Attack On Drones

Yan Songyang
School of Software Engneering
Xi'an Jiaotong University
lapalacayim@gmail.com

Li Siyu
College of Cybersecurity
Sichuan University
sy_lee_real@icloud.com

Wan Ziyi
College of Cybersecurity
Sichuan University
scuderrickwan@gmail.com

Ye Junyan
School of Information and Software Engineering
University of Electronic Science and Technology
2239308357@qq.com

Li Hanxing
School of Cyber Science and Engineering
Wuhan University
t0918555@u.nus.edu

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
The drone, also known as the unmanned aerial vehicle(UAV), is the Aircraft without any human pilot controlling inside. Drones are widely used in many fields, including military, industry, agriculture, photography and so on. We can simply divide them into civilian and military.

The civilian drones, which we are focusing on, are applied to countless aspects of our lives. Farmers use drones to spray pesticides and monitor crop's growth. E-commerce companies such as Amazon use drones to deliver express. Photographers use drones to create from a special perspective. And also people, just like us, using drones just for fun. All in all, the use of drones has penetrated into many aspect of our lives.

Quadcopter, one of the most common types of civilian drones, using Wi-Fi connection or 2.4GHz radio as its way of communication, generally. Some professional drone companies such as DJI may have their own private communication protocols and they are beyond our research.

Within Wi-Fi connection, a drone is WLAN AP(Access Point) itself. If the user wants to control the drone, he needs to connect his smartphone(or other smart devices) with control application to the WLAN created by the drone. And there may be steps to authenticate during the connection establishment process. Then userâĂŹs smartphone could issue instructions to the drone and receive real-time image transmission from drone, after getting the Wi-Fi connection to the drone.

And the other way of communication is using 2.4GHz radio. This is a much simpler communication mechanism, which means it has a lower cost and usually used on low-end drones. 2.4GHz radio technique is widely used in lots of remote controls, and remote control used in toys including drones is the one of the application scenarios. The remote control sending instructions via an agreed frequency in 2.4GHz ISM, and the drone receive these instructions. The massage transmit via 2.4GHz radio broadcasts to anyone that can receive it, which means there isnâĂŹt any connection between remote control and the drone. Not to mention identity verification. So this is a primitive way of control, which is easy to attack.

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.

2.2 Highjack Attack
2.2.1 AT Commands
According to AR.Drone Developer Guide[4], the controller uses port 5556 to send commands in a UDP packet to port

Figure 1: Parrot AR.FreeFlight control interface

Table 1: REF commands

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

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[3]. 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[4], the format command of REF command is

$$AT * REF =< sequence >, < UI > \quad (1)$$

Different REF commands are listed in table 1.

2.2.2 *Attack Process*

The attack consists of the following phases:

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.

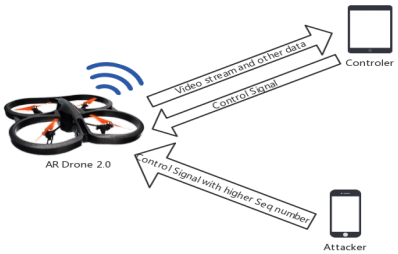

Figure 2: Hijack Attack Scenario

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*

After the previous analysis, we have mastered the WIFI-controlled drone attack method and the whole process. The drone uses the application(FreeFlight 2.0) to control takeoff, landing, flight direction and capture image acquisition. We decided to create another Android application to attack this drone. Then this application can be controlled by a third party and take control of the drone, force the drone to land, and modify the flight direction.This attack scenario is shown in Figure2.2.3.

The attack consists of the following phases:

1. The third-party user uses the Android packet capture application to obtain the target drone IP address,
2. After the third-party user enters the obtained IP address in this application, he can click the button to send a command to control the drone.

Jpcap provides a class JpcapSender for sending packets, which can be used to send IPPackets and its subclasses, including IPPacket, ICMPPacket, TCPPacket, UDPPacket[2]. After defining a corresponding package, we can use the SendPacket function to send packets. Meanwhile, Jpcap can be used to construct IP data packets to implement sending fake IP.

The creation of this new Android app is primarily convenient for any third-party user who can hijack drones directly at the application layer.

3. ATTACK ON HUBSAN

3.1 Communication Principle

Communicating via 2.4GHz radio is widely used in many scenes, and controlling is one of them. The remote control sending instructions via an agreed frequency in 2.4GHz ISM, and the drone receive these instructions. In many types of drones, such as the Hanson H107 Drone we used in our experiment, the massage transmit via 2.4GHz radio broadcasts to anyone that can receive it, which means there isn't

any connection between remote control and the drone. Not to mention identity verification. Because of the broadcast mechanism and connectionless transmission without identifications, this is a primitive way of control, which is easy to attack.

3.2 Attack

Since this drone use broadcast to pass signals. ThereâĂŹs no connection mechanism between controller and drone and it does not use a mechanism to verify the controller, the attack on this drone is relatively simple. We can use the LimeSDR device to attack the drone. Firstly, we can set up the attack environment on the PC with LimeSDR, gqrx and GNURadio, and then monitor the radio signal in GNURadio. The running drone can simultaneously monitor the radio signal at 2.4GHz and receive it. To a specific broadcast band signal, the corresponding command can be obtained by decoding.

3.3 Result

Since the drone does not have a mechanism to establish a connection. We can't get his full control, all we can do is interfere with the controller's control, making it insensitive or ineffective. The easiest way is to replay the attack and resend the received signal after a period of time. At this point, the signal from LimeSDR will cause the drone to get out of control or even fall.

4. DISCUSSIONS

gugugu

5. CONCLUSIONS

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

6. ACKNOWLEDGMENTS

We would like to offer our sincere appreciation and thanks to Professor Hugh Anderson for his guidance, enthusiasm and encouragement during the project. He is always generous in providing all kinds of equipment we might need and we are equally grateful to the School of Computing for this. And we also thank our teaching assistant Tan Wang Leng for his insight and expertise. Without them, we wouldn't have gone thus far.

7. REFERENCES

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

[2] C. Peng. Jpcap-based tcp/ip packet capture and transmission. *Journal of Changji University*, 2008.

[3] 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.

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