Attribute-based Fine-grained Extended Access Control Mechanism for Online Social Networks

Rongna Xie, Lin Yuan, Guozhen Shi, Yazhe Wang and Chao Wang

ABSTRACT

The development of online social networks allows users to communicate with each other and share their resources when and where. However, in the process of data dissemination, the user loses control of the private information if the user shares resources into the social network, which may lead to privacy leakage. In order to solve the above problems, the paper proposes an extended access control mechanism for online social networks. This mechanism not only controls the operation rights of direct users, but also controls the assignable rights of indirect users, achieving the purpose of extended authorization. In this paper, the attribute modeled as a five-tuple is defined in detail, and requirement of each attribute is described. Furthermore, we assign different weights to different operation types of resources, and judge whether the resource operation is satisfied by calculating the degree of trust and the weight, thus determine user’s permissions. Finally, through case analysis and scheme comparison, we prove that the extended authorization mechanism can effectively control the spread of information and protect user’s privacy.

KEYWORDS

Social Networks, Extended Access Control, Attribute, Privacy Protection.

Rongna Xie, Lin Yuan, Guozhen Shi, Yazhe Wang, Chao Wang
Beijing Electronic Science and Technology Institute, Beijing 100070, China
INTRODUCTION

With the rapid development of the Internet, online social networks (OSNs) have gradually entered people's lives. People use online social networks to communicate with family members, friends, colleagues or even strangers, which not only enriches people's lives, but also makes the communication easier and faster. We share our daily dynamics through OSNs, in order to increase the intimacy between people, which increases the risk of information disclosure at the same time. Privacy information is involved in our resources. We send the resources to the social network, but we don't know who will get the resources and how it will be used, which greatly increases the risk of privacy disclosure.

Online social networks can be compared to a large human-centric communication platform where communication and data transmission are essential. However, they lose the right to control resources if users share resources on social network platforms, and the recipients of resources will no longer be restricted in what operation they can do on resources, which is a hidden security risk in social networks. Therefore, during the spread of resources, extended authorization has become an urgent problem to be solved. If we can control the direction in which we share data, we can effectively control the data according to our own wishes, and there will be no random changes or abuses of data recipients, which can reduce the risk of privacy leakage.

At present, there are many models of access control, but none of them take into account the issue of extended authorization after the spread of resources. For example, traditional models of access control, including Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Access Control List (ACL), all have shortcomings such as large amount of management and poor flexibility. Then the role-based access control came into being, making authorization management simple for users and easy to store [1]. Currently the relation-based access control model (RBAC) [2, 3] is the most popular access control mechanism in OSNs. This model system relies on the type, depth or strength of the relationship and it has the most direct expression of the relationship between users. However, this model lacks consideration of user’s attributes. Later, the attribute-based access control (ABAC) methods are incorporated into the existing RBAC model [4], providing users with more flexible access control on data. But these models have two shortcomings: a) none of these models takes into account the issue of extended authorization. By developing an extended authorization policy, we assign users with operational rights to resource, so that users' unauthorized behaviors on data can be controlled during the transmission of data and privacy disclosure can be avoided. b) These models have shortcomings such as low efficiency and large overhead. These models constrain the node user conditions within the specified hops on the
relational path by formulating policy. In this way, when a path is searched, not only the attribute values of each node must be stored, but also the conditional judgement of repeated nodes may be caused, leading to large overhead and reduced efficiency in terms of policy matching. In response to the above problems, we have improved the existing solutions and proposed an attribute-based extended access control mechanism in online social networks. The main contributions are shown as follows:

a) Our work proposes an extended access control mechanism and a formal description is given. This mechanism not only controls the operation rights of direct users, but also controls the assignable rights of indirect users, achieving the purpose of extended authorization. We assign different weights to the operations according to the demand in the online social networks, and we can determine whether the user has the permission of the operation by calculating the degree of trust and the weight.

b) Our work proposes an attribute-based five-tuple policy specification in detail. In this paper, we divide into five types of attributes and we formalize these different types of attributes in detail, making the access control mechanism more visual and fine-grained. It could be a good reflection of the extended access control mechanism.

The remainder of this paper is organized as follows. In Section II, we provide a brief discussion of related research works. Section III discusses the ABEAC (attribute-based extended access control) model; Section IV describes the extended access control mechanism and give some cases for the policy mechanism. In Section V, we further combine the scenarios to demonstrate the usage of the proposed policy specification. In Section VI, we conclude the paper and outline some future work.

RELATED WORK

In this section, we discuss three types of access control models and analyze the progress of various access control models in social networks.

Relationship-based Access Control Model (RBAC)

Social networks can be abstracted as network topologies composed of different users and corresponding relationships. Now RBAC has been widely used in online social networks. Many solutions have been proposed, most of which can be
summarized as using three decision-making factors: relationship type, relationship depth and relationship strength (such as trust). Using this model, we can judge the access control rights of resource according to the relationships with other people, which narrows the scope of users and facilitates the setting of permissions.

Initially, Carminati [5] proposed solutions that associate trust with RBAC, allowing people to specify the strength of connections by assigning trust values to relationships. Guo L [6] also proposed a trust-based privacy protection method for friend recommendation. According to their privacy preferences, users find matched friends and establish social relationships with them. After that, a semantic web-based RBAC solution was proposed, which defines authorization, management, and filtering policies to control the access of users [7]. Yuan Cheng [3] proposed a user-to-user relationship access control (UU-RAC) model, which uses a regular expression-based policy specification language. And a path detection method is proposed to judge all the relational paths that satisfy the specified relationship.

Rule-based Access Control Model

This is an access control model commonly used in social networks. In order to protect user’s information effectively, we can define rules to restrict rights for accessing or transferring. Many researchers use logical rules to protect privacy so that we can adapt to the diversity and dynamics of social networks. For example, Barbara [8] proposed a rule-based WBSNs access control model, which allows rule specification for online resources. Carminati [5] proposed a rule-based access control mechanism, which is based on the execution of complex policies. Subhani S [9] proposed a rule-based image privacy method in social networks, and the access control mechanism is similar to the traditional UCON model. Ma Li [10] proposed a rule-based privacy protection policy, which makes the access control mechanism more flexible and fine-grained.

Attribute-based Access Control Model (ABAC)

Although most RBAC models can clearly and simply express the variety of relationships in social networks, there are not only relationships in social networks, but also a wide variety of resources. At the same time, both the user and the resource itself have attributes, which provides a richer way to describe the qualification between the access user and the resource. Therefore, in addition to
some relational information, the characteristics of attributes, including user name, age, role, location and so on, make the formulation of access control policy more perfect and flexible in the social network with dynamic characteristics. In the work of the above URRAC model, Cheng added attribute information to the relationship-based access control model [6], thus enabling a more fine-grained access control policy. In [11], by using role factors as constraints, an automatic policy description and fine-grained access control model is proposed, where role is a concrete example of attribute.

The models above have not solved the problem of extended access control in the process of data dissemination.

ABEAC MODEL

In this section, we discuss the ABEAC (Attribute-Based Extended Access Control) model for online social networks.

Model Components

We introduce the components of the model, symbol definitions, and so on. We define the following elements:

(1) Subjects(S): Subjects represent a set of registered requesters in the online social networks. We express such user entities as $U_S$.

(2) Objects(O): Objects refer to a group of user entities (U) or resources (S) that the subjects can access according to the allowed permissions. We express such user entity as $O_U$, and express the resource as $O_S$. The types of resources are very extensive, and the common ones include text, pictures, videos, and so on.

(3) Action (AC): Action represents the action that the subject grants to the objects according to the permissions. We divided the operations into general operations and special operations. General operations include viewing, deleting, modifying, and so on. The special operations include sharing, comments, favorites, and so forth.
Policy(P): Policy represents a set of rules that control the ability of a subject to access an object. Here, we divide the policy into two categories, one is system policy and the other is user policy. The system policy(S) represents the default policy specified by the system, and it is the basic requirement for the target to obtain the rights. The user policy represents the individual's customized policy according to their own needs. The policy used to express the user needs is described as OUP and used to express the resources need is described as OSP.

Time(T): T represents the timestamp. Social networks are time-sensitive, and we need to ensure that access requests are legal requests within the validity period. If it exceeds the specified time that the request is illegal.

As can be seen in the Figure 1, in the process of requesting, we use the timestamp T to determine whether the request is valid. We set the policy for the user object $O_u \in O_U$ and the resource object $O_s \in O_S$ respectively, and the object executes the corresponding authority according to the policy.

Policies can be system-specific or user-specified. The system-specified policy is a policy formulated at the social network system level. For example, the system stipulates that the user must register and perform real-name authentication. The user-specified policy refers to the relevant rules for the specified user or resource in the extended authorization process. User-specified policies include OUP and OSP.

Social Network Model Graph

The graph is a common representation of social networks. As shown in Figure 2, we intuitively represent our social network model graph with a simple undirected graph. Each node represents a user, and each edge corresponds to a relationship.
type and the trust strength of the relationship type, and the lowest weight of resource propagation (as shown in the Fig. 2, f stands for friend relationship, and w stands for the minimum right of resource propagation, and the number stands for the strength of trust). The strength of trust here represents the intimacy of the relationship. The trust value of a relationship is calculated by the system according to the historical records. Here we assume that the trust value of each relationship is given, and the lowest weight of the resource is set by the user according to the specific situation. Considering that different resources have different levels and operational rights in the real world, we set the minimum weight to constrain the range of operation.

At the same time, users do not only exist in OSNs in the form of individuals. A class of users based on fixed attributes or contexts belongs to a group of users, as indicated by the dotted line in the figure. For example, the users named A, C and D belong to one type of user group, and the users named B, D and E belong to another type of user group. One user can belong to different user groups, and one user group can contain different users. For example, we compare a company to a social network, where each department of the company is a group of users, and each type of relationship exists in each department.
POLICY MECHANISM

Properties in OSNs

In general, we use a relationship-based access control system model, and we add attribute features based on the model. The traditional relationship-based access control model is relatively simple and efficient. It has an intuitive representation of the relationships (including relationship type, strength, depth, etc.) in OSNs. However, relationships do not fully cover the privacy and security issues of resource in OSNs. The attribute characteristics make the extended access control mechanism more flexible and fine-grained.

There are many attributes of user and resource maintained in the social network. Users keep personal information such as name, age, gender, etc. At the same time, resources also have many attributes, such as type and level attributes, and so on.

For the ABEAC model, we identify three types of attributes: user group attributes, node attributes, and edge attributes. As follows,

1. User group attributes. A class of users with certain characteristics is classified as a user group. User groups contain users with various relationship types, and one user can also be in two or more user groups. This paper does not consider this situation for the time being.

2. Node attributes. Users and resources are represented as nodes on the social graph. Users carry attributes that define their identity and characteristics, such as name, occupation, address, etc. And resources carry attributes that define their type (including texts, images, video types, etc.).

3. Edge attributes. Relationships are represented as edges on the social graph. Each edge has attributes that describe its relationship type and trust level. The type of relationship and the degree of trust determine what operational rights the access user can hold.

Extended Access Control Mechanism

Unlike general access control, extended access control mechanism is more complicated. Here we formally define the basic elements. Firstly, we define Group, N, and E represent user groups, nodes, and edges in the graph; And ATTR (group),
ATTR (n), and ATTR (e) are attributes of user group, node n, and edge e respectively (group ∈ Group, n ∈ N, e ∈ E).

As shown in Figure 2, we abstract the social network into a graph structure. And nodes and edges represent the information of subjects and relationships, respectively. Both the subjects and the relationships carry different attributes, and we specify the policies in the extended access control process based on these attributes. The attribute of user group is defined by the scene and it satisfies our realistic scenario in our lives. We specify that if the attribute of user group is defined, the attribute of user group must be satisfied first, and then the node and edge attributes are satisfied. If they are not specified, we use "_" to indicate.

In addition, we reduced the relationship to three types: strangers, colleagues and friends, which are represented by s, c and f, respectively. The operation type is reduced to three types, which are viewing, modifying, and transferring. The symbol [ ] is used to represent the information of attributes, while the notation<>indicates the start and end of the policy, and the notation () indicates the corresponding relationship attribute that exists. The specific policy specifications are shown as follows.

The policy is represented by a five-tuple P=< [ATTR (resource)], [ATTR (group)], [ATTR (direct user)], [ATTR (indirect user)], [time] >.

(1) [ATTR resource)] indicates the attribute information of the operating resource. We specify it in the form of [(resource, action, condition)], which expresses that the resource needs to satisfy certain weighting conditions to execute the specified operation;

(2) [ATTR (group)] indicates the attribute information of the specified user group. We stipulate that it is expressed in the form of [user. user group name];

(3) [ATTR (direct user)] indicates the attribute information of the direct access user. We classify such attribute information into two types, which named general attributes and relationship attributes. General attributes refer to attributes specified by the user with specific conditions, such as specified users or conditional attributes that meet certain age requirements; relationship attributes refer to attributes that meet certain conditions. We stipulate it in the form of [user, general attributes, (the type of user, the degree of trust)];

(4) [ATTR (indirect user)] indicates the attribute information of the indirect access user. Similarly, we classify this type of attribute information into two types, which named general attributes and relationship attributes. The general attribute refers to the attribute specified by the user with specific conditions; the relationship attribute refers to the attribute that satisfies the condition with certain relationship,
and we specify it in the form of \([\text{general attribute}, (\text{the type of user, degree of trust})]\).

(5) \([\text{time}]\) indicates the time attribute to ensure that the access request is within the valid time range.

For different operations, the demand in the online social networks is not completely in consistent. For example, the number of requests for transferring operations has large amounts, and the number of requests for viewing and modifying is relatively small. Then we assign different weights to the three types of operations to represent the different needs in online social networks. We stipulate that the weights of the three types of operations are 60, 30, and 10, respectively. At the same time, the users with the modifying rights also have the transferring and viewing rights, and the users with the viewing rights also have the transferring rights. Similarly, for different types of relationships, the degree of trust (intimacy) is not the same. We stipulate that the intimacy between 0.5 and 1 is the relationship of strangers, the intimacy between 1 and 1.5 is the relationship of colleagues and the intimacy between 1.5 and 2 is the relationship of friends. We use the weighted value by multiplying the weight and the trust value as a condition for deciding the executable operations.

**Cases for the Policy Mechanism**

We have given the basic formal definition of the policy mechanism above. Now we will show some examples of how to apply it to the ABEAC model.

Example 1: A sets a rule for a word file. He stipulates that the file can be viewed, but needs to meet the requirement of weighted value greater than 45. Then a user group condition is defined as a WeChat group of A’s, and the direct friends of A are required to satisfy the requirement of trust value greater than 1.6 and female. The indirect friend of A must satisfy the requirement of trust value greater than 1.8. Then A can formulate policies as follows:

\[
P1: < [\text{word, view, }> 45], [A, \text{WeChatgroup}], [A, \text{sex = female, (f, }> 1.6)], [(f, > 1.8)], [\text{time1}] >
\]

Example 2: B now sets the rules for an image file. He stipulates that the image file can be transferred, but the weighted value needs to be greater than 50. At the same time, B stipulates that the direct colleagues of B need to satisfy the requirement of trust value greater than 1.2, and the indirect friends of B need to
satisfy the requirement of trust value greater than or equal to 1.6. B does not specify the user group condition. Then B can formulate policies as follows:

\[
P2: < [\text{photo, transfer}, > 50), [B.], [B, (c, > 1.2)], [(f, \geq 1.6)], [\text{time2}] >
\]

Example 3: C now sets the rules for a .xml file. He stipulated that the .xml file could be modified, but the weighted value should be greater than 15. C specifies that the user group condition is one of his friends’ group, and C specifies that the direct friends of C need to satisfy the requirement of trust value greater than 1.7, and the indirect friend of C need to satisfy the requirement of trust value greater than 1.8. Then C can formulate policies as follows:

\[
P3: < [\text{xml, modify, > 15}], [\text{C. Friendgroup}], [\text{C, (f, > 1.7)}], [(f, > 1.8)], [\text{time3}] >
\]

**USE CASE ANALYSIS**

With the development of the online social networks, more and more users communicate with each other and spread resources through the network. WeChat is widely used. In this section, we will demonstrate the process of policy mechanism in the environment of WeChat. Assume that User A has formulate the following policies:

\[
< [\text{pdf, view}, > 45)], [\text{A. WeChatgroup}], [\text{A, (f, > 1.6)}], [(f, > 1.8)], [\text{time}] >
\]

The process analysis is shown as follows:

First, we extract the node attributes and separate the policies: determine that the start node is A and the policy of resource is \((\text{pdf, view}, > 45)\), the policy of user group is the \text{WeChatgroup}, the policy of the relationship is "\text{A, (f, > 1.6)}" and "\text{(f, > 1.8)}".

Secondly, we analyze each policy: first, it is clear that the user group is one of A’s \text{WeChatgroup}, so A can share the specified pdf file in this WeChat group. And this pdf file has the right to view and share. Next we see that the direct friends of A are required to satisfy a trust value greater than 1.6, so we need to judge the corresponding weighted value whether meet the requirements of the minimum weighted value of resources. The calculation shows that the corresponding weighted value is 48, and it meets the requirements of greater than 45. In general, users who have friends with A in the specified WeChat group can view the PDF file.
Thirdly, we need to analyze the policy of extended authorization. A stipulates that a user who has a friend relationship with A’s direct friends and their trust degree is greater than 1.8 can view the file. The calculation shows that the corresponding weighted value is 54, and it meets the requirements of greater than 45. Then his direct friends can stipulate further polices for the resource within the limits of the authority before. We assume that C who is one of A’s direct friends obtains the resource and then stipulates further policies: `< [(pdf, view, > 45)], [C. WeChatgroup1], [C, sex = female, (f, _)], [(f, > 1.9)], [time] >`. In this policy, we see that C shares the resource to another WeChat group, and also stipulates that the direct friends of him can view the resource. Although he does not stipulate the trust level, it needs to meet the requirement of trust value greater than 1.8 which is stipulated before. In addition, he added a new policy, that users of the gender of female are required to meet the requirement, and further extended authorization part analysis is the same as above.

Generally speaking, we should clear two points in the process of analysis: a) the formulation of extended authorization policy should meet the fact that the lower level of policy is a subset of the superior level of policy, so as to ensure that the authority will not be violated; b) we set the minimum range for the operation weight of the resource, this part of the policy is not allowed to be modified.

The example analysis is shown in Table I, compared with the traditional schemes, the proposed scheme takes into account the extended authorization access control mechanism and it is more fine-grained, and efficient.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>extended access control</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td>fine-grained</td>
<td>x</td>
<td>√</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td>efficiency</td>
<td>lower</td>
<td>lower</td>
<td>lower</td>
<td>higher</td>
</tr>
<tr>
<td>overhead</td>
<td>higher</td>
<td>higher</td>
<td>higher</td>
<td>lower</td>
</tr>
</tbody>
</table>

To sum up, this mechanism can take into account the extended access control, and it is fine-grained, efficient and low-overhead.
SUMMARY

The paper proposes an extended access control mechanism to control the unauthorized behavior of users by restricting the operation rights of subsequent users. In the future, further research is needed in the following aspects: propose the possible conflicts of different policies and give the solutions combined with the special background.

ACKNOWLEDGMENTS

Corresponding author: Lin Yuan.

This work was supported by the National key Research and Development Program of China (Grant No.2017YFB0801803).

REFERENCES
