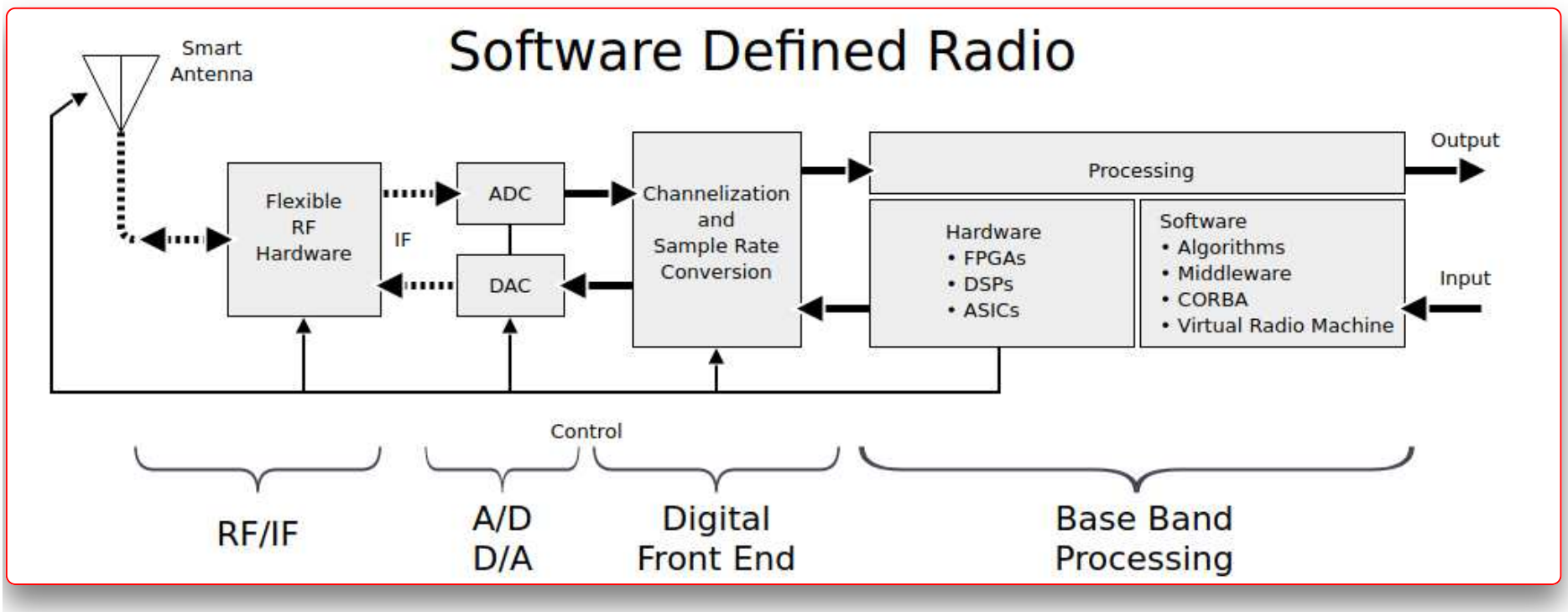
Payatu

IoT Security – Part 8 (Introduction To Software Defined Radio)

Appar

24-June-2020



Introduction

This blog is part of the "IoT Security" series. If you haven't read the previous blogs (parts 1 - 7) in the series, I urge you to go through them first unless you are already familiar with those concepts and want to only read about the current topic.

IoT Security - Part 1 (101 - IoT Introduction And Architecture)

IoT Security - Part 7 (Reverse Engineering an IoT Firmware)

previous blog in the series.

In layman's terms, Software Defined Radio is the implementation of major signal processing components i.e. modulators/demodulators, encoders/decoders, amplifiers, mixers (that are typically implemented in hardware) within the software. These software platforms are very generic and support all types of frequencies as well as different analyses on them. Even though the hardware is still a major requirement (transceiver and antenna) but the introduction of software-defined radio certainly created a wave in IoT as well as other major areas where wireless communication is used and made signal processing much more accessible than it used to be previously.

Wireless communication is one of the major attack surfaces in an IoT environment. SDR is the technology to build these wireless products, analyze the communication, and most importantly break it! Not only does SDR cover all major wireless communication protocols used in IoT i.e. Bluetooth, Zigbee, Wifi, NFC but it offers a vast range of other possible attacks that can be used to compromise the security of a device or infrastructure. A few of these are listed below:

- Cryptanalysis attack
- Side-channel attack like Tempest
- Cellular or Mobile network attacks
- SAT-comm analysis

And many more that we will be covering in the coming blogs.

Prerequisite

> "You can't run away from maths and theory when doing signal processing."

Well someone said it right :P But you don't have to be a maths geek to get started with Software-defined radio but knowledge of the basic concepts and terminologies will provide an edge while assessing your target and will help in a longer run:

- Basics of analog and digital signal
- Concepts of digital signal processing
- Communication systems
- Complex numbers
- Signals and systems
- Types of modulation
- Types of Encoding

We feel that the following topics are more than sufficient to help you get started with RF communication and assist you while learning about SDRs. We have some useful resources at the end of the blog that will help you understand these topics better.

Tools of trade:

> "A tool is but the extension of a man's hand..." -H.W. Beecher

Even though most of the signal processing is done via software but hardware tools are also required to transmit and receive the signals. Some hardware and software tools that are necessary for SDR are listed below(we will elaborate on a few of the tools mentioned below as we proceed):

Hardware

Basically, when we pick an SDR peripheral device, the things to keep in mind are its:

- Operating frequency range

This defines the range of frequency the peripheral device is capable of performing operations upon (Tx and Rx). It's always nice to have a wider operating frequency range at your disposal.

- RX Bandwidth

Greater the RF front end bandwidth (Rx bandwidth), the more our SDR peripheral can gather data around the operating center frequency. Keeping in mind that with wider RF bandwidth we always gather in more noise as well.

- ADC Resolution (in Bits)

Usually, an ADC which has a higher resolution is preferred, but keeping in mind with higher ADC resolution we need to decrease the signal processing overhead such that we can process the samples in real-time. Hence choosing a proper ADC resolution is important.

- Transmiting and recieving capabilities

While most of the peripheral devices can receive(Rx) but not all can transmit(Tx). So it's safe to say a transceiver(Tx-Rx both are present) is preferred as many attacks require transmitting(Tx) of signals as well. Also, based on the requirement, the transceiver can be categorized under half-duplex, full-duplex, and so on.

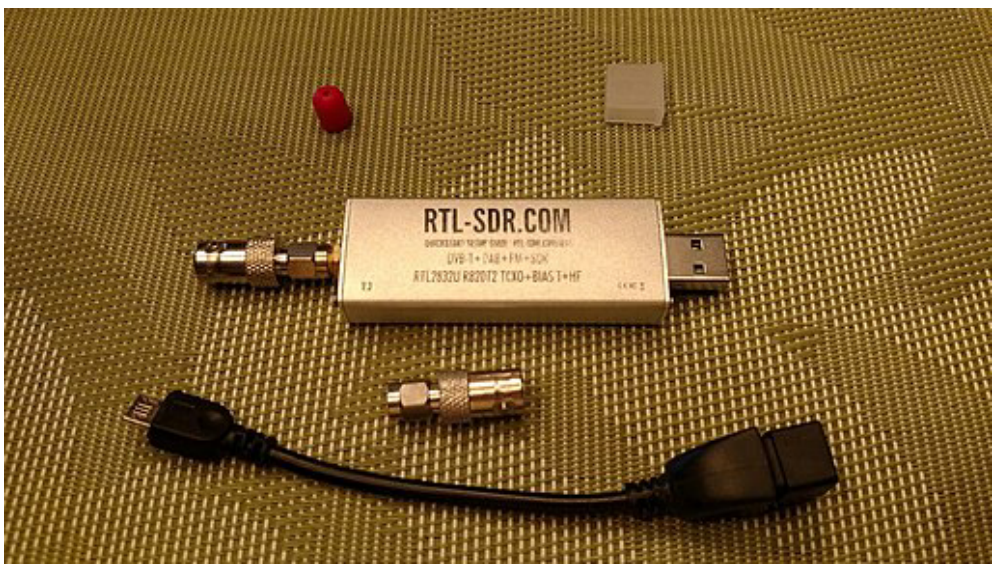
- Cost

This is probably the major factor as most of these peripheral devices cost a lot of money. We need to choose one carefully, that fulfills all our requirements based on assessment type.

Now lets jump into some popular SDR devices present out there:

1) Realtek SDR Dongle (RTL820T2)

Ask any SDR hobbyist or professional as to what their first tool was, It'll probably be an RTL-SDR dongle. Although for a cost this low it provides with a range from 24-1766MHz which is quite impressive. A few can other variants can go up to 2.2GHz. The only setback is that it is an SDR receiver, doesn't have any TX capabilities (not considering leakage from its internal local oscillator). Other popular variants are NooElec R820T, R820T, and Terratec R820T.



RTL-SDR R820T2 Dongle

Image source:**https://commons.wikimedia.org/wiki/File:Rtl-sdr.jpg**

2) HackRF One

It is a widely used and recommended tool by hobbyists due to its comparatively reasonable cost and exceptional frequency range 10MHz to 6GHz (Practical range). It is an SDR transceiver i.e. It has both transmit (Tx) and receive (Rx) capabilities. So for someone who's looking for a massive frequency range, wide bandwidth and transmit capability it's the perfect match.

HackRF One by Great Scott Gadgets

Image source:**https://commons.wikimedia.org/wiki/File:Hackrf-one-img_0005.jpg**

3) BladeRF 2.0 micro

One can't miss out on Blade RF when it comes to a powerful SDR peripheral. It even though has an operating frequency ranging from 47MHz to 6GHz and 56MHz of bandwidth what sets it apart is the presence of a powerful FPGA processor, which means it can easily do some of the signal processing itself on board. Making it an ideal standalone device. Reason being there are quite a few interesting projects based on BladeRF that include:

- **YateBTS**
- **ATSC Transmitter**
- **RAMEAR**

  to name a few.

4) USRP B210

Ettus products are mostly used by professionals and Industries due to their high capabilities. Making it the most expensive peripheral device compared to the others. It has a very high sample rate and a broad tuning rate. Talking of B210, it operates on freq 70Mhz to 6Ghz, being full-duplex and having the maximum sample rate among the above listed of 61.44MS/s.

USRP by Ettus

Image source:**https://commons.wikimedia.org/wiki/File:Usrp.jpg**

Here's a brief comparision between a few popular SDR peripheral devices:

Name	Frequency Range	Bandwidth	ADC Resolution	Tx capability	Price
RTL-SDR R820T2/RTL2838U	0.5 – 1766 MHz	Matches sampling rate, but with filter roll-off	8	NO	USD 24
HackRF One	1 MHz – 6 GHz	20 MHz	8	YES	USD 299
bladeRF	47 MHz – 6 GHz	56 MHz	12	YES	USD 480
USRP B210	70 MHz – 6 GHz	56 MHz	12	YES	USD 1,100
LimeSDR	100 kHz – 3.8 GHz	61.44 MHz	12	YES	USD 299
YARD Stick One	300 MHz – 1GHz	-	8	YES	USD 100

Antennas

While the selection of an antenna following things are kept in mind:

- Antenna Gain

  As most of the gains in the antenna datasheets are referred to an isotropic antenna, it is necessary to see where the 3dB gain and bandwidth are located and do some basic math to see if the antenna is fit for our operation.

- Aperture

  The main objective here is how much signal can we gather or how big of a signal we can gather. Hence it is advisable to choose antenna at the proper center frequency and whose front-facing diameter is good enough to accommodate all incoming signals in them at a time.

- Directivity and bandwidth

  With the main beam pattern of the antenna, we need to see how much gain it has on its main lobe and how much suppression it provides on its sidelobe. If the antenna has a good main lobe with 3dB cut off in its main lobe and complete suppression on its sidelobe then it is perfectly fine to choose such antenna

- Effective length

  With some special antennas like yagi and log periodic it is very much necessary to choose the proper length such that the antenna can operate with maximum efficiency in its center frequency and optimal efficiency in its other frequency.

Based on the requirement and type of assessment the type of antenna is selected. Below are some commonly used antenna for SDR

- Telescopic (Stock antenna with most of the SDR transceivers)
- Discone (Outdoor antenna)
- Vertical (Outdoor antenna)
- Yagi-Uda

Conclusion

We hope this gives you an introduction to the world of RF and SDRs. In this part we covered all the basics and hardware tools required for an SDR assessment. In the next blog, we will look at the software tools that are available and have a look at the classic approach to a target.

Continue to the next part - IoT Security – Part 9 (Introduction to software defined radio)

Resouces:

- **Getting started with Radio Hacking – Part 1 – Radio Frequency basics and theory**
- **Getting Started with Radio Hacking – Part 2 – Listening to FM using RTL-SDR and GQRX**
- **SDR with HackRF by Michael ossmann**
- **University of Illinois Digital signal processing series**