It’s a Bird… It’s a Plane… It’s Drone!

written by Mert SARICA | 1 September 2016

Unmanned Aerial Vehicles (UAVs), commonly known as drones, which can be easily purchased online with just a click and are difficult to track, have recently started to pose a threat to air transportation and privacy, as we can see in the news.

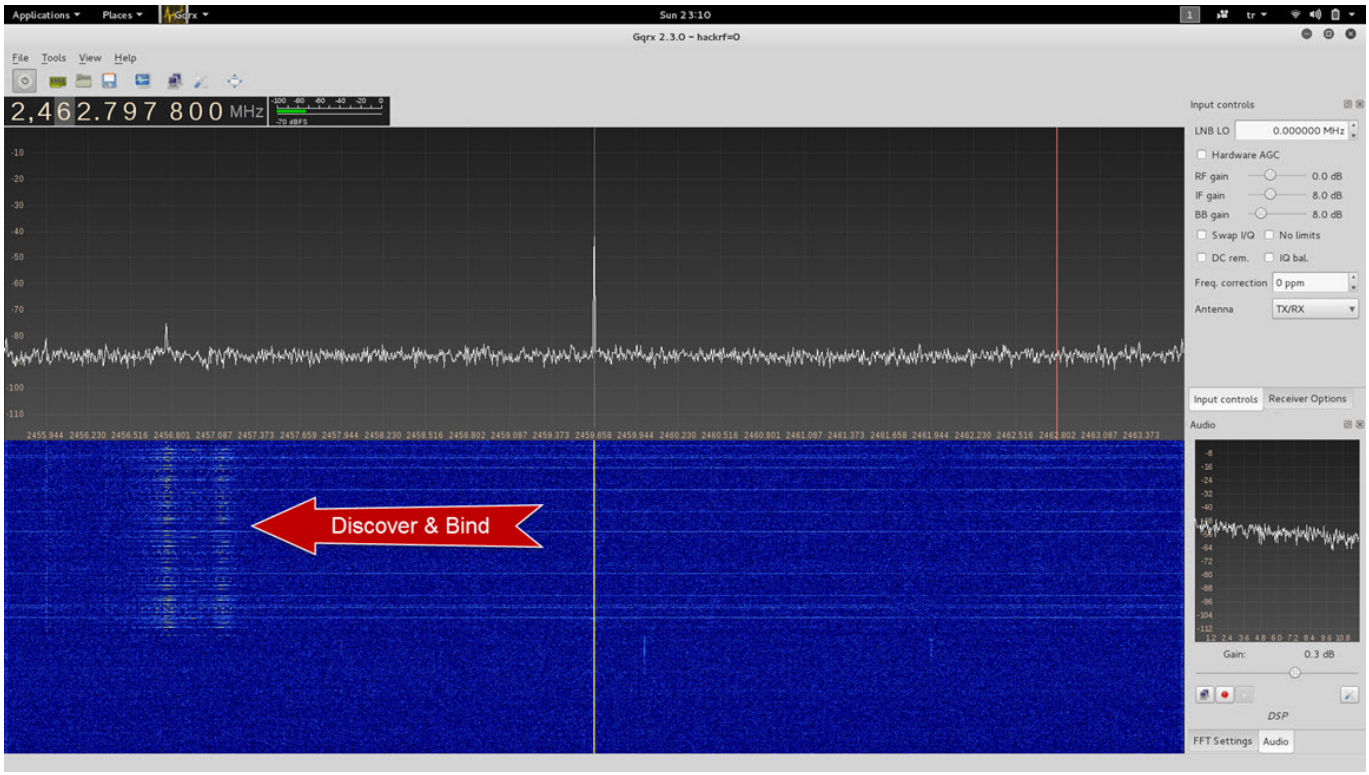
Given this situation, the fight against drones is becoming increasingly important not only worldwide but also in our country. When we look at the studies being done to fight against drones around the world, the Dutch police who hunt drones with eagles, the Tokyo police who catch drones with nets, and the Skyjack study, which allows other drones (Parrot AR.Drone 2) to be hacked, maybe among the most creative works in this field.

In early 2014, I also took my first step into the drone world with the Hubsan X4 H107C (you can access the example video here). As a security expert, I had some questions that I couldn’t shake off while flying the drone. The most curious thing for me was whether the connection between the drone and the controller, which is controlled by the person who is flying the drone, could be manipulated or replayed? If the drone communicated via WIFI, then I could try to hack the WIFI network between the drone and the phone using various tools and devices like Sammy, and try to take over the connection (hijack) or manipulate it like in the Skyjack study. However, my drone, the Hubsan X4 H107C, communicates using its own protocol on the 2.4 GHz frequency, and I thought that analyzing the protocol by monitoring the SPI communication using a Logic Analyzer would be a tedious and costly task.

In this tedious path, to avoid pulling out my hair, I searched on Google to see if anyone had previously analyzed this protocol and I came across Jim Hung’s work (#1, #2, #3, #4). According to Jim Hung’s study, which was done using a Logic Analyzer, it seemed that hijacking or manipulating the

connection between the controller and the X4 theoretically possible, but practically (at least for me) it was not very easy. Based on this study, I began to think about how I could repeat (replay) the signal that was sent, and the HackRF One came to mind, which I had previously experienced that could greatly simplify my job in my garage door research.

Using Jim's study as a guide, my first step was to use the Gqrx SDR aracı tool in Kali to start monitoring the frequency range of 2400 MHz (2.4 GHz) and incrementing by +10 MHz (2410, 2420, 2430…) to detect the discovery (discovery) packet that the controller sends when searching for the X4. I was easily able to detect the discovery packet, and when the X4 responds to the packet, I didn't have much trouble detecting the X4 on that frequency.



After finding the relevant frequency, I then use the command "X4 – turn the propellers (throttle – left stick up)" from the remote control, then began recording the relevant signal with the HackRF One device using the following command help.

```
hackrf_transfer -r Hubsan-2442Mhz-8M-8bit-1.bin -f 2442000000 -l 40 -n 5
```

Then, by sending the signal that I recorded with the following command to the relevant frequency, I saw the X4's propellers move and successfully repeated

the signal between the X4 and the remote control. In this replay attack, I sometimes saw the connection between the X4 and the remote control cut off, which meant that the X4 fell. (Not too bad for fighting against a drone, don’t you think ? :))

```
hackrf_transfer -t Hubsan-2442Mhz-8M-8bit-1.bin -f 2422000000 -x 47
```

In conclusion, it appears that it is possible to misuse the X4 H107C by performing a replay attack with HackRF One (such as causing it to fall). It could be an interesting detail in the fight against drones.

Hope to see you in the next article.