Analysis of Data Privacy and Security In Commercial DJI Drones

Brian C. Eam and John M. Rabang (Adviser: Daehee Kim, Ph.D.)
Department of Computer Science, California State University Stanislaus

Abstract

In the past few years, there has been an upsurge in the types of applications that drones are used in. As the market for commercial drone technology continues to expand, it is crucial to assess whether the security issues that have plagued earlier drone models have been addressed. In conducting this research, we utilized a myriad of software tools in an attempt to penetrate the software defenses of the DJI Mavic Air. We expect to find significant improvements in drone security where vulnerabilities were previously discovered.

Introduction

Drones primarily communicate with other electronic devices by emitting radio signals which propagate outwards in all directions. These signals can be received by any device with a compatible receiver. Data is usually encrypted so that only the intended recipient can decode the data being sent.

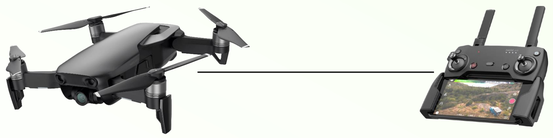

Figure 1: Types of data sent include flight data, GPS coordinates, and other sensor data like temperature and pressure. Drones can also record and live-stream video.

Although drones were originally developed only for military applications, the portability of drones coupled with their versatility made them suitable for other applications as well.

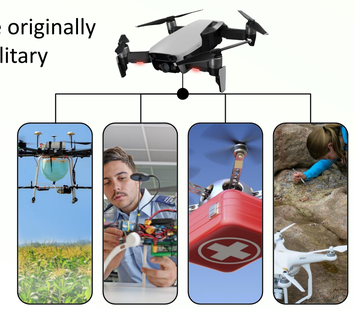

Figure 2: Drones are currently gaining popularity in the fields of agriculture, healthcare, engineering, geology, and many other areas.

Motivation

Studies indicate that people still hold negative perception towards drones. [1] Among their concerns is the possibility that their personal identifiable information stored on drones is not well-secured.

As drones are increasingly being integrated more into different sectors of our society, it is of utmost importance to protect these devices against cybersecurity attacks. Understanding how such attacks are conducted would aid drone manufacturers in strengthening the security of their products.

Related Work

Past research efforts established a few findings:

- The Mavic Air implements a hardware-level protection to prevent the drone from executing code from a tampered version of the drone's operating system. [2]
- Multiple devices are capable of connecting to earlier versions of DJI drones in a given instance. Sensitive data and settings could also be changed mid-flight. [3]

Security Breach Implications

Potential consequences of operating a drone that is subjected to security vulnerabilities:

- Spoofing of GPS coordinates enabling flight on restricted zones.
- Unauthorized users can gain total control of the aircraft.
- Personally identifiable information can be extracted.
- Pictures and media files stored locally within the device can be stolen.
- Attackers can disable sensors that are critical for flight operation.

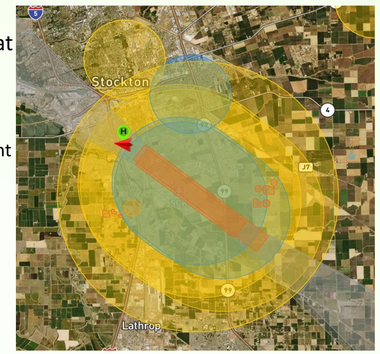

Figure 3: DJI Geo Zone Map. Each color corresponds to a zone with a particular set of flight rules.
Gray: Altitude zones (altitude is restricted)
Yellow: Warning zones (e.g. wildlife protection areas)
Blue: Authorization zones (authorized users only)
Red: Restricted zones (flight is not permitted)

Methodology

We have executed a variety of methods in an attempt to understand the security structure of the DJI Mavic Air drone.

- Used WireShark to analyze the captured data packets extract valuable information such as source and destination IP addresses and other types of data.
- Created VPN to funnel and isolate traffic coming to and from DJI GO 4 app. Data was captured using a packet capture app.
- Decompiled DJI GO 4 app to understand how the app communicates with the drone/remote controller.

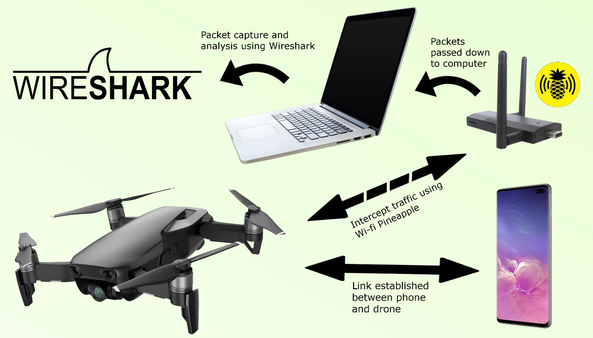

Figure 4: Packets sent between the Mavic Air and the controller device is intercepted, copied, and analyzed. Valuable identifying information such as source and destination IP addresses can be obtained through this method.

Results and Analysis

Here are some of the outcomes from our initial testing:

- We're not able to find valuable information such as stored passwords. Numerous files were also obfuscated after decompilation. Obfuscation was done intentionally by the developers of the app to prevent easy access to sensitive data.

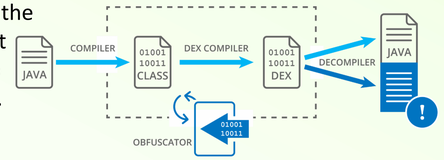

Figure 5: Code obfuscator transforms code into an unreadable stream of characters without affecting the app's functionality. Reverting code back to its original form is impossible in some cases. **[5]**

- The Mavic Air only allowed a single device to be connected to it at any point in time. This significantly made it harder to implement Denial of Service attacks.
- Mavic Air locally broadcasts an identification signal which acts like an "electronic license plate" that is detectable up to 5km. While the main purpose of this feature is for authorities to monitor airborne drones, such feature could open the drone to more sophisticated attacks in the future.
- We were able to unpack the flight logs gathered from the DJI Assistant app. However, the logs were encrypted.

```
HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "appkey" = "25552aad4fa54"
> Form item: "device" = "8d255536d60fad0645e75fbf7a075fe30f8b179a"
> Form item: "plat" = "1"
> Form item: "apppkg" = "dji.go.v4"
> Form item: "appver" = "2035859"
> Form item: "sdkver" = "30104"
> Form item: "networktype" = "wifi"
```

Figure 6: Some examples of information contained within the packets intercepted and captured from the DJI Go 4 app.

Conclusion

We have focused our testing on areas where a vulnerability has been previously identified. Analyzing the results, we conclude that the Mavic Air's security structure is more robust than its predecessors by a significant margin. It should be noted however that our findings does not imply that the Mavic Air's system is fully immune from other vulnerabilities. We plan to expand this research in the future by attempting to capture more critical information from the drone and find other ways on how they could be exploited.

References

[1] Victoria Chang, Pramod Chundury, and Marshini Chetty. 2017. Spiders in the Sky: User Perceptions of Drones, Privacy, and Security. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. ACM, New York, NY, USA, 6765-6776.
[2] Abhishek Vijeev, Vinod Ganapathy, and Chiranjib Bhattacharyya. 2019. Regulating Drones in Restricted Spaces. In Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications. ACM, New York, NY, USA, 27-32.
[3] Fernando Trujano, Benjamin Chan, Greg Beams, and Reece Rivera. 2016. Security Analysis of DJI Phantom 3 Standard.
[4] DJI Mavic Air. https://www.dji.com/mavic-air
[5] Decompiling obfuscated Android applications. https://www.guardsquare.com/zh-hans/blog/decompiling-obfuscated-android-applications