Bir Drone Gördüm Sanki

written by Mert SARICA | 1 September 2016
If you are looking for an English version of this article, please visit here.

Her bütçeyeuygun İnsansız Hava Araçlarının (İHA), genel olarak bilinen adıyla droneların bir tık ile internetten satın alınabildiği ve kolay kolay kayıt altına alınamadığı şu günlerde, hem havayolu taşımacılığı hem de mahremiyet için tehlike oluşturmaya başladığına yazılı ve görsel medyada yer alan haberlerde sıkça rastlamaya başladık.

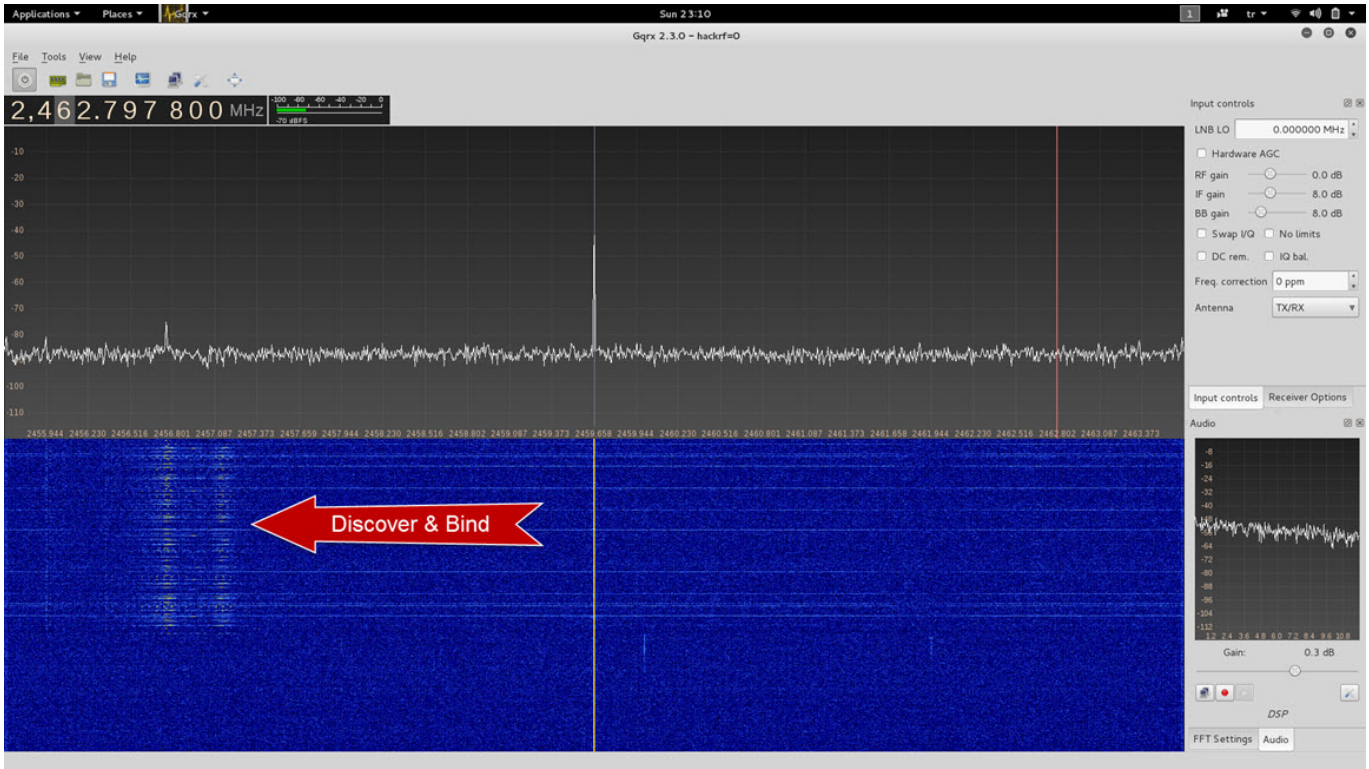
Durum böyle olunca da, dronelar ile mücadele dünyada olduğu kadar ülkemizde de önem kazanmaya başladı. Dünyada dronelar ile mücadele adına yapılan çalışmalara baktığımızda, kartal ile drone avlayan Hollanda Polis'i, ağ atan drone ile droneları avlayan Tokyo Polis'i, diğer droneları (Parrot AR.Drone 2 ise) hacklemeye imkan tanıyan Skyjack çalışması belki de bu alanda en yaratıcı çalışmaların başında geliyor diyebiliriz.

2014 yılının başında ben de Hubsan X4 H107C ile (örnek videoya buradan ulaşabilirsiniz) drone dünyasına adım attım. Drone'u uçururken bir güvenlik uzmanı olarak aklımı kurcalayan bazı sorular oluyordu. Bunlardan en çok merak ettiğim ise drone uçuran bir kişinin kumanda ile drone arasındaki bağlantısı manipüle edilebilir veya tekrarlanabilir miydi ? Eğer drone WIFI üzerinden haberleşiyor olsaydı o zaman Sammy gibi drone ile telefon arasındaki WIFI ağını çeşitli araçlar ve cihazlar yardımı ile kırabilir ve Skyjack çalışmasında olduğu gibi bağlantısını ele geçirmeye (hijack) veya manipüle etmeye çalışabilirdim. Ancak sahip olduğum drone olan Hubsan X4 H107C, kendine özgü protokolü ile 2.4 GHZ frekansından haberleştiği için Logic Analyzer yardımı ile SPI iletişimini izleyerek protokolü çözümlemenin zahmetli ve maaliyetli olacağını düşündüm.

Bu zahmetli yolda, ağrımış saçlarımı dökmeme adına önceden bu protokolü inceleyen olmuş mu diye Google'da arama yaptığımda, Jim Hung'un çalışması dikkatimi çekti. (#1, #2, #3, #4). Jim Hung'un Logic Analyzer ile

gerçekleştirdiği çalışmaya göre kumanda ile X4 arasındaki bağlantıyı çalmak (hijack), manipüle etmek teoride olabilir gibi görünse de pratikte (en azından benim için) pek kolay durmuyordu. Bu çalışmadan yola çıkarak ben de gönderilen sinyali nasıl tekrarlayabileceğimi (replay) düşünmeye başladığımda, aklıma garaj kapısı araştırmamda işimi oldukça kolaylaştırabildiğini tecrübe ettiğim HackRF One geldi.

Jim'in çalışmasının ışığında ilk iş olarak Kali'de yer alan Gqrx SDR aracı ile 2400 MHz (2.4 GHz) frekansından başlayacak şekilde frekansı +10 MHz arttırarak (2410, 2420, 2430…) izlemeye başladım. Kumandanın açıldığında X4'ü aramak için gönderdiği keşif (discover) paketini kolaylıkla tespit edebildim. X4'ten keşif paketine istinaden gelen yanıt üzerine kumanda ile eşleştiğinde ise X4'ü ilgili frekansta tespit etmekte çok zorlanmadım.



İlgili frekansı bulduktan sonra ise kumandadan X4'e pervaneleri çevir (gaz verme – sol çubuk yukarı) komutunu verdikten sonra ilgili sinyali HackRF One cihazı ile aşağıdaki komut yardımı ile kayıt altına almaya başladım.

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

Ardından bu defa aşağıdaki komut ile kayıt altına aldığım sinyali ilgili frekansa gönderdiğimde X4'ün pervanelerinin hareket ettiğini gördüm ve

başarıyla X4 ile kumanda arasındaki sinyali tekrarlayabilmiş oldum. Tekrarlama saldırısında zaman zaman X4’ün kumanda ile olan bağlantısının koptuğunu gördüm ki bu durum X4’ün düşmesi anlamına geliyordu. (Drone ile mücadele adına fena sayılmaz, ne dersiniz ? :))

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

Sonuç olarak X4 H107C’nin HackRF One ile tekrarlama saldırısı yapılarak kötüye kullanılması (düşürülmesi gibi) mümkün gibi görünüyor. Dronelar ile mücadelede ilginç bir ayrıntı olabilir.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.