Fine-grained access control model based on sensitivity calculation by fuzzy mathematics

Yuntao Wang$^{1,2,*}$

$^1$ Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, China
$^2$ School of Cyber Security, University of Chinese Academy of Sciences, Beijing, 100049, China

* Corresponding author’s e-mail: wangyuntao@iie.ac.cn

Abstract. Access control regulates the behavior of legitimate users in the security domain to access and operate resources, and ensures that resources are not used by unauthorized users, in order to protect resources. With the maturity of security label technology, new requirements are put forward for access control of multi-level security network. In this paper, a fine-grained access control model based on sensitivity calculation by fuzzy mathematics is proposed. Fuzzy mathematics is used to comprehensively calculate the sensitivity level of users and files based on their security label attributes. On this basis, the mandatory access control policies are set to make the access control mechanism between users and files more reasonable.

1. Introduction

With the rapid development of Internet, the resource management of single security domain can not meet the increasing demand of distributed resource sharing. Access control provides a good security mechanism for resource sharing in the security domain, and avoids unauthorized access of illegal users to resources[1]. Security labels are the basis of mandatory access control in multi-level security networks. In a multi-level security network, both subject and object have multiple security attributes, and access control based on security labels can achieve the requirements of fine granularity and precise control.

Since the concept of fuzzy random variable was first put forward in the literature[2] in 1978, the fuzzy random variable has been widely concerned by scholars at home and abroad. In the literature[3,4], the fuzzy evaluation method is applied to the evaluation of system safety condition, and the effectiveness of the evaluation method is verified by several examples. To some extent, sensitivity has uncertainty and fuzziness, and it needs to determine the strategy when making access control decisions. Therefore, it can be studied by using fuzzy method.

This paper proposes a fine-grained access control model based on sensitivity calculation by fuzzy mathematics. On the basis of fuzzy mathematics theory, the sensitivity level of target file and target user is determined comprehensively according to multiple security label attributes. When the user initiates the access request, the sensitivity level of the user is compared with the sensitivity level of the file, then different access rights are granted according to the mandatory access control policy.

2. Access control

Access control is the main strategy of information security prevention and protection, its main task is to ensure that the system resources are not used illegally[5]. In the development process of access control
technology, due to the need of data security in the system, many typical access control methods have been proposed, the most representative models among them are Discretionary Access Control, Mandatory Access Control and Role-Based Access Control.

Discretionary Access Control (DAC) is a control method that the owner of the object can freely authorize to decide whether the object can be accessed by other subjects[6]. The core idea of DAC model is that the owner of the controlled object manages the access rights for the object. In autonomous access control, the configuration of permission policy is more flexible, and the way to assign permission by the object owner is simple and direct.

Mandatory Access Control (MAC) is a control method in which the system determines the categories and levels of subjects and the matching relationship between subjects and objects[7]. There are two implementation models of MAC. One is Bell-Lapadula (BLP), in which the subject with low security level has write permission to the object with high security level, and the subject with high security level has read permission to the object with low security level. The other is the Biba model, in which the subject with high security level has write permission to the object with low security level, and the subject with low security level has read permission to the object with high security level.

Role-Based Access Control (RBAC) is a control method that establishes a role set between user and access permission, which is assigned by a special permission manager, associates the user with the role, in order to make the user access the access permissions owned by the associated Role[8]. RBAC model realizes the isolation between subject and object, and through the introduction of roles, the concept of permission group is completed. The granting and revocation of permissions will not affect the subject and object themselves.

With respect to multi-level security network in our country, BMB17 and GB17859-1999 put forward many specific guidance on access control requirements. The consistent content of two standards is that with the improvement of security levels, access control level and particle size are increased. It requires that access control mechanism can achieve complex fine-grained mandatory access control. Security label is the basis of mandatory access control in multi-level security network. In multi-level security network, both subject and object have multiple security attributes. Access control based on security label can achieve fine-grained and precise control requirements.

3. Fine-grained access control model based on sensitivity calculation by fuzzy mathematics

Fuzzy mathematics is a mathematical method to study the regulation of quantity change which belongs to uncertainty and has fuzziness. Fuzzy mathematical system theory can skillfully reveal the essence and laws behind complex phenomena and provide quantitative calculation methods for some seemingly unrelated subjects.

This paper proposes a fine-grained access control model based on sensitivity calculation by fuzzy mathematics, and its architecture is shown in Figure 1. In a multi-level security network with a large number of sensitive files, the sensitivity level of files can be comprehensively calculated according to their security label, and the calculation results can be used as the basis for file storage and access. According to the membership function of fuzzy mathematics, the sensitive level of files is determined, and the sensitive level is classified to ensure more accurate access control. In the multi-level security network, the user also has the security label, and its access level is calculated in the same way, which is used as the basis for accessing files.
3.1. Sensitivity calculation by fuzzy mathematics

According to the security label attribute of the target file, the steps to determine its sensitivity level are as follows:

**Step 1** Establish the factor set.

The security label attributes of file constitute the theory domain of factor set \( U = \{u_1, u_2, \ldots, u_m\} \), in which the element \( u_i \) represents the \( i \)th factor affecting the evaluation object. In this paper, we set the factor set for evaluating the sensitivity level of file as \( U = \{u_1, u_2, u_3, u_4, u_5\} \), where \( u_1 \) represents the security level, \( u_2 \) represents the type of file, \( u_3 \) represents the confidentiality period, \( u_4 \) represents the unit, and \( u_5 \) represents the person in charge.

**Step 2** Establish the evaluation set.

Determine the theory domain of evaluation set \( V = \{v_1, v_2, \ldots, v_n\} \), where the element \( v_j \) represents the \( j \)th evaluation result, which can be represented by different grades, comments or numbers according to the needs of the actual situation. In this paper, we set the evaluation set for evaluating the sensitivity level of file as \( V = \{v_1, v_2, v_3, v_4\} \), where \( v_1, v_2, v_3, v_4 \) respectively represents the sensitivity level I, II, III and IV.

**Step 3** Establish the fuzzy relational matrix between factor set and evaluation set.

The target file is evaluated by each factor \( u_i \ (i = 1, 2, \ldots, m) \) to determine its sensitivity level one by one, which means that the membership degree \( R_i \) of the target file to the fuzzy subset of the sensitivity level can be viewed from a single evaluation factor, and the fuzzy relational matrix \( R \) can be obtained.

\[
R = \begin{bmatrix}
R_1 \\
R_2 \\
\vdots \\
R_m
\end{bmatrix}
= \begin{bmatrix}
\mathcal{r}_{11} & \mathcal{r}_{12} & \cdots & \mathcal{r}_{1n} \\
\mathcal{r}_{21} & \mathcal{r}_{22} & \cdots & \mathcal{r}_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
\mathcal{r}_{m1} & \mathcal{r}_{m2} & \cdots & \mathcal{r}_{mn}
\end{bmatrix}
\] (1)

where the element \( \mathcal{r}_{ij} \) which is located in row \( i \) and column \( j \) of matrix \( R \) represents the membership degree of the fuzzy subset \( v_j \) of sensitivity level judged by the target file from the evaluation factor \( u_i \).

For the measured value \( x \) of each factor \( u_i \) in \( U \), the membership degree of sensitivity level I-IV is calculated according to the membership function. Sensitive files is usually partial small fuzzy distribution, for example, the number of files with high sensitive level is small while the number of files with high sensitive level is big. So our model adopts the partial small fuzzy function, which is commonly
known as "T distribution", to calculate the membership degree. The formula is as follows:

\[ \mu_A = \begin{cases} 
1, & x \leq a \\
\frac{1}{e^{-k(x-a)}}, & x > a 
\end{cases} \]  

If the original data is non-numerical data, the range normalization method is adopted for processing. The formula is as follows:

\[ x'_{ij} = (x_{ij} - \min_{1 \leq i \leq n} x_{ij}) / \Delta x_j \quad (i = 1, 2, ..., n; j = 1, 2, ..., m) \]  
\[ \Delta x_j = \max_{1 \leq i \leq n} x_{ij} - \min_{1 \leq i \leq n} x_{ij} \quad (j = 1, 2, ..., m) \]  

Take an instance, the attribute of security level can be divided into top-secret, secret, confidential and public. Its original attribute can be quantified as (1,2,3,4), then we can obtain (0,0.33,0.67,1) by the range normalization method.

In the example of this paper, the fuzzy relation matrix is set as:

\[ R = \begin{bmatrix} 
R_{11} & R_{12} & \cdots & R_{14} \\
R_{21} & R_{22} & \cdots & R_{24} \\
\vdots & \vdots & \ddots & \vdots \\
R_{51} & R_{52} & \cdots & R_{54} 
\end{bmatrix} = \begin{bmatrix} 
0.35 & 0.39 & 0.22 & 0.04 \\
0.17 & 0.35 & 0.39 & 0.09 \\
0 & 0.30 & 0.44 & 0.26 \\
0.09 & 0.22 & 0.30 & 0.39 \\
0.43 & 0.35 & 0.22 & 0 
\end{bmatrix} \]  

Step 4 Establish weight vector.

Among the security label attributes, different attributes have different influences on the sensitivity of file, so it is necessary to introduce the weight vector \( A = \{a_1, a_2, \cdots, a_m\} \) to reflect the influence of different attributes on the evaluation results. The value of weight vector can be obtained by expert experience or Analytic Hierarchy Process(AHP) method.

In the example of this paper, the weight vector is set as \( A = \{0.35,0.35,0.1,0.1,0.1\} \).

Step 5 Calculate the result of fuzzy evaluation.

\[ B = A \cdot R = (b_1, b_2, \cdots, b_n) \]

In the example of this paper, the fuzzy vector finally obtained is \( B = A \cdot R = (0.23,0.35,0.31,0.11) \).

Step 6 Discriminate.

The maximum membership principle is used to discriminate the sensitivity level of the target file. In the example in this article, the sensitivity level of the target file is level II.

In the multi-level security network, the user also has the security label, so the sensitivity level of user can be calculated in the same way, which is used as the basis for accessing files.

3.2. Fine-grained access control model

Based on the sensitivity calculation above, an access level is assigned to each user and file, and the system determines the access mode according to the sensitivity level of the subject and object. Access modes include:

① Read down: Read operation when the sensitivity level of user is greater than the sensitivity level of file;
② Write up: Write operation when the sensitivity level of user is smaller than the sensitivity level of file;
③ Write down: Write operation when the sensitivity level of user is greater than the sensitivity level of file;
④ Read up: Read operation when the sensitivity level of user is smaller than the sensitivity level of file.

Access control granularity specifies the level at which users access resources and the extent to which the system records user access behavior, such as directory-based authorization granularity, menu-based authorization granularity, file-based authorization granularity, and so on. According to the granularity level, the security system is divided into fine-grained access control system and coarse-grained access control system. The choice of granularity of access control plays an important role in user behavior tracking and auditing. Generally, it is more practical to adopt coarse-grained access control for systems with low security requirements, while for systems with high security level, such as military systems, it
is more inclined to carry out fine-grained access control.

At present, most of the access control mechanisms in sensitive applications refer to several mature models, such as mandatory access control and role-based access control. In business processing, most of them allocate some roles for users on the basis of user's strong identity authentication to get access to some resources. The granularity of setting access control policy based on role is coarse for the reason that a role often contains multiple users. Besides, the mandatory access control is not allowed to be modified, resulting in the inflexibility of permission configuration, which can not meet the needs of multi-level security network.

According to the multiple security label attributes of users or files, the sensitivity level of users and files are comprehensively calculated by fuzzy mathematics, and the mandatory access control policy is set on this basis, which can make the access control mechanism between users and files more reasonable. It meets the actual needs of multi-level security network, which strictly carries out fine-grained control and has more flexible permission configuration. When new requirement appears, there is no need to redefine the level of subject and object, since the sensitivity level can be automatically calculated according to their security label attributes.

4. Conclusions
This paper employs fuzzy mathematics theory to evaluate the sensitivity of users and files, and establishes a fine-grained access control model suitable for multi-level security networks. According to the access control rules, the user's access control to the file is determined by the user permissions and file attributes. Firstly, the sensitivity of the target file is determined by fuzzy evaluation to determine the access control level of the file. Then fuzzy evaluation is also used to determine the authority level of the user. Finally, the mandatory access control domain is set up and the fine-grained access rules are determined to make the access control mechanism between users and files in multi-level security network more flexible and reasonable.

References
[1] Crampton, J. (2003) Specifying and enforcing constraints in role-based access control. In: Eighth ACM Symposium on Access Control Models and Technologies. Como. pp. 43-50.
[2] Kwakernaak, H. (1979) An algorithm for rating multi-aspect alternatives using fuzzy sets. Automatica, 15: 615-616.
[3] Sun, L.Z., Yang, F. (2009) Variable weight fuzzy method for evaluation of uncertain information. Mathematics in Practice and Theory, 39: 12-17.
[4] Xie, J.J., Liu, C.P. (2000) Fuzzy mathematics method and its application. Huazhong University of Science and Technology Publishing, Wuhan.
[5] Shen, H.B., Hong, F. (2005) Survey of research on access control model. Computer Application Research, 6: 9-11.
[6] Graham, G.S., Denning, P.J. (1971) Protection: principles and practice. In: Spring Joint Computer Conference. New York. pp. 417-429.
[7] Bell, D.E., LaPadula, L.J. (1996) Secure computer systems: a mathematical model. Journal of Computer Security, 4: 229-263.
[8] Sandhu, R.S., Coyne, E.J., Feinstein, H.L., et al. (1996) Role based access control models. Computer, 29: 38-47.