Ioana-Gabriela Chelaru
248-1
the 21^{st} of November, 2020

Paper report on

Applying Formal Methods to Detect and Resolve

Ambiguities in Privacy Requirements,

written by *Ioannis Agrafiotis, Sadie Creese, Michael Goldsmith,*

and Nick Papanikolaou,

Published in 2011, found at this address

This article is based on the work done during the EnCoRe project that included the development of a model of consent and revocation used to specific contextual requirements, enabling simultaneously the translation of natural language expressions of consent and revocation needs into an unambiguous form suitable for checking implementations against. It describes all the issues discovered when applying the model in a real-world case study, specifically ambiguities that derive from the challenges and gaps created when the details of the law, regulation, policy, and social factors are combined and applied by computer scientists

The motivation behind this paper consists in the increasing occasions when individuals disclose their personal information via the Internet in order to acquire access to services, products, and benefits of today's society. Nowadays, the concerns regarding the abuse of personal data are rising mainly because individuals are required to give access to third parties, and that weaknesses the control that the owner has over his data leading to an increasing number of incidents where data has been lost, mistreated, or shared without authority.

The article focuses on consent and revocation controls and their practical implications when formalising high-level requirements. It discusses the ambiguities that occurred in the scenarios that were analised, categorisses then into two kinds, according to their existence and proposes the use of formal methods in order to address these problems. The logic used is designed to provide a verification framework for privacy and identity management systems, while the usage o formal methods promises to translate the privacy policies written in natural language into machine readable formats and consists of two models of consens and revocation, more specifically access control model and Hoare logic, both developed to be complimentary to one another.

The access control model is used to formalise the semantics of consent and revocation processed using labelled transition systems, is suited for expressing privacy preferences and it immediately supports policy enforcement architectures, but it does not provide an intuitive language for data subjects to express behaviour regarding the problem. The Hoare logic defines consent and revocation processes with a set of rights and it effectively models them as the application of rights that allow certain permissions.

The case study used for the validation of the models and logic is the Enhanced Employee Data Scenario since it is a well-understood problems and offers interesting issues in terms of managing consent and revocation controls. This study describes a various number of use cases that are meant to illustrate key points affecting the management of consent and revocation, while the employee data scenario focuses on sensitive information like trade union membership, financial details, home address and other family details.

The ambiguities that emerged from the formalisation of the requirements were divided into two classes as follows: the first class holds the ambiguities created from the applications of the law, regulations and policy, for example the data subject wishes to update his personal data, there can be ambiguities emerging as to whether previous data should be deleted or linked with the new data or if the changes should propagate to other parties involved, while the second one consists of ambiguities emerged from complexity of the notion of privacy and the conflict between the desire of the subjects to control their data and the controllers wanting to reduce subject's interference. The two most interesting issues belonging to the second class are aggregation, which means combining pieces of available information in order to unveil more information that may compromise the subjects privacy and anonymity, concerning the cases of data anonimisation when the subject looses his rights over that data.

In order to resolve all of these problems, the articles introduces actions for enabling subjects to update their data by deleting or linking it to the new one, considering the choice of propagating changes made over the data, implementing the choice to keep the subject notified on the processes made over his data, creating new variables to determine when the subject could perform different actions, etc. The future work will consist in validating the extended logic and identifying new ambiguities in the scope of developing a general applicable logic.

In conclusion, this paper manages to demonstrate the impact and importance of using formal methods when formulating clear privacy requirements, it addresses the issue of transforming requirements expressed in natural language into formal notation focusing mainly on consent and revocation controls in a real-world case study that has emerged within the EnCoRe project.