Title!!!!!!!!!

Yan Songyang
Xi'an Jiaotong University
1932 Wallamaloo Lane
Wallamaloo, New Zealand
lapalacayim@gmail.com

Li Siyu
Institute for Clarity in Documentation
P.O. Box 1212
Dublin, Ohio 43017-6221
webmaster@marysville-ohio.com

Wan Ziyi
The Thørväld Group
1 Thørväld Circle
Hekla, Iceland
larst@affiliation.org

Ye Junyan
Brookhaven Laboratories
Brookhaven National Lab
P.O. Box 5000
lleipuner@researchlabs.org

Li Hanxing
NASA Ames Research Center
Moffett Field
California 94035
fogartys@amesres.org

ABSTRACT

Abstract here

Categories and Subject Descriptors

H.4 [**Input/Output and Data Communications**]: Data Communication Devices

General Terms

Theory

Keywords

Drone, Remote Control

1. INTRODUCTION

What is UAV

Many many

Control methods

We focus on radio and Wi-Fi

2. ATTACK ON THE AR.DRONE 2.0

2.1 Technical Specification

The AR.Drone 2.0, equipped with various sensors, uses a Linux operating system based on the kernel version 2.6.27.44. All control commands, telemetry data and the video streams are handled via (unencrypted) 2.4GHz WLAN communication with the controlling device. Users can use iOS and Android devices to control the drone via the official application AR.FreeFlight. Figure 2.1 shows the controller interface running on iPad.

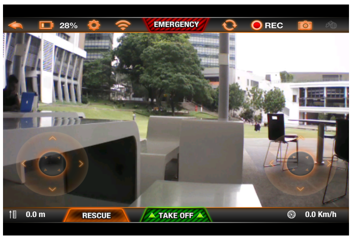

Figure 1: Parrot AR.FreeFlight control interface

2.2 Highjack Attack

2.2.1 AT Commands

According to AR.Drone Developer Guide[3], the controller uses port 5556 to send commands in a UDP packet to port 5556 of the drone. These commands are called AT commands. Because of the instability of UDP connection, the communication protocol allocates ascending sequence number to different commands. This prevents older commands with lower sequence numbers incoming later (due to transmission errors) from executing[2]. This protocol provides an attack method. Attacker can conduct a man-in-the-middle attack with a sequence number which is always higher than the one being sent from the legitimate user.

An AT command begins with the fixed string "AT*", followed by either REF, PCMD or CONFIG. REF commands are single commands such as land or takeoff. PCMD commands are used for flight control. CONFIG commands are used for sending new configuration. To take over a drone, using REF commands is enough. As described in[3], the format command of REF command is

$$AT * REF =< sequence >, < UI > \tag{1}$$

Different REF commands are listed in table 1.

2.2.2 Attack Process

The attack consists of the following phases:

Table 1: REF commands

Command	Function
ATREF=<sequence>,290718208	Take off
ATREF=<sequence>,290717696	Land
ATREF=<sequence>,290717952	Emergency Stop

1. Connection to the drone,
2. Determination of the IP address of the control device,
3. Sending fake land packets with high sequence number.

After booting up, the drone will set up a Wi-Fi hotspot named ”ardrone2_” followed by a random number with 6 digits. The connection to the drone is possible because the network is not protected by any encryption or other access restriction techniques. The ip address of the drone itself is always 192.168.1.1/24.

Once the connection has been built, attacker can scan the subnetwork to determine the IP address of the control device.

To prevent multiple phones trying to control the drone, the drone only accepts packets from the source IP of the controller. But since it’s UDP, it’s simple to spoof the IP address of the controller. Attacker can send a land command to force the drone to come to the ground.[1]

2.2.3 Using Android Device to Conduct Attack

Design an Android App

3. ATTACK ON HUBSAN BLABLABLA

//TODO

4. DISCUSSIONS

gugugu

5. CONCLUSIONS

We..... and....., however... it’s..... great!

6. ACKNOWLEDGMENTS

Thank you, you and You!

7. REFERENCES

[1] drone-hacking. https://github.com/markszabo/drone-hacking. Accessed: 2016-05-11.

[2] J. Pleban, R. Band, and R. Creutzburg. Hacking and securing the ar.drone 2.0 quadcopter - investigations for improving the security of a toy. 01 2014.

[3] P. E. Stephane Piskorski, Nicolas Brulez and F. D’Haeyer. *AR.Drone Developer Guide*. 5 2012.