Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Design of a Shared Parking System with special attention to security aspects

Simon Englert

Supervisor: Prof. Dr. Dmitrienko

http://se.informatik.uni-wuerzburg.de/

Structure

- Introduction (PIBA)
- Related work and background
- System Model and Requirements
- Design
- Security Analysis
- Implementation
- Future Work and Conclusion

Indroduction

- Problem:
  - Amount of parking spaces limited, amount of cars steadily increasing
  - Creation of new parking spaces difficult and expensive
- Idea:
  - More efficient use of existing parking spots
- Benefit:
  - Less frustration when searching for parking sport, fewer trafic jams
  - Less air pollution, less petrol use
- Action:
  - Shared Parking
  - -> Different people are able to use the same parking spot at different times

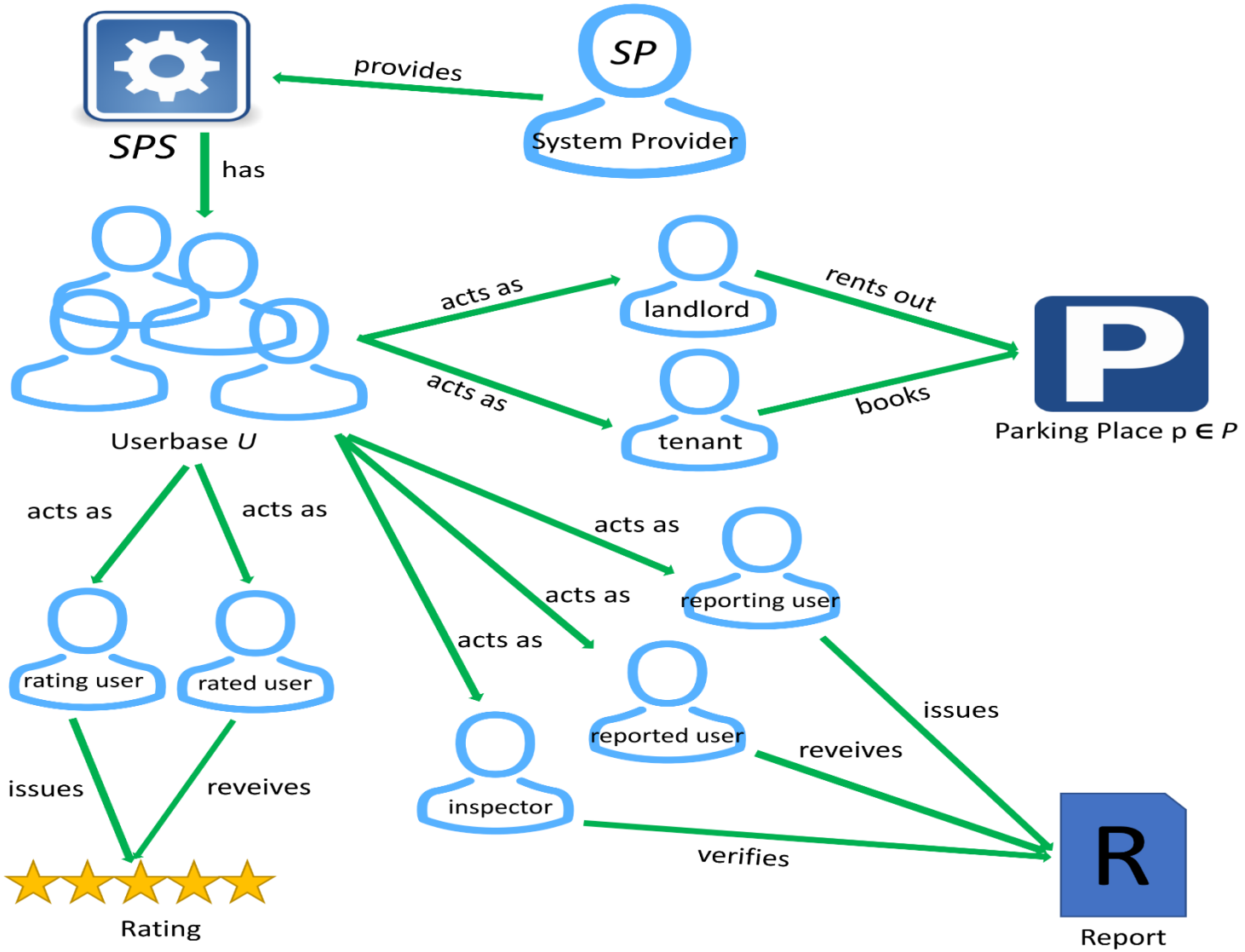
Related work and background

- Great amount of scientific work about ‚intelligent parking systems‘
- Nearly no scientific work about ‚Shared Parking‘
- Few amount of applications that implement Shared Parking
  - Not really successful (success is city based)
  - No information on security aspects

System Model and Requirements – High-level Overview

- Offers an online marketplace where both private and business users can rent and lease parking spaces
- End user particiation through smartphone
- Particular importance is given to handling fraud
- SPS does not aim at preventing unauthorized access to parking spaces, but instead incorporates mechanisms to punish misbehaving users

System Model and Requirements – System Model



System Model and Requirements – Functional Requirements

- Basic rental functions (+ search function via a map)
- Low deployment costs and of the shelf hardware
- Automatic Processing

System Model and Requirements – Adversary Model

- Adversary Model and Classes of Fraud
  - Class 1: stem from the general nature of a shared parking system
  - Class 2: stem from introduction of reputation system, e.g.
    - Corruption attack
    - On-Off attack
    - Re-entry attack
    - …
  - Class 3: exceptional cases that cant be solved without manual intervention

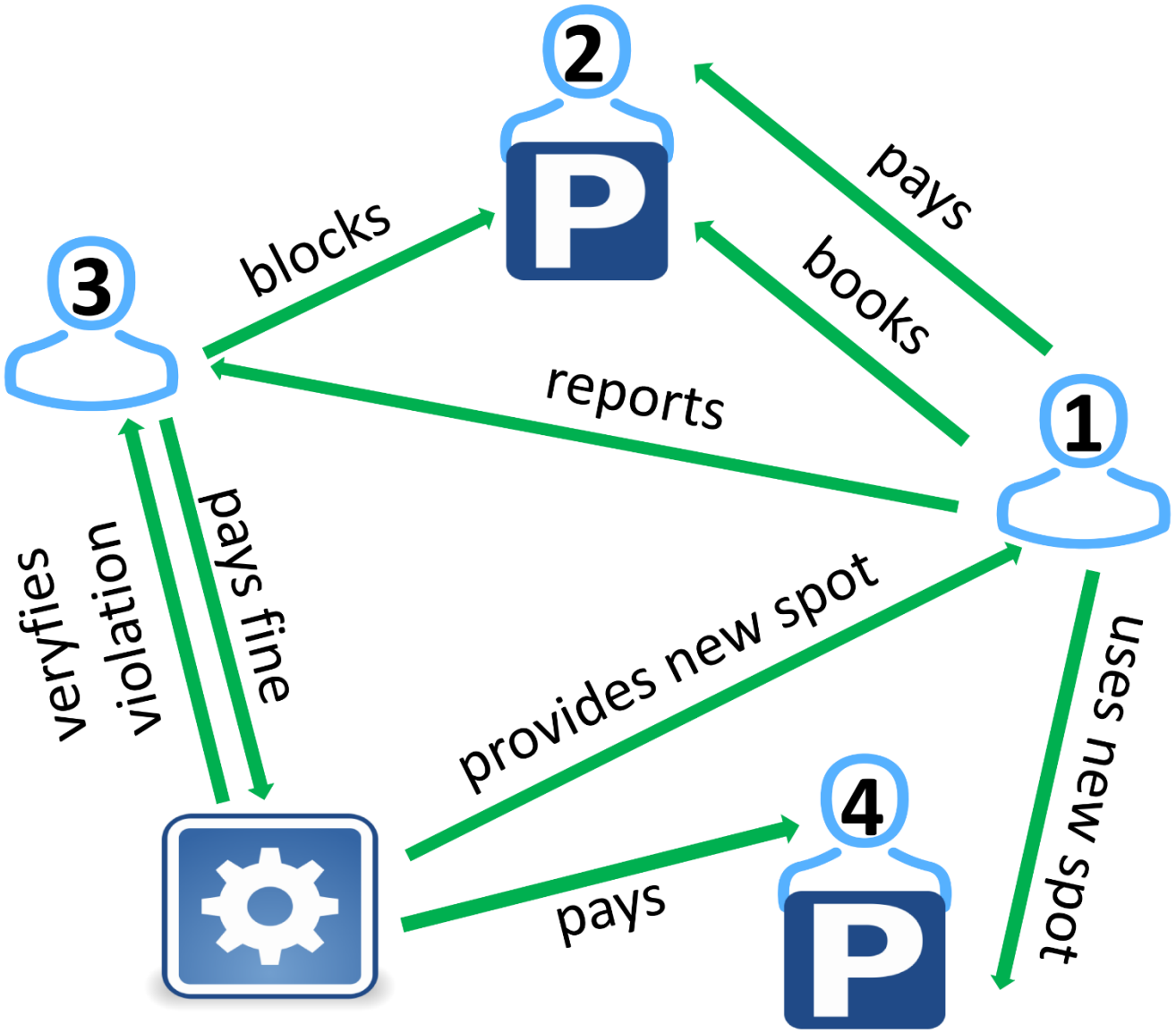
System Model and Requirements – Security Requirements

- Fraud Prevention
- Fraud Detection
- Fraud Punishment
- Fraud Compensation

Design – Features

- Functional Features
- Security Features
  - Rating Module
  - Reporting Module
  - Verification Module
  - Reputation Module
    - Based on Dynamic Trusted Set Based Reputation System for use in Mobile Participatory Sensing Applications
  - Sanctioning and Compensation

Design – Example

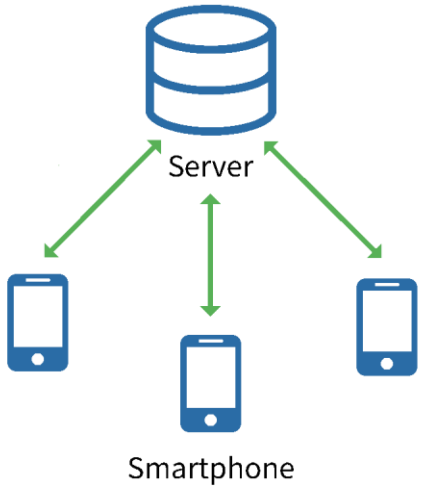


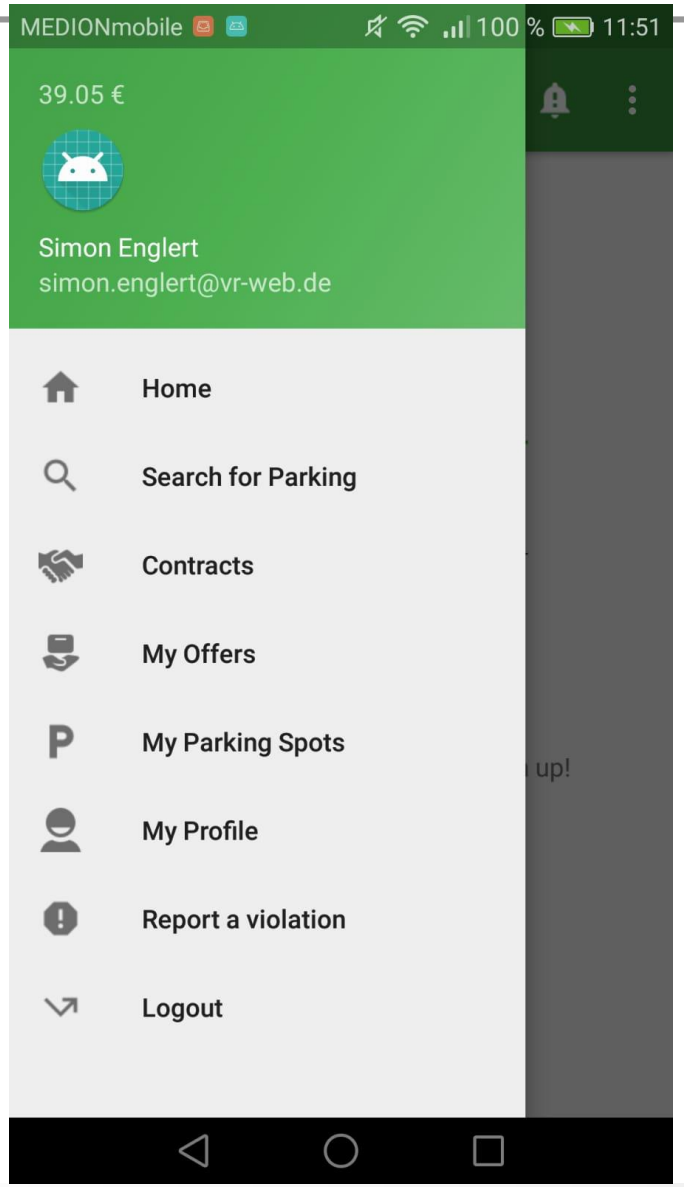
Security Analysis

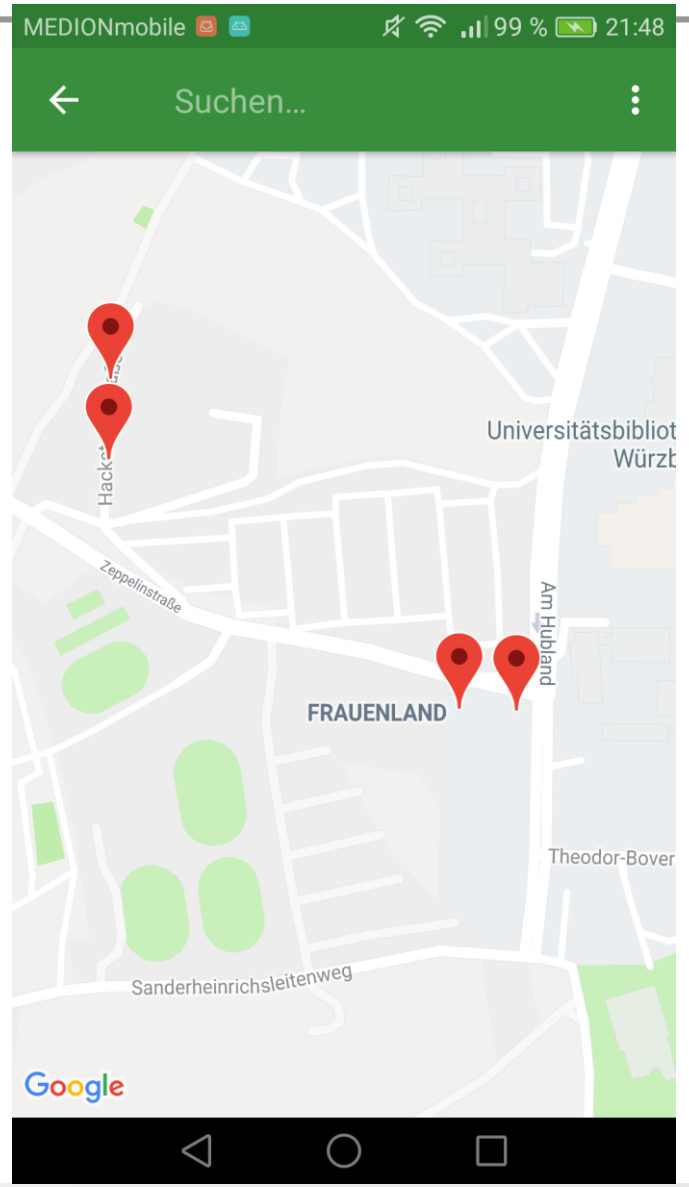
- Fraud Detection
  - Fraud recognition
  - Adversary identification based on reputation system
- Fraud Punishment
  - Based on the ability of adversary identification
- Fraud Compensation
  - Based on the ability of adversary identification
- Fraud Prevention
  - Through Deterration
  - Through Elimination

Implementation

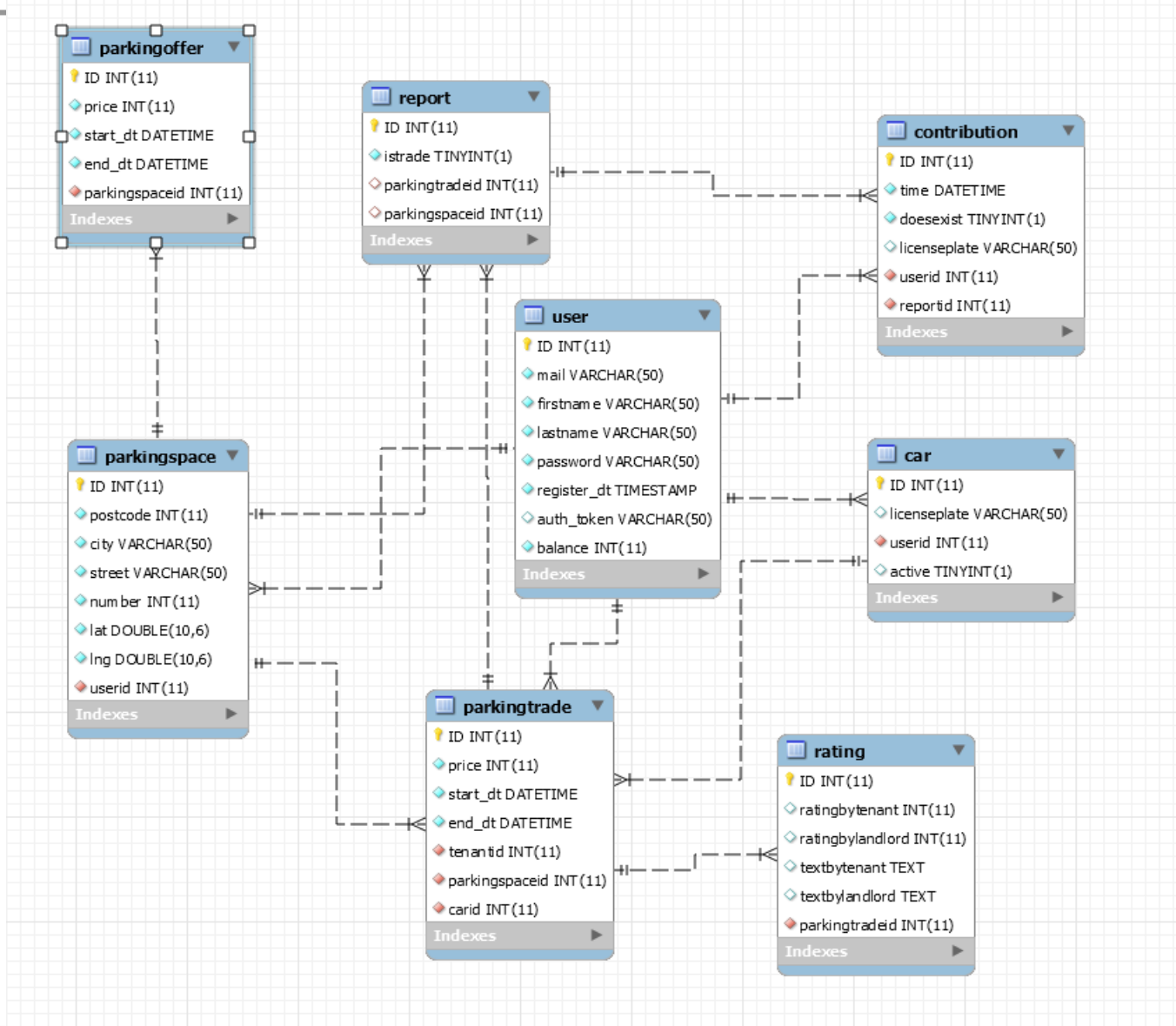
- Database
- Java Web Service
- Java Android Prototype







Implementation



Future Work and Conclusion

- Elaboration of the reputations system
- Extenting the functionality of the prototype
- Testing usability and performance of the app