Research theme for a PhD.

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

Dynamic Epistemic Logics for Privacy

Topic. Online services such as e-admin, e-banking, etc. use complex decision processes (fed by forms) to calibrate the offer (benefits) they make to each applicant. These decision processes require many personal data items, which are subsequently processed and stored. Removing from users' application forms the personal data items, which are not strictly useful for its subsequent evaluation by a service provider, is imposed by privacy laws enacted worldwide, and is useful for both service providers and users.

This project aims at reducing as much as possible the private information the applicant reveals. To fully understand this problem, one needs to formalize the data collection process, the meaning of the expression *strictly useful information*, what can be infer from the data collected, what kind of attacks can be led to obtain private information about the applicant.

Goal. Modal logics have a wild range of applications: epistemic logics have been developed to model knowledge, believes and reasoning; modal logics such as propositional dynamic logic and temporal logics are used to formalize algorithms; deontic logics are used to formalise normative systems (e.g. laws, protocols).

Here, we aim at formalizing and implementing algorithms that reduce the data collected to the strict minimum given a decision process. To formalize this problem, one needs to use modal logics - dynamic epistemic logics among others - to describe the initial problem (data collection and decision procedure) and to understand what is the real exposure, in terms of privacy, of the applicant during this procedure. In a second phase, to implement algorithms, one need to use logical solvers (such as SMT solvers for instance) in addition to traditional programming languages.

Possible research directions. The project involves both theoretic research - formalizing reasoning, privacy, algorithms and attacks with logics - and more practical research implementing the algorithms developed. However, depending on the interests of the applicant, the project could have either a dominant theoretical part, or a dominant applicative part.

References

- R. Fagin, J.Y. Halpern, Y. Moses, M.Y. Vardi. Reasoning About Knowledge. MIT press. 1995.
- H. Ditmarsch, J.Y. Halpern, W. van der Hoek, B.P. Kooi, editors. Handbook of epistemic logic. 2015.
- N. Anciaux, B. Nguyen, M. Vazirgiannis. Limiting data collection in application forms : A real case application of a founding privacy principle. In IEEE PST, 2012.

Laboratory & Team: LIFO, Systems and Data Security
Host institution: INSA Centre Val de Loire
Advisors: Dr. Sabine Frittella and Dr. Benjamin Nguyen
Emails: benjamin.nguyen@insa-cvl.fr and sabine.frittella@insa-cvl.fr
Webpages: http://www.benjamin-nguyen.fr/ and https://sites.google.com/site/sabinefrittellalogic/home