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.

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.
• Personal 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.

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.

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 decompression. Obfuscation was done intentionally by the developers of the app to prevent easy access to sensitive data.

Discussion
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 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.

Conclusion
• 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 traffic, 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.

References