INSTITUTE FOR DEFENSE ANALYSES

DATAWorks 2022: Adversaries and Airwaves: Hands-on Demonstrations with a Software Defined Radio

Peter M. Mancini, Project Leader

Mark R. Herrera
Jason R. Schlup
Stacey L. Allison
Kelly Tran

April 2022

Public release approved. Distribution is unlimited.

IDA Document NS D-33011

Log: H 2022-000094

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

About This Publication
This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-19-D-0001, Task C9096, "Cyber Experimentation and Training Lab," for the Office of the Director, Operational Test and Evaluation. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments
The IDA Technical Review Committee was chaired by Mr. Robert R. Soule and consisted of Shawn C. Whetstone, Brian T. Conway, and Chad A. Brisbois from the Operational Evaluation Division.

For more information:
Peter M. Mancini, Project Leader
pmancini@ida.org • (703) 845-2496

Robert R. Soule, Director, Operational Evaluation Division
rsoule@ida.org • (703) 845-2482

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-33011

DATAWorks 2022: Adversaries and Airwaves: Hands-on Demonstrations with a Software Defined Radio

Peter M. Mancini, Project Leader

Mark R. Herrera
Jason R. Schlup
Stacey L. Allison
Kelly Tran

Executive Summary

This poster serves as a supplement to the Operational Evaluation Division (OED) Cyber Lab breakout session "Adversaries and Airwaves: An Introduction to Wi-Fi / Radio Frequency Hacking." Both that presentation and this poster will be presented at the DATAWorks 2022 conference.

A software defined radio (SDR) is a radio system where components traditionally implemented with dedicated or analog hardware instead are implemented in software. This allows these devices to have incredible flexibility in the types of signals, protocols, and applications a single piece of hardware can support.

This poster presents several hands-on demonstrations using SDRs that DATAWorks attendees can experiment with as they chat with members of the OED Cyber Lab. The goal is to allow attendees to experiment with hardware and software they may not be familiar with, and to demonstrate the wide breadth of applications these ubiquitous, affordable devices can support.

A. Exploring the electromagnetic environment

Using an SDR receiver program,[1] we can investigate what signals are being broadcast in our local environment. Displays are provided in a waterfall plot (power as a function of time and frequency). Attendees can explore the frequency/waveforms of wireless key-fobs, listen in to narrow band FM transmissions, and explore inadvertent noise being emitted by their electronic devices.

B. Decode ADS-B to track aircraft

Automatic Dependent Surveillance-Broadcast (ADS-B) is a real-time surveillance system used by aircraft to broadcast position and aircraft status. Typically transmitted at 1090 MHz, it is the preferred method of surveillance for air traffic control in

[1] Alexandru Csete. gqrx SDR Software Package. https://gqrx.dk/ Accessed March 2022.

the National Air Space. ADS-B transmissions are also unencrypted, allowing anyone with an ADS-B receiver (or an appropriately configured SDR) to collect real-time aircraft information. Attendees will use an SDR and supporting software packages[2] to demodulate and decode these messages, and plot the transmitting aircraft in real time on a map, as shown in Figure 1.

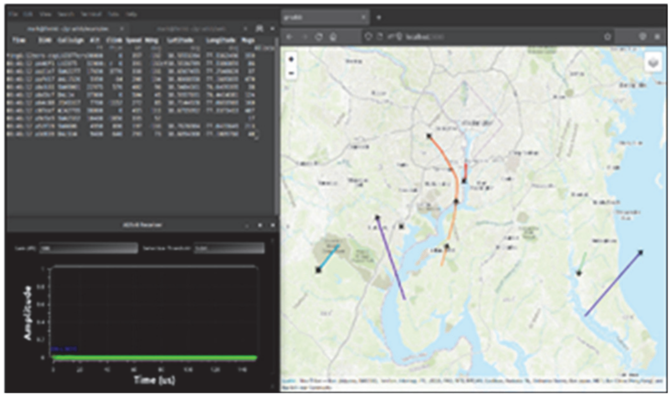


Figure 1. Using an SDR to decode ADS-B aircraft traffic and display flight paths on a map in real-time

C. Sniff noise to spy on monitors

Modern High-Definition Multimedia Interface (HDMI) cables operate at frequencies in the range between 24 to 340 MHz. If the cables lack adequate shielding, there can be electromagnetic leakage – that can be detected via SDR. Our demonstration adapts the *gr-tempest* software package to remotely and passively sniff emanations from an HDMI cable, recreating the display in real time on an attack laptop via an SDR and software.[3] Figure 2 shows an example of this attack.

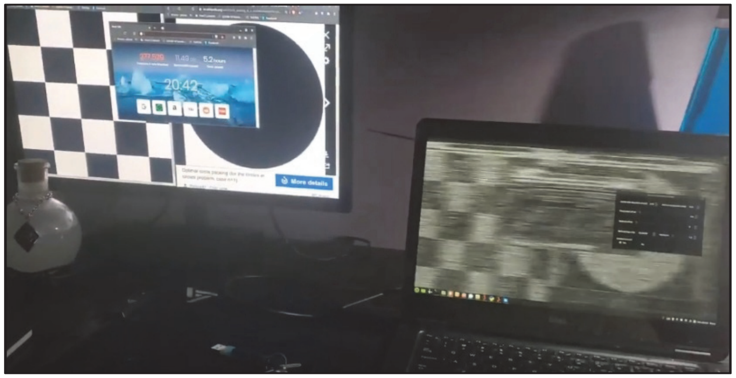


Figure 2. Using an SDR to sniff electromagnetic noise from an HDMI monitor and recreating the image on an attacker laptop

[2] Matt Hostetter. gr-adsb Software Package. https://github.com/mhostetter/gr-adsb. Accessed March 2022

[3] Federico La Rocca. ***gr-tempest*** Software Package. https://github.com/git-artes/gr-tempest. Accessed March 2022.

Adversaries and Airwaves: Hands-on Demonstrations with a Software Defined Radio

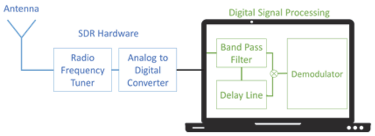
OED Cyber Lab

Institute for Defense Analyses

What is a Software Defined Radio?

A software defined radio (SDR) is a radio system where components traditionally implemented with dedicated or analog hardware instead are implemented in software.

Allows for incredible flexibility in the types of signals, protocols, and applications a single piece of hardware can support.



SDRs are widely available at different levels of capability and price points. Our demonstrations will use an RTL-SDR USB Stick that retails for about $20.

RTL-SDR
Receive Only
24-1766 MHz Tunable Range
(Expandable to 0.5-1766 MHz)
8-bit Analog to Digital Resolution
Receive Bandwidth 2.56 MHz
Temperature Controlled Oscillator

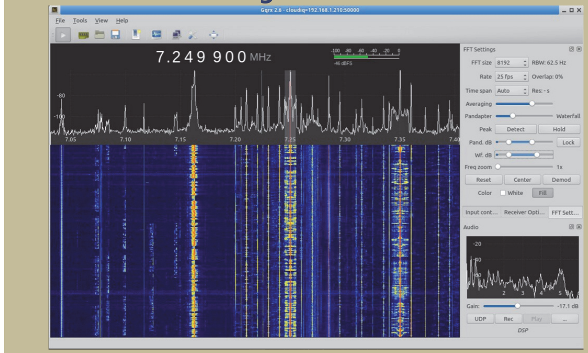
Image Credit: rtl-sdr.com

Other Example Projects

- Maritime Transponder Decoding
- Satellite Data Collection
- AM/FM/Amateur radio
- Passive/coherent radars
- Radio controllers
- Radio astronomy
- Cell Phone GSM networks
- Global Positioning System Sniffing
- Custom radio frequency data transmission protocols
- Side-channel cyber attacks

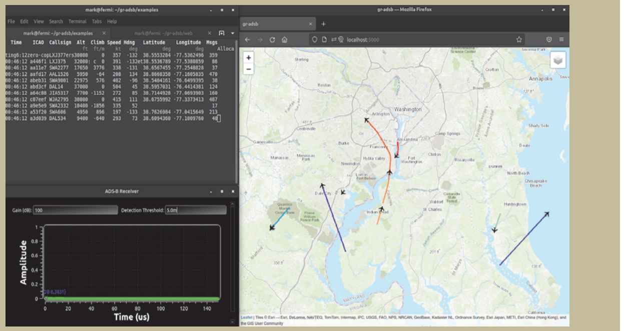
For more examples, demonstrations, and links to new projects: https://www.rtl-sdr.com/

Explore your local electromagnetic environment



FFT size: 8192
RBW: 62.5 Hz
Rate: 25 fps
Overlap: 0%
Time span: Auto
Res: - s
Averaging
Pandapter — Waterfall
Pand. dB
Wf. dB
Freq zoom: 1x
Color: □ White
Gain: -17.1 dB

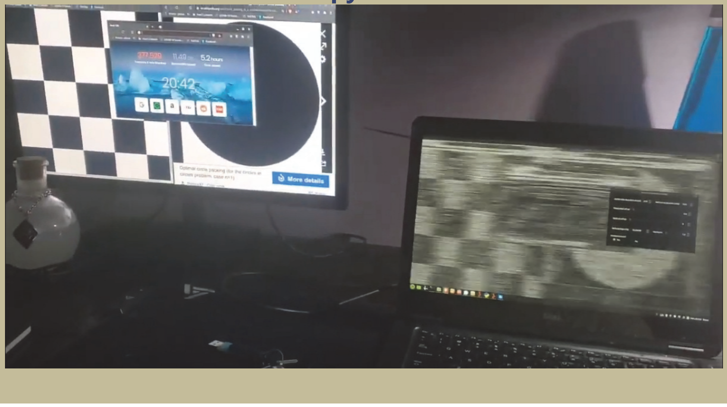
Decode aircraft transponder data



```
 Time     ICAO   Callsign  Alt  Climb Speed Hdng   Latitude   Longitude  Msgs
                            ft   ft/m    kt  deg        deg         deg     Alloca
ting6:12zero-copLXJ377ers30000     0   357 -132  38.5553284 -77.5362496  359
00:46:12 a446f1 LXJ375   32000: c  0   391 -132et38.5536789 -77.5380859   86
00:46:12 aa11e7 SWA2277   17650  3776   338 -131  38.6567455 -77.2548828   37
00:46:12 aafd17 AAL1526    5950   -64   208  134  38.8668358 -77.1605835  470
00:46:12 abeb31 SWA9001   22975   576   402  -96  38.5484161 -76.6499395   38
00:46:12 abd3cf DAL14     37000     0   504   45  38.5957031 -76.4414381  124
00:46:12 a64c88 JIA5317    7700 -1152   272   85  38.7144928 -77.0693903  160
00:46:12 c07eef WJA2795   38000     0   415  111  38.6755992 -77.3373413  407
00:46:12 a9e5e9 SWA2332   10400 -1856   335   52                           17
00:46:12 a53f20 SWA686     4950   896   197 -133  38.7626984 -77.0415649  213
00:46:12 a3d039 DAL534     9400  -640   293   73  38.6094360 -77.1009760   40
```

Gain (dB): 100
Detection Threshold: 5.0m

Sniff electromagnetic noise to spy on monitors



Exploring the electromagnetic environment

Using an SDR receiver program (**GQRX**), we can investigate what signals are being broadcast in our local environment. Displays are provided in a waterfall plot (power as a function of time and frequency).

Things to try:

- Tune into favorite FM radio stations.
- Explore the frequency/waveforms of wireless key-fobs.
- Listen to air traffic control discussions.
- Find and listen to narrow band FM transmissions (e.g. maritime weather).
- Explore inadvertent noise coming from computers and other electronic devices.

Decode ADS-B to track aircraft

Automatic Dependent Surveillance-Broadcast (ADS-B) is a real-time surveillance system used by aircraft to broadcast position and aircraft status.

Typically transmitted at 1090 MHz, it is the preferred method of surveillance for air traffic control in the National Air Space.

ADS-B transmissions are also unencrypted, allowing anyone with an ADS-B receiver (or an appropriately configured SDR) to collect real-time aircraft information.

Using the **gr-adsb** package, we can demodulate and decode these messages, and plot the transmitting aircraft in real time on a map.

Sniff noise to spy on monitors

Modern High-Definition Multimedia Interface (HDMI) cables operate at frequencies in the range between 24 to 340 MHz.

If the cables aren't adequately shielded, there can be electromagnetic leakage – that can be detected by our SDR.

Video is usually transmitted one line of pixels at a time, encoded as a varying current. This in turn induces electromagnetic fields that can be sniffed by our SDR. We can use software to map the field strength to a gray-scale pixel in real time (adapted from *https://github.com/martinmarinov/TempestSDR*).

Our demonstration adapts the **gr-tempest** implementation of this attack to remotely and passively sniff emanations from an HDMI cable, recreating the display in real time on the attack laptop.

About the OED Cyber Lab

The OED Cyber Lab is a standalone, educational computer environment where IDA Research Staff and Sponsors can explore concepts and techniques related to cybersecurity. It provides a safe, guided venue for researchers at all levels of cyber proficiency to experiment with cyber test and evaluation concepts.
Tutorials/modules include:

- Network Enumeration
- Password Cracking
- Vulnerability Scanning
- Network Pivoting and Exfiltration of Data
- MIL-STD 1553 experimentation
- Controller Area Network (CAN) Bus
- Intrusion Detection Systems

Acknowledgments

Thank you to Shawn Whetstone, Brian Conway, and Andrea Kirkpatrick for their review of this poster.

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION

1. REPORT DATE 04-2022	**2. REPORT TYPE** Draft Final	**3. DATES COVERED** **START DATE**	 **END DATE** Apr 2022

4. TITLE AND SUBTITLE
DATAWorks 2022: Adversaries and Airwaves: Hands-on Demonstrations with a Software Defined Radio

5a. CONTRACT NUMBER Separate Contract	**5b. GRANT NUMBER**	**5c. PROGRAM ELEMENT NUMBER**
5d. PROJECT NUMBER C9096	**5e. TASK NUMBER** C9096	**5f. WORK UNIT NUMBER**

6. AUTHOR(S)
Mark R. Herrera; Jason R. Schlup; Stacey L. Allison; Kelly Tran

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Institute for Defense Analyses 730 East Glebe Road Alexandria, Virginia 22305	**8. PERFORMING ORGANIZATION REPORT NUMBER** D-33011-NS H 2022-000094

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**	**11. SPONSOR/MONITOR'S REPORT NUMBER**

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
Project Leader: Peter M. Mancini

14. ABSTRACT

This poster serves as a supplement to the Operational Evaluation Division (OED) Cyber Lab breakout session “Adversaries and Airwaves: An Introduction to Wifi / Radio Frequency Hacking.” Both that presentation and this poster will be presented at the upcoming DATAWorks2022 Conference.

A software defined radio (SDR) is a radio system where components traditionally implemented with dedicated or analog hardware instead are implemented in software. This allows these devices to have incredible flexibility in the types of signals, protocols, and applications a single piece of hardware can support.

This poster presents several hands-on demonstrations using SDRs that DATAWorks attendees can experiment with as they chat with members of the OED Cyber Lab. The goal is to provide attendees the opportunity to experiment with hardware and software they may not be familiar with, and to demonstrate the wide breadth of applications these ubiquitous, affordable devices can support.

15. SUBJECT TERMS
Software Defined Radio; cybersecurity; electromagnetic spectrum operations (EMSO)

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT** SAR	**18. NUMBER OF PAGES** 9
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified		

19a. NAME OF RESPONSIBLE PERSON Peter Mancini	**19b. PHONE NUMBER** 703-845-2496

PREVIOUS EDITION IS OBSOLETE.