Access Control Based on Trust Policy in Open Grid Environment

Liting Gao, Zhenyan Wang
Computer Science and Technology Department, Hebei Institute of Architecture Civil Engineering
Zhang Jia Kou, China
gaoliting@163.com

***Abstract*—This paper proposed a model for user security management. This model can establish the blacklist and white list to achieve the control of the user subsequent actions through monitoring the changing of user trust level. It also can establish trust policy based on assets importance and user trust level, specify the relationship between user trust and assets value and take it as a dynamic trust constraint for access control. The experiments show that this model combines trust level with access control mechanism; it can enhance the user security management.**

Keywords-trust policy; trust constraint; blacklist; white list; grid computing

I. INTRODUCTION

The user is an indispensable factor in computer information system. However the current accident statistics for network security shows that most attacks are also caused by the user, for example, data leakage, unauthorized access and network intrusion. Strengthen the user security management can improve network security and enhance the overall performance of the network.

With the development of Internet, the traditional user management is already difficult to distributed systems. For example, in a grid computing, the traditional user management faces the following problems: 1) the number of user is very large and the uses are located in different security domain; 2) members in different security domain may not know each other; 3) the use's behavior is dynamic and uncertain (When, where and in what ways the users access to what resources is a dynamic and uncertain). For example, when the user conducts cross-domain access, he/she makes an honest act in a security domain meanwhile he/she makes a malicious act in another security domain. This dynamic and uncertain behavior will poses a great security risk to the system. Therefore, how to strengthen the user management is an important issue for enhancing the security of system and grid computing.

The static user management based on digital certificate at present has not met the security needs of open distributed systems. Based on the theory of information security, this paper proposed a model for user security management. This model combines trust level with access control mechanism to enhance the user security management. It can establish the blacklist and white list to achieve the control of the user subsequent actions through monitoring the changing of user trust level. It still can establish trust policy based on assets importance and user trust level, specify the relationship between user trust and assets value and take it as a dynamic trust constraint for access control.

II. USER TRUST MANAGEMENT

The trust calculation model based on user behavior risk assessment takes the most important asset of the system as a starting point, uses qualitative models to establish asset knowledge base, vulnerability knowledge base and threat knowledge base through asset identification, vulnerability identification and threat identification independently. This model can assess potential security risks in user history behavior and use specific formula to calculate the risk value of user behavior. And based on the risk value, the model calculates the user trust level dynamically. The model combines the security risk assessment with the trust mechanism to provide a decision-making basis for system. This basis can reflect the user credibility objectively and truly.

A. System Structure for User Trust Management

According to the trust calculation, the system can identify user credibility dynamically. On this basis, the user trust management model will establish user trust security policy and combine with the access control mechanism to guide the system authorization. This model can strengthen the user security control fundamentally, thus improve the system security. It includes two aspects: the user trust level management and the trust policy management.

The system structure of user trust management is shown in Fig.1 and Fig.2.

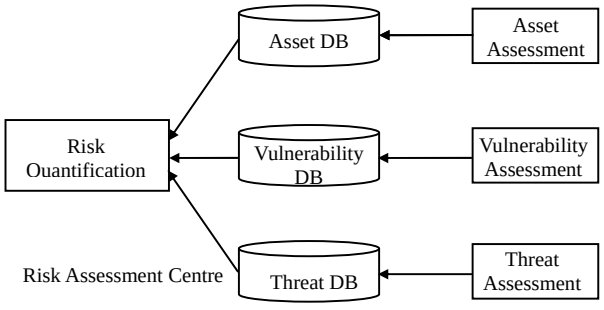

Fig.1 Assessment Center

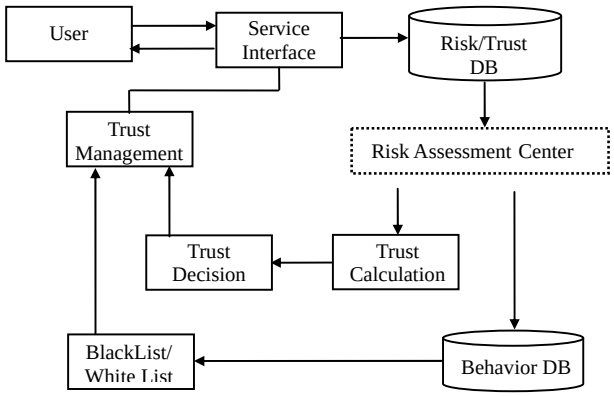

Fig.2 User Trust Management System Model

In Fig.2, the user trust management establishes user trust blacklist and white list through monitoring the change of user trust level. According to the user trust level and asset importance level, it develops the trust policy.

B. User Trust Level Management

The purpose of trust calculation model is to identify the user credibility correctly and provide a reference for the system security policy.

The calculation model proposed in this paper divides the credibility into five levels evenly according to the corresponding indicator value ranges. The classification of trust level can better develop the corresponding security policy. In this trust level classification, the user misuse or malicious use, which threat to assets is less, usually does not cause the user trust level changes. (The trust level changes from a higher level to a lower level). However in these situations, such as the user continuous misuses, the user made several smaller malicious threats within a period of time or the user made a malicious use that cause greater threat to the asset, will cause changes of user trust level. The five trust levels in this model are appropriate. If the classification is too much, the task of system will be more complicated, this will bring greater impact on system performance. In contrast, if the classification is too little, the safety boundary will be too larger; this will bring greater trouble for security control.

The main three steps in user trust level management is shown as follows:

1) By monitoring the change in user trust level, this model identifies the user who trust level has changed.

2) This model establishes the user trust blacklist and white list then strengthens the user's safety monitoring according to the blacklist and white list.

In the user trust level monitoring, if the user trust level drops, it shows that the user recent behavior has caused a loss to the system. The model will notifies the administrator to add this user to user trust blacklist and reduce its ability to access system resources. Then the model will strengthen the control for the user in order to avoid similar damage happen again. If the user trust level rises, it shows that the user recent behavior is legitimate and credible. The model will notifies the administrator to add this user to user trust white list and enhance its ability to access system resources in order to improve the utilization rate of resource.

The data structures of user trust blacklist and white list are included: user identification, user current trust level, update trust level and change of trust level (rise or drop).

In order to monitor the changes of user trust level, this model sets an event trigger on the user trust level database (its name is Utrust). The trigger rule is: when the trust level change attribute (its name is Tchanging) of Utrust changes, the model will make the follow steps:

```
WHEN Monitor (update| Tchanging in Utrust)
IF Value (Tchanging) = = 1 THEN
        add this user to the user trust white list
   ELSE IF Value (Tchanging) = = -1 THEN
        add this user to the user trust blacklist
   ENDIF
ENDWHEN
```

In the program code above, the meaning of Tchanging is shown as follow:

$$Tchanging = \begin{cases} 1, & \text{It represents the trust level rises} \\ 0, & \text{It represents the trust level doesn't change} \\ -1, & \text{It represents the trust level drops} \end{cases}$$

The establishment of user blacklist and white list are not only convenient for system to strengthen control for the user but also facilitate for releasing the information of these users in different security domains timely.

C. Trust Policy Management

In user security management, security policy is the key factor for guiding the user control. User management is not a single concept. It is often related to the other system security mechanisms, such as the access control mechanism. Trust policy management defines the relationship between the user credibility and the ability to access resource through the identification of user behavior. Trust policy management establishes the trust policy and take it as a dynamic constraint for access control mechanism. Trust policy management will guide the systems authorization; enhance the security management for user.

The access control mechanism is the primary means for supporting system security. It can restrict access to the system resources in order to prevent unauthorized user. The existing access control model for distributed applications gives the appropriate permissions according to the user identification based on pre-established access control policy. Although the authorized model it used can achieve the distributed processing for authority, it difficult to keep abreast of the user actual behavior in this distributed, dynamic grid computing. It is difficult for the existing access control mechanism to prevent those sabotages that malicious user made with a legal status. Obviously, it is not appropriate that using access control mechanism simply in the grid computing. New scheme must be introduced in the access control mechanism for grid computing. This new scheme should be able to implement access control according to user trust level rather than its identification

under the condition that the user credibility can not be identified. It will provide security guarantees for the collaboration between the users in different security domain.

In the open distributed system, trust mechanism provides an effective safeguard: it can establish different trust relationships between users or between users and resources in the absence of an authoritative third-party.

Trust mechanism will help system to make security decision. For example, the system can decide whether to allow users to access or decide the user access ability in a particular state. Therefore the purpose of this model proposed in this paper is to determine the user access ability dynamically and form a security policy based on trust according to the change of user trust level. This model can better meet the needs of the user management and enhance system security in the distributed dynamic environment.

In order to better control malicious user destructive behavior and protect sensitive resources, trust policy management establishes appropriate security policy according to user trust level and assets importance level. Every rule in trust policy states the access condition for every kind of assets that has specified value or importance. It includes user trust level, user respective relationships and others system security requirements. For example, only when the user reaches a minimum requirement of trust, he can access some kind of asset or gain specific access authority to some kind of asset.

The trust policy database includes these fields as follow: policy number, asset identification, asset value level, user trust level, user credibility, user respective relationship, context environment and validity.

As a dynamic trust constraint, the trust policy combines trust mechanism with access control mechanism together. It further enriches the policy of access control and enhances the constraints on the system authorization. Trust policy associates the user access ability with his historical behavior. It can ensure the user specific access ability, at the same time it also can constrain user behavior. Trust policy promotes the formation of benign cycle that users have ability to access resources. It can potentially improve the system environment and improve system security. The trust policy is consistent with the dynamic characteristics of grid computing.

III. Examples and Results Analysis

The model proposed in this paper takes the teaching-affair management subsystem as an experimental object in campus grid experimental platform. The teaching-affair management subsystem is responsible for the maintenance and management of a variety of important teaching resources, personal information and student portfolios. It distributes and records the teaching tasks implementation. The experiments tracked and recorded four users behaviors in fifteen days. In order to distinguish the bad user and control his malicious behavior effectively, the model proposed in this paper made risk assessment of user history behavior and calculated the trust level firstly. This work can provide objective decision support for the user trust management. The experiments results are shown in Fig.3.

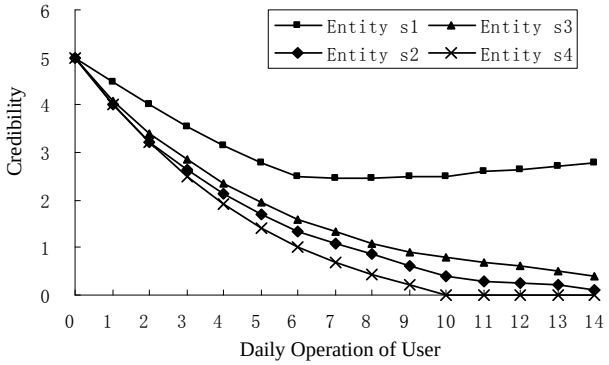

Fig.3 User Credibility Curve Based on Behaviors

Based on the experimental results shown in Fig.3, the experiments tested the changes of the user trust level and tracked the implementation of trust policy.

In the experiments, the model calculated the changes of the users trust level dynamically by using the trigger on the Utrust database. Fig.4 is shown the changes of the four users trust levels in fifteen days.

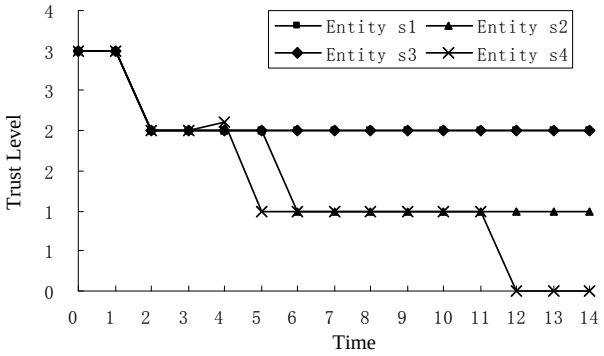

Fig.4 User Trust Level Curve

It can be concluded from the Fig.4, because of the changes of trust level, the user s1, s2, s3 and s4 are all added into user trust blacklist. According to changing curves of user trust level shown in Fig.4, the administrator is able to understand the users trust status more clearly and control the changes of user behavior in the system. The user trust level curve can help administrator detect the change rule about user behavior and take appropriate measures to enhance system security.

The experiment has comparison tests, in which one has a trust constraint proposed in this paper and anther has none. The comparison test verified the identification that the system made when multiple users simultaneous access to related resources. This test includes two purposes: 1) it can verify the user trust blacklist and white list, which are created according to the changes of trust level. 2) it can detect the constraint on the system authorization made by trust policy.

In the comparison test, fifty test users and fifty test resources were built and user credibility, asset importance

level, user trust blacklist, user trust white list and trust policy are all set. To simplify the test, the permissions validation of access control in the test only required that the user trust level was not lower than the threshold set by related resources. And the test set that there is 30% malicious access in each user behavior. Based on the above conditions, the experiments tested the number of interaction failures, which occurred when the system couldn't identify malicious access under the circumstances with trust constraint. And the same experiments were done under the circumstances without trust constraints. The experimental results are shown in Fig.5.

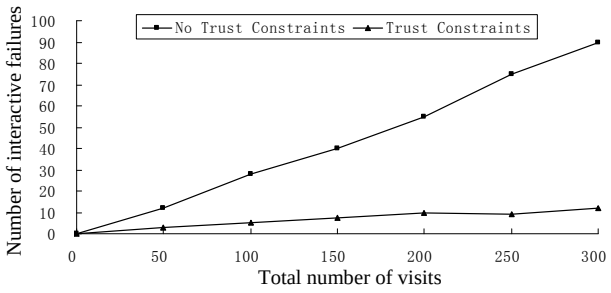

Fig.5 User Access Contrast Test Based on Trust Constraint

It can be concluded from Fig.5, the system can block those malicious accesses effectively according to the changes of user trust level and significantly reduce the number of interactive failure visits in the trust constraint circumstances. The trust constraint can reduce system overhead caused by processing interactive failure access and the security risks caused by processing malicious access. Because the system without trust constraint will not have the pre-treatment of user trust, the number of interaction failures will increase correspondingly when the malicious access become more.

The user trust blacklist, white list and trust policy can provide security guidance for the user management. As the trust constraint for access control, they make up the deficiency of existing access control mechanisms in the distributed dynamic environment, enhance the system specification for user behavior, and improved the system security.

IV. CONCLUSION

This paper designs a user security management model based on trust constraint. This model implements the user trust management based on the trust calculation about user history behavior. Through monitoring the changes of user trust level, this model establishes user trust blacklist and white list in order to better control the user subsequent actions firstly. Secondly, this model establishes the trust policy based on user trust level and asset importance level, it defines clearly the relationship between user trust and asset value to better guide the system authorization. The experimental results show that as trust constraint, the user trust blacklist, white list and trust policy established by this model enrich the access control mechanism and enhanc the constraints of system authority. This model makes it possible that the user access ability is associated with his history behavior. This model enhances the system control of user behaviors and improves the system security. It is also fit for the user security management in the parallel computing and cloud computing.

REFERENCES

[1] Liu Liming. Study on the Key Issue of Grid User Management: [dissertation]. Beijing.Graduated University of Chinese Academy of Sciences, 2005

[2] Xu Yujie. The Research of a Trust Model-Based Task Scheduling Algorithm for Data Grid: [dissertation]. Dalian.Dalian Maritime University, 2010

[3] Tu Jinde, Qin Xiaolin, Dai Hua. Double-authorization Chain Sets Based Access Control Model [J]. Computer Science, 2010, 7: 160-164

[4] Li HaiHua, Du Xiaoyong, Tian Xuan. A Capability Enhanced Trust Evaluation Model for Web Services [J]. Chinese Journal of Computers, 2008, 31(8): 1471-1477

[5] Li Xiaoyong, Gui XiaoLin. Research on Dynamic Trust Model for Large Scale Distributed Environment [J]. Journal of Software, 2007, 18(6):1510-1521

[6] Wu Zhijun, Yang Yixian. Research of Indicator for Information Assurance Evaluation. [J]. Computer Engineering, 2010, 7: 7-10

[7] Yang Xiaoming, Luo Hengfeng, Fan Chengyu. Analysis of risk evaluation techniques on information system security [J]. Journal of Computer Applications, 2008, 8:1920-1923

[8] Wei Yong, Lian Yifeng. A Network Security Situational Awareness Model Based on Log Audit and Performance Correction [J]. Chinese Journal of Computers, 2009, 4:763-772