Location Tracking

Introduction

Mobile phones are often used to connect to the GSM network.

Since no phones that could potentially support Replicant have free software firmware for the modem, currently, the only possible way to avoid location tracking by the phone network is to have the modem powered off. Thus, it is desirable to add support for a way to easily turn off the modem (see #1779).

Implementing some tricks to make location tracking harder or not reliable with free software modem firmware has not been done to our knowledge, and we don't know in which extend it is possible. This page should document research into alternative protocols that could be used to get location privacy. Possible ways to prevent location tracking by the GSM network should also be listed.

Avoiding tracking by the phone network

Silent SMS

Some background information on how silent SMS or ping SMS are used and how they make location tracking possible:
https://en.wikipedia.org/wiki/SMS#Silent_SMS (German wiki article is a lot more detailed: https://de.wikipedia.org/wiki/Stille_SMS)
https://edri.org/edrigramnumber10-2silent-sms-tracking-suspects/
https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector/wiki/glossary-of-terms#user-content-silent-sms

F-Droid has an app that allows to send silent SMS: https://f-droid.org/repository/browse/?fdfilter=silent+sms&fdid=com.itds.sms.ping
The app can be used to send a silent SMS to a Replicant device and the radio log shows how the SMS is processed by the radio interface.

It looks like it is possible to detect silent SMS in Samsung-RIL. We could implement a detection mechanism and if a silent SMS is detected, the SMS is not acknowledged. This would violate the standard, but it could completely prevent tracking by silent SMS and make it a lot harder to track Replicant users that are connected to the phone network. We need to investigate if doing this is illegal in some jurisdictions. Silent SMS might be used to locate the phone's owner in an emergency which would be a feature that users like to have. So silent SMS shouldn't be dropped by default, rather should it be possible to optionally enable this detection mechanism.

This would be comparable to not responding to ping requests as host on an Internet Protocol network. This also violates the standard, but is often considered for security. However, silent SMS can reveal a lot more information about the user than ping requests.