Computer Communications 107 (2017) 75–92

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Situation-based privacy autonomous management for mobile social networks

Ariel Soares Teles[a,b,*], Francisco José da Silva e Silva[a], Markus Endler[c]

[a] Federal University of Maranhão, São Luís, MA, Brazil
[b] Federal Institute of Maranhão, MA, Brazil
[c] Pontifícia Universidade Católica do Rio de Janeiro, RJ, Brazil

ARTICLE INFO

Article history:
Received 26 April 2016
Revised 9 September 2016
Accepted 5 April 2017
Available online 6 April 2017

Keywords:
Mobile social networks
Context-dependent privacy
Situational computing
Fuzzy logic

ABSTRACT

As On-line Social Networks are nowadays largely used by mobile users and their posts potentially reveal - either explicitly or implicitly - much sensitive information about users, privacy control becomes a fundamental issue in such Mobile Social Networks (MSNs). In this paper we advocate that situational computing is the key ingredient for the development of effective mechanisms for privacy control in MSNs. We first describe an on-line survey carried out in order to understand the user's requirements regarding privacy when using MSNs. The results suggest that users have dynamic and context-dependent privacy requirements and also pinpoints which types of context data are more relevant for the decision about the user's willingness to share MSN content. Based on these findings, we propose *SelPri*, a solution developed as a proof of concept in form of an Android mobile social application that is integrated with Facebook. *SelPri* employs Fuzzy Logic to autonomously and dynamically adapt privacy settings of posts in MSNs according to the user's current situation, freeing the user from the hassle of the manual configuration of the privacy settings whenever his/her situation changes. We also describe conducted evaluations of the user experience in using *SelPri* to assess its accuracy to identify user situations, and its usability and effectiveness in meeting the user's dynamic and contextual privacy requirements.

1. Introduction

Nowadays, many On-line Social Networks (OSNs) can be considered Mobile Social Networks (MSNs) [1], in that mobile devices are the primary means of network access and several types of information about the user's context have gained almost same importance as user generated content *per se*. In these MSNs, mobile users are able to share not only content explicitly generated by them but also data and information that is automatically obtained - or inferred - from embedded sensors in mobile devices. Context information and user content are then combined and used for discovering new friends and acquaintances, and establishing and maintaining their social relationships. For example, in several popular MSNs, the user's current position is collected at the mobile device and sent to the service provider, either in response to an explicit user action (e.g., a check-in), or automatically attached as meta-information to user content (e.g., a message post). To exemplify the popularity of MSNs, Facebook currently (June 30, 2016) has around 1.71 billion monthly active users and, among them, 1.57 billion are using services through mobile devices,[1] more than 1/5 of the world population.

An important aspect to be taken into consideration in the design, implementation, and use of such MSNs are privacy issues [2]. Privacy is a fundamental human right, however, in many ways it conflicts with the human necessity of expanding socialization, including the use of MSNs [3]. This use entails a potential conflict between the disclosure of user content (and context information) for the benefit of socialization, on the one hand, and privacy mechanisms to control who can gain access to information, on the other hand. For example, in order to keep alive his/her connections in the OSN, it is expected that a user will frequently add new posts with some personal information, expressing opinions or emotions [4], or just a recent picture of himself/herself or a visited place. Most media content posted in MSNs (e.g., photos, videos and textual messages) are normally much related to the user's daily activities, events and his/her social interactions. This content combined with context information, such as the current time and place of the posting, may reveal much information about the

* Corresponding author. Address (in Portuguese language): Universidade Federal do Maranhão, Programa de Pós-graduacão em Engenharia de Eletricidade. Cidade Universit aria, CEP: 65080-040, São Lus, Maranhão, Brasil.
E-mail addresses: ariel@lsdi.ufma.br, arielsoaresteles@gmail.com (A.S. Teles), fssilva@lsdi.ufma.br (F.J.d. Silva e Silva), endler@inf.puc-rio.br (M. Endler).

[1] http://newsroom.fb.com/company-info/.

http://dx.doi.org/10.1016/j.comcom.2017.04.003
0140-3664/

user's daily routine, his/her habits, preferences, consumer habits, political orientation and even health problems. Of course, all this information is private data and the user should be able to control who exactly has access to it.

Mechanisms to adjust privacy settings currently supported by almost all MSNs only give means for the user to manually define the individual contacts or groups of contacts that can access each content, and do not effectively control the flow of personal information due to the existence of conflicts between privacy control mechanisms and sociability resources [2,5]. Moreover, the user's privacy requirements (also called privacy desires) are inherent to his/her context [6], i.e., the instant of time, the environment in which he/she is located, or any other information that can be used to characterize the situation of an entity [7]. For example, a photo posted by Maria on a Friday night at a nightclub can reveal something about her personal life that she might not want to share with co-workers. The problem addressed by our work is to meet these context-dependent privacy requirements, which entail the following problems in MSNs:

1. The user may not have a clear understanding of which situations/context are sensitive to disclosure of his/her personal information: some situations can be more sensitive or compromising, then revealing more particular aspects about the user's personal life;
2. The user may not be willing or able to manually configure the privacy settings for each situation/context before each posting. Therefore, it is important to reduce the cognitive effort to analyse his/her current situation and type of posted content, and to choose the appropriate privacy setting;
3. Often the user does not have idea of the impact of disclosing personal and contextual information in MSNs. There is an inconsistency between privacy attitudes (i.e., what users desire in regard to their privacy) and privacy behaviours (i.e., how users behave in regard to their privacy), called "privacy paradox" [8], where they reveal personal information often just for drawing the attention from contacts in the MSN;
4. And finally, the user may not be aware of which bits of context information are silently gathered and shared in the MSN.

This paper describes a study conducted with the objective to investigate the privacy requirements of MSNs users and propose a solution that helps them to cope with the context-dependent privacy control settings in an autonomous and dynamic form. To start with, we performed a user study in order to understand these requirements. We collected data about the user's content posting behaviours related to his/her privacy preferences and which were the main context data that is most relevant for their privacy demands. The results show that user's privacy requirements are dynamic and can be hardly managed by the user manually. The analysis of these results guided us in the development of ***SelPri*** (Self-Privacy), a solution developed as a proof of concept in form of a mobile social application with autonomy to dynamically adapt, according to the user's situation, the privacy settings of posts in MSNs. *SelPri* uses the Situational Computing paradigm [9] by means of an inference engine that uses Fuzzy Logic [10] to identify the user's situation for dynamically adjusting privacy settings to the posted content. The current version of *SelPri* was developed for Android smartphones and it is integrated to the Facebook.

This paper brings the following contributions:

- It performs a user study to understand the users[2] content posting behaviours in MSNs related to the privacy preferences;
- It proposes *SelPri*, a solution to meet those requirements exploring the use of situational computing using fuzzy logic as the basic background;
- It describes *SelPri* evaluations regarding its accuracy to identify situations, usability, and effectiveness in meeting the user's dynamic and contextual privacy requirements.

The rest of this paper is organized as follows. Section 2 gives an overview of the areas of situational computing and fuzzy systems. Section 3 shows and discusses the related work. Section 4 describes the user study and a discussion derived from it. Section 5 presents *SelPri* concepts, while Section 6 exposes its architecture and main implementation issues. Next, Section 7 exhibits a conducted evaluation to assess the accuracy of the inference engine to identify situations, and another to know the user satisfaction regarding *SelPri* usability and privacy. In Section 8 we discuss our work. Finally, in Section 9 we drive our conclusions.

2. Background

2.1. Situational computing

The concept of situation is not straightforward to define and may have multiple meanings [11]. In ubiquitous computing a situation is a finite sequence of actions that have occurred describing human behaviours, application and environmental states [9]. Situation refers to "user activity (or concurrent activities) performed in a specific location for a certain period of time" [12]. Anagnostopoulos et al. [9] consider situation awareness as a particular kind of context awareness [7], where situation is viewed as a collection of context data that are logically aggregated. Therefore, situation awareness is not restricted to the use of isolated pieces of context data, but related to combining the relevant context data to correctly identify the user situation [13]. The situational computing paradigm refers to the application of situation awareness in an ubiquitous computing environment, in which a situation-aware application has the ability to interact with the user, learn from the user, and autonomously adapt to the user's current situational context [9].

Situation identification techniques abstract low level context data into more meaningful high level contexts. Many solutions to identify situations from context data in ubiquitous environments have been developed and proposed in the literature. According to Ye et al. [14], they can be classified in: (1) specification-based techniques, which consist of defining specifications that represent knowledge in logic rules and apply reasoning engines to infer situations from inputs – some examples of this technique are Logic Programming, Ontologies and Fuzzy Logic; and (2) learning-based techniques that use machine learning and data mining to explore association relations between sensor data and situations of interest – ranging from the Bayesian Networks and Decision Trees, to Neural Networks and Support Vector Machines. Learning-based techniques are better used in scenarios where it is difficult to define specifications of situations from a large number of noisy sensor data.

2.2. Fuzzy systems

Fuzzy sets are characterized by membership functions that attempt to describe vagueness and ambiguity, which assign to each element in a universe of discourse (or a domain) a degree of membership (i.e., a truth value) ranging from zero (i.e., full exclusion) to one (i.e., full belongingness) [15]. A fuzzy set contains elements that have varying degrees of membership and, because membership values need not to be complete (i.e., not to be one), can also be members of other fuzzy sets on the same universe with different degree of membership. Linguistic variables has values that are

[2] The terms "participant" and "subject" are also used in this text to denote individuals who participated in the conducted studies.