A cross-domain authorization access control model based on security label attribute

Yuntao Wang\textsuperscript{1,2,*}

\textsuperscript{1} Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, China
\textsuperscript{2} School of Cyber Security, University of Chinese Academy of Sciences, Beijing, 100049, China

\textsuperscript{*} Corresponding author’s e-mail: wangyuntao@iie.ac.cn

Abstract. This paper proposes a minimum diffusion and cross-domain security authorization strategy based on security label, which solves the security problems of minimum visible range and cross-domain authorization in access control mechanism. The strategy makes full use of security label attributes, introduces multi-level constraint mechanism in access control, and makes the scope of knowledge controllable in cross-domain authorization. Through the experimental validation of different security domain scenarios, compared with the traditional access control mechanism, the diffusion speed of sensitive files in the access control based on security label attributes is significantly reduced. If the number of security labels is set as $N_{\text{label}}$, and each label has $N_{\text{scale}}$ values, the file diffusion speed of the network is only $\frac{1}{\prod N_{\text{scale}}}$ times that of the linear diffusion speed.

1. Introduction
Sensitive file leakage belongs to Data Leak Prevention (DLP). There are many kinds of protection measures in DLP technology, including storage protection of static data, transmission data leakage and application system data leakage [1]. According to different application fields and technical implementation methods, DLP technology gradually forms different technical solutions, including hybrid identity management, access control, security log and event management, filtering protection, firewall and so on [2]. Using access control to protect data leakage is one of the main ideas.

With the rapid expansion of the network scale, the sensitive attributes of sensitive information are marked in the multi-level security network, and the corresponding improved access control mechanisms are proposed according to the sensitive attributes, which effectively solves some problems such as system integration and preventing the diffusion of sensitive files. The current cross-domain authorization model mainly relies on role association in RBAC [3] and dynamic role transformation in IRBAC [4] to realize file flow and authorization between different domains. This paper mainly discusses the role of security labels in data leakage protection based on access control, in order to enrich the theory and practice of data leakage protection.

2. Detailed mechanism and algorithm design

2.1. Access control constraints based on security label attribute

Attribute can be defined separately as the content of the security label. Its access control constraint is...
formalized as follows:

**Rule 1.**

\[
can\_access(s, o, e, p) \leftarrow f\_\text{decide}(\text{ATTR}s(s), \text{ATTR}s(o), \text{ATTR}s(e), \text{ATTR}s(p))
\]

The label **Unit** and **Dept** represent the unit and department of the user. The access control constraint is formalized as follows:

**Rule 2.**

\[
can\_access(s, o, e, p) \leftarrow f\_\text{decide}\left(\left(\text{Attr}_{\text{Unit}}(s) = \text{Attr}_{\text{Unit}}(o)\right) \cup \left(\text{Attr}_{\text{Dept}}(s) \leq \text{Attr}_{\text{Dept}}(o)\right)\right)
\]

The label **Business** represents the business related attributes of the user. The access control constraint is formalized as follows:

**Rule 3.**

\[
can\_access(s, o, e, p) \leftarrow f\_\text{decide}(\text{Attr}_{\text{Business}}(s) \supseteq \text{Attr}_{\text{Business}}(o))
\]

**2.2. Minimum diffusion strategy**

In multi-level security network, minimizing the diffusion range is the key index to prevent file leakage, which is also the main purpose of this model. The specific strategies are as follows:

**Step 1.** Sensitive files are divided into file sets according to security attributes, and the same set has the same visible range.

**Step 2.** The drafter selects the user as the visible range for a file group, and the user's selection range must match the sensitive file attribute.

**Step 3.** The security management department reviews the optional visible range of the file group.

**Step 4.** When the file is generated, select the file set, select the sensitive level, basis, and other contents, and select the appropriate visible range from the list of users with the largest visible range selected in step 3. The visible range cannot be expanded at will.

The minimum diffusion policy based on security label is formalized as follows:

**Rule 5.**

\[
\text{User}_{\text{permit}} = \{\text{User}_1, \text{User}_2, \text{User}_3, ..., \text{User}_i | \forall \text{User}_i = (\text{User}_i, S\_\text{Level} \\
\geq \text{Docs} \cdot S\_\text{Level}, \text{User}_i, \text{Unit} \in \text{Docs} \cdot \text{Unit}, \text{User}_i, \text{Dept} \\
\geq \text{Job} \cdot \text{Dept}, \text{User}_i, \text{Business} = \text{Job} \cdot \text{Business}, \text{User}_i, \text{ProcTeam} \\
\subseteq \text{Job} \cdot \text{ProcTeam}, \text{User}_i, \text{Business} \supseteq \text{Job} \cdot \text{Business})\}
\]

**2.3. Cross-domain transfer strategy**

The purpose of Security Attributes based Cross-domain Authorization (SABCDA) is to solve authorization conflicts by using the semantics of security attributes. The security attributes of sensitive files are compared with the related security attributes defined by the target company, and the optimal value is selected and approved by the security department.

Suppose that the sensitive file *Doc* is authorized by *Unit1* to *Unit2*. The initial value of *Threshold* is set to 0 and then its value is obtained by comparing \( \text{ATTR}(S\_\text{Level}, \text{Basises}, \text{Business}, \text{Job}, ...) \) of *Doc* with the data of the user group of the target unit. If all the value are same, the value of *Threshold* is set to 1 and the cross-domain authorization is granted to the target user group. Since exact matching is very difficult, the threshold can be limited to a range, such as \([0.8, 1]\). The formula is as follows:

**Rule 6.**
Users = \{User_1, User_2, User_3, ..., User_i\} \forall User_i
= (User_i, S\_Level
\geq Docs\_S\_Level, Threshold((Docs\_Basises~User_i, Basises)
\geq 0.8 && (Docs\_Job~User_i, Job)
\geq 0.8 && (Docs\_Business~User_i, Business) \geq 0.8 ) = true)}

3. Validation and analysis

3.1. Validation environment

The environment mainly includes three different Security Domains (SDomain). Each of them is divided into three sub domains according to different business. Each sub domain has three users, representing high, medium and low security levels respectively. Each user generates a fixed number of sensitive documents as the basic data of flow test. In the multi-level security network, the sender of the file determines the next sending purpose of the file. In this experiment, it is assumed that the sender of all files has the right to send sensitive files to all other users, so as to determine the maximum diffusion range of sensitive files.

1) Users of each security domain can send files to all users of the domain, and each sub domain can send files to users of common business sub domains of other security domains with superior subordinate relationship. Therefore, the security domain can be regarded as a full flow diagram, and the sub domains of different security domains also have flow relationship, which is generally in line with the actual flow situation of multi security domain network. The structure is as shown in Figure 1.

Figure 1. The actual flow process of files in the security domain.

The horizontal and vertical axes of the connected matrix are as follows:
[SubDm1a, SubDm1b, SubDm1c, SubDm11a, SubDm11b, SubDm11c, SubDm12a, SubDm12b, SubDm12c]
And the connectivity equivalence matrix is shown in Figure 2, where "1" represents that the request and transmission can be reached, "0" represents that the request and transmission cannot be reached:
2) The users of three level in Subdlb which belongs to SDomain11 generates n1 confidential files, n2 confidential files and n3 internal files respectively. Other security labels, such as confidentiality period, basis, drafter, time, status, business, task and matters, are configured by default according to the relevant content of the subdomain, and the file sending process starts, Through the Depth First Search (DFS) algorithm of graph, we can get the flow process of files.

3) The users of three level in SubDmlb belong to different tasks or projects respectively. The flow rules of sensitive documents are divided according to tasks or projects of LBAC whose definition will be given in the following section, and other conditions are unchanged. The flow process of documents is shown in Table 1, where “ACM” denotes access control mechanism.

Table 1. The flow process of documents.

| No. | ACM  | 1 Flow | 5 Flows | 10 Flows | m Flows |
|-----|------|--------|---------|----------|---------|
| 1   | DAC  | 2(n1+n2+n3) | 6(n1+n2+n3) | 11(n1+n2+n3) | (m+1)(n1+n2+n3) |
| 2   | MAC  | n1+n2+2n3   | 2n1+6n2+9n3  | 4n1+8n2+12n3  | (m+3+1)n1+2(m/3+1)+(m+1)n3 |
| 3   | RBAC | n1+n2+2n3   | 2n1+6n2+9n3  | 4n1+8n2+12n3  | (m+3+1)n1+2(m/3+1)+(m+1)n3 |
| 4   | LBAC | n1+n2+n3    | n1+n2+n3     | 2(n1+n2+n3)   | (m/9+1)(n1+n2+n3)  |

3.2. Analysis of validation results

1) The diffusion rule of sensitive files of different access control mechanisms is based on the linear speed of file number and flow times, and all access control mechanisms will not be improved at the diffusion level.

2) Autonomous access control (DAC) is the most free access control mechanism. In untrusted networks, it does not restrict file diffusion, and can be regarded as linear diffusion.

3) Mandatory access control (MAC) is equivalent to the sensitive level constraint of security label. Its file diffusion converges to the sensitive level. If the sensitive level of network is $N_{secretlevel}$, the diffusion speed of sensitive files is negatively related to it, i.e., $\frac{1}{N_{secretlevel}}$ times that of the linear diffusion.

4) Role based access control mechanism (RBAC) is similar to mandatory access control, which can significantly reduce the diffusion of sensitive files. If the number of roles in the network is $N_{role}$, the file diffusion is carried out strictly according to the role constraints, and the diffusion speed is negatively related to the number of roles, i.e., $\frac{1}{N_{role}}$ times that of the linear diffusion.

5) The theoretical diffusion speed of security label based access control (LBAC) sensitive files can be significantly reduced. If the number of security labels in the network is $N_{label}$, and each label has $N_{scale}$ values, the file diffusion speed is $\frac{1}{N_{scale}}$ times that of the linear diffusion speed. The fuzzy membership degree problem can be used to further study the access control mechanism of files with security labels.

4. Conclusions

This paper focuses on the research of the minimum authorization policy in the access control mechanism based on security labels. The formal description of the access control mechanism of security labels is
included in the traditional description. The meaning of each label is used to fully explore its control significance in the diffusion of sensitive files. On this basis, the minimum file diffusion and cross-domain security authorization mechanism are formed, and the theoretical verification is carried out. Through the validation, the theoretical diffusion speed of sensitive files in the security label based access control model proposed in this paper can be reduced, which provides an important reference for the increasingly complex security access control scenarios in the industry.

References
[1] Peng, W.P. (2011) Research on some key technologies of data leak preventon based on trusted computing platform. Beijing University of Posts and Telecommunications, Beijing.
[2] Hammer, H., Kongsgard, K.W., et al. (2015) Automatic Security Classification by Machine Learning for Cross-Domain Information Exchange. In: Military Communications Conference. Tampa. pp. 1590-1595.
[3] Xu, S.W., Zhang, X.S., et al. (2013) Design and implementation of security label for electronic documents. Journal of Beijing Electronic Science and Technology Institute, 21: 56-59.
[4] Wang, S.L. (2000) Research on fine-grained multi-domain access control security model for Android System. Information Engineering University, Zhengzhou.