Autonomous Drone Control

John Wright
Raytheon
John_b_wright@raytheon.com

Estimated Team Size: 3

Technologies Expected: OpenWRT, Ozone Widget Framework (OWF), WiFi, iOS, Android

Description: A drone engineered to autonomously seek out, hack, and wirelessly take full control over other drones within wireless distance.

This method to autonomously seek out and take control of other drones via RF interface within the RF range of the quadcopter allows for greater flexibility in tracking the target drone, allows for maintaining a greater range from the target, to avoid detection, and allows the operator to maintain a safer distance. The key is to develop methods and processes to scale up results to other platforms

Tasks:
Task 1 – Vulnerability Research - The quadcopter is controlled using a 5.8GHz remote. Telemetry and live video preview is available through the DJI Vision app (iOS/Android), which connects to the Phantom through a WiFi-network provided by a device called the Range Extender. Range Extender is a small Linux system based on OpenWRT. Document findings.

Task 2 – Exploit Development - Use OpenWRT application to reveal vulnerabilities and develop exploits for those vulnerabilities. Document findings

Task 3 – Deliver Exploit - Use Wifi Pineapple to exploit OpenWRT and provide Situational Awareness (SA) to the Ozone Widget Framework (OWF). Drone detects the wireless signal sent out by a target drone, injects WiFi packets into the target's connection, de-authenticates it from its real controller and then authenticates it to the master drone. Document vulnerability and payload delivery system.