2009 International Conference on Multimedia Information Networking and Security

Global Static Separation of Duty in Multi-domains

Xiaopu Ma
College of Computer Science and Technology
Huazhong University of Science and Technology
Wuhan 430074, P. R. China
College of Computer and Information Technology
Nanyang Normal University
Nanyang 473061, P. R. China
e-mail: xpma@smail.hust.edu.cn

Ruixuan Li
College of Computer Science and Technology
Huazhong University of Science and Technology
Wuhan 430074, P. R. China
e-mail: rxli@hust.edu.cn

Zhengding Lu
College of Computer Science and Technology
Huazhong University of Science and Technology
Wuhan 430074, P. R. China
e-mail: zdlu@hust.edu.cn

Jianfeng Lu
College of Computer Science and Technology
Huazhong University of Science and Technology
Wuhan 430074, P. R. China
e-mail: lujianfeng @ smail.hust.edu.cn

***Abstract*—Separation of duty (SoD) is an important control principle in computer security. In the context of role-based access control, the Static SoD (SSoD) policies can be enforced by Statically Mutually Exclusive Roles (SMER) constraints. This paper studies the problem of SSoD in multi-domains in the context of IRBAC model firstly. Then investigates a question related to multi-domains: the Global SSoD (GSSoD) policy in order to satisfy the global requirements. It shows that directly enforce the problem is coNP-complete. Finally, enforcing GSSoD policies by the Global Statically Mutually Exclusive Roles (GSMER) constraints in IRBAC model is given.**

Keywords-Separation of Duty; global static separation of duty; global statically mutually exclusive roles

I. INTRODUCTION

The principle of Separation of duty (SoD) policy is one of the most important principles in the design of protection mechanisms for secure computer systems [1, 2]. Its purpose is to ensure that failures of omission or commission within an organization are caused only by collusion among individuals and, therefore, are minimized by assigning individuals of different permissions or divergent interests to separate tasks [3]. There are at least two approaches to enforce a SoD policy, one is Dynamic SoD (DSoD), and the other is Static SoD (SSoD). Each SSoD policy states that no k-1 users together have all permissions to complete a sensitive task [4].

Now with the rapid development of network technology and distributed applications, information interaction and cooperation in multi-domains have become increasingly frequent [5]. Basit Shafiq [6] proposed a policy composition framework that integrates the role based access control (RBAC) [7] policies of multiple domains to facilitate secure information and resource sharing in a multi-domains, especially SSoD policy. Xinyu Wang et al. [5] also proposed a security violation detection method for RBAC based interoperation to meet the requirements of secure interoperation among multi-domain systems. However, all of the researchers considered the SSoD policy only about how to enforce the SSoD policy in local domain and how to solve the violation of SSoD policy because of role mapping, to the best of our knowledge. It is our belief that for an integrated system composed of multi-domains, SSoD policy must be done at three levels: firstly the SSoD policy should be enforced in local domain, and then should be solve the violation of SSoD policy because of role mapping, finally the SSoD policy should be enforced at the global domain.

In this paper, we only study the SSoD policy in multi-domains. We define a simple specification for the GSSoD which is a global domain requirement in this paper. Second, we pose and answer the fundamental questions related to enable the use of Global Statically Mutually Exclusive Roles (GSMER) constraints to support the GSSoD policies in multi-domains. We show that directly enforce the GSSoD policies is a coNP-complete problem. Lastly, we show how to use GSMER constraints to enforce the GSSoD policies.

The rest of this paper is organized as follows. We discussed related work in Section 2, and give preliminary definition in Section 3. In Section 4, we study the GSSoD policies in multi-domains and how to directly enforce it and how to use GSMER constraints to enforce it. We conclude this paper in Section 5

II. RELATED WORK

SoD was first introduced by Saltzer and Schroeder [8] as one of the design principles for protecting information, to our knowledge. So the research community has taken an

978-0-7695-3843-3/09 $26.00 © 2009 IEEE
DOI 10.1109/MINES.2009.117

active interest in incorporating SoD controls into computer systems since the late 1980s. One of the rules of Clark and Wilson model [1] required that the system must associate with each user a valid set of programs to be run, and the data center controls must ensure that these sets meet the separation of duty. Since then, several papers have studied SoD.

Although many researchers have considered SoD problems, it should be noted that most existing approaches to SoD only consider constraint sets with precisely two elements, the exceptions being the RCL 2000 specification language [9]. And the distinction between SoD policy objectives and Statically Mutually Exclusive Roles (SMER) constraints, as a mechanism to enforce them, is sometimes not clearly made. For example, Ferraiolo et al. defined SoD as: "A user is authorized as a member of a role only if that role is not mutually exclusive with any of the other roles for which the user already possesses membership." [10]. So Li et al. [4] studied the relationship between Static Separation of Duty (SSoD) policies and SMER constraints and how to enforce SSoD policies by SMER constraints.

With the development of network technology and distributed applications, SoD requirements become an important issue in multi-domains. Several research efforts have been devoted to the topic of policy composition in the multi-domains environment especially the SoD policy [11]. In order to accomplish the interoperation problem, Kapadia et al. [12] presented IRBAC 2000 model which provide a secure interoperability using dynamic role translation base on RBAC. But this method did not consider the problem of the violation of SoD policy which is induced by role mapping between domains. Hence Cuihua Zuo et al. [13] proposed an algorithm to detect the role mapping violates SoD policy. However, both of them did not research the problem of SoD policy in the global domain in order to satisfy the global requirements.

III. PRELIMINARY DEFINITIONS

This section gives a precise definition for the GSSoD policy in multi-domains. It assumes that there are four countably infinite sets: R (the set of all possible roles), U (the set of all possible users), P (the set of all possible permissions), and D (the set of all possible domains)

Definition 1 A k-n-m GSSoD (k-out-of-n-from-m global static separation of Duty) policy is expressed as

$$\text{gssod} < \{p_1, p_{2,} \dots p_n\}, \{D_{1,} D_{2,} \dots D_m\}, k >$$

Where $\{p_1, p_{2,} \dots p_n\} \subset P$ is a set of permissions and $\{D_{1,} D_{2,} \dots D_m\} \subset D$ is a set of domains, n means the number of permission, m means the number of domain such that $2 \leq m$ and k means the total number of users such that

$$\left(\sum_{i=1}^{m} |D_i|\right) = k \wedge \left(\sum_{i=1}^{m} |D_i| \neq 0 \geq 2\right)$$

Where $|D_i|$ means the number of users from domain D_i .This policy means that there should not only have a set of fewer than k users that come from $\{D_{1,} D_{2,} \dots D_m\}$ together have all the permissions in $\{p_1, p_{2,} \dots p_n\}$, but also both of them cannot come from the same domain. In other word, at least k users that come from the different domain $\{D_{1,} D_{2,} \dots D_m\}$ are required to perform a task that needs all these permissions.

Definition 2 (IRBAC state). An IRBAC state γ is a 4-tuple <UA, PA, RH, RP>, in which the user assignment relation $UA \subset U \times R$ associates users with roles in the local domain, the permission assignment relation $PA \subset R \times P$ associates roles with permissions in the local domain, the role hierarchy relation $RH \subset R \times R$ specifies an acyclic relation among roles, and the role mapping relation between multi-domains $RP \subset RL \times RF$ reflects role mappings between local domain roles RL and foreign domain roles RF.

An IRBAC state γ =<UA, PA, RH, RP> determines the set of roles of which each user is a member, and the set of permissions for which each user is authorized, and the set of role mappings for establishes a flexible dynamic role translation between different domains.

Definition 3 (GSSoD Safety) we say that an IRBAC state γ is safe with respect to a GSSoD policy $\text{gssod} < \{p_1, p_{2,} \dots p_n\}, \{D_{1,} D_{2,} \dots D_m\}, k >$ if in state γ no k-1 users come from only one domain together have all the permissions. More precisely

$$\forall u_1, \dots u_{k-1} \in u \wedge \left(\sum_{i=1}^{m} |D_i| \neq 0\right) \geq 2)$$
$$\left(\bigcup_{i=1}^{k-1} \text{auth\_perm}_\gamma[u_i]\right) \not\supseteq \{p_1, p_2, \dots p_n\}$$

An IRBAC state γ is safe with respect to a set E of GSSoD policies if it is safe with respect to every policy in the set, we write this as $\text{safe}_E(\gamma)$.

Now we use an example to illustrate the concepts in this paper. This example is shown in figure 1 and is explained below.

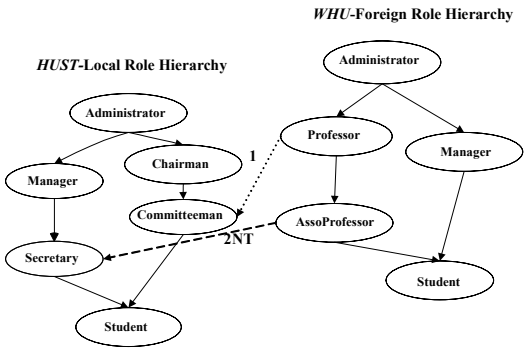

Figure 1. Associations between multi-domains

In Fig. 1, there have two domains, one is local domain HUST, the other is foreign domain WHU. The interoperation between these domains is achieved by introducing role mapping between the local domain and the

foreign domain. There have two types of role mapping: one is transitive associations, in figure 1 we can see $\text{Professor}_{\text{WHU}} \longrightarrow \text{Committeeman}_{\text{HUST}}$ (labeled as 1). Hence the role $\text{Professor}_{\text{WHU}}$ from foreign domain will be translated to the role of $\text{Committeeman}_{\text{HUST}}$. This also implies that all the ancestors of $\text{Professor}_{\text{WHU}}$ will map to the $\text{Committeeman}_{\text{HUST}}$. We also can see non-transitive association $\text{Assoprofessor}_{\text{WHU}} \mapsto \text{Secretary}_{\text{HUST}}$ (labeled as 2NT). Hence $\text{Assoprofessor}_{\text{WHU}}$ will be translated to $\text{Secretary}_{\text{HUST}}$ and deny $\text{Professor}_{\text{WHU}}$ and $\text{Administrator}_{\text{WHU}}$ from inheriting this association.

As an example focusing mainly on the SSoD, consider the thesis defense mentioned above for a student who comes from HUST. In this situation, we need several steps to accomplish the task: (1) the student comes from domain HUST should provide the material and recording the details of the material on the form (P1); (2) the two managers come from HUST should verify the details on the form in order to decide the qualification for the thesis defense (P2); (3) the one chairman comes from HUST organizes the thesis defense (P3); (4) the five committeemen check and approval the thesis defense (P4); (5) the secretary comes from HUST records the details of the thesis defense (P5). According to the traditional definition about SSoD from Li et al. [4], it can get the description as follows:

$$\text{ssod} < \{p_1, p_{2,} p_{3,} p_{4,} p_5\}, k >$$

Where $1<k\leq5$, so there have mainly two problems:

The five people can't finish the thesis defense in the real world; more even, the SSoD policy can't be enforced if all of the committeemen come from the same domain (HUST).

So in Fig. 1, we map the foreign role Professor from WHU to the local role Committeeman in HUST. Then the Professor in WHU can get the Committeeman role in HUST, and also get the permissions of role Committeeman in HUST. Then we can define the GSSoD as follows:

$$\text{ssod} < \{p_1, p_{2,} p_{3,} p_{4,} p_5\}, \{\text{HUST}, \text{WHU}\}, \{10\} >$$

Which means that there should not only exist a set of fewer than ten users that together have all the permissions in {p1, p2, p3, p4, p5}, but also the number of user should not come from the one university. In other word, in the thesis defense situation, we need different committeemen from different university to cooperation. It is the global requirements in the real world.

IV. ENFORCING GSSOD POLICIES IN MULTI-DOMAINS

This section will discuss how to enforce the GSSoD policies in multi-domains in this section. Now given a set E of GSSoD policies, suppose an IRBAC system starts at a state that is safe with respect to E. each time one is about to make a change to the system that may affect safety, one should check whether the IRBAC state safety or not.

A. Directly Enforcing GSSoD Policies

This approach to ensuring that an IRBAC state γ is safe with respect to a set E of GSSoD policies, which turns to be out to be intractable.

Theorem 1 The verification problem of $\text{safe}_{\text{E}}(\gamma)$ is coNP-complete.

Proof. The proof is similar to the one in [4] for the theorem that checking whether an RBAC state is safe or not with respect to a set of SSoD policies is coNP-complete.

We first show that determining that if $\text{safe}_{\text{E}}(\gamma)$is false in NP. If an IRBAC state γ is safe with respect to a set E of GSSoD policies, there must exist an GSSoD policy $\text{gssod} < \{p_1, p_{2,} \dots p_n\}, \{D_{1,} D_{2,} \dots D_m\}, k >$ in E such that k-1 users that comes from different domains together have all the n permissions in the policy, verifying that the guess is correct can be done in polynomial time: compute the union of the $k-1$ users' permissions and check whether it is a superset of the set of permissions in the GSSoD policy.

We now show that determining whether a GSSoD configuration is not enforceable is NP-hard by reducing the set covering problem to it. In the set covering problem, the inputs are a finite set S, a family $F = \{S_1, \cdots, S_l\}$ of subsets of S, and a budget B. The goal is to determine whether there exists B sets in F whose union is S. This problem is NP-complete [14].

The reduction is as follows. Given S, F, and B, constructs a GSSoD policy g as follows: let each element in S map to a permission in the policy, let k be B+1 and let n be the size of S. we have constructed a

$$\text{gssod} < \{S_1, S_{2,} \dots S_n\}, \{k_1, k_2 \dots k_B\} >$$

Where k_i $(1 \leq i \leq B)$ means the number of users that come from the domain i, $F_i = \{S_1, \cdots, S_i\}$ $(1 \leq i \leq B)$ of subset of $\{S_1, S_{2,} \dots S_n\}$ means the permissions from domain i, and $\sum_{i=1}^{B} k_i = k$. It obliviously that the constructed GSSoD configuration is not enforceable if and only if B sets in F cover S. □

While enforcing GSSoD directly is, in general, intractable, efficient algorithms for enforcing GSSoD policies exist when all the GSSoD policies in E have small k and small m. For example, when checking whether γ is safe with respect to a 2-n-2 GSSoD policy,

One only needs to compute the set of permissions of every user and check whether it is a superset of the permissions in the policy. This has a worst-case time complexity of $o((N_{lu} + N_{fu})(N_{lr} + N_{ir} + N_{lp} + N_{ip}))$, where N_{lu} is the number of users in the local domain N_{fu} is the number users from foreign domain that have associations with local domains through role mappings, N_{lr} the number of roles in local domain, N_{ir} the number of association roles through role mappings, N_{lp} the number of permissions in local domain, N_{ip} the number of permissions of association roles through role mappings between foreign roles and local roles.

B. Enforcing GSSoD Policies by Constraints

In RBAC, the SMER constraints are introduced to enforce SSoD policies; our Global Static Mutually Exclusive Roles (GSMER) constraints are directly motivated by it. In this section, we show how to u GSMER constraints to enforce GSSoD policies. We now present a generalized form of such constraints.

Definition 4 (GSMER) A k-n-m GSMER (k-out-of-n-from-m global statically mutually exclusive roles) constraint is expressed as

$$\text{gsmer} < \{r_1, r_2, \dots r_n\}, \{D_1, D_2, \dots D_m\}, k >$$

Where $\{r_1, r_2, \dots r_n\}$ are a set of roles and the other parameters have the same definition as above. This constraint forbids a user from $\{D_1, D_2, \dots D_m\}$ being a member of k or more roles in $\{r_1, r_2, \dots r_n\}$ that comes from only one domain.

Definition 5 (GSMER Satisfaction). We say that an IRBAC state γis safe with respect to GSMER constrain when

$$\forall u \in U \ \left(\left|\text{auth\_roles}_\gamma[u] \cap \{r_1, r_2, \dots r_n\}\right| < k\right)$$
$$\wedge \left(\sum_{i=1}^{m} |D_i| \neq 0\right) > 2$$

It means that no user is a member of k or more roles in $\{r_1, r_2, \dots r_n\}$ that comes from only one domain, and we write this as $\text{safe}_c(\gamma)$.

Theorem 2 The verification problem of $\text{safe}_c(\gamma)$is in P.

Proof. One algorithm for verify $\text{safe}_c(\gamma)$ is as follows. For each k-n-m GSMER constraint in C and for each user and domain in γ, one first computes the set of all the roles the user is a member of in multi-domains, and then counts how many roles in this set also appear in the set of $\{r_1, r_2, \dots r_n\}$ in the GSMER constraint, and also counts how many domains about those roles that belongs to, and finally compares those number with k and 2. This algorithm has a time complexity of $O(N_u N_\alpha M)$, where Nu is the number of users in γ, Na the number of $\{r_1, r_2, \dots r_n\}$in γ, and M is the number of constraints. □

Definition 6 (GSMER enforce GSSoD) Let C be a set of GSMER constraints, and R be a set of GSSoD requirements, we say C enforce R if and only if

$$\text{safe}_c(\gamma) \Longrightarrow \text{safe}_E(\gamma)$$

Theorem 3 Given a k-n-m GSSoD requirements can be enforced by 2-2-2 GSMER constraints sets

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

Proof. The requirement GSSoD means that k users which do not come from the same domain are required to cover all n roles. The constraint set means that every two role sets in $\{r_1, r_2, \dots r_n\}$ that comes from the different domain, then n domains are needed to cover the n roles, as 2 ≤n, thus $\text{safe}_E(\gamma)$ is true. □

V. Conclusion

In this paper, we have studied the problem of SSoD in multi-domains and then defined the GSSoD policy in order to satisfy the global requirements. It has been shown that directly enforce the GSSoD policy is coNP-complete. Then we studied how to use GSMER constraints for enforcing GSSoD policies.

Acknowledgment

This work is supported by National Natural Science Foundation of China under Grant 60873225, 60773191 and 60403027, National High Technology Research and Development Program of China under Grant 2007AA01Z403. The authors would like to thank the anonymous reviewers for their valuable comments.

References

[1] Clark, D. D. and Wilson, D. A comparison of commercial and military computer security policies. In Proceedings of 1987 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, April 1987, pp.184-238.

[2] Clark D.D., and D. R. Wilson. Evolution of a Model for Computer Integrity. In Report of the Invitational Workshop on Data Integrity, Z.G. Ruthberg and W.T.Polk (eds.), NIST Special Publication 500-168, Appendix A, September 1989.

[3]Virgil D.Gligor, Serban I.Gavrila and Dvaid Ferraiolo.On the formal definitions of separation-of-duty policies and their composition. In Proceedings of IEEE Symposium on Research in Security and Privacy, 1998, pp.172-183.

[4]N.Li, Z.Bizri, and M.V. Tripunitara. On mutually-exclusive roles and separation of duty. In Proceeding of the 11th ACM Conference on Computer and Communications Security, 2004, pp. 42-51.

[5]Xinyu Wang, Xiaohu Yang, Chao Huang and Di Wu.Security violation detection for RBAC based interoperation in distributed environment. IEICE TRANS.INF. & SYST., 2008, pp.1447-1456.

[6]Basit Shafiq, James B.D. Joshi, Elisa Gertino and Arif Ghafoor. Secure interoperaion in a multidomain environment employing RBAC policies. IEEE transactions on knowledge and data engineering. 2005, pp. 1557-1577.

[7]Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, et al. Role-based access control models, IEEE Computer, 1996, pp. 38-47.

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

[9]Ahn, G.J., and Sandhu, R. Role-based authorization constraints specification. ACM Transactions on Information and System Security. 2000, pp. 207-226.

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

[11]S. Dawson, S. Qian, and P. Samarati, Providing Security and Interoperation of Heterogeneous Systems, Distributed and Parallel Databases, Aug. 2000, pp. 119-145.

[12]Apu Kapadia, Jalal Al-Muhtadi, R. Campbell, et al. IRBAC2000: Secure interoperability using dynamic role translation. University of Illinois, Technical Report: UIUCDCS-R-2000-2162, 2000.

[13] Cuihua Zuo, Ruixuan Li, Hongmu Han and Zhengding Lu. Security Assurance for Dynamic Role Mapping in a Multi-domain Environment. In Proceeding of the International Conference of Computation and Intelligence and Security, Dec. 2007, pp. 735-739.

[14]C.H.Padaimitrion. Computational Complexity. Addison Wesley Longman, 1994.