Trust-based Access Control in Virtual Learning Community

Shujuan Wang[1]，Qingtang Liu[1,2]
1 Department of Information Technology,Huazhong Normal University, Wuhan,Hubei.P.R.China, wsj_xgz@126.com
2 Engineering Research Center of Education Information Technology, Huazhong Normal University,.Wuhan, Hubei.P.R.China
liuqtang@mail.ccnu.edu.cn

Abstract. The virtual learning community is an important application pattern of E-Learning. It emphasizes the cooperation of the members in the community, the members would like to share their learning resources, to exchange their experience and complete the study task together. This instructional mode has already been proved as an effective way to improve the quality and efficiency of instruction. At the present time, the virtual learning communities are mostly designed using static access control policy by which the access permission rights are authorized by the super administrator, the super administrator assigns different rights to different roles, but the virtual and social characteristics of virtual learning community make information sharing and collaboration a complex problem, the community realizes its instructional goal only if the members in it believe that others will offer the knowledge they owned and believe the knowledge others offered is well-meaning and worthy. This paper tries to constitute an effective trust mechanism, which could promise favorable interaction and lasting knowledge sharing.

1 Introduction

The access control and trust management both are key policies in the information security management, and the application of information technology such as computer technology and network technology in education is obvious to all, E-Learning is becoming a leading instructional mode. The virtual learning community is an important application pattern of E-Learning [4]. It emphasizes students' subjectivity and independency within learning activities, it also emphasizes the cooperation of the members (learners) in the community, the members would like to

share their learning resources, to exchange their experience and complete the study task together. It has already been proved that the virtual learning community is an effective way to improve the quality and efficiency of instruction [4]. at the present time, the virtual learning community are designed using static access control policy by which the access permission rights are authorized by the super administrator, the super administrator assigns different rights to different roles, but the virtual and social feature of virtual learning community makes information sharing and collaboration a complex problem, in which an important aspect is whether the members trust others will offer the knowledge they owned. It could promise favorable interaction and lasting knowledge sharing by constituting an effective trust mechanism.

Access control is more applied in the field of computer security and network security, it is a method to allow or constraint the subject's access to the object through many ways, and it is also a key measure to confirm the system's security. As an open instruction system, the virtual learning community also should take apt access control policy to fulfill the needed security of the learning resource and instruction. The investigation indicated that the virtual learning community's authorization management is mostly based on static access control policy managed by the super administrator. Its basic idea is to grant the members certain rights to access and operate the learning resource.

The general roles in virtual learning community may include administrator, expert, teacher as well as student. The administrator's work is to manage the behaviors of other members, namely experts, teachers and students; the expert's work is to evaluate the resources in the community, to answer the difficult problems; the teacher's work is to organize instruction and learning activity, assign instruction task, supervise the students' study; the students participate in the instruction activity, the team discussion, advance questions, accomplish the task collaborated with others, as well as upload their own knowledge. Actually, there may be other roles in virtual learning community, just depends on the instructional requirement. Having registered as a member in virtual learning community, the user would act certain role and execute corresponding rights.

The members of virtual learning community are mostly quasi-permanent separated in space and time [5]; they contact each other by virtue of e-mail, BBS, community chat-room, and so forth; the anonymous feature of virtual status causes the feeling of strange and distrust. Separation in space and time as well as lack of face-to-face interaction makes mutual trust among members a complicated problem.

The virtual learning community presents some social characteristics [4]; in which trust between two parties is foundational, but the existing virtual learning communities adopt static role-based access control policy, ignoring the constitution and maintain of the trust relations among the individuals.

This paper presented a trust-based access control model in virtual learning community, and realized the access control decision-making based on the members' creditability through integrating trust component into the access control mechanism.

2 Trust-based Access Control Model

In the virtual learning community, embedding trust component into the existing role-based access control [1,2] offers a safeguard mechanism over the interaction among the members, the figure followed is a trust-based access control model which clarifies the relationship among the components.

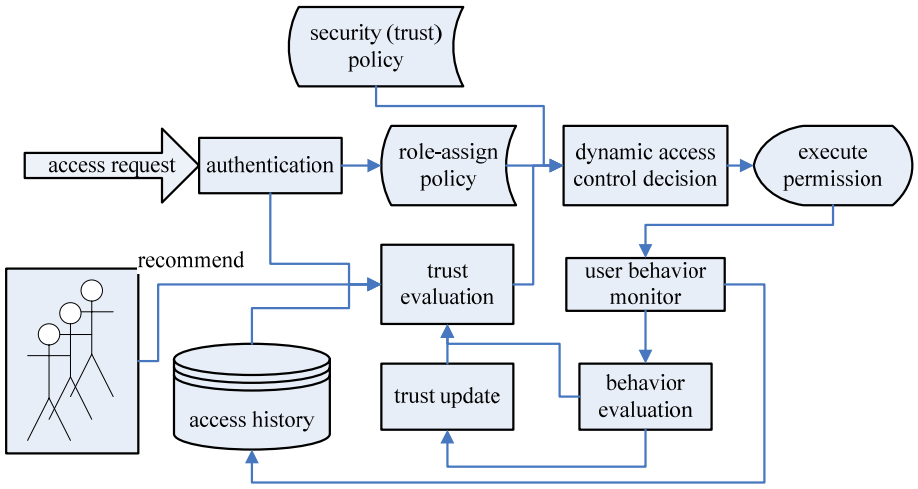

Fig. 1. Trust-based Access Control Model

In this figure, there are several points to be noticed.

(1). Authentication is the first step of access control [6] in virtual learning community, and the primary work is to make it clear that the user is registered member of this community or not, if the answer is yes, judge from the corresponding access history and the trust degree associated with the user's status identity.

(2). Behaviors monitoring includes logging and measuring the state and operative behaviors in virtual learning community. It provides information evidences for the calculation of trust degree, the things need to be monitored mainly include the user's participating degree, the resource's quantity and worthiness he contributed, and so forth. The realization of trust policy relies on corresponding trust mechanism, and behaviors monitor acts a significant role. After an access operation is finished, the access behaviors will be logged and the behaviors will be evaluated, the interaction production should be marked off different trust grade at least; sequentially influences the trust degree evaluation to the target member.

(3). We can analyze the target member's creditability and calculate his basic trust degree referring to his own access history, furthermore, we also have to collect the trust recommendations come from other members who have interacted with target member in this virtual learning community, then we can calculate the

target member's reputation degree in virtual learning community, we get the weight sum of the two value, and name it final trust degree. In addition, as this accessing operation finished, target member's trust degree should be recalculated, overwritten and updated, if it is the first time the user access this virtual learning community and have no access history and no trust degree, we should put him an initial trust degree value in order to assign access rights to him.

(4). In the trust-based access control model, dynamic access control decision-making need to carry through various considerations according to the access request and his creditability.

This figure has clarified the relationships among components and the flow of authorization. Part 3 will explain trust-based authorization in detail.

3 Trust-based Authorization

Role-based access control (RBAC) [1, 2] is a popular mode at the present time, and most virtual learning communities are applying this kind of access control mechanism. In RBAC, the user could manage the access rights upon the resources he owned easily, and the administrator could realize flexible authorization by roles assignment [1, 2, 6], in view of the virtual learning community's social characteristics, we introduce trust into the existing role-based access control and form a trust- consolidated role assignment.

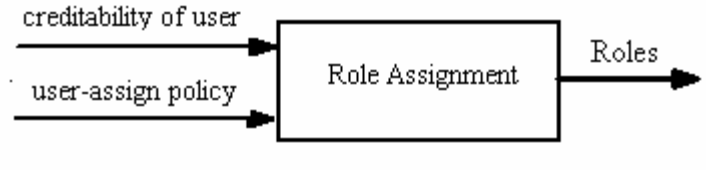

Fig. 2. Trust-consolidated role assignment in authorization

Trust is a complicated conception in interpersonal interaction network, and we could interpret it as the subject's approval to the object's reliability, honesty and ability. The degree of trust is defined as trust degree. Trust degree reflects subject's expectation to the object's to-be behaviors, and this expectation is related to the environment, it is the sum-up to the historical experience.

Trust has more subjectivity, and different people will make different conclusions to same object's trust degree. The judgment will be influenced by various parameters, and trust is content- correlative, trust to one aspect of object may not influence the distrust to another aspect of the same object, so trust only makes sense in certain context. Trust to object will change dynamically along with the update of trust information and the change of member's behaviors. Trust degree in virtual learning community is related to two aspects: the direct trust degree brought by target

member's behaviors in the community and recommendations come from other members. The measure and calculation of trust as well as the Algorithm of the authorization will be explained in brief.

3.1 Measure of Trust Degree

The direct trust brought by target member's behaviors in the virtual learning community can be defined as basic trust degree. The influential factors mainly include the times of the member visited the community, initiated discussion, participated discussion, contributed resources (we need to notice that there will be two-faces: contributing valuable resources and offering useless even vicious resources. We augment the influential factor's value if the resource is valuable, otherwise reduce.), and so forth. The influential parameters set could be expressed as:

$F=\{f1, f2, f3, f4\}$

The significations of the parameters are listed in table 1.

Table 1. Influential parameters sample for trust degree calculation

parameters	signification
f_1	the times of visiting the community
f_2	the times of initiating discussion
f_3	the times of participating discussion
f_4	the times of contributing resources

For the parameters listed in this table is just a sample to clarify the calculation process, it could be different which depends on the type and need of your system.

The basic trust degree is confirmed by virtue of calculating each influential factor, and expressed as:

$$T=\sum_{i=1}^{4} \lambda_i \cdot f_i \qquad (1)$$

λ_i is the weigh of influential factor i, f_i is the value of influential factor i, T is the basic trust degree of target member.

The community's general trust evaluation to the target member is defined as reputation, and it comes from the other members who have interacted with the target member. Generally speaking, except examining the target member's behaviors, his reputation should also be examined in virtual learning community in order to trust the target member. Other members take trust evaluation on target member according to their interaction histories with the target member. The value of reputation is decided by other members' trust recommendations, expressed as （**n** is amount of members in virtual learning community）:

$$R=\sum_{i=0}^{n} \omega_i \cdot r_i \qquad (2)$$

ω_i is the adoptive weight of member i, ω_i *is* related with the own trust degree of member i， r_i is trust recommendation values comes from member i， R is the final reputation value of target member.

So the final trust degree to target member, namely trust degree, can be expressed formally as:

$$T_{final}=\alpha \cdot T+(1-\alpha) \cdot R \qquad 0<\alpha<1 \qquad (3)$$

T_{final} is trust degree of target member, T is the basic trust degree brought by target member's behaviors in virtual learning community, R denotes the reputation value of the target member, α denotes the power of the basic trust value.

3.2 Trust-based Access Control Authorization Algorithm

The trust-based access control authorization could be described as the flow:

(1). Set roles: super administrator(SA), community administrator(A), expert E, teacher(T), student(S), visitor(V) (the super administrator is fixed, community administrator will inherit partial rights of the super administrator);
(2). Set rights: browse the community's resource(S1), participate in community's discussion(S2), upload resource(S3), download resource(S4);
(3). Set the trust degree threshold T*;
(4). Specify basic role(such as visitor), assign initial trust degree $T_{initial}$ to the role, the initial reputation value R is 0;
(5). Measure and calculate trust degree $T_{final}=\alpha \cdot T+(1-\alpha) \cdot R$
(6). If $T_{final} \geq T^*$, judge the role of the user, assign corresponding rights; Else, execute basic role's rights.

With this algorithm, we could set up trustworthy access control mechanism in virtual learning community. We have developed an archetypal module which could realize this authorization algorithm using C# as programming language, and inserted this module into existing virtual community, it works as we described.

4 Conclusion

In this paper, we integrated trust component into the existing access control mechanism, this is an attempt to bring behaviors-based trust management into E-Learning. We advanced a trust-based access control model in virtual learning community through research on the virtual learning communities and access control models existing at the present time, and described the calculation of the trust degree, bring forward trust-based access control authorization algorithm. This model did not depend on any idiographic trust model, for it may be suitable to other opening systems.

Many of these open issues and problems are intertwined and will require an integrated approach to be satisfactorily resolved, and this is the work we should make great efforts in the future.

Acknowledge

This paper is supported by NSFC of China (NO.60673010), partly supported by National Key Project of Scientific and Technical Supporting Programs Funded by Ministry of Science & Technology of China During the 11th Five-year Plan (NO 2006BAJ07B06）, and supported by the Cultivation Fund of the Key Scientific and Technical Innovation Project，Ministry of Education of China（NO705038）.

References

1. R. S. Sandhu, "Role-Based Access Control Models", I*EEE Computer*, 29(2):38-47,（Feb. 1996）
2. D. F.Ferraiolo and D.Richard Kuhn, "Ramaswamy Chandramouli", *Role-Based Access Control* (Artech House,2003), ISBN:1580533701
3. K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System", In: Proc. of the Tenth Intl. Conf. on. Information and Knowledge Management (*ACM CIKM*'01), 310~317(2001).
4. H .L. Ma, "sociological analyses of virtual learning community", *Distance Education in Chin* , 20-24(2006).
5. Z. K. Yang, H. B. Liu and Q. T. Liu, "Application Research for Role Based Access Control Technique in E-Learning", *Application Research of Computers,* 133-136（Oct. 2005).
6. S. Q. Zhang, D.X.Lu,Y.T.Yang, "Trust-Based Access Control in P2P Networks", *Computer Science*, vol.32 No.5, 31-33(2005)
7. E. Bertino, L. Khan, R. Sandhu and B. Thuraisingham, "Secure Knowledge Management: Confidentiality, Trust, and Privacy", *IEEE Transactions on Systems, Man and Cybernetics*, Part A: Systems and Humans, 36(3):429-438, (May 2006)