EDGESOURCE
Solution Focused • People Driven

SECURITY RISKS OF THE AEROSCOPE UPGRADE MODULE WHITEPAPER MARCH 2024

Abstract

In late 2023, Da Jiang Innovations (DJI) released new AeroScope firmware and sent hardware "upgrade modules" to their dealers for customer distribution. Edgesource Corporation (Edgesource) is conducting a reverse-engineering analysis of the new hardware and updated firmware for the AeroScope system. This whitepaper provides an overview of security risks and considerations of the AeroScope system, the upgrade module, and DJI drones. In the Appendices we provide an overview of how a DJI drone system works and interacts with the AeroScope.

This document provides a detailed understanding of the AeroScope system fundamentals, including a technical overview of DJI's proprietary telemetry protocol Drone ID, some well-known AeroScope system vulnerabilities (such as spoofing, software, and hardware supply chain concerns), and a general technical overview of the changes introduced by the new upgrade module.

The purpose of this whitepaper is to educate, advise, and inform readers about the system's features, explain how it operates, dispel common myths and inaccuracies, and discuss security risks. The primary objective of this document is to help all interested parties understand the changes made to the system and the implications of these updates. It also emphasizes the importance of applying effective security measures to these systems, consistent with best practices for all removable hardware for other computer and security systems.

A technical addendum to this whitepaper will be released at a later date, available upon request to approved audiences. The addendum will cover our reverse engineering findings, including firmware and hardware analysis, detailed interface enumeration, a comprehensive evaluation of cryptographic processes, and any other technical details we discovered during our physical inspection of the dongle and all associated firmware updates.

Special thanks to Steve Tisseyre of Aerial Defence, Ltd., David Kovar of URSA, Inc., and Mario Behn of NATO NCIA for their peer reviews and collaboration.

About Edgesource. Since 1997, Edgesource has specialized in providing research, development, test, and evaluation; system engineering and integration; software development; and defense and intelligence services to the U.S. federal government. We collaborated with the Defense Innovation Unit, Defense Digital Service, Joint Counter-UAS Office, and Air Force Research Laboratory to develop the Windtalker™ C-sUAS Sensor System and the Dowding™ Common Operating Picture (COP) system which is deployed with an Authority to Operate (ATO) globally to DoD and federal customers. Our Windtalker™ sensor includes the first secure, cyber-hardened, deployment of DJI AeroScope based on extensive reverse-engineering, analysis and testing.

TABLE OF CONTENTS

TABLE OF FIGURES

CHANGE LOG

Date	Revision
03/01/2024	Original publication

ACRONYMS AND DEFINITIONS

ADS-B	Automatic Dependent Surveillance–Broadcast: A broadcast of telemetry data commonly employed by very large, unmanned aircraft, as well as manned aircraft (such as passenger airlines, cargo aircraft, and even military aircraft in certain airspaces)
ASD-STAN	The industrial association which establishes, develops and maintains European standards on behalf of European aerospace & defence industry.
ASTM	ASTM International
ATO	Authority to Operate
C2	Command and Control
COP	Common Operating Picture
COTS	Commercial off-the-shelf
C-sUAS	Counter Small Unmanned Aircraft Systems
CRYP	Cryptographic Key Exchange Packets in the Drone ID encryption process
DJI	Da Jiang Innovations
DOC	Declaration of Compliance
DSP	Digital Signal Processor
FAA	Federal Aviation Administration
GHz	Gigahertz
GPS	Global Positioning System
JCO	Joint Counter-UAS Office
KEM/DEM	Hybrid Encryption Procedure,
LLVM	Low-Level Virtual Machine, open source compiler and toolkit for building compilers, which are programs that convert instructions into a form that can be read and executed by a computer.
NDAA	National Defense Authorization Act
OcuSync	DJI's proprietary high resolution video transmission solution
OEM	Original Equipment Manufacturer
PRC	People's Republic of China
RC	Remote Controller
RDT&E	Research, Development, Test, and Evaluation
RF	Radio Frequency
RTH	Return-To-Home
UAV	Unmanned Aerial Vehicle
USB	Universal Serial Bus
UUID	Universally Unique Identifier

THE AEROSCOPE AND DJI DRONES

Until recently, the relationship between drones manufactured by Da Jiang Innovations (DJI) and passive Radio Frequency (RF) drone sensors was relatively transparent. The DJI Drone ID signal was unencrypted which made it reasonably easy to detect and open to analysis. This bidirectional openness was perpetuated by DJI's development and sale of the AeroScope sensor specifically to provide the ability to detect their own DJI-manufactured drones in action.

However, early in 2023, rumors started circulating that DJI would no longer manufacture the AeroScope. In March of that year, the product was temporarily pulled from their public website. This sent ripples across the counter small unmanned aerial systems (C-sUAS) industry as speculation grew about the future of this capability, which is relied upon widely across both industry and government. At time of this publication, although the AeroScope remains on their website, global sales appear to have come to a halt. Speculation is that this decision is tied to operations in the Ukraine and internal and external political pressure.

In September 2023, DJI began (via its dealer network) distributing hardware upgrade modules to all AeroScope customers to install on their units. This module (sometimes called a "dongle") is in the form of a USB hardware component with unknown firmware installed. Very little explanation was given for the release of the module and distribution was sporadic and sometimes hampered by lack of information about current owners of fielded AeroScopes.

Most recently, starting in January 2024, DJI began encrypting the Drone ID signal emanating from their newer released models such as the Mavic 3 Series, Mavic Mini 4 Pro and the Avata Pro (when upgraded to the latest firmware). It is not clear yet if DJI will push out encryption to older models such as legacy Mavic Series, Phantom Series, or earlier Mini versions that are globally popular.

It is now understood that one of the vital functions of the AeroScope upgrade module is to decrypt the newly encrypted signal from the DJI drones, so that the sensor can continue to identify them.

But several questions remain –

What else does the upgrade module do?

What unforeseen code or commands lies within?

What are the risks of upgrading or not upgrading these sensors?

These questions and others are what this whitepaper sets out to address.

1.1 TO ENCRYPT OR NOT ENCRYPT, THAT IS THE QUESTION

In September 2023, the news that DJI would begin encrypting the Drone ID data was met with a mixture of reactions. Because DJI drones also broadcast the Federal Aviation Administration's (FAA), ASTM, or ASD-STAN Remote ID (if required by jurisdiction), the impact of encrypting Drone ID may not be directly apparent. After all, isn't Remote ID (RID) supposed to provide for all of the same data elements as Drone ID did, most critically the operator location?

The most significant difference between Drone ID and RID is the underlying physical protocols. While Drone ID is integrated within DJI's proprietary OcuSync protocol (for all newer models), RID makes use of standard WiFi and Bluetooth protocols. By and large, this means that while Drone ID has historically been detectable for many kilometers (sometimes as much as 30+), Remote ID will not – and is likely to achieve 1-2 km max (when in good physical conditions). Coupling this range restriction with network congestion and noise, the protocol is likely to be extremely difficult to distinguish when in dense crowded environments (such as a stadium or an urban city-center).

Beyond the range implications, Remote ID is a relatively new standard, and as such, is currently fraught with implementation differences from vendor to vendor, which make reliable detection of the protocol a challenge. Beyond this, full networks of sensors that only detect RID to address the range limitations are not currently feasible at scale, and will require continued investment to bring online.

All of these limitations will adjust over time, and it is likely that RID will settle into a more widespread and reliable system, but until that occurs, existing protections are critical to remain working – and Drone ID remains one of those.

WARNING

DJI's new hardware upgrade module supports the addition of encryption to its existing AeroScope data signal, which was previously unencrypted. Adding encryption will impact **all** systems that rely on the DJI drone signal for detection, beyond just the AeroScope system.

Along these lines, both of these protocols invoke a similar, and heated discussion: the juxtaposition of the privacy of drone pilots and the security efforts of state, local, federal, and private security entities. With that brief background, and before we discuss further with respect drones, lets step back and look at recent example of a Privacy vs. Safety dichotomy.

Jack Sweeney, a student at the University of Central Florida, has made a series of viral social media accounts that post specific updates regarding the locations of the private jets of a variety of high-profile individuals, such as Elon Musk and Taylor Swift. Both Swift and Musk have threatened Sweeney legally regarding these posts, citing their own personal privacy and safety concerns. Sweeney, however, has taken the position that his work is based upon public data, data that is available to everyone who wishes to retrieve it (particularly ADS-B data); whose purpose is to provide overall understanding of air traffic for continued safety and air security purposes.

This simple situation demonstrates the competing interests; namely individual privacy versus safety and security of a large number of airlines and aircraft. This example is almost a direct match for concerns raised by many drone pilots about the RID and Drone ID standards. On the one hand, privacy rights advocates applaud the ability to fly drones without displaying the location of the drone operator; especially to a broader public, for this reason. However, they are joined by malicious actors who also desire to fly drones as weapons, perform reconnaissance against their adversaries, or transport drugs or contraband without displaying the location of the drone operator.

In the case of legal, commercial, or hobbyist drone flights, most infractions such as entering a no-fly zone over a stadium event are due to lack of understanding of laws and regulations, not because of nefarious actions. In those cases, the ability to identify the location of the drone operator enables first responders to interact with the operator and remove it from flight without offensive mitigation or danger to the community.

In the case of illegal activity such as drug trafficking, it is vital that law enforcement agencies are able to identify the location of the drone operator and not just the drone location, which may be many kilometers away from the pilot. Encryption of this data, with provision of those decryption secrets to vetted entities with law enforcement purpose only, would prevent the general public from misusing the information; and would also enable law enforcement to access the data they require. But it also injects additional unreliability, and worse, since implemented by an adversarial nation, presents potential opportunities for influence with respect to which aircraft are detected and when.

Outside of the civilian market, drones are valuable to both military purposes and wartime humanitarian relief efforts, and the Drone ID broadcast reveals sensitive information about the operator and the drone itself. Depending on “which side” is being considered, we must remember that if drones and Drone ID data are useful to the “good guy”, they are also useful to an adversary. This is a familiar cat-and-mouse game that we play with all technology, and it is further exacerbated by the use of readily available off-the-shelf commercial drones for military purposes.

Finally, for those concerned with the military applications of drone spoofing, encryption does present an additional barrier to creating a realistic spoof that can confuse or overload detection. However, our analysis of the new DJI Drone ID encryption is that this will not present much of a burden on spoofers, meaning that **the benefits of encryption do not extend to a reduction in spoofing**.

1.2 GLOBAL TENSIONS

Although there is no official reason provided by DJI as to why sales of the AeroScope ceased in 2023, there is much speculation that the drone-heavy conflicts in the Ukraine, as well as increased tensions in other parts of the globe are at the center of this decision.

For example, there are credible reports that the AeroScope has enabled Russia to target Ukrainian drone operators (**Figure 1**), while at the same time the functionality of the AeroScope may have been throttled or disabled when in use by Ukrainian forces. This is significant because DJI-

manufactured drones are well established as a preferred tool for not only surveillance and spying, but also as weapons in these conflicts.

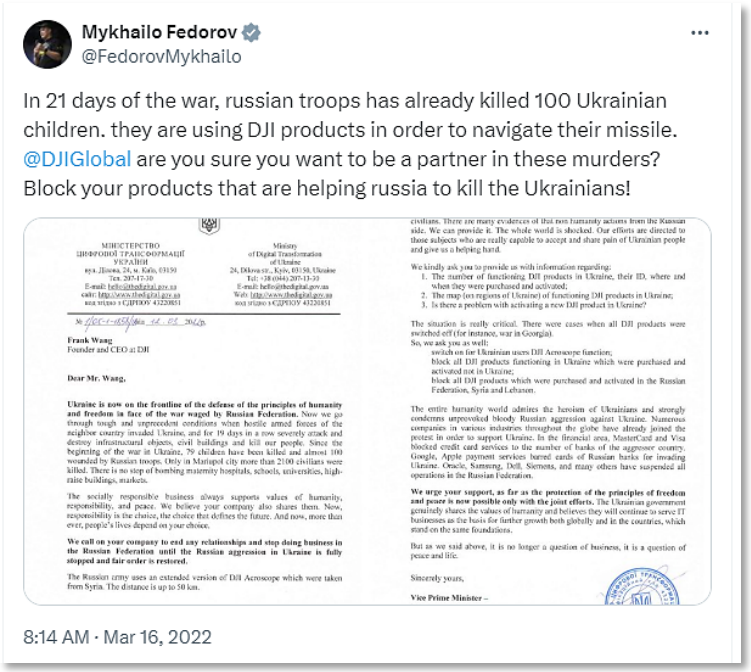


Figure 1: Ukraine Accuses DJI of Enabling Russia, 2022. Mykhailo Federov, Vice Prime Minister for Innovations, Development of Education, Science & Technologies — Minister of Digital Transformation of Ukraine, called out DJI on X (formerly Twitter) for partnering with Russia.

As the use of small drones is becoming prevalent in many conflict zones, there are actors who obviously do not want their drones to be tracked by sensors and do not want their adversaries to be able to spoof drones and throw them off track. **In short, drone operators want to spoof, and drone defenders do not want to be spoofed.** And both parties are extremely likely to be using the same technology, which makes a one-size-fits-all solution impractical.

WHAT IS DJI AND WHY IS THERE A SECURITY RISK?

As a Chinese company headquartered in Shenzen, DJI has faced scrutiny for many years regarding the security, usability, and dependability of their products. DJI manufactures commercial unmanned aerial vehicles (drones) for aerial photography, videography, and other commercial and hobbyist applications. It also designs and manufactures camera systems, gimbal stabilizers, propulsion systems, enterprise software, aerial agriculture equipment, and flight control systems.

Despite concerns about the origins of these products, DJI maintains absolute dominance in the small drone market, accounting for as much as 80% of the world's commercial small drone sales. Their drones are so pervasive that in 2017 DJI won an Emmy Award for the use of its camera drone technology in the filming of popular shows. Around that same time, U.S. police and fire departments began purchasing DJI drones, joining the federal government in their use.

The development of the AeroScope further solidified DJI's position in the C-sUAS market, by providing an extremely cost-effective solution compared to other RF-based systems. And while the AeroScope is a physical device, it relies upon a lower-level protocol for its data from the aircraft Drone ID. **Decoding this signal is the underlying component in many RF-based detection systems, not just the AeroScope.**

Within the U.S. Department of Defense (DoD), nearly all Commercial off-the-shelf (COTS) drones have been restricted in usage since 2018, when the Deputy Defense Secretary signed a memorandum halting their use across the Department, with some exceptions. This restriction, originally internal policy only, was codified in 2020 when the National Defense Authorization Act Sec 848 included a provision banning foreign-made COTS drones. In January 2021, President Trump issued an Executive Order that required an extensive review of the Chinese-made drones in U.S. government fleets, and DJI was later added to the Department of Defense's National Defense Authorization Act (NDAA) Section 1260H entity list of adversary military companies operating in the U.S. While designation on the Section 1260H list alone has no current legal consequences, Section 805 of the FY 2024 NDAA, passed in December 2023, imposes new contracting restrictions on DoD with respect to entities on the Section 1260H list or any entity subject to the control of such an entity. Implementing regulations for this law are forthcoming by DoD[1]. The NDAA further stipulates that DJI drones may only be utilized if they have approved mitigation software installed such as Rizer™ developed by Edgesource.

As a China-domiciled company that manufactures products that can and are used for military purposes, the company certainly has some ties with the People's Republic of China (PRC) government. The PRC, of course is also a close partner to countries that the U.S. and our allies are in conflict with, including Russia, North Korea, and Iran. Because DJI is such a dominant force in both drone and drone sensor manufacturing, they have a stake in both sides of conflicts and can

[1] Akin Gump, Feb 5, 2024. DoD Updates Section 1260H List of Chinese Military Companies Operating Directly or Indirectly in the United States.

theoretically influence outcomes by interfering with the capabilities, reliability, or security of their products, depending on who the end user is.

1.3 THE SECURITY RISK BALANCING ACT

The previous ample availability of the AeroScope and dominant market share of DJI drones has led to a misconception that 'the DJI part of the C-sUAS problem' has already been solved thru mitigations and security risk management. This dependence on AeroScope has given a false sense of security to C-sUAS interests, who mistakenly believed that the openness that existed with unencrypted Drone ID data and availability of the AeroScope would remain in perpetuity. This is far from the truth, however, and it is still crucial to continue researching and analyzing any technology developments from adversarial nations, which requires the collaboration of private companies and governments.

At the same time that the U.S. and our allies have become increasingly concerned with the security risks inherent in DJI products, we are faced with the reality that **there continues to be a deficit of domestic manufacturers that offer products and solutions of comparable technological advancement.** As an example, Skydio, a U.S. company, produces a variety of unmanned systems in the United States, but these devices still do not match the capability, affordability, or dependability of the DJI products. While they continue to slowly close this gap, DJI is not standing still. In 2023 alone, DJI released multiple new models of aircraft and docking solutions, increasing the gap between DJI and other commercial manufacturers. While many drone bans or restrictions aim to close this gap further, these approaches all fall short, as they cutoff access to capabilities needed by first responders, warfighters, and consumers in the absence of a comparable alternative.

The U.S. and allied partners need to maintain access to the AeroScope solution based on its superiority in detecting DJI drones.

As such, it has become necessary to develop several risk mitigations for DJI products—ranging from full offline usage to security wrappers—to resolve these concerns. For example, Edgesource has developed the Windtalker™ passive RF sensor that incorporates the AeroScope but firewalls it from external networks, with data stored, tracked and analyzed on our Dowding™ Cloud common operating platform that has been granted an Authority to Operate (ATO) for use on U.S. government networks. For DJI-manufactured drones, we developed Rizer™ and Wraptor™ which slightly modify the aircraft firmware to protect the data. These capabilities enable cyber-hardening of these drones against foreign data transmission and other embedded security risks. These mitigations are allowed through the 2024 NDAA Section 1823(b)(3) exemption which enables the DoD to operate DJI products under limited circumstances.

Key Point

Nearly all DJI vulnerabilities require physical access to the device to exploit, making mitigations practical and impact lower than comparable vulnerabilities with a remote access.

With proper security, thus far, the AeroScope has proven to be an effective tool for military, law enforcement, and commercial entities. As a result, no comparable solution exists in the market today, and the next-best solutions do not have the same range of detection or are reliant on radars and cameras which do not offer the same capabilities or rich data and are also rife with false detections from birds and other airborne objects and particles.

Furthermore, non-DJI RF systems are not compatible with the DJI upgrade module and will not be able to detect encrypted Drone ID drones without the development of decryption technology of their own, the legality of which is often called into question. This reinforces DJI's ascendancy in the RF sensor market by making only *their* AeroScope sensors capable of detecting *their* drones. This move also forces competitors to spend RDT&E efforts on decrypting the Drone ID signal just to restore access to capabilities that we had at the end of 2023, instead of focusing on the next generation of needs.

The challenge addressed in this whitepaper is evaluating the security impact of updating – or not updating – the system with the module, and if updating how to mitigate the potential risk of introducing unknown capabilities, features, or malicious code.

THE AEROSCOPE MODULE PROBLEM

As we've discussed, to ensure compatibility between the AeroScope unit and the hardware module, DJI released a firmware update that must be applied to each AeroScope prior to installing the hardware module via the DJI Assistant 2 desktop application connected to the internet (or a privately distributed offline upgrade variant). Along with Drone ID decryption, this firmware update brought about several internal changes, as it was the first official update for the AeroScope in many years.

The DJI release note provides a very abbreviated, seemingly benign purpose of this new hardware module:

"*Install the upgrade module to the AeroScope Stationary Unit to support the AeroScope system update and ensure that AeroScope is compatible with future DJI aircraft products."*

This new update module, though, should raise several security concerns and questions, specifically for any customer who has purchased any sort of aftermarket "hardened" or "secured" version of the AeroScope that may conflict with the updates. This is especially true for any governmental organization that has a fleet of AeroScopes connected to or accessed by government networks.

1.4 WHY YOU SHOULD NOT BLINDLY PLUG IN THE DONGLE

As with any computer system or other network-attached system, connecting USB-based devices presents various security risks, ranging from introducing unknown code, to shortening the power supply life. In this context, the upgrade module must be physically attached to an AeroScope, which is relatively limited in its access to additional network components and could give a false sense of security that any threats contain in the upgrade would be contained.

It is not definite that the update dongle is inherently bad – but at this point, *we don't know what we don't know.* It is possible, but not certain, that the updates are 100% safe, non-hostile, and contain no sleeper code or malicious functions that can be activated at a later date.

However, it is also possible that the opposite is true and that in addition to the necessary updates to work with the newly encrypted Drone ID data, it could contain malicious code designed to infiltrate networks if the AeroScope is part of a networked solution or degrade functionality for standalone systems. A third possibility is that most of the update modules are completely safe; but that some, strategically distributed modules for specific AeroScope serial numbers contain threats that are unknowingly installed based on assurances that other installations are benign.

Key Point

For users that have AeroScopes installed and connected directly to a local area network, extreme restraint should be followed before installing the "dongle" and updating firmware.

As with all USB drives and other devices, and in accordance with multiple U.S. government cybersecurity requirements, caution should be used when attaching these USB devices to AeroScopes that already have a direct internet connection, as there is any number of potential means by which data might be exfiltrated (or commands provided) to the AeroScope itself.

The most likely reason for DJI deploying a hardware module, such as this dongle, is that hardware is a better means to prevent exposure of the cryptographic secrets necessary to decrypt these packets. Providing keys or cryptographic processes in firmware or software is not a reliable means of protecting those secrets from exposure, while specifically designed hardware security chips do aim to address this challenge. You might liken this upgrade module to a USB crypto wallet, physically designed to maximize protection of the secrets stored within (even when subjected to hardware level attacks).

1.5 WHAT DOES THE UPGRADE MODULE LOOK LIKE?

The upgrade module release is an add-on attachment that connects to an existing AeroScope via its onboard USB port. The upgrade module was released in a fixed site and a mobile unit version. Fundamentally, these are the same in function and operation; their main difference lies solely in the physical form factor. The fixed site version has additional weatherproofing for external attachment to the fixed site AeroScope system. The mobile version is optimized for inclusion in the black mobile AeroScope case, along with the necessary cables for that connection.

(a) Fixed Site Upgrade Module Kit Contents

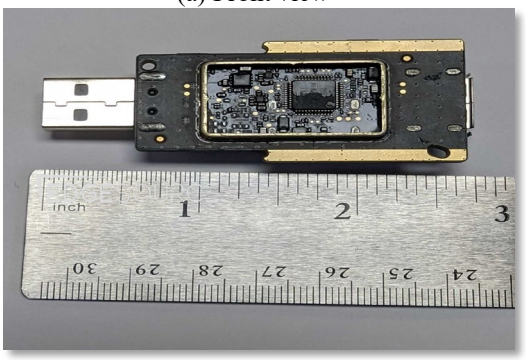
(b) Mobile Upgrade Module Kit Contents

Figure 2: DJI AeroScope Upgrade Module Versions

The upgrade module itself is a small USB drive with DJI's proprietary processing logic. This logic is highly protected by its location within the hardware module as it contains encryption processes and necessary encryption keys for all DJI aircraft. The software was shipped in a physical format to prevent reverse engineering or extraction of those encryption keys. The new upgrade module components are depicted in the picture above in (**Figure 2**).

DJI AeroScope Upgrade Module Disassembled

(a) Front view



(b) Back view; processor removed

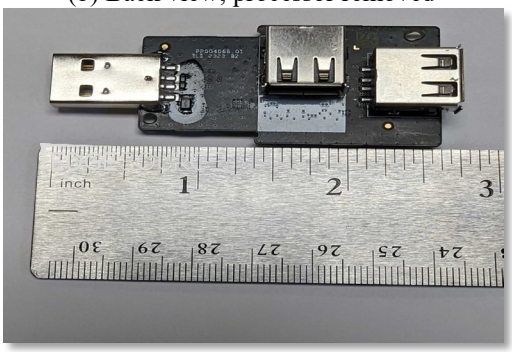


Figure 3: Internal Upgrade Module USB Hub

The AeroScope unit has only one USB port. However, both the unit's fixed site and mobile versions already use that port for other purposes. The upgrade module was designed to solve this problem with a built-in USB hub connecting two devices to the same main USB port. Both sides of this small custom board can be seen in **Figure 3** (a) and (b). The internal processor is depicted below in **Figure 4** after we removed it from the module.

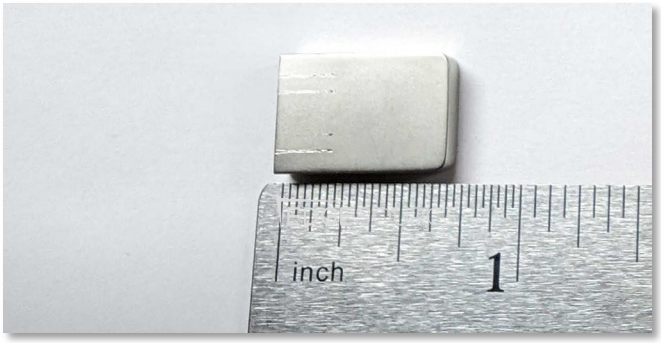


Figure 4: Internal Upgrade Module Processor

1.6 HOW IT WORKS

The following is a brief breakdown of the dongle's operations.[2] Once connected to the AeroScope, the AeroScope onboard firmware will perform an authentication routine. During this multi-step routine, the attached dongle and the AeroScope will exchange a dongle session key, which is used to encrypt all further communications received from the dongle.

[2] Upon approved request, our Technical Addendum will provide a more detailed walkthrough of each process, as well as further annotated photographs of internal components.

- During this process, the session key is exchanged using a public-private encryption algorithm. This public-private keypair is not static and is determined via an adapted key exchange algorithm. This is a security mechanism designed to prevent analysis of captured communications to and from the dongle.
- A significant amount of effort is spent ensuring that the device connecting to the dongle is an AeroScope and that, both before and after connection, listening to communications would yield no information from the dongle

See **Figure 5** for an overview visual of this authentication process.

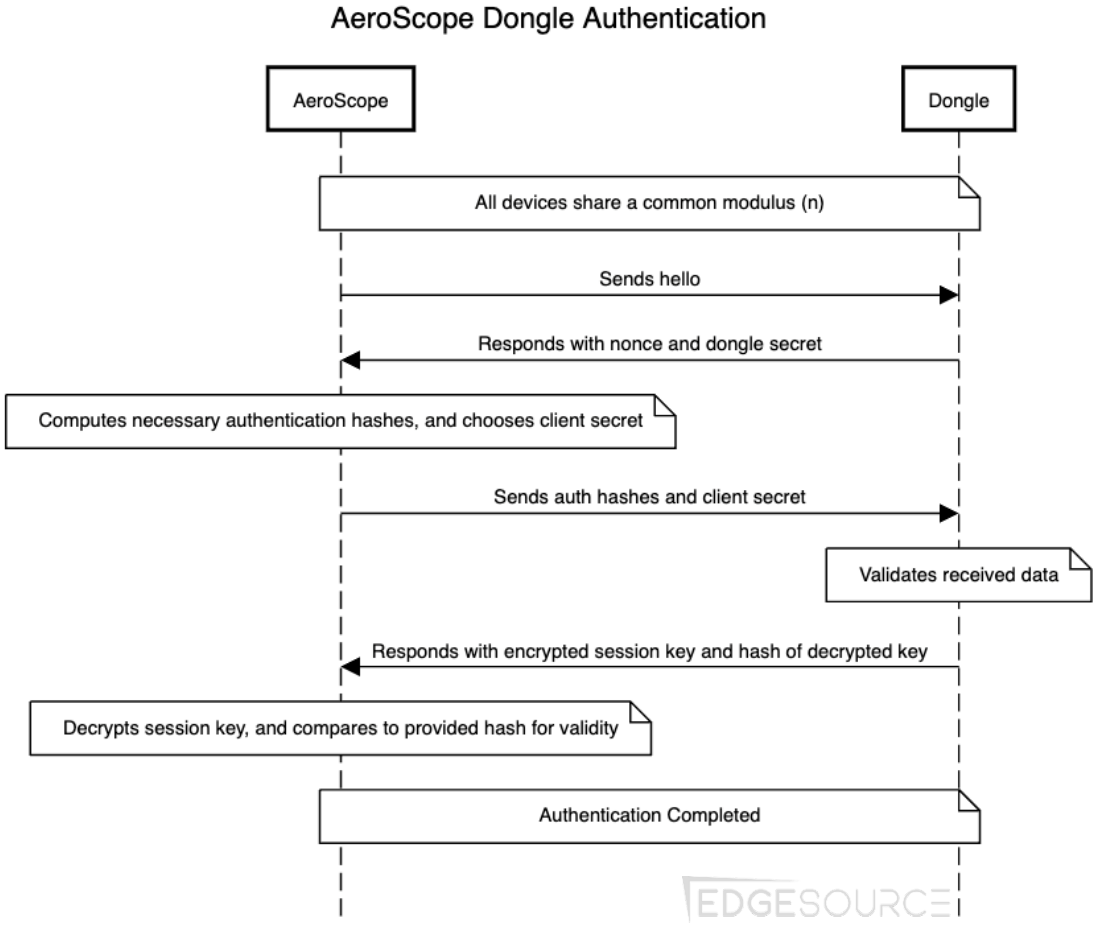


Figure 5: Authentication Sequence

- With an authenticated upgrade module, the AeroScope continues to run like normal – receiving packets of information from older or non-updated aircraft that are not encrypted. These are processed and sent outwards as typical.
- Newer aircraft will send a new cryptographic key exchange packets (CRYP) packet of information that includes an encrypted aircraft session key along with other necessary attributes. This key is generated by the aircraft on boot and is encrypted using an adapted

public-private key scheme. The same key is continually utilized during that boot, and each is identified with a key hash.

- Once the AeroScope receives the CRYP packet, it sends that package of information unmodified along to the upgrade module, which returns the decrypted aircraft session key to the AeroScope.
- The AeroScope stores the aircraft session key along with the unique key hash, and as it receives the original Drone ID packets of data – it decrypts them using this key and the process continues from here as original.

See **Figure 6** for an overview visual of this process.

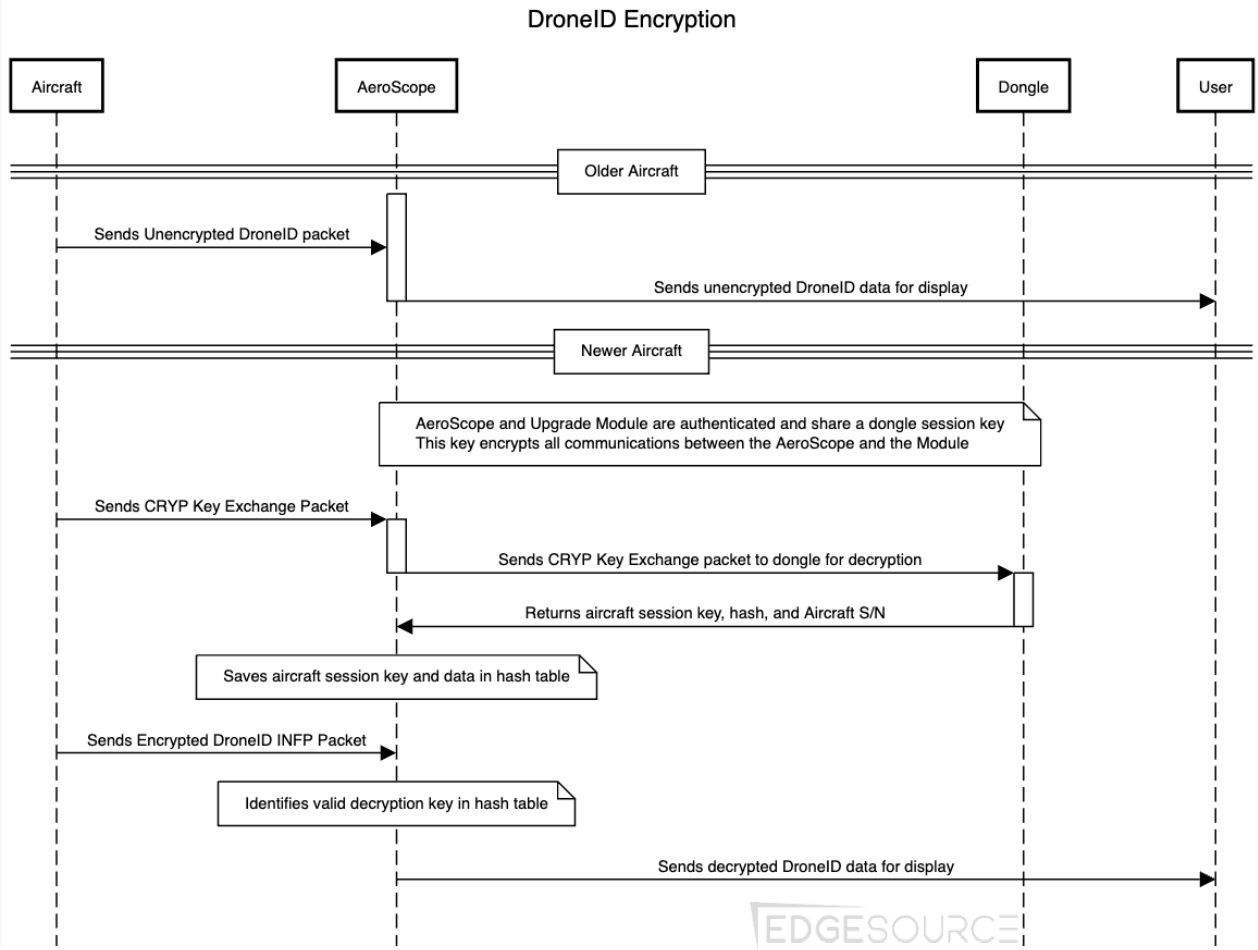


Figure 6: Encryption Sequence

1.7 WHAT WE HAVE LEARNED

First and foremost, our analysis has determined that this module does not offer any expanded detection capability, computation power, or modification to any onboard service on the AeroScope. **Its purported purpose is to securely store the cryptographic keys required to decrypt the Drone ID signals originating from encrypted DJI aircraft.**

However, closer inspection of the dongle has revealed that the software has extensive obfuscation and potentially includes geo-fencing that would enable DJI to restrict usage in certain portions of the world.

Key Point

Our initial research into this Upgrade Module has demonstrated a likelihood that these GPS coordinates could be used to prevent AeroScope usage in certain regions. We are in the process of testing this hypothesis.

Based on our initial analysis of its operation, we've discovered the following notes:

- When connected to the AeroScope, if the AeroScope has a connected GPS Antenna, the upgrade module receives a series of GPS locations from the AeroScope. As GPS antennas are not required, these likewise do not seem to be required for its operation, at least not in a way that has been accurately identified thus far.
- In addition to GPS locations from the AeroScope itself, the CRYP packets also include an encrypted blob of information from the detected UAV. This encrypted information includes the aircraft serial number, GPS position, and other pieces of data. This data is processed by the device, but only the serial number is provided back to the AeroScope; the remainder of this data appears to be utilized within the module.
- When presented with an invalid or improperly encrypted information blob, the dongle refuses to process the decryption and sends an error back to the AeroScope.

Apart from changes to the base code, DJI also started packing the files it ships for the AeroScope with an obfuscation tool. This makes firmware analysis quite difficult and increases the file size by approximately five to ten times by including a large amount of dead code. While these techniques are extremely common in malware, or other malicious applications, they also have strong employment in the software source code protection industry.

For this reason, DJI is no longer available on the Google Play store for delivery of their applications to users, as their use of obfuscation tools does not allow Google to review the application code, and therefore, violates Google Play Store policies. This technique does not immediately mean that malicious code is delivered in these obfuscated applications, nor does it mean that DJI does not have a valid reason for employing source code protection (namely years of product hacks, bypasses, and other changes that make their aircraft operate in ways not originally intended). It does, however, call into question what exactly exists within these code bases (and significantly increases the cost and challenge of reviewing them for security concerns).

Key Point

The binary obfuscation in the dongle makes firmware analysis difficult and increases the file size by five to ten times by including a large amount of packing decryptors and handlers.

1.7.1 Firmware Update Concerns

Coupled with additional hardware specifically designed to prevent analysis of the function, these firmware updates present some extremely troubling patterns. As mentioned previously, most of these protections are taken to secure the cryptographic function they serve; they also prevent further low-level analysis and can represent serious security risks.

Key Point

This new firmware update was designed and developed in China and obfuscated before release. Updating an AeroScope to this new firmware without first asking questions or understanding its contents is a serious risk.

For any leased or managed AeroScope deployments, remote AeroScope firmware updates without discussion or approval represent **severe cybersecurity incidents** and should be addressed.

The most important note in this area is that the updated firmware for the AeroScope, which provided for the usage of the new upgrade module, updates the main processing binary onboard the AeroScope, which manages all external communications as well as the general processing of the received detections.

In previous AeroScope firmware versions, this file was approximately 300 kilobytes (kB) in size and was not designed to prevent analysis, in fact it included debugging symbols (such as function names and other data). These new versions significantly change that by introducing numerous obfuscation and packing concepts designed to delay or prevent firmware analysis, one of which includes utilizing an open-source low-level virtual machine (LLVM) obfuscation tool called Pluto. For comparison, what was previously a 300kB executable has grown to approximately 2 megabytes (MB).

1.7.2 Hardware Supply Chain Concerns

While the physical hardware for the AeroScope can be considered a supply chain risk, its data value and usability with easily applied and readily available risk mitigations have lowered that risk to a readily accepted level, allowing for it to be employed quite widely. Consistent availability is the most mentioned risk and combined with its Chinese origin the hardware supply chain issue is now back in discussion.

Now, with another piece of hardware (“the dongle”) required to operate the system and make it function in the future, DJI has effectively injected another supply chain dependency into its system. From a hardware perspective, these devices ship with little known about the contents of the internal

logic, and **we are potentially developing a new pattern of behavior that accepts unknown hardware modules without testing.**

In many ways, this upgrade module can be categorized as a potential supply chain attack vehicle, either by injecting (or attempting to inject) new code or capabilities into previously secured systems, or simply by attempting to prevent the proper operation of some or all systems, either in a specific region, or worldwide. Unfortunately, risks such as these are a growing reality broadly across the security industry, spanning well beyond the C-sUAS industry. These risks present challenges to various industry participants, and demand action to assess and mitigate; actions that might include stockpiling hardware to mitigate supply chain disruptions or domestic production of replica or replacement hardware. At the end of the day, the physical hardware itself is low risk, we must continue to focus on understanding the firmware and software contained within.

What To Do In The Near Term

The uncomfortable truth is that in order to maintain the visibility necessary to identify, track, monitor, and potentially mitigate DJI drones that are used against allies or are used for illegal activities, we must have a way to decrypt the Drone ID data. At this time, an upgraded AeroScope is the most direct way to maintain that visibility, whether deployed as a standalone system or as a component of an advanced sensor such as the Windtalker™.

However – as was already necessary before the upgrade module was released – we must manage those risks carefully and continue developing alternatives that are not dependent on DJI. **The risk of loss of life and property from not seeing a potentially threatening drone may be higher than the risks in the upgrade module.** Our recommended actions are as follows:

(1) Make sure the systems you are using are secure. Whether you are using a standalone AeroScope, or a system that includes the AeroScope, it is more important than ever to understand your risk profile. This means performing a full security analysis, including specific risks related to each deployment of an AeroScope system before upgrading the AeroScope firmware or attaching the new upgrade module. **We work directly with the U.S. DoD on mitigating these risks** and can help you assess your risk along parameters such as connectivity, threat profile, pattern of life in the vicinity, and more.

It is also imperative to review the security posture and processes employed by all contractors or providers of AeroScope-based systems to ensure appropriate controls and government change control review are implemented before unannounced updates to the underlying covered foreign hardware, firmware, and software.

Beyond systems based on the AeroScope hardware itself, it is vital to fully understand how all RF-based detection systems function, which signals they detect, and if there are blind spots. Many systems provided by various vendors claim to be “independent” or “not reliant” on the AeroScope as they do not utilize the original hardware. In reality, most C-sUAS systems utilize the same DJI Drone ID signals that the AeroScope system detects, and those that don’t are still reliant upon a variety of other DJI controlled data elements (or the Remote ID broadcast) to detect DJI drones. **While the AeroScope has security risks and mitigation tactics, as already discussed at length in this whitepaper, other products that tout their independence from the AeroScope often gloss over the fact that they are impacted by DJI’s new encryption just as much as any AeroScope-based system.** They are perpetually playing a catch-up game as DJI continues to evolve their drones.

(2) Did you (or your vendor) already upgrade your AeroScope? We understand that inevitably some AeroScope upgrade modules have already been installed. From a security perspective it is critical to maintain awareness of when upgrades are applied, what they contain, where they originate, and if there is any need for further review prior to deployment. Firmware upgrades – especially ones that include software and firmware originating from an adversarial foreign country – should never be installed without an initial review, and decision on what risks should be accepted. If an upgrade has already been conducted, we recommend instigating a

security assessment to determine the risk impacts and any mitigations necessary. This may vary based on the risk profile of that specific installation, including whether the AeroScope is networked.

The best practice if you haven't already done the upgrade, is to delay all updates until an appropriate review has been conducted, or a decision has been made to progress with accepting the security risk as a tradeoff for ensuring continuity of detection capabilities. In addition, a vendor should never make an upgrade decision or install an upgrade (especially one originating in China) unilaterally without first consulting with the end user/customer of that device to ensure these changes are reviewed and the risks accepted.

(3) Continue to reverse engineer the upgrade module to fully understand what it contains. It is clear that the AeroScope upgrade module is not something we can ignore. It not only provides vital decryption of now-encrypted DJI Drone ID data, but it also gives us valuable insight into the inner workings of DJI. Reverse engineering the module is a foundational exercise to develop a solution that can perform the same necessary functions of the module, without introducing the risks that come with a Chinese-manufactured hardware and software solution. **Edgesource maintains ongoing reverse engineering, security assessments, and mitigation development in support of our customers and is available for subject matter expertise and consulting to assist you.**

(4) Invest in U.S. domestic or allied small UAS solutions. The abrupt cessation of new AeroScopes in the market, combined with the limited information about the contents of the upgrade module has reminded us, *yet again*, of the continued global imbalance in manufacturing of sUAS equipment and sensors that has perpetuated a vulnerability in security, supply chain, data, and capabilities and will only persist if we do not take this opportunity to invest heavily in this market.

- Continue to prioritize further research on this upgrade module, as well as all DJI systems, to keep pace with market developments.
- Ensure that similar understanding and research is conducted on other existing or emerging aircraft models, from various manufacturers.

WHAT DOES THE FUTURE HOLD?

These potential risks and pitfalls do not mean that we should stop using DJI devices altogether. Retaining access to foreign technology, adversarial or not, provides opportunities for us to research, study, learn, and employ these tools – helping ensure we don't fall behind while capturing lessons learned from adversary's mistakes as well.

DJI continues to be a market leader and will continue to represent a research area for all companies involved in C-sUAS, including RF, radar, camera, and others. No amount of development or research will ever entirely solve these challenges, and future developments and updates are likely to continue the "cat-and-mouse" game in perpetuity.

Our central conclusion is that DJI and China are not a problem that can we ban our way out of.

We must innovate our way out.

This whitepaper's recommendations are not intended to be all-inclusive, as the C-sUAS industry has other priorities and critical topics in addition to the AeroScope.

- We must continue analyzing and reverse engineering current and emerging DJI products including drones and the AeroScope, and likewise not become more complacent with interim mitigations or security layers to manage the risks of products originating in China.
- The United States and our allies must invest in domestic research and development in both the private sector and through the federal contracting landscape to bring advanced technology to market. Until we provide a viable, easily purchased, technologically superior product to the average consumer, DJI sUAS products will keep growing as the new weapon of choice for enemies and criminals alike.
- Ensure that a government-based team is established or continues to be funded to provide unclassified analysis and insights to the government on these types of topics, independent of a specific commercial or government product or capability.
- Coordinate appropriate legislative communication across all relevant agencies in the event that additional authority is required for system use to ensure that future authorities continue to be discussed and understood.

Our follow-on Technical Addendum will include a significantly deeper analysis of how these signals are structured currently (before the upgrade module), what changes follow the upgrade, the systems that might be potentially impacted and how, as well as a detailed analysis of the upgrade module, its affiliated firmware update and the new cryptographic process implemented in this update.

Contact us to receive the Technical Addendum. Distribution may be limited.

APPENDIX A: DISCLAIMER AND OPEN QUESTIONS

This whitepaper is written by Edgesource Corporation for background and general awareness purposes alone and does not reflect the interests, views, or opinions of any other entity, customer or U.S. agency. These statements do not reflect specific guidance, advice, or legal counsel, and are subject to change.

Within the United States (at the time of this publication and subject to expiration or change), federal agencies, by statute, have Counter-Unmanned Aerial Systems authority, which can be applied in relevant, applicable scenarios for coverage over the various legal issues that various C-sUAS systems implicate. For the Department of Defense, for example, C-sUAS authority includes protection of a covered facility or asset (10 USC § 130i(j)(3)). Other federal agencies have a similar provision in 6 USC § 124n(k)(3). These definitions cover most situations but also preclude some, though this is agency-specific.

Questions remain regarding technical, legal, and policy issues that are not answered in this whitepaper. For example, in recent years, the AeroScope system has become a popular choice for organizations that do not have legal authority for drone surveillance. Many legal considerations lend themselves to the reason for this analysis, some of which originate from the fact that DJI is the Original Equipment Manufacturer (OEM) for both the aircraft and the detection system and can, therefore, craft end user license agreements (EULA) and other literature in their favor. As a result, many private entities and governments use AeroScope as a system because they have interpreted that the system may be used legally or without exercising statutory authority. A similar question exists about the legality of collecting the Drone ID data broadcast by the aircraft by sensors other than DJI-manufactured AeroScopes.

Furthermore, given all of the above and the extended legal discussion and history already in this space, does the newly released encryption change, update, or modify any assumptions or determinations used in the past to determine that the AeroScope is ruled as not requiring additional authorities to operate?

These are just a few examples of the vast legal questions surrounding the AeroScope and any C-sUAS system. And, for readers in countries outside of the United States, many similar questions apply as well, aligned to the governing law for that country or region.

APPENDIX B: DRONE ID PROTOCOL

This appendix provides an overview of the Drone ID protocol functionality and operating principles. Since the AeroScope relies on proprietary signals broadcast from their aircraft for detection, the entire system is fully dependent upon the following protocols for full, successful operation:

- **Signal Availability**: That the aircraft continues to broadcast this signal in the same way as anticipated by the AeroScope, in the same format, and with the same encoding and encryption processes.
- **Signal Authenticity**: That only real aircraft are capable of broadcasting this signal in a way that the AeroScope detects and reports as an aircraft.
- **Signal Integrity**: That all data broadcast by the aircraft remains valid, unchanged, and represents accurate information regarding the aircraft's telemetry and position.

You'll note that these align with common information security pillars, and as such, each creates a vulnerability area for the AeroScope system.

Key Point

All security risks related to the Drone ID protocol exist with the Remote ID protocol, the critical difference being the protocol change management and oversight process.

1.8 SIGNAL AVAILABILITY

The AeroScope signal, commonly called the Aeroburst or Drone ID, is a radio-frequency signal broadcast from the aircraft to the AeroScope (or any other listening system) at a static frequency, time, and modulation. While based on OcuSync, the AeroScope signal is much simpler in operation as it does not need to account for noise, interference, and all other variables which actual aircraft uplink and downlink need to address. There are also different versions of this signal for older Lightbridge-based aircraft and DJI Enhanced WiFi-based aircraft.

Since the aircraft must send these signals, each drone is programmed internally to package and send utilizing the same radio the drone uses for command and control. The AeroScope is pre-built with internal modules for receiving and decoding signals from each of their major protocols (OcuSync, Enhanced WiFi, and Lightbridge), which matches the hardware the aircraft uses for sending.

Onboard the AeroScope, low-level acquisition, processing, and demodulation occur in one of an array of Digital Signal Processors (DSPs). Once a packet is received and validated, this data flows through the AeroScope unit before it is pushed outbound to an AeroScope server or, for the mobile units, the onboard CrystalSky screen. The AeroScope does not modify, alter, or process these messages further before sending them to the external display mechanism.

Beyond physical characteristics, since the AeroScope does not perform onboard processing of signals beyond basic validity, the actual data format for these messages is irrelevant to the hardware. Instead, the receiving display software must correctly parse and display received messages; but changes to message protocols, formats, or other information do not affect the hardware.

1.8.1 Threats to Maintaining Signal Availability

There are two main threats in this arena: one) DJI might release a new Drone ID protocol that the existing non-upgraded AeroScopes cannot detect, or two) DJI might significantly change the underlying physical protocol characteristics to render non-upgraded AeroScopes unable to detect aircraft. In both instances, it is important to remember that this discussion revolves solely around the Drone ID package of information, not the aircraft command and control links.

For the first scenario, this would mean that DJI has released a completely new aircraft model that does not utilize any of the same physical hardware as their previous ones. While very unlikely, if this does occur, the AeroScope unit would need to be updated with an additional radio processing module compatible with the new signal. Beyond unlikely, this also would not apply backward to older aircraft – which would also not be able to be updated to the new hardware.

The second scenario is more likely in that DJI will release a significant update to their existing aircraft, which will change the specifications of the Drone ID protocol or even remove it entirely. As these are software or firmware level changes, any changes other than complete signal removal would be resolved by simply updating the DSP processor firmware on each AeroScope.

The new AeroScope Upgrade Module is an example of a significant low-level change in the Drone ID protocol structure. **In this case, the upgrade is designed to implement a layer of encryption over the existing protocol, ensuring that only AeroScopes with an attached upgrade module can successfully decrypt and process those data packages.**

1.9 SIGNAL AUTHENTICITY

Given the widespread availability of DJI aircraft and the AeroScope, the number of potential mitigations for these systems is ever-increasing. From the authenticity point of view, the goal here would be to ensure that any signal considered Drone ID must originate from a DJI aircraft. The same could be said about Remote ID, but in a more general unmanned aircraft systems context. In simpler terms, does the received signal represent one broadcasted by a real aircraft?

Key Question

Does the identified aircraft signal, even though it looks like a real aircraft, represent one sent from a real aircraft?

This is a difficult question to answer definitively, especially with the growing popularity of Drone ID spoofing. Various private and open-source tools are designed to produce a variety of ‘fake’ signals (e.g. “spoofing”), each emulating what a real drone would look like, with or without a real

aircraft. On the detection side, determining what originates from a real aircraft and what is spoofed often comes down to various techniques, from in-depth data analysis to collating detection between different types of sensors. For example, analysis may include the following:

- Does the data broadcast match what is expected from that model or type of aircraft?
  - Answering this is complex and requires understanding what is expected of each aircraft model and firmware. Legitimate aircraft updates, changes, or modifications can alter this data format in a way that appears spoofed when it is not. The same applies to aircraft the operator has hacked, modified, or altered (either with software or hardware modifications).
- Are there detections of multiple expected signals, such as the command-and-control uplink, downlink, and Drone ID?
  - It is possible to correlate between Radio Frequency (RF)-based sensors, a valid approach to address some forms of spoofing. However, this solution falls short when the Drone ID link is detected well outside of another RF system's range, when a spoofer is designed to fully replicate all expected signals from an aircraft, or when the overall data available from each system is insufficient to reliably and accurately relate the different detections.
- Does the RF information match closely with physical representations of the device, such as a radar detection or even an image on a camera?
  - While reliable when present and manually identified, these relations are often difficult to autonomously identify and are even further subject to line of sight or other physical constraints. Beyond this, when multiple aircraft are present (especially if a spoofer is designated to create a fake swarm), a requirement to individually validate each detection significantly delays a defender's ability to identify the real threat.

1.9.1 Threats to Confirming Signal Authenticity

While none of these considerations pose a large direct security risk, they do tend to threaten the usability and accuracy of a particular detection capability. Any RF sensor is rendered almost useless if it continually detects spoofed aircraft. Given this vulnerability, many drone users, especially those in conflict zones, are beginning to utilize spoofing to degrade detection systems that do not include an intelligent spoofing detection mechanism.

With the new encryption process, however, there will be an additional layer of challenge for successful spoofing of an aircraft signal, which also involves properly encrypting and replicating the aircraft signals for the AeroScope to detect and process. Theoretically, since the encryption keys are not necessarily public for this new scheme, this should prevent most spoofing. But, based on the structure of the encryption process from the aircraft, our analysis is that the new encryption will have minimal impact on spoofers. This will be a trivial addition to most spoofing systems, assuming those spoofing developers can reverse engineer the proper packet structures and encryption processes.

For this entire process, DJI turns to an industry standard hybrid encryption procedure, also called a KEM/DEM. First, the Drone ID data packages are encrypted with a symmetric session key, based on AES-128 in CTR mode. Also, for this stage, a random 8-byte IV is generated and transmitted, for each data packet. (Note that AES-128-CTR requires a 16-byte IV, for this DJI simply pads this 8 byte random buffer out to 16 with null bytes). This portion of the process is called the Data Encapsulation Mechanism (DEM).

Once the data is encapsulated in AES-based encryption, it's now time for the Key Encapsulation Mechanism (KEM), which in this case employs the Chinese Standard SM2 algorithm. This is an elliptic-curve based asymmetric encryption and signature algorithm, which is then utilized to encrypt the AES key utilized in the DEM above. Once complete, the final encapsulated key and all required values are transferred from the aircraft over to the AeroScope, where decryption then takes place utilizing the private key to retrieve the encapsulated AES key. And from there, the data can be decrypted and presented.

Key Point

Digital signatures also typically utilize asymmetric encryption, but these algorithms work in reverse. That is, a signed message is encrypted with the private key, which only the key owner should retain access to.

It is challenging to provide legitimate authenticity when thousands of aircraft are required to send authentic signals, and there's always a vulnerability that allows a knowledgeable attacker to replicate those signals.

As all of the information necessary to generate valid packages, both for the data and the keys, generating fake packages is as trivial as extracting the necessary constants for the SM2 elliptic curve, and ensuring that all data packages are encrypted at all stages in the same manner.

1.10 SIGNAL INTEGRITY

Finally, given the previous two sections on ensuring that data is available and authentic from a DJI aircraft, the final critical topic is whether the received data is actually what the aircraft intended to send. The consideration related to Signal Integrity are very similar to those discussed previously regarding Authenticity with one critical addition: are data changes or modifications possible after the Drone ID data is packaged on the aircraft but before it reaches the AeroScope?

In this instance, all AeroScope packets originate from the Flight Controller onboard the aircraft, which has access to the various sensor data necessary to produce the overall packet. The Flight Controller can be considered a trusted component on the aircraft and, in many newer models, is completely distinct from other management modules, which maintain a lower security level. From this point, they are internally routed through the aircraft's systems until they reach the modem, which passes them down to the DSPs for modulation outbound to leave the aircraft as RF signals.

Once the signal leaves the aircraft, modification of its contents is essentially impossible. But, before that, the package of necessary data is routed through a variety of lesser trusted components

on the aircraft, which exposes that data to tampering or modification by an adversary with access to the aircraft's lower level (i.e., less trusted) components. This might not sound easy at first glance, but it's important to remember that public entities already offer or sell root access to these aircraft.

The modem, the sender of these data packages, is one of these lesser trusted modules. This physical distinction makes perfect sense, as all external attacks directed towards a flying aircraft must originate from the inbound RF signals. This, however, means that most drone operators, with the proper experience and guidance, can modify or patch the modem to alter the data broadcast.

Key Point

It has been demonstrated that the Drone ID signal can be completely disabled via modem alterations (this is not the same process as masking Drone ID data via the built-in privacy bit settings, as is offered in many open-source projects).

It likewise has been demonstrated that, instead of removing the Drone ID broadcast entirely, it could be altered just enough to present false information (perhaps retaining the actual aircraft location but sending an incorrect home and pilot location).

Adding encryption to the communication process changes the possibility of altering the data to some extent. Encryption happens within the Flight Controller before broadcasting the message to the modem. Any modification to the data needs to be done within the Flight Controller before encryption, as after encryption, the data cannot be changed without going through decryption first. While this does not eliminate the possibility of stopping the broadcast entirely, it prevents alterations to the data once it leaves the Flight Controller.

APPENDIX C: AEROSCOPE SYSTEM COMPONENTS

The AeroScope system itself also consists of a few different components, mainly the physical AeroScope detection hardware (either a DJI Mobile or AeroScope FS1800), the appropriate antenna sets (Omnidirectional, G8 (directional), or G16 (directional)), and a visualization platform (either DJI's own, or a third party one into which AeroScope data has been integrated, such as Edgesource's Dowding™ Common Operating Pictyre).

1.11 AEROSCOPE UNIT

The AeroScope was sold in two main form factors: a mobile version and a fixed site version. Despite different external appearances, the underlying hardware is the same between these units, so there is only one firmware for the AeroScope systems. In recent years, the availability and production of both versions and the AeroScope units' overall availability have been questioned, but there are still thousands in operational usage worldwide.

1.11.1 AeroScope Mobile

The mobile version of the device comes in a small, foldable black case. It reveals two small omnidirectional antennas that detect signals in mobile environments. This case is not weatherized and is typically only used for short-duration events. The built-in CrystalSky monitor comes with a mobile-optimized monitoring application that presents basic information to the user while operating the device. In addition to the two omnidirectional antennas on the top, the mobile unit also includes a USB port, Ethernet, power, two batteries, and two additional RF antenna ports on the case. The CrystalSky monitor is connected to the USB port to access the detection data, which is then displayed on the monitor (**Figure 7**).

Figure 7: AeroScope Mobile Unit (AS-P1800)

1.11.2 AeroScope Fixed Site

The fixed site unit (**Figure 8**) is optimized for outdoor usage and is weatherized for installation onto a pole or in another more permanent location. While it can also be utilized with omnidirectional antennas, this unit is designed to use the directional antenna sets as described below.

In addition to the four antenna connectors, this unit includes a power, ethernet, USB port, and debugging ports on the bottom.

Figure 8: AeroScope Fixed Site (AS-FS1800)

1.12 AEROSCOPE ANTENNAS

There are three main antenna types for the AeroScope.

1.12.1 Omnidirectional

These small round black antennas typically ship with the AeroScope Mobile units and connect at the top of the open case for detection. They can be seen attached to the mobile AeroScope pictured in (**Figure 7**). These dual-band antennas cover 2.4 GHz and 5.8 GHz; the frequencies that DJI devices utilize for their broadcasts.

1.12.2 G8 Antenna

The G8 Antenna Set (**Figure 9** below) is a complete 360-degree coverage set, including four dual-band, 90-degree directional antennas. These four antennas are mounted on a bracket that spaces them appropriately and allows for vertical adjustment. Like the omnidirectional antennas, these are also dual-band antennas – covering 2.4 GHz and 5.8 GHz.

1.12.3 G16 Antenna

The G16 Antenna set is the largest DJI sells for use with the AeroScope system. These units sell in sets of eight, which provides a 90-degree sector of coverage. These eight include four 2.4 GHz antennas and four 5.8 GHz antennas, each with 22.5 degrees of individual coverage. Four AeroScope systems are required to achieve full 360-degree coverage with the G16 antenna system, including four complete antenna sets and four fixed site nodes, as pictured below in **Figure 10**.

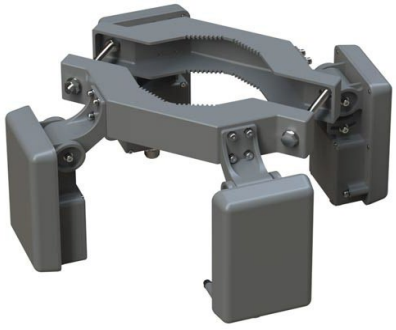


Figure 9: AeroScope G8 Antenna

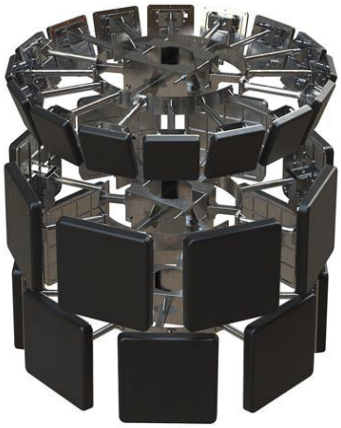


Figure 10: AeroScope G16 Antenna

APPENDIX D: DRONE SYSTEM OVERVIEW

This appendix provides a brief overview of the typical DJI drone pilot setup and how it interacts with the AeroScope and other RF sensors.

1.13 TYPICAL DRONE SETUP

There are three major components necessary to fly: the aircraft, the Remote Controller (RC), and a mobile phone or tablet (if not built in via a DJI Smart Controller). Pilots also need a DJI account and the proper flight app installed and logged into on your smart controller, mobile phone, or tablet.

Once all those bits are ready, you'll turn the aircraft on, ensure that it is correctly paired with the RC and that everything connects properly on your ground station app. The app will give you some basics about the aircraft and ensure everything functions correctly. When ready, you can take off and fly the aircraft, during which you'll see the video, telemetry, and various options displayed on the mobile phone screen.

1.14 DATA ELEMENTS & SIGNALS

When flying, DJI aircraft maintain various radio-based communications – which differ based on the aircraft model. These include the following, though not every aircraft has all of these available:

- **WiFi**: Generally used for Command and Control (C2) on a few older models, such as the Spark, Mavic Air, and Mavic Mini. Also, it was optional via a physical switch on the Mavic Pro and Mavic Pro Platinum. These typically operate via a DJI-enhanced WiFi link, making the specifications slightly different than standard WiFi. Most newer DJI aircraft retain a WiFi communications capability, which is rarely utilized for anything other than basic aircraft updates and management.
- **Automatic Dependent Surveillance–Broadcast (ADS-B)**: Enterprise models and some newer consumer models include a built-in ADS-B receiver, which warns the pilot of a larger aircraft. This is an entirely passive receiver.
- **Remote Control (RC) Uplink**: This is the main communication link between the aircraft and the pilot. There have been slight variations over the years, but the two major DJI links are Lightbridge and OcuSync (excluding the enhanced WiFi covered above). Various levels of encryption on this link have been introduced over time, from simple pairing protection to full telemetry encryption. This signal originates from the RC and is received by the aircraft.
- **Video Downlink**: Complimentary to the uplink, this signal originates from the aircraft and relays the live video back down to the controller. This link is also based on the previous proprietary link structures. Video feeds are not typically fully encrypted.
- **Drone ID Broadcast**: A separate broadcast of telemetry data, founded on the main C2 protocol for the aircraft. For OcuSync, this signal is entirely separate from the C2 communications. Previously, it was not encrypted at all.

- **Remote ID Broadcast**: This broadcast provides a Remote ID-compliant signal, which includes ASTM International (ASTM) F3411-compliant messages and data elements. As the Remote ID standards evolve, these broadcasts will likely be updated to comply. As of the time of writing, DJI devices achieve compliance utilizing a WiFi broadcast, though Remote ID allows Bluetooth 4 or 5 usage. As of publication, 32 DJI models have an accepted Remote ID Declaration of Compliance (DOC), and one model (the Mavic Pro Platinum) has a rescinded DOC.

Aside from most internal communications, a variety of critical data elements are collected and transmitted in the Drone ID and Remote ID data broadcasts. We'll focus simply on Drone ID in this paper, as Remote ID data elements are defined in other standards that are publicly available. The following Drone ID elements are broadcast with every Drone ID signal, even if the values are unchanged from a previous broadcast. The following briefly overviews some of these data elements and where they originate.

- **UAV Location**: This is the Global Positioning System (GPS) position of the aircraft, along with a few different altitude measurements. When an aircraft does not fully have a GPS lock, these fields might appear as 0.0/0.0 or invalid values.
- **Home Location**: When the aircraft first begins takeoff, it records its location for when it may later need to Return-To-Home (RTH). This location is broadcast when available and remains the same across an entire flight unless changed by the pilot (done via the app) or modified by an external counter system.
- **Pilot Location**: When available, the aircraft will rebroadcast the location of the drone's operator – which is collected via the attached mobile phone or smart controller.
- **Pilot Universally Unique Identifier (UUID)**: When the user logs into their mobile pilot app, the app records a numeric identifier that is unique to that user's login. Beneficial to track a single pilot to multiple aircraft, especially in hostile zones.
- **Attitude Information**: Originating from the flight controller, these data fields include the roll, pitch, and yaw of the aircraft.
- **Velocities**: Also originating from the flight controller, these fields indicate the aircraft velocity in three distinct directional vectors (north, east, and up).
- **Other Data**: A variety of other metadata is also broadcast, for easy data reconstruction on the detection side. This also includes flags for when the aircraft is airborne, when the motors are enabled, and if any privacy options are toggled on.

Key Point

The UUID broadcast is only a numeric value; however, it would be possible for DJI themselves to affiliate that number with a given user's DJI account information (which might include name, email, title, flight history, and other data). Currently, only DJI has this capability and would have to approve and respond to any such requests for information.