null Pkt as EOF: True



```
'RfCat, the greatest thing since Frequency Hopping!'

Research Mode: enjoy the raw power of rflib

currently your environment has an object called "d" for dongle.  this is how
you interact with the rfcat dongle:
    >>> d.ping()
    >>> d.setFreq(433000000)
    >>> d.setMdmModulation(MOD_ASK_OOK)
    >>> d.makePktFLEN(250)
    >>> d.RFxmit("HALLO")
    >>> d.RFrecv()
    >>> print d.reprRadioConfig()


In [1]: 
```

Replay Attack

Replay Attack against PKE system of Cars

- RECORD

```
hackrf_transfer -r 43378000.raw -f 43378000
```

- TRANSMIT

```
hackrf_transmit -t 43378000.raw -f 43378000
```

Case study: Dallas Siren Hack

- Network Types
  1. Single Frequency Network
  2. Radio Repeater Network
- Command Transmission
  1. Analog RF Network
  2. Digital Repeater Network

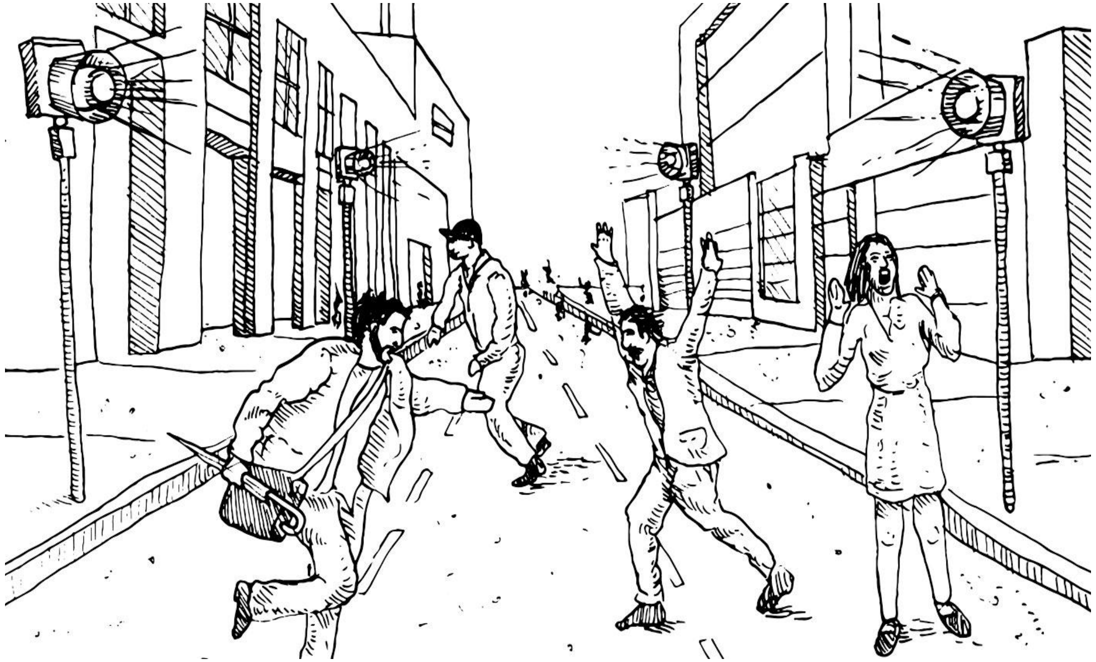


Illustration by D. Thomas Magee

Replay Attack (Disadvantages)

- Zero knowledge
- Effective even if the message is encrypted

- Cannot create a valid message from scratch
- Cannot “play” with messages - many times you’d like to modify a message based on the original one
- Tamper with ID and Command
- Perform input validation attacks

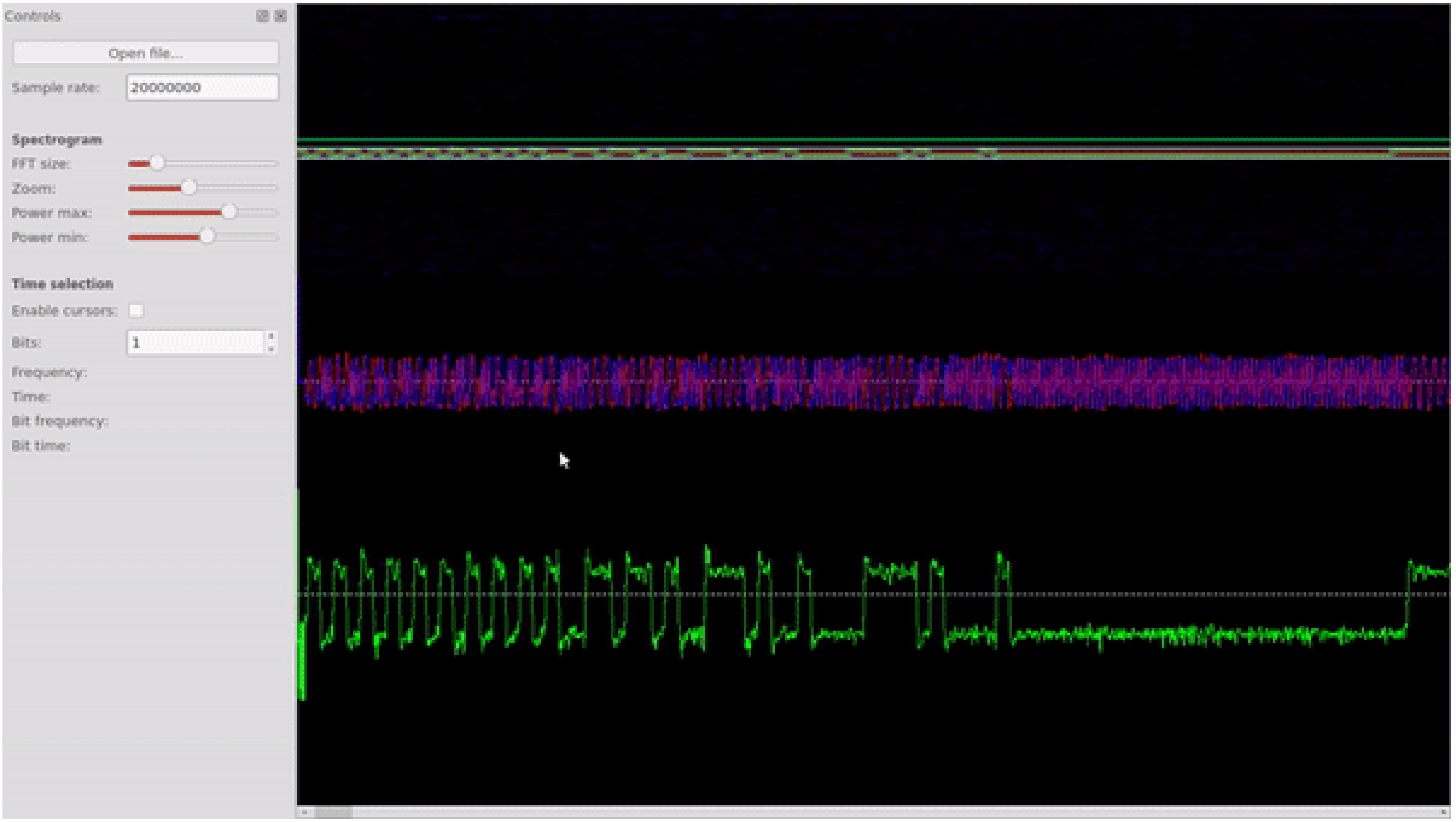
How is it done?

Documented Process:-

1. Record the signal with the SDR dongle and GQRX
2. Demodulate and Decode with Audacity in binary (1s & 0s)
3. Convert the Binary to Hex (0x)
4. Replay with RFcat libraries

Signal Hunting

1. Capture & Record
2. Analyze
3. Demodulate
4. Decode
5. Informational Packets



Sample rate: 20000000

Enable cursors: □

Bits: 1

Frequency:

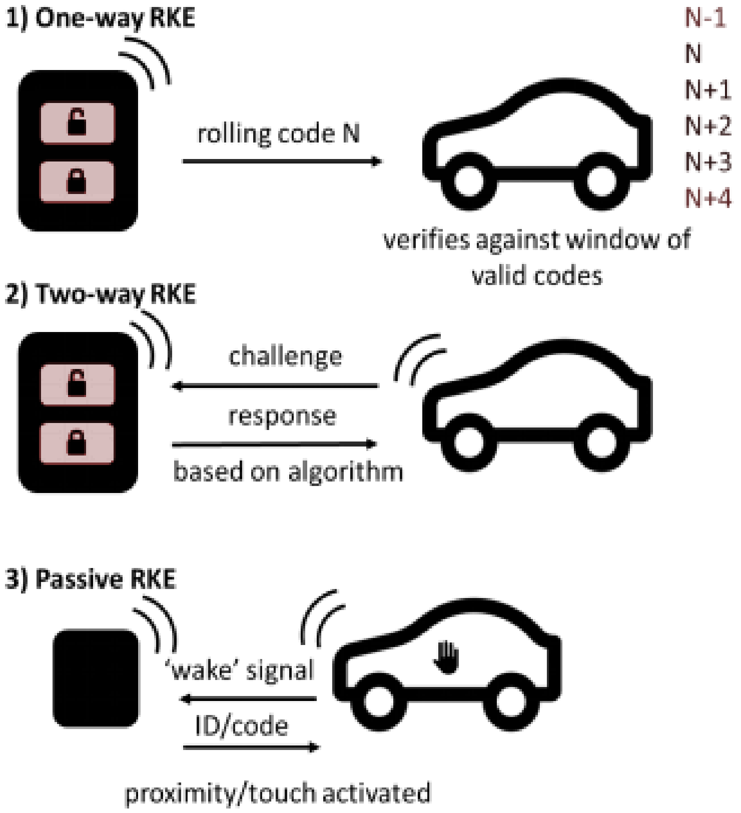
Time:

Bit frequency:

Bit time:

Case study: Car RKE

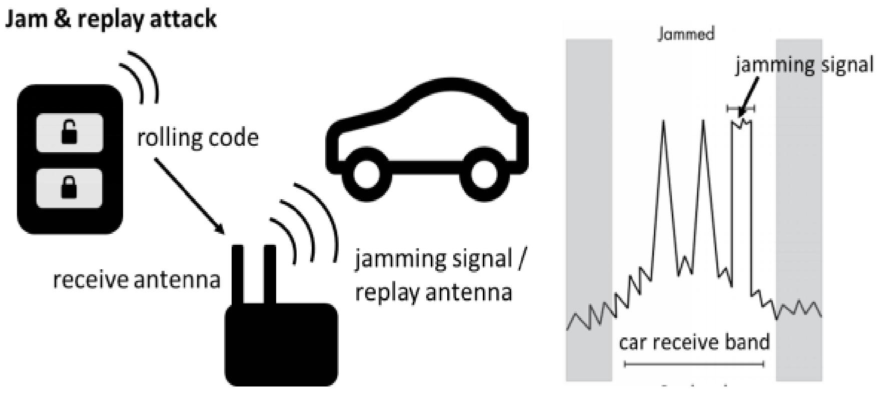
- Relay Hack by Qihoo 360, with a pair of gadget for just $22. (Passive RKE)
- RollJam device by Samy kamkar, to steal secret codes from key. (Two-way RKE)



Case study: Car RKE

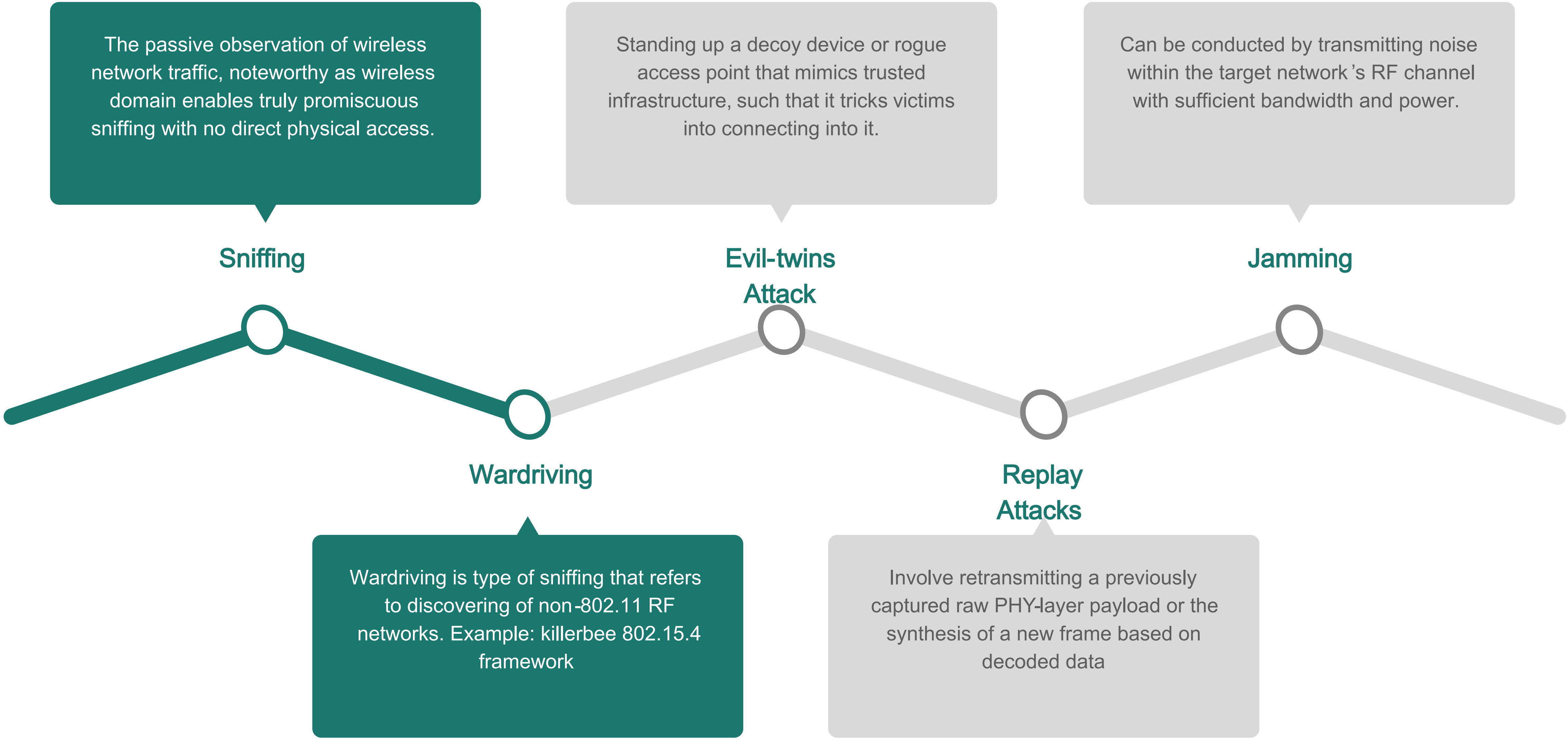
Possible Prevention:

- Requiring timing constraint in the call-and-response communication of car and key.
- Keep your keys in faraday bag that blocks radio transmissions.



RF Protocols

Types of RF Attacks



Sniffing

The passive observation of wireless network traffic, noteworthy as wireless domain enables truly promiscuous sniffing with no direct physical access.

Wardriving

Wardriving is type of sniffing that refers to discovering of non-802.11 RF networks. Example: killerbee 802.15.4 framework

Evil-twins Attack

Standing up a decoy device or rogue access point that mimics trusted infrastructure, such that it tricks victims into connecting into it.

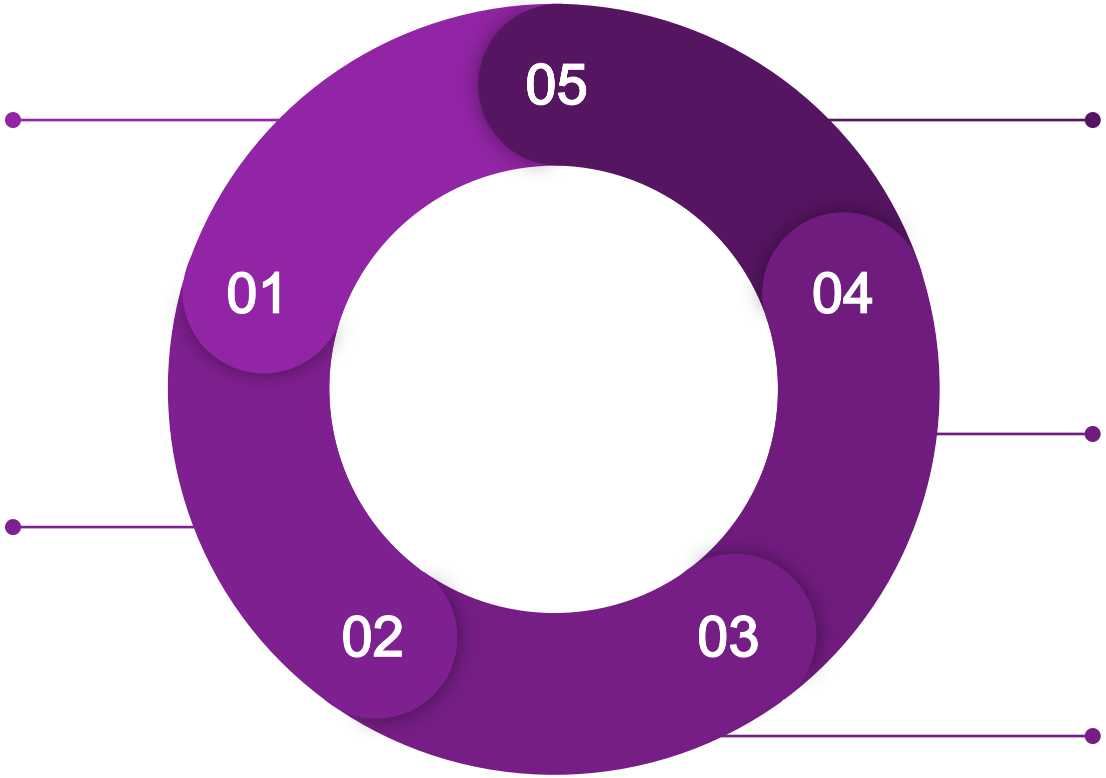
Replay Attacks

Involve retransmitting a previously captured raw PHY-layer payload or the synthesis of a new frame based on decoded data

Jamming

Can be conducted by transmitting noise within the target network’s RF channel with sufficient bandwidth and power.

Internet of Radio Vulnerability



Rogue Cell Towers

Used to hijack cellphone connections, and to break 2-factor authentication to listen to calls and read texts.

Rogue Wi-Fi Hotspots

Impersonate legitimate Wi-Fi networks, and might be used for MITM attacks to sniff network traffic and steal credentials.

Vulnerable Wireless Devices

Low-end keyboard/mouse dongle can expose to RF attack through keystroke injection, which may expose the larger network to insider attacks.

Eavesdropping/ Surveillance Devices

Voice activated FM & GSM, or other radio bugs

Unapproved IoT Emitters

Sensors often have multiple data radios, 802.11 is known, but what if also transmitting on other frequencies like Zigbee, or LORA.

Privacy, Rules, and Regulations:

- Check FCC and ARRL Regulations:
  - FCC 97.313 An amateur station must use the minimum transmitter power necessary to carry out the desired communications.
  - No station may transmit with a transmitter power exceeding 1.5 kW PEP.
- Steps for Compliance for IoT Organisations
  - Be aware of the data collected and processed.
  - Understand the functionality & implement consent.
  - Record everything to meet the requirements of privacy act.
  - Be aware of the privacy by design, and default.

Walk through of what we covered

- RF security requires you to look beyond the server side and mobile app security
- For simple replay, a good SDR device will just do
- It is advised to analyze the transmissions and reverse engineer them
- “security by obscurity” is often encountered
- Now let’s secure the RF world.. 😊

“APPLY”

- Attend related RSAC Sessions:

  Connected Cars: A Security and Privacy by Design Study 10 Years in the Making PRV-W03

  Wednesday, Mar 06 | 09:20 A.M. - 10:10 A.M.

  Shadow IoT Hacking the Corporate Environment: Office as the New Smart Home SBX1-W2

  Wednesday, Mar 06 | 09:00 A.M. - 09:30 A.M.

  Wireless Offense and Defense, Explained and Demonstrated! SBX3-R1

  Thursday, Mar 07 | 08:00 A.M. - 09:00 A.M.

  Cryptojacking Meets IoT HTA-R02

  Thursday, Mar 07 | 08:00 A.M. - 09:00 A.M.

- Get Started with SDR from greatscottgadgets.com

Thank You..!

Harshit Agrawal

harshit.nic@gmail.com

@harshitnic

Himanshu Mehta

mehta.himanshu21@gmail.com

@LionHeartRoxx