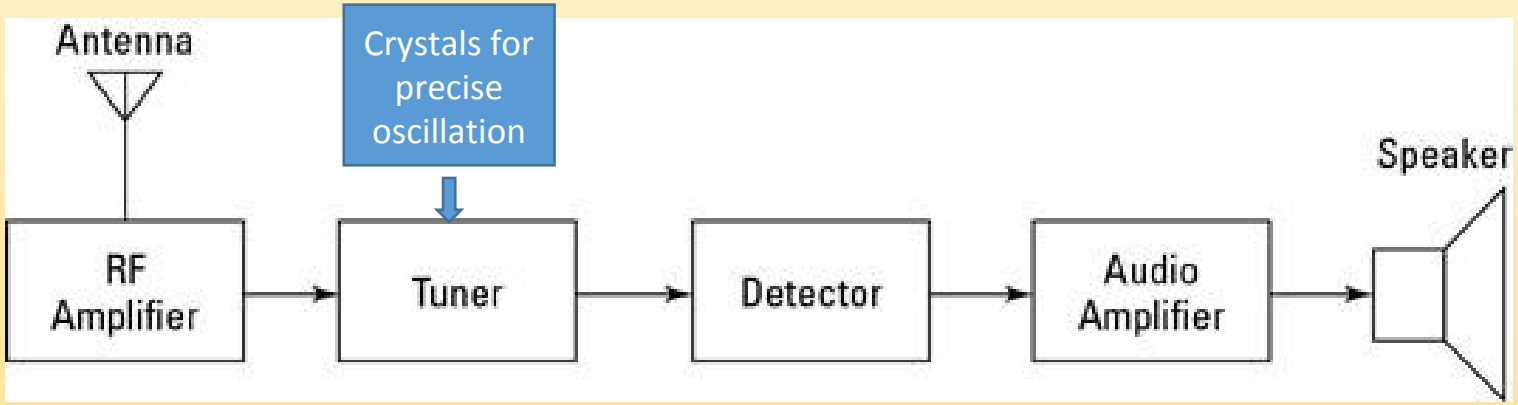
Software Defined Radio

Bruce Barnett
@grymoire

Traditional Radio Receiver



Amplifies Antenna Signal

Selects Frequency

Converts Waveform into information

Isolate and Process Information

User Interface

Everything is Analog

What if

- What if you can just digitize the entire spectrum, just like a .WAV file?
- Then once it's digitized, you use software to do
  - Select the frequency
  - Filter out extra noise
  - Amplify the signal
  - Convert the signal into digital (modulation)

Software-Defined Radio

History of SDR

- 1984 E-Systems – concept
- 1991 SPEAKeasy – DARPA Funded
- 1997 JTRS – created by DoD
- 2001 – GNU Radio software created
- 2004 FCC first approval of a commercial SDR
- 2009 First commercial single-chip RF front-end
- 2010 Ettus offers hardware for GNU Radio

Commercial SDR's

- Ettus - $600-$5000
- In 2013 – Someone discovered the $40 REALTEK TV Dongle w/RTL2832U could be used as a SDR.
- Extreme Frenzy
- List of available SDR's https://en.wikipedia.org/wiki/List_of_software-defined_radios

Low cost SDR's

- EZCap USB 2.0 DVB-T/DAB/FM Dongle
  - RTL2832U A/D Convertor and USB data pump
  - Tuner Chip

Chip	Frequency
E4000	52Mhz-2200Mhz
FC0012	50Mhz-1100Mhz
FC0013	50Mhz-1700Mhz
R820T	24Mhz-1800Mhz
R828D	24Mhz-1800Mhz
R820T2	24Mhz-1800Mhz

Sources

- Amazon
- www.rtl-sdr.com
- www.nooelec.com

Things to Consider besides tuner

- Shielding
- Temperature Compensated Oscillator (TCXO)
- Antenna connector
- Antenna

SDR Antenna Connectors

Type	Male	Female	Specs Used
BNC			RTL-SDR RF Coax Video
MCX			RTL-SDR Fragile
SMA			Hackrf Yardstick One RTL-SDR
RP SMA			WiFi Routers, Ubertooth, UD100, CrazyRadio PA, Reverse Polarity
uFL			LimeSDR SMT 30 uses only!

Recommended SDR

http://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles/

- RTL2832U/R820T2
- SMA connector
- TXCO
- Metal case w/passive cooling
- $25

RTL-SDR Blog V3 R820T2 RTL2832U 1PPM TCXO SMA Software Defined Radio with 2x Telescopic Antennas

Commercial/hacker SDR's

Device	Freq	Cost	Resolution	Trans/Receive
Rtl-sdr	22Mhz-2.2Ghz	$20-$40	8	R
hackrf	10 MHz to 6 GHz	$300	8	T/R (half duplex)
bladerf	300 MHz – 3.8 GHz	$420	12	T/R (Full Duplex)
sdrplay	10-khz-2Ghz	$129	12	R
sdrplay2	1kHz-2GHZ	$169	12	R
airspy	24 MHz – 1.750 GHz	$199	12	R
MyriadRF	300 MHz – 3.8 GHz	$299	12	T/R (Full Duplex)
limeSDR	100 kHz to 3.8 GHz	$299	12	T/R(Full Duplex)

SDR Stores

Receivers

- http://www.rtl-sdr.com
- http://www.nooelec.com
- http://www.amazon.com

Antennas

- The above stores plus
- http://www.wa5vjb.com/ - Low cost PCB antennas
  - Best antennas are tuned for certain frequencies

Installation of software

- Use your package manager # Kali - install kali-linux-sdr
- `[sudo] pip install PyBOMBS`
- `gnu-buildradio script`
- From source # Ubuntu - yes, Kali - no
  - `apt-get install python-apt libfreetype6-dev ocl-icd-opencl-dev thrift-compiler python-opengl`
  - `git clone https://github.com/gnuradio/pybombs.git`
  - `cd pybombs`
  - `python setup.py build`
  - `sudo python setup.py install`
  - `pybombs recipes add gr-recipes git+https://github.com/gnuradio/gr-recipes.git`
  - `pybombs recipes add gr-etcetera git+https://github.com/gnuradio/gr-etcetera.git`
  - `pybombs prefix init ~/SDR [-a myprefix] -R gnuradio-default`
  - `source ~/SDR/setup_env.sh`
  - `pybombs -p <alias> install <package1>`
  - `pybombs update`

Quick demo of some SDR tools

FM Radio

- FREQ=103.9
- rtl_fm -f ${FREQ}e6 -M wbfm -s 200000 -r 48000 - | aplay -r 48k -f S16_LE

dump1090 Flight tracker

- `git clone https://github.com/antirez/dump1090.git; make`
- `./dump1090 --enable-agc --aggressive --net --net-http-port 8080`
- `Then go to http://127.0.0.1:8080/`

Spectrum Analyzer (Waterfall table)

- gqrx

GNU Radio Companion

- we'll get there in a bit……

What can you received with a SDR?

- Receive nearly anything
  - AM/FM/HAM radio
  - ADB-S – Real-time Flight Tracking
  - ACARS – Communication between airplanes & Ground
  - Police/Fire/Emergency bands
  - Industrial Bands
  - APT images from NOAA weather satellites
  - TETRA - Terrestrial Trunked Radio
  - Smart Meters
  - TPMS – Tire Pressure Monitor System
  - AMSAT – Meteors
  - Mars
  - Iridium Satellites
  - D-STAR – Digital Voice/Amateur Radio
  - GSM/Cell phone (**this is illegal**)
  - … and anything wireless

- http://www.grymoire.com/Security/Hardware.html

The Industrial, Scientific and Medical (ISM) Bands

Industrial, Scientific, and Medical Bands

The following table came from **Wikipedia:**

Frequency range		Bandwidth	Center frequency	Availability
6.765 MHz	6.795 MHz	30 kHz	6.780 MHz	Subject to local acceptance
13.553 MHz	13.567 MHz	14 kHz	13.560 MHz	Worldwide
26.957 MHz	27.283 MHz	326 kHz	27.120 MHz	Worldwide
40.660 MHz	40.700 MHz	40 kHz	40.680 MHz	Worldwide
433.050 MHz	434.790 MHz	1.74 MHz	433.920 MHz	**Region 1** - Europe, Africa, parts of the Middle East, Russia, etc.
902.000 MHz	928.000 MHz	26 MHz	915.000 MHz	**Region 2** - North and South America
2.400 GHz	2.500 GHz	100 MHz	2.450 GHz	Worldwide
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz	Worldwide
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz	Worldwide
61.000 GHz	61.500 GHz	500 MHz	61.250 GHz	Subject to local acceptance
122.000 GHz	123.000 GHz	1 GHz	122.500 GHz	Subject to local acceptance
244.000 GHz	246.000 GHz	2 GHz	245.000 GHz	Subject to local acceptance

If you are exploring the RF spectrum, a very useful reference that can identify licenced ISM frequencies in your area (i.e. Zip Code) is **Radio Reference** - which lists the "owners" of certain frequencies based on your location/ZIP code.

Step 1: Audio Voyerism

Step 1: Look up local frequencies

- Frequencies by zip code, city, state, etc http://www.radioreference.com/apps/db/

Step 2: Select zip code 12207

Step 3: listen

- Use gqrx

Step 4: Bookmark interesting frequencies

Yo, hackers……

Examples of SDR Hacking

- Remote Keyless Entry (Car, garage, etc.)
- Garage Door openers
- Wireless Keyboards
- Wireless alarm systems
- RFID
- RC-controlled devices/drones
- IoT/Zigbee/802.15.4
- Pagers

Suggested 4-step methodology for hacking

1. Use OSINT to learn as much about the target first
2. Use gnuradio-companion, etc to learn how to decode data
3. Use dedicated radio hardware to generate attacks
4. Profit

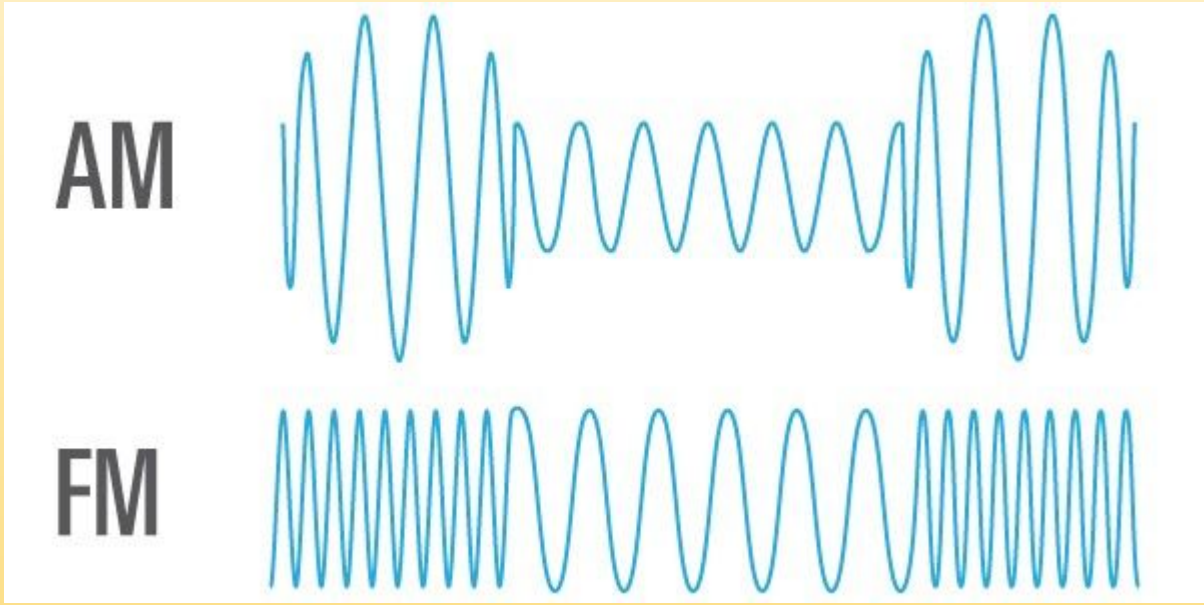
OSINT info gathering

- Become familiar with public/ISM frequencies
  - http://www.grymoire.com/Security/Hardware.html
- Get FCC ID from device and get info from FCC
  - https://fccid.io/ #example nhv-WB1U711
  - https://www.fcc.gov/oet/ea/fccid
- Manufacturer's documents
- Physical device info, parts, data sheets

Using SDR gnu-radio companion

- Hook it up to your SDR
- Can select specific frequency, modulation, etc.
- Decode the data
- Graph the data
- Generate audio, data, file, etc.
- A demo, but first……

Modulation and complex numbers



Modulation and complex numbers

GNURadio Companion

Drag + Drop objects

Connect them together

Match Variables types

Make sure everything is connected

run

Hack the Airwaves

Steps (Marc Newlin/Matt Knight)

- https://conference.hitb.org/hitbsecconf2017ams/materials/D1T4%20-%20Marc%20Newlin%20and%20Matt%20Knight%20-%20So%20You%20Want%20to%20Hack%20Radios.pdf
- Characterize the channel (center frequency, width, etc.)
- Identify the modulation (On/Off Keying [OOK], PWM, etc.)
- Determine the symbol rate
- Synchronize

Signal Identification Wiki

http://www.sigidwiki.com/wiki/Signal_Identification_Guide

Artemis

- http://markslab.tk/project-artemis/ (Windows)

HDSDR Autocorrelation Mode (Windows, Linux w/wine)

- http://www.hdsdr.de/
- https://sites.google.com/site/g4zfqradio/hdsdr-autocorrelation

Use dedicated hardware to attack

- IM-ME
- Sub 1Ghz USB Dongles
  - Don’s Dongle (TI CC1111 EMK) w/rfcat (Python)
  - Yardstick one (400Mhz-915Mhz) w/rfcat
- 2GhZ USB Dongles
  - Atmel's AVR RZUSBSTICK
  - CrazyRadio PA/Logitech Unified Receiver
  - Ubertooth (Bluetooth)
  - Senwio Sniffer (780/868/915/2400 MHz)
- Transceivers
  - RFM69HCW (315,433,868 and 915MHz)
  - RFM95W (868-915Mhz)
  - nRF24L01+ (2.4Ghz)

rfcat and Yardstick one

https://leonjza.github.io/blog/2016/10/02/reverse-engineering-static-key-remotes-with-gnuradio-and-rfcat/

http://andrewmohawk.com/2015/08/31/hacking-fixed-key-remotes-with-only-rfcat/

Not all dongles are the same

Some do not allow “raw” or non-standard packets

Dongle	Type	Software	Library
ubertooth	Bluetooth	blue-hydra	bluez
yardstickone	281-361 MHz, 378-481 MHz, and 749-962 MHz	rfcat Metasploit Hardware Bridge	
SENA UD100	Bluetooth	blue-hydra	bluez
CrazyRadio PA Logitech Unifying Receiver	2.4Ghz (Long Range)	mousejack, jackit	http://tmrh20.github.io/RF24/
nRF24L01	2.4Ghz		http://maniacbug.github.com/RF24 https://github.com/BastilleResearch/nrf-research-firmware.git

Metasploit's Hardware bridge + Yardstick One

Garage door brute-force cracker

1. Start the yardstick bridge

   cd ~/Hq/rfcat
   ./rfcat_msfrelay

2. start metasploit

   msfconsole -q
   use auxiliary/client/hwbridge/connect
   set httpusername msf_relay
   set httppassword rfcat_relaypass
   run

   sessions

   sessions 1
   run post/hardware/rftransceiver/rfpwnon FREQ=915000000 BINLEGTH=6 REPEAT=2

Basic References

- https://wiki.gnuradio.org/ - Wiki
- https://github.com/dimitriblock/gr-cheatsheet Cheat Sheet
- https://github.com/cn0xroot/RFSec-ToolKit Very large list of RF tools/talks
- http://www.rtl-sdr.com/youtube-talk-hunting-rogue-wifi-devices-using-hackrf-sdr/
- https://wiki.gnuradio.org/index.php/Guided_Tutorial_GRC official tutorial
- **http://greatscottgadgets.com/sdr/** Video Training

Training/Tutorials

- http://hackaday.com/2015/11/11/getting-started-with-gnu-radio/
- https://www.youtube.com/watch?v=qDb9-EhbNno - How To Set Up an SDR Radio
- https://www.youtube.com/watch?v=OFRwqpH9zAQ - TR17 NGI TRACK1 So You Want To Hack Radios Matt Knight, Marc Newlin
- Google search “balint seeber gnuradio site:youtube.com”
  - https://www.youtube.com/watch?v=drsgh_PZmJ8 DEF CON 23 - Wireless Village - SIGINT & Blind Signal Analysis w/ GNU Radio & SDR
  - https://www.youtube.com/watch?v=N0p3_ES2dBU Hacking the Wireless World with Software Defined Radio - 2.0

More bookmarks……

https://www.youtube.com/watch?v=OFRwqpH9zAQ - TR17 NGI TRACK1 So You Want To Hack Radios Matt Knight, Marc Newlin

Google search “balint seeber gnuradio site:youtube.com”

https://github.com/leonjza/ooktools On-off keying tools for your SD-arrrR

https://leonjza.github.io/blog/2016/10/02/reverse-engineering-static-key-remotes-with-gnuradio-and-rfcat/

https://github.com/comaeio/OPCDE/blob/master/hack%20wireless%20scada.pdf Using SDR for SCADA

http://www.mwrf.com/systems/summarizing-advances-sdr-technology info on next gen SDR

http://www.rtl-sdr.com/youtube-talk-hunting-rogue-wifi-devices-using-hackrf-sdr/

Install instructions http://www.fieldxp.com/install/

https://github.com/cn0xroot/RFSec-ToolKit list of tools

http://greatscottgadgets.com/sdr/

http://hackaday.com/2015/11/11/getting-started-with-gnu-radio/

http://blog.atx.name/reverse-engineering-radio-weather-station/

https://z4ziggy.wordpress.com/2015/05/17/sniffing-gsm-traffic-with-hackrf/

https://bytebucket.org/rootbsd/433mhz-ask-signal-analysis/raw/5f4937e4efb2198abcc375b8aefee41421941fca/pdf/433MHz_ASK_sginal_analysis-Wireless_door_bell_adventure-1.0.pdf - 433MHz ASK signal analysis doorbell w/hackrf

Compares different devices https://www.crowdsupply.com/lime-micro/limesdr

http://www.rtl-sdr.com/a-tutorial-on-using-rtl-sdr-with-labview-creating-a-simple-fm-demodulator

https://github.com/znuh/re-DECTed DECT

https://www.sv1afn.com/projects.html - various projects RF detector, etc.

Came across this cool tool to create timing diagrams from json code: http://wavedrom.com/

http://andrewmohawk.com/2015/08/31/hacking-fixed-key-remotes-with-only-rfcat/ RFCAT

http://fatsquirrel.org/oldfartsalmanac/random/reverse-engineering-a-vintage-wireless-keypad-with-an-rtl-sdr/

http://v3gard.com/tag/rfcat/

GSM.GPRS

https://www.insinuator.net/2016/07/notes-on-hijacking-gsmgprs-connections/

Rfcat

Anycon HHV
Twitter: @anyconhhv
Facebook Group: Albany Hardware Hackers

What speedtalk topics are you interested in?

- RFID (RFidler, Chameleon-Mini)
- Side channel attacks (Chip Whisperer-Lite)
- 2.4Ghz (blue-hydra, Mousejack)
- General (Bus Pirate)
- Logic Analyzers (Saleae, OpenScope)
- JTAG programmers and debuggers (GoodFET, JTagulator, Shikra, BlackMagic Probe)
- Oscilloscopes (DSO Quad, OpenScope)
- General (Beer)

Thanks

Twitter: @grymoire