Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

geoinformation engineering
ikg eth zurich

A model of privacy conflicts in sharing mobile spatial data

Autor: Athanasios Mantzaras
Head: Prof. Dr. Martin Raubal
Supervisors: Dr. Simon Scheider, Dr. Paul Weiser

Master Thesis, Automn Semester 2015

Motivation and Goals

There are many techniques used nowadays to address risks arising from location information exposure. These techniques can be grouped into the following categories:

- Query enlargement techniques
  - Spatial cloaking (Obfuscation, Mixed zones)
  - Temporal cloaking
- Fake location techniques
- Encryption based techniques

What do they miss ?

Privacy risks cannot be efficiently addressed without knowing the potential conflict of interest between different actors. Therefore it is important to collect and analyze examples of conflicts between different actors.

The health insurance case

The interest of an individual doing mountain biking may be to share information to find new tracks. At the same time he or she wants to pay a low premium for health insurance. The interest of the company is to get a high premium in order to increase its profits. The kind of information in this example is activity information derived from trajectories. The usage of this information is what puts the individuals under risks, meaning that it is used against their interest. The company uses the information to find out that the individual performs an activity (e.g. mountain biking) that might cause injury that later the insurance company would have to cover. This is better perceived with Figure 1.

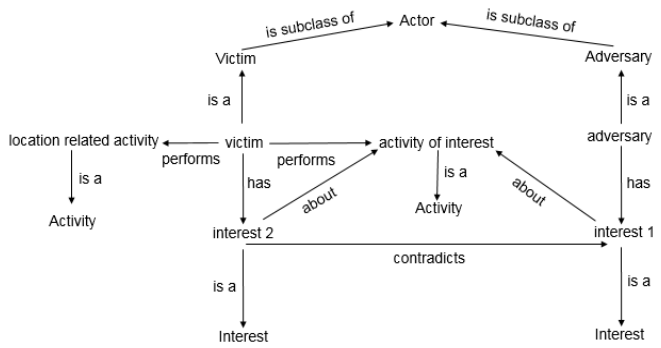

Figure 1: A first empirically founded model of conflict of interest

Goals

a) The collection of cases of misuse from mobile personal spatial data that reflects the known variety of threats and conflicts of interest.

b) Based on these empirical cases, to suggest a model of potential conflicts of interest between different agents (private persons, companies) that could be used to (automatically) detect or infer potential threats in a given situation of sharing data.

c) To show potential benefits of such a model.

Approach

In order to reach the goals, cases of misuse in sharing mobile personal spatial data (such as trajectories) are gathered and then investigated to identify the threats and conflicts of interest. Ontologies define basic concepts in a domain of interest and the relations between them (Noy and McGuinness, 2001). In this thesis an ontology is developed based on the guide proposed by the aforementioned authors that consists of the following steps:

- Competency questions
- Definition of classes in the ontology based on cases
- Arrangement of the classes (hierarchy)
- Slots and allowed values
- Iteratively revise and refine the ontology
- Test the ontology

The evolvement of the first empirically founded model of conflict of interest into an ontology is shown on Figure 2.

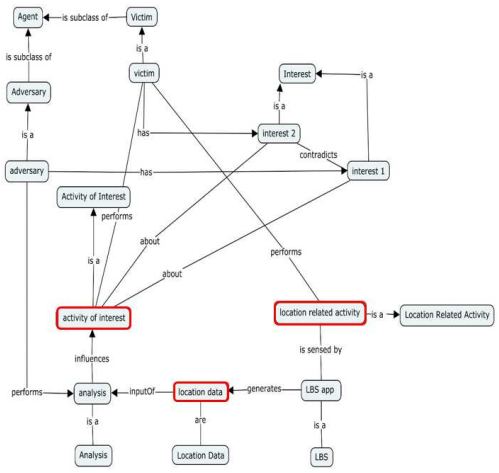

Figure 2: Ontology visualization with Cmap software

Location data are the link between the location related activity of the victim and the activity of interest.

Formalization of the ontology in RDF

After sketching the ontology with Cmap, it needs to be formalized in RDF (Figure 3).

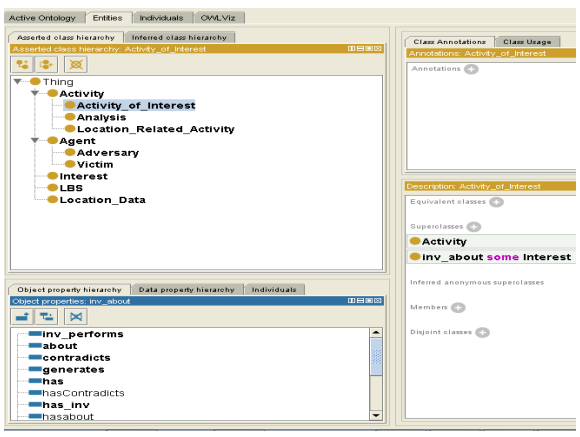

Figure 3: Formalization of the ontology in RDF

Case studies

Stalk

An example of that case could be Sophia who has a relationship and lives in the same apartment with Lucas. After some time Sophia and Lucas split up and Sophia decides to leave the residence to Lucas and find another apartment for herself. Lucas doesn't like the decision of Sophia. Also Sophia wants to have no contact with Lucas in the future and keeps her new address secret from him. After moving out she dates another guy. Let's suppose that Sophia uses a LBS for her navigation needs in the new neighborhood. Now if Lucas finds out the location information (new address) of Sophia, he might stalk her and therefore intrude her privacy. Another possible threat could be to insult her, so the threats are apparent in this case.

Spam messaging

Similarly one could consider the case where Anna visits a mall and uses a special LBS for navigation purposes between the different stores. Let's assume that Nick an employee of the store situated in that mall gains access to the location information of Anna that has entered the mall. Then it would be to the store's interest to promote its products. Then the store might send a message to Anna with special discounts that they have or new products that they want to promote. In this case the threat for Anna is to be bothered with messages from third parties that she doesn't know.

Figure 4: Spam messaging

Conclusion and discussion

Attainment of goals

- The developed pattern can be applied to a class of diverse cases, and therefore there is hope to come up with a general pattern.
- The developed model puts the conflict of interest in the center of attention

Potential application of the model to social networks

- Social networks have the profile of the users (city of residence, relationship status etc.)
- Social networks may access the physical location of the user through GPS sensor
- An algorithm could combine profile and physical location data to infer dangerous places that do not fit the profile (e.g. night club for married user)
- Social networks could warn the user based on the model of conflicts of interest for possible threats

Limitations

The model only deals with existing threats and not possible threats