POSTDOCTORAL FELLOWSHIP

OPEN POSITION

DESCRIPTION

The IMPACT Project **Citizen Trust in the Digital word** (Digitrust) within the context of Lorraine Université d'Excellence (LUE) Program is inviting applications for a post-doctoral position (100%, 12 months) to work on the topic of **Privacy Control for Online Social Media**. Applications are invited from those with a PhD qualification and publications in a directly relevant area (computer science, probability and statistics, security, privacy or data-mining). The applicants should have a passion for collaborating in inter-disciplinary research and the academic skills to be part of a research team aiming to make a high impact.

TERMS AND TENURE

This one-year position will be based at the LORIA in Nancy, France, in Pesto team. The group works on both fundamental and applied aspects of security and privacy in protocols and social networks.

The post-doctoral researcher is expected to contribute to the design, analysis and development of original solutions for self-controlled privacy in social networks. By combining algorithmic and statistical approaches, the objective is to prevent sensitive information dissemination with high probability.

The target start date for the position is **01/01/2022**, with possible extension.

Gross Salary per month: **2845 euros**.

HOW TO APPLY

Applicants are requested to submit the following materials:

- Curriculum Vitae - Your most recently updated C.V. including list of publications
- Cover Letter
- Statement of Research

For more information about this position and for application (including CV with references, relevant publications, motivation letter), please contact:

Abdessamad Imine
Phone : +33 3 54 95 85 35,
abdessamad.Imine@loria.fr

Michaël Rusinowitch
Phone : +33 3 83 59 30 20
michael.Rusinowitch@loria.fr

with cc to Maira Nassau
(Digitrust Project manager)
maira.nassau@loria.fr

POSTDOCTORAL FELLOWSHIP

OPEN POSITION

Deadline for application is ***15/10/2021***. Applicants will be interviewed by an Ad Hoc Commission by ***01/11/2021.***

JOB LOCATION

Nancy, Lorraine, France.

DETAILED ANNOUNCEMENT

Description of research topic :

The growing interest in online social networks (like Facebook, LinkedIn, Twitter, etc) has led to collecting huge amount of data produced by users without precautions. The majority of these networks provide control functions to limit the visibility of certain data (such as friend list, wall posts and images) to a specific user group. However, most of users are unaware of the risks associated with the publication and exchange of personal data on social networks. Even if awareness exits, either the users usually ignore how to configure the security settings to protect their personal data or these control functions are not sufficient to enforce some privacy properties. For example, publishing and sharing location information on Twitter could easily lead to a burglary. Additionally, users have no full control over the usage of the data they generated. Indeed, this data is either accessible to other friends or sold by the owner of the social networking site to business companies for producing more revenue. Accordingly, the risks due to naive data sharing are constantly increasing, allowing privacy attacks with unfortunate consequences, and making people very reticent to remain socially active (e.g. staying connected with friends and expanding friendship circle).

To get online social activities with greater confidence and less risk, it is imperative to develop user-centric solutions for protecting personal data. Indeed, since privacy is simply the restriction persons can enforce on their proper data [1], it is crucial to devise tools that allow users to control themselves the usages that their data can be destined to. Thus, a better understanding of the sensitivity of the shared content allow us to effectively assist users during their interactions with social networks. This assistance has as main objective to detect and minimize the dissemination and use of personal information of users. For instance, early warning a user that a publication of a message on her/his profile might reveal her/his religious affiliation would avoid accidentally sharing sensitive information and would provide high assurance in social networks.

UNIVERSITÉ DE LORRAINE

POSTDOCTORAL FELLOWSHIP

OPEN POSITION

Description of methodology :

The objective of this post-doctoral position is devising an environment for monitoring interactions in social networks based on user defined privacy requirements. This environment is expected to have the following functionalities:

1. Definition of sensitive information

Each user has a profile containing some personal attributes (such as gender, age, location and religious and political affiliations) and describing relationships and interactions with other users. To better understand privacy expectations of social networks' users, we plan to conduct qualitative and quantitative surveys for determining perceptions and preferences of users on the data/information that they consider sensitive. These surveys must be anonymous. In this case, they may be achieved using protocols well suited to social networks [2]. From the results of these surveys, we will define cost functions in order to quantify user privacy based on sensitive information. Note that this quantification enables us to measure and report potential privacy risks.

2. Identification 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. Extensive experiments will be conducted on real social network datasets to demonstrate the effectiveness of both attacks.

3. Countermeasures against privacy vulnerabilities

When privacy vulnerability is detected, it may arise from one or several users linked by friendship relations. Any countermeasure should be fair (i.e. it does not affect the privacy of other users) and optimal (i.e. it does not isolate completely user from the friendship circle). 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 [3, 4, 5] (used for offline publication) for online user interactions.

4. Risk prediction

The objective of this functionality is to provide preventive solutions against any potential risk that threatens the user privacy on social networks. To do this, two tasks will

be planned: (i) The first one consists in predicting risk for prospective user interactions. Thus, we can simulate the risks involved when the user wants to publish information (e.g., a post, a photo or a video) on her/his profile. (ii) As for the second task, it suggests countermeasures for some risky interactions (e.g. publishing a photo without tags). To predict and minimize or eliminate potential privacy risks, it is necessary to develop a methodology based on probabilistic models, which analyzes a social graph and builds classes of users (w.r.t the risks involved and the users' profile). These classes will serve as base to recommend different actions in order to preserve or improve the user privacy.

References

[1] G. Gürses and B. Berendt. "The social web and privacy: Practices, reciprocity and conflict detection in social networks". In *Privacy-Aware Knowledge Discovery, Novel Applications and New Techniques*, F. Bonchi and E. Ferrari, Eds. CRC Press, 2010, pp. 395-429.

[2] B. T. Hoang and A. Imine. "Efficient Polling Protocol for Decentralized Social Networks". To appear in *International Symposium On Stabilization, Safety and Security for Distributed Systems* (SSS), 2015.

[3] 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.

[4] 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.

[5] H. H. Nguyen, A. Imine and M. Rusinowitch. "A Maximum Variance Approach for Graph Anonymization". In *Symposium on Foundations and Practice of Security* (FPS), Best paper, 2014, pp. 49-64.