Title: Privacy Control for Online Social Networks

Contact:

Abdessamad Imine
LORIA-INRIA, Nancy, France
Tel: 0354958535
email: abdessamad.imine@loria.fr

Michaël Rusinowitch
LORIA-INRIA, Nancy, France
Tel: 0383593020
email: michael.rusinowitch@loria.fr

This project is partially supported by MAIF Foundation project: “Protection of Personal Information on Social Networks”

Description:

The majority of social networks (like Facebook, LinkedIn, etc) provide control functions to limit the visibility of certain data (such as friend list, wall posts and images) to a specific user group. To get online social activities with greater confidence and less risk, it is imperative to devise tools that allow users to control themselves the usages that their data can be destined to. These tools assist users to detect and minimize the dissemination and use of personal information.

The objective of this internship is to contribute to the design of an environment for monitoring interactions in social networks based on user defined privacy requirements. This environment is expected to have the following functionalities:

1. Detection of privacy vulnerabilities
Privacy risks may appear either directly after online data publication (e.g. finding a user's phone number within a wall post) or indirectly through an inference of private information (e.g. deducing sexual orientation from some friendship relations). In this part, we will propose a methodology for characterizing and building direct and indirect attacks. For direct attacks, given a user target, we will provide efficient algorithms for crawling a social sub-graph in order to fix a subset of attributes. Since indirect attacks allow extracting information not explicitly stated in user profiles, we will combine algorithmic and statistical approaches to infer data with high probability.

2. Protection against privacy vulnerabilities
When privacy vulnerability is detected, it may arise from one or several users linked by friendship relations. To eliminate or minimize privacy vulnerabilities, we plan to explore two trade-off techniques. The first one must combine optimally two possible actions: (a) hiding sensitive attributes (such as home address, email address and phone number) and (b) not disclosing some friends to others. Besides a binary logic (publish or hide), the second technique enables us to change the semantics of the published information in such a way it becomes less accurate (or noised). This technique has to adapt some anonymization methods [1, 2] (used for offline publication) for online user interactions.

References

[1] H. H. Nguyen, A. Imine and M. Rusinowitch. “Anonymizing Social Graphs via Uncertainty Semantics”. In *ACM Symposium on Information, Computer and Communications Security* (ASIACCS), 2015, pp. 495-506.

[2] H. H. Nguyen, A. Imine and M. Rusinowitch. “Differentially Private Publication of Social Graphs at Linear Cost”. To appear in *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (ASONAM), 2015.

Key words: Social networks, Privacy, Statistical Machine Learning, Graph Algorithmics, Data Mining.