GNU Radio

Software Defined Radios

by

Aaron Grothe

Disclaimer

GNU Radio can transmit in frequencies that are protected by the FCC. For the most part these are very low power devices but please still be mindful of that

GNU Radio can also do certain activities such as replay attacks which can get you in trouble with the DMCA

In short be careful

What is GNU Radio?

GNU Radio is a Software Defined Radio (SDR)

What is a Software Designed Radio?

A Software Designed Radio is a radio that uses general purpose hardware and software to transmit and receive Radio

Typically this is done by using a USRP Universal Software Radio Peripheral

One more time

While you can receive AM transmissions with nothing more than a Crystal Diode and an antenna receiving more complex transmissions such as FM requires custom chips

An SDR does as much of this as possible in software so you have a true general purpose radio

Three last terms

USRP - Universal Software Radio Peripheral - SDRs made and sold by Ettus Research

UHD - USRP Hardware Driver - drivers to allow you to access the USRP

Some people write their own custom software using the UHD software

DVB-T - Digital Video Broadcast Terrestial - original purpose of the RTL2832 receivers

FM Radio Demo

Lets fire up a simple demonstration of GNU Radio to show how an FM Radio can work

Demo

Lets take a look at the parts from the Demo

Receiver - RTL2832 Dongle

Software - GNU Radio stack

Program - Basic FM receiver

Receiver - RTL2832 Dongle

Typically an SDR costs $250-$2,000

Several companies make them like Ettus and Funcube Dongle

Antti Palosaari - Discovered that some DVB-T receivers could be used as basic SDRs

There are limits for the receiver such as 8-bit, has certain sampling limitations but it is still pretty amazing

You can typically buy one of these receivers for $20.00!!!

Software GNU Radio

For this demo I've used a recent pull of the GNU Radio git repository on this system

Program - Simple FM Receiver

The Simple FM Receiver is based on a diagram put together by 2h20 in their tumblr blog

Lets open the radio up using the gnuradio-companion program and take a quick look

So we've seen a quick demo of GNU Radio

What else can you do?

Basic Radios AM/FM/Shortwave
RFID Hacking
GSM Snooping
Passive Radar
Satellite Reception
P25 decryption and analysis
Hacking Wireless PC Locks

Lets take a quick look at a couple of those

RFID Listening and Modification

http://tech.mit.edu/V128/N30/subway/Defcon_Presentation.pdf

Used a conventional USRP

P25 Listening

P25 is the digital radio communication standard used by most safety agencies Federal/Local/State for communication

http://www.youtube.com/watch?v=wShOLgW2tmI

balint256 has a lot of good examples of using the RTL2832 on youtube

Satellite Reception

A quick example from MegaOscarVideos

http://www.youtube.com/watch?v=zuyHpx1tnWI

Uses a simple dish to receive information from the Inmarsat network

GNU Radio

GNU Radio goes back to 2001

Licensed under GPL v3

Support a variety of Radios (Ettus Research, Funcube Dongle's and now the RTL2832)

How to install GNU Radio

There are several ways to build the GNU Radio Stack

Many of them are incredibly painful with a combination of magic/voodoo and animal sacrifice

OR you can use the build-gnuradio script from Shirleys Bay Radio Astronomy Consortium

Hint use the build-gnuradio script

There is also a windows version as well

How does GNU Radio work

3 Parts to our Simple Radio

1. rtl.grc - high level XML-description of program
2. rtl.grc is converted to python for execution
3. core components of GNU Radio are written in C++ for performance purposes

GNU Radio and VMs

There have been a couple of projects to create Virtual Machine with GNU Radio

USB performance under VMs is kind of limited so this hasn't worked out too well yet

A LiveUSB stick might also have issues as you might be competing for USB bandwidth

There is a project trying to put together a demo CD with some pre-canned feeds and a Knoppix remaster as a demo project

How to improve your GNU Radio Experience

Electrical Noise is the Killer to GNU Radio

GNU Radio on my Imac at home is much clearer than it is on my Laptop

Couple of things to consider

Pulling the USB power for your card from an adapter instead of the machine, even consider batteries for cleaner power

There are several howtos on where chokes can be put into the system

How to Improve your GNU Radio Experience (cont)

A faster computer will improve your experience especially if you are doing receiving and conversion at the same time

You can grab a stream to a file (which will be huge) and then process it. This can be used to do some simple replay attacks almost out of the box

Desktops tend to be quieter than Laptops just due to the additional space and the metal cases

Bit more about RTL2832 Dongles

Three major places to buy them

DealExtreme - http://www.dealextreme.com

Ebay - http://www.ebay.com

Aliexpress - http://www.aliexpress.com

I've bought a dongle from both DX and Ebay, have not used Aliexpress yet

Bit more about RTL2832

Not all DVB-T receivers use the RTL2832 chip the following is a quick guide to them

RTL-SDR compatibility guide - http://www.reddit.com/r/RTLSDR/comments/s6ddo/rtlsdr_compatibility_list_v2_work_in_progress/

Is it worth it?

Always wanted to play around with GNU Radio but the initial $1000.00 price tag was just too high

For $20.00 it has been quite a bit of fun and I am looking to figure out quite a bit more about GNU Radio

An Easier Path

GQRX - http://www.oz9aec.net/index.php/gnu-radio/gqrx-sdr

GQRX is a high level interface to GNU Radio written in Qt

The latest versions 2.1 and up support the RTL2832 interface

Lets fire it up and take a look

Couple of Other Projects

HDSR - High Definition Software Radio - http://www.hdsdr.de/

Windows only

Closed Source

Freeware

Interface is supposed to work well on netbooks

Other Projects (Continued)

Winrad - http://www.winrad.org/

Windows only

Open Source - only request you not use their name

Freeware

Not updated in two years

Looking for a new coder if you are good with Borland/Codegear/Embarcadero get in touch

Also need to use File based access

Links - 1 of 4

GnuRadio's site - http://www.gnuradio.org

Hack A Day - http://www.hackaday.com - lots of interesting stuff, has a radio section

RTL-SDR compatibility guide - http://www.reddit.com/r/RTLSDR/comments/s6ddo/rtlsdr_compatibility_list_v2_work_in_progress

Links (Continued) - 2 of 4

ARRL's site on SDR - http://www.arrl.org/software-defined-radio

Getting Started with RTL-SDR website (good info) http://www.thepowerbase.com/2012/06/getting-started-with-rtl-sdr/

Links - 3 of 4 (Continued)

Fun Stuff, Yea blog - http://2h2o.tumblr.com./ - basis for GNU Radio FM radio in the talk

GQRX - http://www.oz9aec.net/index.php/gnu-radio/gqrx-sdr

Links - 4 of 4 (Continued)

OZ9AEC's web site - http://wiki.oz9aec.net/index.php/Main_Page - home of GQRX and some other interesting projects such as the dvb transmitter

GNU Radio Tutorial Page (Balint's new Youtube channel) - http://www.youtube.com/playlist?list=PL618122BD66C8B3C4&feature=view_all