RIZER Support on Legacy Aircraft

LT Ryan Beall, USN
ryan@diux.mil

ENS Daniel Flack, USN
dan.flack@diux.mil

3 August, 2018

Summary

This paper summarizes RIZER's support for DJI legacy aircraft. DIU Rogue Squadron defines "legacy" unmanned aerial systems (UAS) as any DJI UAS without an onboard Linux CPU (or utilizes DJI GO 3) such as the Phantom 2, Phantom 3, Inspire 1, Matrice 100, and Matrice 600. While Linux CPUs are standard on any newly released DJI UAS, older systems do not have this hardware.

RIZER is DIU Rogue Squadron's tool for mitigating cyber vulnerabilities in DJI UAS. It enables custom firmware, establishes a firewall for Internet traffic, disables onboard WiFi, initiates an RC lock, removes blackbox flight logs, and disables No-Fly Zones (NFZs). It supports nearly all modern DJI drones, as listed on the Rogue Squadron website at rogue.diux.mil. However, legacy systems are not fully compatible with the RIZER software architecture.

**RIZER offers only limited support for legacy aircraft.** DIU Rogue Squadron does not recommend the use of the Phantom 3 Standard, Phantom 3 4K, or Phantom 3 SE drones, except when required (i.e. for C-UAS testing), due to a datalink vulnerability. Rogue Squadron does support the use of RIZER for other legacy drones, but only if users understand the caveats and limitations and plan accordingly. Rogue Squadron GCS apps block "phone-home" behavior for legacy platforms, but other features are not available. This document walks through limitations in detail. Table 1 summarizes features available on different legacy drones.
Datalink Vulnerability Considerations

DIU Rogue Squadron does not recommend the use of Phantom 3 Standard, Phantom 3 4K, or Phantom 3 SE drones because of an important difference in the datalink architecture. Specifically, these drones establish a WiFi connection between the RC (Remote Controller) and Android/iOS device, which RIZER does not defend against. Newer systems do not have this connection.

Legacy platforms establish a WiFi connection between the RC and phone/tablet using two distinct links: an 802.11 WiFi link to the phone/tablet, and the drone’s C2 (command and control) link (which may also include full motion video). Both of these links transmit on 2.4/5.8 GHz ISM band, but should be considered separate and distinct. One link communicates up to the UAS, and the other acts as a relay of the C2 telemetry and video data to the phone/tablet application. This style of link introduces a vulnerability by requiring the app on the phone/tablet to have access to WiFi. RIZER doesn’t support this type of RC, which is used on the Phantom 3 Standard, 4K, and SE (Special Edition).

Newer DJI RCs provide the C2 and video data to the phone/tablet app via USB. DJI switched to this style of connection because it drastically reduces latency and improves reliability. This hardwired connection removes the necessity for the application to have access to WiFi and therefore is not a vulnerability.

Ground Control Station (GCS) Considerations

DIU provides three ground control stations, all of which block phone-home behavior and are compatible with legacy drones: RS GO 3, Rosetta Drone SECURE, and ATAK GO SECURE. The only
difference from newer systems is that legacy systems require RS GO 3 instead of the more modern
RS GO 4, and some newer features are missing.

RS GO 3 and RS GO 4 are patched versions of DJI’s own applications, DJI GO 3 and DJI GO 4. Legacy
aircraft use DJI GO3 (Phantom 3 Series, M100, M600, Inspire 1). Newer platforms utilize DJI GO 4
(Mavic, Phantom 4 series, M200, Spark, Inspire 2). The Rogue Squadron version patch out all “phone
home” behavior to DJI’s servers.

RS GO 4 recently went through a vast tech refresh which added features like offline waypoint mission
support and Latitude Longitude (or MGRS) overlay on the application. RS GO 3 is next on the list for
a refresh, but won’t be complete until September 2018.

Rogue Squadron has developed a separate GCS app that enables use of DJI drones on any MAVLINK
capable GCS (Ground Control Station), while also blocking “phone-home” behavior: **Rosetta Drone
SECURE**. This is Rogue Squadron’s recommended GCS going forward. Extensive testing as been
conducted on contemporary platforms, but no testing has been conducted on legacy platforms due
to a lack of demand. M600 testing on **Rosetta Drone Secure** will likely start September 2018.

DIU also distributes a secure version of the Raytheon/BBN ATAK GO app, which should be compatible
with legacy platforms but has also not been extensively tested with these platforms.

### RIZER Caveats for Legacy Aircraft

RIZER addresses known security vulnerabilities in DJI products and unlocks additional functionality for
warfighters. Some RIZER features are not compatible with legacy aircraft, or have important caveats,
because of differences in hardware architecture. These include:

- blocks phone home behavior
- offline activation
- disables no fly zones
- custom firmware for restriction removal

The following are short summaries of some of RIZER’s capabilities with respect to legacy aircraft only.
For full feature list of RIZER’s capability on contemporary aircraft, visit [rogue.diux.mil](rogue.diux.mil).

### Block Phone-Home Behavior

Per the previous section, all three of Rogue Squadron’s GCS apps block phone-home behavior. RS
GO 3 blocks all Internet traffic using Android’s highly restrictive permissions framework, guaranteeing
that no traffic enters or exits the app, and ensuring that no data leaks to cloud-based servers. Unlike
man-in-the-middle solutions that rely on external hardware, this is a pure software solution; troops do
not need to carry and additional piece of hardware. Rosetta Drone SECURE and ATAK GO SECURE
utilize a VPN to block outgoing Internet traffic, except to authorized IP addresses.

### Custom DIU Aircraft Firmware

The newer versions of RIZER modifies and cryptographically signs custom firmware. This is critical,
because superficial methods of exploiting DJI hardware—such as making simple parameter changes
to disable altitude restrictions—no longer work. Direct access to firmware grants low-level access to hardware, and makes almost any modification possible. For example, RIZER offers the ability to modify firmware that disables drone LEDs and RC buzzers to support covert operations. It can also tune flight performance to warfighter needs.

Rogue Squadron has provided modified firmware to DOD users for use of legacy aircraft, but only if compatible with the RIZER architecture. Bandwidth for custom firmware will not be allocated to platforms that cannot meet minimum security standards.

Disable No-Fly Zones and Remove Altitude Restrictions

In most cases, RIZER cannot disable no-fly zones or remove altitude restrictions for legacy aircraft. The one exception is the M600, which allows for NFZ removal in the app. DIU has done limited work on Phantom 3s for particular customers, but these tools are not production-ready. DIU does not plan to do any further product development for legacy aircraft.

RC Handset Lockout

With modern drones, RIZER locks out the RC handset if the user is not using a hardened GCS like RS GO, Rosetta SECURE, or ATAK GO SECURE. This prevents troops from accidentally leaking data by using an unauthorized app. **RC Handset Lockout is not implemented on any Legacy Aircraft.** This is a constraint of the aircraft not having a Linux CPU, which is where DIU implements the RC lockout feature. Users should understand that careless or negligent troops could use unauthorized apps, resulting in data leakage.

Black Box Sanitization

DJI drones log a significant amount of on-board data, such as flight path and sensor values. This data can be retrieved using open source tools. **Black Box sanitization on legacy platforms is currently only supported on the Matrice 600.** Contemporary platforms heavily rely on the Linux CPU to handle the Black Box data and therefore can be eliminated.

DIU Rogue Squadron maintains a **Matrice 600 Manager tool**, which allows users to manually wipe the Black Box after every flight. This solution requires compliance by operators. DIU does not offer tools for removing Black Box data from other legacy aircraft.

Platform-by-Platform Summary

DJI Phantom 3

The Phantom 3 has two RC variants and only the USB variants are compatible with **RS GO 3**.

Three models have WiFi RC’s: **Standard, 4K, and SE** as stated above. Two have USB cable connections to the RC: **Pro and Advanced**. The former three Phantom 3 models connect to paired mobile
devices, which control select functions on the aircraft via WiFi. These RCs have no hard-wired connection option. RIZER disables WiFi connections in the Android application. This precludes the use of Phantom 3 aircraft with WiFi-exclusive RCs. As such, RIZER only supports the Phantom 3 Pro and Advanced models, which are controlled via the RS GO 3 mobile application. For more information, visit rogue.diux.mil.

DJI Inspire 1

The Inspire 1 utilizes a USB style RC and is compatible with RS GO 3. As listed in Table 1, not all features supported by RIZER are offered by this platform as it has had the lowest demand signal from the DOD. Currently (although feasible), No Fly Zone removal for this platform is not supported.

DJI Matrice 100

The Matrice 100 utilizes a USB style RC and is compatible with RS GO 3. As listed in Table 1, not all features supported by RIZER are offered by this platform as it has had the lowest demand signal from the DOD. Currently (although feasible), No Fly Zone removal for this platform is not supported.

DJI Matrice 600/600 pro

The Matrice 600 series utilizes a USB style RC and is compatible with RS GO 3. As listed in Table 1, not all features supported by RIZER are offered to this platform largely due to hardware constraints and less development time being spent on the less prolific platform. Customer feedback/operational requirements are always welcome.

Recommendations

- DIU Rogue Squadron DOES NOT recommend the use of Phantom 3 Standard, 4K, and SE where even the lowest of mitigation would be required.

- DIU Rogue Squadron recommends RIZER for controlled use of any other legacy aircraft. Where mission/location constraints may dictate stricter mitigation measures, careful consideration should always be given to understanding the aforementioned differences between RIZER supported features respective to legacy versus contemporary aircraft (as defined above).