issues have to be addressed: information disclosure from social network users and/or from their friends. Therefore the following investigate anonymization and obfuscation techniques for preventing unintentional sensitive put the hand on the origin of threats and design effective countermeasures. This approach allows us to prevent them from publishing data that may endanger the privacy. To that end, we investigate potential privacy attacks, study their feasibilities and analyse their impacts. This approach allows us to put the hand on the origin of threats and design effective countermeasures. To do that, the thesis will investigate anonymization and obfuscation techniques for preventing unintentional sensitive information disclosure from social network users and/or from their friends. Therefore the following issues have to be addressed:

1. Detection of privacy vulnerabilities. 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. Among these attributes, some are considered to be sensitive according to General Data Protection Regulation and national regulations. 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 sensitive information (e.g. deducing sexual orientation from some friendship relations). In this stage, the goal is to propose a methodology for characterising and building direct and indirect attacks. Direct attack will exploit privacy policies' inconsistency. For inference attacks one can rely on recent advances in machine learning and natural language processing.

2. Countermeasures design and implementation. When a sensitive attribute is vulnerable to an inference attack, the proposed inference algorithm will provide explanations such as an ordered list of publications (attributes, friends, posts, pictures ...) that have probably lead to the leak. This can be exploited to investigate effective countermeasures. However two situations have to be distinguished: (a) either the problematic publications are all originating from the user himself or (b) some of these publications originate from relations. To eliminate or minimize privacy vulnerabilities, two techniques should be explored. The first one amounts to hide attributes that help inferring the sensitive ones

**Context**

This position is open in team Pesto from Loria and Inria Nancy-Grand Est.

The contacts persons for information and application are:

Dr. Abdessamad Imine abdessamad.imine@loria.fr

Dr. Michael Rusinowitch michael.rusinowitch@inria.fr

**Main activities**

**Project description**

The thesis objective is to provide social network users with an application to audit their profile and prevent them from publishing data that may endanger their privacy. To that end, we investigate potential privacy attacks, study their feasibilities and analyse their impacts. This approach allows us to put the hand on the origin of threats and design effective countermeasures. To do that, the thesis will investigate anonymization and obfuscation techniques for preventing unintentional sensitive information disclosure from social network users and/or from their friends. Therefore the following issues have to be addressed:

1. Detection of privacy vulnerabilities. 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. Among these attributes, some are considered to be sensitive according to General Data Protection Regulation and national regulations. 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 sensitive information (e.g. deducing sexual orientation from some friendship relations). In this stage, the goal is to propose a methodology for characterising and building direct and indirect attacks. Direct attack will exploit privacy policies' inconsistency. For inference attacks one can rely on recent advances in machine learning and natural language processing.

2. Countermeasures design and implementation. When a sensitive attribute is vulnerable to an inference attack, the proposed inference algorithm will provide explanations such as an ordered list of publications (attributes, friends, posts, pictures ...) that have probably lead to the leak. This can be exploited to investigate effective countermeasures. However two situations have to be distinguished: (a) either the problematic publications are all originating from the user himself or (b) some of these publications originate from relations. To eliminate or minimize privacy vulnerabilities, two techniques should be explored. The first one amounts to hide attributes that help inferring the sensitive ones...
these attributes are provided by the privacy vulnerability analysis step. The second technique enables one to change the semantics of published information in such a way it becomes less accurate (or noised). This last technique has to be adapted from some anonymization methods used for offline publication [Nguyen16].

Some references


Skills

Applicant for this position must have an MSc or equivalent in computer science or Telecommunications.

The candidate should have:
- strong background in some of the directly relevant area (algorithmic, machine learning, statistics, security and privacy, data-mining).
- experience in developing prototypes (preferably in Python)
- good oral and written communications skills

A detailed CV (including grades and/or ranking, references, master thesis, publications if applicable) should be sent to the contact persons.

Benefits package

- Subsidised catering service
- Partially-reimbursed public transport

Remuneration


Monthly salary after taxes: around 1596,05€ for 1st and 2nd year. 1678,99€ for 3rd year. (medical insurance included).