FADe

Matrix Document for Local Coordinating Organizations LCO’s

1. What is the FADe project II?

The project seeks to apply the methodology proposed in the Crocodile Hunter project developed by the Electronic Frontier Foundation to detect equipment used in telephone surveillance scenarios, specifically in 4G / LTE networks. To carry out this detection, individual devices or sensors need to be used.

Its main objectives are:

1. Collaborate with the team behind the methodology proposed by Crocodile Hunter, detecting the use of IMSI-Catchers in 2 cities in Latin America.
    - 1.1. To apply, document, and test methodological variations using technical tools.
    - 1.2. Share the results with local freedom of expression organizations and/or independent media in repressive, violent contexts and under surveillance.

This methodology seeks to detect the use of cellular communications surveillance devices or IMSI-Catchers in a given area, which pretend to be real antennas of mobile operators to intercept the communications of an arbitrary group of users. Crocodile Hunter software seeks to perform this detection with a high degree of reliability without leaving traces on the mobile network by not interacting with any cellular antenna. At this time, the methodology requires the configuration of a sensor. More information about the project can be found in:
https://github.com/EFForg/crocodilehunter

2. What do the FADe project II sensors look like?

Are composed of:

1. High frequency radio.
2. Battery or power bank.
3. GPS device
4. A pair of high-range antennas.
5. Raspberry Pi4.
6. USB-A or USB-C cable

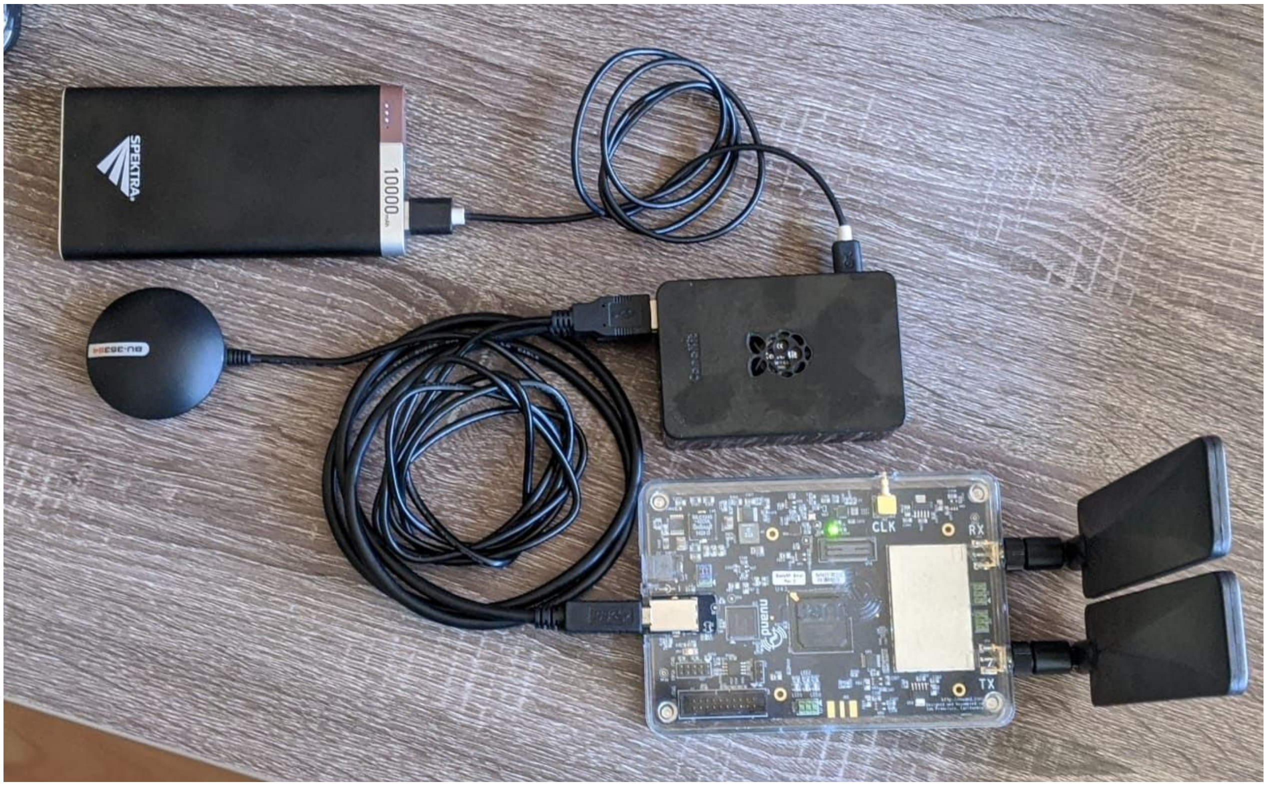

Figure. 1 Prototype sensor FADe II

These sensors can be operated in two ways:

- **Fixed location,** collecting all possible data for an extended period of time. E.g., a sensor located in a drawer, closet, car glove box, etc.
- **Mobile location**, collecting data in real-time in different locations. E.g., The sensor is mounted on a vehicle, motorcycle, etc.

3. For how long is the monitoring done?

The scope of the project proposes monitoring until the last day of November 2020. At the end of said monitoring, each team must be returned to the corresponding OCL (local coordinating organization).

4. How do you operate a FADe II sensor?

1. The battery or power bank must be charged (it is recommended to charge every 12 hours). The device must be connected as follows:
    a. Connect the high-range antennas to the high-frequency radio.
    b. Using the USB to USB-C cable, connect the battery or power bank to a USB-C port on the Raspberry Pi4 case.
    c. Connect the GPS device to a USB port on the Raspberry Pi4 case.
    d. Connect the radio to a USB port on the Raspberry Pi4 case.

2. When connecting the parts described above, the radio should illuminate a green light (this may take several seconds).

3. After the light is on, the sensor is working.

Note. The above described applies to the building of the sensors for the first time. Subsequently, connecting and disconnecting the battery or power bank will be enough to turn the sensor on or off.

5. How to solve some common problems when operating the FADe II sensor?

a. The sensor stopped collecting information:

1. The charge in the power bank may be exhausted.

b. The cable was disconnected:

2. It should be possible to connect again without problems.

c. The software is not loading data

3. This may be due to failures with the coverage of the GPS unit. As a general rule, with this type of device, they must have a flashing LED indicator. If it is fixed, it means that it is not receiving a GPS signal correctly. It can be moved to a place with a better open sky view, depending on geographical conditions; even having it behind glass can affect reception quality.
4. It's possible that the sensor does not have internet access. It is suggested to check the ethernet cable or the wifi networks that the device must access.

6. Who are those involved in the FADe I and II project?

1. **Seaglass (USA).** Creators of the methodology and infrastructure for data collection. A team of security researchers from the University of Washington to measure IMSI-catcher use in a city.
2. **Crocodile Hunter. (USA).** Creators of the methodology and infrastructure for data collection. EFF (Electronic Frontier Foundation) team of security researchers to measure IMSI-catcher use in a city.
3. **South Lighthouse (Chile).** Coordinating organization in charge of planning, monitoring and control, consulting, and training related to the development of the region's project.

7. What are the general risk considerations for using these sensors?

a. Sobre el comportamiento de los sensores

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

For cases where the sensor is located in a fixed place with a Wi-Fi connection or moving on the street and can enjoy Wi-Fi connection on an occasional scheduled basis (for example, at night or at other times planned), a line can be dispensed with the phone number for the sensor, making it even more difficult to track 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. When analyzing the content of the files on the phone, it cannot be determined for what purpose is this data there, or even what this information represents. In conventional telephones, no information is stored differently from what it would have if it were new from the factory.

c. About data transmission

The connection made between the androids 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 monitoring the connection can determine that the phone or the Wi-Fi network used is sending data to the corresponding server. With this consideration at the design level, the server used is not used for other applications to avoid its connection with other projects and initiatives. This server is not currently known for developing this or any other project. Finally, the information flow is compatible with the use of a traffic obfuscation and/or encryption tool installed on the phone and turned on at the time of data transmission.

d. About some measures taken to increase security

- The compiled data will be published after being collected to allow moving the sensors and anonymizing the data.
- The published data will not have exact location information to prevent or compromise their location. 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 keep the sensor in an inconspicuous place. As long as GPS signals can be received, the sensor will work without problems, even inside a bag, seat, vehicle trunk, etc.
- In the event of a revision, whoever is doing it can be informed that this sensor is used in academic research on the city's cellular signal's quality.
- If the context is a very high risk, it is recommended to follow the recommendations in the event of a potential seizure described below.

f. Recommendations in the event of a potential seizure

- **In general:** In the case of a low risk of potential seizure, we recommend only disconnecting the cables and turning off the sensor. In case of medium risk, we recommend removing the MicroSD card from the sensor. In high risk, we recommend deleting the information available on the MicroSD card. In a critical hazard, the sensor could be disposed of completely. Each Local Coordinating Organization may establish with the sensor operators when the risk of seizure is low, medium, high, or critical.

South
LIGHTHOUSE

For more information please visit https://fadeproject.org/

AA/october-2020