IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. V (Jul – Aug. 2014), PP 94-98
www.iosrjournals.org

Multi-Party Access Control Mechanism in Online Social Networks

[1]Sreeja S., [2]Riji N Das.
[1,2]*Dept. of Computer Science & Engg. Sree Buddha College of Engg.Alappuzha, Kerala, INDIA*

Abstract: *Social networking is an essential part of life for people around the world these days. Social networking is a form of social media, used for interactive, educational, informational or entertaining purposes. Even though social media comes in many forms all of them are related to each other. Social networking is also a tool to create and join groups, learn about latest news and events, play games, chat and to share music and video. Some social networks provide facilities to the users' to partition their group of friends based on social community, organization, geographical location, or how well they knows each other. The main challenge in social network is the sharing of data among heterogeneous users. The proposed method provide a systematic mechanism to identify and resolve privacy conflicts for data sharing, and different access control mechanisms.*
Keywords: *Social Networks, Privacy, Access Control, Security*

I. Introduction

An Online Social Network (OSN) is a web-based service that allows individuals to: (1) construct a public or semi-public profile within the service; (2) articulate a list of other users with whom they share a connection; (3) view and traverse their list of connections and those made by others within the service.

The first social networking website, sixdegrees.com, was launched in the year 1997.This company was the first of its kind; it allowed user to list their profiles, provide a list of friends and then contact them. However, the services provided by the company did not do very well due to that reason it eventually closed three years later. The other elements that are noted at Social network websites are these sites required users to give their profiles but they could not share other people's websites. In the year of 1999 Live Journal was created. It was created in order to facilitate one way exchanges of journals between friends. Another company in Korea called CY world added some social networking features in the year 2001.This was then followed by Lunar Storm in Sweden during the same year. They include things like diary pages and friends lists. Additionally, Ryze.com also established itself in the market. It was created with the purpose of linking business men within San Francisco. The Company was under the management of Friendster, LinkedIn, Tribe.net and Ryze. The latter company was the least successful among all others. However, Tribe.net specialized in the business world but Friendster initially did well but this did not last for long.

Now a days the most significant Social networking websites commonly used by the people especially by the youngster are, Friendster, Myspace, Facebook, Downlink, Ryze, SixDegrees, Hi 5, LinkedIn, Orkut, Flicker, YouTube, Reddit, Twitter, FriendFeed, BharatStudent etc.

II. Related Works

The word privacy has different meanings, ranging from personal privacy to information privacy, each with their own definition. Most of the social networking sites offer the basic features of online interaction, communication, and interest sharing; also it allows individuals to create online profiles that other users can view. One of the most important issues address in this context is the security and privacy of sensitive information. Currently there are no specific regulations for OSNs and they are treated as an information service that is an online database of information.

The use of personal information in social networks raises new privacy concerns and requires insights into security problems. Online social networks have recently emerged as a challenging research area. Social networks typically try to define some set of rules for the user, to define who can view their information and who cannot. The problem with this is that users that have access to the sensitive, hidden data of another user can simply use their ability to publish to spread that data to users whom are not supposed to have access to it. This will lead to the disclosure of the sensitive data and their by increasing the privacy risk.

A. Sources Of Users Profile Leakage

Leakage of information through poor privacy settings**:** Most social network users are not careful about their privacy settings. Many open their profile to the public so anyone can access and see their information. Also, many social networking sites default privacy setting is still not safe such as in Facebook, a friend of a friend who the user does not know can still see his information. However, even the safest privacy setting, there are still flaws that allow attackers to access user's information.

Leakage of information to 3 rd party application: Many social networking websites such as Facebook provide an API (Application Programming Interface) for 3rd party developers to create applications that can run on its platform. These 3rd party applications are very popular among social network users. Once users add and allow 3 rd party applications to access their information, these applications can access user's data automatically. It is also capable of posting on users' space or user's friend's space, or may access other user's information without user's knowledge

B. Current scenario

Famous social network sites, such as Facebook and MySpace, currently provide simple access control mechanism that allows users to manage and control access to information contained in their own spaces. However, users have no control over data residing outside their spaces. For example, if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo, even though the tagged friends may have different privacy concerns about the photo. To address such a critical issue some basic privacy settings and mechanisms have been offered by existing OSNs (repot abuse, remove tags etc.). These basic protection mechanisms also have limitations; the final decisions that are made in the case of a shared data among multiple users are sometimes too loose or restrictive.

C. Rule Based Access Control Model

Carminati et al [3] proposed a Rule based access control model for social networks .It is a semi-decentralized architecture, in which the access rules are specified in terms of relationship type and trust metrics by individual users in a discretionary way. The system also has a centralized certificate authority to ensure the authenticity of the relationship, while access control enforcement is carried out on the decentralized user side. This scheme only allows a single controller, i.e. the owner of the resource to specify access control policies.

D. Multiparty Access Control For Online Social Networks

Hongxin Hu et al. proposed a multiparty access control model (MPAC), along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. Three attack scenarios in the current OSN are specified, such as profile sharing, relationship sharing and content sharing to identify the risks due to the lack of collaborative control in OSNs. They proposed a voting scheme for decision making of multiparty control and a Strategy-based conflict resolution scheme.This MPAC model gives an aggregate decision making for conflict resolution and give an opportunity to the controller to analyses the over and under sharing of the data.

E. Circle Based Multiparty Access Control For Google+

In this paper they formulated a circle-based multiparty access control model (CMAC) to identify the need of collaborative authorization requirements in Google+, along with a multiparty policy specification scheme and a policy enforcement mechanism. In this paper in addition to the content sharing, the collaborative control for circle sharing is considered, i.e., the privacy of users in a shared circle. In CMAC model the controller can specify a positive and negative policy to include or exclude a specific group to share resources. To eliminate the potential disclosure of a data due to dissemination is controlled by a restrictive conflict resolution strategy called Deny – Override.

III. Access Control In Osn

This section deals with the requirement analysis of multiparty access control in OSNs. This paper mainly analyze three scenarios profile sharing, content sharing and relationship sharing to identify the risks due to the lack of collaborative control in OSNs.

A. Controllers In OSN

For a shared data in OSN there are multiple controllers are there, so according to the sharing pattern in addition to the owner of the data, some other controllers are included in the OSN environment, they are

Contributor: Let d be a data item published by a user u in someone else's space in the social network. The user u is called the contributor of d.

Stakeholder: Let d be a data item in the space of a user in the social network. Let T be the set of tagged users associated with d. A user u is called a stakeholder of d, if u is in T.

Disseminator: Let d be a data item shared by a user u from someone else's space to his/her space in the social network. The user u is called a disseminator of d.

B. Policy Specification

To control user access over shared data associated with multiple controllers a better access control policy is needed. In the proposed model, each controller of a shared resource can set one or more rules that specify who can access the resource.

- Accessor Specification
  The set of users who are permitted to access the shared data are called accessors .An accessor specification is defined as
  at ={UN,RT,GN}
  Where, UN: User name; RT: Relationship type and GN: Group name .
- Data Specification
  The data specification is defined as a tuple < dt; sl >.
  Where, dt: Data item and sl: Sensitivity level ranges from 0 – 1.
- Access Control Policy
  An access control policy is defined as
  P =<controller; ctype; accessor; data; effect >, where, controller is a user who can control the access of data ,ctype is the type of the controller and effect is the authorization effect of the policy i.e., permit or deny

C. Policy Evaluation

Policy evaluation process checks the access request against the access control policy specified by the controller, and the evaluation process returns a response with the decision (either permit or deny) indicated by the effect element in the policy. If more than one controller are their then the decisions from all controllers are aggregated to make a final decision for the access request. Since data controllers may have different decisions (permit and deny) for an access request, conflicts may occur. To avoid these conflicts in multiparty policy evaluation a systematic conflict resolution mechanism is needed. A strong conflict resolution strategy may provide a better privacy protection. Meanwhile, it may reduce the social value of data sharing in OSNs. Therefore, it is important to consider both privacy and sharing loss.

IV. IDENTIFYING And Resolving Privacy Conflicts

a) Identifying Privacy Conflict

Each controller of the shared data item has a set of trusted users who can access the data item. The set of trusted users represents an accessor space for that controller. To identify the privacy conflicts a space segmentation approach [] is used to partition accessor spaces of all controllers of a shared data item into disjoint segments. From that disjoint segments the conflicting accessor space are identified.

b) Threshold Based Conflict resolution

If all the controllers are treated as equally, for e.g. consider the scenario of sharing, tagging and writing comments on others profile, in such cases a combined decision making is necessary .For that purpose threshold based conflict resolution is used, sharing loss and privacy risk is considered as the threshold for decision making.

Measuring Privacy Risk

Allowing access to an untrusted controller leads to privacy risk. Privacy risk is calculated by considering the following factors

- Number of privacy conflicts: The number of the untrusting controllers conflict segment i
- General privacy concern of an untrusting controller: The general privacy concern of an untrusting controller j is denoted as pc_j in the range [1, 5]
- Sensitivity of the data item: The sensitivity level of the shared data item explicitly chosen by an untrusting controller j is denoted as sl_j
- Visibility of the data item: The visibility of the data item with respect to a conflicting segment captures how many accessors are contained in the segment i, denoted as n_i.
- Trust of an accessor: The trust level of an accessor k is denoted as tl_k, which is an average value of the trust levels defined by the trusting controllers of the conflicting segment for the accessor.

PR of Conflicting Segment 'i' due to untrusted controller 'j' is calculated as

$$PR(i,j) = (1 - pcj * slj) * \sum_{k \in accessor\ (j)} (1 - tlk)$$

Overall privacy risk of Conflicting segment 'i 'is

$$PR(i) = ni \sum_{j \in Controllersa\ (i)} PR(i,j)$$

Measuring Sharing Loss

When the decision of privacy conflict resolution for a conflicting segment is "deny", it may cause losses in data sharing, since there are controllers expecting to allow the accessors in the conflicting segment to access the data item. Similar to the measurement of the privacy risk, four factors are adopted to measure the sharing loss for a conflicting segment.

The overall sharing loss SL(i) of a conflicting segment 'i' is computed as follows:

$$SL(i) = \sum_{j \in controllersT\ (i)} (1 - pcj * slj) * \sum_{k \in accessor\ (i)} tlk$$

The final decision is made automatically by OSN systems with this threshold-based conflict resolution as follows:

$$Decision = \begin{cases} Permit & \text{if } SL(i) \geq PR(i) \\ Deny & \text{if } SL(i) < PR(i) \end{cases}$$

Resolving Score

An optimal solution for privacy conflict resolution should cause a little more privacy risk when allowing the accessors in some conflicting segments to access the data item, and gets lesser loss in data sharing when denying the accessors to access the shared data item. Thus, for each conflict resolution solution s, a resolving score RS(s) can be calculated using the following equation:

$$RS(s) = \frac{1}{\sum_{i \in CSp} PR(i) + \sum_{j \in CSd} SL(j))}$$

Where, CS_p and CS_d denote permitted conflicting segments and denied conflicting segments respectively in the conflict resolution solution s.

The optimal conflict resolution CR between privacy risk and sharing loss can be identified by finding the maximum resolving score:

$$CR = \max(RS(s))$$

Once the privacy conflicts are resolved, we can aggregate accessors in permitted conflicting segments CSp and accessors in the non-conflicting segment ps together to generate a new accessor list (AL) as follows:

$$AL = (\bigcup_{i \in CSp} Accessor(i) \cup Accessor(ps))$$

V. Conclusion

In this day and age where social networking is common place to almost everyone. Many people register for social networks in a single-minded attempt to connect with old friends and to meet new ones, without considering the privacy implications. The proposed method mainly aims to identify and resolve privacy conflicts occurred in the Social network environment. As an initial step, a prototype of Facebook is implemented. The prototype model also allows the users to set a privacy setting that includes friends, group and sensitivity of the content. For the conflict identification a space segmentation method is used, in which the entire users' space is partitioned into superset, subset, disjoint set or partially matched. This will helps to identify privacy conflict. For the conflict resolution, tradeoff between privacy risk and sharing loss of a particular conflicting segment is calculated.

References

[1]. Facebook Privacy Policy. http://www.facebook.com/policy.php/.
[2]. Google+ Privacy Policy . http://www.google.com/intl/en/+/policy/.
[3]. D. Boyd and N. B. Ellison. Social network sites: Definition, history, and scholarship. Journal Of Computer-Mediated Communication, 13(1):210–230, 2007.
[4]. H.Hu., G.-J. Ahn, and J. Jorgensen. Enabling Collaborative Data sharing in Google+. Technical Report ASU-SCIDSE-12-1, April 2012.http://sefcom.asu.edu/mpac/mpac+.pdf.
[5]. 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.
[6]. Hu,Hongxin,Ahn,Gail-joon,Jorgensen,Jan,"Multiparty Access Control for Online Social Networks: Model and Mechanisms"Knowledge and data Engineering on ,IEEE Transaction,July 2013
[7]. H. Hu, G. Ahn, and K. Kulkarni. Anomaly discovery and resolution in web access control policies. In Proceedings of the 16th ACM symposium on Access control models and technologies, pages 165–174. ACM, 2011.