



Documento matriz para Organización Coordinadora Local

1. ¿FADe II. De qué se trata el proyecto?
2. ¿Cómo son los sensores de FADe II?
3. ¿Cómo se opera un sensor FADe II?
4. ¿Cómo solucionar algunos problemas comunes al operar el sensor FADe II?
5. ¿Por cuánto tiempo se hará el monitoreo?
6. ¿Quiénes son los involucrados en el proyecto FADe I y II?
7. ¿Cuáles son las consideraciones de riesgo generales por tener estos sensores?
 - a. Sobre el comportamiento de los sensores
 - b. Sobre la información contenida en los teléfonos celulares que componen el sensor
 - c. Sobre la transmisión de datos
 - d. Sobre algunas medidas tomadas para incrementar la seguridad
 - e. Recomendaciones en caso de una potencial revisión
 - f. Recomendaciones en caso de una potencial incautación

1. ¿De qué se trata el proyecto FADe II?

El proyecto busca aplicar la metodología propuesta en el proyecto Crocodile Hunter desarrollada por la Electronic Frontier Foundation para detectar equipamiento usado en escenarios de vigilancia telefónica, específicamente en redes 4G/LTE. Para llevar a cabo esta detección se necesitan usar ciertos dispositivos o sensores.

Sus objetivos principales son:

1. Colaborar con el equipo detrás de la metodología propuesta por Crocodile Hunter, detectando el uso de IMSI-Catchers en 2 ciudades de América Latina.
 - 1.1. Para aplicar, documentar y probar variaciones metodológicas utilizando herramientas técnicas.
 - 1.2. Compartir los resultados con organizaciones locales de libertad de expresión y / o medios de comunicación independientes en contextos represivos, violentos y bajo vigilancia.

2. ¿Qué es el proyecto Crocodile Hunter?

Esta metodología busca detectar el uso de dispositivos de vigilancia de comunicaciones celulares o IMSI-Catchers en un área determinada, los cuales se hacen pasar por antenas reales de operadoras móviles para interceptar las comunicaciones de un grupo arbitrario de usuarios. El software de Crocodile Hunter busca realizar esta detección con un alto grado de confiabilidad y sin dejar rastros en la red móvil al no interactuar con ninguna antena celular. En este momento la metodología requiere la configuración de un sensor. Más información del proyecto se encuentra en <https://github.com/EFForg/crocodilehunter>

6. ¿Cómo son los sensores de FADe II?

Están compuestos por:

1. Radio de alta frecuencia.
2. Batería o power bank.
3. Dispositivo GPS
4. Un par de antenas de alto alcance.
5. Raspberry Pi4.
6. Cable USB-A ó USB-C



Figura. 1 Sensor tipo FADe II

Estos sensores pueden ser operados de dos formas:

- **Ubicación fija**, recopilando todos los datos posibles en un período de tiempo prolongado. Ej. sensor dispuesto en un cajón, armario, guantera de auto, etc.
- **Ubicación móvil**, recopilando datos en tiempo real en diferentes localizaciones. Ej. El sensor está dispuesto en un vehículo, motocicleta, etc.

4. ¿Por cuánto tiempo se hará el monitoreo?

El alcance del proyecto propone hacer el monitoreo hasta el último día del mes de noviembre de 2020. Al final de dicho monitoreo, cada equipo deberá ser devuelto a la OCL (organización coordinadora local) correspondiente, y estos a su vez al equipo coordinador del proyecto.

7. ¿Cómo se opera un sensor FADe II?

1. Se debe cargar la batería o power bank (se recomienda cargar cada 12 hrs). Es dispositivo debe estar conectado de la siguiente manera:
 - a. Conectar las antenas de alto alcance al radio de alta frecuencia.
 - b. Con el cable USB a USB-C, conectar la batería o power bank a un puerto USB-C del case de la Raspberry Pi4.
 - c. Conectar el dispositivo GPS a un puerto USB del case de la Raspberry Pi4.
 - d. Conectar el radio a un puerto USB del case de la Raspberry Pi4.
2. Al conectar las piezas antes descritas, el radio deberá encender una luz de color verde (esto puede demorar varios segundos).

3. Una vez encendida la luz, el sensor está funcionando.

Nota. Lo anterior descrito aplica para la el armado del sensor la primera vez que se vaya a encender. Posteriormente, conectar y desconectar la batería o power bank será suficiente para encender o apagar el sensor.

8. ¿Cómo solucionar algunos problemas comunes al operar el sensor FADe II?

a. El sensor dejó de recopilar información:

1. Puede pasar que la carga en el power bank esté agotada.

b. El cable se desconectó:

1. Se deberá poder conectar de nuevo sin problemas.

c. El software no está cargando datos

1. Esto puede deberse a fallas con la cobertura de la unidad GPS, como regla general con este tipo de dispositivos, deben tener un indicador LED parpadeando, si está fijo, quiere decir que no está recibiendo señal GPS de forma adecuada, se puede trasladar a un lugar con mejor vista de cielo abierto, dependiendo de las condiciones geográficas, incluso tenerlo detrás de un vidrio puede afectar la calidad de la recepción.
2. Es posible que el sensor no tenga acceso a internet, se sugiere revisar el cable ethernet o las redes wifi que debe acceder el dispositivo.

9. ¿Por cuánto tiempo se hará el monitoreo?

El alcance del proyecto propone hacer el monitoreo hasta el último día del mes de noviembre de 2020. Al final de dicho monitoreo, cada equipo deberá ser devuelto a la OCL (organización coordinadora local) correspondiente, y estos a su vez al equipo coordinador del proyecto.

10. ¿Quiénes son los involucrados en el proyecto FADe I y II?

1. **Seaglass (EEUU)**. Creadores de la metodología e infraestructura para la recolección de datos. Equipo de investigadores de seguridad de la Universidad de Washington para medir el uso de IMSI-catcher en una ciudad.
2. **Crocodile Hunter. (EEUU)**. Creadores de la metodología e infraestructura para la recolección de datos. Equipo de investigadores de seguridad de EFF (Electronic Frontier Foundation) para medir el uso de IMSI-catcher en una ciudad.
3. **South Lighthouse (Chile)**. Organización coordinadora a cargo de la planificación, monitoreo y control, consultoría y capacitación relacionado con el desarrollo del proyecto en la región.

11. ¿Cuáles son las consideraciones de riesgo generales por tener estos sensores?

a. Sobre el comportamiento de los sensores

El comportamiento de los sensores emula la presencia de un teléfono celular convencional, por lo que no emite ningún tipo de señal sospechosa, y no puede ser categorizado como un equipo hostil o riesgoso. La diferencia entre este sensor y un teléfono convencional radica en que el sensor está diseñado para guardar y procesar la información bruta de conexión con las torres celulares.

Para los casos en donde el sensor esté ubicado en un lugar fijo con conexión Wifi o movilizándose en la calle, y pueda gozar de conexión Wifi de forma ocasional programada (por ejemplo en las noches o en otros momentos agendados) se puede prescindir de una línea telefónica para el sensor, haciéndolo aún más difícil de rastrear ya que ningún equipo estará afiliado a la red celular en el momento en que el sensor captura información.

b. Sobre la información contenida en los teléfonos celulares que componen el sensor

En el caso del teléfono android, este solo recopilará datos crudos de las antenas celulares cercanas transmitiendo información sin hacer ningún análisis local para determinar el uso de tecnologías de vigilancia, por lo que al analizar el contenido de los archivos en el teléfono no se puede determinar con qué finalidad están estos datos ahí, o incluso qué representa esta información. En el caso de los teléfonos convencionales, no se almacena ningún tipo de información diferente a la que tendría si estuviera nuevo de fábrica.

c. Sobre la transmisión de datos

La conexión hecha entre los teléfonos androids y el servidor de la Universidad de Washington se realiza de forma cifrada. Esta conexión no es ofuscada o desviada mediante proxy/VPN/Tor por lo que cualquiera que monitoree la conexión puede determinar que el teléfono o la red wifi usada está enviando datos al servidor correspondiente. Con esta consideración a nivel de diseño, el servidor usado no es utilizado para otro tipo de aplicaciones para evitar su vinculación con otros proyectos e iniciativas. Este servidor no es conocido en la actualidad por desarrollar este o cualquier otro proyecto. Finalmente, el flujo de información es compatible con el uso de alguna herramienta de ofuscación y/o cifrado de tráfico que se pueda instalar en el teléfono y encender al momento de hacer la transmisión de datos.

d. Sobre algunas medidas tomadas para incrementar la seguridad

- Los datos compilados serán publicados posterior a la recopilación de los mismos para permitir mover los sensores y anonimizar los datos obtenidos.
- Los datos publicados no tendrán información de ubicación exacta para no comprometer la ubicación de los mismos y que pueda ser vinculada a casas, oficinas u otros lugares de interés en donde estuvieran los sensores.

- La información de las organizaciones y personas participantes será publicada sólo si estos así lo desean, de otro modo serán tratados como aliados anónimos.

e. Recomendaciones en caso de una potencial revisión

- Para evitar compromisos particulares se recomienda tener el sensor en un lugar poco visible, ya que siempre que se puedan recibir señales GPS el sensor funcionará sin problemas aunque esté dentro de un bolso, asiento, maletero de vehículo, etc.
- En caso de una revisión se puede informar a quién la esté realizando, que este sensor es usado en una investigación académica sobre la calidad de la señal celular en la ciudad.
- Si el contexto es de muy alto riesgo se recomienda seguir las recomendaciones en caso de una potencial incautación descritas a continuación.

f. Recomendaciones en caso de una potencial incautación

- **En general:** En el caso de un riesgo bajo de potencial incautación recomendamos sólo desconectar los cables y apagar el sensor. En caso de riesgo medio recomendamos además extraer la tarjeta MicroSD del sensor, y en un riesgo alto recomendamos además eliminar la información disponible en la tarjeta o destruirla. En caso de riesgo crítico, se pudiera desechar el sensor completamente. Cada Organización Coordinadora Local podrá establecer con los operadores de sensores cuando el riesgo de incautación es bajo, medio, alto o crítico.

Un proyecto de,



Para más información, por favor visite <https://fadeproject.org/>

AA/octubre-2020