Security Applications of Software Defined Radio

Joe Jesson (KC2VGL)
John DeGood (NU3E)
Rebecca Mercuri (KA3IAX)

Princeton ACM / IEEE Computer Society
February 18, 2016 Princeton, NJ

Outline of Tonight's Meeting

- Joe Jesson – Overview of RF Monitoring;
  + How SDR Tuners Work
- John DeGood – Aircraft Monitoring Applications
- Rebecca Mercuri – Getting Started with SDR
  + Resources

20 minutes for each talk (strictly enforced!)

5 minutes Q&A after each talk

Open Q&A and discussion at end

Legalities

- Currently, listening on SDR is legal
- Certain types of listening may not be legal
- Recording may or may not be legal
- The SDR dongle is receive-only
- Broadcasting is not legal without a license

- Radio licenses for the Amateur (Ham) Bands are available from the FCC:
  - Ham Cram and Exam at TCF ($15 to test)
  - Local Ham Clubs have training and can help you
  - David Sarnoff Radio Club meets 3rd Tues Sept-June at the Princeton Red Cross http://n2re.org

Where to Purchase SDR Gear?

- Our SDR dongles (with antenna) are ordered from http://adafruit.com They also sell adapter cables.
- Various SDR vendors are online and on Amazon.
- Prices range from $7 to $300+
- BEWARE! Some vendors are unscrupulous!
- Check out vendors and manufacturers at http://www.eham.net/reviews/
- Adapter cables convert from MCX to other connectors to allow experimentation with random wire and other antennas.

See:
http://www.hamuniverse.com/randomwireantennalengths.html

How to Get Started

- The remote control and mini-CD that comes with the Adafruit SDR are useless here.
- Connect your SDR dongle to a USB port on your computer and extend the cable to the antenna.
- Setting the small antenna on a pie plate may improve reception.
- Download the Quick Start Guide document from http://www.rtl-sdr.com/rtl-sdr-quick-start-guide/
- Basically you will download a zip file, uncompact the file, run zadig.exe to swap the SDR driver, and then you can run SDRSharp.exe.

Additional Documentation

- Adafruit.com, provides a (free!) 19-page manual that will take you step-by-step through the software setup and gives tips on how to use many of the SDR# software features.
- Be sure to perform the driver installation WITH the dongle inserted (you only need to do this once per computer). The manual can be downloaded at:

  https://learn.adafruit.com/downloads/pdf/getting-started-with-rtl-sdr-and-sdr-sharp.pdf

Operating Systems

- SDR# runs on other operating systems, but the instructions here are for Windows.
- Experiment on your own if you have Mac or Linux.
- SDR# can run from a Linux boot USB (see Joe for more info on how to do this).
- Raspberry Pi versions are also available!
- http://rtl-sdr.com has a wealth of info and links for SDR, constantly being updated with more.
  See their BIG list of SDR software at:

http://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/

More Things To Do With SDR

- Reverse engineering hacks for wireless doorbells, weather stations, and even door openers: http://www.rtl-sdr.com/tag/reverse-engineering/
- Facebook page that has application ideas for SDR: https://www.facebook.com/rtlsdrblog
- More user-friendly FM radio tuner (though I still like picking out the stations via the visual spectrum): https://github.com/GeoNomad/radioreceiver
- This one shows the audio spectrum in 3D (instead of 2D): https://github.com/ttrftech/threejs-spectrum
- GQRX is another variation of SDR software. Their presentation pdf gives some of the math behind this technology. See: http://gqrx.dk/

Enjoy!

Let us know what you are doing with SDR Radio:

<mercuri@acm.org>