How Vulnerable are Small Unmanned Aerial Systems (sUAS) to Cyber Attack?

Derian Bautista
Security Studies & International Affairs
Contact: Bautisd1@my.erau.edu

Abstract

Small unmanned aerial systems (sUAS), often referred to as 'drones,' consist of aeronautical hardware, CPU, RAM, onboard storage, 802.11 Wi-Fi or other radio communication links, sensors, camera(s), and a controller used by the pilot-in-command. Some have suggested that a drone is essentially a flying computer. As such, drones are potentially susceptible to cyber attacks. To test this hypothesis on one such drone, a Holy Stone HS100 (See Figure 1) was acquired to test against various forms of cyber attack. We identified cyber-related vulnerabilities and exploits for the drone, and then performed attacks to identify the feasibility, practicality, and significance of the attack, as well as their effects on the drone's ability to maintain a safe and functional flight.

Figure 1: HolyStone HS 100 Drone

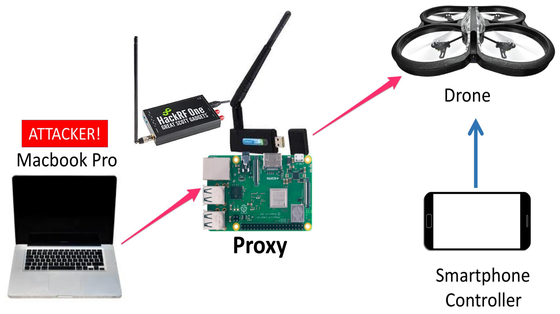

Figure 2: Hardware attack architecture

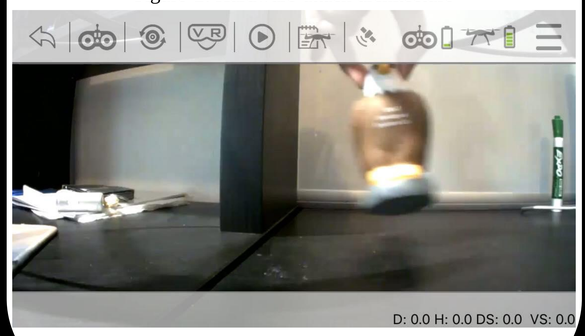

Figure 3: Deauthentication attack on the HS 100

Methodology

To create accurate research, we aimed at simulating these attacks through a set up that would be likely from a real-world bad actor. We developed a small, inexpensive, and portable attack platform consisting of the credit card-sized Raspberry Pi Model 3 B+ running Linux, which served as a network proxy, combined with (primarily) open source vulnerability assessment and attack software. Additional hardware included secondary external wireless adapters capable of running in monitor and promiscuous modes (either at 2.4 or 5GHz frequencies) See Figure 2. A small battery powered proxy allows a malicious actor to attack cyber-physical systems covertly by physically hiding the attack platform, as well as obfuscating attribution (e.g., MAC and IP address). A vulnerability assessment was conducted to identify vulnerabilities for the drone. The Holy Stone uses Wi-Fi for the First Person Video (FPV) feed, and RF for the Command & Control link. The drone also served as a Wi-Fi access point running DHCP. The Holy Stone also comes with a dedicated physical controller, and uses a smart phone for the FPV video feed.

Attack Hardware Cost

- Used Laptop: $150
- Raspberry Pi 3 B+: $40
- External Wireless Adapter: $25
- Software: Free

Results

The Holy Stone drone was vulnerable to several exploits and attacks:

1) Communication links between the controller and drone did not require authentication. Multiple users could connect to the drone simultaneously, and using a de-authentication attack, allow a threat actor to take control of the drone.
2) Exposed unencrypted telnet and FTP services. (Note: The drone's FTP server could not be connected to.)
3) No authentication mechanism in place for login via telnet. This allows multiple users to connect to the drone without authenticating.
4) Telnet access dropped the user into an unrestricted superuser account. Using the "turnoff" and "reboot" commands dropped the FPV link from the drone to the controller, requiring a physical reboot of the drone in order to reconnect.
5) A de-authentication attack was performed on the FPV video link between the controller and the drone, resulting in a loss of the FPV video feed (See Figure 3).
6) No authentication was required to connect from the smart phone (used for FPV) and the drone. This link was unencrypted, which allowed us to eavesdrop on the connection.

Conclusion & Recommendations

The purpose of this research was to identify vulnerabilities and exploits related to a single hobbyist drone. We found that the drone provided remote access without any mechanism for authentication, and the communication links were not encrypted. When connecting over telnet or FTP, users were dropped into a superuser account, which has unrestricted access to commands, files, and directories. We identified onboard destructive commands, including commands to delete files and directories, kill processes, and turn the drone off. We performed Wi-Fi de-authentication attacks resulting in disconnects between the controller and drone. Uploading and downloading files via FTP could theoretically be possible on the HS100 should the FTP server be running. While this drone has multiple vulnerabilities, these results are by no means generalizable to other drones, and certainly not military drones, which are entirely different animals.