EDGESOURCE

To Dongle or Not to Dongle: That is the Question

Assessing the security risks of the DJI AeroScope upgrade module, which supports foreign government-specified encryption of the data signal.

Da Jiang Innovations (DJI)'s AeroScope drone detection platform has proven to be an effective security tool for military and law enforcement. It identifies and tracks drones in real time, providing AeroScope users with information like flight status, path and pilot location for drones up to 50 kilometers away. This data stream enables users to make fast and informed responses as soon as possible, mitigating the potentially harmful effects of consumer drones in and around public spaces, government facilities, infrastructure and other no-fly zones.

Yet despite its efficacy as a public safety tool, AeroScope now comes with major security risks. Despite discontinuing the system in 2022, in 2024 — after only a few months of notice — DJI introduced a new encryption mechanism to their AeroScope system, along with a hardware upgrade in the form of a USB device, or dongle. Unmitigated, this update significantly impacts the AeroScope's ability to reliably process data at a large scale and introduces further vulnerabilities to the system.

Encryption enables foreign governments to potentially conceal drones based on geographic location and serial number. It also renders DJI drones invisible to non-upgraded AeroScopes, undermining the effectiveness of counter-small unmanned aircraft systems (C-sUAS) and creating serious blind spots in U.S. airspace surveillance. Finally, non-DJI radio frequency (RF) systems are incompatible with the dongles, rendering them useless in detecting encrypted DJI aircraft.

Windtalker.

In short, the very system you bought for safety is no longer safe, making it necessary to develop risk mitigation strategies for DJI products. For example, Edgesource Corporation has developed the Windtalker™ passive RF sensor that incorporates AeroScope but firewalls it from external networks, preventing AeroScope from phoning home to the DJI servers.

Yet questions remain. Even if the dongle's primary function is to enable decryption of the newly encrypted signals from DJI drones, what else does the upgrade module do? What unknown code or commands do the modules contain? What are the risks of upgrading — or not upgrading — the sensors?

Mounting Global Tensions: Threats to National Security

This is not the first time DJI has faced scrutiny as a security risk. The company manufactures drones, gimbals, cameras and other products that can — and are — used for military purposes. Recognizing these threats, the U.S. Department of Defense (DoD) began restricting commercial off-the-shelf (COTS) drones in 2018. In 2021, a presidential executive order required extensive reviews of certain government-made drones in U.S. government fleets. And in 2020, the U.S. Department of Commerce added DJI to its list of entities that act contrary to U.S. national security and foreign policy interests.

Yet despite these and other concerns, DJI has dominated the small drone market, accounting for as much as 80 percent of the world's commercial small drone sales. Even while recognizing the inherent security risks in DJI products, we are faced with the reality that there is no domestic alternative that manufactures products and solutions of comparable technological advancement.

The Purpose of the Dongle: Benign or Malicious?

The new upgrade modules support the addition of encryption to DJI's previously unencrypted AeroScope data signal. Specifically, its function is to securely provide for the decryption of the SM2 key exchange packets.

Yet despite the dongle's seemingly benign purpose — to "support the AeroScope system update and ensure that AeroScope is compatible with future DJI aircraft products"

— it raises several security concerns. For example, the additional hardware device will receive basic telemetry information from broadcasting aircraft, such as its GPS location and serial number, and may reject decryption based on a variety of potentially unknown factors. These risks are especially alarming for any federal organization that has a fleet of AeroScopes connected to or accessed by government networks.

As with any computer or system attached to a network, connecting USB devices presents risks, ranging from introducing unknown code to shortening the power supply life. In this context, it remains uncertain whether the updates are 100-percent safe and non-hostile. We also don't know if they contain sleeper code or malicious functions that can be activated at a later date.

Even if the dongle does everything DJI says it will do — i.e., providing the necessary updates to enable AeroScope to work with the newly encrypted Drone ID data — the dongle could still contain malicious code designed to infiltrate networks or degrade the functionality of standalone systems.

To explore these possibilities, Edgesource has been reverse engineering the new hardware and updated firmware for the AeroScope system. What follows is our analysis.

How the Upgrade Works

The AeroScope upgrade module is an example of a significant low-level change in the Drone ID protocol structure. In this case, the upgrade implements a layer of encryption over the existing protocol, ensuring only AeroScopes with an attached upgrade module can successfully decrypt and process those data packages. Here is a quick overview the dongle's operations once it's plugged into the AeroScope system:

- After connecting the dongle to AeroScope, the onboard firmware performs a multi-step authentication routine. During this process, AeroScope and the dongle exchange a session key, which encrypts all further communications from the dongle.
- A significant amount of effort is spent ensuring the device connected to the dongle is an AeroScope. Once the module is authenticated, AeroScope runs like normal, including receiving information packets from older or non-updated aircraft that aren't encrypted.
- Newer aircraft send a new cryptographic key exchange packet (CRYP) of information that includes an encrypted aircraft session key, along with other necessary attributes.
- Once AeroScope receives the CRYP packet, it sends that unmodified information to the upgrade module, which returns the decrypted aircraft session key to AeroScope.
- AeroScope stores the aircraft session key and unique key hash. As it receives the original Drone ID packets of data, it decrypts them using this key.

Windtalker 3.0 bypasses the dongle that DJI released for users to continue operating AeroScope.

Reverse Engineering Revelations

While the dongle's purported purpose is to securely store the cryptographic keys required to decrypt the Drone ID signals originating from encrypted DJI aircraft, closer inspection of the dongle has revealed that the software has extensive obfuscation. It also potentially includes geo-fencing, which would enable DJI to restrict the platform's usage in certain parts of the world. Based on our analysis of the dongle, we have also discovered:

- If there is a connected GPS antenna, AeroScope sends GPS locations to the dongle.
- The CRYPs include encrypted information from the detected UAS including the aircraft serial number and GPS position. While this data is processed by the device, only the serial number is provided to AeroScope. The rest of the data is used 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 AeroScope.

Obfuscation and Firmware Update Concerns

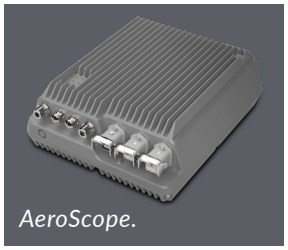
The software obfuscation tool makes analyzing the firmware difficult and increases the upgrade file size by roughly five to ten times by including a large amount of dead code. Because these techniques are common in malware, DJI is no longer available in the Google Play Store. The obfuscation tool prevents Google from reviewing the application code, violating its store policies.

We should note, obfuscation doesn't immediately point to malicious code. It also doesn't mean DJI doesn't have a valid reason for employing source code protection.

It does, however, call into question what exists within these code bases and significantly increases the cost and challenge of reviewing them for security concerns.

In addition, the updated firmware, which supports the dongles, updates AeroScope's onboard main processing binary, which manages all external communications and general processing of received detections. In previous 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, on the other hand, introduce numerous obfuscation and packing concepts designed to delay or prevent firmware analysis. One, for example, uses Pluto — an open-source low-level virtual machine (LLVM) obfuscation tool, causing this previously 300-kB executable file to grow to roughly 2 megabytes in size.


AeroScope.

In short, this new firmware update was obfuscated before release. Updating AeroScope to this firmware without first asking questions or understanding its contents poses a serious security risk.

What Do We Do Now?

In order to maintain the necessary visibility to identify, track, monitor and potentially mitigate DJI drones used against us or are 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 Windtalker™.

In partnership with the DoD's Defense Innovation Unit (DIU), Windtalker was developed by Edgesource, which was tasked with cyber-wrapping AeroScope, enabling it to safely operate without DJI influence. Windtalker maintains AeroScope's functionality but isolates the system, severing all connections to foreign governments and allowing only your server to see the drone data. Today, Windtalker is a trusted solution to protect U.S. officials.

In addition to implementing Windtalker, we recommend the following actions to further mitigate security risks:

- **Make sure the systems you're using are secure.** 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.
- **Find out if you or your vendor already upgraded your AeroScope.** We understand that inevitably some AeroScope upgrade modules have already been installed. In this case, we recommend performing a security assessment to determine the risk impacts and any mitigations necessary.
- **Reverse engineer the upgrade module to fully understand what it contains.** In addition to providing vital decryption of now-encrypted DJI Drone ID data, the upgrade module gives us valuable insight into the inner workings of DJI. Reverse engineering the module can help us develop a solution that can perform the same necessary functions of the module — but without introducing the risks that come with a foreign-manufactured hardware and software solution.
- **Invest in U.S. domestic or allied small UAS solutions.** There is a global imbalance in manufacturing sUAS equipment and sensors, creating a vulnerability in security, supply chain, data and other capabilities. These issues will only persist if we don't take this opportunity to invest heavily in this market.

To learn more, please visit: http://aeroscopeupgrade.com/

RESOURCES

- DJI AeroScope Release Notes (2023).
- Executive Order on Protecting the U.S. From Certain Unmanned Aircraft Systems (2021).
- Addition of Entities to the Department of Commerce's Entity List (2020).
- Pentagon Memo Grounds Air Force Special Ops Quadcopters (2018).

PURCHASE INQUIRIES

Customer support provided by our manufacturing partner, Trust Automation. To learn more, visit our website to email customersupport@trustautomation.com, or call us at +1 805.544.0761

TRUST™ AUTOMATION, INC.