A $49 Aerospace Cybersecurity Lab: RF Data Communications for Undergraduate Cybersecurity Education

Richard Hansen
Capitol Technology University, USA
rhhansen@captechu.edu

Zachary Klein
University of Maryland, USA
zklein@umd.edu

***Abstract* – Radio Frequency (RF) communications are essential for aircraft and satellite operation. The current generation of Software Defined Radios (SDRs) has increased the capabilities of equipment at a cost that brings this technology in reach for economically disadvantaged institutions and students. Labs are designed to provide immediate feedback to accelerate experimentation and learning. The novelty and technology associated with aerospace platforms can stimulate students' interest and motivation. These lessons can be applied to other attack surfaces such as automotive and 5G communications.**

Keywords
Radio Frequency, RF, Software Defined Radio, SDR, aviation, satellite, aerospace, data communications, cybersecurity, ADS-B, ACARS

1. Introduction

Radio frequency (RF) communications can be an attack surface for safety- and mission-critical systems and utilities [1] [2]. Cybersecurity programs often present RF communications through discussions of Wifi and cellular phone networks without providing instruction in RF fundamentals [3]. Undergraduate RF engineering courses are an alternative. They typically require a full semester and require advanced coursework in engineering mathematics which are not a part of many cybersecurity programs. [4] This paper proposes the use of software-defined radios (SDRs) to teach RF fundamentals through reception and exploitation of aerospace data communications. The aviation community has recognized the need for cybersecurity services [5] as has the United States Department of Defense (DoD) satellite community [6].

Figure 1: Software Defined Radio - USB "Dongle" form factor

Software Defined Radios (SDRs) provide an inexpensive and straightforward method of providing RF education to aspiring Cyber professionals. A USB "dongle" radio costing $25 can be used with a desktop or laptop computer to receive aircraft data feeds and weather images from weather satellites. Aircraft and weather satellites can be received regularly from almost any location in the United States. The computing requirements are low, allowing economically disadvantaged institutions to provide an effective education with a very modest investment. SDRs provide a graphical representation of the frequency spectrum which is useful for learning and experimentation.

SDRs digitally sample the amplitude of the energy in a range of frequencies millions of times each second. The output is a series of scalar measurements which are processed on the computer. Algorithms in software are used to display graphical representations of signals and for demodulation of voice and data communications. Inexpensive SDRs were originally developed to receive digital television (DTV) on laptops and PCs. Experimentation showed that they could be tuned to other frequencies and software could be used to demodulate many different kinds of signals. There are many software packages for Windows, MacOS and Linux available [7].

The graphical representation of signals is important. As shown in *Figure 2* below, students can observe a dynamic picture showing frequency and amplitude information for all signals in the selected range.

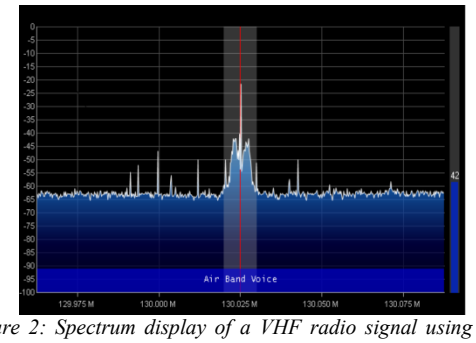

Figure 2: Spectrum display of a VHF radio signal using SDR# (SDR Sharp) software for Windows and a USB "dongle" SDR

The goal for exercises using SDRs is to develop competency at the first, second, and third levels (Remembering, Understanding, and Applying) of the Revised Bloom's [8]. Hands-on labs can teach students to classify RF signals by their characteristics, progressively realizing the goal of competency at Bloom's Level 3 (Application).

Jerome Bruner's Theory of Discovery proposes that students use their own past experiences and knowledge to discover new facts and relationships. As stated by McLeod [9], "Bruner proposes that learners' construct their own knowledge and do this by organizing and categorizing information using a coding system. Bruner believed that the most effective way to develop a coding system is to discover it rather than being told it by the teacher." The labs are designed to support and encourage experimentation with rapid feedback that progressively builds new knowledge.

Students can classify the components of their observations based on characteristics of signals such as frequency, bandwidth, modulation, and output. The sensory aspects, such as seeing real-time changes in frequency and amplitude and listening to the resulting output, help students rapidly discover the properties of different signal types and receiver settings.

On a wide scale the students can see separations between signals and relate this to existing knowledge of TV channels and FM station frequencies. Close-up views show changes in signals as they are modulated with information. This provides a method of learning RF fundamentals that is not based on mathematics. Some SDR software, such as GNU Radio [10], provide the ability to process different signal types by linking together code that can be represented as blocks on a diagram. Students can create new designs in a matter of minutes using software. This hands-on experimentation provides for rapid experimentation with immediate feedback on their actions.

RF can be further classified as a type of electromagnetic radiation (EM) that uses space itself as the medium for transmission, as does light. Other classifications for EM include electrical signals passing through an ethernet cable with metallic conductors, reflected light or radio signals carrying information about an object (size, distance) through space, and light carrying data signals in a fiber optic cable. When EM is used for communications its characteristics are classified as OSI Layer 1 properties, serving as a starting point for discussions of the OSI Model.

2. EXERCISE DESIGN

Receiving these signals is free of any requirements for licensing or registration. The activities below are legal anywhere in the United States and in many other countries. As mentioned above a key goal is development of competency up to Bloom's Level 4 through hands on experimental activities.

2.1 FM Broadcast Radio

FM broadcast radio is an example of analog communications and provides a good introduction to basic principles. The visual display of a range of frequencies shows how FM stations are grouped together in the same frequency space, a band, and they are separated by enough distance so their signals do not interfere, the separation is greater than the bandwidth.

The SDR# (pronounced SDR Sharp) [11] software can be used to display signals in the FM band and listen to the demodulated output. *Figure 3* below shows an example of the display. The X-axis shows the frequency of signals and the Y-axis shows relative strength on a logarithmic scale. The "waterfall" display at the bottom shows the strength of signals over time.

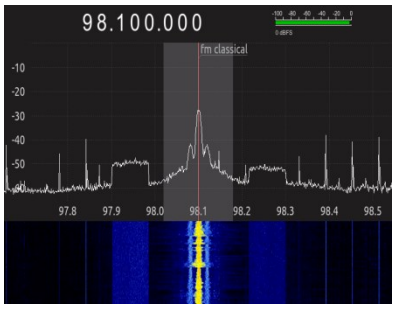

Figure 3: Spectrum display of an FM radio signal and adjacent signals using SDR# software and an RTL SDR Radio

Modest guidance can assist with developing classifications using this display. The term "band" refers to sets of adjacent frequencies that have common characteristics or share a common use. When receiving a signal in the FM broadcast band students can be encouraged to tune lower and higher in frequency until they could no longer find stations. They can also "zoom out" to larger amounts of spectrum to make the search easier. The term "band" and their own observations will help students create a new method of classifying information.

Bandwidth is another key characteristic of RF communications. It is generally related to quantity of information passing in a unit length of time (bits-per-second or a range of audio frequencies). The real-time display can be "zoomed in" to provide a very granular measurement of the upper and lower limits of spectrum used by the signal. Students may find the waterfall display is even more useful for this task.

Bandwidth is used to help define a channel. A channel has a center frequency as well as upper and lower frequency limits. Students can be told that in the US stations have 0.2 MHz/200 KHz channels. They can be asked to estimate the extra space left between channels and speculate on other features of the channel system.

2.2 Digital Aircraft Data

ACARS refers to the Aircraft Communications, Addressing and Reporting System [12]. It uses an analog voice channel to carry digital information. In the United States it can be received on a frequency of 130.45 & 131.5 MHz as shown in the left half of *Figure 4* below.

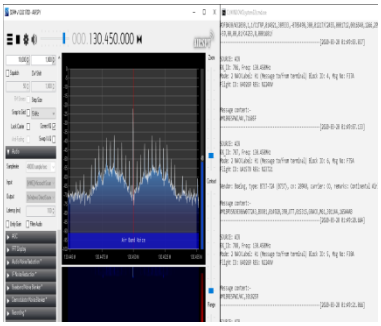

Figure 4: Spectrum display of ACARS signal and several decoded messages from a separate window

This image shows the use of SDR# software to receive the signal with AcarSDeco2 software [13] to demodulate the signal and provide the digital output. Students can hear "bursts" of digital information from SDR# and see the corresponding data output in another window.

The OSI model is applicable to both windows. SDR# is showing the characteristics of the OSI Layer 1 analog signal. The ACarsDeco2 window shows Layer 2&3 information (source address, sequence number, and contents of the message).

Students can be encouraged to tune away from the center frequency and see the effect on the signals. Other settings such as bandwidth and modulation can be changed and the effects observed.

After a period of experimentation, a Socratic dialogue can be held to ensure students are meeting the learning objectives of competency at Bloom's Level 3. They should compare and contrast their observations on these first two types of signals. Questions to stimulate discussions may include:

- Why are frequencies on one axis and power/strength on the other?
- How could color or other techniques be helpful in displaying the strength or other characteristics of a signal?
- What new insights do I have from the watching movement on the spectrum display and corresponding digital output?

A rule that proved effective was the "and" rule. After a student voices an observation, other students must precede their comments with the word "and." This creates a supportive feedback loop and encourages students to use their observations to build upon those of others.

The last activity is a "Point of View" exercise. It can be useful for students to view themselves as attackers (Red Team) and Defenders (Blue Team). Students can be challenged to modify network attack scenarios to the RF domain, such as Denial of Service (DoS) and spoofing. They can be challenged to suggest modifications to protocols that would provide resilience against these attacks.

2.3 Aircraft Location Information

Many aircraft are required to broadcast their location using the Automated Dependent Surveillance-Broadcast (ADS-B) technology on a frequency of 1090 MHz. ADS-B systems broadcast GPS-enhanced location and identification data to help air traffic controllers manage traffic. SDR# for Windows can be used with other packages to display location and identification information as shown in *Figure 5* below. On Linux, the Dump1090 [14] software can be used to receive and display information in textual format.

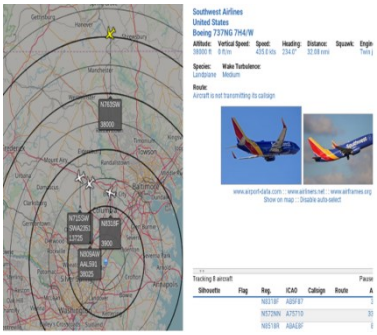

Figure 5: ADS-B display and aircraft information lookup

Figure 5 above shows the output from the Virtual Radar Server for Windows [15] software which displays aircraft identification, location and altitude information. Observation of the display can reveal from which directions and at what altitudes traffic can be received. *Figure 5* shows the coverage with an antenna placed in a north-facing window.

ADS-B is an excellent subject for a Red Team-Blue Team discussion. This service is critical for managing traffic and for collision avoidance. Spoofing and denial-of-service attacks could have severe consequences. An examination of the protocol in terms of the CIA triad will show students its lack of provisions for security. It also shows the need for cybersecurity professionals to be involved in designing these systems.

2.4 Satellite Data

The United States and other countries have a placed weather satellites in polar orbits approximately 500 miles above the earth. They take and transmit images showing cloud cover and other details using a format calls APT (Automatic Picture Transmission). The Heavens Above website [17] provides information for predicting satellite passes with detailed information. This is a challenging undertaking and may be impractical given the time constraints for undergraduate education.

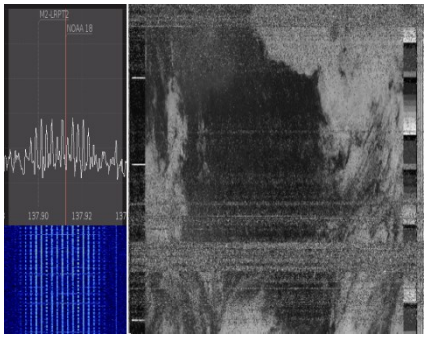

Figure 6: NOAA weather satellite signal and a decoded image

If *Figure 6* above, signals are displayed by using the GQRX [17] software for Linux to receive the signal and record the demodulated output to an audio file. The audio is then decoded with the NOAA-APT software [18]. Windows software such as SDR# can also be used with the Windows version of NOAA-APT.

The reception of satellite signals is much more challenging than the previous exercises. An unobstructed view of the sky is needed and the antenna and receiver should be outdoors. Signals can only be received from the time the satellite rises over the horizon (Acquisition of Signal or AOS) to when it

goes below the horizon (Loss of Signal or LOS). The Heavens Above website is one source for these details.

The challenges presented by satellite signals acts as a Capstone exercise. It provides opportunities to apply learning from the other exercises and to observe new phenomena such as doppler shift.

3. CONCLUSIONS & APPLICATION TO OTHER AREAS

The ability to see a representation of the RF spectrum in real-time is a powerful tool for teaching. Students receive immediate feedback on their actions and can quickly switch between macro and micro scales to examine frequencies and modulation. Students claimed that the ease of experimenting with SDRs made the exercises fun and interesting.

The SDRs can be used to view other unseen and unintentional communications. Electromagnet interference (EMI) is produced by digital circuitry in computer systems. It can interfere with the reception of radio signals and can also provide a means of covertly extracting information. Students can demonstrate this for themselves. An antenna can be created by wrapping one or more loops of wire around a laptop or desktop computer and connecting it to the SDR's antenna input. Students should then select AM modulation and reboot or power on the computer. By tuning through frequencies at the bottom of the SDR's range students will hear many different sounds as the system proceeds through the boot process. These signals have been exploited to extract encryption keys from a PC in under a minute [19].

RF-based telecommunications are used in many parts of our daily lives. Key fobs for automobiles and garage door openers often operate in the 315 MHz range. Inexpensive SDRs can be used to capture and investigate data transmissions used by these devices.

For a larger investment SDRs such as the HACKRF ONE, available on Amazon and Ebay, can both receive and transmit at frequencies up to 5 GHz. The RF output is low enough for legal use in the unlicensed spectrum used by these devices. In a shielded environment it can be used for more complex experiments with technologies such as GPS and cellular systems to include 5G.

4. EQUIPMENT LIST

These exercises are designed to be independent of the specific type of SDR used. A minimal set of equipment can be purchased for approximately $49. Included is a "BNC" cable adapter which provides a standard interface for use with experimental and ready-made antennas for specific purposes.

Software-Defined Radio, RTL-SDR R820T2, $24.99, Amazon
Purpose: Receives signals for display and demodulation on PC

RTL-SDR Dipole Antenna kit, $14.95, Amazon
Purpose: Captures electromagnetic energy for the receiver

BNC Female Adapter to MCX Male Connector, $8.99, Amazon
Allows us for use of home-made and commercial antennas.

5. ACKNOWLEDGEMENTS

The Maryland Space Grant Consortium (MDSGC) provided funding for a Computer Engineering student, Mr. Zachary Klein, to assist with research on use of Software Defined Radios and other technology for communications with High Altitude Balloons at the edge of space. The MDSGC has agreed to publication of information in this paper. Mr. Klein worked diligently and creatively to develop configurations and provide data. He assisted with input on the exercises and with creating graphics for this paper. Capitol Technology University was kind enough to allow the use of its campus and facilities for this research. Dr. Win Wenger provided valuable guidance on the works of Drs. Piaget and Burner and applying their methods. Drs. William Butler and Sandy Antunes provided much helpful input and encouragement.

REFERENCES

[1] Cyber Vulnerabilities & Mitigations in the Radio Frequency Domain. (n.d.). Retrieved April 3, 2020, from https://www.sbir.gov/node/1208173

[2] Sun, C.-C.; Liu, C.-C.; Xie, J. Cyber-Physical System Security of a Power Grid: State-of-the-Art. *Electronics* 2016, *5*, 40.

[3] Newhouse, W., Keith, S., & Scribner, B. (2017, August). National Initiative for Cybersecurity Education NIST 800-181, KSA K0274

[4] ENEE407: Design & Testing of RF and Microwave Devices. (n.d.). Retrieved March 20, 2020, from https://ece.umd.edu/course-schedule/course/ENEE407

[5] International Civil Aviation Organization, Addressing Cybersecurity in Civil Aviation, (n.d.). Retrieved March 20, 2020, from https://icao.int/cybersecurity/Documents/A40-10.pdf

[6] Barrett, B. (19AD, September 17). The Air Force Will Let Hackers Try to Hijack an Orbiting Satellite. Retrieved from https://www.wired.com/story/air-force-defcon-satellite-hacking/

[7] The BIG List of RTL-SDR Supported Software. Retrieved March 21, 2020, from https://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/

[8] Mcdaniel, R. (2020, March 25). Bloom's Taxonomy. Retrieved from https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

[9] Mcleod, S. (2019). Bruner - Learning Theory in Education. Retrieved from https://www.simplypsychology.org/bruner.html

[10] The Free & Open Source Radio Ecosystem · GNU Radio. (n.d.). Retrieved March 25, 2020, from http://www.gnuradio.org/

[11] SDR# and Airspy Downloads. (n.d.). Retrieved April 5, 2020, from https://airspy.com/download/

[12] SKYbrary Wiki. (n.d.). Retrieved April 5, 2020, from https://www.skybrary.aero/index.php/Aircraft_Communications,_Addressing_and_Reporting_System

[13] Sergsero. (2018, December 8). AcarSDeco2. Retrieved April 5, 2020, from http://xdeco.org/?page_id=42

[14] ADS-B using dump1090 for the Raspberry Pi. (n.d.). Retrieved April 6, 2020, from https://www.satsignal.eu/raspberry-pi/dump1090.html

[15] Virtual Radar Server. (n.d.). Retrieved April 6, 2020, from http://www.virtualradarserver.co.uk/

[16] Heavens Above. (n.d.). Retrieved April 7, 2020, from https://www.heavens-above.com/

[17] GQRX (n.d.) Retrieved April 6, 2020, from https://gqrx.dk/download

[18] NOAA-APT (n.d.). Retrieved April 6, 2020, from https://noaa-apt.mbernardi.com.ar/download.html

[19] Thomson, I. (2017, June 24). AES-256 keys sniffed in seconds using €200 of kit a few inches away. Retrieved from https://www.theregister.co.uk/2017/06/23/aes_256_cracked_50_seconds_200_kit/