2012 International Conference on Networks and Information (ICNI 2012)
IPCSIT vol. 57 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V57.03

Future Directions in Access Control for Online Social Networks

Adnan Ahmad and Brian Whitworth

Institute of Information and Mathematical Sciences
Massey University, Auckland, New Zealand

Abstract. Access control is the process by which authorized users are granted permission over resources. Access control models incorporate application requirements in their design and thus evolve with the applications. The rise of online social networks (OSN), like Facebook, has posed new requirements over the privacy of users' data due to the presence of heterogeneous privacy circle. The traditional models cannot be used for this new type of applications for the complexity of millions of users interacting with each other. Different access control models for OSN are proposed based on relationships, trust, rule semantics, or history between the user and the requestor, however, rights delegation, rights transfer, reputation management and transparency are still ignored by the research community. To address these concerns and challenges, further research is needed. This paper reviews these challenges and presents a number of future research directions for access control models in the context of OSN.

Keywords: Access control, Delegation, Online Social Networks, Transparency, Trust

1. Introduction

The first access control model was built with the emergence of multi-user computing, when the need arose to restrict the users sharing the same system interfering each other's data [1]. As computing evolved, it not only modifies the object space but also affects the operation types and other requirements of access control system. Due to variations in application design, the access control approach has been modified to work for military, commercial applications, organizational structures, distributed applications, medical data, peer-to-peer networks, and grid environment [2-6].

In the last decade, we have seen extreme multi-user systems emerge – online social networks (OSN) where millions of users share billions of resources on daily basis and manage each other access rights [7]. As access to these resources depend on the number of interactions between the owner and the requestor, the complexity of these systems increases geometrically with size, not linearly. Today, Facebook claims to have more than 900 million active users having 125 billion friend connections, which makes the access combinations quite enormous. The access control system for OSN needs to incorporate the social requirements of the community in its design.

Privacy is one of the social requirements for OSN, as connecting to others raises privacy concerns [8]. People want to contribute personal stuff to these networks without worrying about its unauthorized disclosure or its use in any inappropriate way [10]. Another is Locke's idea that one should own what one creates, whether a book, a painting or an online photo [9]. If so, everything posted on an OSN should be owned, and conversely if people own their posts, they should manage their access. Ownership of newly created online objects is critical to OSN success for social reasons.

Our previous works [10 – 13] discuss how basic rights can be legitimately incorporated in access control. This paper now reviews the challenges and advances in access control for OSN with respect to socio-technical design principals – first define the social requirements then design a technical solution to fulfil them. This ensures that technical design doesn't impede social needs, i.e. it avoids a socio-technical gap. The technical design may also support or enhance social rules and needs [14].

2. Access Control in OSN

Traditional access control models can be categorized into discretionary access control (DAC), mandatory access control (MAC) and role-based access control (RBAC). DAC [2] assume that objects belong to owners who can manage their access, while MAC [2] and RBAC [15] assume a central trusted computing authority to support an organization security policy. As ownership is fundamental in OSN, DAC driven models are the only choice, however system wide groups and their centralized management in DAC don't suit the OSN environment. Some major differences between the access control for traditional applications and OSN are:

Table 1: Differences between the requirements of OSN and traditional access control models

Traditional Systems	Online Social Networks
Access based on role/position in organization	Access based on relationship with the owner
Centralized authorization servers	Distributed authorization servers
System wide global roles	Local roles
System wide centralized administration	Local administration
Rights associated with users/roles	Rights associated with domains/objects
Static policies	Dynamic privacy policies
Homogeneous privacy policies	Heterogeneous privacy policies
Global object visibility	Local visibility
Works with roles	Works with domains

Past OSN security research has mainly focused on statistical analysis techniques while preserving members' privacy [16]. Some relatively new approaches to OSN access management are based on trust and relationships, e.g. D-FOAF (Friend of a Friend) is an ontology based distributed identity management system for OSN that manages access rights in terms of trust level and path length between two users [17]. In another approach, centralized trust management is used to determine the security level of users and resources [18]. A semi-decentralized access control model is presented in [7] where users are categorized in terms of relationship depth and trust level, and dRBAC [4] manages trust in coalition environments by decentralized access control. In general, current access control models for OSN are based on trust [18], history [19], reputation [7] and relationships [20]. Some other models use a combination of one or more of these properties to manage access between users in OSN, e.g., a combination of trust and relationships is explored in [4], relationship, depth and trust are explored in [7], and relationship type, owner administration and local roles are explored in [10].

The models manage the access rights of users quite well in OSN applications, however, the extension of these models to accommodate more sophisticated rights set can be consider as the future of access control. As OSN are built around the social requirement of the community, their access control should incorporate more social rights than traditional applications.

3. Future Research Directions

Some of the identified common regions where the OSN research can be extended are rights delegation, rights transfer, trust mechanisms and object classifications. This section presents some insights about these research directions.

3.1. Delegation

Delegation is a process which allows a user *A* to authorize another user *B* to access resources on his behalf [21]. Delegation is important for any access control model, but currently there is no delegation model for OSN. The delegation models for traditional applications can be categorized into three types, i) machine to machine delegation, where one object acts on the other's behalf [21], ii) user to machine delegation, where objects act on user's behalf [22], and iii) user to user role delegation, where users delegate roles to other users [23].

Delegation model for OSN can work on various design options, a) the delegation can operate on complete or partial set of rights; b) the model may only allow user *A* to delegate rights on the complete set of authorized resources or it may work on particular resource; c) The model may or may not allow user *A* to exercise the delegated right; and d) the model may allow user *B* to further delegate the right to another user; however in all the above cases user *A* may able to revoke the rights from user *B*. These options introduce the potential of designing more than one delegation model but the one based on socio-technical design may suit the nature of OSN application the most. For example, investigating and developing new user to user delegation architectures, which ensure to consider the social requirements of ownership, local administration and relationships will be quite useful. These models will give great control over information and introduce new means of collaboration among users of OSN.

3.2. Rights Transfer

Rights transfer is a process which allows user *A* to permanently give away his rights to another user *B*, who becomes the new owner. Rights transfer for traditional systems is explored in [23, 24], however, there is no access control model for OSN that supports rights transfers. Investigating this area and designing some user to user rights transfer model provides an interesting future research direction in OSN access control.

Rights transfer model for OSN can work on various design options, a) one may transfer the complete or partial set of rights over some resource; b) the model may allow to transfer rights on the complete set of authorized resources or it may work on subset of authorized resources; c) The model should not allow user A exercise the transferred right; and d) the model should allow user B to further transfer the right to another user; however in all the above cases user A may not able to revoke the rights from user B. The transfer model is quite straight forward; the design options only allow working on partial/complete right set and partial/complete resource set, and the choice should be made on socio-technical design, but other options should be kept same for consistency and to make the model recursive.

3.3. Implementation

Another future direction can be the implementation of the proposed delegation and transfer models as a component of security kernel for OSN and include all the proposed options to the users. The implementation can take advantage of web semantic ontologies for its inter-reference qualities and use Google stream as the simulation agent. This simulation and implementation may able to suggest solutions to some of the other interesting debates posed by the current research, e.g. whether centralized or distributed implementation architecture will be more suitable for OSN applications; and whether client or server side management of policy credentials is better for load management in OSN. Also the implementation can be tested against various network attacks to suggest an error resilient approach suitable for OSN. Additionally as the content retrieval for a user is based on their social circle, the implementation may give insights about storing data in more efficient way. The implementation would be an interesting addition to the literature OSN security.

3.4. Reputation Model

Another interesting research direction for access control in OSN is reputation model. The model may able to calculate the reputation of a user in a community by how much trustworthy the community considers the user. The reputation model that rates users in a community can have multiple implications like it can suggest the user to opt for delegation or transfer model based on the reputation of the requestor, or an access control model can be designed that allows access to resources based on the reputation of the user.

The reputation model for delegation/transfer model will determine whether a particular user is trustworthy enough to delegate/transfer him some rights. The model can use some reputation rating system calculated on user's previous transactions. This kind of model will introduce an automatic trust evaluator, which suggest about the allocation model for users of particular trust level. The model should be distributed, dynamic and flexible to suggest the level of delegation/transfer based on the requestor's reputation. However, due to the dynamic nature of OSN and heterogeneous users' policies, designing a reputation model presents an interesting challenge to the researchers.

3.5. Transparency

Another interesting research direction is the introduction of transparency, so users know about what to expect rather than making social errors. In general, transparency is the right to view rights that affect you. Transparency in access control will provide readable error messages for guidance to what users can do, in terms of allowed rights. In social terms, transparency of access control rules both lets users anticipate and avoid social errors and reduces community governance corruption as people see the permissions of others [25]. The goal is that social rights are not only applied but also seen to be applied, as this is critical for trust and synergy.

Some design options for transparency model are: a) the model may generate statements that subject *X* has permission *P* over object *O*; b) before putting any object into a space, the object owner may sign a contract with the space owner that they have such rights over the object and space; c) upon entering any space the model may notify the user that they have such rights over the space and the objects within it. These design options will help in designing a transparency model that translates the possible actions of the security kernel.

3.6. Object privacy classifier

Currently, resources in OSN are managed independently regardless to their disclosure level, but OSN resources can be put into groups, like a photo album, that can then be given a privacy classification, e.g. to let only family view the family photo album. Creating object classes to define privacy levels reduces rights management complexity and increases usability. This phenomenon is current available in coarse form in current OSN. However there exists no object classifier model which can determines the disclosure level of objects based on the contents using some machine learning technique.

The proposed design for that object classifier is as follows: The objects that belong to an object class can be grouped together under some label (default $L1\ (\tau)$), i.e. $O \rightarrow OC_{\tau}$, where τ is the set of all security labels that are used for confidentiality levels. These labels should be hierarchical and may form a lattice under a partial order > such that $L1 > L2$ if and only if $L2 \in L1$.

4. Summary

This paper reviewed a number of research challenges related to the advancement of access control research for OSN. A number of research papers have been explored to identify the key challenges and technical advances in the field. Major differences between access control model for traditional application and OSN are highlighted, and the conclusion was drawn that the access control for OSN is more social and user oriented than traditional and poses interesting challenges due to heterogeneous privacy policies.

Based on the above, future research directions have been provided in the area of rights delegation, rights transfers, implementation of the proposed models, reputation models and object classification for OSN. These advancements can help the research community in better understanding of the domain, and in better and more secure privacy models for users.

5. Acknowledgements

This work has been sponsored by National Science Foundation (NSF), USA, under award number 0968445. “OKES: An open knowledge exchange system to promote meta-disciplinary collaboration based on socio-technical principles”.

6. References

[1] Karp, A. H., Haury, H. and Davis, M. H. (2009), “From ABAC to ZBAC: The Evolution of access control models”, Technical Report HPL-2009-30, HP Labs.

[2] TCSEC, Trusted Computer Security Evaluation Criteria (TCSEC), DOD 5200.28-STD. Department of Defense, 1985.

[3] Ferraiolo, D., and D. R. Kuhn, “Role-Based Access Control,” in Proceedings of the NIST-NSA National (USA) Computer Security Conference, 1992, pp. 554–563.

[4] Freudenthal, E., Pesin, T., Port, L., Keenan, E. and Karamcheti, V., dRBAC: Distributed role-based access control for dynamic coalition environments. In Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS 2002), Jul 2002.

[5] Morchon, O. G. and Wehrle, K "Modular context aware access control for medical sensor networks", SACMAT 2010

[6] Thompson, M., Johnston, W., Mudumbai, S. Hoo, G. Jackson, K. and Essiari, A. Certificate-based access control for widely distributed resources. In Proceedings of the Eighth Usenix Security Symposium, pages 215–228, Aug 1999.

[7] Carminati, B., Ferrari, E. and Perego, A. (2008), "Enforcing access control in web-based social networks" ACM Transactions on Information & System Security.

[8] Simpson, A. "On the need for user-defined fine-grained access control policies for social networking applications". Workshop on Security in Opportunistic and social networks, 2008.

[9] Locke, J. "An essay concerning human understanding". Oxford University Press, 1975.

[10] Ahmad, A. and Whitworth, B. "Distributed Access Control for Social Networks". International conference of information assurance and security, IAS'11, 2011.

[11] A. Ahmad, and B. Whitworth, "Access Control Taxonomy for Social Networks", Proc. International conference of information assurance and security (IAS'11) 2011.

[12] B. Whitworth, A. de Moor, and T. Liu, "Towards a Theory of Online Social Rights", in R. Meersman, Z. Tari, P. Herrero et al. (Eds.): OTM Workshops LNCS 4277, pp. 247 – 256, Springer-Verlag Berlin Heidelberg, 2006.

[13] B. Whitworth, and A. deMoor, "Legitimate by design: Towards trusted virtual community environments". Behaviour & Information Technology Journal, 22:1, p31-51, 2003.

[14] N. V. Patel., "Theory of Deferred Action: Exploring the Boundaries of and Between Socio-Technical Systems Design", Design Principles & Practices 3(4), 285-296, 2009.

[15] [15] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-Based Access Control Models," IEEE Computer 29(2), 1996.

[16] B. Carminati, E. Ferrari, and A. Perego, "Security and privacy in social networks," In Encyclopedia of Information Science and Technology, 2nd Edition, volume VII, pages 3369–3376. IGI Publishing, Sept. 2008.

[17] S. R. Kruk, S. Grzonkowski, H. C. Choi, T. Woroniecki, and A. Gzella, "D-FOAF: Distributed identity management with access rights delegation," In proc. of the 1st Asian Semantic Web Conference (ASWC 2006), pages 140–154. Springer Verlag, 2006.

[18] Ali, B. Villegas, W. and Maheswaran, M. "A trust based approach for protecting user data in social networks," In proc. of conference of the center for advanced Studies on collaborative research (CASCON'07), pages 288–293, 2007.

[19] Fong, P. W. L., Anwar, M., and Zhao, Z., "A Privacy Preservation Model for Facebook-Style Social Network Systems". 14th European Symposium on Research In Computer Security (ESORICS'09), volume 5789 of Lecture Notes in Computer Science, pages 303-320, Saint Malo, France, September 21-23, 2009.

[20] Tapiador, A., Carrera, D. and Salvachúa, J. (2011), "Tie-RBAC: an application of RBAC to Social Networks". Web 2.0 Security and Privacy, Oakland, California.

[21] Varadharajan, V., Allen, P. and Black, S. (1991), "An Analysis of the Proxy Problem in Distributed systems". IEEE Symposium on Research in Security and Privacy. Oakland, CA.

[22] Gasser, M., and McDermott, E. (1990), "An Architecture for practical Delegation in a Distributed System". IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, CA.

[23] Barka, E. and Sandhu, R. A Role-Based Delegation Model and Some Extensions, NISSC 2000.

[24] J. Crampton and H. Khambhammettu. Delegation in role-based access control. International Journal of information Security, 7(2):123–136, April 2008.

[25] J. Kooiman, M. Bavinck, R. Chuenpagdee, R. Mahon, R. Pullin, "Interactive governance and governability: an introduction," The Journal of Transdisciplinary Environmental Studies, 7(1), 2008.