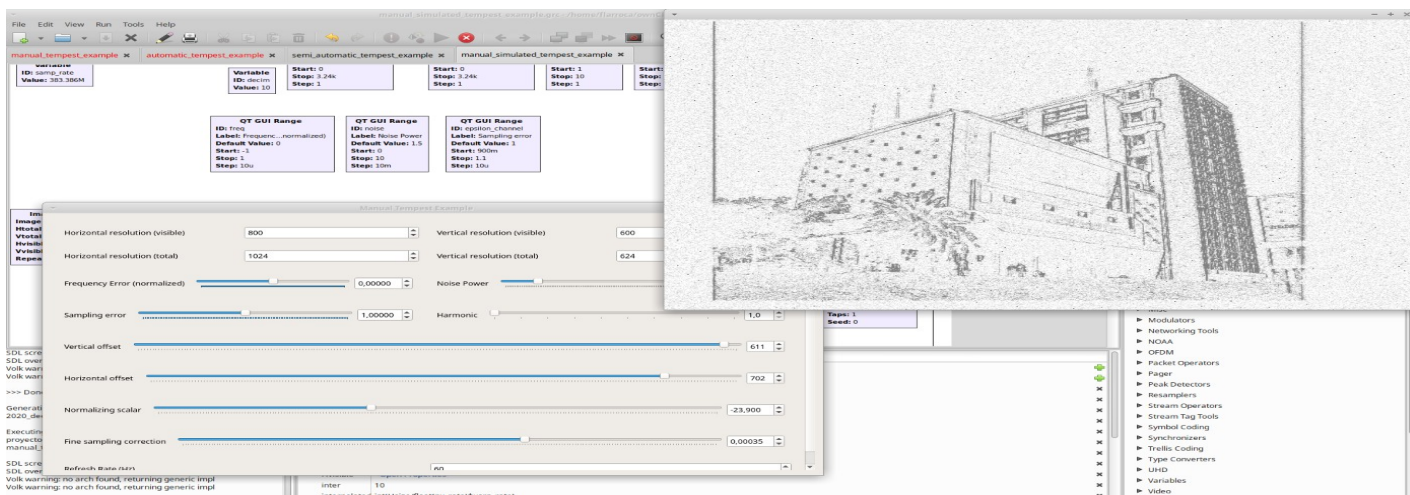


Facultad de Ingeniería. Instituto de Ingeniería Eléctrica.

Análisis de Redes, Tráfico y Estadísticas de Servicios

Proyecto: Espionaje por Emisiones Electromagnéticas



En 2020 desarrollamos gr-tempest, una re-implementación de TempestSDR para GNU Radio. El código está disponible en <https://github.com/git-artes/gr-tempest>.

Ejemplo de su uso en el siguiente video:

<https://www.youtube.com/watch?v=oTCu8HTaN3Y&t=14s>

Nuestro primer paso en el área de TEMPEST fue el trabajo de tesis de Maestría en Ingeniería Eléctrica desarrollado por Pablo Menoni bajo la dirección de Federico “Larroca” La Rocca. Defendida en 2018.

Resumen

En este trabajo se profundiza en el estado del arte y se muestran algunos aspectos de las vulnerabilidades que ocurren a partir de emanaciones de ondas electromagnéticas, a las cuales están sujetos la gran mayoría (sino todos) de los modernos sistemas de información.

A partir de la detección y procesamiento de esas emanaciones, se dejan en evidencia las debilidades desde el punto de vista de seguridad y privacidad que estas acarrearán. Estos aspectos se pueden

vulnerar en un gran número de sistemas de información, por individuos con conocimientos acerca de teoría electromagnética, de los adquiridos en cursos de grado universitario, y un manejo de software a nivel programador, junto con el empleo de herramientas de hardware de bajo costo como SDR.

El trabajo se aborda tomando como punto de partida el espionaje de emanaciones provenientes de la interfaz VGA, en particular del desarrollo hecho por Martin Marinov de la Universidad de Cambridge, Reino Unido, para luego extenderlo a las emanaciones de la interfaz HDMI.

Documentos, repositorio y demostraciones

- [gr-tempest 2.0: Mejoras a la Implementación de Tempest en GNU Radio](#). Pablo Bertrand, Felipe Carrau y Victoria Severi, Noviembre 2021. Tesis de grado.
- [Espionaje por Emisiones Electromagnéticas](#). Pablo Menoni, Diciembre 2018. Tesis de maestría.
- [gr-tempest](#). Re-implementación en GNU Radio de TempestSDR.
- [Repositorio tesis](#). Contiene los scripts usados durante la maestría de Pablo Menoni, su descripción, y otros archivos de interés.
- [Video demostrativo](#).

Grabaciones

Registro de señales de radiofrecuencia emanadas por la interfaz de video.

Las grabaciones fueron realizadas con GNU Companion 3.7.10.1 tomando como fuente un SDR USRP B200 de Ettus, y pueden ser descargadas en los siguientes links:

- [grabacion1.dat](#) Antena Ikusi modelo Flash HD NANO, distancia antena-interfaz 2m.
- [grabacion2.dat](#) Antena LP09650 de Ettus, distancia antena-interfaz 0,8m.
- [grabacion3.dat](#), Antena Ikusi modelo Flash HD NANO, distancia antena-interfaz 3m.
- [grabacion4.dat](#). Una grabacion excelente.

Características comunes a todas las grabaciones

- Resolución de la pantalla espiada: 1024×768 @60Hz.
- Frecuencia de muestreo en el SDR: 30MHz.
- Interfaz espiada: VGA, Monitor AOC de 19"

Más y mejores grabaciones. Son todas a un monitor BenQ de 22" a una resolución de 1024×768, pero a distintas tasas de muestreo. El nombre del archivo es auto-informante:

- [grabacion_splitter_40M_1344_806_px_freq_64995840.dat.bz2](#)
- [grabacion_splitter_50M_1344_806_px_freq_64995840.dat.bz2](#)
- [grabacion_splitter_40M_1344_806_px_freq_64995840_video.dat.bz2](#)

Ponemos a disposición además una grabación de la interfaz HDMI:

- [grabacion_HDMI.dat](#), Antena Ikusi modelo Flash HD NANO, distancia antena-interfaz 0.5m

Características adicionales

- Resolución de la pantalla espiada: 1024×768 @70Hz.
- Frecuencia de muestreo en el SDR: 40MHz.
- TV Samsung LN26C450, interfaz HDMI3

Fuente: <https://iie.fing.edu.uy/investigacion/grupos/artes/es/inicio/>