FADe

Matrix Document for

Local Coordinating Organizations LCO’s

1. What is the FADe project about?
2. What is the SEAGLASS methodology?
3. How do the sensors look like?
4. How long will the monitoring be done?
5. What are the risk considerations for having these sensors under use?
    a. About the behavior of the sensors.
    b. About the information contained in the cell phones that make up the sensor.
    c. About data transmission.
    d. About some measures taken to increase security.
    e. Recommendations in the event of a potential revision.
    f. Recommendations in the event of a potential seizure.

1. What is the FADe project about?

The project seeks to apply the SEAGLASS methodology developed by the University of Washington to detect equipment used in telephone surveillance scenarios. To carry out this detection, certain devices or sensors need to be used.

2. What is the SEAGLASS methodology?

This methodology looks forward to detect the use of cellular communication surveillance devices or IMSI-Catchers in a certain area, which are posing to be as real antennas of mobile operators to intercept the communications of an arbitrary group of users. The SEAGLASS methodology seeks to perform this detection with a high degree of reliability and without leaving traces on the mobile network by not interacting with any cellular antenna. At this time the methodology requires the implementation of a sensor and the use of an Android application. More information on the project can be found at https://seaglass.cs.washington.edu/

3. How do the sensors look like?

They are made up of two (2) cell phones connected by a cable. In more detail, an Android smartphone with a particular application and a conventional phone used as an antenna.

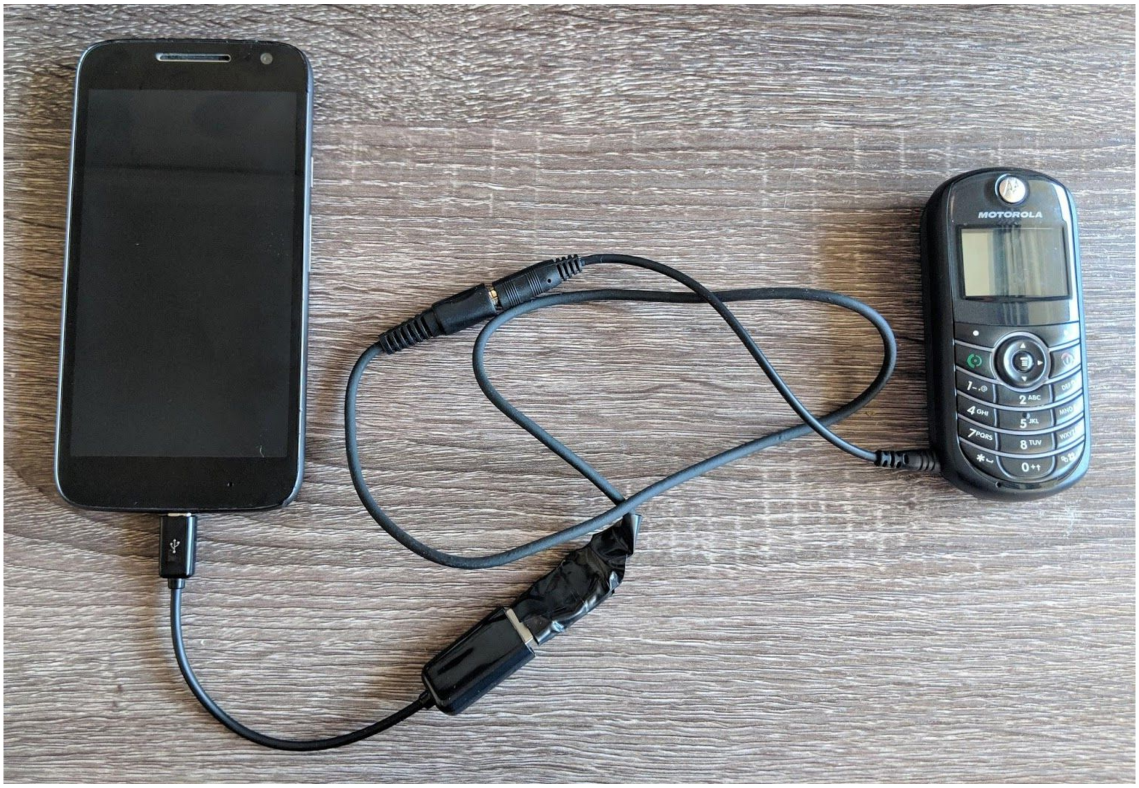

Figure. 1 Sensor type

These sensors can be operated in two different ways:

- **Fixed location.** They can even be located inside a drawer, closet, bookcase, etc.
- **Mobile location.** Arranged inside a backpack, trunk or glove compartment of a car, motorcycle, etc.

4. How long will the monitoring be done?

The scope of the project proposes to monitor for a term of 60 to 90 days in row. At the end of this monitoring process, each device or sensor should be returned to the corresponding LCO (local coordinating organization), and this one in turn to the project coordinating team.

5. What are the risk considerations for having these sensors under use?

a. About the behavior of the sensors.

The behavior of the sensors emulates the presence of a conventional cell phone, so it does not emit any kind of suspicious signal, and cannot be categorized as a hostile or a risky device. The difference between this sensor and a conventional telephone is that the sensor is designed to store and process the raw information of connection with the cell towers.

For cases where the sensor is located in a fixed location with Wifi connection or even moving it around the city, connected to Wifi on an occasionally scheduled basis (e.g. at night or at other scheduled times), it's possible to skip having a SIM card or mobile line for the sensor, making it even more difficult for the cell phone to be tracked since no equipment will be affiliated with the cellular network at the time the sensor captures information.

b. About the information contained in the cell phones that make up the sensor

In the case of the Android phone, it will only collect raw data from nearby cellular antennas, transmitting information without doing any local analysis to determine the use of surveillance technologies, therefore, when analyzing the content of the files on the phone, it cannot be determined for what purpose is this data there, or even what does this information represent? In the case of conventional telephones, no type of information is stored other than what you would have if it were new from the factory.

c. About data transmission.

The connection made between the android phones and the University of Washington server is made in encrypted form. This connection is not obfuscated or forwarded by proxy/VPN/ Tor, so anyone who monitors the connection can determine that the phone or the wifi network used is sending data to the corresponding server. With this design-level consideration, the server used is not used for other types of applications to avoid linking it with other projects and initiatives. This server is not currently known for developing this or any other project. Finally, the flow of information is compatible with the use of an obfuscation and/or traffic encryption tool that can be installed on the phone and switched on when data is transmitted.

d. About some measures taken to increase security.

- Each phone will be linked to a Google account to handle updates to the SEAGLASS app. Each of these Google accounts will be different and not linked to each other with other phones, nor to recovery numbers of people within the country.
- The compiled data will be published, after its collection to allow moving the sensors and anonymizing the data obtained.
- The published data will not have exact location information so as not to compromise their location and that can be linked to houses, offices or other places of interest where the sensors were.
- The information of the participating organizations and individuals will be published only if they so wish, otherwise they will be treated as anonymous allies.

e. Recommendations in the event of a potential revision.

- To avoid particular compromises, it is recommended to have the sensor in an inconspicuous place, since whenever GPS signals can be received, the sensor will work without problems even if it is inside a bag, under a seat, vehicle trunk, etc.
- In the event of a potential revision, it can be reported to who is conducting it, that these two phones are used in academic research on the quality of cellular signal in the city.
- If the context is very high risk, it is recommended to follow the recommendations in case of a potential seizure described below.

f. Recommendations in the event of a potential seizure.

- **For conventional (feature) phone:** the moment the cable is disconnected and the power button is pressed for about 4 seconds, the phone turns off and can be powered on by its factory operating system, leaving no trace of any monitoring activity.

- **For the smartphone:** since it is an android phone with a particular app, there will be no compromise indicator on this device in addition to the application as such, which can be analyzed to know its behavior. If you have time in the corresponding context, you can uninstall the application and at that moment the collected data would be deleted and it is much more difficult to detect the type of activity for which it was being used. However, a specialized forensic analysis can reveal the existence of the application in question and the nature of its operation, so in a case of extreme risk it is a viable option to do a factory reset or even discard the smartphone, an option that as far as possible we recommend avoiding due to the difficulty of replacing.

- **In general:** In the case of a low risk of potential seizure, we recommend only disconnecting the cable from the telephones and turning off the conventional one. In case of medium risk we also recommend uninstalling the SEAGLASS app, and in high risk we also recommend doing a reset to factory settings of the smartphone. In case of critical risk, the smartphone and the connecting cable could be thrown away. Each Local Coordinating Organization may establish with sensor operators when the risk of seizure is low, medium, high or critical.

South
LIGHTHOUSE

AA/may-2019