RF Exploitation: IoT/OT Hacking with SDR

Himanshu Mehta

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

Harshit Agrawal

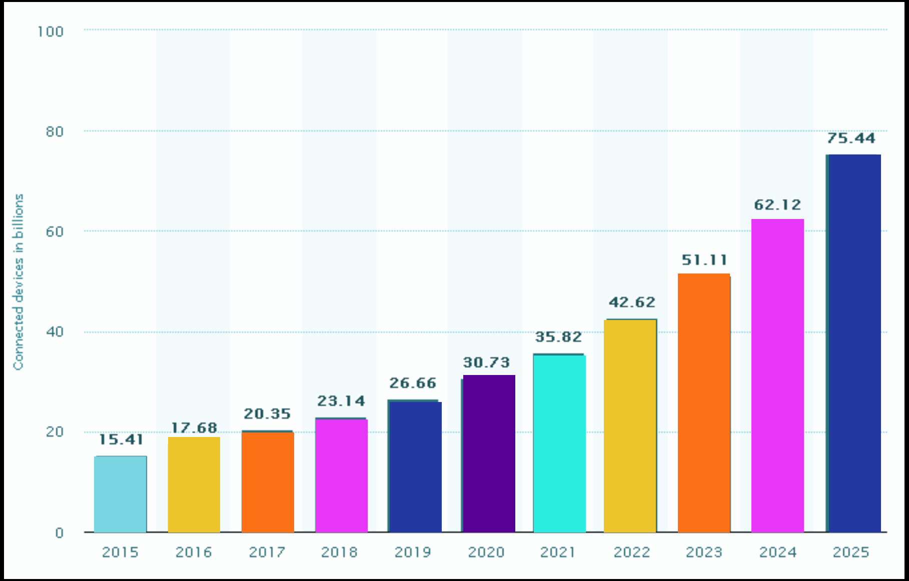
Security Researcher
MIT Academy of Engineering, Pune
harshit.nic@gmail.com
@harshitnic

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:

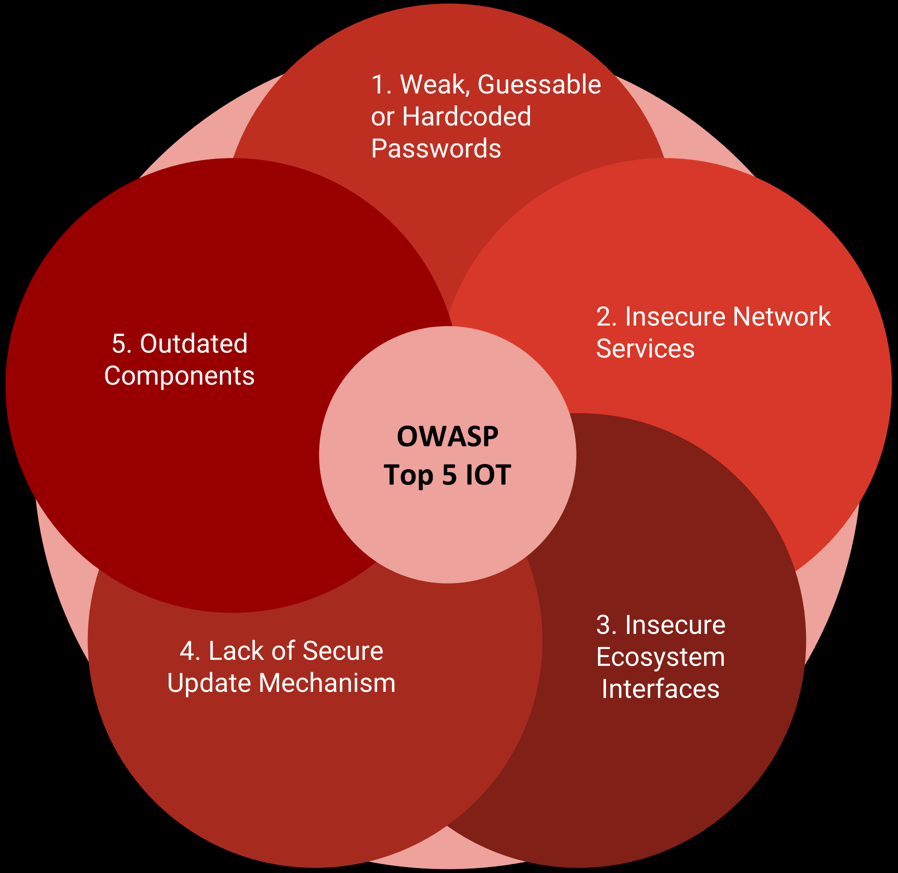
- This statistic shows the number of connected devices (Internet of Things; IoT) worldwide from 2015 to 2025.
- By 2020, the installed base of Internet of Things devices is forecasted to grow to almost 31 billion worldwide.



▶

Evolving IoT/OT landscape:

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



OWASP Top 5 IOT

1. Weak, Guessable or Hardcoded Passwords

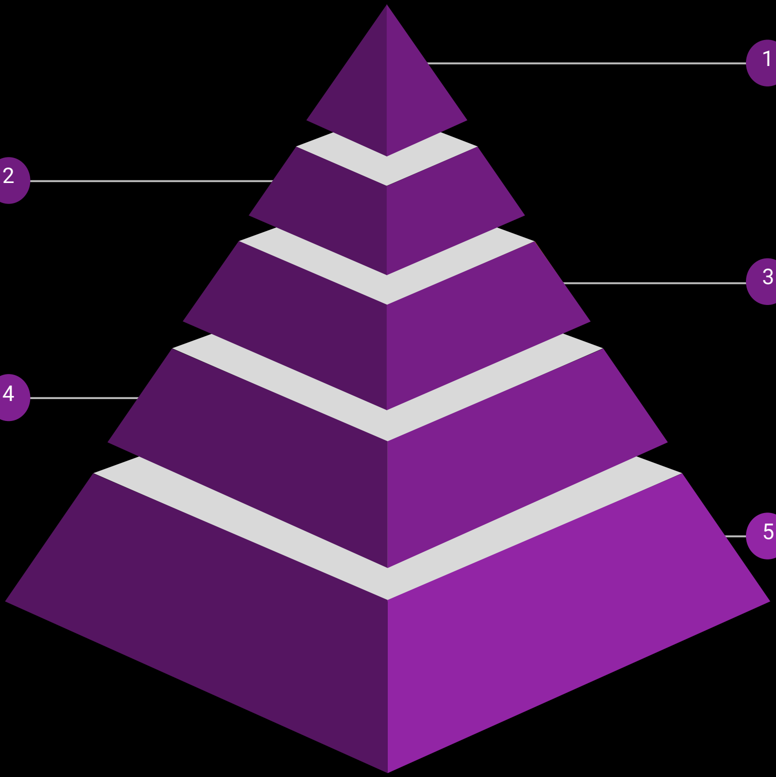
2. Insecure Network Services

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 Outdated Components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”

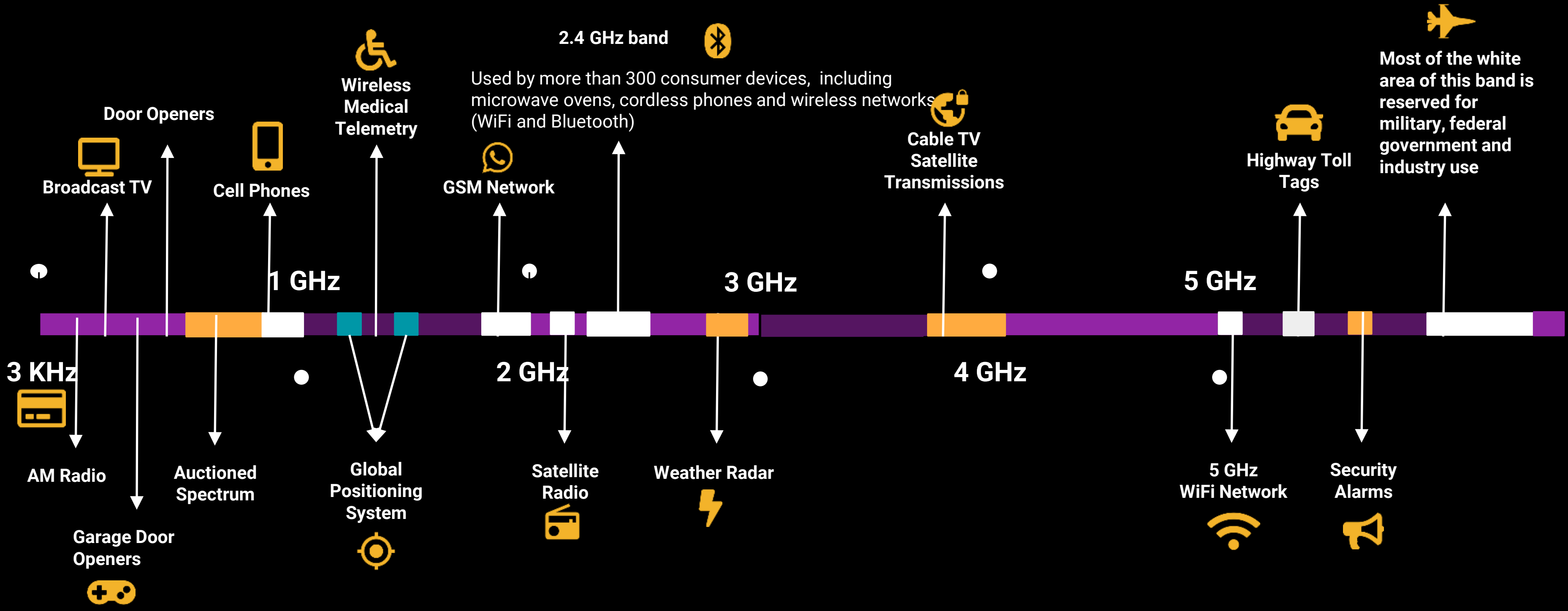
Cloud Service
Cloud services provide the repository and access control between the “things” and its controller.

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.

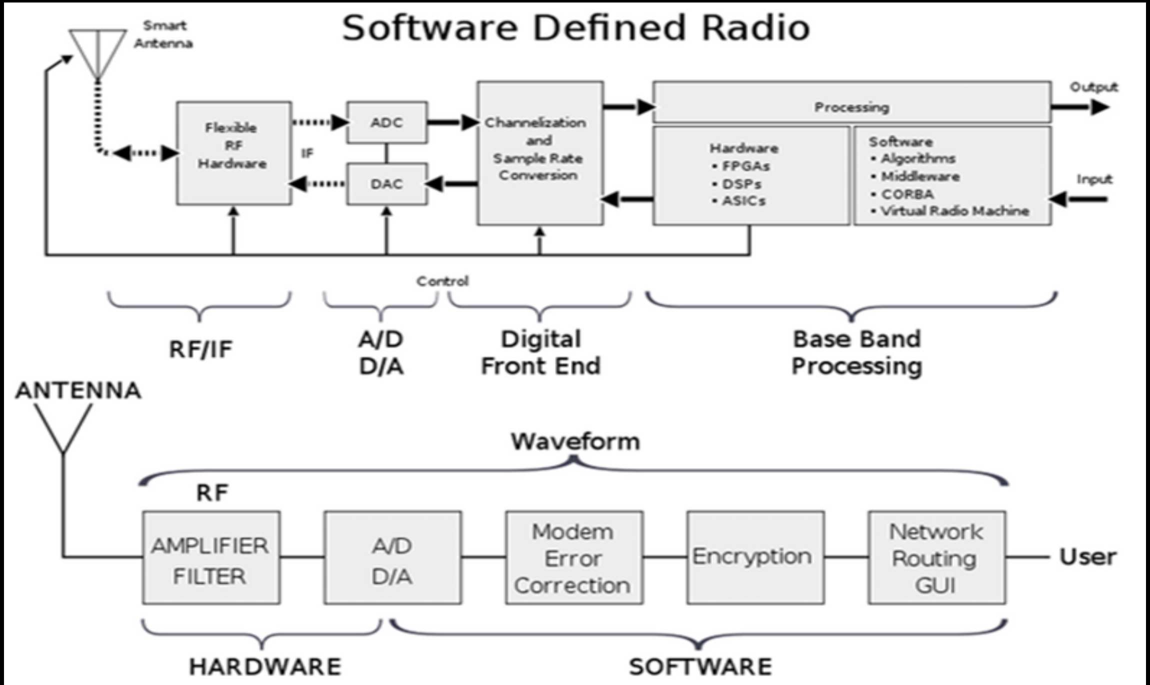
Inside the radio wave spectrum?


Door Openers
Broadcast TV
Cell Phones
Wireless Medical Telemetry
2.4 GHz band
Used by more than 300 consumer devices, including microwave ovens, cordless phones and wireless networks (WiFi and Bluetooth)
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?

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

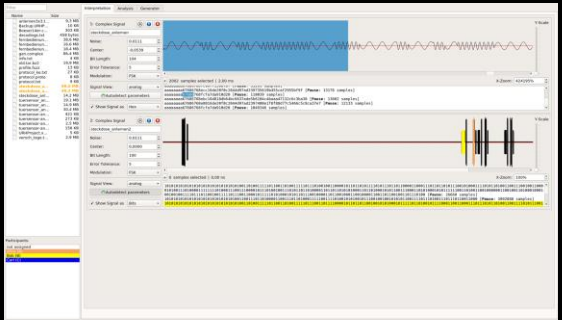


Hardwares and Softwares:

RTL-SDR.COM
QUICKSTART SETUP GUIDE: RTL-SDR.COM/QSG
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO+BIAS T+HF
V.3
CE

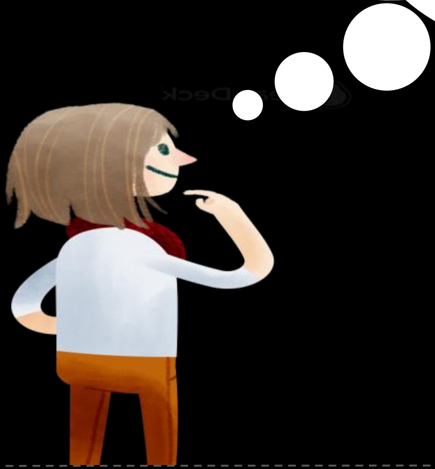
GNU Radio

Audacity®

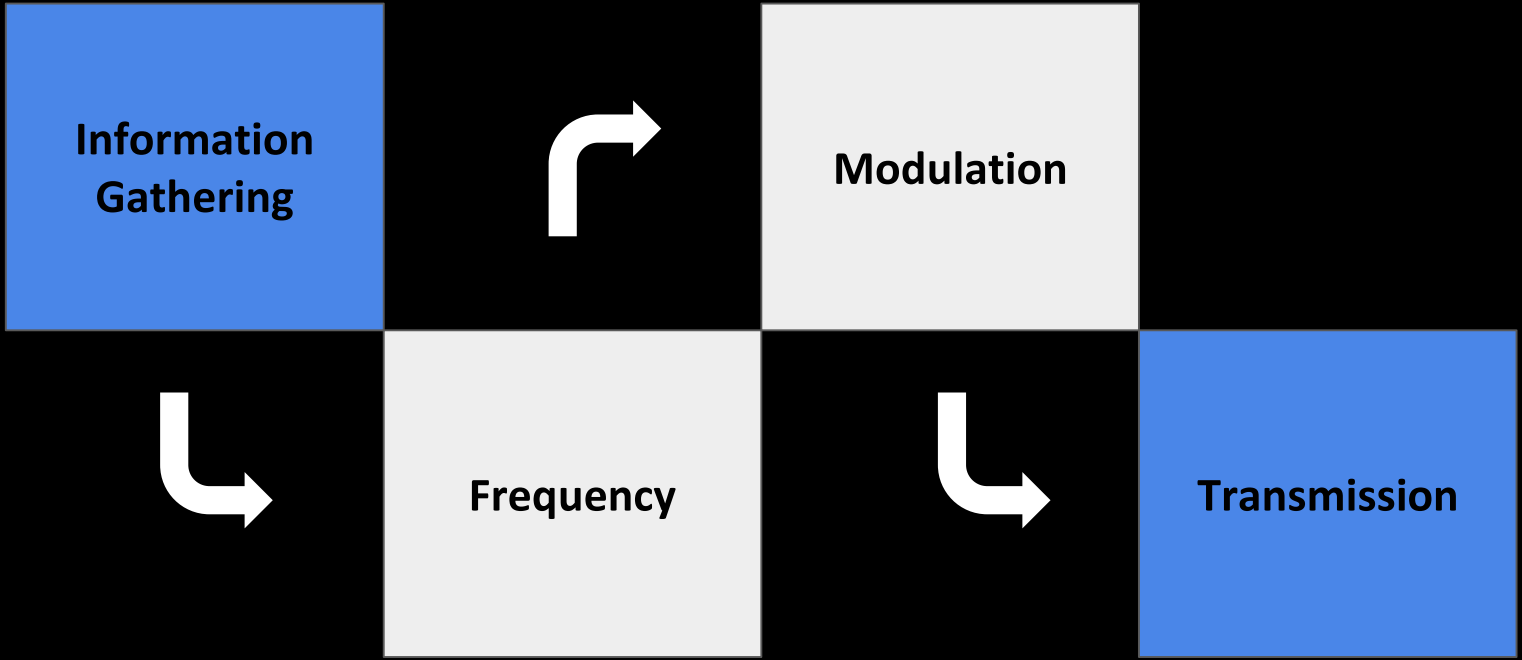


Initial Profiling of our device

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



Phases of RF Attacks:



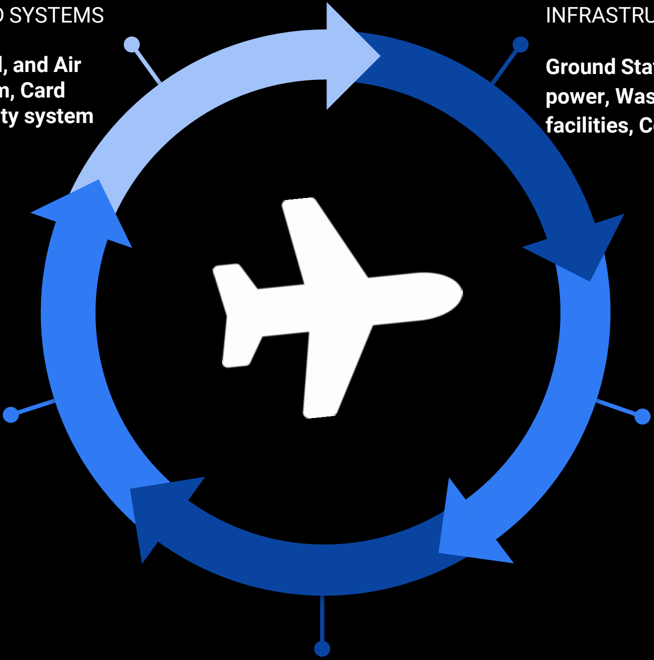
Information Gathering

Frequency

Modulation

Transmission

IoT Components in Aviation



COMBINED SYSTEMS

Air Traffic Control, and Air Navigation System, Card access and security system

INFRASTRUCTURE

Ground Stations, Back-up power, Waste control, Parking facilities, Communication

SENSING

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

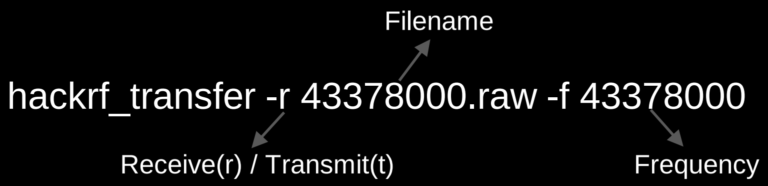
ACTUATING

Door access, Elevator, Heater/AC, Fire alarms

COMPUTING

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

Replay Attack



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

Filename

Receive(r) / Transmit(t)

Frequency

(Advantage)

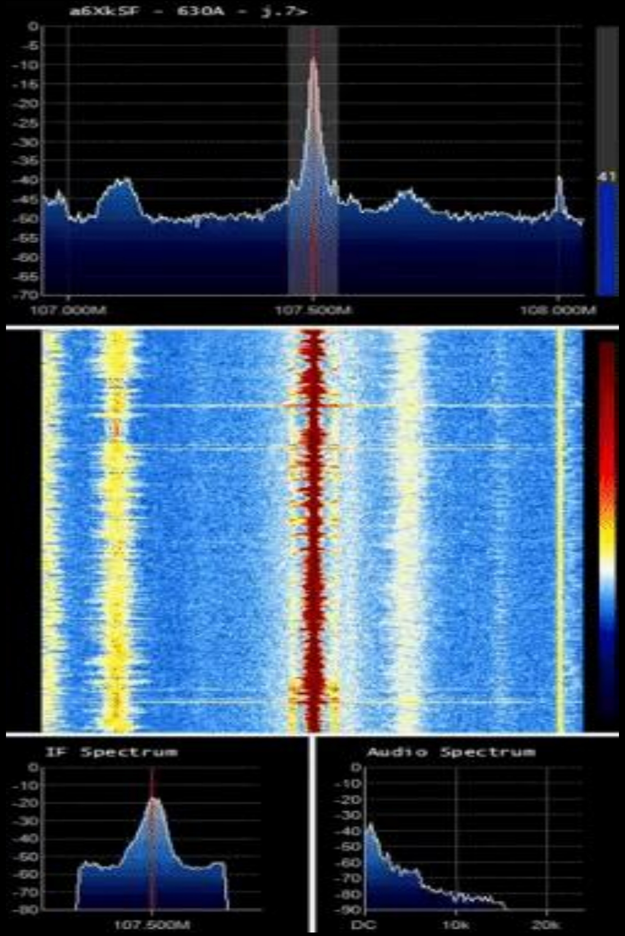
- Zero knowledge
- Effective even if the message is encrypted

(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

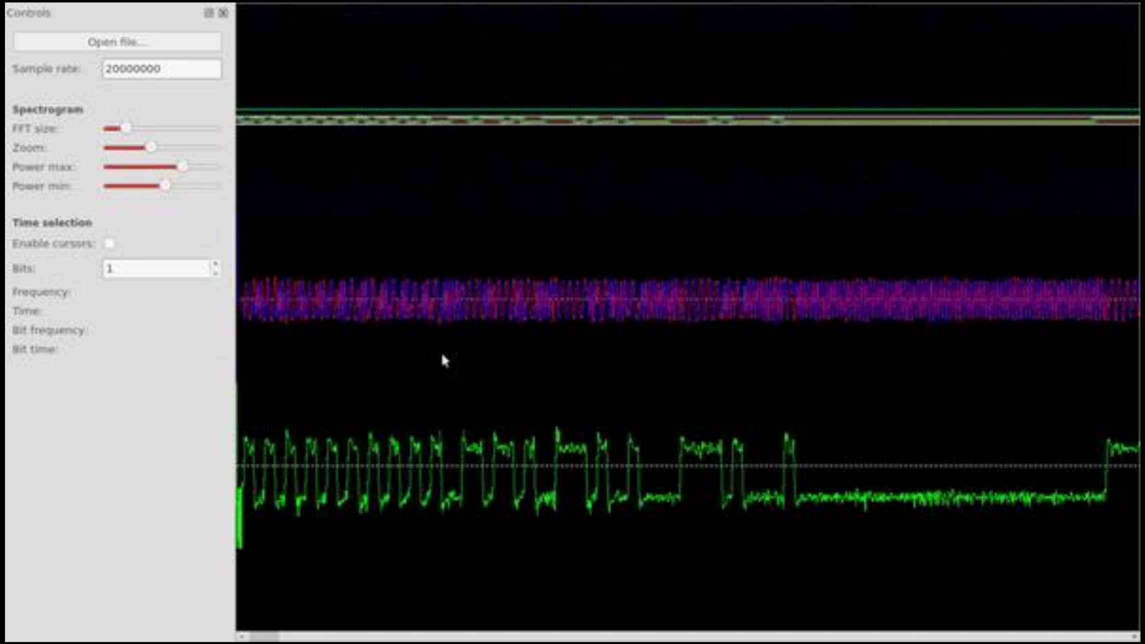
PHY LAYER

- 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



Sample rate: 20000000

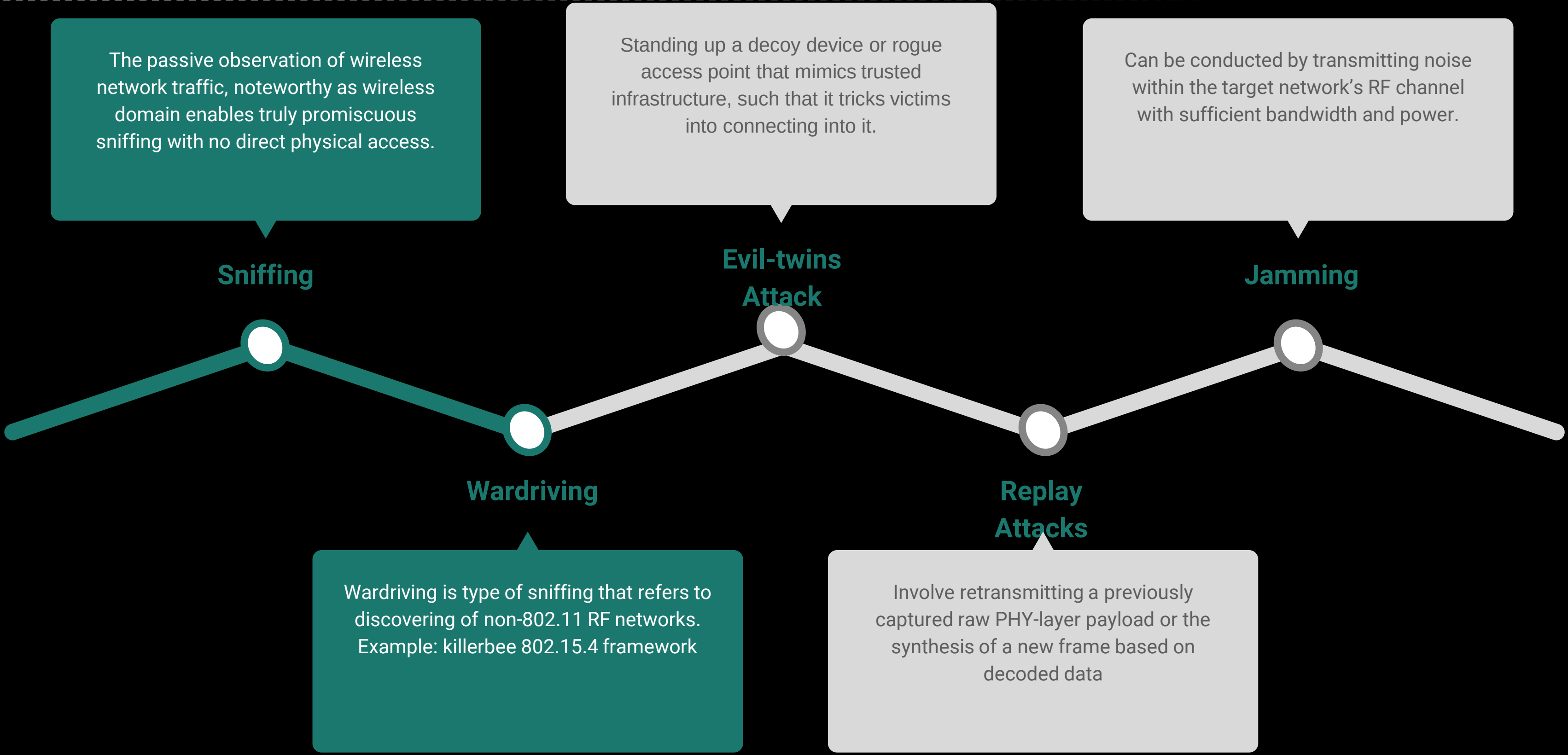
Bits: 1

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

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.

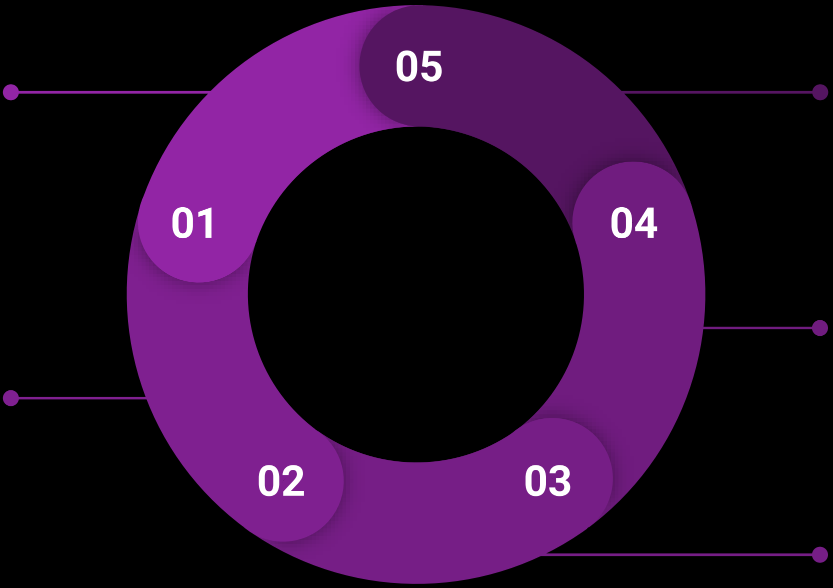
Replay Attacks

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 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