SNIFFING THE AIRWAVES WITH RTL-SDR

Yashin Mehaboobe
ArcanumX
#WHOAMI?

- **Security researcher, OpenSecurity**
- **Organiser, Defcon Kerala**
- **Likes hardware hacking, malware analysis and CTFs**
- **Invited to Kaspersky CyberConference, Nullcon, c0c0n, Toorcon San Diego and Defcon Kerala and Bangalore**
RADIO 101

• You have a transmitter and receiver
• Signals are encoded into a sine wave
• Frequency of the sine wave is different for different transmitters
• Antennas used for extending the range
RADIO 102

- What's important:
  - Modulation
  - Frequency range
  - Transmitting power
MODULATION

- Amplitude modulation
- Frequency modulation
- Phase modulation
STATUS OF SECURITY IN RADIO

- Security is low
- Encryption support exists but is not utilized
- Easily sniffable
- Hardware for sniffing usually expensive
- Security through obscurity
BEFORE SDRS

- Mixers, filters were all implemented in hardware
- Different radios for different frequencies
- Singular purpose
ENTER THE SDR

• Most components implemented in software.
• Allows you to choose the filter, amplifiers and detectors
• Use soundcard as ADC.
• Ranges from cheap (RTL-SDR) to expensive (USRP)
VARIOUS TYPES OF SDR

- HackRF
- BladeRF
- USRP
- Softrock
- RTL-SDR
ENTER THE RTL-SDR

• Discovered by Eric Fry
• Found that RTL2832U gives raw I/Q
• Cheap ($14-$20)
• Good frequency range (~25MHz to ~1700MHz)
• Currently compatible with a lot of software
**RTL SDR TYPES**

- **Mainly two types:**
  - **Elonics E4000 Chipset (rare)**
    - Best for reception
    - 64-1700MHz
    - Slightly more expensive
  - **Realtek R280T Chipset**
    - Easier to find
    - 24MHz to 1850 MHz
    - Cheaper
    - Slightly less sensitive
WHAT CAN YOU DO WITH IT?

- Listen to anything in the compatible frequency range
- Use upconverters and downconverters to receive above and below
- Listen to GSM, GPS, NOAA satellite images, Tire pressure monitors and more
- Easy access to the world of SDR
“SOFTWARE” DEFINED RADIO

- Lot of software popped up after rtl-sdr
- Many preexisting ones were patched with support
- Some are really difficult to set up (*cough* GNU Radio *cough*)
- Kali >1.05 / Pentoo
- Would still need to reinstall rtl-sdr library
• **Windows only**
• **Easy to use**
• **Zadig drivers**
• **Plugin friendly**
• **Recommended: Use the install script**
ADSB

- AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST
- 1090 MHz
- USE DUMP1090, ADSBSharp OR SIMILAR
- TRANSMITS LOCATION, ALTITUDE, SPEED, HEADING ETC
- COLLINAR, DISCONE, VERTICALLY POLARIZED ANTENNA, GROUND PLANE, J POLE
DSD

• Digital Speech Recorder
• Walkie Talkies
• P25 Radios
• ETC
DSD RUNNING ON WINDOWS
GNU RADIO

- Difficult to install and configure
- Versatile and one of the most powerful
- Block architecture
- Sources produce data
- Sinks allow you to save or display outputs
- Using gr3.6.5
RTL_SDR CODEBASE

- Testing the presence and perform basic SDR output/transfer
- \texttt{RTL\_fm (Basic fm receiver)}
- \texttt{RTL\_test (tests if the device is attached)}
- \texttt{RTL\_sd\_raw I/Q data)}
- \texttt{RTL\_tcp (to transmit raw I/Q)}
- \texttt{Kal\_rtl-\_sd\_r will need to be reinstalled}
GQRX

- Similar functionality to SDRSharp
- Preinstalled in Kali
- FFT + Waterfall display
- Built on top of GnuRadio
- Allows remote control
AIS

- Automatic Identification System
- Two channels: Channel 87 (161.975 MHz) and Channel 88 (162.025 MHz)
- Heard as blips
- Can be fed via virtual audio cable to AISMON or shipplotter
- Sound heard as blips
ACARS

- **Aircraft Communications Addressing and Reporting System**
- **~133 MHz. Varies regionwise**
- **Usually don’t contain location information (unlike ADS-B)**
- **Used in avionics systems (seems gibberish)**
- **Audio piping method to decode**
- **Antenna: J Pole, Discone, colinear**
NOAA SATELLITES

- Weather image satellites
- Circularly polarized antenna required
- Works at 137 MHz
- Software: Orbitron, wxtoimg, vb-cable, sdrsharp
- Antennas: Ground plane, turnstile, QFH
GP ANTENNA USED
GSM

![SDR screenshot](image-url)
IDENTIFYING SIGNALS

- Identify using the waterfall
- Identify the modulation used
- Frequency tells you a lot
- Also strength of the signal
MODIFICATIONS

- Interference limiting
- New antennas
- LNA
ANTENNAS

- Ground plane
- Discone
MCX CONNECTOR
SMA CONNECTOR
UPCONVERTERS

- Upconverters allow you to listen to frequencies below the RTL SDR range
- Nooelec Ham It Up Upconverter is a good choice
- Pass through and upconvert may be mixed
- Connect power and SDR
GOTCHAS

- Version of GRC
- RTLSDR module blacklisting
- Antenna
- Interference
- Wrong frequencies
SO WHAT ABOUT TX?

- Use HackRF
- RF CAT is a low cost alternative
- BladeRF
- Generic 433 MHz transmitters
SNIFFING WITH OTHER HARDWARE

- NRF24L01+ allows you to sniff BLE
- RFCat is good for sniffing and replaying
- Ubertooth One
THANK YOU!