Technische Universität München, Department of Informatics

Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

Thesis M.Sc.

MeasrDroid –
Privacy-preserving distributed smartphone measurement

Background

In recent years, cellular devices pushed into the domain of global computer networks. Most of today's mobiles are connected to the Internet, yet only little data on the structure and topology of mobile networks is available. To overcome this situation, the Android-based *MeasrDroid* project has been brought to life.

Gathering data for several years, MeasrDroid has evolved into a rich and productive measurement framework. Collected data sets include information about device hardware, radio cells, network configuration including wifi, transfer statistics and active measurements, location data obtained by GPS and other techniques as well as a comprehensive set of environment parameters like earth's geomagnetic field, acceleration/gravitiy, lighting and gyroscope data. There is a broad variety of questions that can be answered using this data to learn more about mobile networks, and about the behaviour of its users.

Motivation

Since its initial deployment, the requirements have changed: Data privacy is becoming more relevant and users expect computer systems which cope with their own data to be privacy-preserving. Currently, MeasrDroid features various privacy-preserving and security features, but is a centralized system collecting data on a single server. The server is heavily secured against attackers, but it still demands the trust of its users. Here, a new research question arises: What changes are necessary to achieve privacy- preservation of such a system and in consequence to make trust superfluous?

Approach

Your main goal is to design a new privacy-preserving system infrastructure for the MeasrDroid framework. In a first step you are to develop an architectural concept, which respects user privacy while still allowing individuals access their own measured data.

In a second step, you develop a prototype of this new architecture, which includes the modification of the existing smartphone application and the server-side software framework to realize confidential data transfer.

We assume that central components of the MeasrDroid framework may still be suitable to carry out their task of collecting sensor data and handling interaction with the participating smartphones. At the same time, the system should only act as a broker that is unable to actually analyze the data it transfers. This requirement shall be fulfilled by measures of cryptography. To this end, each user should get an individual virtual machine acting as the final recipient of the user's information. The VM remains under the full control of the user, hence, it alone can access the sensor data to provide an interface for personalized analysis.

Requirements

If you are interested in working on this topic, you should meet the following requirements:

- Independent work style and explorative nature
- Strong background in security and privacy
- Programming experience (Java and Python)

Contact

Dipl.-Inf.Johann Schlamp schlamp@net.in.tum.de
Dr. Holger Kinkelin kinkelin@net.in.tum.de
Marcel von Maltitz, M. Sc. vonmaltitz@net.in.tum.de