

A role-based security information flow model in grid environment

Yihe Liu¹, Shuang Zhang^{1, 2*}, Yuping Qin²

¹College of computer science, Neijiang Normal University, Neijiang, 641000, China

²The engineering & technical college of Chengdu university of technology, Leshan, 614000, China

Received 1 March 2014, www.cmmt.lv

Abstract

Security is an important component of a grid, and it directly affects the development of the grid and the practical application of the grid system software. According to the practical application problem (namely realization of the role-based management) in the role management occurring in the information application system of my school, a role-based security information flow model is proposed from the point of view of guaranteeing the information security. In this paper, the object concept in the general network environment is expanded, and the organization security classification of an object and relation between the security classification and the role set are used to classify the security and define the strategy for information flow, finally a security information flow model based on the grid environment is presented. The safe classify of the object is divided by the related information of role set, the organization security classifications, and classifications etc. At the same time, the information flow role is described. A new secure information flow model based on rules and grid environment is described using these methods. It is proven from strict mathematical justification that the new model satisfies properties of the finite lattice and least upper bound operator, and it is reasonable and safe. Furthermore, it is an extension of the BLP model and the role-based information flow model as well as extension of the security information flow model in the general network environment. Therefore, it is significant to the study of grid security.

Keywords: Grid Security, BLP model, Rule, Information flow model

1 Introduction

With the rapid development of the internet technology, thousands of types of high-performance computers are distributed on the internet. How to expand and use these network resources has become the research direction of scientists in the future. This is development prospects of the grid.

The grid security is an important part of the grid, which directly affects development of the grid and practical application of the grid system software. To construct a reasonable information security model is not only the need of information security, but also the necessary means of completing an information security project. At present, there are various information security models, such as BLP model [1] and the information flow model [2]. They have different characteristics, and play a very important role in formal description of information security. Most of the existing [3-5] information flow models are developed based on the reference [2], and all are presented in the general network environment.

Current research on grid security mainly focuses on the security certificate, access control, data integrity, communication confidentiality, non-repudiation of user behaviour, as well as single sign-on [7-9] in the network environment. Grid workflow and other properties are discussed in the reference [10-11]. In the reference [12], the information flow in the network environment is

studied. In this study, the information flow model proposed in the reference [12] in the network is modified. Furthermore, role and other concepts are introduced in combination with the reference [6], and information security flow in the network is discussed again from another perspective.

Content of this paper is as follows: the second section introduces related concept and known information flow models. In the third section, new concept introduced in the new model is first presented, such as role decomposition and security function; next security class, definition of expanded subjective & objective bodies, security policy, and definition of the symbol \oplus are introduced finally the model description is given. In the fourth section, explanation of the model is given as well as proving of relevant properties. The fifth section summarizes the paper.

2 Related concept

2.1 GRID AND GRID SECURITY

In the grid environment, different autonomous domains or virtual organizations compose the entire grid computation environment capable of providing the service for the external, But resource nodes in each autonomous domain or virtual organization can cooperate to complete different services, if tasks submitted by the

* *Corresponding author* e-mail: zhangshuanghua1@126.com

grid user can not be finished in an autonomous domain or a virtual organization, then the grid server of this autonomous domain or virtual organization will request resource nodes of other autonomous domains or virtual organizations to complete it through cooperation. The physical view of grid security is shown in Figure 1 [13].

In this paper, the discussion is developed on the basis of the GSI security strategy [14] in grid Globus environment.

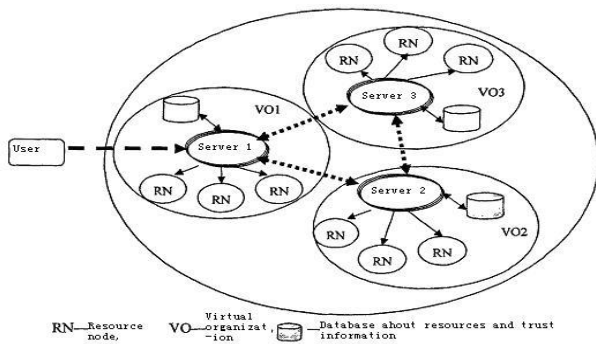


FIGURE 1 Physical view of grid security

2.2 BASIC SECURITY MODEL

2.2.1 Basic concept

Firstly, some known concepts are presented.

Subject and object: there exist a quantity of computer operation involved with the security. anything implementing operation is called the subject, such as process; they are expressed with $s_1, s_2, \dots, s_i, \dots$, or s , and their set is denoted as S . anything which is operated is called the object, denoted with $o_1, o_2, \dots, o_j, \dots$, or o , and their set is denoted as O .

Suppose there are m virtual organizations in the entire grid Globus environment, a subject represents a user or the user process in the environment. The local resource subject set corresponding to virtual organizations VO_i is denoted with S_VO_i , and the corresponding local resource object set is denoted with $O_VO_i (i=1,2,\dots,m)$.

Security classification: in this paper, security classifications (confidentiality grade) of the subject and object are measured in a specific way [14]. Confidentiality grade of the subject s is denoted with $T(s)$, and $T(o)$ indicates that of the object o .

According to BLP model [1], the system is at security status (confidentiality), so the following needs to be satisfied: reading up and writing down are not allowed. For this reason, if $T(s)$ is not less than $T(o)$, then the subject s can read the object o , and if $T(s)$ is not larger than $T(o)$, then the subject s can write the object o .

2.2.2 Decomposition of subject and object

Decomposition of subject [12]: when the subject s needs to access simultaneously the virtual organizations VO_1, VO_2, \dots, VO_m , the resource proxy needs to map a Globus

subject to one or more subjects belonging to the local resource, so decomposition of s in a virtual organization is expressed as $s_j=(s_VO_1, s_VO_2, \dots, s_VO_m)$, where the j th component indicates the subject in the j th virtual organization mapped from the Globus subject. if s_j need not be mapped to the virtual organization VO_j , then the corresponding component is noted with $s_VO_j_\varnothing (j=1,2,\dots,m)$.

Decomposition of Object [12]: when the object o needs to be decomposed to virtual organizations VO_1, VO_2, \dots, VO_m , o_j decomposed and expressed as $o_j=(o_VO_1, o_VO_2, \dots, o_VO_m)$ in the virtual organization, where the j th component is the part decomposed from the object o to the virtual organization VO_j , and if the object o need not be decomposed to the virtual organization VO_j , then the corresponding component may be denoted with $o_j_VO_j_\varnothing (j=1,2, \dots, m)$.

When a subject or an object not in a virtual organization, with decomposition expression, the security classification of subject s /object $o (T(s) /T(o))$ is converted to a m -dimension vector function, in which a component can be defined like the related definition in the general network environment, such as: $T(s)=(T(s_VO_1), T(s_VO_2), \dots, T(s_VO_m))$.

2.2.3 Security classification of organization

Security classification of organization [12]: supposes the existing grid is divided into m independent virtual organizations $VO_1, VO_2 \dots VO_m$ in accordance with the access request, and each virtual organization is given a different security grade, so this is called security classification of the organization, denoted with **net** (Net_name). A net (Net_name) corresponds to the organization classification of virtual organization Net_name, denoted with net (Net_name)=(net(VO₁),net(VO₂),...,net(VO_m)).

Suppose $net(VO_i)=\max_{o \in O_VO_i} \{T(o)\}$ and when $o=(o_VO_1, o_VO_2, \dots, o_VO_m)$, $net(o)=\max\{T(o_VO_1), T(o_VO_2), \dots, T(o_VO_m)\}$.

2.2.4 RBAC model

The basic idea of the RBAC model [5] is responsibility separation, and this is similar to an organization. In the RBAC model, the user is given a role, a role is awarded with permissions, and the permissions are associated with operations, the user gets the relevant permissions of the role through the role, so as to complete some operations. This paper is subject to the most basic concepts of the RBAC model.

Suppose the system has a role set $R=\{r_1, r_2, \dots, r_n\}$; the role set of the object o is denoted with $OR(o)$; While the user owned by the object o through the role is denoted $OS(o)$.

2.2.5 Denning Information flow model

Denning's [2] information flow model is defined by $FM = \langle N, P, SC, \oplus, \rightarrow \rangle$, where N is an object finite set, P is a finite process set (subject set), SC is a security class set, the class-combining operator \oplus is an associative and commutative binary operator. For classes of any two operands, \oplus demonstrates the class to, which the result operand generated from any binary function of the two operands belongs. A flow relation \rightarrow indicates information flow between pairs of security classes. For classes A and B , we write $A \rightarrow B$, only if information in class A is permitted to flow to class B . Information is said to flow from class A to class B .

The security requirements of the model are simply stated: a flow model FM is secure if and only if execution of an operation sequence cannot produce a flow that violates the relation \rightarrow . Under certain assumptions, $\langle SC, \rightarrow, \oplus \rangle$ forms a finite lattice:

- (1) $\langle SC, \rightarrow \rangle$ is a partially ordered set.
- (2) SC is a finite set.
- (3) SC has a lower bound of L such that $\forall A \in SC, L \rightarrow A$.
- (4) \oplus is a least upper bound operator on SC .

Where the class-combining operator \oplus is also a least upper bound operator, it has the following properties for all $A, B, C \in SC$:

- (a) $A \rightarrow A \oplus B$ and $B \rightarrow A \oplus B$.
- (b) $A \rightarrow C$ and $B \rightarrow C \Rightarrow A \oplus B \rightarrow C$.

3 A new information flow model based on grid environment

3.1 NEW MODEL DESCRIPTION

In order to give new information flow model under the grid environment, we give some new definitions in the following.

3.1.1 Role decomposition

Similar to decomposition of the object, decomposition of the role set $OR(o)$ owned by the object o may be expressed as follows:

$$OR(o) = (OR(o)_{VO1}, OR(o)_{VO2}, \dots, OR(o)_{VOm}).$$

Similar to decomposition of the subject, decomposition of the subject $OS(o)$ owned by the object o through the role may be expressed as follows:

$$OS(o) = (OS(o)_{VO1}, OS(o)_{VO2}, \dots, OS(o)_{VOm}).$$

3.1.2 Security function

Object Security function: it is used to describe the ultra four-dimensional vector function relevant to security classification of the virtual organization, security classification, and related roles of the object, denoted as

$$T(\text{net}(\text{Net_name}), T(o), OR(o), OS(o)) \text{ or } T(\text{net}(o), T(o), OR(o), OS(o)).$$

The set U indicates the complete set consisting of all ultra four-dimensional security function vectors.

3.2 DESCRIPTION OF NEW MODEL

The grid security information flow model proposed in this paper is defined as follows:

$FM = \langle O, S, SC, \oplus, \rightarrow \rangle$ is a security information flow model based on the grid environment, in which information flows only from the virtual organization with the low security classification to the one with the high security classification, where O and S are the object set and the process (subject) set of the whole grid. They are finite sets. SC is the security class of the model, defined in Section 3.2.1. The strategy \rightarrow is defined in Section 3.2.3. The operation \oplus is defined in Section 3.2.4.

The relevant concepts are described and discussed as follows.

Suppose that O' is an actual object set and S' is an actual subject set (processes set) of the whole grid, they are finite sets; SC' is the set of actual security classes.

U' is the set of all actual ultra four-dimensional security function vector defined in Section 3.1.2.

SC' is the set of security classes divided according to all actual ultra four-dimensional security function value, and obviously it is a finite set, and the $U' \subseteq U$.

3.2.1 Security class #o

Definition 1: the security class of the object o , indicated $\#o, \#o = \{ o \mid o \in O, \#o = \{ o \mid o \in O, T(\text{net}(o), T(o), OR(o), OS(o)) \text{ are invariable} \}, \text{ as } \forall o' \in \#o, \text{ there are } T(\text{net}(o'), T(o'), OR(o'), OS(o')) = T(\text{net}(o), T(o), OR(o), OS(o)) \}$

Hence $SC' = \{ \#o \mid o \in O \}$, SC' is a finite set.

We will discuss U' and U , and expand the concept of O', S', SC' .

3.2.2 Empty object and empty subject

Empty object: $\forall \alpha \in U, \text{ but } \alpha \notin U'$. Then we will expand a object o , which satisfies $T(\text{net}(o), T(o), OR(o), OS(o)) = \alpha$. Except name and the ultra four-dimensional security function vector, the object has no other characteristics. When a subject accesses the object, no available information is leaked. For example, an empty file has only name and we say that the object is an empty object. An empty object set is denoted with O'' .

Empty subject: any object performing operation related to the above empty object is called the empty subject and its set is denoted as S'' .

$$\forall o \in O'', \text{ then } SC'' = \{ \#o \mid o \in O'' \}.$$

The previously described $s_i_{VO_j_\phi}, o_j_{VO_i_\phi}$ can actually be considered empty subject and empty object

respectively.

$\forall o \in O$, then $SC = \{ \#o | o \in O \}$. $O = O' \cup O''$, $S = S' \cup S''$, $SC = SC' \cup SC''$.

When expanding the concept of O' , S' , SC' , we make use of them together with the general concept, don't make any distinction between them.

Now they are denoted again: $O = O' \cup O''$, $S = S' \cup S''$, $SC = SC' \cup SC''$.

Where O is a object set, S is a subject set (processes set) for total grid network, SC is a security classes set, and they are finite sets.

3.2.3 Description of security policy

Definition 2: security flow policy:

For any objects o_1 and o_2 , if information can flow from o_1 to o_2 , then the security class of o_1 is controlled by o_2 's, or they are equivalent, namely:

Axiom: $\forall o_1, o_2 \in O, o_1 \rightarrow o_2$ if and only if $net(o_1) \leq net(o_2), T(o_1) \leq T(o_2), OR(o_1) \supseteq OR(o_2)$ and

$OS(o_1) \supseteq OS(o_2)$, both of them are true.

Further explanation is presented as follows:

- Meaning of $\cdot \leq, \geq, \supseteq$ operations

\leq, \geq were comparison operation of "less than or equal to" and "greater than or equal to" of real numbers, $T(o_1) \leq T(o_2)$ is defined as follows: corresponding components of two m -dimension vectors are used for computation through \leq operation. $T(o_1) \geq T(o_2)$ has the similar definition.

The operator \supseteq represents containing operation between two sets. $OR(o_1) \supseteq OR(o_2)$ and $OS(o_1) \supseteq OS(o_2)$ are defined as follows: the sets of the corresponding components of two m -dimension vectors are used for computation through " \supseteq " operation.

- **The object is not defined in the decomposition of a virtual organization**

When $o_{1_VO_i_j}$ is a component of the source object O_1 , the definition in this paper is presented as follows:

$$T(o_{1_VO_i_j}) = \min_{j \in \{1, 2, \dots, m\}} \{T(o_{_VO_j})\}$$

$$OR(o_{1_VO_i_j}) = \bigcup_{j \in \{1, 2, \dots, m\}} OR(o_j)$$

$$OS(o_{1_VO_i_j}) = \bigcup_{j \in \{1, 2, \dots, m\}} OS(o_j)$$

When a component of objective object O_2 is VO_{j_k} is the definition in this paper is presented as follows:

$$T(o_{2_VO_j_k}) = \min_{j \in \{1, 2, \dots, m\}} \{T(o_{_VO_k})\}$$

$$OR(o_{2_VO_j_k}) = \bigcup_{j \in \{1, 2, \dots, m\}} OR(o_k)$$

$$OS(o_{2_VO_j_k}) = \bigcup_{j \in \{1, 2, \dots, m\}} OS(o_k)$$

3.2.4 The definition of " \oplus "

Definition 3: the operator " \oplus " is defined as follows:

$$\forall o_1, o_2 \in O, \\ \#o_1 \oplus \#o_2 = \{ o | T(net(o), T(o), OR(o), OS(o)) \\ = T(\max(net(o_1), net(o_2)), \max(T(o_1), T(o_2)), \\ OR(o_1) \cap OR(o_2), OS(o_1) \cap OS(o_2)), o \in O \}.$$

The $\max(net(o_1), net(o_2))$ for a maximum of two real numbers, $\max(T(o_1), T(o_2))$ is defined as follows:

$$\max(T(o_1), T(o_2)) = \{ \max(T(O_{1_VO_1}), T(O_{2_VO_1})), \\ \max(T(O_{1_VO_2}), T(O_{2_VO_2})), \dots, \max(T(O_{1_VO_m}), \\ T(O_{2_VO_m})) \}.$$

$OR(o_1) \cap OR(o_2)$ and $OS(o_1) \cap OS(o_2)$ have similar definition.

On the basis of the above assumption, the model $FM = \langle O, S, SC, \oplus, \rightarrow \rangle$ described in this section is a security lattice model in the grid environment.

4 Discussion of new model

We discuss the rationality of the new model from the following aspects.

4.1 THE RATIONALITY OF " \rightarrow " DEFINITION

According to the first hypothesis, the subject s and the operating objects o_1 and o_2 , $s = (s_VO_1, s_VO_2, \dots, s_VO_m)$, meet the condition $s_VO_j \in S_VO_j$, this shows that the subject is mapped to one or more subjects belonging to the local resource through relevant strategy. It accords with the most basic requirements for grid security.

When $o_1, o_2 \in O$ and belong to the same virtual organization, $net(o_1) = net(o_2)$, then flow directions of o_1 and o_2 are determined only according to the priority levels of security classification and role natures of the two objects. According to references [3] and [6], $T(o_1) \leq T(o_2)$, $OR(o_1) \supseteq OR(o_2)$, and $OS(o_1) \supseteq OS(o_2)$ are used to define $o_1 \rightarrow o_2$, which complies with security requirements of the general network environment. At the moment, because no information flows out of the virtual organization, so it meets design requirements of the entire network.

When $o_1, o_2 \in O$ and they don't belong to the same virtual organization, according to the relevant definition, only when $net(o_1) \leq net(o_2)$, $T(o_1) \leq T(o_2)$, $OR(o_1) \supseteq OR(o_2)$ and $OS(o_1) \supseteq OS(o_2)$ are true, $o_1 \rightarrow o_2$ is true.

The first condition is satisfied only when O_1 and O_2 are from the virtual organizations with the low-level and the high-level security classification respectively. Furthermore, O_1 and O_2 should meet the second condition which is necessary for the common information flow; otherwise they cannot flow from the virtual organization with the low-level security classification to the one with the high-level security classification. So they satisfy

design requirements of the general network security. Moreover, the third or the fourth condition complies with design requirements of the entire grid security in accordance with the description in the reference [5].

In addition, when the source object or objective object is not decomposed in a virtual organization, it meets the above security requirements as per definitions of security classifications of the subject and the object.

Thus, definition of "→" in Section 3.2 is reasonable.

4.2 <SC, →> IS A PARTIALLY ORDERED SET

Theorem 1: <SC, →> is a partially ordered set.

Proof: we verify it from reflexivity, transitivity and anti-symmetry of <SC, →> .

- Reflexivity: $\forall o \in O, o \rightarrow o$.

Suppose $T(o_VO_i) \leq T(o_VO_i)$, $OR(o_VO_i) \supseteq OR(o_VO_i)$, and $OS(o_VO_i) \supseteq OS(o_VO_i)$ ($i=1,2,\dots,m$), $net(o) \leq net(o)$, $T(o) \leq T(o)$, $OR(o) \supseteq OR(o)$ and $OS(o) \supseteq OS(o)$ are true, so is $o \rightarrow o$.

- Transitivity: $\forall o_1, o_2, o_3 \in O, o_1 \rightarrow o_2$ and $o_2 \rightarrow o_3$, here has $o_1 \rightarrow o_3$.

$$\forall o_1, o_2, o_3 \in O, o_1 \rightarrow o_2 \text{ and } o_2 \rightarrow o_3.$$

So $net(o_1) \leq net(o_2)$, $T(o_1) \leq T(o_2)$, $OR(o_1) \supseteq OR(o_2)$, $OS(o_1) \supseteq OS(o_2)$,

and $net(o_2) \leq net(o_3)$, $T(o_2) \leq T(o_3)$, $OR(o_2) \supseteq OR(o_3)$, $OS(o_2) \supseteq OS(o_3)$. The following can be derived accordingly.

$T(o_1_VO_i) \leq T(o_2_VO_i)$, $OR(o_1_VO_i) \supseteq OR(o_2_VO_i)$, $OS(o_1_VO_i) \supseteq OS(o_2_VO_i)$ and $T(o_2_VO_i) \leq T(o_3_VO_i)$, $OR(o_2_VO_i) \supseteq OR(o_3_VO_i)$, $OS(o_2_VO_i) \supseteq OS(o_3_VO_i)$ ($i=1,2,\dots,m$).

therefore $T(o_1_VO_i) \leq T(o_3_VO_i)$, $OR(o_1_VO_i) \supseteq OR(o_3_VO_i)$, $OS(o_1_VO_i) \supseteq OS(o_3_VO_i)$ ($i=1,2,\dots,m$) are true.

According to the definition of decomposition, $T(o_1) \leq T(o_3)$, $OR(o_1) \supseteq OR(o_3)$, $OS(o_1) \supseteq OS(o_3)$ are true, and obviously $net(o_1) \leq net(o_3)$ is true, and so is $o_1 \rightarrow o_3$.

- Anti-symmetry: $\forall o_1, o_2 \in O, o_1 \rightarrow o_2$, and $o_2 \rightarrow o_1$, $\#o_1 = \#o_2$.

Suppose $net(o_1) \leq net(o_2)$; $T(o_1) \leq T(o_2)$, $OR(o_1) \supseteq OR(o_2)$, $OS(o_1) \supseteq OS(o_2)$ and $net(o_2) \leq net(o_1)$, $T(o_2) \leq T(o_1)$, $OR(o_2) \supseteq OR(o_1)$, $OS(o_2) \supseteq OS(o_1)$, the following can be derived:

$T(o_1_VO_i) \leq T(o_2_VO_i)$, $OR(o_1_VO_i) \supseteq OR(o_2_VO_i)$, $OS(o_1_VO_i) \supseteq OS(o_2_VO_i)$ 且 $T(o_2_VO_i) \leq T(o_1_VO_i)$, $OR(o_2_VO_i) \supseteq OR(o_1_VO_i)$, $OS(o_2_VO_i) \supseteq OS(o_1_VO_i)$ ($i=1,2,\dots,m$).

$T(o_1_VO_i) = T(o_2_VO_i)$, $OR(o_1_VO_i) = OR(o_2_VO_i)$, $OS(o_1_VO_i) = OS(o_2_VO_i)$ ($i=1,2,\dots,m$).

So $T(o_1) = T(o_2)$, $OR(o_1) = OR(o_2)$ and $OS(o_1) = OS(o_2)$ are true. obviously $net(o_1) = net(o_2)$ is true.

It can be seen from the above, derivation that <SC, →> is a partially ordered set.

4.3 SC HAS A LOWER BOUND #O_{LOWEST}

SC has a lower bound, denoted as #O_{lowest}.

$$\#O_{lowest} = \{ o | T(net(o), T(o), OR(o)), OS(o) = T(\min(net(o), \min(T(o)), \bigcup_{o' \in O} OR(o')), \bigcup_{o' \in O} OS(o')), o \in O \}.$$

According to the above definition #O_{lowest} is always present and #O_{lowest} → #o.

4.4 SOME PROPERTIES OF ⊕

Property 1: $\forall o_1, o_2, o_3 \in O, \#o_1 \rightarrow \#o_1 \oplus \#o_2, \#o_2 \rightarrow \#o_1 \oplus \#o_2$

Proof: (1) because of the definition of $net(o_1)$ and $net(o_2)$

So $net(o_1) \leq \max(net(o_1), net(o_2))$, $net(o_2) \leq \max(net(o_1), net(o_2))$ is true.

(2) because of the definition of $\max(T(o_1), T(o_2))$, So $T(o_1) \leq \max(T(o_1), T(o_2))$, $T(o_2) \leq \max(T(o_1), T(o_2))$ are true.

(3) when $i=1,2,\dots,m$

$OR(o_1_VO_i) \supseteq OR(o_1_VO_i) \cap OR(o_2_VO_i)$, $OS(o_1_VO_i) \supseteq OS(o_1_VO_i) \cap OS(o_2_VO_i)$

so $OR(o_1) \supseteq OR(o_1) \cap OR(o_2)$ and $OS(o_1) \supseteq OS(o_1) \cap OS(o_2)$ are true.

Similarly, $OR(o_2) \supseteq OR(o_2) \cap OR(o_1)$ and $OS(o_2) \supseteq OS(o_2) \cap OS(o_1)$ are true.

On the basis of the definition of \oplus and the above analysis, the following can be derived:

$$\#o_1 \rightarrow \#o_1 \oplus \#o_2, \#o_2 \rightarrow \#o_1 \oplus \#o_2.$$

Property 2: $\forall o_1, o_2, o_3 \in O, \#o_1 \rightarrow \#o_3, \#o_2 \rightarrow \#o_3$, so $\#o_1 \oplus \#o_2 \rightarrow \#o_3$

Proof: (1) Suppose $net(o_1) \leq net(o_3)$, $net(o_2) \leq net(o_3)$, $\max(net(o_1), net(o_2)) \leq net(o_3)$ is true.

(2) Suppose $T(o_1) \leq T(o_3)$, $T(o_2) \leq T(o_3)$, $\max(T(o_1_VO_i), T(o_2_VO_i)) \leq T(o_3_VO_i)$ ($i=1,2,\dots,m$) is true.

so is $\max(T(o_1), T(o_2)) \leq T(o_3)$.

(3) $\#o_1 \rightarrow \#o_3$

$OR(o_1_VO_i) \supseteq OR(o_3_VO_i)$, $OS(o_1_VO_i) \supseteq OS(o_3_VO_i)$ ($i=1,2,\dots,m$)

$\#o_2 \rightarrow \#o_3$

$OR(o_2_VO_i) \supseteq OR(o_3_VO_i)$, $OS(o_2_VO_i) \supseteq OS(o_3_VO_i)$ ($i=1,2,\dots,m$),

so the following can be derived:

$OR(o_1_VO_i) \cap OR(o_2_VO_i) \supseteq OR(o_3_VO_i)$, $OS(o_1_VO_i) \cap OS(o_2_VO_i) \supseteq OS(o_3_VO_i)$ ($i=1,2,\dots,m$). $OR(o_1) \cap OR(o_2) \supseteq OR(o_3)$, $OS(o_1) \cap OS(o_2) \supseteq OS(o_3)$

According to the definition of \oplus and the above analysis, $\#o_1 \oplus \#o_2 \rightarrow \#o_3$ is true.

5 Conclusions

In this study, on the basis of elements of grid security, the concept of role decomposition, the ultra four-dimensional security function of the object are defined by means of the characteristics of the security formation flow model in general network environment.

A new information flow model based on the grid environment is described by defining the information flow strategy by means of the ultra four-dimensional safety function value of the object.

According to the analyses, it is proved that the model is safe and reasonable. The model can reflect the information flow in the grid environment well, and this is helpful for description of security information flow in the

grid environment.

Because the grid environment is too complicated and the thesis length is limited, practical application of the information flow model in this study will be detailed in a separate paper.



Acknowledgment

This work is supported by Sichuan province academic and technical leader training funded projects 12XSJS002.Sichuan provincial department of science and technology project 2013ZR0089. Sichuan province department of education natural science point item 12ZB192, 13ZA0003, 14ZB0360, 14ZB0363.

References

- [1] Bell D E, Lapadula L J 1973 Secure computer system[R]:mathematical foundation MTR-2527, Mitrecorp, Bedford, MA (NTIS AD771543)
- [2] Denning D E 1976 A lattice model of secure information flow *Communications of the ACM* **19**(5) 236-43
- [3] Sandhu Ravi S 1993 Lattice-Based Access Control Model *IEEE computer* **26**(11) 9-19
- [4] Liu Yihe, Shen Chang Xiang 2005 An Information Security Function and Application Model *Journal of Computer Aided Design & Computer Graphics* **17**(12) 2734-38 (In Chinese)
- [5] Sandhu R S, Samarati P 1994 Access control: principles and practice *IEEE communications* **32**(9) 40-8
- [6] Liu Yihe, Liu Jiayong 2004 An Information Flow Model Based on Roles and Applications *Journal of Sichuan University (Engineering Science Edition)* **36**(5) 94-7 (In Chinese)
- [7] May Phyo Oo, Thinn Thu Naing 2007 Access Control System for Grid Security Infrastructure *IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology – Workshops* 299-302
- [8] Han Bing 2006 Study on data management and the security problem Under the grid environment. Chinese Scientific and Technical University master's degree paper, in Chinese, 2006
- [9] Xiaoqin Huangetc 2005 *An Identity-Based Model for Grid Security Infrastructure* ISSADS2005, LNCS3563 258-66 Springer-Verlag Berlin Heidelberg
- [10] Bivens H 2001 *Grid work flow* Albuquerque:Sandia National Laboratory
- [11] Zhou Jian-tao 2008 A Review on the Grid Workflow and Its Key Technologies *Journal of Inner Mongolia University* **39**(5) 581-9 (In Chinese)
- [12] Liu Yi-he Security Information Flow Model Based on Grid Environment *Computer Science* **38**(6) 157-60 (In Chinese)
- [13] Wфттп Fang 2009 *Study under the grid environment's trust mechanism* Nanjing Posts and telecommunications University master's degree paper (in Chinese)
- [14] *The Globus Project [EB / OL]* <http://www.globus.org/>

Authors

	<p>Yi He Liu, born in April, 1964, Neijiang, China</p> <p>Current position, grades: Professor in Neijiang Normal University University studies: Doctor of Cryptography in Sichuan University Scientific interest: Intra-body communication, Cryptography Publications: 2 Patents, 46 Papers Experience: He received the Ph.D. degree in Sichuan University, Chengdu, Sichuan, China, in 2005. Since 2009, he has been involved in research in the areas of intra-body communication. He is currently a Professor, Neijiang Normal University.</p>
	<p>Shuang Zhang, born in May, 1983, Leshan, China</p> <p>Current position, grades: Lecturer in The Engineering & Technical college of Chengdu University of Technology University studies: Doctor of Electrical & Electronic Engineering in University of Macau. Scientific interest: Intra-body communication, Cryptography Publications: 2 Patents, 25 Papers Experience: He received the Master degree in control Engineering from the Graduate University of Chinese academy of sciences, Beijing, China in 2011. Since 2011, he has performed research in the areas of Digital Image Processing, Digital signal processing, Intra-body communication. He is now a lecturer, department of electronic information and computer technologies, The Engineering & Technical college of Chengdu University of Technology. At the same time, He is now a Ph.D. student in the Department of Electrical and Electronics Engineering, Faculty of Science and Technology, University of Macau.</p>
	<p>Yu Ping Qin, born in March, 1984, Leshan, China</p> <p>Current position, grades: Lecturer in The Engineering & Technical college of Chengdu University of Technology University studies: Master of basic mathematics in Sichuan Normal University. Scientific interest: Intra-body communication, Cryptography Publications: 2 Patents, 25 Papers Experience: She received the Master degree in control Engineering from the Sichuan Normal University, Chengdu, China in 2011. Since 2011, she has performed research in the areas of Partial differential equation, Intra-body communication. She is now a lecturer, The Engineering & Technical college of Chengdu University of Technology.</p>