Vulnerabilidades usando SDR

SDR = Software Defined Radio

Carlos Ledesma Peña

Trabajo de Fin de Grado, E.T.S. de Ingeniería Informática

Índice

¿Por qué es importante la seguridad informática?

La mayoría de los sistemas informáticos en producción no se encuentran aislados, sino que automatizan la gestión de la información en otros sistemas, información sensible...

- **Correos electrónicos:** ¿Y si terceros pudiesen leer nuestra correspondencia electrónica? (confidencialidad).
- **Transferencias bancarias:** ¿Y si se pudiese cambiar el destinatario de una transferencia bancaria? (integridad).
- **Gestión de intervenciones de ambulancias:** ¿No morirían personas si las ambulancias llegan tarde por estar el sistema caído? (disponibilidad).

La preocupación por la radiocomunicación

¿Debe preocuparnos la seguridad de los sistemas que usan radiocomunicación?

Características de un ataque

Un ataque puede ser llevado a distancia y anonimamente (y a más distancia de lo normal para ese sistema).

John Hering con su rifle BlueSniper, con el que es posible interactuar con dispositivos Bluetooth a más de kilómetro y medio de distancia.

Uso y posible abuso

El número de dispositivos que usan radiocomunicación aumenta con el tiempo:

- Un router *Wi-Fi*, unos auriculares *Bluetooth*, un pasaporte con *RFID*, un teléfono móvil, otros dispositivos usando protocolos propietarios...

Las herramientas de ataque cada vez son más baratas y más fáciles de usar:

- Dispositivos usando tecnología SDR por apenas 20 dólares, y software gratuito y relativamente simple con interfaz gráfica.

Índice

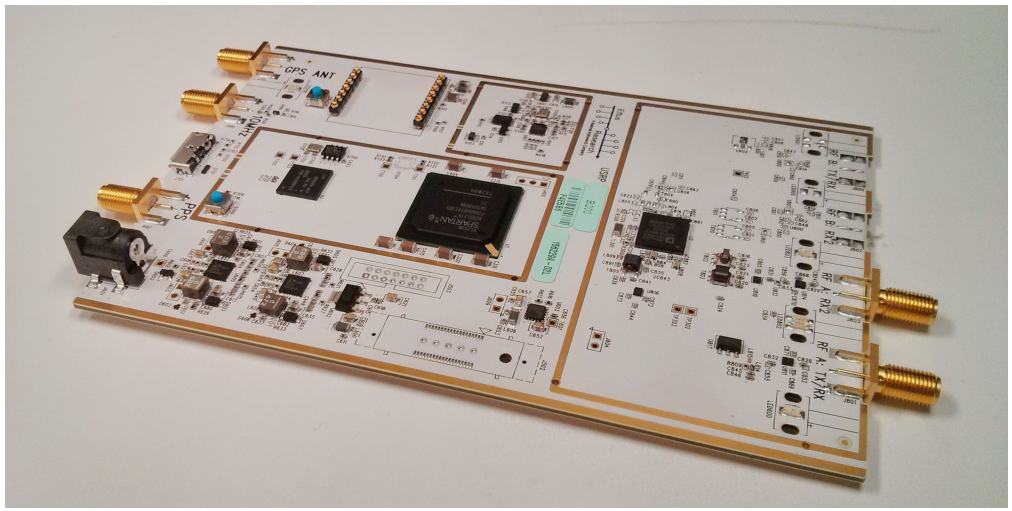
Vulnerabilidad, radio y sofware defined radio

Antes de empezar, es conveniente dar algunas definiciones:

- **Vulnerabilidad:** Error de diseño o implementación en un sistema que puede ser aprovechado para comprometer la confidencialidad, integridad o disponibilidad de éste.
- **Radio:** Tecnología que transmite o recibe sin cables radiación electromagnética para transferir información. También se llama así al sistema o dispositivo incorporando esta tecnología.
- **Software defined radio:** Radio en la cual algunas o todas las funciones de las capas físicas están implementadas en software.

En la práctica

La mayoría de los dispositivos SDR de consumo que se utilizan junto con un ordenador personal, básicamente sintonizan a una frecuencia y capturan una banda determinada, digitalizándola y enviándola al PC, donde se hará el resto de operaciones (separación en canales, demodulación, decodificación, división en tramas...).



Comienzos

- **Década de los 70:** Interés por parte del sector de defensa en un sistema de radio flexible.
- **1984:** Prototipo primitivo de SDR, únicamente recepción.
- **1991:** Comienzo del programa *SPEAKeasy*, que buscaba crear un dispositivo único que fuese compatible con varios dispositivos existentes.
- **1998:** Primera versión de *SignalMaster*, una de las primeras plataformas de desarrollo SDR.
- **2001:** Creación de *GNU Radio*, el entorno de desarrollo open source más importante.
- **2006:** Salida al mercado de *Small Form Factor*, la primera plataforma de desarrollo SDR completa y autónoma.

Índice

Comienzos

- **Década de los 70:** Interés por parte del sector de defensa en un sistema de radio flexible.
- **1984:** Prototipo primitivo de SDR, únicamente recepción.
- **1991:** Comienzo del programa *SPEAKeasy*, que buscaba crear un dispositivo único que fuese compatible con varios dispositivos existentes.
- **1998:** Primera versión de *SignalMaster*, una de las primeras plataformas de desarrollo SDR.
- **2001:** Creación de *GNU Radio*, el kit de desarrollo open source más importante.
- **2006:** Salida al mercado de *Small Form Factor*, la primera plataforma de desarrollo SDR completa y autónoma.

Índice

Seguridad

- **2005:** Versión mejorada de *BlueSniper*.
- **2007:** Ataque sobre teclados inalámbricos.
- Ataque sobre el pasaporte europeo.
- **2008:** Michael Ossmann repasa en Black Hat sobre el estado de la seguridad de las radiocomunicaciones, y advierte que SDR accesible es peligroso.
- Ataque sobre el sistema de tarjetas del metro de Boston y de pago remoto en peajes.
- **2009:** Ataque práctico sobre *GSM*.
- **2010:** Lectura de *RFID* a larga distancia.
- **2011:** Ataque sobre *GRPS/EDGE* y *UMTS/HSPA*.

Índice

Estado actual

- En 2010, Eric Fry se da cuenta de algo extraño al realizar ingeniería inversa a un *driver* de un dispositivo *USB* para recepción *FM* y *DAB+*. Lo que viaja del dispositivo al PC no es audio, sino muestras de la señal en una etapa intermedia entre la señal de radiofrecuencia y el audio.
- En 2012 nace el proyecto *rtl-sdr*, que proporciona una interfaz para usar estos dispositivos como SDR's (sólo recepción, pero muy asequibles).
- Interés en integrar SDR en la comunidad de pentesting, con nuevas herramientas que permiten inyectar paquetes de diversos protocolos al vuelo.

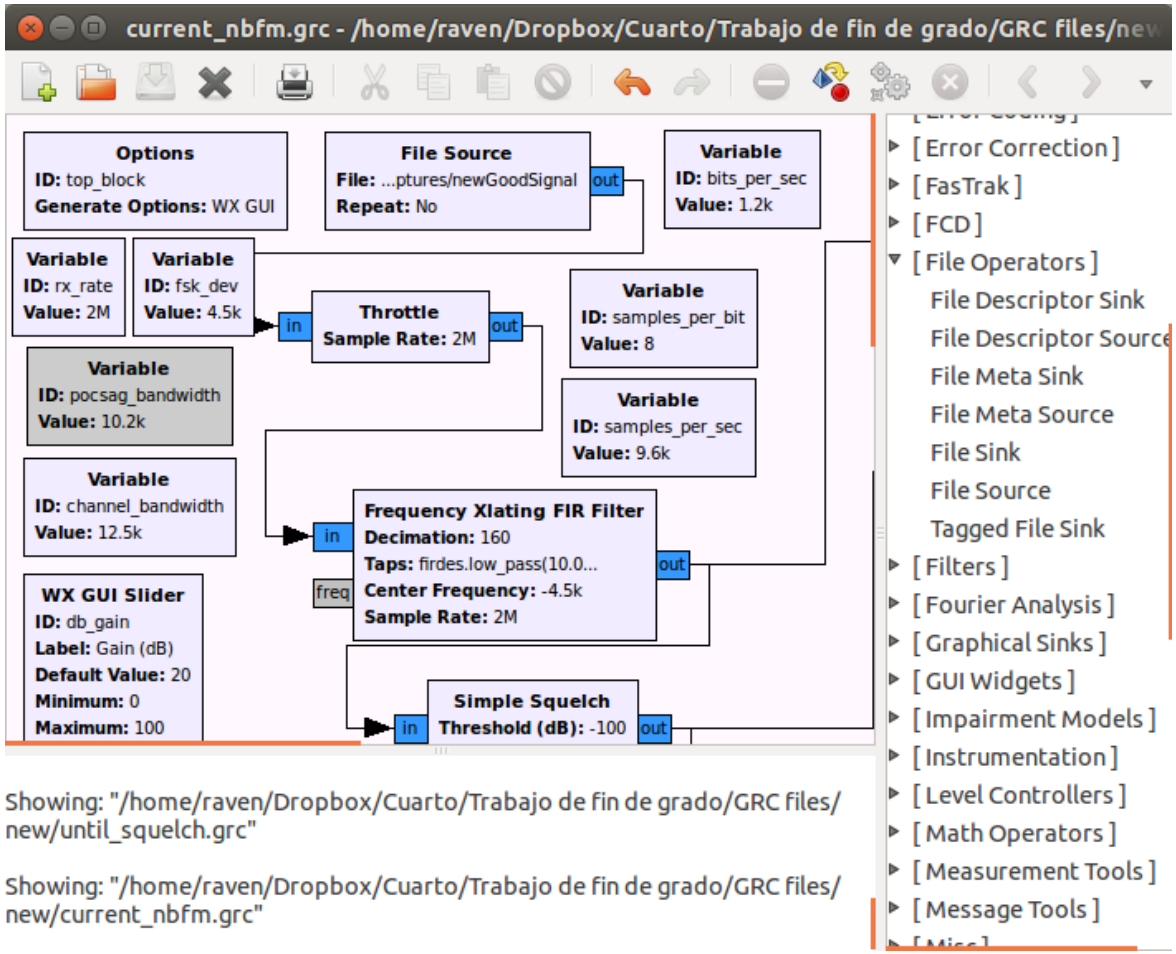
Índice

¿Qué es GNU Radio?

GNU Radio es un entorno de desarrollo *open source* multiplataforma de procesamiento de señales en general, si bien está especializado en SDR, pero no limitado a ello.

- Ofrece una interfaz gráfica, *GRC*, además de las interfaces para *Python* y *C++*. La de *Python* es una envoltura de la de *C++*, y la gráfica una envoltura de la de *Python*.
- La interfaz gráfica sirve para crear diagramas de flujo, con conexiones entre bloques que representan funciones de procesamiento de señales.
- Los bloques pueden ser de entrada o salida, para interactuar con el exterior (parte hardware de SDR, tarjeta de audio, disco duro...), o de entrada y salida, implementando funciones en sí.

GRC


current_nbfm.grc - /home/raven/Dropbox/Cuarto/Trabajo de fin de grado/GRC files/new
Options
ID: top_block
Generate Options: WX GUI
File Source
File: ...ptures/newGoodSignal
Repeat: No
out
Variable
ID: bits_per_sec
Value: 1.2k
Variable
ID: rx_rate
Value: 2M
Variable
ID: fsk_dev
Value: 4.5k
in
Throttle
Sample Rate: 2M
out
Variable
ID: samples_per_bit
Value: 8
Variable
ID: pocsag_bandwidth
Value: 10.2k
Variable
ID: samples_per_sec
Value: 9.6k
Variable
ID: channel_bandwidth
Value: 12.5k
in
Frequency Xlating FIR Filter
Decimation: 160
Taps: firdes.low_pass(10.0...
Center Frequency: -4.5k
Sample Rate: 2M
out
freq
WX GUI Slider
ID: db_gain
Label: Gain (dB)
Default Value: 20
Minimum: 0
Maximum: 100
Simple Squelch
Threshold (dB): -100
in
out
[Error Correction]
[FasTrak]
[FCD]
[File Operators]
File Descriptor Sink
File Descriptor Source
File Meta Sink
File Meta Source
File Sink
File Source
Tagged File Sink
[Filters]
[Fourier Analysis]
[Graphical Sinks]
[GUI Widgets]
[Impairment Models]
[Instrumentation]
[Level Controllers]
[Math Operators]
[Measurement Tools]
[Message Tools]
Showing: "/home/raven/Dropbox/Cuarto/Trabajo de fin de grado/GRC files/new/until_squelch.grc"
Showing: "/home/raven/Dropbox/Cuarto/Trabajo de fin de grado/GRC files/new/current_nbfm.grc"

Índice

¿Qué es un pager POCSAG?

Al ataque

- Tras escanear en el rango de frecuencias que menciona el *pager* en su parte de atrás, y los avisos que alcanzo a capturar se emiten en la misma frecuencia.
- Construyo el diagrama de flujo (no sin mucho esfuerzo) para decodificar con arreglo al estándar *POCSAG* y efectivamente, se ajusta al estándar. Cada disposivo tiene un ID, y suena cuando se emite el suyo.
- Modifico el diagrama de flujo y creo un bloque personalizado para *GRC* para imprimir en consola los ID's según se capturan los avisos.

Dificultades encontradas

- Dominio completamente nuevo para mí, y falta de base sólida a la hora de resolver los problemas (días de diagnóstico por problema).
- *GRC* no está hecho para aprender a base de prueba y error desde el principio, no es fácil saber qué está fallando ni por qué (curva de aprendizaje elevada).
- Limitaciones del hardware, mi portátil usa *USB 2.0*, lo que limita el ancho de banda capturable de una vez, además de no tener potencia de procesamiento suficiente y descartar muestras si se usaban varias operaciones simultáneamente.

Índice

Conclusiones

- Desde el punto de vista económico y humano, es necesario invertir en la seguridad de los sistemas informáticos. No sólo se protege de las malas intenciones, sino de las buenas intenciones equivocadas.
- La "seguridad" por oscuridad no es seguridad, si un sistema necesita que su forma de funcionar no sea pública para ser seguro, no es seguro igualmente. *Sólo la clave debe ser desconocida para el resto*.
- No se le ha prestado suficiente atención a la seguridad de las radiocomunicaciones en el pasado, y ahora se dispone de herramientas basadas en SDR que facilitan aprovecharse de sistemas vulnerables. Hay que prestarle atención desde ya.

Índice

Utilidades

- Aprender conocimientos básicos de radio (inquietud personal).
- Incorporar una nueva herramienta de trabajo (es posible que se incorpore en labores de pentesting).
- Servir de guía de inicio rápido a SDR a los investigadores del departamento.
- Obtener el título de Graduado en Ingeniería Informática.

¡Gracias por vuestra atención!