Design Engineering

ISSN: 0011-9342
Issue: 10 | Pages: 117 - 127

Specifying and Enforcing the Principle of Static Separation of Duty in Multi Domain

Xiaopu Ma[1,*], Li Zhao[2], Wenpeng Zhang[1]
[1]School of Software, Nanyang Normal University, Nanyang, Henan, China
[2]School of Computer and Information Technology, Nanyang Normal University, Nanyang, Henan, China
*Corresponding Author: Xiaopu Ma

Abstract:

Role-based access control model (RBAC) has broadly applied in different enterprises to provide security protection for enterprise security products. In these systems, the important aspect and principle are some constraints. In this model the most frequently mentioned constraint is separation of duty constraint policy that includs static separation of duty constraint policy and dynamic separation of duty constraint policy respectively. However, little research has been done to specify and enforce the principle of static separation of duty under multi domain. Based on the current research status,on the basis of IRBAC 2000, we first descirbe and study the static separation of duty in two domains. Then give a general definition of global static separation of duty and strict global static separation of duty in order to satisfy the multi domain security requirement and management in real scenario. We also study the computational complexity of global static separation of duty. Furthermore, we put forward a methodto enforce global static separation of duty through global mutually exclusive role constraint in multi domain.

Keywords*: RBAC; Static Separation of Duty; Global Static Separation of Duty; Strict Global Static Separation of Duty; Global Mutually Exclusive Role Constraint.*

I. INTRODUCTION

RBAChas more advantages than other models that make it more suited for solving security and management requirements in different organizations[1]. Thus, it has broadly applied in different enterprise to provide security protection for enterprise security products. We can notget an integrated RBAC model if there is no constraint policy in RBAC on the one hand, on the other hand the administrator also cannot lay out the higher-level organizational policy on other security officers[2]. In the context of RBAC one of the main constraint policies is separation of duty(SoD) constraint policy[3]. In general, there are static separation of duty (SSoD) constraint policy and dynamic separation of duty (DSoD) constraint policy respectively in order to overcome collusion and other security requirements in different situations and systems[4]. Furthermore, previous researchers have given a more descriptions of SoDconstraint

Design Engineering
ISSN: 0011-9342
Issue: 10 | Pages: 117 - 127

policy and relationships among different SoD properties, such as Operational Dynamic Separation of Duty, Object-based Dynamic Separation of Duty and so on.

Nowadays with the distributed application and network technologyrapid development, information cooperationandinteractionin multi domain has become more and more frequently. In order to provide information interaction, information sharing and cooperation in multi domain, researchers introduced IRBAC 2000 model to satisfy the requirements[5]. In this model, foreign user can obtain the local access authorization using dynamic role translation in order to cooperate in multi domain. Since then, researchers put forward the different methods for security interoperability of across-domain in this model or proposed other model based on this to satisfy the across-domain security requirements. For example, Basit Shafiq et al. proposed a policy compound framework that integrates the originalRBAC policiesto accomplish resource sharing and security requirements in multi domain[6]. In order to satisfy the security demands of secure interoperation in multi domain, some security violation detection algorithms are also proposed. For example,Jianfeng Lu et al. proposed an approach to employ UCON policies to satisfy the secure interoperation in multi domain surroundings[7]. In fact, collaboration in such multi domain surroundingneed to integrate all of the local domain policies into one integrated global domain security policy in order to provide security requirements among multi domain. However, most researchers only consider about how to execute and solve the violation of SSoD constraint policy in each local domain or in role translation between different domains to our knowledge. However, an integrated SSoD constraint policy in multi domain should be guaranteed from three aspects:

1. First, the constraint policy in each domain should be enforced, in other words, all the subjects in the local domain must obey the local SSoD constraint policy;

2. Second, the constraint policy between the multi domain should be enforced, in other words, the violation of SSoD constraint policy should be solved along with role mapping between domains;

3. Furthermore, the constraint policy should be guaranteed in the whole domain, inother words, we need consider the whole security requirements in order to construct the integrated globalSSoD constraint policy in the multi domain environment.

In fact, SSoD constraint policy may be wrong if we just consider the requirements in each single domain or between domains along with role mapping. In other words, even the SSoD constraint policy in the first two levels is enforced, the SSoD constraint policy also can be violated in the global domain. Consider the following example of thesis defense at the university. The task can be done as follows:

1. Degree applicant provides relevant materials (such as the research paper,academic record and so on) to reflect the academic level in order to take part in the thesis defense;

2. Administrative department of the university will verify the relevant materials in order to decide whether the degree applicant meets the conditions of thesis defenseor not;

3. The university administrative department will organize the thesis defense for the degree applicant;

4. In order to evaluate the quality of the thesis respondent, the administrative department of the university will organize the dissertation committee in order to check and approve the thesis defense. For decreasing the error of the commissioner`s judgement, the committee members must contain relevant specialists from other university or other agency.

In this thesis defense, we need different specialists to cooperate with the thesis defense in order to obey the SSoD constraint policy in the local domain (university) on the one hand; on the other hand we also require the specialists should come from the different university (domain) to cooperate with the thesis defense in order to obey the SSoD constraint policy in the global domain. However, the existing SSoD constraint policy cannot solve this problem. Hence, we define the SSoD constraint policy between two domains based on IRBAC 2000 model (ISSoD) and the Global Static SoD (GSSoD) constraint policy and Strict Global Static SoD (SGSSoD) constraint policy in multi domain which all take the domain information into the traditional SSoD constraint policy firstly. Furthermore, we intuoduce the Global Statically Mutually Exclusive Role (GSMER) constraint, use it to enforce GSSoD constraint policy in multi domain and prove that direct execution ofGSSoD constraint strategy is a coNP-complete problem. Finally, the method of using GSMER constraint to implement GSSOD constraint strategy is given.

In this paper, in Section 2 we disscuss the related work. In Section 3, the relevant definition and description are given. Then in Section 4, the paper showsthe way of enforcing GSSoD constraint policy directly and how to use GSMER constraint to enforce GSSoD constraint policy in multi domain. In Section 5, we conclude this paper and look forward to the future.

II.RELATED WORK

As far as we know, in order to protect information security and system secuirty requirements, the SoD constraint policy is firstly proposed by Saltzeret al. as one of the basic design criteria in computer security systems[8]. Since then, several researchers have studied SoD constraint policy based on different perspectives[9]. One of the best-known formal definitions of SoD constraint policy is described by researchers, in which removed all ambiguities of informal definition, and offered a wide choice of implementation strategies to describe the different type of SoD constraint policy and their relationships. Furthermore, Jianfeng Lu et al. introduced a set-based specification scheme to specify and enforce the SSoD constraint policy in UCON access control model[7]. Ferraiolo et al. defined SSoD constraint policy based on role as: Any user cannot obtain any role that are mutually exclusive to the user already obtained roles[2]. However, something that’s not very clear between SMER constraint guarantee mechanism and SSoD constraint policy objectives. Thus, Li et al. discussed thedistinguish between them and put forward the mechanism of how to enforce SSoD constraint policy by SMER constraint mechanism[10].

Furthermore, with the rapid development of various technologies have provided the possibility for interoperation between different domains in the distributed surroundings and real world. In the distributed environment, interoperability provides an approach to share resources and services between different domains. Hence, SSoD constraint policy become an important issue in these situation in order to provide the security for the resources and services in different situation and different domains. Several researchers composited each local domain SSoD constraint policy into an integrated SSoD constraint policy in multi domain environment to meet the security needs among the whole domain. For example, Kapadia et al. proposed IRBAC 2000model to support cross domian operation through dynamic rolemapping in order to realize cooperation between different domains[5]. However this role translation method can lead to SSoD constraint policy violation through role mapping between different domains. Thus, some algorithms to detect the SSoD constraint policy violation are proposed by researchers in multi domain. For example, Ma et al. also put forward the global static separation of duty constraint policy in multi domain, however, the research content is not comprehensive[11].

To this aim,we present a definition to describe SSoD constraint policy between two domains based on IRBAC 2000. We also consider different important variations of SSoD constraint policy in multi domain, including GSSoD constraint policy and SGSSoD constraint policy. Both of the GSSoD constraint policy and the SGSSoD constraint policy impose more stringent restrictionson the number of users from the different domains than SSoD constraint policy between two domains. Furthermore, we also study the computational complexity of GSSoD constraint policy and propose an approach to enforce GSSoD constraint policy by GSMER.

III. PRELIMINARY

In this section, we first describe a simple definition for SSoD constraint policy in IRBAC 2000 model. Then we will give a general definition of GSSoD constraint policy and SGSSoD constraint policy to satisfy the global requirement in multi domain.

It supposes that IRBAC 2000 has four countable infinite sets: R (all possible role set), U (all possible user set), P (all possible permission set), and D (all possible domain set).

Definition 3.1: (IRBAC State) An IRBAC state can be described as a four tuples $\gamma = < UA, PA, RH, RP >$, we use $UA \subseteq U \times R$ to describe users to roles assignment relationship in the local domain, $PA \subseteq R \times P$ to describe roles to permissions assignment relationship in the local domain, $RH \subseteq R \times R$ to reflect the role hierarchy relationship in the local domain, and $RH \subseteq RL \times RH$ to describe roles RL in the local domain to roles RF in the foreign domain relationship through role translation mapping.

An IRBAC state determines each user's role set (we use $auth\_role(u)$ to describe the role set belong to u), and each user's permission set (we use $auth\_perm(u)$ to describe the permission set belong to u), and the set of roles generated by dynamic mapping between two domains. Hence we can define the global static separation of duty constraint policy in IRBAC 2000 as follows:

Definition 3.2: (ISSoD: SSoD Constraint Policy in IRBAC 2000) A *k-n-2*SSoD (k-out-of-n-from-2 domain global static separation of duty) constraint policy in IRBAC 2000 can be expressed as

Design Engineering
ISSN: 0011-9342
Issue: 10 | Pages: 117 - 127

$$ISSoD < \{p_1, p_2, ..., p_n\}, \{D_1, D_2\}, k >$$

In the formula, each p_i corresponds a permission in the system, *n* represents an integer, *k* is an integer, and the condition $1 < k \le n$ is satisfied. This constraint policy does not allow less than *k* users from the same domain to have whole permissions in the permission sequence $\{p_1, p_2, ..., p_n\}$. In other words, this policy ensures that at least *k* users from two domains $\{D_1, D_2\}$ can obtain the whole permissions in $\{p_1, p_2, ..., p_n\}$ to implement a task. More general, the global static separation of duty constraint policy in multi domain can be defined as follows:

Definition 3.3: (GSSoD: SSoD Constraint Policy in Multi Domain) A *k*-*n*-*m*SSoD (k-out-of-n-from-m domain global static separation of duty) constraint policy in multi domain can be expressed as

$$GSSoD < \{p_1, p_2, ..., p_n\}, \{D_1, D_2, ..., D_m\}, k >$$

where each D_i corresponds a domain in the system, the number of permissions is *n*, the number of domains is *m* and the sum of users' number is *k* such that

$$(\sum_{i=1}^{m} |user(D_i)|) = k \wedge (\sum_{i=1}^{m} (|user(D_i)| \ne 0) \ge 2)$$

we use $|user(D_i)|$ to describe the number of users from D_i domain. The GSSoD constraint policy does not allow less than *k* users from the same domain to have whole permissions in the permission sequence $\{p_1, p_2, ..., p_n\}$. It can be seen clearly that the SSoD constraint policy in IRBAC 2000 is a special case of GSSoD constraint policy in multi domain when there is only two domains. Under more special situation, we can use $GSSoD < \{p\}, \{D_1, D_2, ..., D_m\}, k >$ to describe that there should not have less than *k* users from different domain that all of them have the same permission *p*.

Meanwhile, there may be further limited the users' number in each domain. In this situation, we can describe the strict GSSoD constraint policy as follows:

Definition 3.4:(SGSSoD: Strict GSSoD Constraint Policy in Multi Domain) A Strict *k*-*n*-*m*GSSoD (k-out-of-n-from-m domain global static separation of duty) constraint policy in multi domain can be expressed as

$$SGSSoD < \{p_1, p_2, ..., p_n\}, \{D_1, D_2, ..., D_m\}, \{k_1, k_2, ..., k_m\} >$$

where k_i describes the users' amount from corresponding D_i domain such that

$$|user(D_i)| = k_i \wedge (\sum_{i=1}^{m} (|user(D_i)| \ne 0) \ge 2)$$

This SGSSoD constraint strategy describes that no less than k_i users from D_i domain can jointly have the total permissions in $\{p_1, p_2, ..., p_n\}$. That means at least k_i users from corresponding D_i domain can obtain all these permission in $\{p_1, p_2, ..., p_n\}$. Under more special situation, we can use $SGSSoD < \{p\}, \{D_1, D_2, ..., D_m\}, \{k_1, k_2, ..., k_m\} >$ to describe that there

ISSN: 0011-9342
Issue: 10 | Pages: 117 - 127

should not have less than k_i users from corresponding domain D_i that all of them own the same permission *p*.

It can be seen that GSSoD constraint policy is a special case of SGSSoD constraint policy. It is also easy to see that the traditional SSoD constraint policy is a special case of all of the above SSoD constraint policy when there is only one domain. Hence, we can describe the relationships among the above static separation of duty constraint policy as follows:

$$SSoD \subset ISSoD \subset GSSoD \subset SGSSoD$$

Now we use a simple two domains example based on IRBAC 2000 to illustrate the concept in this paper. There are local domain *HUST* University andforeign domain *WHU*University in Fig 1. In local domain, there are a lot of roles such as Administrator, Chairman, Manager, Committeeman, Secretary and Student. In foreign domain, there are Administrator, Professor, Manager, AssoProfesser and Student. We can realize interoperation based on role mapping between these two domains. There are two kinds of role mapping between them: one is transitive association such as $Professor_{WHU} \rightarrow Committeeman_{HUST}$ (labeled as 1). In this situation, foreign domain role $Professor_{WHU}$ will be translated to the local domain role $Committeeman_{HUST}$, at the same time all the ancestors of foreign domain role $Professor_{WHU}$ also will map to the local domain role $Committeeman_{HUST}$. The other type of role mapping is non-transitive association such as $Assoprofessor_{WHU} \mapsto Secretary_{HUST}$ (labeled as 2NT). In this situation, foreign domain role $Assoprofessor_{WHU}$ will be translated to local domain role $Secretary_{HUST}$ on the one hand, on the other hand this translation deny foreign role $Professor_{WHU}$ and $Administrator_{WHU}$ from inheriting this association.

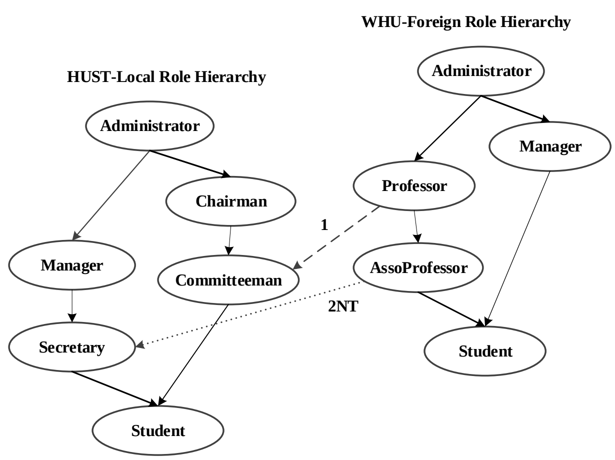

Fig 1: Role mapping between HUSTdomain and WHU domain

Based on IRBAC 2000 model, we discuss the thesis defense issue mentioned above. In this question, it can be accomplished by several steps as follows:

ISSN: 0011-9342
Issue: 10 | Pages: 117 - 127

1. The pleader comes from university *HUST* that provides the relevant information to reflect the academic level in order to take part in the thesis defense (This operation is described as permission p_1);

2. The administrative department should verify the relevant information to determine the qualifications of the thesis defense (This operation is described as permission p_2);

3. The chairman from *HUST* university will organize and defend the dissertation (This operation is described as permission p_3);

4. The seven committeemen include the chairman check and approve the thesis defense (This operation is described as permission p_4);

5. The secretary takes detailed notes for the thesis defense issue (This operation is described as permission p_5).

Based on the traditional SSoD constraint policy, it can't describe the seven committeemen must come from the different domain (university). In this situation, we can assign the committeeman from *HUST* and *WHU* with the permission p_4. Hence, we can use the GSSoD constraint policy to describe this requirement in order to overcome the above disadvantage as follows:

$$GSSoD < \{p_4\}, \{HUST, WHU\}, 7 >$$

The above GSSoD constraint policy does not allow fewer than seven users that come from the same university which all have the permissions p_4. That is to say, users from different universities are required to complete a task together. Furthermore, we can use the SGSSoD constraint policy to describe the situation that the number of committeemen is limited. Obviously, this is the embodiment of real security needs in the real world. For example, we require the 4 committeemen must come from the foreign domain *WHU* can be described as:

$$GSSoD < \{p_4\}, \{HUST, WHU\}, \{3,4\} >$$

The above SGSSoD constraint policy does not allow fewer than three committeemen from *HUST*University and four committeemen from *WHU*University to do the thesis defense together.

IV.ENFORCING GSSoD CONSTRAINT POLICY IN MULTI DOMAIN

In multi domain, we need determine and enforce the system's security requirements in order to make the information and resource security. Hence we should define the safety for the multi domain as follows. (In this paper, we just consider the system's safety under GSSoD constraint policy and the way of enforcing GSSoD constraint policy in multi domain because SGSSoD constraint policy can be divided into a set of SSoD constraint policy and SSoD constraint policy and ISSoD constraint policy both belong to GSSoD constraint policy.)

Definition 4.1:(GSSoD Safety) If in the multi domain state γ, there are no any $k-1$ user permissions from the same domain have the same elements in $\{p_1, p_2, ..., p_n\}$, we say the multi domain state γ is safe. More precisely

$$\forall u_1, u_2, ..., u_{k-1} \in U \wedge (\sum_{i=1}^{m}(|user(D_i)|) = 1)$$

we have

$$\{p_1, p_2, ..., p_n\} \not\subset (\bigcup_{i=1}^{k-1} auth\_perm(u_i))$$

An multi domain environment state γ is safe under a set of GSSoD constraint policy E if it is safety for each constraint policy in the set constraint policy E, this multi domain situation is writedas $safe_E(\gamma)$. Now given a set of GSSoD constraint policy E, assume that the beginning of the security system is safety based on the set of GSSoD constraint policy E. One need to judge the security of every operation that can affect the system security. Hence, we can define the safety checking problem for GSSoD constraint policy as follows:

Definition 4.2:(SC-GSSoD) The GSSoD constraint policy safety checking problem is defined as follows: Given an multi domain state γ and a set of GSSoD constraint policy E, determine if $safe_E(\gamma)$ is true.

(1) Directly Enforcing GSSoD Constraint Policy

This approach can guarantee a multi domain state γ can be safe corresponding to a series of GSSoD constraint policy E, which proves to be difficult.

Theorem 1:coNP-complete is the verification problem of SC-GSSoD.

Proof.We check the multi domain state is safe or not based on a series of GSSoD constraint policy is coNP-complete using the similar theorem in [10] to check if an RBAC state is safe on the basis of a series of SSoD constraint policy.

We firstly show that confirming that if $safe_E(\gamma)$ is false which is denoted by $\overline{SC-GSSoD}$ in NP. If an multi domain state γ is not safety based on a set of GSSoD constraint policy*E*, there must exist an GSSoD constraint policy

$$GSSoD < \{p_1, p_2, ..., p_n\}, \{D_1, D_2, ..., D_m\}, k >$$

in the set of GSSoD constraint policy E where $k-1$ users' permissions from the same domain have the same elements in $\{p_1, p_2, ..., p_n\}$. Hence, we can calculate the $k-1$ users' permissions and verify whether each user permissions in the permissions set $\{p_1, p_2, ..., p_n\}$ in thisGSSoD constraint policy.

We reduce this problem to the set cover problem, and determine whether the GSSoD configuration in multi domain is NP hard. According to the setcover issue, The input element are a finite set *S*, the subsets of *S*construct a family $F = \{S_1, S_2, ..., S_l\}$,and the budget is *B*. The goal is to verify whether there are *B* sets in *F*, and the union of these *B* sets is *S*. Prove that the problem isNP-complete[12].

The conversion can be done in the following ways. For a given *S*, *F* and *B*, the corresponding GSSoD constraint policy can be constructed as follows: we assume each element in the set *S* corresponds to each permission in the constraint policy, *m* corresponds to the

ISSN: 0011-9342
Issue: 10 | Pages: 117 - 127

amount of set elements in set F, and n corresponds to the amount of elements in set S, $S_i(1 \le i \le m)$ of subset of $\{p_1, p_2,..., p_n\}$ means the users' permission set from domain $D_i(1 \le i \le m)$. Thus, we can constructed a GSSoD constraint policy $GSSoD < \{p_1, p_2,..., p_n\}, \{D_1, D_2,..., D_m\}, \{k_1, k_2,..., k_m\} >$. Where $k_i(1 \le i \le B)$ means users' number from D_i domain and $\sum_{i=1}^{m} k_i = k$. Obviously, the goal is to verify if there exists B set $\sum_{i=1}^{B} k_i = k$ in F whose union is $S = \{p_1, p_2,..., p_n\}$. To put it another way, if and only if the B set in F covers S, the GSSoD configuration built in multi domains is not enforceable.□

According to the proof, it can be seen that it is intractable to enforce GSSoD constraint policy directly in multi domain. However, we can enforce GSSoD constraint policy in multi domain efficiently when the GSSoD constraint policy sequencein *E*in multi domain all have small number of users *k* and small number of domains *m*. For example, one just need calculate the user's permission set and determine if it is a superset of the permission set in the policy when $k = m = 2$. Obviously, it can be seen that the time complexity under worst conditions is $O((N_{lu} + N_{fu})(N_{lr} + N_{ir} + N_{lp} + N_{ip}))$, where N_{lu} means the number of local domainusers, N_{fu} means the number of foreign domainusers based on role mappings, N_{lr} means the local domainroles' number, N_{ir} meanstheassociation roles' number through role mappings, N_{lp} means the local domainpermissions' number, N_{ip} means permissions' number according to association roles based on role mappings .

(2) Enforcing GSSoD Constraint Policy by Constraint

In RBAC system, SMER constraint is often used to enforce SSoD constraint policy. Our GSMER constraint is directly motivated by it. We firstly present a generalized form of GSMER constraint and study how to introduce GSMER constraint to graranteeGSSoD constraint policy in multi domain.

Definition 4.3:(Global SMER)A k-n-m GSMER (k-out-of-n-from-m domain GlobalSMER)constraint in multi domain is described as

$GSMER < \{r_1, r_2,..., r_n\}, \{D_1, D_2,..., D_m\}, k >$

Where each element in $\{r_1, r_2,..., r_n\}$is a role. This GSMER constraint prevents a user from only one domain that the user is a member of k or more roles in role set $\{r_1, r_2,..., r_n\}$.

Definition 4.4: (GSMER Satisfaction) We say a state γ in multi domain is safecorresponding to GSMER constraint if in state γ no user comes from only one domain have k or more roles in role set $\{r_1, r_2,..., r_n\}$. More precisely

$$\forall u \in U \wedge (\sum_{i=1}^{m} (|user(D_i)| \ne 0) = 1)$$

we have

$$| auth\_roles(u) \cap \{r_1, r_2,..., r_n\} | < k$$

Theorem 2: The verification problem of $safe_c(\gamma)$ isin P.

Proof. The verification of $safe_c(\gamma)$ is as follows. We firstly compute each user's role set in multi domain, and then calculate the intersection between them and $\{r_1, r_2, ..., r_n\}$ for each GSMER constraint in C. Secondly we calculate the domain number of those roles belong to. Finally, we compare the results with the users' number k and the domains' number 2 respectively. The time complexity of the algorithm is $O(N_u N_a M)$, where N_u is users' number, N_a is roles' number and M is constraints' number. □

Definition 4.5:(GSMER Constraint Requirement Enforce GSSoD Constraint Policy) Let $C$is a series of GSMER constraint requirement, and R is a set of GSSoD constraint policy requirement, we say C enforce R if and only if $safe_c(\gamma) \rightarrow safe_E(\gamma)$.

Theorem 3: Given a k-n-m GSSoD constraint policy requirement canbe enforced by 2-2-2 GSMER constraint sets as

$$\bigcup_{i \neq j, x \neq y}^{i,j \in [1,n], x,y \in [1,m]} \{C = GSMER < \{r_i, r_j\}, \{D_x, D_y\}, 2 >\}$$

Proof. The GSSoD constraint policyrequirementdescribes that k users should cover all n roles on the one hand,on the other hand, all of them cannot come from the same domain. The GSMER constraint sets mean that every two role sets in$\{r_1, r_2, ..., r_n\}$that cover all n rolesfrom different domain ($n \geq 2$), thus $safe_E(\gamma)$ is true.□

V. CONCLUSIONS

We discussed the disadvantages of traditional separation of duty constraint policy in multi domain and also defined the ISSoD constraint policy, GSSoD constraint policy and SGSSoD constraint policy in order to overcome the insufficient of the traditional separation of duty constraint policy to satisfy the global domain security requirements in this paper. The results show that it is coNP-complete to implement GSSoD constraint strategy directly in multi domain. Furthermore,we also given how to use a set of GSMER constraints to enforce GSSoD constraint policy in multi domain. One question that has yet to be resolved is to find the least restrictive set of GSMER constraints to enforce the GSSoD constraint policy.

ACKNOWLEDGEMENTS

The work is finished under the support of the Joint Fund for National Natural Science Foundation of China and Henan Province for Fostering Talents under grant no. U1304619. We would like to express our heartfelt thanks to all of anonymous for their help and advice.

REFERENCES

[1] Ferraiolo, D. F., Cuigini, J. A., Kuhn, D. R.(1995)Role-based access control (RBAC):Features and motivations, Proc. of the 11th Annual Computer Security Applications Conference: 241-248

ISSN: 0011-9342
Issue: 10 | Pages: 117 - 127

[2] Ferraiolo D, Sandhu R, Gavrila S, Kuhn D, Chandramouli R.(2001) Proposed NIST standard for role based access control, ACM Transactions on Information and System Security, 4(3): 224-274

[3] S. Jha, N. Li, M.Tripunitara, Q. Wang, W. Winsborough. (2008) Towards formal verification of role-based access control policies, IEEE Trans.Depend. Sec. Comput. 5(4): 242-255

[4] S. Jha, S. Sural, V. Atluri, J. Vaidya(2018) Specification and verification of separation of duty constraints in attribute-based access control. IEEE Transactions on Information Forensics and Security13(4): 897-911

[5] A. Kapadia,J. Al-Muhtadi, R. Campbell, D. Michunas (2000) IRBAC2000:Secure interoperability using dynamic role translation, Technical Report: UIUCDCS-R-2000-2162

[6] Basit Shafiq, James B.D. Joshi, Elisa Gertino, Arif Ghafoor.(2005) Secure interoperation in a multi domain environment employing RBAC policies, IEEE transactions on knowledge and data engineering17(11):1557-1577

[7] Jianfeng Lu, Ruixuan Li, Zhengding Lu, Jinwei Hu, Xiaopu Ma (2009) Specification and enforcement of static separation-of-duty policies in Usage Control, ISC: 403-410

[8] J. H. Saltzer, M.D. Schroeder(1975) The protection of information in computer systems, Proc. of the IEEE, 63(9): 1278-1308

[9] Clark, D.D., Wilson, D. (1987) A comparison of commercial and military computer security policies, Proc.of 1987 IEEE Symposium on Security and Privacy: 184-238

[10] N.Li, Z.Bizri, M.V.Tripunitara (2004) On mutually exclusive roles and separation of duty, Proc. of the 1lth ACM Conference on Computer and Communications Security: 42-51

[11] Xiaopu Ma, Ruixuan Li,Zhengding Lu, Jianfeng Lu(2009)Global static separationof duty in multi-domains,Proc. of the 2009 international conference on multimedia information networking and security: 506-509

[12] C.H. Padaimitrion(1994)Computational Complexity, Addison Wesley Longman.