Rule-Based Access Control for Social Networks

Barbara Carminati, Elena Ferrari, and Andrea Perego

DICOM, Università degli Studi dell'Insubria, Varese, Italy
{barbara.carminati, elena.ferrari, andrea.perego}@uninsubria.it

Abstract. Web-based social networks (WBSNs) are online communities where participants can establish relationships and share resources across the Web with other users. In recent years, several WBSNs have been adopting Semantic Web technologies, such as FOAF, for representing users' data and relationships, making it possible to enforce information interchange across multiple WBSNs. Despite its advantages in terms of information diffusion, this raised the need of giving content owners more control on the distribution of their resources, which may be accessed by a community far wider than they expected.

In this paper, we present an access control model for WBSNs, where policies are expressed as constraints on the type, depth, and trust level of existing relationships. Relevant features of our model are the use of certificates for granting relationships' authenticity, and the *client-side* enforcement of access control according to a rule-based approach, where a subject requesting to access an object must demonstrate that it has the rights of doing that.

1 Introduction

Web-based social networks (WBSNs) [1] are online communities which allow Web users to publish resources (e.g., blogs) and to establish relationships with other users, possibly of different type ("friend", "colleague", etc.), for purposes which may concern, e.g., entertainment, religion, dating, or business. One of the recent trends in WBSNs is the adoption of Semantic Web technologies, in particular FOAF [2,3], to represent users' personal data and relationships [4]. Thanks to this and to the adoption of decentralized authentication systems such as OpenID [5], it has been made simpler to access and disseminate information across multiple WBSNs. If this has been quite a relevant improvement with respect to the previous situation, it is now necessary that resource owners have more control over information sharing. In fact, differently from 'traditional' social networks, where usually each user knows the others, WBSNs are quite larger, and each node (i.e., user) has direct relationships with only a subgraph of the network. As a consequence, it may be not appropriate to make available any information to all the users of one or more WBSNs. So far, this issue has been addressed by some of the available Social Network Management Systems (SNMSs) by allowing users to state whether a specific information (e.g., personal data and resources) should be public or accessible only by the users with whom the owner of such information has a direct relationship. Such simple access control strategies have the advantage of being straightforward, but, on one hand, they may grant access to non-authorized users, and, on the other hand, they are not flexible enough in denoting authorized users. In

R. Meersman, Z. Tari, P. Herrero et al. (Eds.): OTM Workshops 2006, LNCS 4278, pp. 1734–1744, 2006.

fact, they do not take into account the 'type' of relationship existing between users and, consequently, it is not possible to state that only, say, my "friends" can access a given information. Moreover, they do not allow to grant access to users who have an indirect relationship with the resource owner (e.g., the "friends of my friends").

We think that more sophisticated access control mechanisms can be enforced in the current WBSNs, dealing with such issues. Besides relationships, some other information can be used for this purpose. In fact, the graph of a WBSN allows us to exploit the notion of *depth* of a relationship, which corresponds to the length of the shortest path between two nodes. The depth of a relationship may be a useful parameter, which allows us to control the propagation of access rules in the network. Moreover, in some WBSNs, users can specify how much they trust other users, by assigning them a *trust level*. Such information is currently exploited for purposes which encompass the primary objectives of a WBSN, e.g., as a basis for recommender systems, but it can be used as well to denote the subjects authorized to access a resource in terms of their trustworthiness. Note that the notion of trust applies also to users with an *indirect* relationship—i.e., a relationship with depth greater than 1—, and thus we can combine the usage of depth and trust in access policies.

In this paper, we propose a rule-based access control model for WBSNs, which allows the specification of access rules for online resources where authorized subjects are denoted in terms of the relationship type, depth, and trust level existing between users in the network. To the best of our knowledge, this is the first proposal of an access control model for social networks. The different tasks to be carried out to enforce access control are shared among three distinguished actors—namely, the owner of the requested resource, the subject which requested it, and the SNMS. More precisely, we adopt the approach outlined by Tim Berners-Lee & al. in [6], where access control is enforced client-side, since access to resources is granted if the requestor is able to demonstrate that he/she satisfies given requirements. For this purpose, users' relationships are represented by a specific OWL vocabulary we designed, REL-X [7], whereas access rules are expressed in Notation 3 Logic (N3) [8], and then evaluated by the Cwm reasoner [9] against the existing relationships in order to generate a proof.

The remainder of this paper is organized as follows. Section 2 discusses access control requirements of social networks. Section 3 summarizes the main features of our approach, whereas Sect. 4 illustrates the proposed access control model. Then, Sect. 5 describes the system architecture of the prototype being implemented. Moreover, a running example of how access control is enforced is provided in Sect. 6. Finally, Sect. 7 concludes the paper and outlines future research directions.

2 Access Control in Web-Based Social Networks

In this section, we discuss which are the basic requirements that an access control mechanism for WBSNs should satisfy. However, before discussing access control issues in social networks, we need to briefly introduce what a social network is and how we represent it.