Available online at www.sciencedirect.com

ScienceDirect

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

ELSEVIER

Computers & Security

A new access control scheme for Facebook-style social networks[☆]

Jun Pang [a,b,*], Yang Zhang [a]

[a] University of Luxembourg, Faculty of Sciences, Technology and Communication, 6, rue Coudenhove-Kalergi, L-1359, Luxembourg
[b] University of Luxembourg, Interdisciplinary Centre for Security, Reliability and Trust, 4, rue Alphonse Weicker, L-2721, Luxembourg

ARTICLE INFO

Article history:
Received 2 February 2015
Received in revised form
22 April 2015
Accepted 27 April 2015
Available online xxx

Keywords:
Social networks
Access control
Privacy
Hybrid logic

ABSTRACT

The popularity of online social networks (OSNs) makes the protection of users' private information an important but scientifically challenging problem. In the literature, relationship-based access control schemes have been proposed to address this problem. However, with the dynamic developments of OSNs, we identify new access control requirements which cannot be fully captured by the current schemes. In this paper, we focus on public information in OSNs and treat it as a new dimension which users can use to regulate access to their resources. We define a new OSN model containing users and their relationships as well as public information. Based on this model, we introduce a variant of hybrid logic for formulating access control policies. We exploit a type of category information and relationship hierarchy to further extend our logic for its usage in practice. In the end, we propose a few solutions to address the problem of information reliability in OSNs, and formally model collaborative access control in our access control scheme.

1. Introduction

Online social networks (OSNs) are among the most popular web services during the past ten years and have attracted a huge amount of users all over the world. For example, Facebook, the leading OSN service, has more than one billion active users monthly.[1] OSNs are playing an important role in our daily life by providing a platform for users to present themselves, articulate their social circles, interact with each other etc.

With the large amount of data maintained in OSN websites, privacy concerning users' personal information inevitably becomes an important but scientifically challenging problem. Access control schemes (e.g., see Sandhu, 1993; Sandhu et al., 1996; Abadi, 2003; Abadi and Fournet, 2003; Li et al., 2005; Byun et al., 2005; Rasmussen et al., 2009; Liu et al., 2012) are naturally introduced to protect users' private information or resources in OSNs. They can be used to guarantee that resources are only accessible by the intended users, but not by other (possibly malicious) users. Users can control

[☆] This article is a revised and extended version of Pang and Zhang (2014) that has appeared in the proceedings of the 9th IEEE Conference on Availability, Reliability and Security (ARES 2014).

[*] *Corresponding author*. University of Luxembourg, Faculty of Sciences, Technology and Communication 6, rue Coudenhove-Kalergi, L-1359 Luxembourg. Tel.: +352 466 644 55625; fax: +352 466 644 35625.
E-mail address: jun.pang@uni.lu (J. Pang).

[1] http://newsroom.fb.com/.

http://dx.doi.org/10.1016/j.cose.2015.04.013

the access to their own information or resources with access control schemes supplied by OSNs. The existing schemes, including the ones proposed by the research community, are mainly *relationship-based*, i.e., whether a user is able to access the information depends on the relationship between him and the owner, e.g., 'friends' or 'friends of friends'.

Due to their own nature and the development of information and communications technology, OSNs admit quick and dynamic evolutions. Many new services and methods for user interaction have emerged. For instance, users can play online games with friends or find people who share similar interests. More recently, with the increased popularity of GPS-enabled mobile devices, OSNs have evolved into geo-social networks – users can tag posts and photos with their geographical locations, find nearby friends and post check-in of some places to share their comments. OSNs are also emerging as important social media – people use OSNs to publish news, organize events or even seek for emergent help. For example, Facebook and Twitter play an extremely important role during the rescue process for the "April 2011 Fukushima earthquake"; and in summer 2014, the "Ice Bucket Challenge" have achieved a huge success through social media.[2] (In Section 3, we will take Facebook as a typical example and discuss its developments in the past few years.)

With these evolutions, more information and activities of users are made available in OSNs. As a result, new access control schemes are needed to capture these new developments. Let us illustrate this need by a few scenarios in OSNs.

- Someone broke the window of Alice's expensive car and took her purse when she parked the car in the area of Montparnasse in Paris. Alice publishes a status in the OSN to see if anyone can provide her some clue to find the purse back. She doesn't want everyone to know that she has an expensive car, and people who live in other areas or cities won't be able to give her any useful information. Therefore, she intends to choose people who live in the Montparnasse area as audiences of her status.
- Bob wants to organize a fundraising party for children's rare diseases. He doesn't want to make this event public as certain sensitive information of the participants can be leaked, e.g., it is possible that some participants' family members may suffer from the disease. Instead, Bob only wants people who are linked with a certain number of charities (through donations, volunteering, etc) as him to attend the party.
- Charlie has some friends who work at the rival company of his own employer. These friends invited him to attend the party organized by their company. Charlie publishes a photo taken at the party. Apparently, it is not a good idea for his colleagues and boss to see this photo. Thus Charlie wants no one but his friends who work at this rival company to see it.

In relationship-based schemes, a resource owner cannot exploit any other information but user relationships between him and the requester when defining access control policies. Therefore, the above requirements cannot be fully and precisely formulated in the current schemes proposed in the literature.

Contributions and Outline. In order to solve the identified problems, we propose a new access control scheme for OSNs. We focus on public information existing, e.g., in Facebook (Section 3), and show that it can be used to group users based on their attributes, common interests and activities. Public information can thus be considered as a new dimension for users to regulate access to their resources. As a consequence, we propose a new OSN model containing both a user graph and a public information graph (Section 4). We then extend a hybrid logic (Bruns et al., 2012) to express this type of access control policies (Section 5). The expressiveness of our scheme is extensively discussed through a number of real-life scenarios (Section 6). We further identify two special semantic relations, i.e., *category relation* among public information and *relationship hierarchy*, which allow us to express certain types of policies in a concise way (Section 7 and Section 8). To address the problem of information reliability in OSNs, we propose to add endorsement and trust into our policy formulas (Section 9). In addition, we formally model the collaborative access control in Section 10 within our new access control scheme.

After the introduction, we give a brief overview of related work in Section 2. Section 11 compares our access control scheme with existing schemes in the literature. We discuss several issues related to our scheme in Section 12 and conclude our paper with some future work in Section 13.

2. Related work

Relationship-based access control, driven by OSNs, was first advocated in Gates (2007) and defined as an access control paradigm based on interpersonal relationships. Carminati et al. proposed the first relationship-based access control model in Carminati et al. (2009a), where the relationships between the qualified requester and the owner are interpreted into three aspects, i.e., relationship type, depth and trust level. In Carminati et al. (2009b), the authors used semantic web technology including OWL and SWRL to extend the model of Carminati et al. (2009a). They also proposed administrative and filtering policies which can be used for collaborative and supervising access control, respectively. Fong et al. proposed an access control scheme for Facebook-style social networks (Fong et al., 2009), in which they model the access control procedure as two stages. In the first stage, the requester has to find the owner of the target resource; then in the second stage, the owner decides whether the authorization is granted or not. Their access control policies are mainly based on the relationships between the requester and the owner. Moreover, they proposed several meaningful access control policies based on the graph structure of OSNs, such as *n*-common friends and clique. In Fong (2011), Fong introduced a modal logic to define access control policies for OSNs. Later Fong and Siahaan (2011) improved the previously proposed logic to further support policies like *n*-common friends and clique. In Bruns et al. (2012), the authors adopted a hybrid logic to describe policies which eliminates an exponential penalty in expressing complex relationships such as *n*-common friends. This hybrid logic is

[2] http://en.wikipedia.org/wiki/Ice_Bucket_Challenge.