

Chapter 21

Access Control Models for Online Social Networks

Rula Sayaf
KU Leuven, Belgium

Dave Clarke
KU Leuven, Belgium

ABSTRACT

Access control is one of the crucial aspects in information systems security. Authorizing access to resources is a fundamental process to limit potential privacy violations and protect users. The nature of personal data in online social networks (OSNs) requires a high-level of security and privacy protection. Recently, OSN-specific access control models (ACMs) have been proposed to address the particular structure, functionality and the underlying privacy issues of OSNs. In this survey chapter, the essential aspects of access control and review the fundamental classical ACMs are introduced. The specific OSNs features and review the main categories of OSN-specific ACMs are highlighted. Within each category, the most prominent ACMs and their underlying mechanisms that contribute enhancing privacy of OSNs are surveyed. Toward the end, more advanced issues of access control in OSNs are discussed. Throughout the discussion, different models and highlight open problems are contrasted. Based on these problems, the chapter is concluded by proposing requirements for future ACMs.

INTRODUCTION

Online social networks (OSNs) are social networks that are established through web-based services through which people can foster social relationships. Sites such as LinkedIn, Facebook, Google+, MySpace, etc. are therefore type of OSNs (Hafez Ninggal & Abawajy, 2011), but also blogging services, peer-to-peer, collaborative and content sharing sites such as Youtube and Flickr, and

social bookmarking services such as CiteULike are also types of OSNs.

Users of OSNs create their own social spaces and upload different types of personal data such as photos, videos, texts, etc. OSNs facilitate easy social interaction by allowing users to establish relationships and connect to other users, who may be friends in the offline world or strangers.

One of the fundamental features of OSNs is the ability to share personal data with others in a

relatively privacy-preserving manner. The recent surge of interest in OSNs has been coupled with serious privacy and security concerns, primarily caused by the lack of proper data protection means (Cutillo, Molva, & Strufe, 2009). For instance, users' privacy concerns have affected the popularity of MySpace. Studies have showed that due to lack of privacy control on MySpace, users have abandoned this OSN (Baracaldo, López, Anwar, & Lewis, 2011) and have migrated to other OSNs for their better privacy-preserving means.

Access control mechanisms are employed in OSNs to enable users to control the dissemination of their own data and protect their privacy accordingly (Abiteboul et al., 2005). Other approaches are employed to protect rights and ownership of data, such as digital rights management (Rodriguez, Rodriguez, Carreras, & Delgado, 2009), which we will review later, and watermarking of individual data (Bedi, Wadhai, Sugandhi, & Mirajkar, 2005). Both these approaches and access control models are intended to improve privacy preservation of OSN users.

However, there are many underlying problems in access control mechanisms used in current OSNs. First, only a small percentage of users change the default access control settings to define their own access control policies (Gross & Acquisti, 2005). Second, when these access control mechanisms are used they fail to address the required fine-grained control to avoid privacy violations (Masoumzadeh & Joshi, 2010). The sensitive personal data in OSNs requires a high-level of protection by means of appropriate access control (Gates, 2007). An inherent challenge is how to define an appropriate ACM to regulate access to OSNs' users' data. ACMs should offer a fine-grained control that captures the specific structure and features of an OSN. Mostly, data dissemination is based on relationships represented in the OSN. Therefore, simple access control lists (Cankaya, 2011) and even more advanced classical ACMs

fail to satisfy access control requirements of OSN, as they are not based on the specific properties of social relationships.

Recently, various ACMs have been specifically proposed to address OSN privacy-protection requirements. In this chapter we focus on OSN-specific problems and requirements and how those are tackled by different ACMs.

BACKGROUND AND PRELIMINARY NOTIONS

Online Social Networks

A *social network* (SN) is a set of people connected to each other by social relationships. *Offline Social Networks* refer to real-world social communities. *Online Social Networks* (OSNs) are web-based services that offer the functionality of creating a personal representation of one's self through which one can socialize with others. A *user* is represented in the OSN via a profile to which personal data can be added. An *owner* is a user who adds her data, referred to as *objects*, and can share them with others.

A main feature of OSNs is the articulation of various types of relationships between profiles to facilitate the social communication with others. The social communication includes various activities such as sharing objects, creating groups, organizing online and offline events, etc.

Users in an OSN and their relationships form a *social graph*. Nodes and links in the graph denote users and relationships, respectively (Carminati, Ferrari, & Perego, 2006b). Each pair of users in the graph is connected via a path of links between them. The distance between two users measures the number of links of the shortest path between the two corresponding nodes. The social graph is commonly utilized as an abstraction of OSNs upon which ACMs are formalized.

32 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/access-control-models-for-online-social-networks/115029

Related Content

Teaching Students about Online Professionalism: Enhancing Student Employability through Social Media

Thomas Lancaster (2014). *Digital Arts and Entertainment: Concepts, Methodologies, Tools, and Applications* (pp. 1153-1174).

www.irma-international.org/chapter/teaching-students-about-online-professionalism/115066

Jungian Reflections on South African Cinema: An Exploration of Cinema and Healing

Chris Broodryk (2016). *Exploring the Collective Unconscious in the Age of Digital Media* (pp. 197-213).

www.irma-international.org/chapter/jungian-reflections-on-south-african-cinema/145266

Asynchronous and Synchronous Learning and Teaching

Nguyen Tien Dung, Pham Chien Thang and Ta Thi Nguyet Trang (2023). *Multidisciplinary Applications of Computer-Mediated Communication* (pp. 1-16).

www.irma-international.org/chapter/asynchronous-and-synchronous-learning-and-teaching/321355

The Influence of Groupthink on Culture and Conflict in Twitter

Godfrey A. Steele and Niekitta Zephyrine (2018). *Reconceptualizing New Media and Intercultural Communication in a Networked Society* (pp. 223-249).

www.irma-international.org/chapter/the-influence-of-groupthink-on-culture-and-conflict-in-twitter/202783

Public Relations and AI

Hakan Irak (2024). *Advancements in Socialized and Digital Media Communications* (pp. 151-162).

www.irma-international.org/chapter/public-relations-and-ai/337946