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

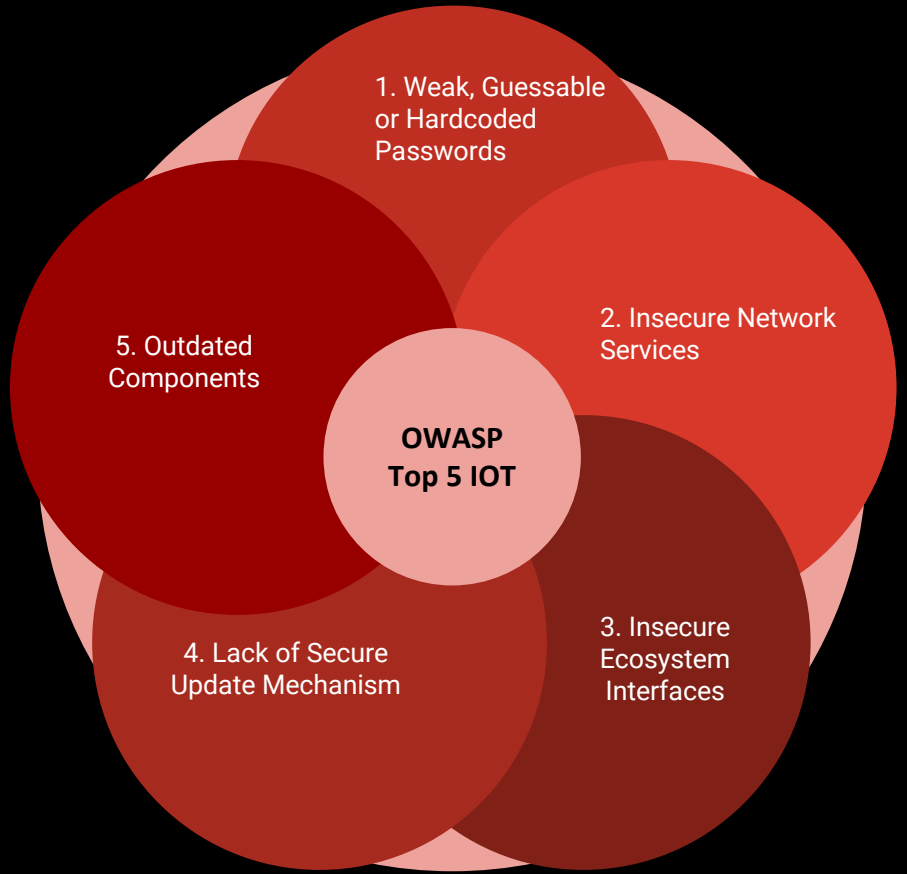
- Evolving radio technology landscape
- Security applications of Software Defined Radio
- What makes securing RF communications unique
- Top wireless Vulnerabilities
- Privacy, Rules and Regulations for RF

IoT:

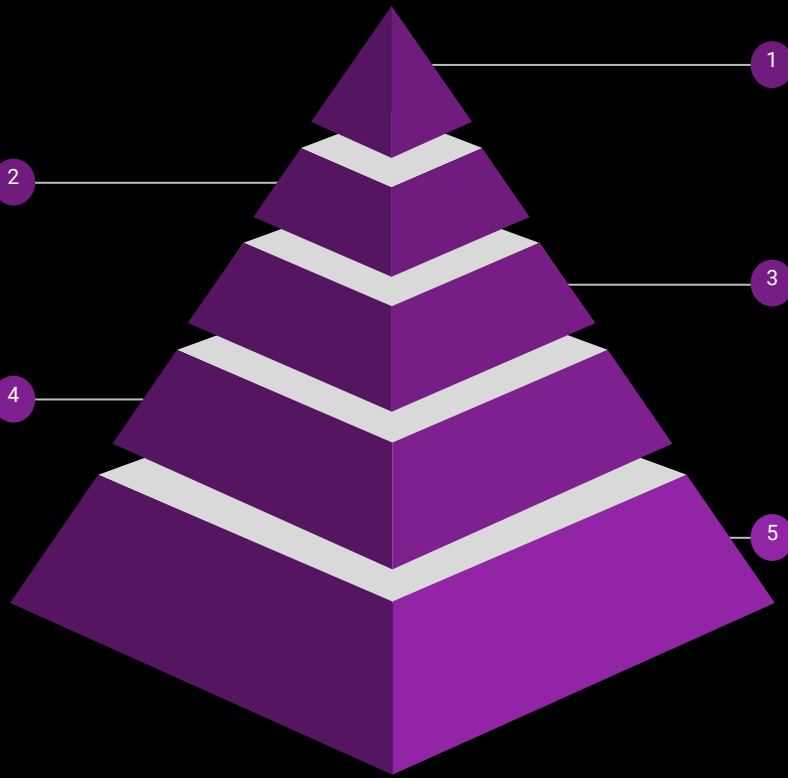
- This statistic shows the number of connected devices (Internet of Things; IoT) worldwide from 2015 to 2025.
- By 2020, the installed base of Internet of Things devices is forecasted to grow to almost 31 billion worldwide.

Evolving IoT/OT landscape:

The combined markets of the Internet of Things (IoT) will grow to about $520B in 2021.



Internet of things threat model



Controlling Device
Smartphone, tablets and other smart devices can control all types of “things”

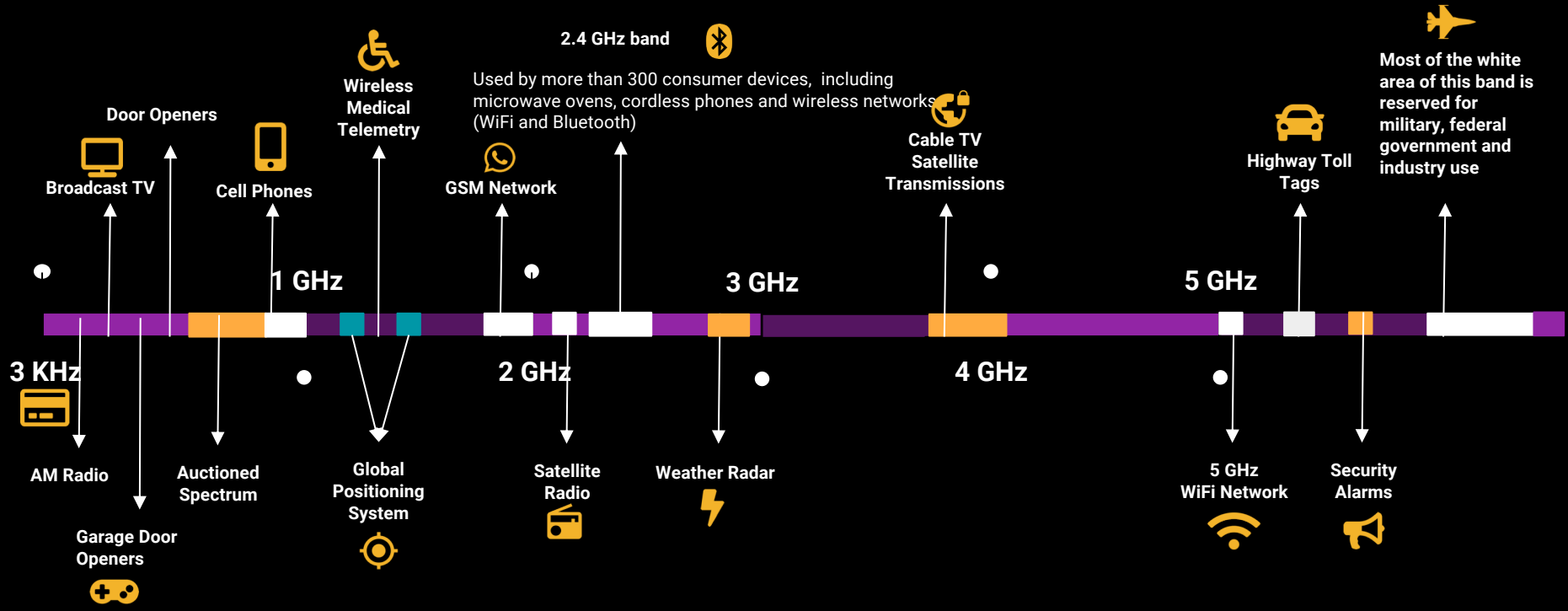
Cloud Service
Cloud services provide the repository and access control between the “things” and its controller.

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.

Inside the radio wave spectrum?

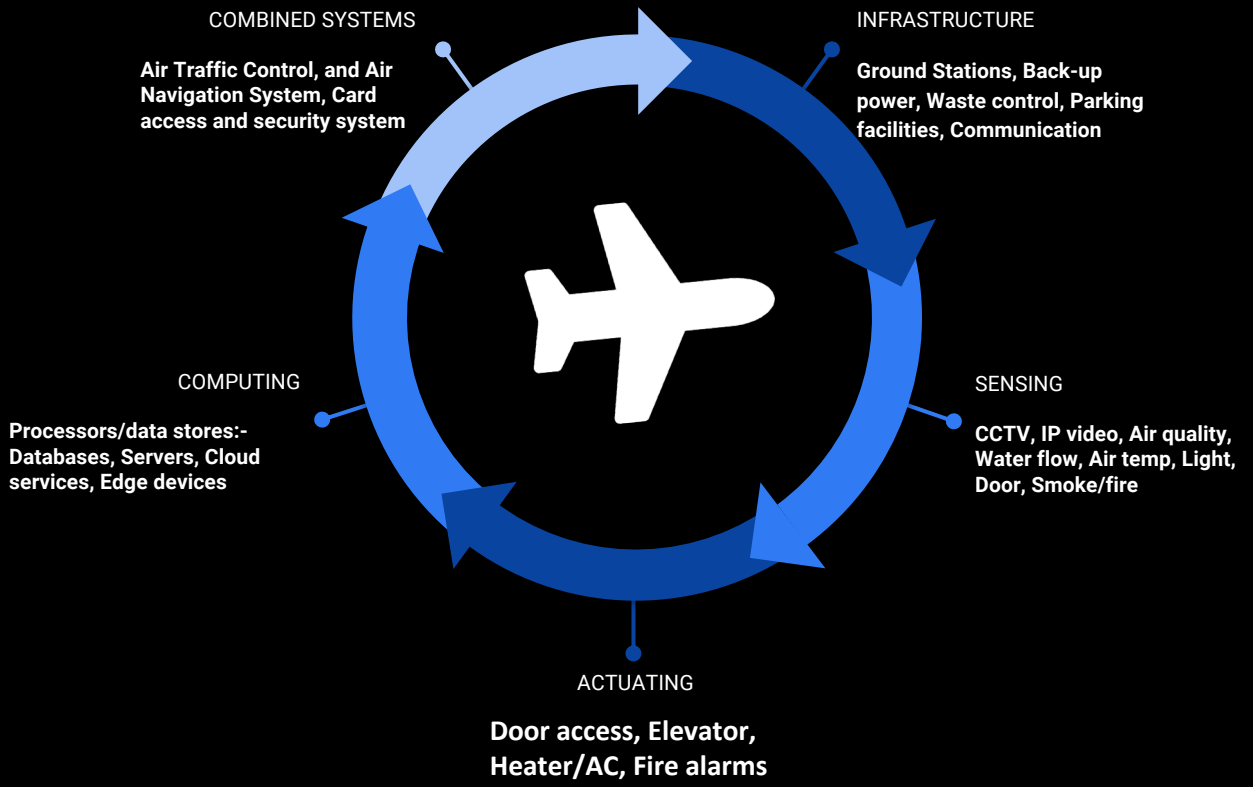


Why Focus on RF Security?

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

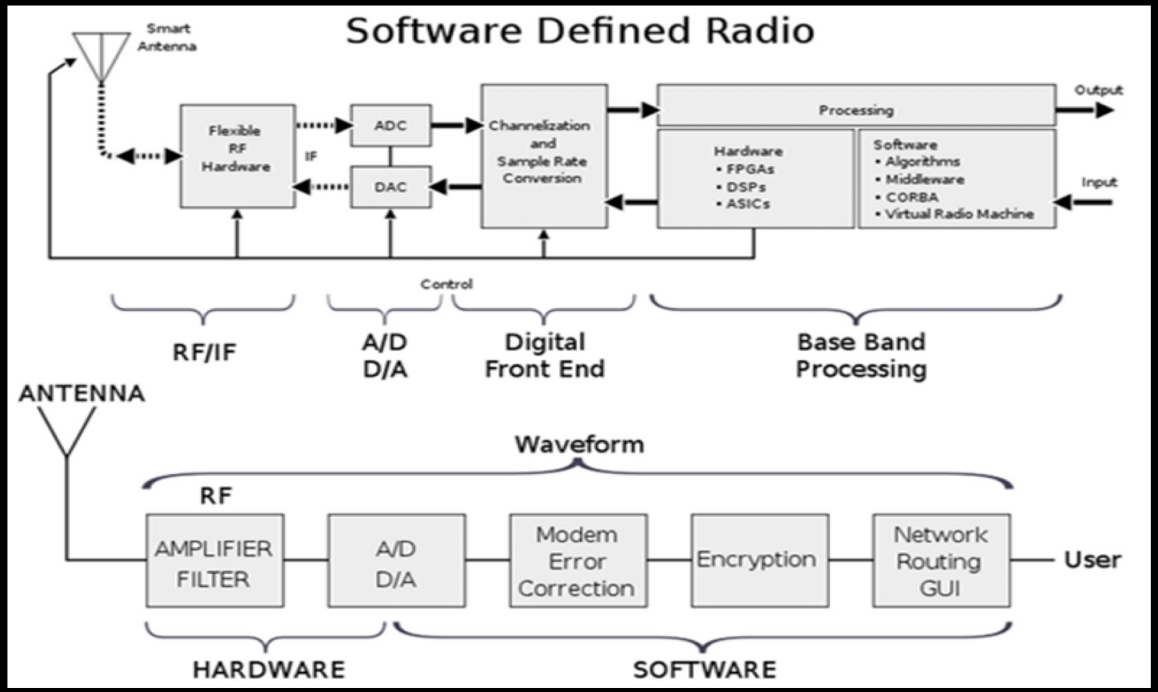
Why Focus on RF Security?

IoT Components in Aviation



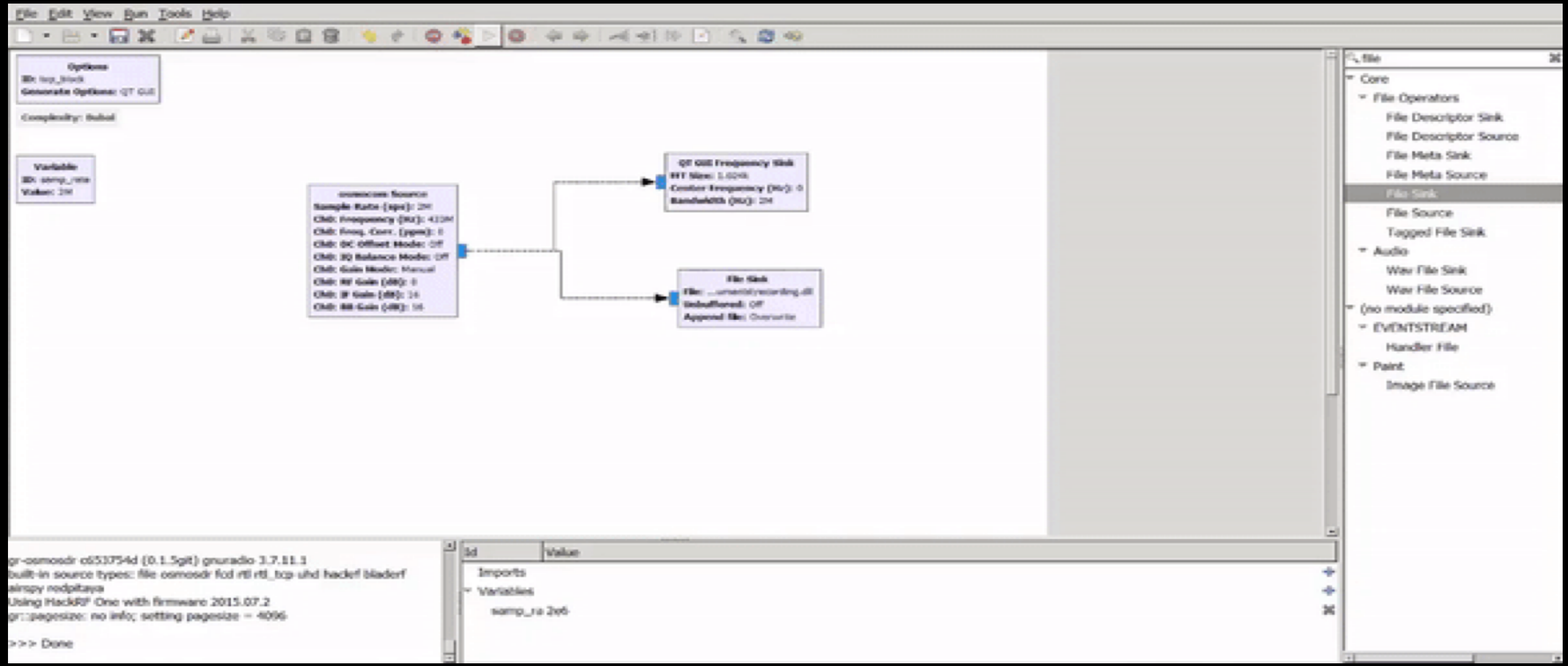
So what is SDR?

- 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

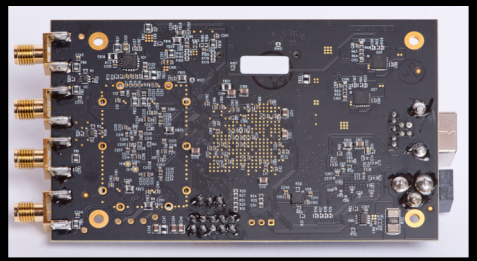
- GNU Radio is a framework that enables users to design, simulate, and deploy real-world radio systems.

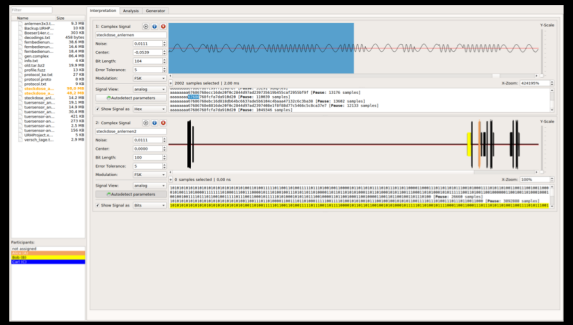


Hardwares and Softwares:

GNURadio

Audacity®

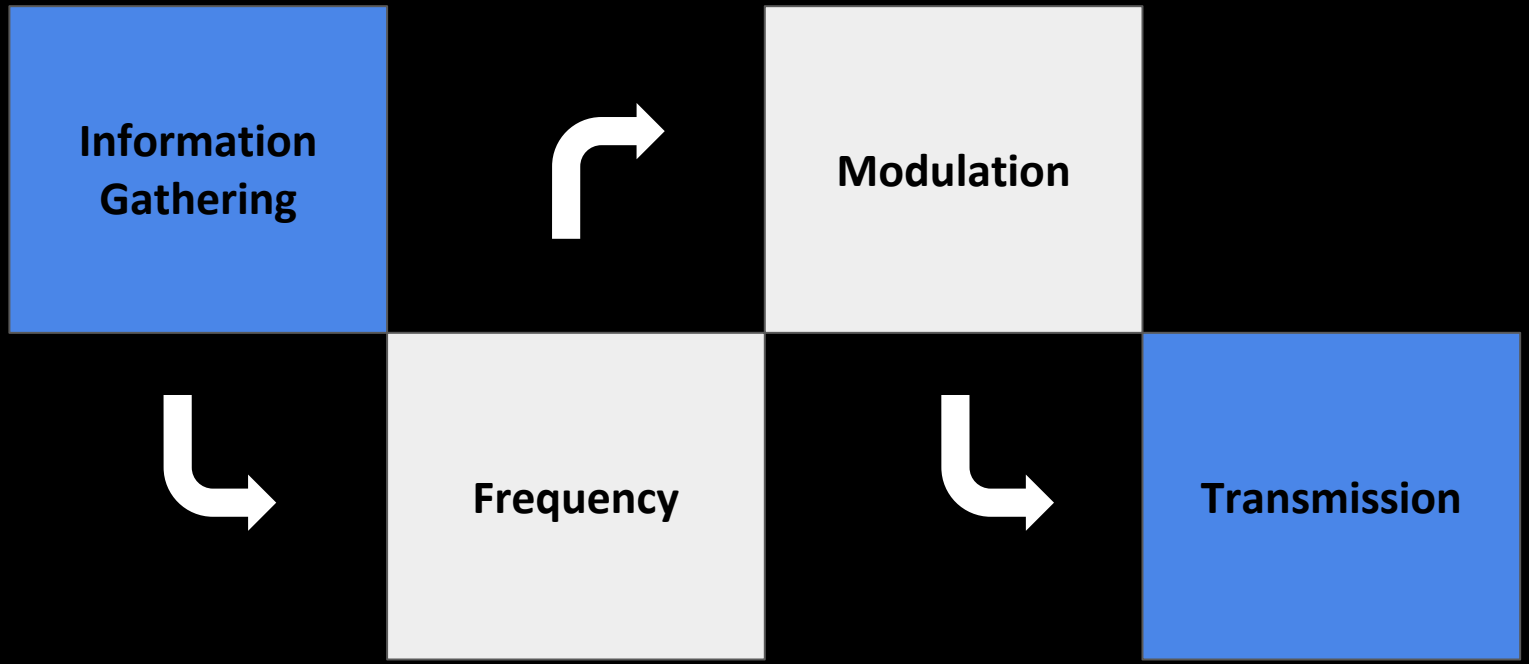




Initial Profiling of our device

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

Phases of RF Attacks:



Information Gathering:

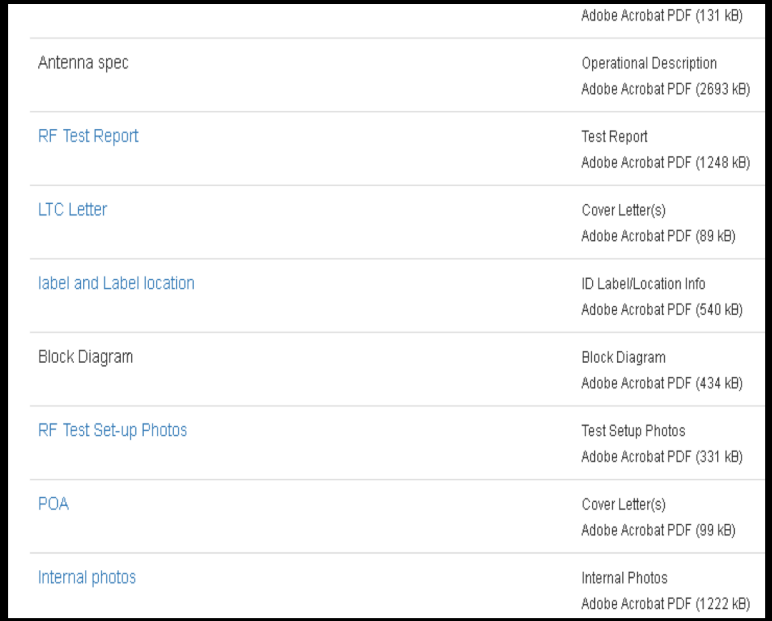
- A good starting point – if you have some luck –search for the FCC ID:
- https://www.fcc.gov/general/fcc-id-search-page
- Demo: https://fccid.io/Y8PFJ17-1

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**

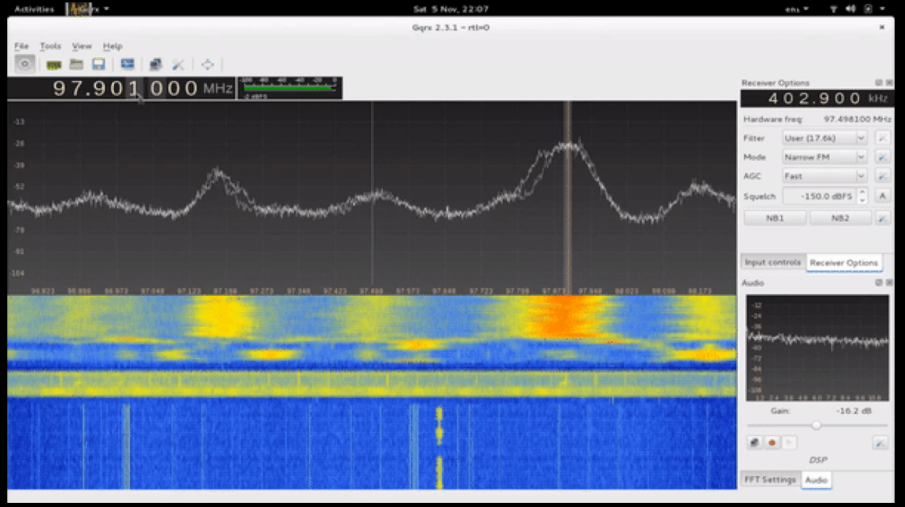


	Adobe Acrobat PDF (131 kB)
Antenna spec	Operational Description Adobe Acrobat PDF (2693 kB)
RF Test Report	Test Report Adobe Acrobat PDF (1248 kB)
LTC Letter	Cover Letter(s) Adobe Acrobat PDF (89 kB)
label and Label location	ID Label/Location Info Adobe Acrobat PDF (540 kB)
Block Diagram	Block Diagram 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:

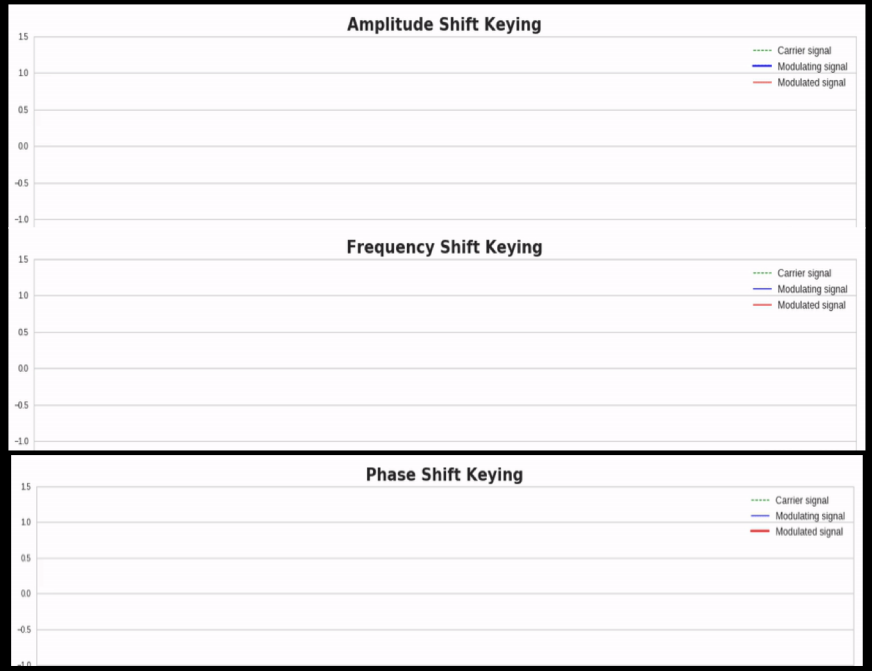
Use a Spectrum Analyzer (GQRX)

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



Modulation:

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



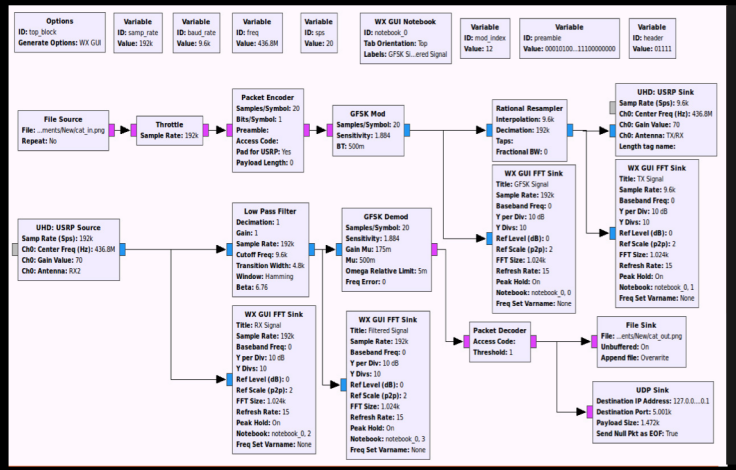
Source:Attify Inc

Transmission:

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

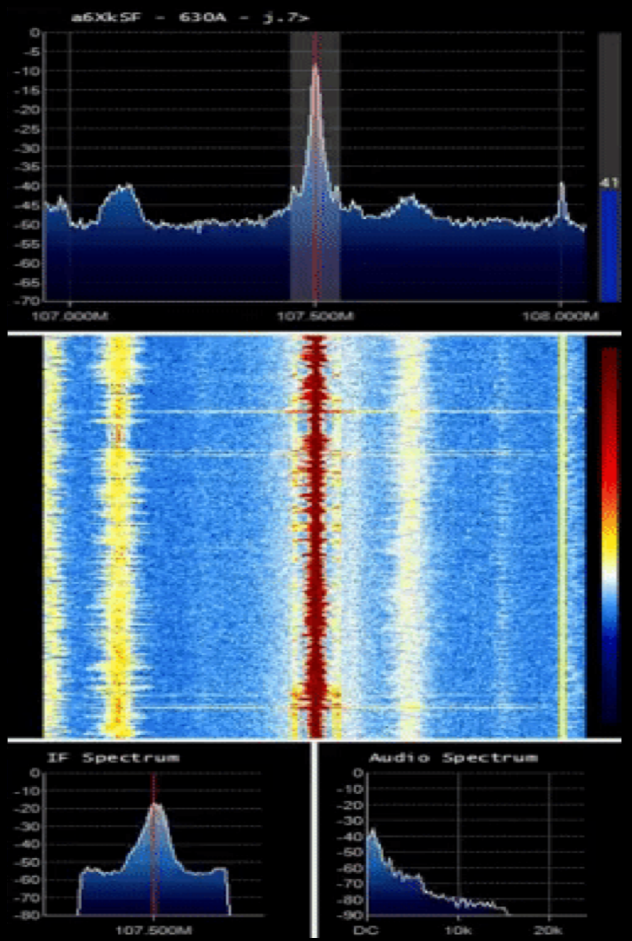
  Option 1: Use a flow graph

  Option 2: Command Line RF tool



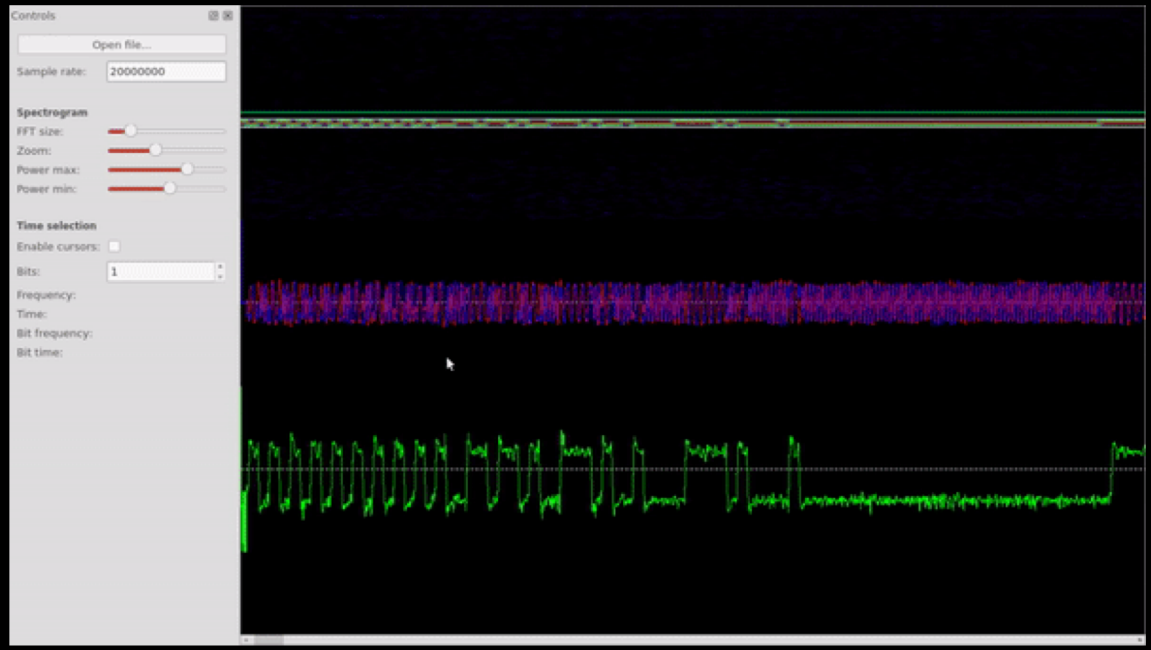
PHY LAYER

- 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



Signal Hunting

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



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

Replay Attack

(Advantage)

- Zero knowledge
- Effective even if the message is encrypted

(Disadvantages)

- 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

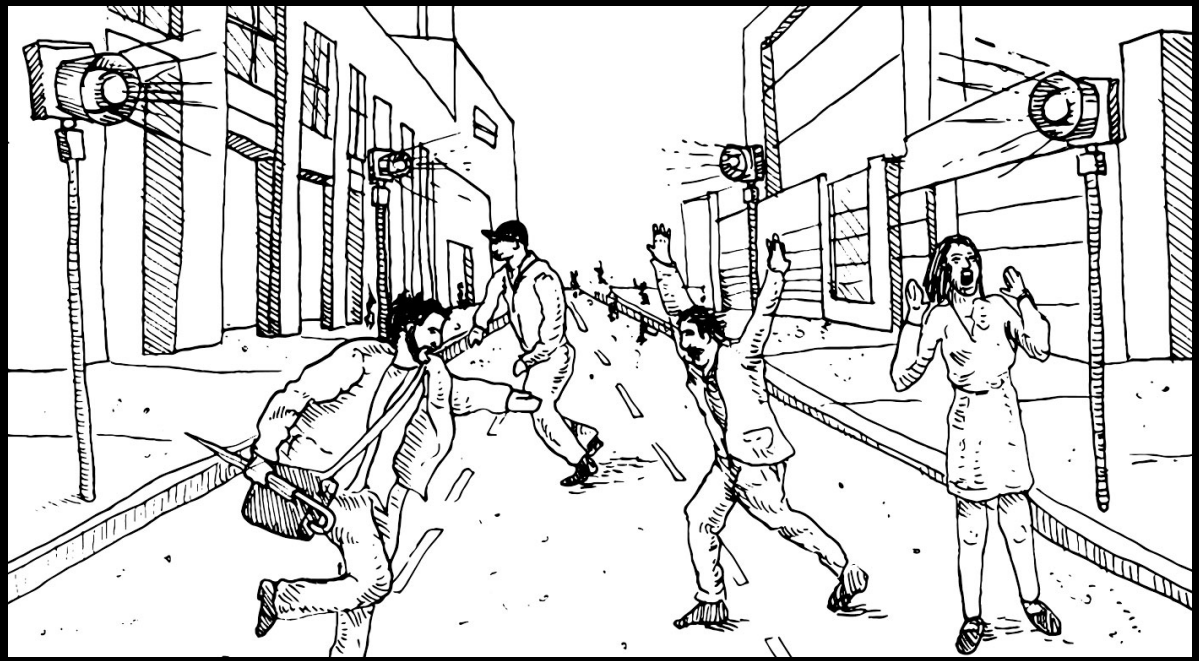
Demo:

Case study: Dallas Siren Hack

•Network Types
1. Single Frequency Network
2. Radio Repeater Network

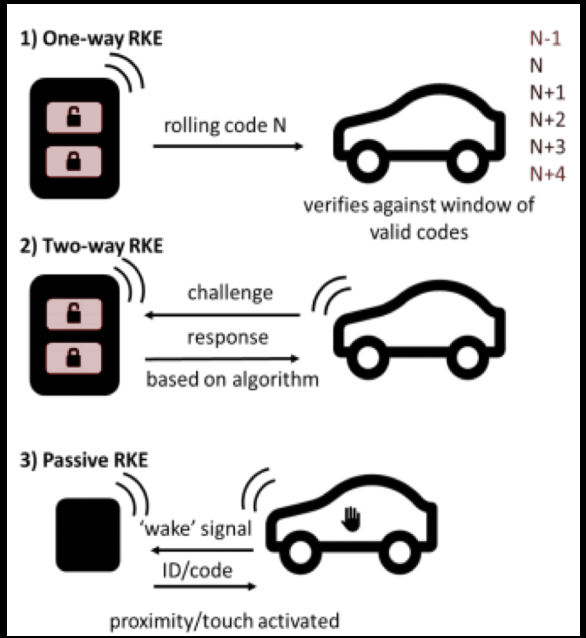
•Command Transmission
1. Analog RF Network
2. Digital Repeater Network

Illustration by D. Thomas Magee



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)

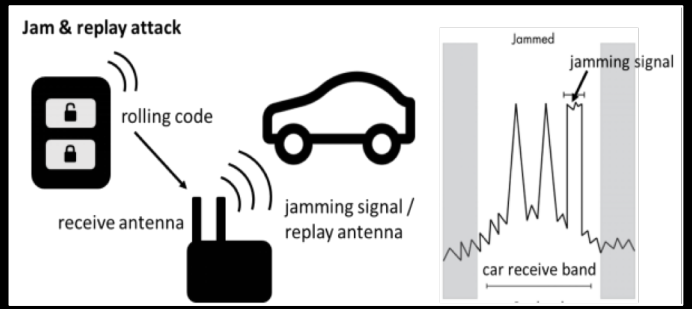


Demo:

Case study: Car RKE:

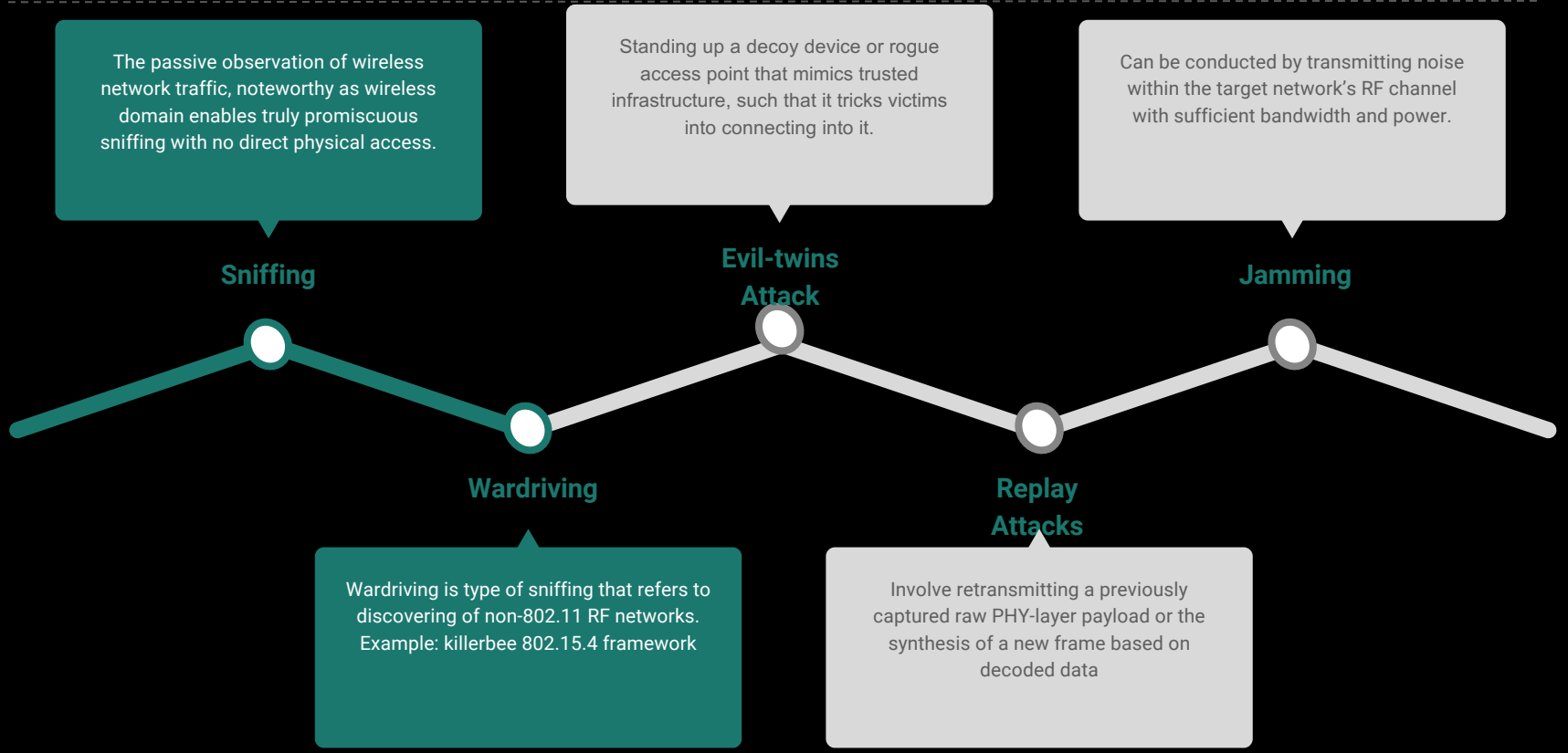
Possible Prevention:

- 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



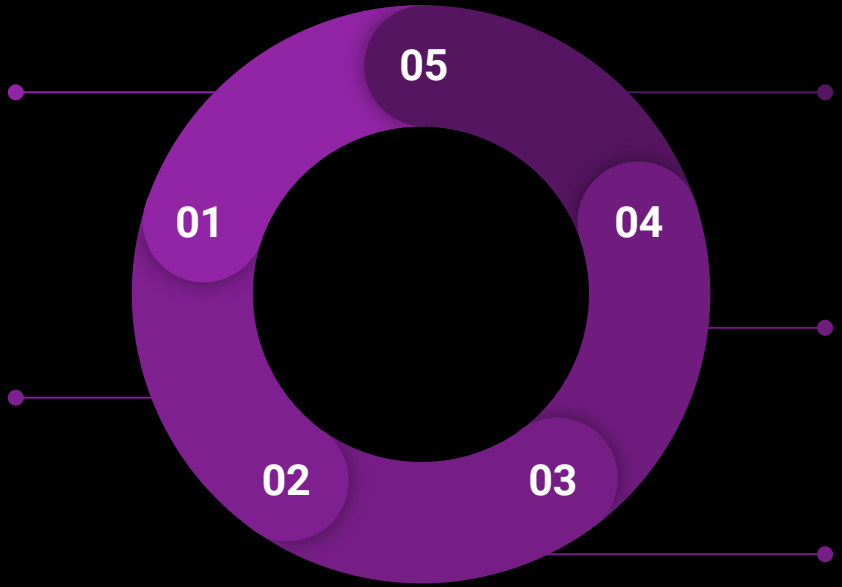
Internet of Radio Vulnerabilities

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.. ☺

Thank You..!

Harshit Agrawal

harshit.nic@gmail.com

@harshitnic

Himanshu Mehta

mehta.himanshu21@gmail.com

@LionHeartRoxx