Journal of Southeast University (English Edition) Vol. 24, No. 3, pp. 393 – 396 Sept. 2008 ISSN 1003—7985

Multi-level access control model for tree-like hierarchical organizations

Yu Guangcan Li Ruixuan Lu Zhengding Mudar Sarem Song Wei Su Yonghong

(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: An access control model is proposed based on the famous Bell-LaPadula (BLP) model. In the proposed model, hierarchical relationships among departments are built, a new concept named post is proposed, and assigning security tags to subjects and objects is greatly simplified. The interoperation among different departments is implemented through assigning multiple security tags to one post, and the more departments are closed on the organization tree, the more secret objects can be exchanged by the staff of the departments. The access control matrices of the department, post and staff are defined. By using the three access control matrices, a multi granularity and flexible discretionary access control policy is implemented. The outstanding merit of the BLP model is inherited, and the new model can guarantee that all the information flow is under control. Finally, our study shows that compared to the BLP model, the proposed model is more flexible.

Key words: multi-level access control; hierarchical organization; multiple security tags

The tree-like hierarchical organization contains a serial of hierarchical departments. Every department administers lower departments and accepts administration from higher departments. The tree-like hierarchical organization model is shown in Fig. 1[1]. For convenient description, the organization model is simplified as shown in Fig. 2. In this figure, the uppermost root department represents the organization in Fig. 1. This organization model is often adopted by governments or armies and it is necessary to conduct research on rigorous access control models for the organization model.

The famous BLP model was proposed by Bell and LaPadula[2], and it was widely used to formally describe or prove the security character of computer systems[3-8]. Later, the BLP model was expanded and applied to the SecLinux operation system[9]. The BLP model synchronizes DAC and MAC policies elegantly.

The BLP model and its expanded models are excellent access control models, but when these models are applied to a tree-like hierarchical organization, the following problems appear:

1) If there are a lot of departments in an organization, giving categories to every subject and object is a troublesome work.

2) Since every subject has only one security tag which consists of category and classification, it is very difficult for users in different departments to intercommunicate.

3) In the BLP model, security tags are given to subjects directly. If multi users work together on the same post and have the same security tag, the security tag must be repeatedly given to every user.

4) The access control matrix is too rigid. It controls access solely to objects for every subject, and it cannot control access to objects more roughly, such as users in the same department. Also, operating on the access control matrix is a troublesome work.

To solve the problems of the BLP model mentioned above, we propose a multi-level access control model for tree-like hierarchical organizations.

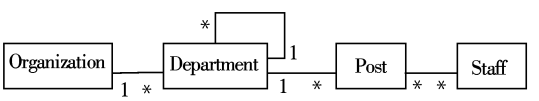

Fig. 1 Tree-like hierarchical organization model

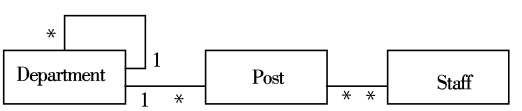

Fig. 2 Simplified tree-like hierarchical organization model

1 Basic Components of the Multi-Level Access Control Model

The basic components of our multi-level access control model include departments (DP), posts (P), staff (S), security tags (T), objects (O), access matrices (MS, MD, MP), access rules (ω), and sessions. Detailed definitions of the above components are as follows:

- $\mathrm{DP} = \{\mathrm{dp}_1, \mathrm{dp}_2, \ldots, \mathrm{dp}_u\}$ is the set of departments;
- $P = \{p_1, p_2, \ldots, p_w\}$ is the set of posts;
- $S = \{s_1, s_2, \ldots, s_n\}$ is the set of staff;
- $\mathrm{DH} \subseteq \mathrm{DP} \times \mathrm{DP}$ is a partial relation on DP called department hierarchy or department subjection relation and it is written as $\geqslant_d$. DH must satisfy the following conditions: 1) If $\mathrm{DP} \neq \varnothing$, then $\exists\, d_0 \in \mathrm{DP}$, $\forall\, d_i \in \mathrm{DP}$, $d_0 \geqslant_d d_i$, where d_0 is the highest hierarchical department, called root department; 2) $\forall\, d_i, d_j, d_k \in \mathrm{DP}(j \neq i, k \neq i)$, if $d_j \geqslant_d d_i$, $d_k \geqslant_d d_i$, then $d_j \geqslant_d d_k$, or $d_k \geqslant_d d_j$. This means, except for the root department, every department has only one direct upper department. $\forall\, d_i, d_j \in \mathrm{DP}$, if $d_j \geqslant_d d_i$ and $i \neq j$, then, this can be written as $d_j >_d d_i$;
- posts: $\mathrm{DP} \rightarrow 2^P$ is a function that maps each department dp_i to the subset of P ($\mathrm{posts}(\mathrm{dp}_i)$). Since $\forall\, d_i, d_j \in \mathrm{DP}(i \neq j)$, $\mathrm{posts}(d_i) \cap \mathrm{posts}(d_j) = \varnothing$. That is, every department may have multi posts, but every post belongs to only one department. dp: $P \rightarrow \mathrm{DP}$ is a function that maps each post p_i to the single department $\mathrm{dp}(p_i)$;
- $\mathrm{SA} \in P \times S$ is a many-to-many post-to-staff assignment relation;

Received 2008-04-15.

Biographies: Yu Guangcan (1974—), male, graduate; Li Ruixuan (corresponding author), male, doctor, associate professor, rxli@hust.edu.cn.

Foundation items: The National Natural Science Foundation of China (No. 60403027, 60773191, 70771043), the National High Technology Research and Development Program of China (863 Program) (No. 2007AA01Z403).

Citation: Yu Guangcan, Li Ruixuan, Lu Zhengding, et al. Multi-level access control model for tree-like hierarchical organizations[J]. Journal of Southeast University (English Edition), 2008, 24(3): 393 – 396.

- $O = \{o_1, o_2, \ldots, o_m\}$ is the set of objects;
- $C = \{c_1, c_2, \ldots, c_p\}$ is the set of classifications. Also, the symbol $\geqslant_c$ is the sequence relation on set C, $\forall c_i, c_j \in C (j \neq i)$, if $c_i \geqslant_c c_j$, then, c_i has a higher classification than c_j. Also, $\forall c_i, c_j \in C$, if $c_j \geqslant_c c_i$ and $i \neq j$, then it is written as $c_j >_c c_i$;
- $A = \{r, w, e, a, c\}$ is the set of access attributes, where r, w, e, a, c represent read, written, execute, append and control, respectively.
- RA = $\{g, r, c, d, a\}$ is the set of request elements, where g, r, c, d, a represent get or give, release or rescind, change or create, delete or deactive and active, respectively.
- D = {yes, no, error, ?} is the set of decision, where yes, no, error, or ? represent that a request is agreed, rejected, a mistake, or an uncertain, respectively.
- $T \in \mathrm{DP} \times C$ is the set of security tags and $\langle T; \geqslant_t \rangle$ is a partial relation. $\forall (d_i, c_j), (d_k, c_l) \in T$, if $d_i \geqslant_d d_k$ and $c_j \geqslant_c c_l$, then $(d_i, c_j) \geqslant_t (d_k, c_l)$. We say that (d_i, c_j) has a higher security tag than (d_k, c_l). Also, dp: $T \rightarrow$ DP is a function that maps each security tag (d_i, c_j) to a department d_i. Finally, c: $T \rightarrow C$ is a function that maps each security tag (d_i, c_j) to a classification c_j. $\forall t_i, t_j \in T$, if $t_j \geqslant_t t_i$ and $i \neq j$, then it is written as $t_j >_t t_i$.
- MS, MP, and MD represent access matrices of staff, posts and departments, respectively. MS is a $(\#S) \times (\#O)$ matrix, where $(\#S)$ represents the amount of the staff set. $\mathrm{MS}_{(i,j)}$ ($\mathrm{MS}_{(i,j)} \subseteq A$) represents access privileges for the staff s_i ($s_i \in S$) to the object o_j ($o_j \in O$). Also, $\mathrm{MS}_{(i,j)}$ can be written as $\mathrm{MS}(s_i, o_j)$. $\mu_s = \{\mathrm{MS}_1, \mathrm{MS}_2, \ldots\}$ is the set of staff access matrices. MP is a $(\#P) \times (\#O)$ matrix, where $\mathrm{MP}_{(i,j)}$ ($\mathrm{MP}_{(i,j)} \subseteq A$) represents access privileges for post p_i ($p_i \in P$) to object o_j ($o_j \in O$). Also, $\mathrm{MP}_{(i,j)}$ can be written as $\mathrm{MP}(p_i, o_j)$. $\mu_p = \{\mathrm{MP}_1, \mathrm{MP}_2, \ldots\}$ is the set of post access matrices. And MD is a $(\#\mathrm{DP}) \times (\#O)$ matrix, where $\mathrm{MD}_{(i,j)}$ ($\mathrm{MD}_{(i,j)} \subseteq A$) represents access privileges for the department d_i ($d_i \in$ DP) to the object o_j ($o_j \in O$). Also, $\mathrm{MD}_{(i,j)}$ can be written as $\mathrm{MD}(d_i, o_j)$. $\mu_d = \{\mathrm{MD}_1, \mathrm{MD}_2, \ldots\}$ is the set of department access matrices.
- $F = \{f \mid f = (f_1, f_2, f_3)\} = (2^T)^P \times T^O \times P^S$, where $(2^T)^P = \{f_1 \mid f_1: P \rightarrow 2^T\}$ gives security tags for every post. $\forall p_i \in P$, if $\forall t_j \in f_1(p_i)$, then $\mathrm{dp}(t_j) \geqslant_d \mathrm{dp}(p_i)$. That is, the departments of security tags which adhere to a post must be higher than the departments of the post which adhere to or the same as that post. $\forall t_j, t_k \in f_1(p_i)$, if $\mathrm{dp}(t_j) \geqslant_d \mathrm{dp}(t_k)$, then $c(t_k) \geqslant_c c(t_j)$. That is, for the security tags of a post, the higher a department is, the lower the clearance corresponding to that department is. Also, $T^O = \{f_2 \mid f_2: O \rightarrow T\}$ gives security tags to every object. $P^S = \{f_3 \mid f_3: S \rightarrow P\}$ gives active posts to every staff and $(2^S)^P = \{f_3^{-1} \mid f_3^{-1}: P \rightarrow 2^S\}$ gives all the staff who are activating a post.
- A session maps a staff to a post and a staff can only create one session. However, when a staff activates a post, a session is created and when the staff deactivates the post, the session is ended.
- $V = P(S \times O \times A) \times \mu_d \times \mu_p \times \mu_s \times F$ is the set that represents the states of the systems. $\forall v \in V$, $v = (b, \mathrm{MD}, \mathrm{MP}, \mathrm{MS}, f)$ is the element that expresses a state of the system. Also, $b \subseteq S \times O \times A$ is the element that expresses the access privileges to objects which the staff currently obtains. MD expresses the departments access matrix currently; MP expresses the posts access matrix currently, and MS expresses the staff access matrix currently. Finally, f expresses the security tags of all the posts (activated by the current staff) and objects.
- $R = S^+ \times \mathrm{RA} \times S^+ \times O \times X$ is the request set, where $S^+ = S \cup \{\varnothing\}$, $X = A \cup \{\varnothing\} \cup F$. $\forall r \in R$, r is a five tuple, $r = (\sigma_1, \gamma, \sigma_2, o_j, x)$, where $\sigma_1, \sigma_2 \in S^+$ express staff s_1, s_2, respectively; $\gamma \in \mathrm{RA}$ is a request element, $o_j \in O$ is an object, and x is an access privilege, a null, a security tag of a staff or object, or a post that the staff wants to activate.
- ρ: $R \times V \rightarrow D \times V$ is a rule function, where R is a request set; D is a decision set, and V is a state set. $(R_k, v_n) \in R \times V$, $\rho(R_k, v_n) = (D_m, v^*)$, for the request R_k, the decision of the system is D_m and the state of the system transfers from v_n to v^*. ω is the set of the rule functions.

Because this model is an expanded model of the BLP model which is applied to tree-like hierarchical organizations, some basic definitions of our model (including system, system appearance, system action, indices, request sequences, decision sequences, state sequences etc.) are the same as in the BLP model. For simplicity, we will not describe them in this paper repeatedly. However, the relationships among the main components of our multi-level access control model are shown in Fig. 3.

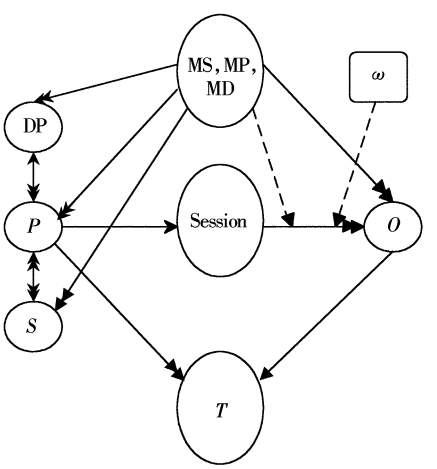

Fig. 3 Multi-level access control model for tree-like hierarchical organizations

2 Security Property Definitions

Using the components defined in the previous section, in this section, we give some important security properties by the following definitions:

Definition 1 Discretionary security property (ds-property):

For $\forall v \in V$, $v = (b, \mathrm{MD}, \mathrm{MP}, \mathrm{MS}, f)$, v satisfies ds-property $\Leftrightarrow$ for $\forall (s, o, x) \in b$, the following conditions are satisfied: $x \in \mathrm{MS}(s, o)$, $x \in \mathrm{MP}(f_3(s), o)$, or $x \in \mathrm{MD}(\mathrm{dp}(f_3(s)), o)$.

Definition 2 Simple security property (ss-property):

For $\forall v \in V$, $v = (b, \mathrm{MD}, \mathrm{MP}, \mathrm{MS}, f)$, v satisfies ss-property $\Leftrightarrow$ for $\forall (s, o, x) \in b$, the following conditions are satisfied: $x = e$ or $x = a$ or $x = c$, or ($x = r$ or $x = w$) and $\exists t \in$

$f_1(f_3(s))$, $t \geqslant f_2(o)$. That is, there is at least one security tag corresponding to the post which is higher than the security tag of the object.

Definition 3 $*$-property

For $\forall v \in V$, $v = (b, \mathrm{MD}, \mathrm{MP}, \mathrm{MS}, f)$, v satisfies $*$-property $\Leftrightarrow \forall s \in S$, if $o_1 \in b(s: w, a)$ and $o_2 \in b(s: r, w)$, then $f_2(o_1) \geqslant_t f_2(o_2)$.

However, some new components (such as department, post, security tags, and set of post) are proposed in our model. Compared to the BLP model, the ds-property and ss-property are greatly changed. These changes made our model more flexible and usable. However, the $*$-property has kept its original essence and it is changed outside the model; so, our model inherits the most prominent character of the BLP model and it can also control the information flow in the system.

3 Theorems

Some major theorems and conclusions of the BLP model were given in Ref. [10]. Since our model is an expanded model of the BLP model, theorems 1 and 2, which are presented in Ref. [10], are also suitable for our model, hence, they are introduced directly in this section without proofs. As ss-property is redefined in our model, theorem 3 is redefined and proved in this section. However, since theorem 4 is changed outside and has kept its essence, it has been given a new expression and there is no need for proof.

Theorem 1 If ω is an ss-property which keeps the rule set and z_0 is an initialization which satisfies ss-property, then $\sum(R, D, W, z_0)$ is an ss-property satisfied system.

Theorem 2 If ω is a $*$-property which keeps the rule set and z_0 is an initialization which satisfies $*$-property, then $\sum(R, D, W, z_0)$ is a $*$-property-satisfied system.

Theorem 3 Let $v = (b, \mathrm{MD}, \mathrm{MP}, \mathrm{MS}, f)$ satisfy an ss-property, $(s, o, x) \notin b$, $b^* = b \cup \{(s, o, x)\}$, and $v^* = (b^*, \mathrm{MD}, \mathrm{MP}, \mathrm{MS}, f)$:

1) Let $(x = e, x = a, \text{or } x = c)$, then v^* satisfies the ss-property.

2) Let $(x = r \text{ or } x = w)$, then v^* satisfies the ss-property $\Leftrightarrow \exists t \in f_1(f_3(s))$, $t \geqslant_t f_2(o)$.

Proof $\forall (s', o', x') \in b^*$, let $(s', o', x') \neq (s, o, x)$, $(s', o', x') \in b$. Since v satisfies the ss-property, (s', o', x') must satisfy one of the following conditions: 1) $x' = e$, $x' = a$, or $x' = c$; 2) $(x' = r \text{ or } x' = w)$ and $\exists t \in f_1(f_3(s'))$, $t \geqslant f_2(o')$.

Let $(s', o', x') = (s, o, x)$, one of the following two conditions can be satisfied based on the proposition given above: 1) $x' = e, x' = a$, or $x' = c$; 2) $(x' = r \text{ or } x' = w)$ and $\exists t \in f_1(f_3(s'))$, $t \geqslant f_2(o')$.

Based on definition 2, the system state v^* can satisfy the ss-property.

Theorem 4 $v = (b, \mathrm{MD}, \mathrm{MP}, \mathrm{MS}, f)$, where v can satisfy $*$-property and $(s, o, x) \notin b$. Let $b^* = b \cup \{(s, o, x)\}$ and $v^* = (b^*, \mathrm{MD}, \mathrm{MP}, \mathrm{MS}, f)$:

1) Let $x = e$ or $x = c$, then v^* satisfies $*$-property.

2) Let $x = a$, then v^* satisfies $*$-property $\Leftrightarrow \forall o' \in b(s: r, w)$, $f_2(o) \geqslant_t f_2(o')$.

3) Let $x = r$, then v^* satisfies $*$-property $\Leftrightarrow \forall o' \in b(s: a, w)$, $f_2(o') \geqslant_t f_2(o)$.

4) Let $x = w$, then v^* satisfies $*$-property $\Leftrightarrow$ the following three conditions must be satisfied at the same time: a) $\forall o' \in b(s: r)$, $f_2(o) \geqslant_t f_2(o')$; b) $\forall o' \in b(s: a)$, $f_2(o') \geqslant_t f_2(o)$; c) $\forall o' \in b(s: w)$, $f_2(o') = f_2(o)$.

Finally, by using theorems 3 and 4, we can construct rule set ω which satisfies ss-property and $*$-property easily.

4 Conclusions

In this paper, we propose a multi-level access control model for tree-like hierarchical organizations. Our model can solve the problems of the BLP model mentioned above and improve the BLP model by doing the following steps:

1) The tree-like hierarchic organization model is defined as a formal definition.

2) A new concept called post is proposed. Security tags are assigned to post, and users are also assigned to post. Users can activate their post to obtain corresponding security tags.

3) One or more security tags is/are assigned to a post. This leads the users in different departments to intercommunicate easily.

4) The access control matrices are redefined. Based on the new concept, a multi-granularity and flexible discretionary access control is implemented.

Finally, based on the proposed method above, our model modifies simple security properties and discretionary security properties of the BLP mode, and retain $*$-property. It inherits the most prominent merits of the BLP model that keep control on information flow and at the same time give more flexibility to the model.

References

[1] Wang Yuanyuan, Cheng Jun, Zheng Yuelin. Design of organization administration model on workflow system [J]. *China Management Informationization*, 2006, **9**(12): 5 − 7. (in Chinese)

[2] Bell D E, LaPadula L J. Secure computer systems: unified exposition and multics interpretation, ESD-TR-75-306[R]. Bedford, MA, USA: The Mitre Corporation, 1976.

[3] Li Ruixuan, Zhao Zhanxi, Wang Zhigang, et al. A BLP model based on access history [J]. *Computer Science*, 2006, **33**(7): 286 − 288. (in Chinese)

[4] Li Lan, He Yongzhong, Feng Dengguo. A fine-grained mandatory access control model for XML documents [J]. *Journal of Software*, 2004, **15**(10): 1528 − 1537. (in Chinese)

[5] He Jianbo, Qing Sihan, Wang Chao. Analysis of two improved BLP models [J]. *Journal of Software*, 2007, **18**(6): 1501 − 1509. (in Chinese)

[6] Verschuren J, Govaerts R, Vandewalle R. Realization of the Bell-LaPadula security policy in an OSI distributed system using asymmetric and symmetric cryptographic algorithms [C]//*Proc of Computer Security Foundations Workshop*. IEEE Computer Society Press, 1992: 168 − 178.

[7] LaPadula L J. Foreword for republishing of the Bell-LaPadula model [J]. *Journal of Computer Security*, 1996, **4**(9): 233 − 238.

[8] Focardi R, Martinelli F. A uniform approach for the definition of security properties [C]//*Proc of World Congress on Formal Models*. Springer, 1999, **1708**: 794 − 813.

[9] Liu Wenqing, Qing Sihan, Liu Haifeng. Design of a modified BLP security model and its application to secLinux [J]. *Jour-*

nal of Software, 2004, **13**(4): 567 - 573. (in Chinese)
[10] Wang Guilin, Qing Sihan, Ni Xizhen, et al. The Bell-LaPadula formal model for secure computer systems [J]. *Computer Science*, 2003, **12**(7): 89 - 92. (in Chinese)

树形层次化组织机构中的分级访问控制模型

於光灿　李瑞轩　卢正鼎　Mudar Sarem　宋　伟　苏永红

(华中科技大学计算机科学与技术学院,武汉 430074)

摘要:在 BLP 模型基础上提出一个新的分级访问控制模型,模型中建立部门之间的层次关系,提出岗位这一新的概念,简化了安全标记指派这一烦琐工作. 通过为岗位指派多个安全标记,实现上下级及平级部门之间的互相沟通,在树形层次中靠得越近的部门,其职员之间可交流的客体密级越高. 定义 3 个层次的访问矩阵,实现多种粒度的灵活的自主访问控制. 模型在增加灵活性和实用性的同时保证信息的流动始终处于系统的控制之下,继承了 BLP 模型最突出的优点,并通过形式化证明的方式对模型进行了验证.

关键词:分级访问控制;层次化组织机构;多安全标签

中图分类号:TP311