RF Dünyası ve Güvenlik

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

Çocukluğumdan beri uzaktan kumanda ile kumanda edilebilen garaj kapıları her zaman ilgimi çekmiştir. Yaşım ilerledikçe ve mesleğimde de ilerledikçe, merakımı pratiğe dönüştürmeye ve RF ile haberleşen bu sistemleri, güvenlik araştırmacısı gözüyle incelemeye karar verdim.

Kumanda ile kapılar nasıl haberleşiyor, sinyalleri izlemek mümkün mü, deneme yanılma (brute force) saldırısı veya daha önce gönderilmiş ve kayıt altına alınmış sinyalleri tekrarlama (replay) saldırısı ile tekrar göndererek kapıları açmak mümkün olabilir mi ? gibi soruları kendi kendime sormaya başladıkça, kendimi RF okyanusunu kayıkla geçmeye çalışan cesur, hevesli ama tecrübesiz bir denizci olarak görmeye başlamıştım.

Yıllar içinde RF ile ilgili çok sayıda makale okudukça, bilgim ile birlikte aklımı kurcalayan sorular da bir o kadar arttı. Tam bu sorular altında ezilmeye başlamışken, imdadıma NOPcon güvenlik konferansında da sunumunu izleme fırsatı bulduğum Ahmet CİHAN yetişti ve RF dünyasının sis perdesi benim için aralanmış oldu.

2014 yılından bu yana, bıkmadan usanmadan RF dünyası ile ilgili aklıma takılan tüm sorulara gece gündüz demeden, içtenlikle yanıt verdiği ve bugün bu yazıyı kaleme alabilmemde fazlasıyla emeği geçtiği için Ahmet CİHAN'a teşekkürü bir borç bilirim :)

Yazının ikinci paragrafında belirtmiş olduğum sorulara yanıt aradığım bu çalışmada, ilk işim sırasıyla kumandanın hangi frekansta çalıştığını bulmak (büyük olasılıkla 433 MHZ'dir ancak 315 MHZ de olabilir.) ve hangi modülasyonu kullandığını bulmak (büyük ihtimalle Amplitude-Shift Keying (ASK)'dır ancak FSK, PSK da olabilir.) oldu.

Yakın zamanda okuduğum Abusing the Internet of Things kitabının yazarı, modülasyonu güzel bir benzetmeyle anlatmıştı. Aynı benzetme üzerinden ilerleyecek olursam, ağzımızdan çıkan basınç dalgaları, karşı tarafa ulaşırken hava dediğimiz bir ortamda ilerlemektedir. Bu örneğe göre ağzımızdan çıkan basınç dalgasının, havada ilerleyecek dalgaya çevrilmesine (radyo sinyaline) modülasyon diyoruz. Bu dalganın (radyo sinyalinin), karşı

tarafa iletilmesi esnasında kullandığı başka bir dalgaya ise taşıyıcı sinyal (carrier wave) diyoruz.

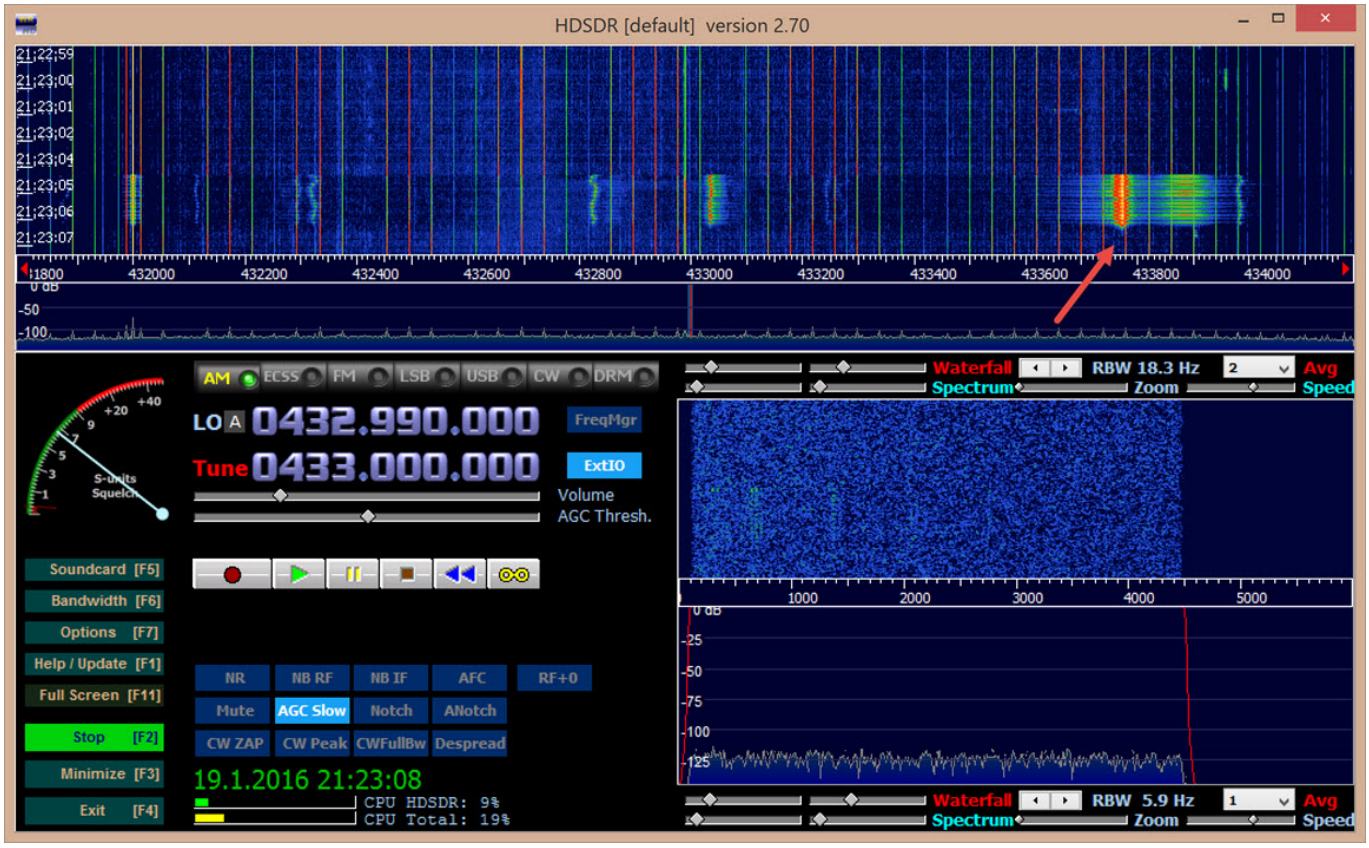
Kumandanın hangi frekansta çalıştığını bulmak için kumandanın içini açıp rezonatörün üzerinde yazan rakama (R433T gibi) bakabilirdim. Tornavida ile çok fazla uğraşmak istemediğim için Deal Extreme'den 10$'a satın aldığım RTL2832U dijital tv alıcısı ve ücretsiz temin edilebilen HDSDR programı ile frekansı tespit etmeye karar verdim.

Dijital TV alıcıyı USB bağlantı noktasına bağladıktan ve HDSDR programını çalıştırdıktan sonra frekansı 433 MHZ'e (ISM bant planlaması gereği tahmin yürüttüm), modülasyonu ise AM olarak ayarlayıp F2 (start) tuşuna bastığımda, kumandanın ilgili bandı ve frekansı kullandığını gördüm. (Kumanda üzerinde herhangi bir butona bastığınızda, ilgili frekansta bir hareketlilik görüyorsanız bu durum, kumandanın ilgili frekansta veya o frekansa yakın bir frekans aralığında çalıştığına işaret etmektedir.)

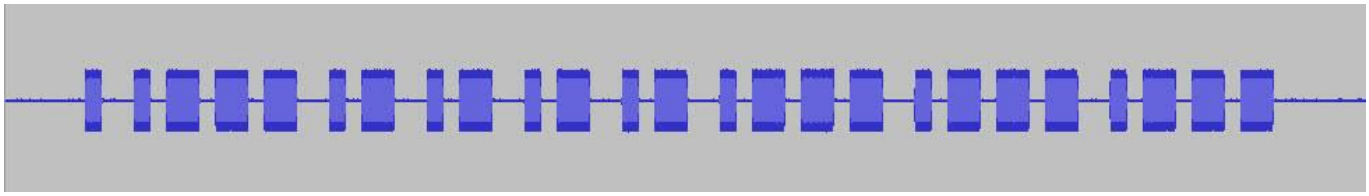

SCORPION


ON
DIP
1 2 3 4 5 6 7 8 9 10


DVB-T+DAB+FM



Modülasyonu tespit etmek için ise HDSDR'de kayıt ettiğim sinyali Audacity adındaki ücretsiz ses düzenleme ve kaydetme yazılımı ile incelediğimde bunun ASK / OOK olduğunu gördüm. Sadece kumandada yer alan mikro anahtar dizisine (dipswitch) bakarak, gönderilen sinyalin 10 bit olabileceğini düşünebilirdim ancak kayıt ettiğim sinyale Audacity ile baktığımda, bunun aslında 12 bit olduğunu gördüm. (Sondaki bit ile aslında 13 bit gibi görünse de 12 bit olduğunu ve son bitin altbaşlık (footer) olduğunu yazının devamında göreceksiniz.)



Sinyali kendi içinde çözümleyip, aşağıdaki resimde olduğu gibi yüksek, alçak ve açık işaretleri, 0, 1 ve O şeklinde veriye çevirdiğimde, mikro anahtar dizisi ile örtüştüğünü ve başarılı bir şekilde sinyali veriye çevirdiğimi kısaca kumandayı kopyalayabilecek veriye (rf koduna) sahip olduğumu

görebildim.

Bundan sonra gerisi ister Arduino, ister Raspberry Pi ile veriyi ASK ile modüle edip, garaj kapısına göndermeye kalmıştı. Tabii bunun için öncelikle 4$'ı gözden çıkarıp bir RF alıcı ve verici kiti almam gerekti. (Bu gibi güvenlik araştırmalarında zahmete giremem diyenleriniz var ise, benim gibi 330$ verip HackRF One kiti alarak tüm bu zahmetten kurtulabilirler. Bu arada ücretsiz Software Defined Radio (SDR) ve HackRF One eğitimine de buradan ulaşabilirsiniz.)

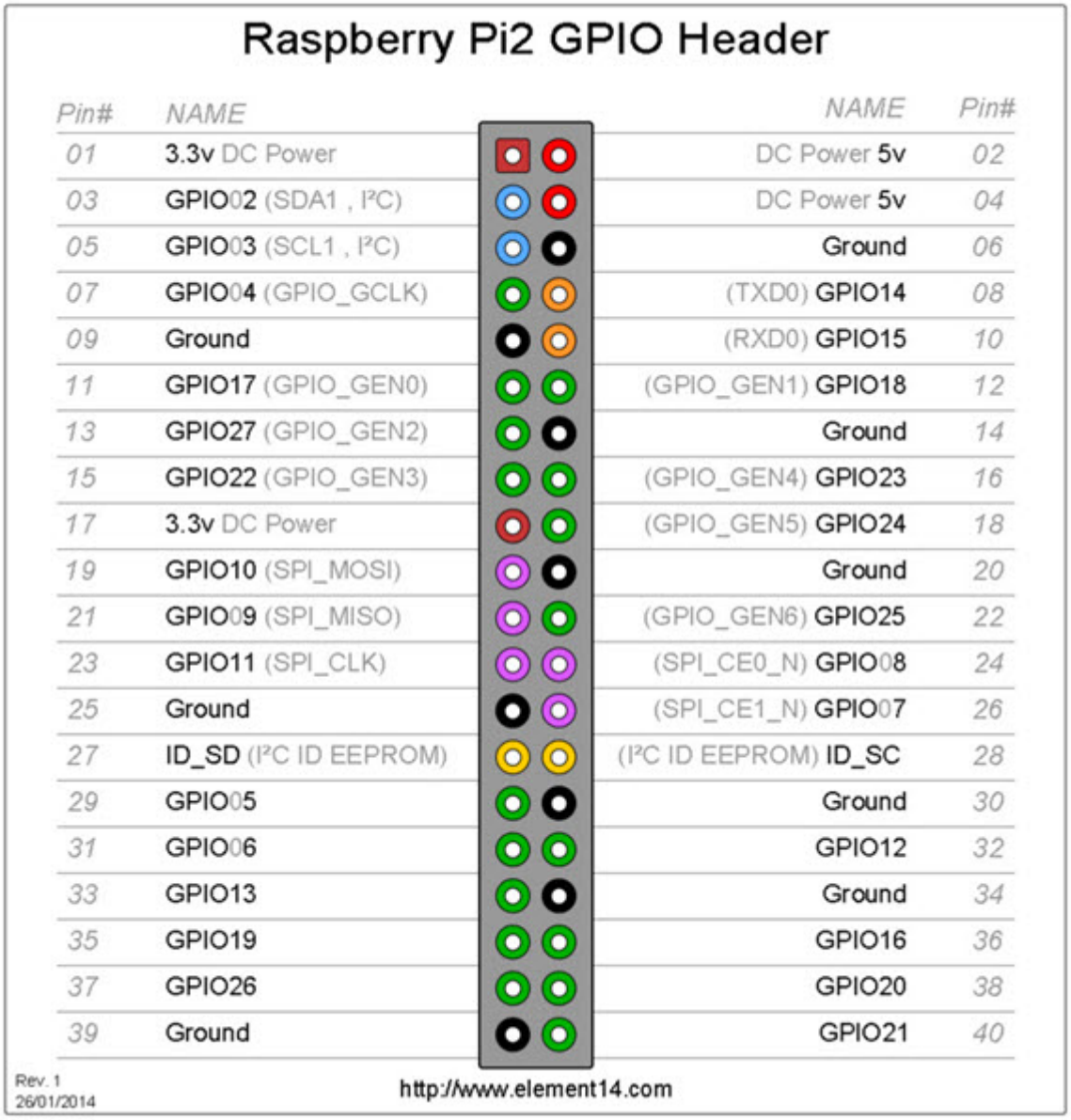
Öncelikle HackRF One cihazına o kadar para verdiğim için işleri ne kadar kolaylaştırabileceğini tecrübe etmek istedim. Bunun için daha önceden RF araştırmalarında kullanmak için satın aldığım RF prizleri üzerinde bir çalışma gerçekleştirdim. RF prizlerin kumandasını Hack RF One aygıtının antenine tutup, kumanda üzerinde yer alan ve prize elektrik akımı vermek için kullanılan butona (ON) basılı tutmaya başladıktan sonra aşağıdaki komut ile HackRF One'ın gönderilen sinyalleri aşağıdaki videoda yer aldığı üzere kolaylıkla kayıt altına aldım.

```
hackrf_transfer -r Funk-433Mhz-8M-8bit.bin -f 433000000 -s 8000000 -l 40
```

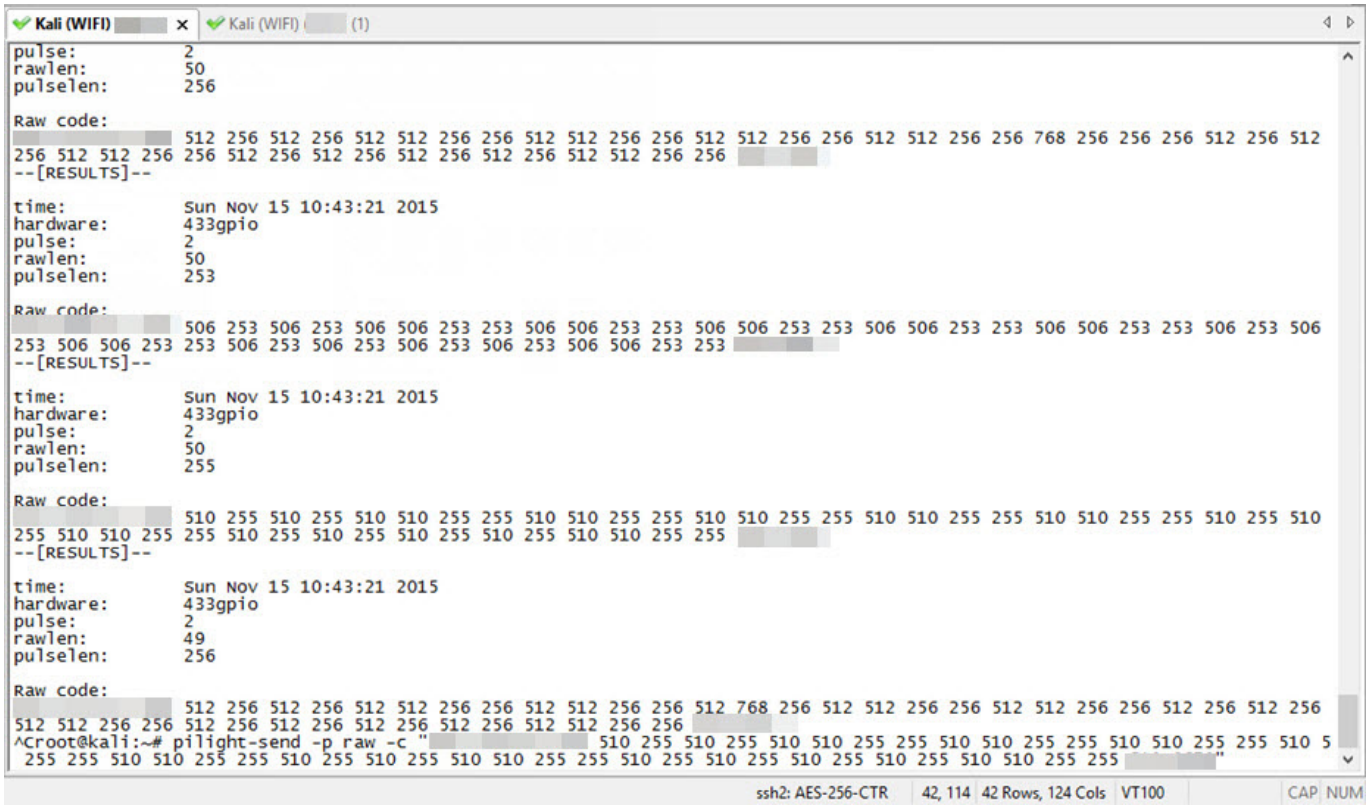
Sinyalleri 30 saniye kadar kayıt ettikten sonra aşağıdaki komutu çalıştırarak, HackRF One aygıtının kayıt ettiği sinyalleri RF prize göndermesini sağladım. Kısa bir süre sonra RF prize bağlı lambanın yandığını ve sinyalin HackRF One ile çok kolay bir şekilde tekrarlanabildiğini (REPLAY) tecrübe ettim.

```
hackrf_transfer -t Funk-433Mhz-8M-8bit.bin -f 433000000 -s 8000000 -x 47
```

HackRF One yerine Raspberry Pi ile ilerlemek isteyenler ise 3$'a satın alacakları RF alıcı ve vericiyi Raspberry Pi'nin GPIO pinlerine bağladıktan sonra pilight adındaki ve akıllı cihazları Raspberry Pi üzerinden yönetmek için geliştirilmiş olan bu araçtan faydalanabilirler.



Raspberry Pi ile ilerlemek için ilk olarak pilight-debug komutu ile RF sinyallerini dinlemeye başlayan pilight aracı ile garaj kumandasının kapı açma butonuna basıldığında gönderdiği sinyali (RF kodunu) kayıt altına aldım. Ardından da pilight-send -p raw -c komutu ile tespit ettiğim RF kodunu kapıya göndererek aşağıda yer alan videoda görüleceği üzere kapıyı başarıyla açabildim :)



pilight aracı ile aynı sistemi ve benzer kod dizilimini kullanan garaj kapılarına deneme yanılma (brute-force) saldırısı yapmak pratikte ne kadar kolay sorusuna yanıt bulmak için ise öncelikle RF kodunu 1, 0 ve O şeklinde grupladım. (Gruplama ile ilgili örnekler ve detaylı bilgi için pilight'ın wiki sayfasından faydalanabilirsiniz.)

(Sansürlenmiştir) O

510 255 510 255 1
510 510 255 255 0
510 510 255 255 0
510 510 255 255 0
510 510 255 255 0
510 510 255 255 0
510 255 510 255 1
510 510 255 255 0
510 255 510 255 1

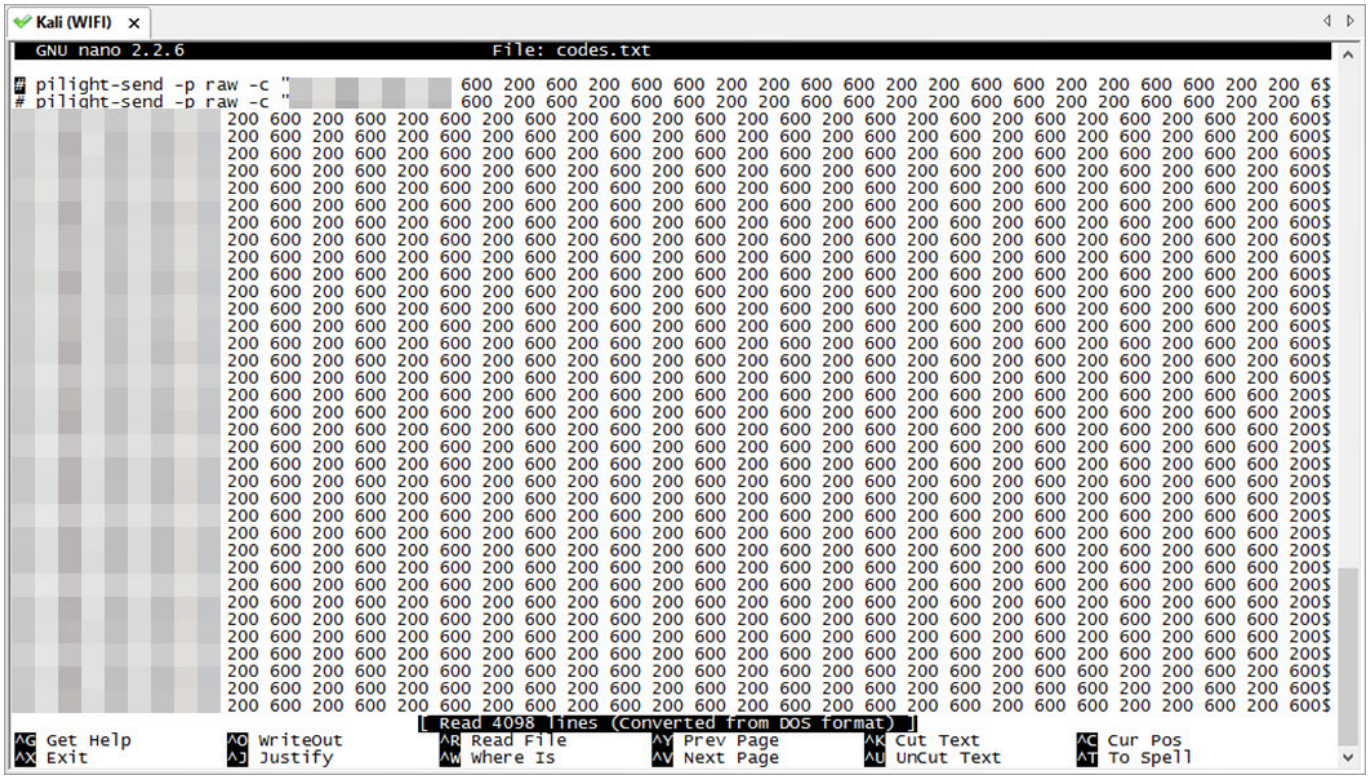
510 255 510 255 1

510 510 255 255 0

(Sansürlenmiştir) altbaşlık (footer)

Kumandanın 12 bit uzunluğunda bir sinyal gönderdiğini bildiğim için 1 olan değerlerin 0, 0 olan değerlerin 1 olacağını ve ilk bit olan O'nun da bir farklı değere sahip olabileceğini (kısaca yüksek ise düşük, düşük ise yüksek işaret gibi) göz önünde bulundurarak, bu garaj kapısının kapıyı açmak için 2 üzeri 12 yani 4096 farklı RF kodundan birini kabul edeceğini hesaplamam pek zor olmadı.

Python ile daha önceden hazırlamış olduğum 4096 tane RF kodunu, pilight aracı ile garaj kapısına gönderen Garage Door Bruteforcer isimli bir araç hazırladım. 3 dakika sonunda bu aracın, garaj kapısına 500 tane RF kodu gönderebildiğini gördüm. (Basit bir hesaplama ile bu aracın, garaj kapısını açacak kodu ~30 dakikada üretebileceğini söyleyebiliriz. OpenSesame gibi bir cihaz ile ise bu süreyi saniyeler mertebesine indirmek de mümkündür.)



Bu tür saldırılara baktığımızda, deneme yanılma saldırıları ve tekrarlama saldırılarının statik kod kullanan RF alıcılara karşı başarılı olduğun görüyoruz. Günümüzde üretilen modern araba kilit ve kumanda sistemlerine, alarm sistemlerine, garaj kapı sistemlerine baktığımızda ise çoğunun güvenli

olarak kabul ettiğimiz değişken (rolling) kod kullandığını görebiliriz. Sonuç olarak bu tür saldırılara karşı değişken kod kullanan sistemleri kullanmak doğru bir tercih olacaktır.

Bu yazının RF dünyasına adım atmak isteyen güvenlik uzmanları ve güvenlik araştırmacıları için faydalı olacağını ümit ederek, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.