Computer Communications 76 (2016) 12–25

Contents lists available at ScienceDirect

Computer Communications

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

Privacy-driven access control in social networks by means of automatic semantic annotation

Malik Imran-Daud*, David Sánchez, Alexandre Viejo

UNESCO Chair in Data Privacy, Department of Computer Science and Mathematics, Universitat Rovira i Virgili, Avda. Països Catalans, 26, 43007 Tarragona, Spain

ARTICLE INFO

Article history:
Received 24 November 2014
Revised 1 January 2016
Accepted 3 January 2016
Available online 8 January 2016

Keywords:
Social networks
Access control
Semantic annotation
Privacy

ABSTRACT

In online social networks (OSN), users quite usually disclose sensitive information about themselves by publishing messages. At the same time, they are (in many cases) unable to properly manage the access to this sensitive information due to the following issues: (i) the rigidness of the access control mechanism implemented by the OSN, and (ii) many users lack of technical knowledge about data privacy and access control. To tackle these limitations, in this paper, we propose a dynamic, transparent and privacy-driven access control mechanism for textual messages published in OSNs. The notion of privacy-driven is achieved by analyzing the semantics of the messages to be published and, according to that, assessing the degree of sensitiveness of their contents. For this purpose, the proposed system relies on an automatic semantic annotation mechanism that, by using knowledge bases and linguistic tools, is able to associate a meaning to the information to be published. By means of this annotation, our mechanism automatically detects the information that is sensitive according to the privacy requirements of the publisher of data, with regard to the type of reader that may access such data. Finally, our access control mechanism automatically creates sanitized versions of the users' publications according to the type of reader that accesses them. As a result, our proposal, which can be integrated in already existing social networks, provides an automatic, seamless and content-driven protection of user publications, which are coherent with her privacy requirements and the type of readers that access them. Complementary to the system design, we also discuss the feasibility of the system by illustrating it through a real example and evaluate its accuracy and effectiveness over standard approaches.

1. Introduction

Online social networks (OSN) such as Twitter, Facebook, Google+, Myspace, etc., are platforms where people interact with each other by publishing messages. In these platforms, users can build their own social circles of friends and join social groups or communities. In these groups and communities, strangers may connect with each other according to their common interests, views or activities [1]. In social networks, users spend most of their time in publishing or accessing information about such activities. Very frequently, the published content may contain sensitive data such as date of birth, political views, religious views, medical-related information or others.

Publicly shared content containing that sensitive information can be easily revealed by means of messages, profile data or social apps (like games). This data may portray a person's social or inner life [2], which constitutes a serious privacy issue. Social networks such as Facebook[1] and Twitter[2] consider trusted and non-trusted users as friends [3], but the trust of such friends cannot be measured [1]. As a result, sensitive information may be revealed to non-trusted users. Moreover, Johnson's analysis [4] concludes that the majority of users are more concerned with internal threats of privacy (i.e., from friends) rather than strangers. For this reason, most of the OSN friends are considered untrustworthy to share sensitive information. On the other hand, according to the *European Union Agency for Fundamental Rights & Council of Europe* [5], this sensitive information needs to be protected from untrusted third parties, because it can be exploited by such parties for their own benefit [6].

In the last few years, OSNs (such as Facebook) introduced some measures to improve users' privacy by implementing access control features. In order to incorporate such access control, the user

* Corresponding author. Tel.: +34 977 558270; fax: +34 977 559710.
E-mail address: malikimran.daud@urv.cat, imrandaud@gmail.com (M. Imran-Daud).

[1] http://www.facebook.com
[2] https://twitter.com/

http://dx.doi.org/10.1016/j.comcom.2016.01.001
0140-3664/

profile is broken down into small customizable elements [7]. In order to manage the access to related resources, the information can be classified as “public”, “private”, “friend” or “friend of friend” [8]. According to Aïmeur et al. [7], these features are unreliable or fail to provide desirable results, because they are not fully understood [9] or it is difficult for the users to manage them correctly [4]. Furthermore, while configuring privacy settings, users need to perform a tedious job of defining policies for each user, type of resource and to classify those resources.

In order to overcome these shortcomings, the scientific community has proposed some access control solutions (Masoumzadeh et al. [10] & Carminati et al. [11, 12]) that take into consideration the type of resources to be protected (e.g., photos, videos, wall messages, etc.) before allowing/rejecting an access request. These methods rely on ad-hoc structures (i.e., application ontologies) that provide a preliminary modeling of the resources. In order to manage the access control, the users or the OSN administrators need to define access control rules for each resource type. The proposed solutions bear some limitations. On one hand, the classification of resources is coarse grained, fixed and rigid. Similarly, access control policies are applied as a whole on the object or resource, regardless of their actual contents or sensitiveness. As a result, the access to the resource is binary, that is, complete access or complete restriction. For example, if a user declares *WallMessages* as private for a special group of friends, all the published messages will be hidden from that category of friends, regardless the messages contain any sensitive information or not. Furthermore, it is usually difficult for the users to configure the access control policies, since they may not be familiar with such notations and privacy issues.

In order to address the limitations introduced above, in this paper, we present a new scheme to enforce access control over resources published in social networks. We next summarize the main contributions of our work:

- We propose a transparent, dynamic and privacy-driven access control mechanism. Privacy is ensured by automatically protecting the content of messages to be published according to the privacy requirements of the publishers. The privacy requirements are defined by stating the type of information and the level of detail that is allowed to be accessed by each type of publisher’s contact within the OSN. Contrary to access control policies defined over specific resources, such requirements are only defined once in a generic way and can be intuitively stated. Moreover, the user does not need to have a priori privacy notions.
- Contrary to related works, the privacy assessment is performed by semantically analyzing the contents to be published in an automatic way. Moreover, instead of evaluating the privacy for a resource (e.g., a publication) as a whole, our approach examines the privacy risk of each part of the resource individually (i.e., each textual term in a message).
- The semantics that drive the privacy assessment are gathered by means of an automatic semantic annotation process, which relies on available knowledge bases (i.e., DBPedia[3]) and several linguistic tools.
- In contrast to the binary access control policies proposed by other researchers (which just completely allow or deny the access to a resource), our access control enforcement provides each type of reader with a sanitized version of the original publication that is coherent with the privacy requirements specified by the publisher for that type of reader. The different sanitized versions are semantically coherent with regard to the original publication, and are created automatically according to the semantic annotation process and the privacy risk assessment.

The rest of this paper is organized as follows. In Section 2 we review the available literature on this topic. In Section 3 we present our access control mechanism and give a detailed description of its different components and how potential policy conflicts are managed. Section 4 illustrates the feasibility of the proposal through a real example. In Section 5 we evaluate the system, under the perspectives of feasibility, scalability and accuracy of the privacy protection. Finally, in Section 6 we provide some conclusions and present some lines of future work.

2. Related work

As introduced in the introduction, OSNs incorporate limited access control features in order to manage sensitive publications. More specifically, Facebook incorporates an option to split a list of friends into different categories, which are family friends, close friends, OSN groups or within the customized list of friends [4]. As a result, a user can specify the allowed categories before sharing her publications. However, such efforts are not practical enough because of the following reasons: (i) the burden of configuring this access control for each publication, which requires knowledge about the privacy risks inherent to the publications and (ii) the lack of flexibility of the system, because it is either granted or forbidden access to each publication. In fact, according to the survey conducted by Liu et al. [13], only a 37% of the users are satisfied with this kind of privacy settings.

Researchers have also contributed to enhance the privacy of the users in OSNs. As a result, Carminati et al. [11, 12] categorized users and resources in an ad-hoc ontology in order to annotate OSN-related publications and modeled their relationships. In both schemes, the access control is enforced according to the relationships modeled in the ontology, and it is based on the trust level, type and depth of the relationships within users. Similarly, in Masoumzadeh et al. [10], the authors proposed a social network ontology to categorize different types of resources (e.g., photos, messages, etc.). Moreover, an access control ontology was also proposed in order to model the access control policy rules. In other related schemes, Pang et al. [14, 15] modeled users, their social relationships and their publically shared information (e.g., profile data and their publications) within different graphs. In this scheme, the access control is managed by means of policies that contain constraints and access rules for target users on the content that is publically shared by the owner. Access control is thus enforced by following the interrelationships of the users and their shared content within the graphs, and access decisions are taken according to rules defined in the policy. The solutions proposed by these authors have some common limitations. They are not flexible to modifications in the ontology, profiles or other contents, because they should undergo with a lot of manual changes in the ontology and also in the annotation of resources. Moreover, there is no mechanism defined to evaluate the sensitiveness of the resources, which leads the system to provide a coarse grained access. Therefore, the access to the resource is binary, that is, complete access or complete restriction. Besides, a lot of manual management by the users and the social network administrator is required in order to configure policies for each type of resource.

In another scheme, Cheng et al. [8] proposed a relational access control model, which is based on the concept of user to user and user to resource-based relationships. They proposed a regular expression-based language in order to specify access control policy rules. Moreover, they developed a path checking algorithm to determine relationships among the users and the resources from a social graph. In this solution, access is granted based on the

[3] http://dbpedia.org/About