Documento matriz para

Organización Coordinadora Local OCL

1. ¿De qué se trata el proyecto?
2. ¿Qué es la metodología SEAGLASS?
3. ¿Cómo son los sensores de FADe?
4. ¿Por cuánto tiempo se llevará a cabo la recolección de datos?
5. ¿Cuáles son las consideraciones de riesgo generales por tener estos sensores?
    a. Sobre el comportamiento de los sensores
    b. 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 FADe project ?

El proyecto busca aplicar la metodología SEAGLASS desarrollada por la Universidad de Washington para detectar equipamiento usado en escenarios de vigilancia telefónica. Para llevar a cabo esta detección se necesitan usar ciertos dispositivos o sensores.

Los objetivos principales son:

1. Colaborar con el equipo detrás de la metodología propuesta por SEAGLASS, detectando el uso de IMSI-Catchers en 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 la metodología SEAGLASS?

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. La metodología SEAGLASS 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 implementación de un sensor y el uso de una aplicación Android. Más información del proyecto se encuentra en https://seaglass.cs.washington.edu/

3. ¿Cómo son los sensores de FADe?

Están compuestos por dos (2) teléfonos celulares conectados por un cable. Más en detalle, un teléfono inteligente Android con una aplicación particular y un teléfono convencional usado como antena.

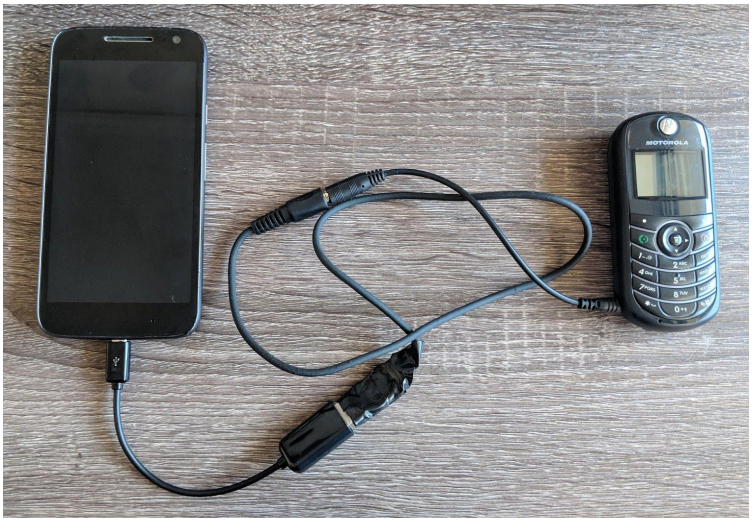

Figura. 1 Sensor tipo

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 dispuesto en un vehículo, motocicleta, etc.

4. ¿Por cuánto tiempo se llevará a cabo la recolección de datos?

El alcance del proyecto propone recolectar datos por un plazo de entre 60 a 90 días seguidos. Al final de este proceso de monitoreo, cada dispositivo o sensor debe devolverse a la OCL (organización coordinadora local) correspondiente, y esta a su vez al equipo coordinador regional del proyecto.

5. ¿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 tuviera 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

- Cada teléfono estará vinculado a una cuenta Google para manejar las actualizaciones de la app SEAGLASS. Cada una de estas cuentas Google será diferente y no vinculadas entre sí con otros teléfonos, ni con números de recuperación de personas dentro del país.
- 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 estuvieron 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 estos dos teléfonos son usados 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

- **Para el teléfono convencional:** en el momento en que se le desconecta el cable y se presiona el botón de encendido alrededor de 4 segundos, el teléfono se apaga y puede encender con su sistema operativo de fábrica, sin dejar rastros de cualquier actividad de monitoreo.

- **Para el teléfono inteligente:** dado que es un teléfono android con una app particular no habrá ningún indicador de compromiso en este dispositivo además de la aplicación como tal, la cual puede ser analizada para saber qué comportamiento tiene. En caso de tener tiempo en el contexto que corresponda se podrá desinstalar la aplicación y en ese momento se eliminarían los datos recopilados y es mucho más difícil detectar el tipo de actividad para la que estaba siendo

utilizada. Sin embargo, un análisis forense especializado puede revelar la existencia de la aplicación en cuestión y la naturaleza de su funcionamiento, por lo que en un caso de extremo riesgo es una opción viable hacer un reinicio de fábrica al teléfono inteligente o incluso desecharlo, opción que en la medida de lo posible recomendamos evitar por la dificultad de reponer.

- **En general:** En el caso de un riesgo bajo de potencial incautación recomendamos sólo desconectar el cable de los teléfonos y apagar el convencional. En caso de riesgo medio recomendamos además desinstalar la app SEAGLASS, y en un riesgo alto recomendamos además hacer un reinicio a valores de fábrica del teléfono inteligente. En caso de riesgo crítico, se pudiera desechar el teléfono inteligente y el cable de conexión. 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,

South
LIGHTHOUSE

AA/mayo-2019