INL/LTD-19-55545
Revision 2

Aviation Cyber Initiative Unmanned Aircraft System Information Security Risks Limited Scope Test & Evaluation

October 2019

OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: *Exemption No. 4, Commercial/Proprietary (FOIA may apply)*.

Department of Energy review required before public release

Name/Org: Brooks Cooper/M310 Date: 09/12/2019
Guidance (if applicable) ______________________

Idaho National
Laboratory

The INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the United States (U.S.) Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/LTD-19-55545
Revision 2

Aviation Cyber Initiative Unmanned Aircraft System Information Security Risks Limited Scope Test & Evaluation

October 2019

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Contract DE-AC07-05ID14517

This page intentionally left blank.

EXECUTIVE SUMMARY

A preliminary and limited cybersecurity test and evaluation (T&E) of four unmanned aircraft systems (UASs) were recently completed by the United States (U.S.) Department of Homeland Security's (DHS's) Cybersecurity and Infrastructure Security Agency (CISA) at Idaho National Laboratory (INL) under the Aviation Cyber Initiative (ACI). The T&E effort supports the DHS CISA National Risk Management Center (NRMC) UAS Campaign and the U.S. Department of Interior (DOI) Office of Aviation Services (OAS) UAS program. The four systems analyzed are manufactured by Dà-Jiāng Innovations Science and Technology Co., Ltd (DJI), Autel Robotics, and Parrot SA, and are operated by various government departments and agencies—as well as by many commercial entities and private consumers. At the request of DOI OAS, DJI's Matrice 600 Pro and Mavic Pro 2 drones with government editions (GEs) of its software, Autel's EVO drone, and Parrot's ANAFI system were all analyzed within INL's interference-free environment where data was collected and examined. The analysis covered the communications system to determine if there are ways to capture sensitive data or if data is being exfiltrated to other networks. The limited-scope analysis showed there are no major areas of concern related to data leakage, thereby supporting that the multi-layered mitigations DOI has in place (including the use of built-to-specification GE software, firmware, and hardware) are in fact working as designed to meet their published security requirements. Minor effects of the wireless tests are presented here, which will require continuous defense-in-depth actions and management of the operational environment to mitigate additional concerns. A deeper analysis of the hardware, software, firmware, and wireless signals to include further protocol analysis of the data and telemetry stream to reduce security risk is suggested.

This page intentionally left blank.

CONTENTS

FIGURES

ACRONYMS

ACI	Aviation Cyber Initiative
ADS-B	Automatic Dependent Surveillance – Broadcast
CISA	Cybersecurity and Infrastructure Security Agency
CRC	cyclic redundancy check
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
DB	Decibels; also abbreviated as dB
dBm	Decibels in milliwatts as a radio power ratio usually in reference to one milliwatt
DC	Direct Current (in radio frequency nomenclature, this means zero frequency or constant polarity)
DHS	U.S. Department of Homeland Security
DJI	Dà-Jiāng Innovations Science and Technology Co., Ltd
DOD	U.S. Department of Defense
DOI	U.S. Department of Interior
DOS	denial-of-service
DOT	U.S. Department of Transportation
DSP	digital signal processing
EIRP	effective isotropic radiated power
FAA	U.S. Federal Aviation Administration
FCC	U.S. Federal Communications Commission
FHSS	frequency hopping spread spectrum
g	gram
GE	government edition
GHz	gigahertz
GIS	geographic information system
GLONASS	GLObal NAvigation Satellite System
GPS	global positioning system
gpsd	GPS daemon
gpsmon	GPS monitor
GRC	GNU Radio Companion
HDMI	high-definition multimedia interface
I2C	inter-integrated circuit bus
INL	Idaho National Laboratory
IP	Internet protocol

IR	infrared
ISM	industrial, scientific, and medical
JTAG	Joint Test Action Group
km	kilometer
LAN	local area network
LIDAR	Light Detection and Ranging
LiPo	lithium polymer
LOE	Line of Effort
LOS	line of sight
mAh	millilamp hour
MHz	megahertz
mm	millimeter
MPH	miles per hour
ms	millisecond
NRMC	National Risk Management Center
NSAS	National Strategy for Aviation Security
NTIA	National Telecommunications and Information Administration
OAS	Office of Aviation Services
OFDM	Orthogonal Frequency Division Multiplex
OT&E	operational test and evaluation
PCAP	packet capture
RF	radio frequency
SDI	serial digital interface
SDR	software defined radio
SPI	serial peripheral interface
sUAS	small unmanned aircraft system
T&E	test and evaluation
TCP	transmission control protocol
U.S.	United States
UAS	unmanned aircraft system
UAV	unmanned aircraft vehicle
USB	universal serial bus
USG	United States Government
Wi-Fi	wireless fidelity
WPA2	wireless protected access 2

INTRODUCTION

The unmanned aircraft system (UAS) airspace continues to grow exponentially as the utility for these devices become more evident in many categories of industry. In a 2016 Goldman Sachs report [1], the forecast for UAS markets will grow to over $100 billion globally by 2020. This is primarily due to active campaigns in the private and military sectors, which is mostly driven by commercial goals—even though the military sector is larger at the present time [2]. Clearly, the popularity of UAS devices is obvious and will continue to become even more pervasive as the market is driven mostly by the commercial sector. These devices will become more of a commodity and revenue will be driven from many services, so ultimately the price for UAS devices will be driven downward, much like office printers are relatively inexpensive, but services and maintenance on them is primarily where company revenues are derived. As the price per unit is driven downward, more sophisticated systems will become available to a variety of users, whether they have nefarious intentions or not. UASs are flown in the following sectors [1]:

- construction
- agriculture
- insurance claims
- offshore oil/gas & refining
- police
- fire
- coast guard
- journalism
- customs & border protection
- real estate
- utilities (e.g., electrical, water, natural gas, etc.)
- pipelines
- mining
- clean energy
- cinematography
- and many more.

As can be seen from this list, several critical infrastructure sectors can be or are being affected by UAS use with substantial growth in the UAS market expected in the years ahead. In the case of the United States (U.S.) Department of Interior (DOI), employees are tasked with fulfilling an extremely diverse set of missions. Overall trends point to continued growth in the adoption and utilization of UASs for all of those diverse missions. Across DOI's nine bureaus active in the UAS program, UAS missions include providing situational awareness through video or still photos, integrating precise landscape survey instruments, creating centimeter-level accuracy to three-dimensional models, and using drones to position sensors where no other means of doing so exist. The combination of DOI mission diversity and a UAS industry poised with ingenuity has fueled the expansion of this program. In fiscal year 2018 alone, DOI completed 10,342 flights across project (72%), fire (14%), volcano (14%), and hurricane (1%) support areas [3].

Of particular concern is the supply chain for UASs. The top UAS platform, component, and commodity manufacturers are dominated by those based in China. This is due in large part to the overhead for Chinese manufacturing costs as opposed to those based in the U.S., which is radically less. Once upon a time, there were U.S.-based UAS companies that held top positions in the market, but today they do not have a substantial market share or have been met with business failures due to mismanagement or inferior manufacturing designs [4],[5]. Additionally, although these were U.S.-based UAS companies, their UASs were all manufactured in China. Even for the few small U.S.-based companies that manufacture UASs in the U.S. (e.g., Birdseyeview Aerobotics), the technical and economic viability of their UAS products relies on electronic components manufactured in China. This phenomena also extends to UASs produced by companies in countries allied to the U.S. As an example, the ANAFI commercial drone produced by Parrot is made in China. The reality of commercial drones parallels the reality of all modern-day commercial electronics (e.g., TVs, radios, computers, monitors, smart speakers, smartphones, cameras, etc.). They are manufactured in or contain significant components and commodities produced overseas in countries like China. As such, with growing demand and utility for numerous operations and tasks, and in attempt to keep costs low—especially with very large fleets, perhaps in the thousands—the U.S. Government (USG) is currently faced with two predominant choices to meet the current demand for highly capable, cost-effective small unmanned aircraft systems (sUAS): (a) work with industry and government agencies to establish pertinent security requirements and then establish testing and verification protocols to validate compliance with those requirements; or (b) suspend the use of commercial sUASs across the federal government until such time that a capable, cost-effective "pure-U.S." commercial drone can be developed and produced by a reconstituted U.S. electronics industry.

To continue the discussion on the current supply chain, Dà-Jiāng Innovations Science and Technology Co., Ltd (DJI) dominates the list of UAS manufacturers in market share due to substantially low overhead costs, time-to-market, and innovative hardware and software designs, which make their products immensely competitive with other manufacturers, but very compelling to consumers [6]. DJI's products have a relatively low initial cost investment, exhibit very high functionality and features, and operate robustly even in the most demanding environmental conditions and radio frequency (RF) noise. DJI's competitors, especially U.S.-based ones, will have difficulty in capturing significant portions of the UAS market in the future. A detailed study of the cybersecurity effects of foreign manufacturing on electronics components is out of scope for this document, but is mentioned here because the same principles apply in other sectors and should remain a concern for cybersecurity professionals so that mitigation strategies can be constructed in an attempt to reduce risk.

The Autel EVO is also manufactured in China from a U.S.-based company called Autel Robotics, which was established in 2014 in Bothell, Washington, USA, but is a subsidiary of the Chinese company Autel Intelligent Corporation [7]. Autel is a direct competitor to DJI and has even brought patent infringement litigation against them as recently as 2018 [8].

In order to inform ongoing DOI Office of Aviation Services (OAS) risk assessment efforts, a preliminary analysis was performed to determine the wireless and application security of the four UASs that were on loan from DJI, Autel, and Parrot. It should be noted that the two DJI UASs came pre-loaded with special government editions (GEs) of DJI's software. Generally speaking, the analysis included tests and analysis of control, telemetry, and video signals from the platform to the controller and messaging from the controller to the application. These tests and evaluations included any data that could be demodulated from the systems and analyzed with cybersecurity tools to determine whether data exfiltration was emanating from or targeting external networks or servers. The details of this evaluation are provided in this report.

BACKGROUND

In support of this project, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) representative to the Aviation Cyber Initiative (ACI) requested the Idaho National Laboratory (INL) ACI Project Manager provide limited-scope test and evaluation (T&E) support under Line of Effort (LOE) 3: "Manage and Mitigate Risk from Unsecured UAS for the DHS National Risk Management Center (NRMC)'s Campaign Plan: Unmanned Aircraft System Information Security Risks."

As part of accomplishing LOE 3, the goal of the efforts outlined within this document is to support information security risks without inhibiting the ability of the USG and private sector partners to benefit from the adoption and employment of emerging UAS technology. The campaign plan is intended to complement DHS efforts to implement the U.S. Federal Aviation Administration (FAA) Reauthorization Act of 2018 (Pub. L. No. 115-254) and does not contradict or supersede those efforts or any language in that act.

As detailed in the "DOI UAS Program 2018 Use Report" [3] and other publicly available agency documents, DOI's involvement in this initiative stemmed from their leadership in the development and adherence to strong sUAS performance and security requirements. In 2014, following five years of UAS operational test and evaluation (OT&E) work, DOI OAS personnel and over 300 subject matter experts from various DOI bureaus developed the Master UAS Requirements for the DOI. In 2015, while conducting UAS market research, the OAS determined that the privacy policy of the largest provider of UASs in the U.S.—DJI—did not meet the UAS data management assurance standards contained in the Master UAS Requirements for the DOI. Specifically, they did not meet DOI's requirement to be able *"to decline and lock out any device information sharing including telemetry through aircraft, software or applications preventing any automated uploads or downloads."*

In 2016, DOI awarded its first contract for fleet sUASs to a U.S.-based company whose aircraft met all relevant technical and DOI bureau price requirements. Shortly thereafter, this company (3D Robotics) ceased the manufacturing of UASs as a result of market competition. Subsequent OAS market research to identify additional UASs to meet the growing demand of DOI bureaus for inexpensive and highly capable aircraft indicated that the remaining UASs available from U.S.-based companies were up to ten times less capable for the same price, or up to ten times more costly than similarly capable DJI aircraft. OAS immediately began working with DOI bureaus and federal partners, as well as the drone industry, to identify, develop, and field potential solutions that met DOI's three data management and risk mitigation requirements listed in the Master UAS Requirements for the DOI. In 2017, working with the U.S. Department of Defense (DOD), OAS identified a potential solution and began developing a flight test plan to assess the suitability of this solution across a range of DOI bureau UAS missions. In 2017, OAS was also approached by DJI with an offer to collaborate on the development, testing, and potential fielding of a customer-focused enterprise solution that would meet DOI's UAS data management and risk mitigation requirements for enterprise level managed data sharing controls. Draft specifications for the new "private edition" (later referred to as "government edition" [GE]) included custom software, firmware, and UAS hardware editions for two specific DOI-selected DJI drones (e.g., Matrice 600 Pro, Mavic Pro). Provisions to include flight testing of GE-equipped DJI aircraft were later added to the flight test plan. Additionally, OAS collaborated with one industry and two federal partners (including DHS, CISA, and INL) with expertise in data management assurance testing to conduct targeted assessments of GE hardware, firmware, and software.

Campaign Plan: Unmanned Aircraft System Information Security Risks

The primary focus of the DHS/CISA Campaign Plan: Unmanned Aircraft System Information Security Risks is taking short-term actions to mitigate information security risks related to the adoption of UAS technology by government and critical infrastructure operators. These information security risks may pose operational risks, in turn, to DHS, the USG, and state, local, tribal, territorial, and private sector partners.

Aviation Cyber Initiative (ACI)

The ACI was launched in early 2016 to define, analyze, and reduce cyber-risks to civil aircraft. In 2018, the ACI's scope was broadened by the National Strategy for Aviation Security (NSAS) to reduce cybersecurity risk to the nation's aviation ecosystem and effectuate cybersecurity objectives outlined in NSAS supporting plans. The ACI is a tri-chaired task force led by DHS, DOD, and the U.S. Department of Transportation (DOT) to reduce cybersecurity risks and improve cyber resilience to support safe, secure, and efficient operations of the nation's aviation ecosystem. The ACI strategic objectives are accomplished by identifying, prioritizing, and mitigating cybersecurity risks impacting civil and military aviation through interagency and private industry coordination efforts. This project supports one of the ACI's objectives to identify, assess, and analyze cyber-threats, vulnerabilities, and consequences within the aviation ecosystem through research, development, testing, and evaluation initiatives.

CYBER THREATS

Generally, there are several critical areas of a UAS providing an attack surface: (1) the hardware; (2) the wireless communications subsystems; (3) the sensor subsystems; (4) the controller; and (5) the handheld application.

Hardware Threat

Hardware attacks can occur if and when UASs are stored or when maintenance is performed. If access is not protected, direct attacks on the hardware can be exploited to contaminate data and perturb the functioning of the aircraft, or worse yet, redirect sensitive data to an unintended location. These types of attacks can also be implemented or installed during manufacturing and supply-chain delivery. This is typically a configuration management and supply chain issue, both of which are out of the scope of this report, but may result in data leakage—the negative consequences of malfunctioning UAS devices during a critical task. If the system is suspected of being hardware-compromised, more sophisticated hardware inspection and possibly reverse-engineering would be required to uncover any malicious modifications.

Hardware manufacturing has many unanswered questions about whether the sensitive operational data is secure. With today's global economy and manufacturing taking place in numerous locations around the world, it would be impossible to guarantee secure data without some formal security mitigation methods. The best that can be done is to secure the outgoing and incoming data with a well thought-out defense-in-depth strategy, so that even if the devices are attempting to transmit data to unintended locations, these transmissions can be monitored and caught by users and cybersecurity professionals in a timely manner. Likewise, any incoming data in the form of software updates, patches, and/or configuration data should be monitored and scrutinized for potential malicious threats.

Wireless Threat

Cyber-threats to wireless communications subsystems may include, but are not limited to, the items included in the following list. Many more sophisticated attacks on other wireless subsystems that do not appear in the simple platforms in this report are also listed here for completion. For more information, refer to Ref. [9]:

- Control signal interference, otherwise known as jamming, can occur in different situations, such as using an overwhelming signal power from an attacking source or by protocol jamming, which is usually some kind of signal transmission that closely matches the legitimate signal waveform or the frequency hopping spread spectrum (FHSS) channel enumeration [10]. Jamming will not be covered in this report since there are numerous studies in the literature, and would therefore be out of scope for the analysis. In addition, signal interference provides very little or no data to be leaked as this is more of a denial-of-service (DOS) attack than an attempt to collect sensitive information.
- Control signal takeover by an attacking signal. Again, this is out of scope for the purposes of this analysis; however, takeover in general is of great concern since control of a signal may occur by some other method other than by radio signal attack, such as through data leakage, lack of configuration management, and/or mismanaged encryption keys and passwords.
- Telemetry data sniffing to locate the platform and the possibility of spoofing control data and information.
- Since there are known vulnerabilities in wireless fidelity (Wi-Fi) that are not adequately patched against the latest vulnerabilities, an attacker can use widely available cyber-tools, such as aircrack-ng, to compromise a Wi-Fi connection to the UAS. Weak Wi-Fi passwords increase the likelihood of Wi-Fi attacks.
- Record and replay attacks work in some circumstances when communications traffic is unsophisticated, unencrypted, or both. Examples of unsophisticated traffic include those that do not use checksums, packet IDs, synchronization IDs, cyclic redundancy checks (CRCs), etc. Encryption decreases the possibility of this method, unless the encryption itself is not sophisticated or uses an old certificate and/or key.

Sensor Threat

Sensor subsystems can be quite vast on larger and complex UASs, such as on military grade systems. For example, some systems not only have global positioning system (GPS) receivers, but may also have magnetometers, barometers, altimeters, Automatic Dependent Surveillance – Broadcast (ADS-B) receivers, inertial measurement units, radar, sonar, Light Detection and Ranging (LIDAR), and infrared (IR) sensors, to name a few. Systems such as these measure their range in tens to hundreds of miles versus hundreds of yards and single digit miles. The smaller and less sophisticated the UAS, the less the number of sensors required to keep navigation simple for relatively short flights and are usually only operable within line of sight (LOS). Most consumer-grade systems only have GPS sensors that may include an altimeter or barometer to measure altitude for slightly more professional grade systems. So, the following is one single sensor for low-end UAS cyber-threats. For a more complete discussion of these and many other sensors, see Ref. [9]:

- GPS spoofing attacks. Many systems are vulnerable to GPS spoofing attacks in regards to location and possibly system clock-time. This is due, in large part, to heavy dependence on GPS signals so that the platform has an awareness of its own location and can possibly synchronize timing data within the signal. Not all UASs synchronize their system clocks to GPS time, but it is critical to have time synchronization for encryption. Many systems have very sensitive GPS receivers and will acquire a signal at low latency for reliability and safety requirements. The downside is that these signals are typically set at a higher power level than legitimate signals tend to be what the receiver will attach to—unless sophisticated receiver algorithms are used to determine a correct signal source. Timing and signal source location are used frequently to mitigate this problem, but at a higher expense to the UAS.

- GPS jamming will cause a UAS to lose its location and become lost in airspace. Many UASs will not operate if they do not sense a GPS signal and calculate a position. Pilots can still operate the UAS without a GPS if the system is configured to do so before flight operations. This is a common scenario for indoor flight operations, but very rare for an outdoor flight plan.

Controller Threat

- The controller is subject to the same threats as noted in the 'Hardware Threat' section, but it also has the added attack surface of two types of communication interfaces: universal serial bus (USB) and Wi-Fi. Theoretically, this may open the controller up to yet other attacks when a handheld device like a tablet or smartphone is connected to it, since the device may have connectivity to some type of network, such as a local area network (LAN) or cellular network, which may have access to the Internet. The handheld device may already be compromised and it may be just a matter of connecting to the controller so that some type of exploit could be installed unbeknownst to the pilot. Further analysis of this potential attack surface would be necessary to determine feasibility and likelihood.

Application Threat

Since the application is installed on a smartphone or tablet, there may be a chance that malicious code or functions could be run against the app and, thus, the controller or the platform. What may also be possible is that the application could be modified to exfiltrate data to an unintended location or cause malfunctions in the rest of the UAS.

UNMANNED AERIAL SYSTEMS (LIMITED-SCOPE ANALYSIS PROJECT FOCUS)

This analysis focused on one item of concern: data leakage. The communication subsystems were subjected to several tests, most of which are part of the wireless communications package and application network activity, if any. Many of the cyber-threats as discussed in the previous section are not part of the scope of this analysis. Much literature exists on gaining control of the UAS, jamming navigation, and denying services. What this report does cover is the analysis of the communications system to determine if there are ways to capture sensitive data or if that data is being exfiltrated to other networks.

The short-term goal of this evaluation included the high-level examination of the communications subsystem, not an invasive examination of the hardware, firmware, or the inner workings of the UAS. Of particular concern was whether the handheld device application or the controller would attempt to send information to an outside network. Secondarily, the investigation reviewed the security of the streaming video and control/telemetry data. This evaluation included passive capture of raw radio signal data and analysis, but did not involve any deep reverse-engineering of the captured signal data or invasive reverse-engineering of the firmware or device hardware. These are tasks left to a more long-term analysis project and would have to involve UAS hardware that could be disassembled and subject to a battery of tests and deep inspection of individual system chips and memory. The DOI OAS platforms were not subjected to this level of analysis in keeping with the limited-scope agreement that was designed to validate performance to their published data management assurance and security requirements. The UAS hardware used in this analysis was on loan from the manufacturer to the DOI, who requested a passive cybersecurity analysis of its systems in accordance with DOI's published UAS requirements. No functionality, flight, or performance tests were performed on any of the systems. That level of testing was accomplished by DOI during a 15-month, 2,200 flight test plan across numerous DOI mission applications. This limited-scope analysis was completed exclusively in an interior laboratory environment.

Targeted Platforms Analyzed

As discussed previously, four platforms from three manufacturers were loaned to INL for this limited-scope analysis based on the determination of DOI OAS from their current UAS inventory. Due to their high procurement and maintenance costs, DOI loaned a DJI Mavic Pro, a DJI Matrice 600 Pro, an Autel EVO, and a Parrot ANAFI to DHS CISA researchers at INL so their respective functionalities could be tested to determine potential cyber-risks. DJI also provided DOI OAS with a GE of the DJI platform, controller firmware, and application software to provide an even higher level of security.

DJI Mavic Pro

Below are the physical attributes and functional features of the DJI Mavic Pro UAS (see Figure 1). The Mavic Pro horizontally spans approximately 14 inches (~355 millimeters [mm]) at diagonally opposing rotors (center to center) without the propellers.

Figure 1. DJI Mavic Pro with mounted camera (Source: bhphotovideo.com).

Here are some relevant features of the commercial edition from the DJI website[a]:

- Weight: 1.65 pounds with battery, propellers, and gimbal cover attached
- Max speed is 40 Miles per hour (MPH) without wind
- Max service ceiling above sea level: 16404 ft. (5000 m)
- Max flight time: 30 minutes @ 15.5 MPH and no wind
- Max hover time: 27 minutes with no wind
- Maximum travel distance with one full battery and no wind: 9.3 miles (13 kilometers [km])
- Satellite positioning systems: GPS or GLObal NAvigation Satellite System (GLONASS)
- Operating frequencies (U.S. Federal Communications Commission [FCC] specification only):
  - 2.4 to 2.4835 gigahertz (GHz)
  - 5.150 to 5.250 GHz
  - 5.725 to 5.850 GHz
- Transmit Power (effective isotropic radiated power [EIRP] and FCC):
  - 2.4 GHz <=26 decibel-milliwatts (dBm)
  - 5.2 GHz <=23 dBm
  - 5.8 GHz <=23 dBm

[a] https://www.dji.com/mavic.

- FHSS: DJI Ocusync proprietary
- Transmit range between remote controller and aircraft (FCC): ~4.3 mi (7 km)
- USB ports: Lighting, Micro USB Type-CTM
- Wi-Fi (GE configuration with no Wi-Fi):
  - 2.4 GHz and 5 GHz
  - Max Transmission Distance: 262 ft. (80 m)
- Battery:
  - Lithium Polymer (LiPo 3S)
  - Capacity: 3830 Millilamp Hours (mAh)
  - Voltage: 11.4 V

DJI Matrice 600 Pro

Below are the physical attributes and functional features of the DJI Matrice 600 Pro UAS (see Figure 2). The Matrice 600 Pro horizontally spans approximately 48 inches from opposing rotors (center to center) without propellers.

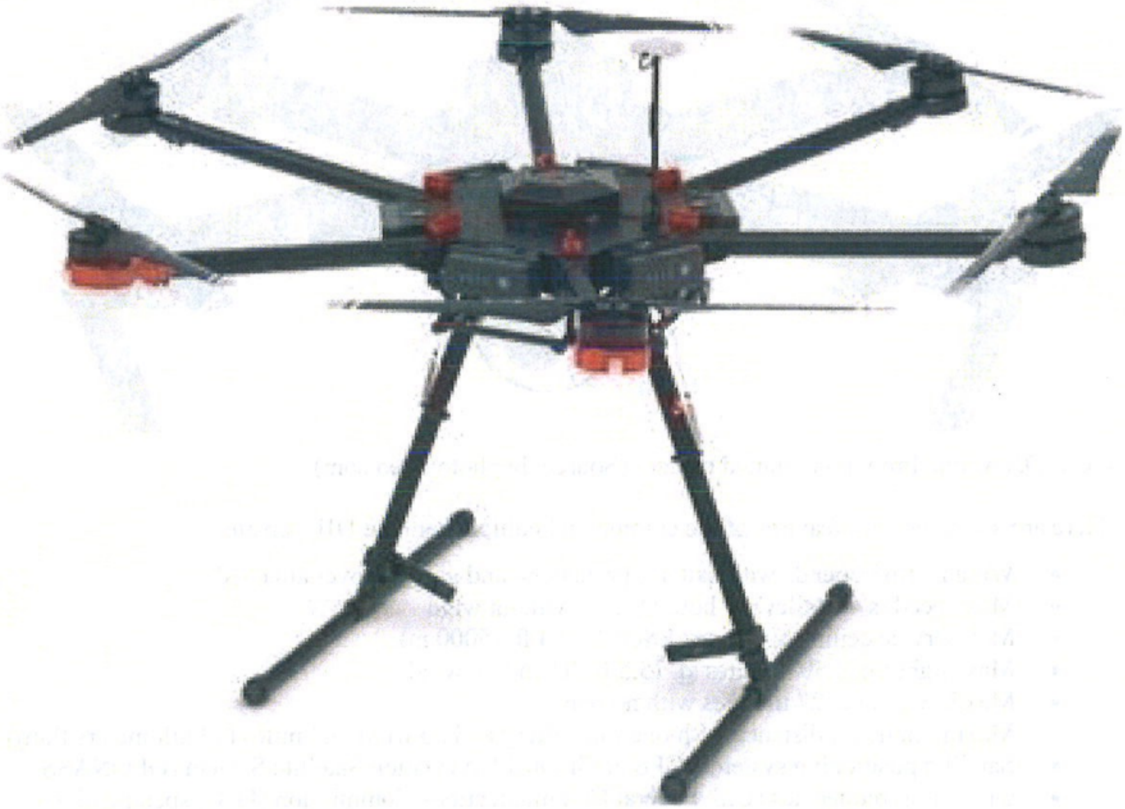

Figure 2. DJI Matrice 600 Pro without gimbal or camera (Source: dji.com).

Here are some relevant features of the commercial edition from the DJI website[b]:

- Weight: 20 lbs. (9.1 kg) to 21.1 lbs. (9.6 kg), depending on battery type
- Max Takeoff Weight: 33.29 lbs. (15.1 kg)
- Max Speed: 40 MPH (18 ms) with no wind
- Max service ceiling above sea level: 8202 ft. (2500 m)

[b] https://www.dji.com/matrice600.

- Hovering Time: 35 min (no payload), 16 min (12.1 lbs. [5.5 kg] payload) with lighter batteries; with heavier batteries: 40 min; 18 min
- Operating frequencies:
    - 2.4 GHz to 2.483 GHz
    - 5.725 GHz to 5.825 GHz
- Max Transmission Distance (FCC): 3.1 miles (5 km)
- Transmit Power (EIRP):
    - 13 dBm @ 5.8 GHz
    - 20 dBm @ 2.4 GHz
- Video Output Ports: high-definition multimedia interface (HDMI), serial digital interface (SDI), USB
- Batteries – type TB47S or TB48S:
    - Quantity: 6
    - Lithium Polymer (LiPo 6S)
    - Weight: 1.3 lbs. (595 g) or 1.5 lbs (680 g)
    - Capacity: 4500 mAh or 5700 mAh
- Supports numerous gimbals and thus cameras; tested platform configured with Zenmuse X5 gimbal and camera

Autel EVO

Below are the physical attributes and functional features of the Autel EVO UAS (see Figure 3). The EVO spans approximately 13.3 inches (~338 mm) diagonally opposing rotors (center to center) without the propellers.

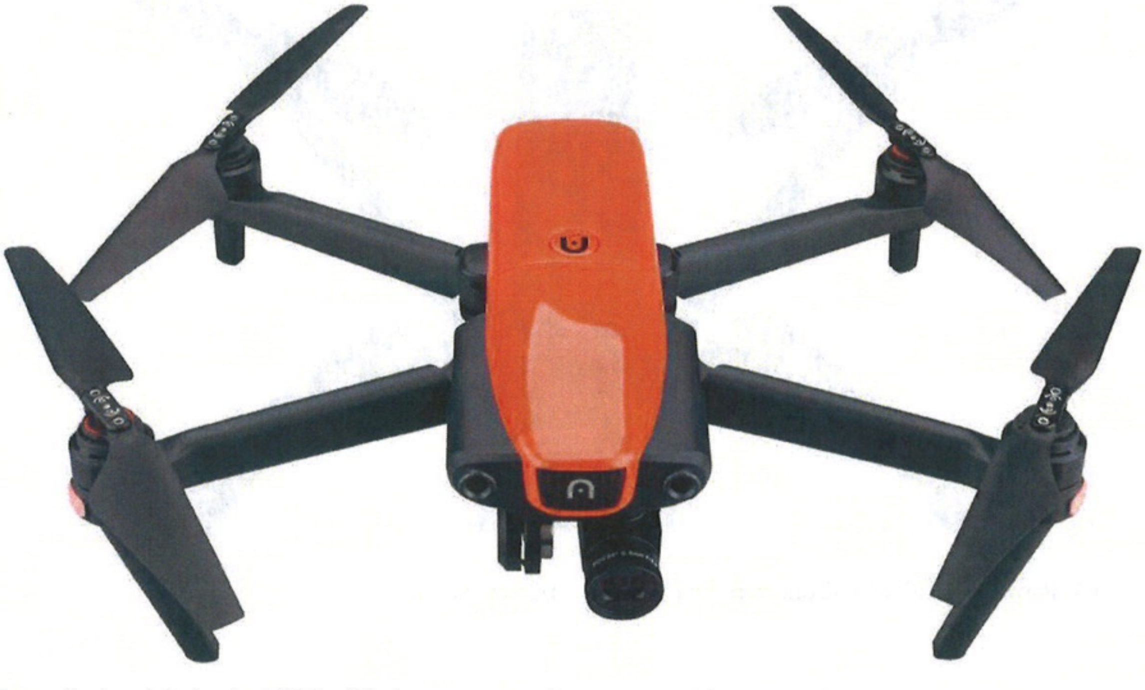

Figure 3. Autel Robotics EVO with drone camera (Source: auteldrones.com).

Here are some relevant features of the EVO from the Autel Robotics website[c]:

- Weight: 1.9 lbs. (863 grams [g])
- Max Speed: 44.7 MPH (20 ms)
- Max Ascent/Descent Speed: (5ms/3ms)
- Hovering Time: 30 min
- Operating frequencies:
  - RF Receiver Operating Frequency: 2.4 GHz to 2.4835 GHz
  - Video Link Frequency: 2.4 GHz to 2.4835 GHz
- Max Transmission Distance: 4.3 miles (7 km)
- Transmit Power (EIRP):
  - FCC: <= 26 dBm @ 2.4 GHz
- Batteries:
  - Quantity: 1
  - Lithium Polymer
  - Weight: 1.3 lbs. (595 g)
  - Capacity: 4300 mAh

Parrot ANAFI

Below are the physical attributes and functional features of the Parrot ANAFI UAS (see Figure 4). The ANAFI spans approximately 9.4 inches (~240 mm) diagonally opposing rotors (center to center) without the propellers.

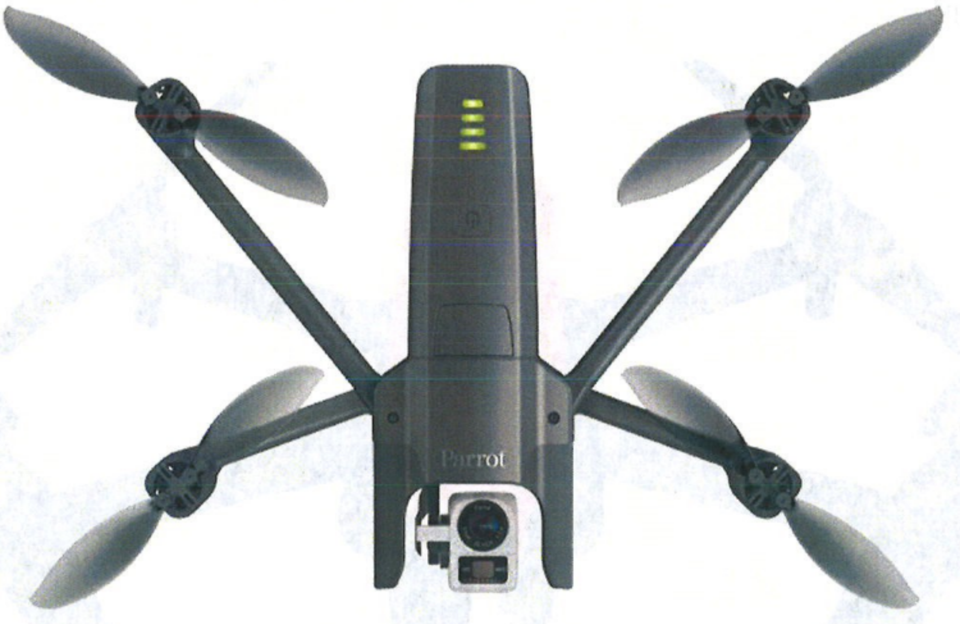

Figure 4. Parrot ANAFI with drone camera (Source: parrot.com).

[c] https://auteldrones.com/products/evo.

Here are some relevant features of the ANAFI from the Parrot website[d]:

- Weight: .7 lbs. (320 g)
- Max Speed: 34.2 MPH (15.3 ms)
- Max Ascent/Descent Speed: (4 ms)
- Max Flight Time: 25 min
- Operating frequencies: 2.4 GHz or 5.8 GHz:
  - RF Receiver Operating Frequency: 2.4 GHz to 2.4835 GHz
  - Video Link Frequency: 2.4 GHz to 2.4835 GHz
- Radio Protocol: Wi-Fi 802.11a/b/g/n
- Max Transmission Distance: 2.48 miles (4 km) LOS with no interference
- Transmit Power (EIRP):
  - FCC: <= 26 dBm @ 2.4 GHz
- Batteries:
  - Quantity: 1
  - High Density LiPo
  - Capacity: 2700 mAh

Cybersecurity Data Leakage Analysis Process Approach (Methods & Materials)

UAS Architecture

In order to discuss the report, a general architecture of the platforms will be reviewed here, which will be specific to the platforms examined during the analysis process. Typically, a UAS consists of three components: (1) the airborne platform itself (shortened to 'platform'); (2) the handheld flight controller (shortened to 'controller'); and (3) the handheld device with the application (shortened to 'app'), assuming it is installed in a handheld device such as a smartphone or a tablet. Figure 5 provides a depiction of a typical UAS architecture. Variations of this architecture may exist, but for the purposes of this analysis, this is what a typical setup looks like.

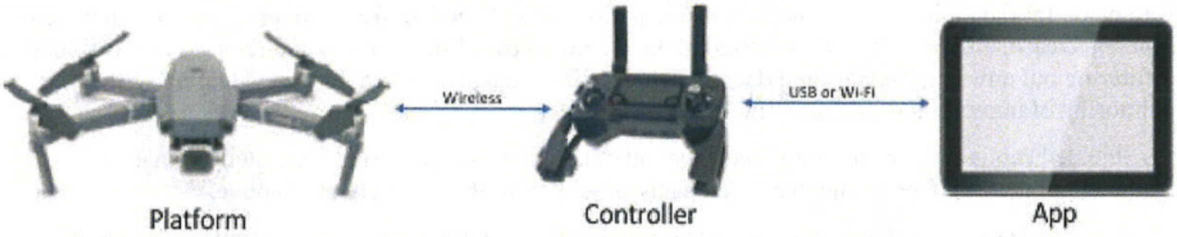

Figure 5. Typical UAS architecture.

Typical Architecture Communication

The controller is central to all communications of the system. The controller communicates via a control signal or some other type of digital command to the platform. The platform responds to commands given over the wireless connection, which is usually a proprietary command set and may be transmitted over a common industry standard wireless protocol, such as wide-band and FHSS protocol, or via something as simple as Wi-Fi, or in some emerging cases, Zigbee. The controller typically receives telemetry and video if the platform is configured with a camera. The video data is typically streamed to the controller separately from the telemetry data and—in most, if not all, cases—separately from the control signal. The telemetry and video data are usually packetized data. The controller sends a data

[d] https://www.parrot.com/us/drones/anafi.

stream directly to the app using either a USB-connected cable or Wi-Fi connection, depending on the controller, how it is configured, and based on manufacturer design or some type of customization (**Note:** The GE does not support Wi-Fi). The app may or may not be connected to some other network and may or may not operate unless there is some type of authentication or access control mechanism that could be centralized in a cloud application or Internet-based server.

The exception to the typical architecture in this report is Parrot's ANAFI platform, which acts as the central point of communications via Wi-Fi at 2.4 GHz. The Wi-Fi access point is built into the aircraft and the controller connects to the aircraft instead of the opposite. In addition, the app connects to the aircraft as well and can be used exclusively without the controller. Many low-end, consumer grade systems use this architecture.

General Security Analysis Approach

There were two main areas examined for data leakage. The first was the communications transmissions between the three basic UAS components from a wireless perspective. The second was via network access by the controller and/or app, if any, to determine if any data leakage exists, which may require an app behavior with binary review, and controller behavior with firmware review and, possibly, via reverse-engineering of the components.

Wireless Communications Analysis

This section addresses the analysis environment, the hardware and software tools, and the processes used to perform the wireless communications analysis.

Radio Signal Analysis Working Environment Laboratory

Analysis work was performed in an RF-shielded chamber in the laboratory, even though the signals are in the industrial, scientific, and medical (ISM) bands, generally speaking, to avoid interference with Wi-Fi or other office-type radio signal operations, thus avoiding interference by the same operational equipment. ISM radio bands are typically unlicensed, but regulated by the FCC, and are often quite congested. The work area and building contains numerous operational Wi-Fi access points. As such, many other experiments involving radio signals in the ISM bands were also ongoing, so considerations were made for the radio spectrum neighborhood in order to collect data from the target systems that were as pure as reasonably possible. This increased the effectiveness of the analysis and reduced the workload of filtering out unwanted signals and data. Isolation of the signals is critical to the evaluation so that the monitoring of unpublished signals could be performed.

Shielded cabling was also used to reduce or attenuate radio signals being generated by analysis equipment in the chamber, as much as reasonably possible, for the same effect as above.

The chamber was used to contain licensed signals, such as GPS L1 signals, to simulate operational environments. Almost any signal can be transmitted in the chamber, licensed or not, since it does not interfere with other transmissions in the laboratory or externally in the surrounding area; therefore, no FCC licensing or National Telecommunications and Information Administration (NTIA) authorization was required to perform these tasks.

The chamber is capable of shielding frequency signals from Direct Current (DC) up to 60 GHz at or near 100 decibels (dB) of power. A certification of attenuation effectiveness was completed by ETS-Lindgren, the manufacturer of the chamber, in 2014. The transmission power levels of laboratory equipment were less than 10% of the chamber maximum and were not higher than 6 GHz of the radio frequency, which were well within the protection limits of the chamber.

Radio Signal Analysis Tools

Several pieces of equipment were used when performing radio signal analysis in the laboratory. Hardware tools were purchased off-the-shelf, while additional software tools were also used for further analysis.

The hardware tools used for this analysis include:

- A Tektronix RSA306B Spectrum Analyzer attached to a Microsoft Surface Pro 4 to control operation of the spectrum analyzer hardware and to display radio frequency and signal plots using various methods, up to 40 megahertz (MHz) wide in real-time and snapshot frequency at one-second intervals for wider than 40 MHz of spectrum width. Higher fidelity analyzers are available, but the RSA306B was more than adequate for the task.
- Dell Precision laptops with Wi-Fi hardware capable of going into 'Monitor' mode to capture Wi-Fi signals, if any. The Wi-Fi hardware is designed with the Atheros chipset. Laptops are loaded with the Linux operating system with various software tools as noted below.
- Wi-Fi dongles built-in with the Atheros chipset.
- National Instruments/Ettus B210 software defined radios (SDRs) with coverage from 70 MHz to 6 GHz RF transmit and receive at full-duplex, and up to 56 MHz of continuous bandwidth on USB power.
- Great Scott Gadgets HackRF One, with coverage of 1 MHz to 6 GHz radio frequency transmit and receive at half-duplex, and up to 20 MHz of continuous bandwidth on USB power.
- A Yaesu FTA-750L aviation navigational transceiver, capable of receiving various aviation signals and GPS radio signals. Primarily used to monitor GPS simulation environment.
- General purpose USB-based GPS receivers for monitoring GPS signals on analysis equipment computers.
- Wi-Fi access point within the RF-shielded chamber with Internet access. The access point has a wired-connection via fiber-optic cable that eliminates RF-leakage as opposed to when Ethernet cabling is used through the chamber shielding.
- Appropriate antennas that cover the expected frequency ranges from 1 MHz to 6 GHz.

The software tools used for this analysis include:

- A Tektronix SignalVu-PC for Microsoft Windows, which allows the analyst to perform vector signal analysis, locate signals in spectrum, review radio signal waveforms, and analysis using real-time and mixed-domain oscilloscopes within the software. The software is capable of presenting signal characteristics, such as power level and statistics of various modulations within amplitude, frequency, phase, time, and analog modulations.
- A GNU Radio Companion (GRC), which is primarily used with an SDR to build and design specific radio protocols that have the ability to capture and transmit based on a 'flow graph' that the analyst models in the graphical environment. For this project, it is being used to capture raw signal data and then to 'replay' that data for further analysis.
- Wireshark is used for packet capture (PCAP) data analysis, which can be used to determine security implications of the data, such as encryption usage, if any. In this case, demodulated signal data converted to PCAP format was required.
- GPS SDR Sim was used to generate simulated GPS radio signal data to simulate an open-air environment in which the UAS equipment is operated.

- General purpose GPS monitoring software, such as gpsmon (GPS Monitor) and gpsd (GPS Daemon), which can be installed in most Linux operation system variants, may be used.
- An Aircrack-ng suite of tools, specifically airodump-ng, were used to capture and demodulate Wi-Fi packets for both the 2.4 and 5.8 GHz bands. Airodump-ng can capture data on a specific channel or set of channels and dump the data into PCAP-formatted files for later analysis in Wireshark. The data can also be directed into Wireshark to remove the file-saving step. The tool will be used to monitor Wi-Fi, if any, on all channels including channels 13 and 14 in the 2.4 GHz ISM band, which are non-U.S. channels, according to the Wi-Fi rules of the FCC for the U.S. All channels will be monitored in the 5.8 GHz band, as well.
- Geographic information system (GIS) mapping software, such as Google Maps, Google Earth, or another mapping application, to overlay the map with the simulated location of the platform. This may also be used to determine simulated locations for the platform to 'fly' in during the chamber analysis.

Radio Signal Analysis Process Overview

These are the high-level steps that were taken to perform an analysis of the radio signals transmitted by the UAS system:

- A study of the operation of the platform being assessed by using printed documentation or online information provided by the manufacturers, third-party experts, and professionals.
- A further analysis of radio channels and protocols used by exploring the FCC licensing, if any, and related information in the FCC database. Usually the device contains or is labeled with an FCC ID that can be used to pinpoint the FCC submission. Online documentation can reveal a general radio spectrum band to search for the specific channel of the platform. If protocols are mentioned in the documentation, this provides a way to determine the demodulation/modulation method of the signal into data that could be captured in a file that could be post-processed, depending on the protocols used.
- A sweep of the target spectrum band and an analysis of the radio signals to determine the center frequencies using laboratory spectrum analyzer equipment.
- Once the determination of the center frequency of every signal on each platform is determined, then the signal data is captured using data tools capable of receiving the signal and collecting the raw data or demodulated PCAP-formatted data into files on the local file system of a general-purpose computer.
- Raw data can then be further analyzed to determine if the manufacturer designed their protocol using established standards, which may be demodulated for further analysis.
- Raw data can be used for playback to determine if the device is vulnerable to playback attacks.
- PCAP-formatted data will be analyzed at the protocol level.

Platform Preparation

In order to simulate an open-air environment within the RF-shielded chamber and to operate the platforms without causing damage to rotors and other parts of the platform hardware, the rotors were removed and the platforms were secured in a safe position.

Most platforms require a position in a three-dimensional location space in order to operate, so a GPS signal must be provided to operate properly. A dynamic signal to simulate latitudinal, longitudinal, and elevational movement was provided.

Note: This may or may not provide the actual environment necessary to determine if malware or data leakage is present in the platform, controller, and/or the app since, generally speaking, malware, in many cases, will not operate in a simulated environment if it is detected.

Security Analysis of Radio Signal and Data

In order to determine the effectiveness of the security of specific platforms, several testing vectors are incorporated into the process:

- As part of the radio signal analysis process outlined above, the raw data can be captured using SDRs and replayed to determine effects of repeated data streams to the platform. This is a commonly used method in network penetration assessment to determine if the server and/or applications are tracking data with a sequence or synchronization ID/counter to mitigate replay attacks and to help determine if the data is encrypted or not. This method is also effective in determining operational disruption effects as a means of doing simplistic protocol jamming.
- Using the acquired signal and/or data for analysis in order to determine the modulation of the data so that, if possible, demodulation may be performed to some level. Since the platforms use and transmit both telemetry and video data, this analysis step will determine if open-air capture will uncover any sensitive data-streaming from the platform to the controller and the controller to the app.
- If a standard non-encrypted modulation has been determined by an attacker, all data becomes exposed and would be very easy to determine platform IDs, telemetry data, control data, or destinations of data to and from the platform, to and from the controller, or to and from the app, which may be connected to a network or the Internet.
- The network, if any, will also be monitored for any possible data leakage from connected apps, if connected at all.
- GPS effects are determined by setting the environment with a fixed-position GPS signal, as well as a dynamic GPS radio signal to simulate movement with dynamic latitudinal and longitudinal positions. This will test the location effects, if any, on the platform and provide a simulation environment for the platform to operate in. This also has implications on whether or not a simulated GPS signal can affect a platform or not. Various locations were chosen to determine if location provides a vector of leakage.
- As part of the Wi-Fi PCAP analysis, if any, further Wireshark packet analysis of the data was performed to determine if destinations other than the desired location exists. This also determines the effectiveness of the security configuration, if any.

App and Controller Firmware Analysis

This activity was composed of several activities to determine data leakage, most likely, at a network level and perhaps a high-level review of binary file elements to determine if malware exists in either the app or the controller firmware. This activity was performed within scope and task scheduling permits.

Network Monitoring

As the systems were assessed, wireless and wired networks were monitored and analyzed for data leakage. Logs, if any, were accessed and analyzed on the controller, in the app, and in the operating systems of the app and networking components.

Reverse-Engineering

One area of concern is reverse-engineering on certain elements of the app and the controller firmware. Reverse-engineering was scoped to limit the amount of effort. Much can be learned from just the system configuration once the firmware has been opened and exposed to the analyst. Only a small subset of binary executables and configuration files were assessed. This subset will be determined and documented during the preliminary examination and then targeted.

The app and its contents were exposed and reviewed similarly to the firmware. Again, much can be determined by reviewing the static configuration of the app that is not allowed by the user. In addition, a small subset of binary executables were chosen for deeper analysis using the following binary reverse-engineering tools.

Exported Data Analysis

An analysis of exported data was executed to determine if any exposure, exploits, or embedded binary executables existed. Encryption methods were also analyzed.

Note: Since the evaluation systems were used for this overall task, a system that oversees operational use was taken out of service to provide the best scenario for review.

The following is a list of the basic hardware and software tools that were used to perform the analysis activity. The laboratory has access to equipment that will allow for firmware extraction and chip-level inspection of device hardware using various electronics debugging adapters, de-soldering stations, high-fidelity microscopes, and/or chip removal and dissection tools. The laboratory also has access to a numerous set of software tools related to firmware extraction, binary file dissection instruments, reverse-engineering devices, and deep executable binary analysis tools.

Hardware Tools

- If required and if time permitted, firmware extraction tools were used—depending on the chipset and hardware configuration of the platform, controller, and hardware interface was used—that could have been either an inter-integrated circuit (I2C) bus, a serial peripheral interface (SPI), a Joint Test Action Group (JTAG), etc.
- Network taps to monitor transmission control protocol (TCP)/Internet protocol (IP) network traffic.
- Routers or switches configured to monitor all traffic and capture it.
- USB taps or proxies for those apps and devices that are connected via USB.

Software Tools

- Wireshark to analyze network traffic captured during an assessment run.
- Ida Pro or Ghidra or other binary reverse-engineering software.
- Other numerous binary extraction and analysis tools to expose embedded files within a firmware file structure.
- Malware analysis tools and/or sandboxes to review files for possible malware patterns, exfiltration, or external network accesses, if any.
- App operating system specific tools to monitor network traffic, if any.

Formal Documentation and Reporting

As each system is analyzed, careful documentation of the following areas will be noted in a separate findings document:

- System being analyzed, manufacturer name, firmware version, app version, etc.
- Radio center frequency, if any.
- Radio or network protocol.

- Possible exploit or identified leakage.
- What is being leaked?
- Method used to find or discover the leakage.
- Affected files, binaries, logs, and their names.
- External destinations, if any, found or captured.
- Conditions such as location, elevation, and simulated or real.
- Vector.
- Impact.
- Attack vector.
- Attack or leakage complexity.
- Privileges required.
- Likelihood of exploit.
- Mitigations and or best practices.
- Description of leakage.

LIMITED-SCOPE ANALYSIS FINDINGS

Review of Communications Protocols

The analysis team at INL performed a short literature study on Lightbridge and Ocusync communications protocols in preparation for further hands-on research and analysis of the platforms being assessed [.11][.12]. These two technologies appear frequently in the DJI manuals and specifications. Simple searches found literature and video on both technologies. Some of the literature includes discussion and analysis of interference of spread spectrum communications as used in unmanned aircraft vehicles (UAVs), as well as a security analysis of FHSS [.13],[.14], which is the basic protocol used by many platforms, but specifically those products manufactured by DJI. The Autel device also uses FHSS, but does not use any branding of the technology to market it. However, based on preliminary analysis, it looks similar to DJI's technology. The goal of this small review of their protocols was to understand the technology of the platform in question and to understand FHSS of UAVs in general. No effort was made to develop any techniques to duplicate the numerous studies that have already been performed due to the limited scope of this analysis.

According to DJI and Refs. [.15],[.16],[.17], and [.18], Ocusync is the next generation of Lightbridge. DJI is transitioning from Lightbridge to Ocusync to reduce hardware manufacturing costs and upgrades through the use of SDR-based architecture, which will incorporate more software-defined functions and less hardware-defined components. The Matrice 600 Pro currently uses Lightbridge 2.0, while the Mavic Pro is configured with Ocusync. Both technologies use FHSS for the control signal and encrypted Orthogonal Frequency Division Multiplex (OFDM) for the video stream. There are subtle differences between the radio signals and modulation of each technology, but they are essentially the same waveforms between the platform and the controller. As such, this report will not distinguish between the two and refer to both of them as FHSS. The Mavic Pro has the capability to switch between 2.4 GHz and 5 GHz spectrum automatically, while the received Matrice 600 Pro operates at 2.4 GHz only.

No literature references could be found for the Autel system that provided details of the FHSS designed into their products. However, spectrum analysis revealed the FHSS operating on their systems appears to be in the 2.4 GHz band from the controller to the platform. Video streaming waveform also looked similar to DJI's systems.

The Parrot system does not use FHSS, but does use Wi-Fi for all of its operations, including video streaming. According to their documentation, the system has a range of up to two and a half miles, which would require an environment of no interference from other radio frequency signals and physical objects and is not as much of a problem relative to the other systems in this report. Compared to FHSS, using Wi-Fi limits the flight range of the Parrot system and is more sensitive to radio frequency signals in the same band, much like Wi-Fi access points are affected in an office environment. FHSS, on the other hand, is a very robust signal that is less affected by interference from radio signals in the same frequency and has a much greater range of flight distance.

Setup DJI Matrice 600 Pro, DJI Mavic Pro, Autel EVO, Parrot ANAFI, and Associated Tablet/Phone Applications

The Matrice 600 Pro (see Figure 6), Mavic Pro (see Figure 7), Autel EVO (see Figure 8), and Parrot ANAFI (see Figure 9) platforms were setup within the laboratory inside of the RF-shielded chamber. In order to test and evaluate the platforms and provide a physically safe operational environment, the rotors on each platform were removed, while leaving each motor intact for full rotational function. The DJI platforms were supplied with DJI GE firmware in both the aircraft and the controller. The Autel EVO and Parrot ANAFI were supplied commercially off-the-shelf from DOI with no special editions for government use.

DJI tablet/phone commercial applications were also installed on Android phones and tablets. DJI GE hardware and software were supplied and installed as well. Autel and Parrot apps were installed on phones and tablets from an app store. This was done to perform access control integrity between the commercially available application versus the GE version only available to USG agencies and departments. A commercial account was setup with DJI so that the commercially available application could be installed and used in these tests, which would occur against the government-supplied platforms and controllers as noted above. No commercial accounts were necessary to operate the Autel and Parrot apps, although the companies may be relying on app store account information to realize user data, but this was not investigated. However, the Autel and Parrot systems operated freely without requiring authentication to vendors' servers as required by DJI commercial apps. DJI GEs do not require authentication to DJI servers.

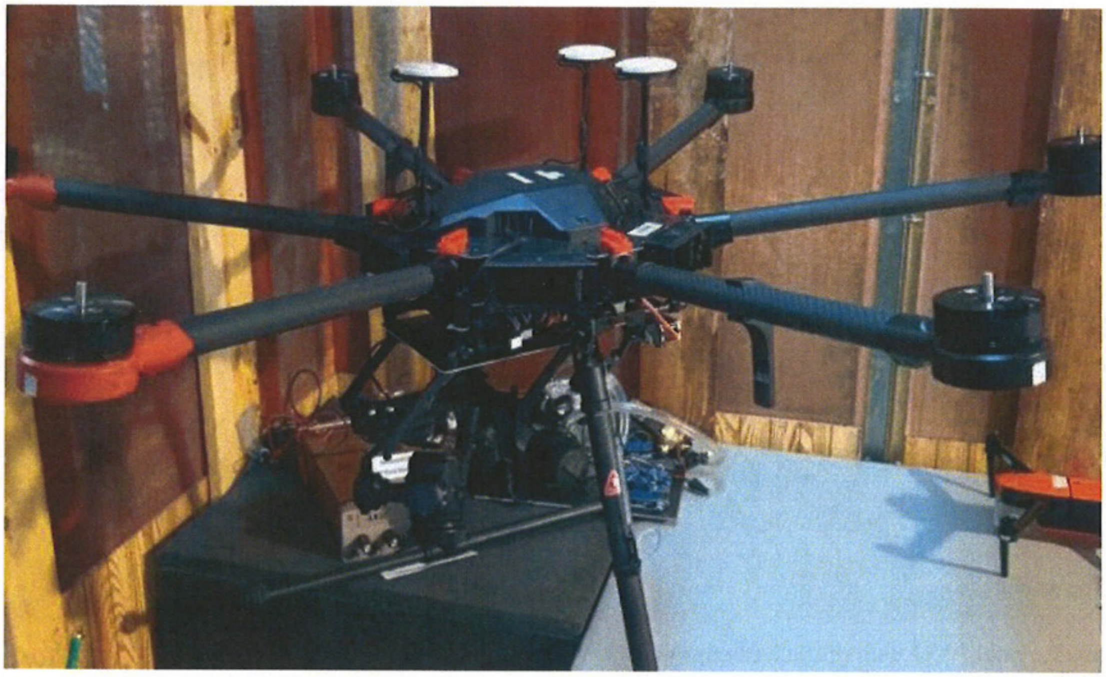

Figure 6. DJI Matrice 600 Pro within the RF-shielded chamber with propellers removed.

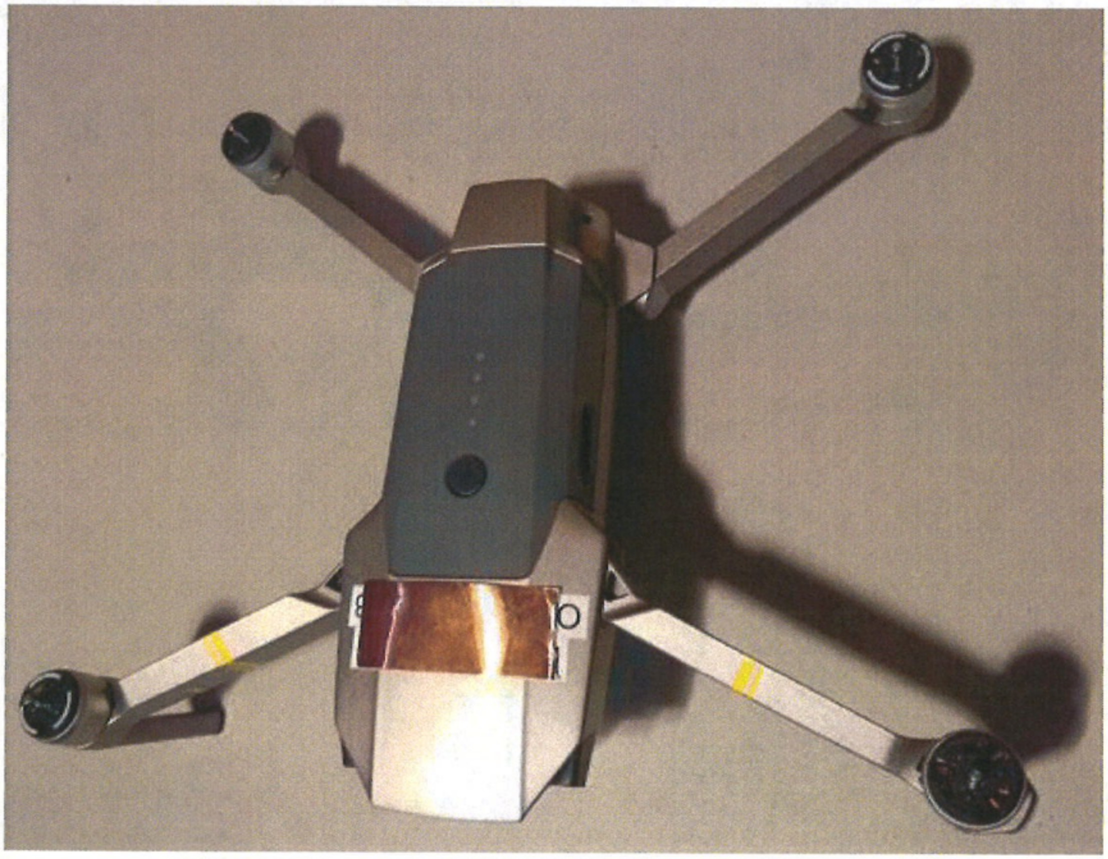

Figure 7. DJI Mavic Pro with propellers removed.

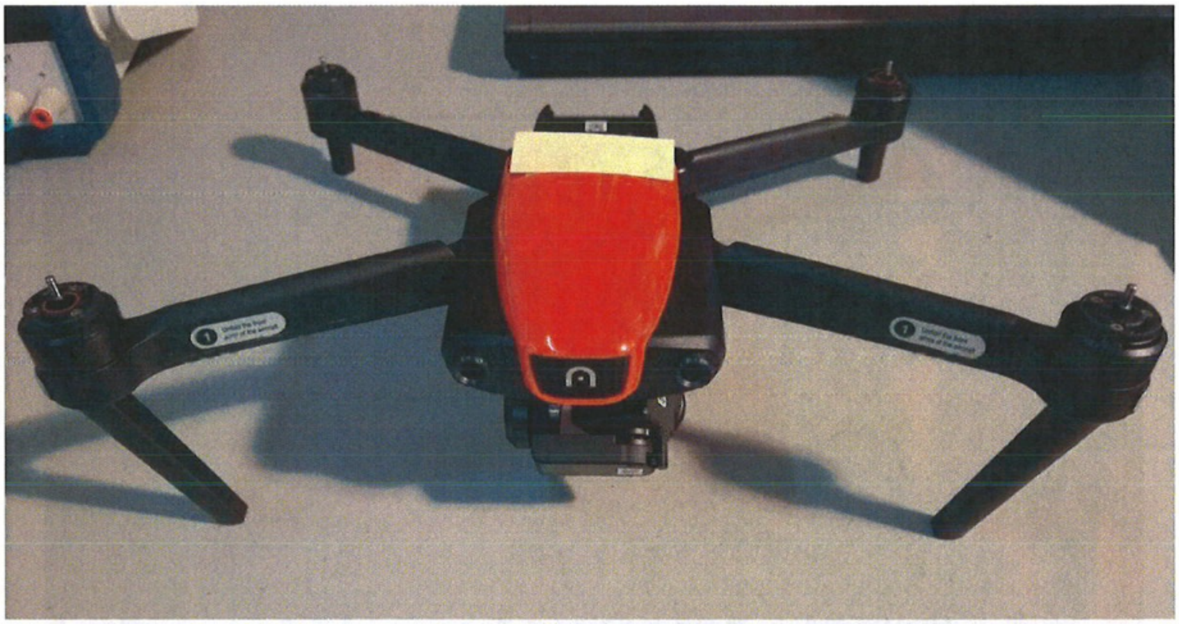

Figure 8. Autel EVO with propellers removed.

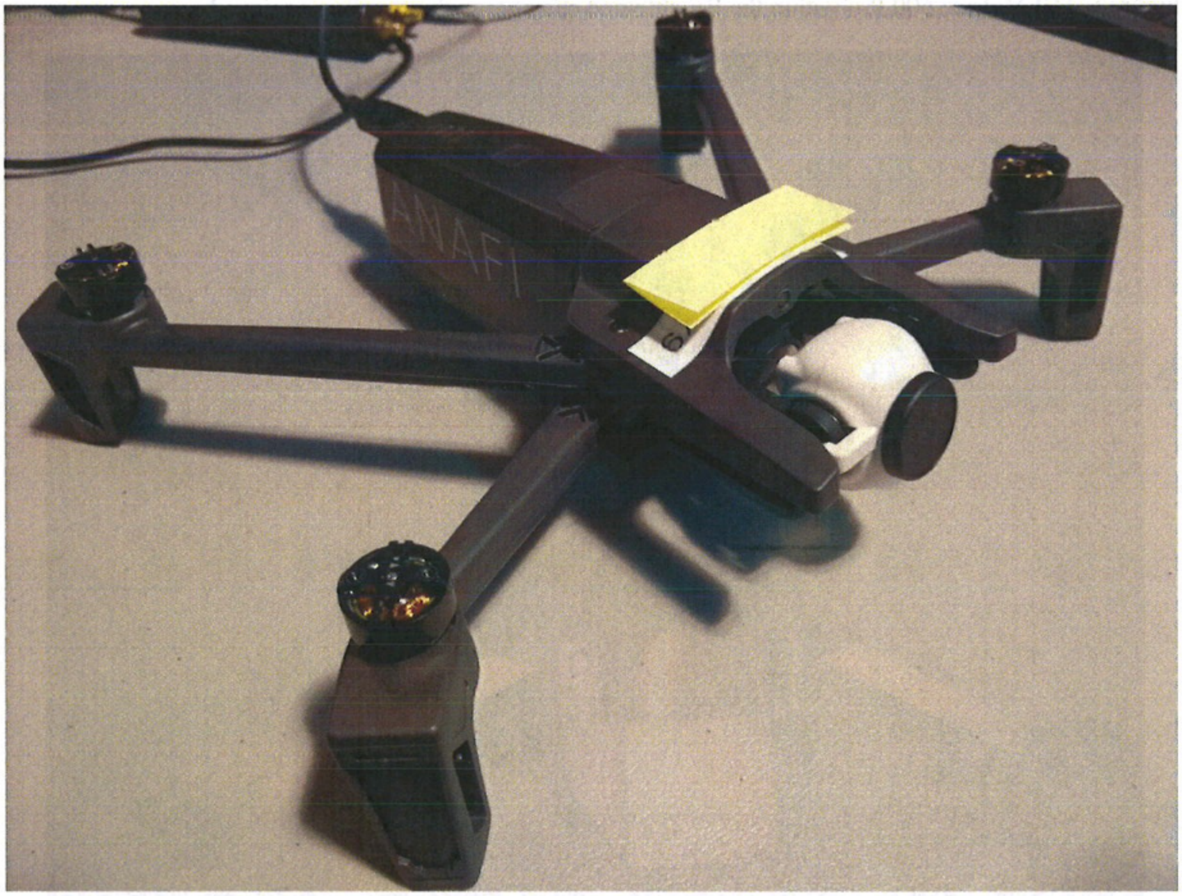

Figure 9. Parrot ANAFI with propellers removed.

Setup GPS Simulation Environment

The motivation for setting up the GPS simulation signal was to provide an environment that could virtualize the outside world and coax the platforms into operation so that the devices would not go into operational modes without GPS, which would make them behave differently than in a real outdoor operational environment that DOI pilots would be exposed to. A github project called gps-sdr-sim was used with heavy modifications to provide the simulation environment.

Since there are several wireless research projects collocated in the same laboratory environment, GPS testing and simulation equipment needed no installation or setup for this analysis. The GPS simulator can be configured to simulate a single static location so that a GPS receiver can calculate its position relative to the given signal. The simulator can also be configured to provide a set of locations so that a GPS receiver can calculate its position over this set, so that it appears to the receiver to be 'moving' within an X, Y, and Z coordinate plane relative to the signal, at speed, according to the deltas between the individual locations and frequency of receipt as provided by the simulator and transmission by the SDR.

Spectrum Analysis of Platforms

The analysis included the use of a Tektronix RSA306B spectrum analyzer (see Figure 10) attached to a Microsoft Surface Pro 4 tablet. This is the recommended configuration given by Tektronix for this analyzer, which reduces cost and provides mobility and flexibility in analyzing waveforms in an environment internally or externally. The UAS platform signals are well within the capabilities of the spectrum analyzer to detect minute signal transmissions and channel changes. The key aspect of the tool was to visually characterize the signals of the platforms signal(s) within the spectrum.

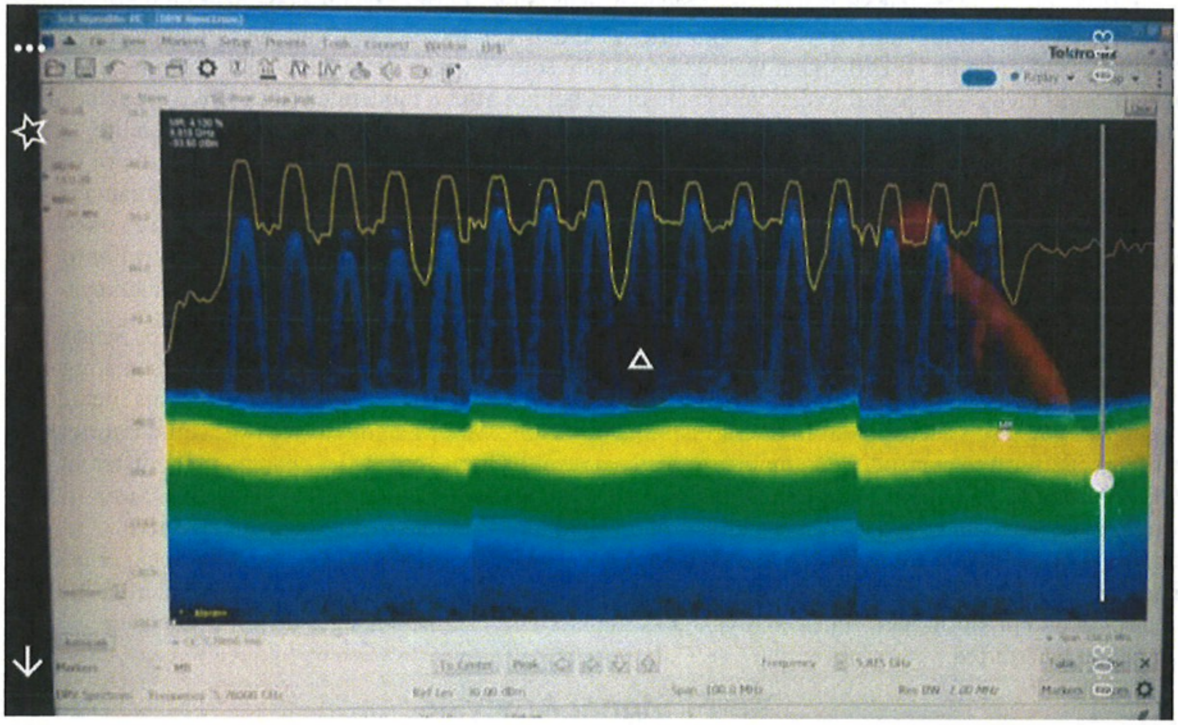

Figure 10. Ocusync waveform on the Tektronix RSA306B.

The spectrum analyzer identified a large bandwidth signal in the 5 GHz range for the Mavic Pro. Except for the Parrot device, the platforms use 80 MHz of bandwidth with a singular control signal of 10 MHz channel-width that switches channels using FHSS across the entire band. The signal frequency for the Mavic Pro seems to be fixed and is centered at 5.78 GHz, which is within the 5 GHz ISM band boundary. On the Matrice 600 Pro and the EVO, the signal is within the 2.4 GHz band.

As a side note, ISM bands are used by many manufacturers of radio equipment due to the bands being unlicensed, but regulated by the FCC. This also allows consumers/pilots to use these devices without the requirement of a FCC radio license. FAA requirements still apply to pilots operating these devices.

As discussed above, the Lightbridge/Ocusync signal provides control, telemetry, and video data. The control and telemetry data are transmitted over FHSS, while the video is transmitted via encrypted OFDM. Initial views of the FHSS signal were attempted with SDRs, such as the HackRF One and Ettus B210. Due to the width of the FHSS band and the speed of the channel switching, viewing the signal with anything other than a spectrum analyzer is beyond the capability of most consumer-grade SDR hardware. Higher-end SDR hardware costing a magnitude more could possibly work, but the available spectrum analyzer made this work much simpler. It also made it much less likely that the FHSS signal would be compromised with entry-level SDR equipment. More sophisticated or faster digital signal processing (DSP) equipment would likely be used in this case and be very specialized. This is not to say that entry-level SDR equipment couldn't be used to cause interference or effects on the platform or the controller, but to take control would require more sophisticated efforts and expense. Further discussion on SDR effects appears later in this report.

The spectrum analyzer displayed an OFDM signal when video-streaming was activated. According to the DJI documentation, this stream is supposed to be encrypted. Further reverse-engineering work would be required to determine the encryption algorithm used between the platform and the controller. In addition, capturing the OFDM signal would also require some work to demodulate the streaming data, which could then be subjected to decryption attempts, but not after a moderate effort. One caveat to this, though, is that there is no apparent way to configure the encryption or set an encryption key on the platform between the controller and the platform, so, theoretically, if the encryption key is static or there is no encryption key but only encoding of the data, then the possibility exists that the video stream could be compromised. This effort falls outside the scope of this analysis and would likely involve reverse-engineering of the protocol and/or a review of the firmware on both the platform and the controller to discover the method of encryption, if any, and the method of storage of security certificates and keys.

The frequency of the OFDM signal is not fixed as the controller appears to attempt Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol in an attempt to de-conflict with existing signals (for example, Wi-Fi or other radios) in the preferred frequency. One of the experiments included configuring a Wi-Fi access point to the same frequency as the OFDM signal to see if it would interfere with the platform to controller communications. This resulted in the controller changing to a different OFDM frequency to begin communications. No attempt was made to interfere on all frequencies as this would have been out of scope for the analysis and would likely not have resulted in an effective interference of flight operation since the platform is controlled by FHSS and is less likely to experience interference. However, the video stream may experience interference from an external signal after the controller and platform perform CSMA/CA at startup because channel changes do not occur after operation has started.

Wi-Fi Signal Analysis

The Parrot ANAFI and the commercial version of the Mavic Pro are designed to communicate via Wi-Fi or USB. The Matrice 600 Pro's only method of communication is by USB to the app; as such, no further discussion is required for the 600. The Autel Evo does not have Wi-Fi connection capability. With the GE of the controller installed on the Mavic Pro, no Wi-Fi is available for configuration.

A Wi-Fi scan revealed that no Wi-Fi transmissions emanated from the GE configuration of either the platform or the controller in question. Commercial versions of the Wi-Fi access point for the Mavic Pro 2 is configured with wireless protected access 2 (WPA2) encryption and a weak default password, which could easily be cracked with penetration testing tools in a relatively short time, so use of the GE firmware was warranted. It would also be best practice to not use Wi-Fi to connect to the controller from the app if, for some reason, Wi-Fi was made available by default. Operators should be cautioned about its use and should take appropriate measures to either disable Wi-Fi and use a wired connection or mitigate the issue by configuring strong pre-shared keys/passwords and limit exposure to unknown entities, if possible.

Since the Parrot system does not use FHSS for any communications, a Wi-Fi access point is built into the platform. Wi-Fi scans revealed WPA2 beacons emanating from the platform even while the controller was switched off. Having the access point built into the platform makes it possible to operate the system from either the controller and/or the app. The analysts assume the Parrot system comes preconfigured with a password from the factory, but have no idea regarding the strength of that default password. The fact of the matter is, if a new password is to be set, the controller has to connect to the platform first, and then a password can be set within the controller and the platform. In addition, the password has to be propagated to the app. It appears there is no function within the app to change the password. Theoretically, if the Parrot system is configured with a weak password or a default password from the factory, then it will require a password change before any operational use. If not changed, weak or default passwords may be revealed with simple Wi-Fi cyber-penetration tools in a very short time.

The analysts assume that if the platform uses any Wi-Fi for control and video streaming, such as what is found in the Parrot system, then it will be subject to much more accidental and intentional interference and, possibly, cyber-exploitation than a system designed using FHSS and may also affect flight range, since Wi-Fi has a theoretical range limit, which is a lot less than the FHSS would be. A best-practice recommendation would be to not use any UASs with Wi-Fi as a communications medium.

FHSS Signal Replay Analysis

One of the targets of this analysis was to determine if the video stream and/or telemetry data is replay-able against the UAS. In order to perform this exercise, a GRC Python script and SDR were setup to capture the Lightbridge/Ocusync raw signal data in an attempt to analyze it further and to perform a replay analysis. On a side note, only a short duration of time can be captured since signal data capture accumulates extremely large amounts of data in the hundreds of megabytes to gigabytes per second. Once the raw signal data was captured and saved into files, another GRC script was executed to replay the signal from those files. With the platforms operational, the signal data was replayed and the effects were noted. After several attempts, the video stream remained unaffected within the controller and/or app with no impact or interference in the visible display. However, the telemetry data was somewhat affected by the replay exercise as it would change, somewhat, from the play in progress to what was being replayed. The theory for this was that the video stream may be unaffected due to the claim that it is being communicated over encrypted OFDM, while the telemetry data may not be protected either with no encryption or packet sequencing. It may be that the FHSS control signal is not fully protected. More extensive testing activity should be performed to determine the extent of the data protection, if any.

GPS Signal Effects

In order for the platforms to operate similarly to an operational outdoor environment, a spoofed-GPS signal is generated in the environment, relative to the laboratory's current location. With this configuration, latitude, longitude, and altitude will be conveyed in a simple L1 signal of 1575.42 MHz, since most GPS receivers will operate without L2 and other signals. We discovered the platforms will operate on a simple L1 signal. We verified the operation of the location of the platform, as it was displayed in the controller and app versus no location since the RF-shielded chamber does not allow external signals to be received.

Since the platforms worked with the simulated GPS signal, the assumption was made that our testing efforts were sufficient to presume that most any GPS spoofing would work on the platforms. As we were testing other functions of the platforms, other experiments were occurring within the shielded chamber that required a dynamic or 'moving' GPS signal. As a result, the GPS signal from the other project affected the behavior of one of the platforms. In effect, the platform was traveling at a high rate of speed in an oval with a circumference of about 12 miles centered on the laboratory. The display portrayed this behavior with rapid movement over a map and as positional data changing according to new positions received and showing a high rate of speed in excess of 500 MPH, clearly beyond the limits of the platforms, unless you consider an anomalous high-wind weather pattern. One conclusion to the GPS effect was that the GPS receivers on the platform are very sensitive and will lock into just about any GPS L1 signal in a very short amount of time. In addition, speed is not a factor in the operation of the limitations of the devices. None of the geo-fencing features were tested in this evaluation, but could be at a later time to determine if the device's behavior would change due to the spoofing tests.

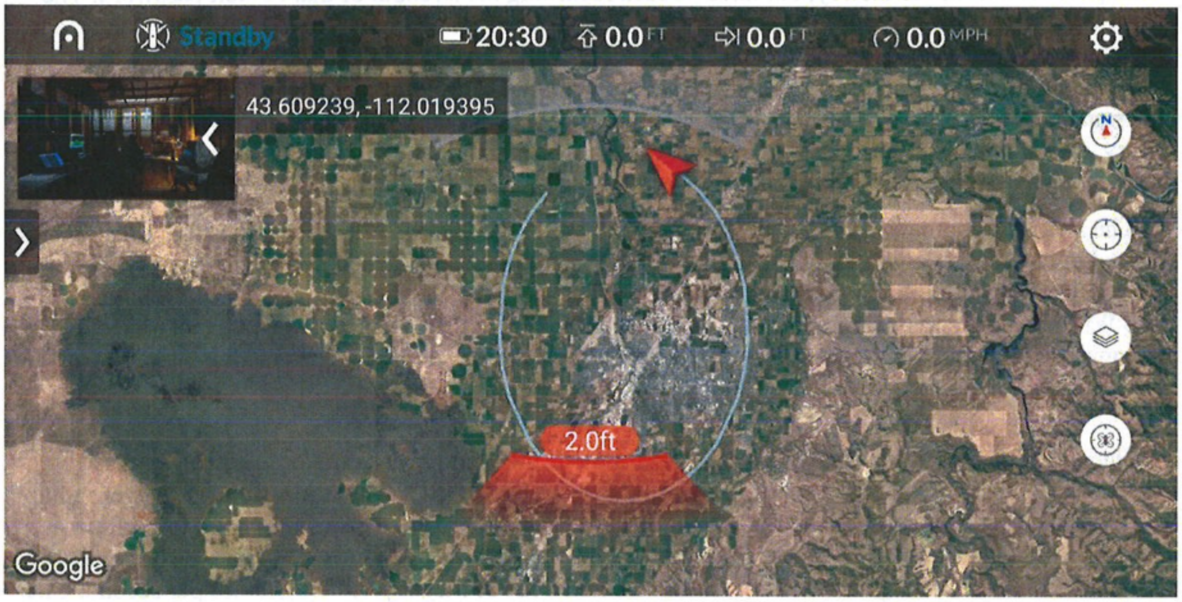

Figure 11. Screen shot showing GPS effect on the Autel EVO.

There was one limit that was discovered on the Autel EVO that the other platforms did not exhibit. There appears to be a flight distance limit that made the system somewhat inoperable. The exact number was not determined, but a limit of around 15,000 horizontal feet was exceeded. Apparently, when this limit is reached, the system automatically goes into a landing state. However, with dynamic GPS movement (see Figure 11), the system was unable to land using the automatic landing feature. Setting the system to manual landing mode could not be performed either. Finally, the dynamic GPS signal had to be set to a static location so that the platform could land. Figure 12 shows the maximum distance and speed of the Autel EVO.

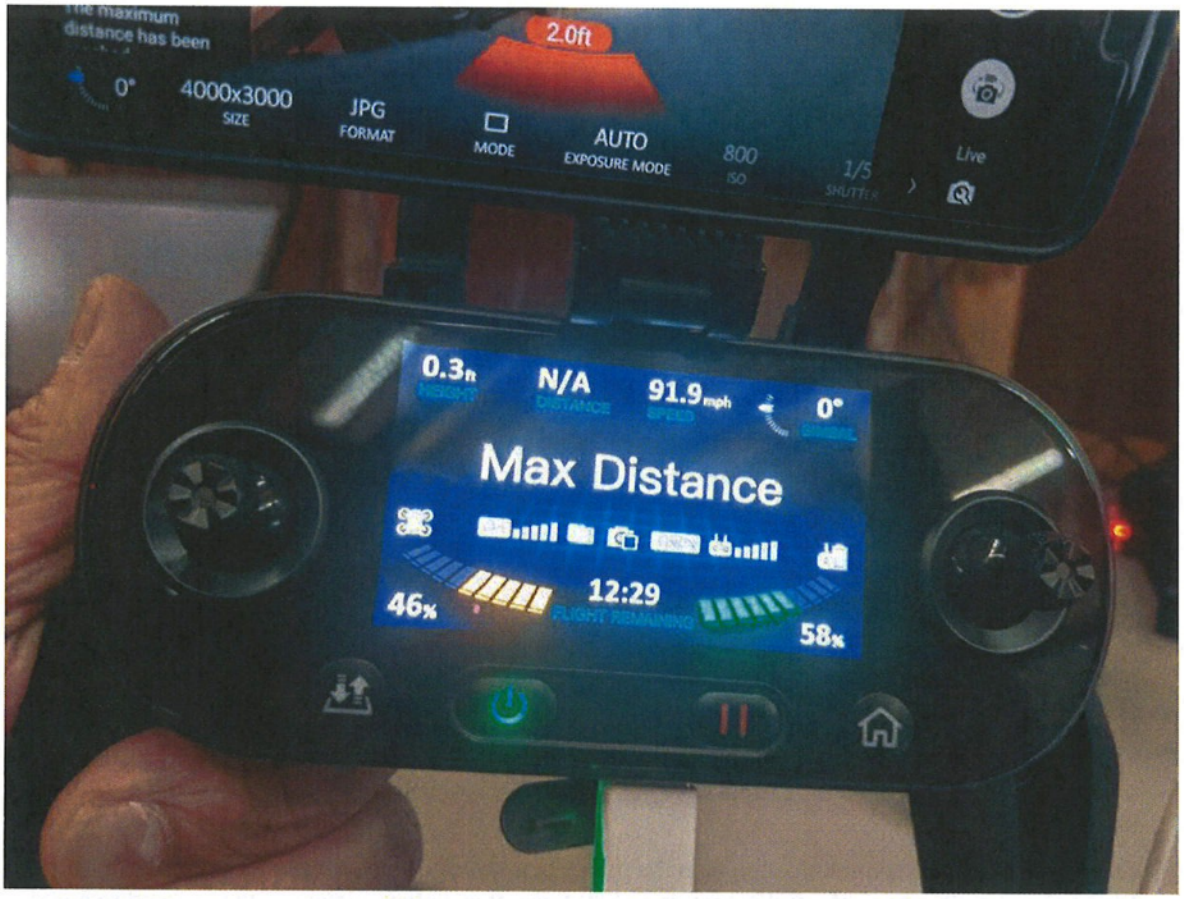

Figure 12. Max distance and speed of the Autel EVO.

App Security Analysis

Two editions of the DJI app were tested—the GE app and the commercially available app. The commercial version is what is available for download at public app stores and interfaces to the controller either by USB or via Wi-Fi, depending on the platform and its configuration. The GE is only available to be used by USG entities with specialized firmware installed on the controller and the platform.

Only the commercial editions of the app were available for the Autel EVO and the Parrot ANAFI. Unlike the DJI commercial app, no authentication or registration was required to fly the UAS. Although there may have been an indirect registration when downloading the apps via app store requirements, no further registration was required. Operation of the systems was allowed without any external network connectivity.

The DJI commercial app operation was tested against the GE controller and platform. Configuration to operate the app with the controller could not be completed, so no further testing was required due to the incompatibility between the two.

Network access and traffic were analyzed and no data leakage or attempts to connect to Internet services were found within the interference-free analysis environment.

ANALYSIS LIMITATIONS

Due to the short duration within INL's interference-free analysis environment, a deeper examination of the hardware, software, firmware, and wireless signals could not be performed. It is recommended that further protocol analysis of the data and telemetry stream be performed to reduce the security risk.

Since the rules of engagement did not allow invasive analysis of the systems, a deeper and more invasive analysis of the platforms and controllers were prevented. As noted above, a UAS that has been used out in field operations would allow a more deep and thorough cybersecurity inspection of its systems.

RECOMMENDATIONS UAS CYBER-THREAT MITIGATIONS

Best Practices

- Formal configuration management practices should be used to track the changes to hardware, firmware, and any other software being used to operate a UAS. Software may include the app, the operating system, and other unrelated apps installed on the handheld device. If possible, implementing a change control reporting process should definitely be employed to track hardware replacements, firmware updates and versions, app versions, and dates of installation and upgrades or patching, and most importantly those who made changes and who authorized them.
- A USB connection from the app to the controller should be used whenever possible, instead of through a wireless connection, such as Wi-Fi or Bluetooth.
- If Wi-Fi must be used, the use of strong passwords (i.e., no dictionary words, using a mix of upper and lower case alpha characters, numeric characters, special characters and a long length according to organizational policy) should be used. Changes to passwords should be implemented on a frequent basis.
- The use of FHSS for communication with the platform is strongly encouraged as opposed to using Wi-Fi or some other type of wireless protocol. FHSS is not as vulnerable out of the box and requires much more sophistication to attack effectively since it uses a wide-band and incorporates high-speed frequency hopping. FHSS is still vulnerable to attack, but not nearly as vulnerable as Wi-Fi, Bluetooth, Zigbee, or other similar protocols are because they are very well known, the frequency bands are much narrower than those used in FHSS, and they are within the bandwidth of many cyber-hardware and software tools. UAS FHSS should not be confused with Bluetooth FHSS as it has a much shorter range.
- Make cybersecurity hygiene of data handling a priority, especially with USB flash drives, network connectivity, and application hygiene on handheld devices where the app is installed.
- Isolate app devices and do not allow multipurpose use of the handheld devices to be used to operate UASs. For example, do not use a tablet to access email or the Internet and then use it as part of the UAS operational environment.
- When upgrading firmware and apps, perform a cybersecurity analysis on a subset representative of the fleet of UAS devices once the devices are upgraded, or a more invasive analysis of the software files and firmware that are part of the upgrade.
- Perform consistent and frequent analysis of UAS network traffic, if any.
- Use a defense-in-depth strategy to guard against the infiltration and exfiltration of UAS operational data. If possible, use air-gapped networks to store data if classification requirements warrant it. Reduce or eliminate connectivity to the Internet directly from the app and/or the app host and the controller.

- If applicable and appropriate, update any encryption keys and security certificates as frequently as configuration management policies allow. The higher the frequency of change, the more the risk is reduced.

Procurement Considerations

Supply chain management is a very large and complex problem. As mentioned before, the manufacture of UAS devices is a process involving many designers and suppliers from all across the world. Very few systems are actually designed and built in the U.S. due to the higher costs to produce individual components. Most of the procurement opportunities make their way from foreign manufacturers, which have very low labor costs that can perform the same labor for pennies on the dollar. Without bringing manufacturing back to the U.S. purely on cybersecurity grounds, a defense-in-depth strategy must be incorporated along with a robust cybersecurity T&E of products with periodic sampling of the fleet to determine data leakage, if any.

CONCLUSION AND PATH FORWARD

At a glance, the four platforms analyzed within an interference-free environment do not appear to be leaking any data.

Short-Term Actions

Perform continuous risk analysis and create a defense-in-depth strategy to mitigate the potential for data leakage. No data leakage was found during the limited-scope analysis, but that does not mean it cannot happen with the right conditions and circumstances. DOI's published flight test and technical evaluation report of July 2, 2019, does speak to this by applying additional risk mitigation layers. The report also points out the interim nature of the current GE solution and DOI's continuing work toward a long-term, cloud-based solution that is Federal Risk and Authorization (FedRAMP) compliant.

Perform follow on testing of operational UASs from the DOI. The operational system will have gone through real-world usage and logging and may have embedded data needing to be analyzed. The target systems perform data logging, which will need to be evaluated to determine if the behavior of the system and its security level are adequate.

Long-Term Actions

In addition, the following long-term actions are strongly encouraged:

- Protocol analysis of the data and telemetry stream be performed for many platforms and not just the ones listed in this report.
- High-level software reverse-engineering of an operational system to determine security level and posture of the app's communication subsystem and confidentiality/data integrity algorithms.
- Perform high-level firmware reverse-engineering of an operational system to determine the same results of the software reverse-engineering above.
- To further the depth of analysis, a high-level hardware reverse-engineering of an operational system to determine the same results as the two bullets just above.
- Further configuration management analysis and mitigations to ensure confidentiality, integrity, and availability of the systems.
- Perhaps perform a supply chain verification to determine the path of delivery and increase integrity and reduce risk as much as reasonably possible.

REFERENCES

1. Goldman Sachs & Co. LLC, "Drones: Reporting for Work," Goldman-Sachs, 2016. Available at: https://www.goldmansachs.com/insights/technology-driving-innovation/drones/.

2. Castellano, F., "Commercial Drones Are Revolutionizing Business Operations," TopTal, 2019. Available at: https://www.toptal.com/finance/market-research-analysts/drone-market.

3. U.S. Department of Interior, "Unmanned Aircraft Systems (UAS) Program 2018 Use Report," 2018, Available at: https://www.doi.gov/sites/doi.gov/files/uploads/doi_fy_2018_uas_use_report.pdf.

4. Mac, R., "Behind the Crash of 3D Robotics, North America's Most Promising Drone Company," Forbes, 2016. Available at: https://www.forbes.com/sites/ryanmac/2016/10/05/3d-robotics-solo-crash-chris-anderson.

5. Joshi, D., "Commercial Unmanned Aerial Vehicle (UAV) Market Analysis – Industry trends, companies, and what you should know," Business Insider, 2017. Available at: https://www.businessinsider.com/commercial-uav-market-analysis-2017-8.

6. Valentak, Z., "Drone Market Share Analysis & Predictions for 2018 – DJI Dominates, Parrot and Yuneec Slowly Catching Up," Drones Globe, 2017. Available at: http://www.dronesglobe.com/news/drone-market-share-analysis-predictions-2018/.

7. DroneVideos, "Drone Company Autel, Giving DJI a Run For Their Money," June 17, 2019. Available at: https://dronevideos.com/drone-company-autel-giving-dji-a-run-for-their-money/.

8. Nene, V., "Microsoft Rallies Behind DJI in Drone Litigation with Autel Robotics," DroneBelow, November 26, 2018. Available at: https://dronebelow.com/2018/11/26/microsoft-rallies-behind-dji-in-drone-litigation-with-autel-robotics/.

9. Kim, A., Wampler, B., Goppert, J., Hwang, I., and Aldridge, H., "Cyber-Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles," Purdue University, Sypris Electronics, 2012. Available at: https://www.researchgate.net/publication/268571174_Cyber_Attack_Vulnerabilities_Analysis_for_Unmanned_Aerial_Vehicles.

10. Humphreys, T., Ledvina, B., Psiaki, B., O'Hanlon, B., and Kintner, P., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," University of Texas at Austin, 2008. Available at: https://repositories.lib.utexas.edu/handle/2152/63316.

11. Mad RC, "DJI Mavic 2 – Ocusync 2.0: What is it & What's Compatible? + How is it different from Lightbridge?," YouTube, 2018. Available at: https://www.youtube.com/watch?v=gfqcSv9sR0A.

12. PhillyDroneLife, "Ocusync vs Lightbridge Face-Off: Who Wins?," YouTube, 2018. Available at: https://www.youtube.com/watch?v=H7XUyHeIrmM.

13. Pärlin, K., Alam, M., and Moullec, Y., "Jamming of Spread Spectrum Communications Used in UAV Remote Control Systems," Tallinn University of Technology, Estonia, 2017. Available at: https://digi.lib.ttu.ee/i/file.php?DLID=9378&t=1.

14. Shin, H., Choi, K., Park, Y., Choi, J., and Kim, Y., "Security Analysis of FHSS-type Drone Controller," WISA 2015 Revised Selected Papers of the 16th International Workshop on Information Security Applications, Volume 9503, pp. 240–253, 2015, School of Electrical Engineering, KAIST, Daejon, Republic of Korea. Available at: https://dl.acm.org/citation.cfm?id=2950219.

15. DJI, "Mavic Pro User Manual V2.0," 2017. Available at: https://dl.djicdn.com/downloads/mavic/Mavic%20Pro%20User%20Manual%20V2.0-.pdf.

16. DJI, "DJI Assistant 2 Release Notes," 2017. Available at: https://dl.djicdn.com/downloads/dji_assistant/20190327/DJI+Assistant+2+Release+Notes(1.2.5).pdf.

17. DJI, "Matric 600 Pro User Manual v1.0," 2017. Available at: https://dl.djicdn.com/downloads/m600%20pro/20180417/Matrice_600_Pro_User_Manual_v1.0_EN.pdf.

18. DJI, "DJI Assistant 2 for Matrice Release Notes," 2019. Available at: https://dl.djicdn.com/downloads/dji_assistant/20190527/DJI+Assistant+2+For+Matrice+Release+Notes(2.0.8).pdf.