Mobile Communication RRC Message Security Analysis (Master Thesis)

Background

In this topic an analysis of RRC messages in 4G and 5G should be done. There exist several different kind of these messages with different functions and level of information content. The focus should lay on messages related to the connection. The analysis should consider privacy and security aspects. After the theoretical review and analysis, the practical part should focus on an attack. An implementation of one security and privacy aspect should be done as a proof-of-concept with Open Source hard- and software.

Objectives

This thesis provides an opportunity for students to gain hands-on experience with 4G, 5G technology through the following activities (varying complexity, depending on the type of thesis):

- Security and availability analysis of specific RRC messages
- Implementation of an attack
- Practical evaluation with testing of commercial smartphones Documentation and Reporting: Document the research process, experimental setups, findings, and challenges encountered during the research.

Requirements

Candidates should possess basic programming skills (C/C++ and Python) and have an interest in networking and wireless communication technologies. Although prior knowledge of 4G, 5G technology is beneficial, it is not mandatory. Familiarity with wireless communication protocols, network security principles, and basic hardware interfacing is advantageous.

Application Process

All applications must be submitted through the application website INTERAMT:
https://www.interamt.de/koop/app/trefferliste?partner=339
(Abschlussarbeiten Bachelor / Master)

Carefully note the information provided on the site to avoid any issues with your application.
Your application should include

- a short CV
- a current transcript of records
- the keyword “T3-MK-RRC” as a comment

For any questions or further details regarding this thesis and the application process, please feel free to contact ZITiS T3 (t3@zitis.bund.de) or PD Dr. Corinna Schmitt.