Drone Security and the Mysterious Case of DJI's DroneID

- I. INTRODUCTION
  - In summary, our main contributions are Security Analysis、DroneID、Drone Fuzzing
- II. PRIMER ON DJI DRONES
  - A. Communication Interfaces and Protocols
    - USB
    - UART -- Universal Asynchronous ReceiverTransmitter
    - Wireless Physical Layer: Bluetooth, WiFi, and OcuSync
    - DUML -- DJI Universal Markup Language
    - DJI Fly / DJI Go 4 App
  - B. Drone Firmware
    - Depending on their complexity, the drones we analyzed use different operating systems (OSes).
  - C. Drone Hardware
    - Flight Controller
    - Video encoding & collision avoidance SoC
    - Remote Control
    - Transceiver
    - WiFi / Bluetooth Chip
    - Additional Sensors and Other Hardware
  - D. Wireless Physical Layer
- III. SECURITY ANALYSIS WITHOUT PHYSICAL ACCESS
  - A. Threat Model 1: Passive Attacker
  - B. Wireless Link
    - DroneID Receiver
    - Spectrum Analysis
    - Demodulation
    - Decoding
    - Performance
    - Performance
- IV. SECURITY ANALYSIS WITH PHYSICAL ACCESS
  - A. Threat Model 2: Active Attacker
  - B. Overview
  - C. Initial Manual Analysis and Interactive Access
    - Manual Static Analysis
      - a) S1 SoC Firmware Signature Verification Bypass:
      - b) SDRH File Delivery via Fastboot
      - c) Backdooring the Sparrow Transceiver Firmware
    - Hardware Analysis
  - D. Dynamic Analysis – Fuzzing
    - a) Drone Fuzzer Design
      - DUML Protocol
      - UI Oracle
      - Input Blocks
      - Fuzzing Loop
    - b) Implementation
    - c) Experiment Setup
    - d) Results
    - e) Case Studies
      - (1) Arbitrary Command Execution (#14).
      - (2) Arbitrary Serial Number (#15)
      - (3) Unlocking ADB Root shell (#1).
    - f) Roadblocks and Limitations of Fuzzing
- V. DISCUSSION AND LESSONS LEARNED
  - a) Current State of Drone Security
  - b) EU and US Regulations for Drone Identification
  - c) Active Attacker without Physical Access
  - d) Data Integrity
  - e) Applicability to Other Vendors
  - f) Ethical Considerations and Research Artifacts
  - g) Lessons Learned
- VI. RELATED WORK
  - a) Drone Research
  - b) Fuzzing
- VII. CONCLUSION