Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 17 (2013) 14 – 20

Procedia Computer Science

Information Technology and Quantitative Management

(ITQM2013)

Relation Based Access Control in Campus Social Network System

Zhao Du[a,]*, Yuguang Liu[b], Ye Wang[c]

[a] *Information Technology Center, Tsinghua University, 100084 Beijing, China*
[b] *Beijing Educational Network and Information Center, 100875 Beijing, China*
[c] *School of Automation, University of Science and Technology Beijing, 100083 Beijing, China*

Abstract

As one of the most popular network applications, online social network system has gained huge adoption in the past few years. Campus social network system is a special type of social network system which focuses on providing information communication, knowledge sharing, and online collaboration services to campus users in colleges and universities. In this paper, we discuss the design of relation based access control in campus social network system which is decided by the collective efforts system designers, system administrators, and especially users of the system. Generally speaking, relation based access control in campus social network system is defined in terms of users can establish relationships; and they can also assign relation based permissions on information and resources when they release them. It consists of user-centered access control and group-centered access control which deal with access control of information and resources released in users' personal space and groups' shared space respectively. Once a campus social network system is put online, access control in it is actually decided by the collective intelligence of its users. Specifically, it's built upon collective intelligence that is reflected through users' identity, their social relationships and permissions that they set on their profile and created content. In a word, relation based access control in campus social network system adopts a collective intelligence model.

Selection and peer-review under responsibility of the organizers of the 2013 International Conference on Information Technology and Quantitative Management

Keywords: Relation Based Access Control; Campus Social Network System; Collective Intelligence; Web 2.0 Applications; Scenario Analysis

1. Introduction

With the huge adoption that online social network systems have gained in the past few years, they are growing up to be one of the most popular Internet services and considered to be the representative of new generation Internet applications. The primary purpose of online social network systems is to connect users through network by providing online interaction, communication, and collaboration services to them. Although different online social network systems have different goals and usage patterns, the most common model of them is based on the presentation of the participant's profile and the visualization of his/her network of relationships to others [1]. Campus social network system is a special type of social network system which targets campus users in colleges and universities. The focus of it is to provide information communication, knowledge sharing and especially online

* Corresponding author. Tel.: +86-10-62792958 ; fax: +86-10-62784612 .
E-mail address: dz@cic.tsinghua.edu.cn .

Selection and peer-review under responsibility of the organizers of the 2013 International Conference on Information Technology and Quantitative Management
doi:10.1016/j.procs.2013.05.003

collaboration services to them [2]. At the same time, campus social network system also collects, keeps, and uses various kinds of personal and group relationships in the cyberspace of the colleges or universities. The sum of personal and group relationships forms a huge and sophisticated social network which is valuable assets both for individual campus users and for its belonging colleges or universities [3]. Access control to resources and services is an important topic for campus social network system as the same as it is for all computer systems. It is the mechanism by which services know whether to honor or deny requests. Different from access control in traditional computer systems which is determined by the joint efforts of system designers and administrators; access control in campus social network system and other Web 2.0 applications is determined by the collective efforts of system designers, system administrators, and especially users. Since the majority of users in campus social network system are equal, the focus of access control in the system is not to control the web pages or services that users can access, but to control the information and resources that users can access through web pages or services. In other words, users in campus social network system can access similar web pages or services, but they are probably to get largely different information and resources through these web pages or services.

Relation based access control in campus social network system is defined in terms of users can establish relationships; and they can also assign relation based permissions on information and resources when they release them. Once a campus social network system is put online, access control in it is actually decided by the collective intelligence of its users. Specifically, relation based access control in campus social network system is built upon users' identity, their social relationships and permissions that they set on their profile and created content. The core idea of it is the collective intelligence reflected by the elements we mentioned above. In a word, relation based campus social network system adopts a collective intelligence model.

Based on the above considerations, we propose the design of relation based access control in our campus social network system. It is defined in terms of two considerations: users can establish relationships; they can also assign relation based permissions on information and resources when they release them. It consists of two principal parts: user-centered access control and group-centered access control. The former part deals with access control of information released in users' personal space, and the latter part deals with access control of information released in groups' shared space. By this way, relationships become a means for naming many-to-many mapping between users and permissions.

In the following sections, we begin by an introduction and comparison of access control for traditional computer systems and Web 2.0 applications. Then the relationship model of campus social network system and the design of relation based access control in the system are examined in detail. After that, we will make vivid scenario analysis of user-centered access control and group-centered access control to get deeper understanding of relation based access control. Finally, the conclusion of the paper is presented.

2. Access Control for Traditional Computer Systems and Web 2.0 Applications

Access control to resources and services is a classical and important topic for computer systems. It is fundamental and critical to computer systems' security. Since the appearance of computer systems featured by multiple applications and served multiple users in the 1970s, there is heightened awareness of data security issues. Specifically, access control is about how to ensure that only authorized users were given access to certain data or resources [4]. Generally speaking, access control is the mechanism by which services know whether to honor or deny requests. It often consists of four problems: identification, authentication, authorization and access decision [5].

2.1. Access Control for Traditional Computer Systems

Before the emergence and glory of Web 2.0 applications, access control in computer systems is usually determined by the joint efforts of system designers and administrators. System designers decide the access model that computer systems adopt; and system administrators are responsible for the configuration of access rules in computer systems. Typical access control models for the traditional computer systems include Mandatory Access Control (MAC, or Lattice Based Access Control (LBAC)), Discretionary Access Control (DAC), Role Based Access Control (RBAC), Attribute Based Access Control (ABAC), distributed Role Based Access Control (dRBAC), and authoriZation Based Access Control (ZBAC) etc. In these models, MAC and DAC are two most classical ones [6, 7]. RBAC was introduced after MAC and DAC. It is the most famous and widely used access

control model [4, 6, 7, 8]. ABAC deals with fine-grained access control of web services at both the service level and the parameter level in dynamic and distributed environment [9, 10]. dRBAC combines the advantages of RBAC and trust-management systems to create a system that offers both administrative ease and a decentralized, scalable implementation of access control in highly dynamic coalition environments [11]. ZBAC seeks to solve cross domain access control problems in computer systems using Service-Oriented Architecture (SOA) [5, 12]. These models aim to provide solutions to access control problem in different application scenarios. Although they have their own advantages and disadvantages, there is no absolutely best one. Furthermore, they are not necessarily exclusive. Some of them can be combined to realize more suitable access control for practical computer systems.

2.2. Access Control for Web 2.0 Applications

Different from access control in traditional computer systems, access control in Web 2.0 applications is relation based. It is determined by the collective efforts of system designers, system administrators, and especially users. System designers decide the access model that Web 2.0 applications will adopt as they do in traditional computer systems, system administrators are in charge of confirmation or setting of specific attributes of user identify. The responsibility of configuring fine-grained access rules is largely transferred to users. In most cases, once a Web 2.0 application is put online, access control in the system is actually decided by the collective efforts of all users. Since the majority of users of Web 2.0 applications are equal, the focus of access control in the system is to control the information and resources that users can access through web pages or services. That is to say, although users in a Web 2.0 application can access similar web pages or services, they will get different information and resources through these web pages or services.

Relation based access control in Web 2.0 applications is built upon the collective intelligence that is reflected through users' identity, their social relationships and permissions that they set on their profile and created content. Firstly, since Web 2.0 applications target individual users and provides various forms of content creation and sharing services to them, users' identity should still be the basic access control concern as it is in all other access control models. Secondly, most Web 2.0 applications allow users to establish personal relationships with other users and member relationships with groups, and access control in Web 2.0 applications is usually built upon the social relationships of personal relationships and member relationships [13, 14]. Thirdly, users have full rights to decide who can access their contents as they are the owner of contents in Web 2.0 applications. They are allowed to set access rules for their created content in Web 2.0 applications. The access rules may be default rules for all content created by an individual user, or specific rule for an entry in the content created by an individual user.

It's noteworthy that users' identity, their social relationships, and permissions on user profiles and user created contents are all created through the collective behavior of a large amount of users. In a word, relation based access control in Web 2.0 application adopts a collective intelligence model.

3. Relation Based Access Control in Campus Social Network System

As a typical Web 2.0 application, relation based access control in campus social network system adopts a collective intelligence based model which is built upon users' identity, their social relationships and permissions that they set on their profile and created content. Since social relationships of users are the core element of relation based access control model, the relationship model of campus social network system is one of the most important factors of the model. For this reason, we will firstly introduce the social relationship model of campus social network system. After that, we are going to make detail analysis of the relation based access model built upon the social relationship model.

3.1. Relationship Model of Campus Social Network System

Relationship model of campus social network system consists of five types of relationships which can be divided into two categories. The first category contains two types of relationships between users; the second category contains three type of relationship between users and groups. The two types of relationships between users are two-directional confirmed friend relationship and one-directional confirmed follow relationship. Users in campus social network system can further divide their friends and followed users into multiple lists. The three types of relationship

between users and groups include owner relationship, manager relationship and member relationship. It's noteworthy that a relationship between a user and a group can be converted into a set of relationships between the user and all other members of the group. Once a user establishes any relationship with a group, he/she will be connected with the owner, managers, and all existing and future members of the group.

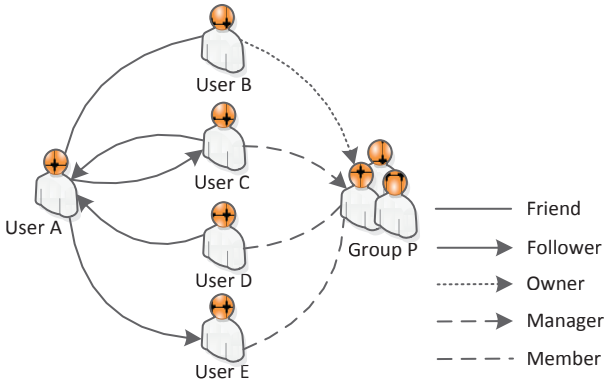

Fig. 1. Relationship Model of Campus Social Network System

As shown in figure 1, there are five connections between users and four connections between users and groups. User A has one friend (user B) and two followers (user C and user D); he is also the follower of two users (user C and user E). Group P has one owner (user B), one manager (user C) and two members (user D and user E).

3.2. Relation Based Access Control in Campus Social Network System

The core responsible of relation based access control in campus social network system is to decide the information that users can access in the system. It is built upon the relationship model of the system. As we have mentioned above, there are two categories of relationships in campus social network system: relationships between users, and relationships between users and groups. Therefore, relation based access control in campus social network system consists of two principal parts: user-centered access control and group-centered access control. The former part deals with access control of information released in users' personal space, the latter part deals with access control of information released in groups' shared space.

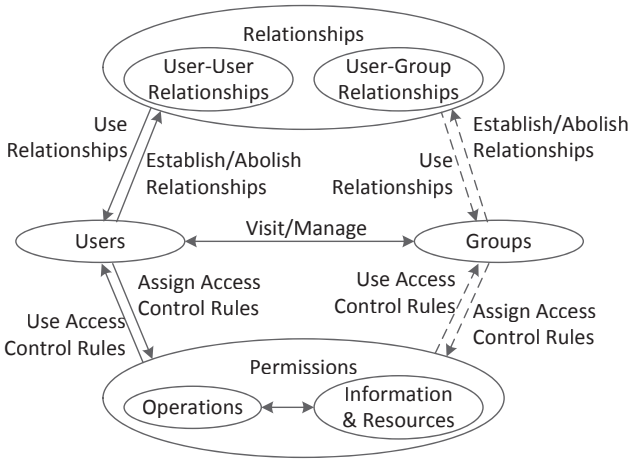

Fig. 2. Relation Based Access Control in Campus Social Network System

As shown in figure 2, relation based access control in campus social network system includes eight basic

elements including users, groups, user-user relationships, user-group relationships, relationships, operations, information and resource, and permissions. "Users" not only refers to human beings including students, faculties, staff members, and alumni who will use campus social network system; but also refers to public accounts in the system which represents various kinds of organizations on campus. "Groups" refers to the shared entity of specific sets of users. There are several types of groups including public groups, private groups, and agency groups in campus social network system. Different types of groups have different attributes on group visibility, membership establishment, and information visibility etc. "Relationships" refers to relationships in the system, it contains "User-User Relationships" between users and "User-Group Relationships" between users and groups. "Permissions" refers to the approval to perform operations on information and resources in the system which is determined by the permissions that their owners have set on them and relationships between owners and visitors of them. "Information and Resources" refers to content created by users. "Operations" on information and resources in the system includes read, write, modify, comment, forward, share, and recommend etc.

4. Scenario Analysis of Access Control in Campus Social Network System

Because relation based access control in campus social network system can be divided into user-centered access control and group-centered access control, we are going to make detailed scenario analysis on the two types of access control respectively. By this way, we are expected to be able to get deeper understanding of relation based access control. It's noteworthy that scenarios of user-centered access control and group-centered access control are similar in the basic procedure.

4.1. Scenario Analysis of User-Centered Access Control

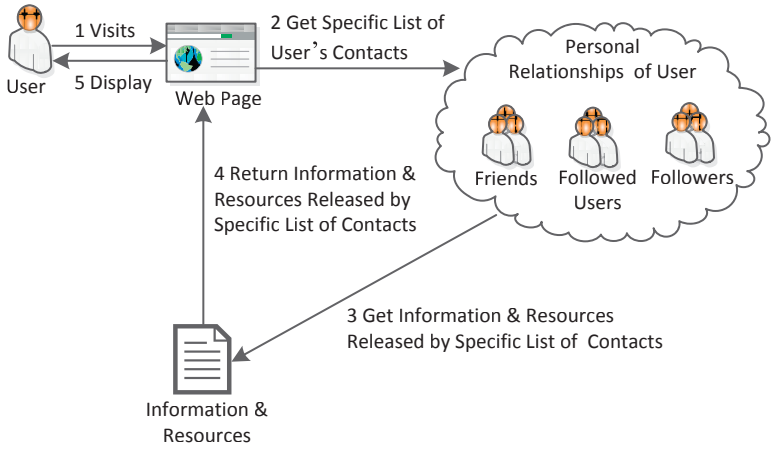

Fig. 3. Typical Scenario of User-Centered Access Control

Figure 3 depicts a typical scenario of user-centered access control. When a user in campus social network system visits a web page for personal services, he/she may want to get information and resources released by his/her contacts in the system. Contacts of users include friends, followed users, and followers. Although different web pages can provide different services, the majority of them need to get a specific list of the user's contacts at the beginning. Then the system will get the information and resources released by the list of contacts. After that, the obtained information and resources together with the list of contacts will be returned to the requested web page. Finally, the requested page is generated and displayed to user.

4.2. Scenario Analysis of Group-Centered Access Control

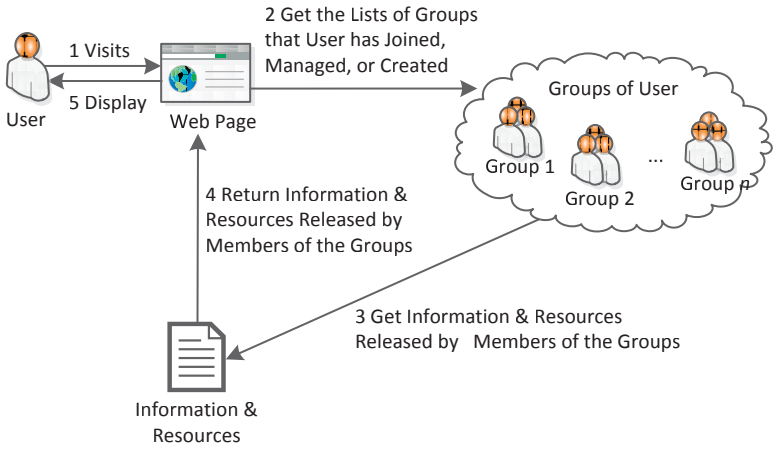

Fig. 4. Typical Scenario of Group-Centered Access Control

Scenarios of group-centered access control are similar to that of user-centered access control. The difference lies in the second and the third step. As shown in figure 4, when a user in the system visits a web page for group services, he/she usually wants to get information and resources released by the members of the groups his/she has joined, managed, or created. Then the system will get the information and resources released in the groups. After that, the obtained information and resources together with the list of groups and their members will be returned to the requested web page. Finally, the requested page is generated and displayed to user.

5. Conclusion

Access control to resources and services is important for campus social network system. It is the mechanism by which services know whether to honor or deny requests. Access control in campus social network system is relation based access control which adopts a collective intelligence model. Relation based access control is decided by the combinational efforts system designers, system administrators, and especially users of the system. The model consists of eight basic elements: users, groups, user-user relationships, user-group relationships, relationships, operations, information and resource, and permissions. It is built upon the relationship model of the system. Specifically, it's decided by collective intelligence reflected though users' identity, their social relationships and permissions that are set on user profile and user-created content. Relation based access control in campus social network system can be divided into user-centered access control and group-centered access control. The analysis of their application scenarios shows that they have similar process procedure.

Acknowledgements

This work is supported by the Beijing Education and Science "Twelfth Five-Year Plan" (No. CJA12134).

References

1. R. Gross and A. Acquisti, "Information Revelation and Privacy in Online Social Networks", Proceedings of the 2005 ACM workshop on Privacy in the electronic society. pp. 71-80, ACM New York, NY, USA, 2005.

2. Z. Du, X. Fu, C. Zhao, T. Liu, Q. Liu, and Q. Liu, "Multi-Domain Cloud Social Network Service Platform Supporting Online Collaboration on Campus", Proceedings of the 2012 2nd IEEE International Conference on Cloud Computing and Intelligent Systems, pp. 365-

369, 2012.

3. N. B. Ellison, C. Steinfield, and C. Lampe, “The Benefits of Facebook “Friends”: Social Capital and College Students' Use of Online Social Network”, Journal of Computer-Mediated Communication, Vol. 12, No. 4, pp. 1143–1168, 2007.

4. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E, “Youman. Role-Based Access Control Models. Computer”, Vol. 29, No. 2, pp: 38-47, 1996.

5. A. H. Karp, “Authorization-Based Access Control for the Services Oriented Architecture”, Proceedings of 2007 Military Communications Conference, pp. 160-167, 2007.

6. R. S. Sandhu and P. Samarati, “Access Control: Principles and Practice”, IEEE Communications Magazine, Vol. 32, No. 9, pp. 40-48, 1993.

7. S. Osborn, R. Sandhu, and Q. Munawer, “Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies”, ACM Transactions on Information and System Security, Vol. 3, No. 2, pp. 85-106, 2000.

8. D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhm, and R. Chandramouli, “Proposed NIST standard for role-based access control”, ACM Transactions on Information and System Security, Vol. 4, No. 3, pp. 224-274, ACM New York, NY, USA, 2001.

9. L. Wang, D. Wijesekera, and S. Jajodia, “A Logic-based Framework for Attribute based Access Control”, Proceedings of the 2004 ACM workshop on Formal methods in security engineering, pp. 45-55, ACM New York, NY, USA, 2004.

10. H. Shen and F. Hong, “An Attribute-Based Access Control Model for Web Services”, Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE Computer Society, pp. 74-79, 2006.

11. E. Freudenthal, T. Pesin, L. Port, E. Keenan, and V. Karamcheti, “dRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments”, Proceedings of 22nd International Conference on Distributed Computing Systems, pp. 411-420, 2002.

12. A. H. Karp, H. Haury, and M. H. Davis, “From ABAC to ZBAC: The Evolution of Access Control Models”, HP Labs Technical Report HPL-2009-30, February 2009.

13. A. Tootoonchian, K. K. Gollu, S. Saroiu, Y. Ganjali, and A. Wolman, “Lockr: Social Access Control for Web 2.0”, Proceedings of the first workshop on Online social networks. pp. 43-48, ACM New York, NY, USA, 2008.

14. F. Giunchiglia, R. Zhang, and B. Crispo, “RelBAC: Relation Based Access Control”, Proceedings of 4th International Conference on Semantics, Knowledge and Grid, pp. 3-11, 2008.