Secure Systems Group, University of Helsinki

Masoud Naderpour, Andrey Shorov, Valtteri Niemi

Privacy-preserving Carsharing for Autonomous, Connected Cars

Background

- Carsharing services are getting more popular everywhere.
- Such services can be categorized in two major categories: *peer-to-peer* and *corporate* services.
- In corporate carsharing service, a company owns and manage the whole fleet.

Motivation

- In current corporate model, the service provider gets to know the identity and whereabouts of the user.
- Specifically, the following privacy sensitive information are known to service provider:
  - User's identity
  - Precise pickup and drop-off locations
  - Precise pickup and drop-off times
  - Full trip trajectory
- Autonomous cars will change the model of car sharing service in near future.

Corporate Carsharing Ecosystem

- In our design we consider the following entities to be involved in a privacy preserving car sharing scenario:
  - user
  - car
  - service provider
  - mobile network operator
  - payment operator
  - insurance company
  - law enforcement

Challenges

- **Identity Privacy:** user's identity should be kept anonymous towards service provider as long as user behaves. In case of emergency or law enforcement's request, service provider should be able to de-anonymize the target user.
- **Location Privacy:** service provider monitors (collects) continuously the whereabouts of its fleet to provide on-demand service (to improve the quality of the service at a later time). The solution should consider protection of user's location privacy, while maintaining the functional requirements of service provider.
- **Reputation System:** service provider should be able to keep a ranking system of users while individual trips of a user should be unlinkable.
- **Payment Process:** service provider should be assured the user has enough credit to pay for the service. Payment transactions should be anonymous.

Design & Building Blocks

Our design initially targets protection of user's identity. We use different privacy enhancing technologies to provide *identity privacy*.

- Pseudonymization proxy: a middle entity issues one-time pseudonymous IDs to protect real identities.
- Anonymous credentials: anonymous credentials enable cars to authenticate users anonymously.
- Anonymous payment: payment tokenization enable users to anonymously pay for the service. Alternatively, mobile network operator could be leveraged for billing using user's mobile subscription.

Help us! Please fill the questionnaire.