ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Access Control Models for Online Social Networks: A Review

[1] M. Divya Bharathi, [2] M. Anand

[1]PG Student (CSE), Dept. of CSE, Sri Vidya College of Engineering and Technology, Virudhunagar, Tamil Nadu, India

[2] Assistant professor, Dept. of IT, Sri Vidya College of Engineering and Technology, Virudhunagar, Tamil Nadu, India

ABSTRACT: Nowadays, online social networks have gained considerable popularity due to convenient and easy communication, social relationship with individuals with the same characteristics, anonymity, and no need to physical move. One of the most important issues in social networks is the security and privacy of users' shared information. This large amount of personal information need appropriate security setting to be protected from unauthorized access and unwanted disclosure. In this paper existing access control models for social networks were examined, highlighting not only benefits and advantages, but also weaknesses of these models. Also, an evaluation was done against several criteria drawn from these models for assessing them.

KEYWORDS: Access control, Privileges, Social networks, Security models.

1. INTRODUCTION

The spread use of internet made gradually reduction of traditional human relationships. So, these relationships were simulated through an internet-based service, named "social network" which allows individuals to construct a public or semi-public profile and connect with the others using social networks. A social network service is described in [1] as "A Web site that provides a virtual community for people interested in a particular subject or just to "hang out" together. Members create their own online "profile" with biographical data, pictures, likes, dislikes, and any other information they choose to post. They communicate with each other by voice, chat, instant message, video-conference, and blogs, and the service typically provides a way for members to contact friends of other members".

Nowadays, online social networks have gained considerable popularity due to convenient and easy communication, social relationship with individuals with the same characteristics, anonymity, and no need to physical move. More and more people use social networks to share interests and make friends. Also, social networks help users overcome geographical barriers. One of the most important issues in social networks is the security and privacy of users' shared information. These large amounts of personal information need appropriate security setting to be protected from unauthorized access and unwanted disclosure. This information could be misused by any adversary. Also, she can use this information to harm the users.

For the protection of sensitive data existed in online social networks from unauthorized access it is important to ensure that access to these information is allowed only to authorized users. So, there should be access control mechanisms for accessing users' information in online social networks. However, providing fine-grained access control in a distributed online social network is a new and challenging problem and so far, there is not a complete solution for it [1]. In this paper existing access control models of social network are investigated and in addition to their details, benefits and weaknesses of them are highlighted. Access Control Models for social networks are discussed in the following section in a detailed manner.

DOI: 10.15680/IJIRCCE.2015. 0311056

II.ACCESS CONTROL MODELS FOR SOCIAL NETWORKS

R. Baden et al. [2] presented Persona, an OSN where users dictate who may access their information. Persona hides user data with attribute-based encryption (ABE), allowing users to apply fine-grained policies over who may view their data. Persona provides an effective means of creating applications in which users, not the OSN, define policy over access to private data. New cryptographic mechanisms are demonstrated that enhance the general applicability of ABE. It is shown that how Persona provides the functionality of existing online social networks with additional privacy benefits. Implementation of Persona is described that replicates Facebook applications and show that Persona provides acceptable performance when browsing privacy-enhanced web pages, even on mobile devices.

S. Braghin et al. [4] provide a framework that allows users to define highly expressive access policies to their resources in a way that the enforcement does not require the intervention of a (trusted or not) third party. This is made possible by the deployment of a newly defined cryptographic primitives that provides - among other things - efficient access revocation and access policy privacy. Finally, implementation of the framework is provided as a Facebook application, proving the feasibility of the approach.

G. Bruns et al. [5] proposed the paradigm of relationship-based access control to address this issue, and modal logic has been used as a technical foundation. Here that hybrid logic -- a natural and well-established extension of modal logic -- addresses limitations in the ability of modal logic to express certain relationships. A fragment of hybrid logic is identified and is used for expressing relationship-based access-control policies, show that this fragment supports important policy idioms, and demonstrate that it removes an exponential penalty in existing attempts of specifying complex relationships such as "at least three friends".

Improving social network access control systems appears as the first step toward addressing the existing security and privacy concerns related to on-line social networks. To address some of the current limitations, B. Carminati et al. [8] proposed an extensible fine grained access control model based on semantic web tools. In addition, authorization, admin and filtering policies are proposed that depend on trust relationships among various users, and are modeled using OWL and SWRL. Besides describing the model, the architecture of the framework is presented in its support.

B. Carminati et al. [10] presented 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 the 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.

B. Carminati et al. [11] illustrate a decentralized security framework for WBSNs, which provide both access control and privacy protection mechanisms. In the 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.

B. Carminati et al. [12] proposeed an access control mechanism for Web-based social networks, which adopts a rule-based approach for specifying access policies on the resources owned by network participants, and where authorized users are denoted in terms of the type, depth, and trust level of the relationships existing between nodes in the network. Different from traditional access control systems, the mechanism makes use of a semidecentralized architecture, where access control enforcement is carried out client-side. Access to a resource is granted when the requestor is able to demonstrate being authorized to do that by providing a proof. In the article, besides illustrating the main notions on which the access control model relies, all the protocols underlying the system and a performance study of the implemented prototype is presented.

J. Crampton and J. Sellwood [16] recently introduced a variant of relationship-based access control based on the concepts of relationships, paths and principal matching, to which will refer as the RPPM model. In this paper, the RPPM model can be extended to provide support for caching of authorization decisions and enforcement of separation of duty policies. These extensions are natural and powerful. Indeed, caching provides far greater advantages in RPPM than it does in most other access control models and are able to support a wide range of separation of duty policies.

J. Crampton and J. Sellwood [17] developed a formal access control model that makes use of ideas from relationship-based access control and a two-stage method for evaluating policies. The policies are defined using path conditions, which are similar to regular expressions. Semantics for path conditions are defined, which is used to develop a rigorous method for evaluating policies. The algorithm required to evaluate policies and establish its complexity. Finally, the advantages of the model using an example and describe a preliminary implementation of the algorithm is presented.

P. W. Fong [18] proposed Relationship-Based Access Control (ReBAC) which is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships. This work explores what it takes to widen the applicability of ReBAC to application domains other than social computing. To this end, an archetypical ReBAC model is formulated to capture the essence of the paradigm, that is, authorization decisions are based on the relationship between the resource owner and the resource accessor in a social network maintained by the protection system. A novelty of the model is that it captures the contextual nature of relationships. A policy language based on modal logic is defined for composing access control policies that support delegation of trust. A case study in the domain of Electronic Health Records is used to demonstrate the utility of the model and its policy language. This work provides initial evidence to the feasibility and utility of ReBAC as a general-purpose paradigm of access control.

P. W. Fong at al. [19] takes a first step in deepening the understanding of this access control paradigm, by proposing an access control model that formalizes and generalizes the privacy preservation mechanism of Facebook. The model can be instantiated into a family of Facebook-style social network systems, each with a recognizably different access control mechanism, so that Facebook is but one instantiation of the model. It also demonstrates that the model can be instantiated to express policies that are not currently supported by Facebook but possess rich and natural social significance. This work thus delineates the design space of privacy preservation mechanisms for Facebook-style social network systems, and lays out a formal framework for policy analysis in these systems.

H. Hu and G.-J [24] proposed a multiparty authorization framework that enables collaborative management of shared data in OSNs. An access control model is formulated to capture the essence of multiparty authorization requirements. It also demonstrates the applicability of the approach by implementing a proof-of-concept prototype hosted in Facebook.

S. Jahid et al. [27] proposed EASiER, an architecture that supports fine-grained access control policies and dynamic group membership by using attribute-based encryption. A key and novel feature of the architecture, however, is that it is possible to remove access from a user without issuing new keys to other users or re-encrypting existing cipher texts. This is achieved by creating a proxy that participates in the decryption process and enforces revocation constraints. The proxy is minimally trusted and cannot decrypt cipher texts or provide access to previously revoked users. EASiER architecture and construction is described to provide performance evaluation, and prototype application of the approach on Facebook.

S. R. Kruk et al. [28] presented D-FOAF, a distributed identity management system which deploys social networks. It is shown that how information inherent in social networks can be utilized to provide community driven access rights delegation and algorithms for managing distributed identity, authorization and access rights checking is analyzed. Finally it shows how the social networking information can be protected in a distributed environment.

A. Masoumzadeh and J. Joshi [29] proposed an access control model based on Semantic Web technologies that take into account the above mentioned complex relations. The proposed model enables expressing much more fine-grained access control policies on a social network knowledge base than the few existing models. The applicability of the approach is demonstrated by implementing a proof-of-concept prototype of the proposed access control framework.

III.CONCLUSION

By the development and popularity of social networks, it is need to be access control mechanisms in them. In this paper a comprehensive study of authorization mechanisms for social network was provided. Several models were identified by their basic components and architecture. Also, their benefits and weaknesses were examined. At last, these models were assesses based on criteria which were drawn from identified models.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

REFERENCES

[1] Nasim R (2010). Privacy-Enhancing Access Control Mechanism in Distributed Online Social Network, Master's Thesis in Computer Science, at the Software Engineering of Distributed Systems Master's Program Royal Institute of Technology.

[2] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: an online social network with user-defined privacy. ACM SIGCOMM Computer Communication Review, 39(4):135– 146, 2009.

[3] S. Braghin, V. Iovino, G. Persiano, and A. Trombetta. Secure and policy-private resource sharing in an online social network. In PASSAT 2011, pages 872–875. IEEE, 2011.

[4] G. Bruns, P. W. Fong, I. Siahaan, and M. Huth. Relationship based access control: its expression and enforcement through hybrid logic. In Proceedings of the second CODASPY, pages 117–124. ACM, 2012.

[5] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. A semantic web based framework for social network access control. In Proceedings of the 14th ACM SACMAT, pages 177–186. ACM, 2009.

[6] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pages 1734–1744. Springer, 2006.

[7] B. Carminati, E. Ferrari, and A. Perego. A decentralized security framework for web-based social networks. Int. Journal of Info. Security and Privacy, 2(4), 2008.

[8] B. Carminati, E. Ferrari, and A. Perego. Enforcing access control in web-based social networks. ACM Trans. Inf. Syst. Secur., 13(1), 2009.

[9] J. Crampton and J. Sellwood. Caching and auditing in the RPPM model. In Security and Trust Management, pages 49–64. Springer, 2014.

[10] J. Crampton and J. Sellwood. Path conditions and principal matching: a new approach to access control. In Proceedings of the 19th ACM SACMAT, pages 187–198. ACM, 2014.

[11] P. W. Fong. Relationship-based access control: protection model and policy language. In Proceedings of the first CODASPY, pages 191–202. ACM, 2011.

[12] P. W. Fong, M. Anwar, and Z. Zhao. A privacy preservation model for facebook-style social network systems. In Computer Security–ESORICS 2009, pages 303–320. Springer, 2009.

[13] H. Hu and G.-J. Ahn. Multiparty authorization framework for data sharing in online social networks. In Data and Applications Security and Privacy XXV, pages 29–43. Springer, 2011.

[14] S. Jahid, P. Mittal, and N. Borisov. Easier: Encryption-based access control in social networks with efficient revocation. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pages 411–415. ACM, 2011.

[15] S. R. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and H.-C. Choi. D-FOAF: Distributed identity management with access rights delegation. In The Semantic Web–ASWC 2006, pages 140–154. Springer, 2006.

[16] A. Masoumzadeh and J. Joshi. OSNAC: An ontology-based access control model for social networking systems. In Social- Com 2010, pages 751–759. IEEE, 2010.

DOI: 10.15680/IJIRCCE.2015. 0311056