IGI PUBLISHING **ITJ 4752**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Information Security and Privacy, Volume 2, Issue 4
edited by **Hamid R. Nemati © 2008, IGI Global**

A Decentralized Security Framework for Web-Based Social Networks

Barbara Carminati, Università degli Studi dell'Insubria, Italy

Elena Ferrari, Università degli Studi dell'Insubria, Italy

Andrea Perego, Università degli Studi dell'Insubria, Italy

ABSTRACT

The wide diffusion and usage of social networking Web sites in the last years have made publicly available a huge amount of possible sensitive information, which can be used by third-parties with purposes different from the ones of the owners of such information. Currently, this issue has been addressed by enforcing into Web-based Social Networks (WBSNs) very simple protection mechanisms, or by using anonymization techniques, thanks to which it is possible to hide the identity of WBSN members while performing analysis on social network data. However, we believe that further solutions are needed, to allow WBSN members themselves to decide who can access their personal information and resources. To cope with this issue, in this article we illustrate a decentralized security framework for WBSNs, which provide both access control and privacy protection mechanisms. In our system, WBSN members can denote who is authorized to access the resources they publish and the relationships they participate in, in terms of the type, depth, and trust level of the relationships existing between members of a WBSN. Cryptographic techniques are then used to provide a controlled sharing of resources while preserving relationship privacy.

Keywords: *Access control; Data security; Digital Segnature; Encryption; Internet Privacy; Internet Trust; Social Networks*

INTRODUCTION

The last few years have seen an increasing diffusion of social networking Web sites (Staab, Domingos, Mika, Golbeck, Ding, Finin et al., 2005), where users can establish relationships and share resources, opinions, and contacts for a variety of purposes (recreational, work, dating, etc.). As a result, today Web-based Social Networks (WBSNs) make publicly available a huge amount of possibly sensitive and private information, which may be used with purposes different from what was intended by the users who released it. As a matter of fact, such information is regularly exploited not only by companies for marketing purposes, but also by governments and institutions (such as colleges),

in order to track the behaviors/opinions of specific persons, and, in the worst case, by online predators (Barnes, 2006). In addition, Semantic Web technologies, such as FOAF and other RDF-based vocabularies (Brickley & Miller, 2005; Davis & Vitiello Jr., 2005; Golbeck, 2004) are currently widely used in WBSNs for publishing personal profiles, relationships, and trust levels (Ding, Zhou, Finin, & Joshi, 2005), thus making easier to access users' data across multiple WBSNs.

In order to deal with these issues, most of today WBSNs allow a user to specify whether a given information must be public or accessible only by the users with whom he/she has a direct relationship. Such simple access control paradigm has the advantage of being straightforward and easy to be implemented, but it suffers from several drawbacks. On the one hand, it may either grant access to non-authorized users or limit too much information sharing, and, on the other hand, it is not flexible enough to express the heterogeneous access control requirements that different WBSN users may have. For instance, such access control paradigm does not take into account the 'type' of the relationships existing among users. Consequently, it is not possible to state access control policies such as "only my friends or my colleagues can access a given piece of information.

We believe that more sophisticated and flexible mechanisms are therefore required, thanks to which WBSN members can denote which users can access the information they publish. A straightforward solution to this issue is to allow a resource owner to explicitly list the set of WBSN members authorized to access a given resource. This could be expressed by traditional access authorizations, which, in their basic form, are tuples $\langle s, p, o \rangle$, where s is the subject authorized to access object o under privilege p (Bertino & Sandhu, 2005). However, such an approach is not suitable for dynamic and distributed environments as WBSNs are, since a member may be required to update the authorizations applying to his/her resources whenever he/she knows new members or if old relationships he/she has with other members have been revoked. In such a scenario, it is preferable to *intensionally* denote authorized members by specifying the *requirements* they must satisfy to access a given resource. According to this approach, whenever any modification to the state of the WBSN structure occurs, the set of authorized members will dynamically change, without the need of modifying the existing authorizations.

So far, a variety of access control models have been proposed which denote authorized users in terms of their characteristics, and not only by their identities. The role-based model—for example, Ferraiolo, Kuhn, and Chandramouli (2003)—is the most popular one; others are those based on credentials—for example, Agarwal, Sprick, and Wortmann (2004); Winslett, Ching, Jones, and Slepchin (1997)—or certificates—for example, Palomar, Estevez-Tapiador, Hernandez-Castro, and Ribagorda (2006); Thompson, Johnston, Mudumbai, Hoo, Jackson, & Essiari (1999). A similar approach can be applied to WBSNs. In fact, WBSN members usually publish resources having in mind a specific audience consisting, for example, of their friends or colleagues. In other words, in a WBSN context, *relationships* can be used as a basis for specifying authorizations, such as "only my friends can access this resource" or "only WBSN members who are both friends and colleagues of mine can access this resource." Based on such considerations, in (Carminati, Ferrari, & Perego, 2006) we proposed an access control model for WBSNs, where authorizations are specified in terms of the *type*, maximum *depth*, and minimum *trust level* of a relationship. As far as access control enforcement is concerned, we have adopted the *client-side* approach outlined by Weitzner, Hendler, Berners-Lee, and Connolly (2006), where access to resources is granted if the requestor is able to demonstrate that he/she satisfies the requirements stated by the specified access rules, that is, he/she is able to demonstrate to have the relationships required by the authorizations.

However, when client-side access control is adopted, attention should be paid to the fact