A Security Analysis of drones: Attacks and Countermeasures

Vishal Dey
School of Computer Science and
Technology
Indian Institute of Engineering
Science and Technology
Shibpur, Howrah - 711103
Email: vishal.dd2014@cs.iiests.ac.in

***Abstract*—The abstract goes here.**

I. Introduction

II. Drones Architecture

A. DJI Phantom 4 Pro

B. Parrot Bebop 2

III. System Overview

A. DJI Phantom 4 Pro

1) Drone:

2) Remote Controller:

3) Mobile Device:

B. Parrot Bebop 2

1) Drone:

2) Mobile Device:

IV. Motivation

V. Related Works

A. WiFi insecurities

B. SkyJack

C. Maldrone

VI. Attacks performed

A. DJI Phantom 4 Pro

1) Cracking DJI SDK: removing authentication between app and mobile

2) Reverse engineering firmware:

3) GPS Spoofing:

B. Parrot Bebop 2

1) WiFi attacks: multiple Wifi connections

2) Deauthenticating owner:

3) Open Telnet: shut down the drone

4) Open FTP port:

5) Snooping into the WiFi and packet capture: flight commands and video are passed as UDP packets and the initial connection setup is done by TCP

6) Additional vulnerabilties:

a) Reversing firmware:

b) Changing config files: modifying /etc/passwd file may brick the drone or changing some passwords may cause the owner not be able to telnet into it, or connect to the drone

VII. Comparison of two drones

VIII. Future Work

IX. Proposed countermeasures

X. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

[1] Andrew J. Kerns *Unmanned Aircraft Capture and Control via GPS Spoofing*, Journal of Field Robotics 31(4), July 2014