Linkability of Failure Messages (LFM) is a security hole in the Authentication and Key Agreement (AKA) procedure.

The LFM flaw was first reported in 3G [2] and it has also been proven to work in 5G [1]. Compared to IMSI catchers, the use of the flaw for identifying nearby subscribers has two limitations: First, the attacker has to know the ID of a person of interest that they are looking for. Only these subscribers with known IDs can be detected, it is not possible to find the ID of a new subscriber without knowing / guessing it.

Second, LFM requires an attacker to probe every new device that connects to their fake base station for every ID that they are looking for. In addition to probing every new device, the attacker also needs to contact an authentic mobile network to obtain authentication requests for each person of interest.

Due to these limitations, the LFM flaw is less powerful than previously used IMSI catchers. The objective of this project is to examine the scalability and practicability of exploiting the flaw on a larger scale.

**Advisors**

Oliver Zeidler