Project Activity Overview

Drone Project: Security Analysis- attacks and Countermeasures

By

Vishal Dey

Motivation

- Spying and monitoring
- Photography
- Defence
- Handling situations like firefighting, human rescue and adverse terrain
- Delivering goods by Amazon and Domino’s
- Security threats

DJI Phantom 4 Pro

- **Vulnerabilities**
  - Vulnerabilities in DJI SDK: crack the DJI SDK, remove authentication between server and DJI app by decompiling and patching code
  - Reverse Engineering firmware
  - GPS Spoofing over DJI Phantom 4 Pro using LabSat
  - Control and Video transmitted using RF, thus can be scanned and manipulated using SDR equipments like HackRF obscuring live feed

DJI Phantom 4 Pro

- **Countermeasures**
  - Use encryption/packer to protect library files.
  - Use obfuscator to prevent decompiling, reverse-engineering files
  - SDK authentication, now being done only between the app and server, drone must also be included in the one-time authentication.
  - Anti-spoofing and anti-jamming
  - Detect fake GPS signals using latency, bit delays, checking GPS subframe data
  - Encrypt the entire firmware binary, the encryption key must be stored in the hardware, some of the binaries in P4 pro are encrypted and signed

Parrot Bebop 2

- **Vulnerabilities**
  - Open WiFi: multiple connections, vulnerable to all WiFi attacks, deauthenticate the owner
  - Open FTP access: root access to entire FS is possible changing some config files
  - Open telnet with root access: crash-land the drone killing the main process: ‘dragon-prog’
    - *telnet 192.168.42.1*
    - *kill -9 $(ps -e | grep ‘dragon-prog’)*
  - MAC Spoofing

Parrot Bebop 2

- **Countermeasures**
  - Adding WPA security to the WiFi
  - Hidden SSID so that it does not appear in the available networks
    - Open telnet and execute the command:
    - bcmwl closed 1
  - MAC address filtering
    - Open telnet and execute the command:
    - bcmwl mac <MA:CA:DD:ID:01> <MA:AC:DD:ID:02>
    - bcmwl macmode 2
  - Add Telnet password

Future Work

- Radio Frequency Spectrum Analysis for DJI Phantom 4 Pro
- Design of a video encryption module for reliable transmission
- ArduPilot for Bebop 2

Conclusion

- Harder than expected due to non-determinism of robotics and unavailability of proper hardware
- DJI Phantom4 Pro is much more secure than Parrot drones as Phantom4 Pro communicates and sends video over RF which requires costly hardware to intercept whereas Parrot Bebop uses open WiFi
- Drones shall remain vulnerable to GPS spoofing unless receiver also have the capability to detect spoofing like SAASM used by military- thus need for developing anti-spoofing and anti-jamming recivers

Q & A

Thank You