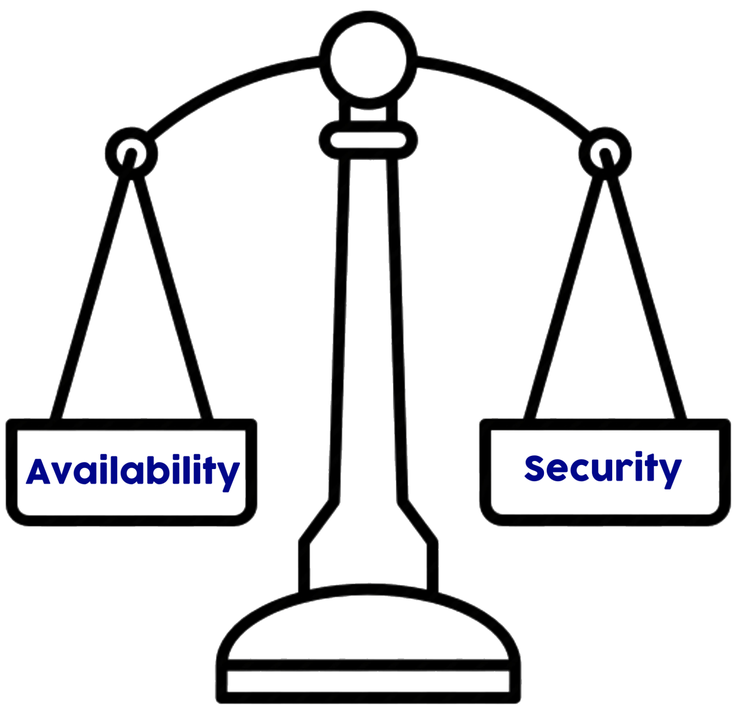
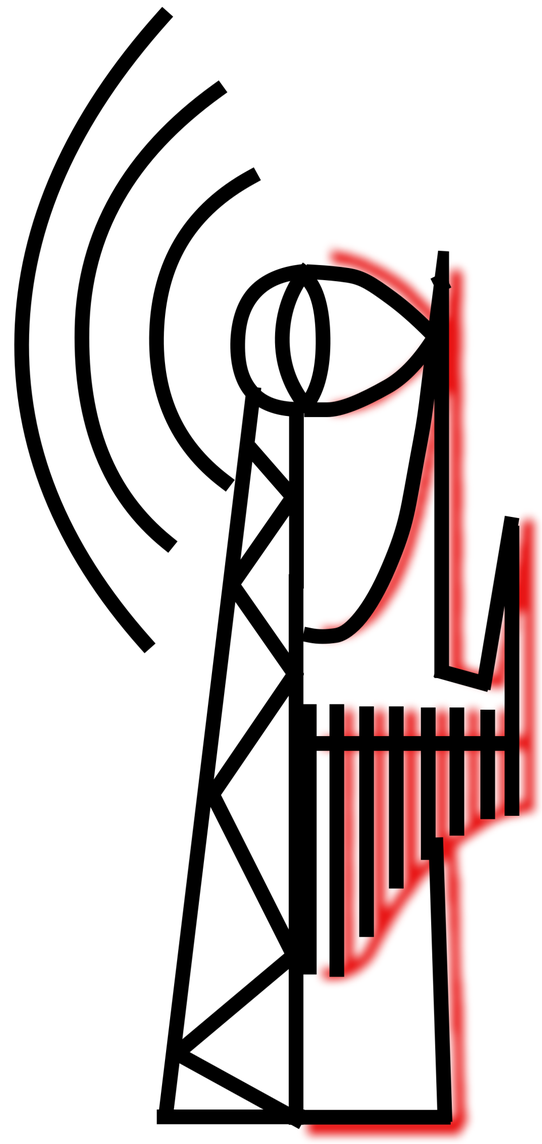
Intrusive device against LTE mobile networks

12



The LTE design made a tradeoff. There are messages from the base station, that are accepted even without security handshake. While these messages were supposed to increase availability of the network, they also create a security risk.

We can create a fake LTE base station. This station will present itself as a real one, and transmit these messages to the mobile phones that attempt to connect to it.



Using this method, this fake base station can do:

1. **Targeted denial of service until the device restarts,**
2. **Force it to use insecure GSM network,**
3. **Capture the identity of SIM card (which can be used to attack privacy of the network)**

Easy interface,
single installer,
battery powered
compact size.
We keep it simple stupid.

Timotej Kamenský
xkamen24(at)stud.fit.vutbr.cz