International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.19-32
http://dx.doi.org/10.14257/ijsia.2014.8.1.03

Modeling and Analysis of SMER Constraints Violation in IRBAC 2000 Model Based on Colored Petri Nets

Meng Liu[1,2,*] and Xuan Wang[1]

[1]*Computer Application Research Center, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen 518055, China*
[2]*School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai 264209, China*
liumeng@sdu.edu.cn
**The corresponding author*

Abstract

Interoperable Role-Based Access Control (IRBAC) 2000 model can be used to accomplish security interoperation between two or more administrative domains via role association and dynamic role translation. However, Static Separation of Duties (SSoD) is not considered in the IRBAC 2000 model, so the problem of inter-domain static mutual exclusive roles constraints violation can arise. This paper proposes a novel method based on colored Petri nets to model and analyze IRBAC 2000 model so as to detect static mutual exclusive roles (SMER) constraints violation. The necessary and sufficient conditions for SMER constraints violation in the IRBAC 2000 model are demonstrated. A graphical detection model based on Colored Petri net of SMER constraints violation is presented and then a more complicated case study is used to illustrate the efficiency of the proposed model. Moreover, some prerequisites for avoiding SMER constraints violation and guaranteeing the model security while adding new role association or user-role assignment are also discussed, analyzed and detailed based on colored petri net model in this paper.

Keywords: *Interoperation, static separation of duties, static mutual exclusive roles, dynamic role translation, colored Petri nets, prerequisites*

1. Introduction

Kapadia *et al.*, propose the IRBAC2000 model to be used to make meaningful access control decisions for secure interoperability between two security domains under the Role-based Access Control (RBAC) model [1, 2] and the model introduces an approach that quickly establishes a flexible policy for dynamic role translation (DRT) using role associations [3]. As we all know, secure interoperation is a key issue to protect shared data and information between two domains. RBAC supports three well-known security principles: least privilege, separation of duties and data abstraction. However, secure interoperability between two domains must guarantee two principles [4]: (1) Security: Any access not permitted within an individual system must also be denied under secure interoperation. (2)Autonomy: Any access permitted within an individual system must also be permitted under secure interoperation. Separation of duties (SOD) is one of three basic principles supported by RBAC, but reference [6] points out that it is possible to occur SMER constraints violation because that SSoD is out of consideration in IRBAC2000 model and analyzes several kinds of cases for SMER constraints

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2014 SERSC

violation due to dynamic role translation in detail. Moreover, reference [6] proposes an approach to check the security problem and provide a protective mechanism utilizing prerequisite conditions to enforce the security of the IRBAC 2000 model. Zhai *et al.*, [7] continue to study and explore the problem and point out that the conclusions in [6] are incomplete. In [6] they only discuss the case of one role in the foreign domain inheriting from roles belonging SMER constraints violation in the local domain and do not consider the SMER constraints violation in the local domain owing to one improper user-role assignment in the foreign domain, which is the underlying cause. So the approach and prerequisite conditions in [6] are all incomplete and a new detection approach and prerequisite conditions statements are presented to guarantee the security of IRBAC 2000 model. These approaches in [6] and [7] are all used to discuss the problem from the perspective of mathematical logic and logical reasoning, which is abstract, complicated and not intuitive. Petri net has a graphical representation and a well-defended rigorous semantics and can be used to verify security requirements. Therefore a novel method of analyzing the problem based on colored Petri nets (CPN) is proposed in this paper, which is very easy and visualized to be used to analyze the SMER constraints violation problem.

2. Preliminaries

The important concepts of the IRBAC2000 model and SMER constraints violation are described as follows. The details can refer related literature.

2.1. IRBAC2000 Model

The IRBAC2000 model can enforce interoperation by role associations between any two management domains [3], so the case of interoperation between two domains is discussed in this paper. Suppose that there are two domains, Domain D_0 and Domain D_1, and the local domain is D_0, the foreign domain is D_1. The role set of the local domain can be denoted by R_0 and the role set of the foreign domain can be denoted by R_1. The role hierarchy for the role set R_0 can be denoted by H_0, and the role hierarchy for the role set R_1 can be denoted by H_1. Suppose that x and y are two roles in the same domain, which all come from domain D_0 or D_1. $y \geq x$ means that y is an ascendant, and x is a descendant of y, or all permission of x are also permissions of y, and all users of y are also users of x. Associations are used to enforce dynamic role translation from R_1 of the foreign domain to R_0 of the local domain so as to accomplish the authorization function between two administrative domains. Suppose that $x \in D_0$, $y \in D_1$, then one association from y to x denotes that all permissions of x can be inherits by y such that all users of y in Domain D_1 can activate x and all descendants of x, and the required permissions can be available. Two kinds of associations can be defined: transitive and non-transitive associations. A transitive association from y to x can be denoted by $y \rightarrow x$, and this implies that y and all ascendants of y will map to x and all descendants of x. A non-transitive association from y to x can be denoted by $y \rightarrow_{NT} x$, and this implies that y can map to x but all ascendants of y will be forbidden directly to map to.

In Figure 1, an example of IRBAC2000 model is shown. We can see the association from $Guest_{R_1}$ to $Guest_{R_0}$ (labeled as 1), which can be denoted by $Guest_{R_1} \rightarrow Guest_{R_0}$. The association is a transitive association and this implies that $Guest_{R_1}$ and its ascendants, { $Doctor_{R_1}$, $Nurse_{R_1}$,

 Copyright ⓒ 2014 SERSC

$Director_{R_1}$} can be translated to $Guest_{R_0}$. The association labeled as 2 is a non-transitive association and can be denoted by $Doctor_{R_1} \rightarrow_{NT} Researcher_{R_0}$. $Doctor_{R_1}$ can be translated to $Researcher_{R_0}$,but $Director_{R_1}$ cannot be translated directly to $Researcher_{R_0}$, *i.e.*, all users of $Director_{R_1}$ cannot activate directly $Researcher_{R_0}$ of domain D_0. Because all users of one role can acquire the membership of all descendants of the role in RBAC model, all users of $Director_{R_1}$ can be translated to $Researcher_{R_0}$ by the membership of $Doctor_{R_1}$. So we do not have to consider whether one association is transitive or not while analyzing the SMER constraints violation problem.

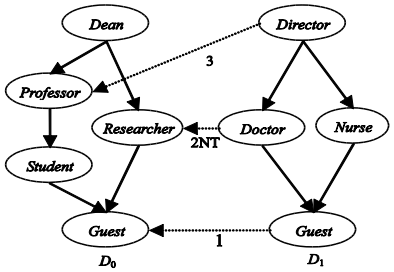

Figure 1. An Example of Dynamic Role Translation of IRBAC 2000 in Reference [7]

2.2. SMER Constraints Violation

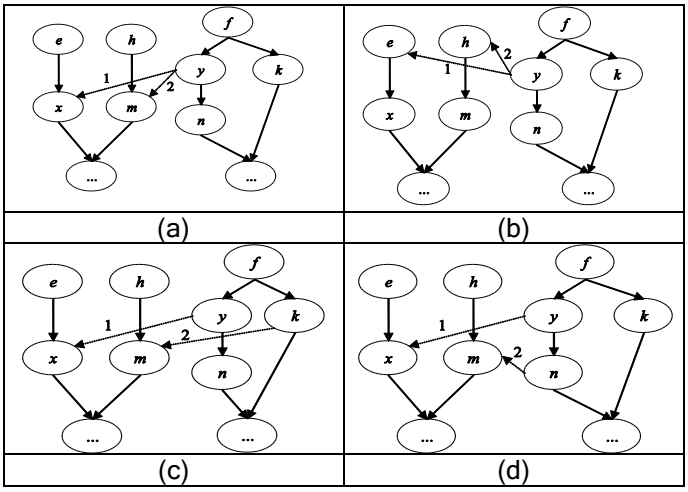

Figure 2. Four Cases of SMER Constraints Violation in Reference [6]

Four kinds of cases of SMER constraints violation in IRBAC2000 model are discussed and analyzed in [6]. In Figure 2, suppose that x and m belong the same SMER constraint. In Figure 2(a), y of the foreign domain can be translated directly to x and m of the local domain whatever the two associations labeled 1 and 2 are transitive or not according to discussion in [6]. y can acquire directly the memberships of x and m, which are mutual exclusive roles, and any one user of the foreign cannot be assigned to y. In Figure 2, y can be translated to e and h of the local domain directly. Because of $e \geq x$ and $h \geq m$, role y

can be translated to x and m in the local domain indirectly whatever the two associations labeled as 1 and 2 are transitive or not. Similarly, any one user of the foreign cannot be assigned to y in Figure 2. In Figure 2, y and k can be translated to x and m of the foreign domain respectively. According to $f \geq y$ and $f \geq k$, f can be translated to x and m of the local domain indirectly and f is an unusable role if the two associations are transitive. In Figure 2, according to reference [6] whether association 1 is transitive or not, if association 2 is transitive, y can be translated to x and m and y is an unusable role. These discussions are all possible cases. Because we do not have to consider whether the association is transitive or not,so f in Figure 2, y and f in Figure 2 must be unusable roles whatever whether the two associations are transitive or not.

Zhai *et al.*, [7] continue to discuss the SMER constraints violation problem and point out that the conclusions in [6] are incomplete. They claim that the underlying reason for occurring SMER constraints violation in IRBAC2000 model is one improper user-role assignment in the foreign domain. Though there are not any unusable roles according to dynamic role translation, SMER constraints violation also occurs if one improper user-role assignment in the foreign domain is presented. For example, in Figure 2, any SMER constraints violation will not occur if there are not any users assigned to f in the foreign domain. In Figure 3, x and m are a pair of SMER constraints, and any roles cannot be translated to x and m simultaneously. But there will be one user u assigned to f and k, the user u will be translated to x and m indirectly and SMER constraints violation will occur. So the underlying reason for occurring SMER constraints violation is just that one improper user-role assignment in the foreign domain.

The formal definition of SMER constraints is $(\{r_1, r_2, ..., r_n\}, m)$ in [5], where each r_i is a role, and m and n are integers such that $1 < m \leq n$. Such a constraint is said to be canonical of cardinality m when $m = n$. Every SMER constraint $(\{r_1, r_2, ..., r_n\}, m)$ can be equivalent expressed as a group of new constraints such as $(\{r_{i_1}, r_{i_2}, ..., r_{i_m}\}, m)$ $1 \leq i_j \leq n$. For example, SMER $(\{r_1, r_2, r_3\}, 2)$ can be equivalent expressed as { $(\{r_1, r_2\}, 2)$, $(\{r_2, r_3\}, 2)$, $(\{r_1, r_3\}, 2)$ }. Only SMER type such as $(\{r_1, r_2, ..., r_m\}, m)$ is considered in [7], so the SMER constraints violation detection algorithm in [7] must be executed several times to be able to accomplish the general $(\{r_1, r_2, ..., r_n\}, m)$ violation detection. But our approach in this paper needs only one execution and can also detect several SMER constraints simultaneously, *e.g.*, $(\{r_1, r_2, ..., r_{n_1}\}, m_1)$ and $(\{r_1, r_2, ..., r_{n_2}\}, m_2)$.

3. Colored Petri Nets and Detection Model

3.1. Some Definitions for CPN

The terminologies of Petri nets and Colored Petri nets are illustrated in this section.

Definition 1. (*Petri nets, PN*) A Petri net (N, M_0) is a net

- $N = (P, T, F, W)$ with an initial marking M_0 where,
- P is a finite set of places of cardinality $|P|$;

 Copyright ⓒ 2014 SERSC

- T is a finite set of transitions such that $P \cap T = \varnothing$ and $P \cup T \neq \varnothing$;
- $F \subseteq (P \times T) \cup (T \times P)$ is the flow relation;
- W is a weight function such that $W(x,y) \in N^+$ If $(x,y) \in F$ and $W(x,y) = 0$ if $(x,y) \notin F$. For any $X, Y \subseteq P \cup T$, we denote

$$W(X,Y) = \{W(x,y) | x \in X, y \in Y, (x,y) \in F\};$$

- M_0, a $|P|$ -dimensional vector, is a function $M_0 : P \to N$ such that $M_0(p)$ represents the number of tokens in place $p \in P$.

Definition 2. (*Firing rule*) A transition $t \in T$ is enabled at a marking M if and only if $\forall p \in P$: $M(p) \geq W(p,t)$. Firing (or executing) transition t results in changing marking M to a reachable marking M', where $\forall p \in P$: $M'(p) = M(p) - W(p,t) + W(t,p)$.

Definition 3. (*pre-set*, *post-set*, *input set* and *output set*) For $x \in P \cup T$, ${}^\bullet x = \{y | (y,x) \in F\}$ and $x^\bullet = \{y | (x,y) \in F\}$ are called the *pre-set* (*input set*) and *post-set* (*output set*) of x, respectively. For a set $X \subseteq P \cup T$, and $X^\bullet = \cup_{x \in X} x^\bullet$.

Definition 4. (*firing sequence* and *reachability*) Let M, M' be markings, t be a transition, and σ be a transition sequence in a Petri net (N, M_0). $M[N, \sigma > M'$ means that M' is reachable from M by firing σ. $M[N, * > M'$ means that M' is reachable from M by firing an unspecified sequence. $R(N,M)$ denotes the reachability set of N starting from M, i.e., the smallest set of markings such that: (a) $M \in R(N,M)$;(b) If $M' \in R(N,M)$ and $M'[N, t > M''$ for some $t \in T$, then $M'' \in R(N,M)$.

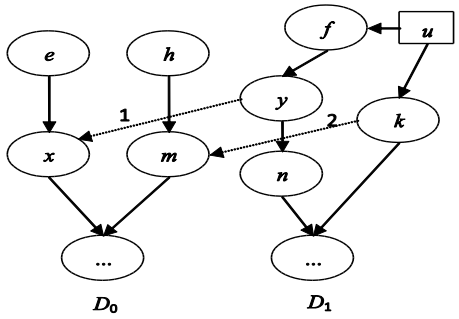

Figure 3. SMER Constraints Violations caused by User/Role Assignment

The idea of CPN is to introduce the notion of token types. Tokens are differentiated by colors, which may be arbitrary data values. Each place has an associated type determining the kind of data that the place may contain. The precise definition can be found in [9].

Definition 5. (*Colored Petri nets*, *CPN*) A Colored Petri net is a tuple *CPN*= $(\Sigma, P, T, A, V, C, G, E, I)$, where

- Σ is a finite set of non-empty types, also called color sets. The set of types determines the data values and the operations and functions that can be used in the arc expressions, guards and initialization.
- P is a finite set of places.

Copyright ⓒ 2014 SERSC

- T is a finite set of transitions.
- A is a finite set of arcs such that: $P \cap T = P \cap A \quad = T \cap A = \varnothing$.
- V is a node function $V: A \to (P \times T) \cup (T \times P)$.
- C is a color mapping $C: P \to \Sigma$. The color function C maps each place p to a type $C(p)$, which means that each token on p must have a data value that belongs to $C(p)$.
- G is a guard function. It is defined from T into expressions such that $\forall t \in T$: $Type(G(t))$ =Boolean and $Type(Var(G(t))) \subseteq \Sigma$. For any transition $t \in T$, the guard of t is a boolean expression, where all variables have types that belong to Σ.
- E is an arc expression function. It is defined from A into expressions such that: $\forall a \in A$: $Type(E(a)) \quad = C(p)_{MS}$ and $Type(Var(E(a))) \subseteq \Sigma$, where p is the place of $V(a)$. For any arc $a \in A$, the type of $E(a)$ is the multi-set $C(p)_{MS}$, which means that $E(a)$ must evaluate to multi-sets over the type of the adjacent place p. Moreover all variables in an arc expression $E(a)$ have a type in Σ.
- I is an initialization function. It is defined from P into closed expressions such that: $\forall p \in P: Type(I(p)) = C(p)_{MS}$. I maps each place $p \in P$ into a closed expression that must be of type of $C(p)_{MS}$.

The firing rule for a CPN is similar to that for a classical Petri net, except that the markings and weights are represented as multiple dimensional vectors. CPN is just a folding of several ordinary Petri nets with the same net structure. Hence, CPN is equivalent to an ordinary Petri net and the reachablity analysis techniques for ordinary Petri nets are also applicable for the CPN model. Usually, colors in the CPN are used to distinguish different types of data. In this paper, we don't use the G part, a guard function, of the CPN definition. More information can be found in [8, 9].

3.2. CPN Model of SMER Constraints Violation Detection

Suppose that there are two domains, D_0 and D_1. D_0 is the local domain and D_1 is the foreign domain. R_0 denotes the role set of the local domain and R_1 denotes the role set of the foreign domain. The role hierarchy for the role set R_0 can be denoted by H_0, and the role hierarchy for the role set R_1 can be denoted by H_1. U denotes the user set of D_1, and UA denotes the user-role assignment in the domain D_1.

Definition 6. $\forall r_i \in R_k, \forall r_j \in R_k$ such that $r_j \geq r_i$, we can say that in the domain D_k, r_j is an ascendant (ancestor) of r_i, and r_i is a descendant (offspring) of r_j, $(r_j, r_i) \in H_k$.

Definition 7. A dynamic role association (DRT) (y, x) from the domain D_1 to the domain D_0 can be denoted by $y \to x$, where $y \in R_1$, y is a role of the foreign domain D_1, and $x \in R_0$, is a role of the local domain D_0.

As we noted above, we won't consider whether the association is transitive or not, so the association type will not be taken into account while detecting SMER constraints violation.

Definition 8. $\exists u \in U, \exists r_i \in R_1, \exists (u, r_i) \in UA$, (u, r_i) represents one user-role assignment in the domain D_1.

Definition 9. *SMERS* represents a set of all *SMER* constraint in an IRBAC 2000 model.

 Copyright ⓒ 2014 SERSC

Definition 10. *DRTS* represents a set of all *DRT* in an IRBAC 2000 model.

The construction algorithm from IRBAC 2000 model with SMER constraints to CPN model is shown in Table 1.

Table 1. A Construction Algorithm of CPN Model

Input: one IRBAC 2000 model (D_0, D_1, R_0, R_1, H_0, H_1, U, *UA*, *SMER*S, *DRTS*)
Output: a CPN model for IRBAC 2000 model
(1) For each role r in the domain D_0 introduce a place r
(2) For each role r in the domain D_1 introduce a place r
(3) For each user $u \in U$ in the domain D_1 introduce a place u
(4) For each r in the domain D_0 introduce a transition t, such that
$^\bullet t = r, t^\bullet = \{r' \mid \exists r' \geq r, (r', r) \in H_0\} \cup \{r' \mid \exists r' \in R_1, r' \rightarrow r\}$
(5) For each r in the domain D_1 introduce a transition t, such that
$^\bullet t = r, t^\bullet = \{r' \mid \exists r' \geq r, (r', r) \in H_1\} \cup \{u \mid (u, r) \in UA\}$
(6) For each SMER constraint $S_i \in SMER$S do
For each $r_j \in S_i(\{r_1, r_2, ..., r_n\}, m)$ do
Add a new token s_{ij} into the place r_j

Though our approach can be used to model and analyze several SMER constraints simultaneously, for simplicity, we will discuss only one SMER constraint.

Definition 11. A colored Petri net *CPN* for an IRBAC 2000 model, $\exists u \in U$, $\exists M \in R(M_0)$, $M(u)$ represents a set of token in the place u while M is the current reachable marking.

Suppose that there is a SMER constraint $S_1 = (\{r_1, r_2, r_3\}, 2)$, $M(u)$ may make $\{r_1, r_1, r_2\}$.

Definition 12. A function *remdupl* (L) removes duplicates from the set L, where *L is* a set of token L, e.g., $L = \{r_1, r_1, r_2\}$, *remdupl*(L) $= \{r_1, r_2\}$.

Definition 13. A function *length* (L) returns the number of elements in the set L.

Definition 14. We define $L = \{r_1, r_1, r_2\} = \{2 \cdot r_1, r_2\}$.

Theorem 1. A DRTS can violate SMER constraint $(\{r_1, r_2, ..., r_n\}, m)$ in an IRBAC 2000 model, if and only if for *CPN* model, $\exists u \in U$, $\exists M \in R(M_0)$ such that *length* (*remdupl* $(M(u)) \cap \{r_1, r_2, ..., r_n\}) \geq m$.

Proof 1 For the "if" part, we know that if in the *CPN model*, $\exists u \in U$, $\exists M \in R(M_0)$ such that *length* (*remdupl* ($M(u)) \cap \{r_1, r_2, ..., r_n\}) \geq m$, then $\exists u \in U$, $\exists M \in R(M_0)$, $\exists(\delta_1, \delta_2, ..., \delta_k)$ and $\exists(\lambda_1, \lambda_2, ..., \lambda_k)$ where $1 \leq \delta_i \leq n$, $m \leq k \leq n$, $1 \leq \lambda_i$, $1 \leq i \leq k$, such that *remdupl* ($M(u)) \cap \{r_1, r_2, ..., r_n\} = \{r_{\delta_1}, r_{\delta_2}, ..., r_{\delta_k}\}$. So $\{r_{\delta_1}, r_{\delta_2}, ..., r_{\delta_k}\} \subseteq$ *remdupl* ($M(u)$), and then $\cup\{\lambda_i \cdot r_{\delta_i}\} \subseteq M(u)$. According to the construction algorithm of CPN model in Table 1, we can know that one user u can be translated to every role in the role set kindly in the IRBAC2000 model. And ($\{r_{\delta_1}, r_{\delta_2}, ..., r_{\delta_k}\} \subseteq \{r_1, r_2, ..., r_n\}) \wedge (m \leq k \leq n)$, so a DRTS can violate SMER constraint $(\{r_1, r_2, ..., r_n\}, m)$ in an IRBAC 2000 model.

For the "only if" part. According to the construction algorithm of CPN model in Table 1,

obviously, we know that if a DRTS can violate SMER constraint $(\{r_1, r_2, ..., r_n\}, m)$ in an IRBAC 2000 model, then $\exists u \in U$, $\exists M \in R(M_0)$ and $\exists(\delta_1, \delta_2, ..., \delta_k)$ and $\exists(\lambda_1, \lambda_2, ..., \lambda_k)$ where $1 \le \delta_i \le n$, $1 \le \lambda_i$, $m \le k \le n$, $1 \le i \le k$ such that $\cup\{\lambda_i \cdot r_{\delta_i}\} \subseteq M(u)$, so *length* (*remdupl* $(M(u)) \cap \{r_1, r_2, ..., r_n\}) \ge m$.

3.3. Detection Approach

A CPN model can be built from an IRBAC2000 model according to the construction algorithm of CPN model in Table 1. Then the detection problem of SMER constraints violation is translated into analyzing the reachable marking or reachability graph of a CPN. It can be analyzed by some powerful and mature Petri net analysis tool, for example CPN tools. According to Theorem 1, we can decide whether there exists SMER constraints violation. If there is a reachable marking M for one user u that satisfied *length* (*remdupl* $(M(u)) \cap \{r_1, r_2, ..., r_n\}) \ge m$, then the IRBAC2000 model will violation SMER constraint $(\{r_1, r_2, ..., r_n\}, m)$. We use the detection approach using the present CPN tools to analyze the SMER constraint violation problem. And the approach is a very good way to visualize exactly the role hierarchy and the dynamic role translation between the two domains.

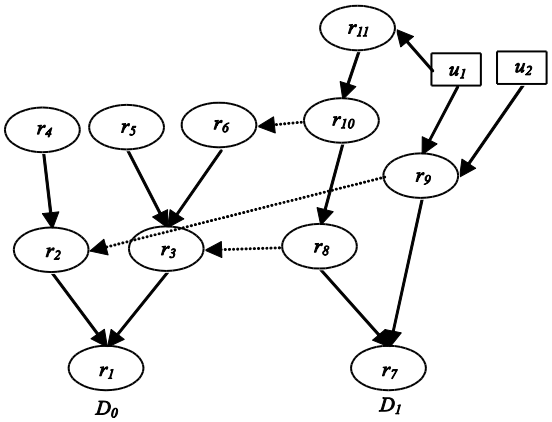

Figure 4. A Case Study of IRBAC 2000 Model

We show a case study to be used to verify our approach. First, an IRBAC 2000 model is shown in Figure 4.

In Figure 4, there are six roles, $\{r_1, r_2, r_3, r_4, r_5, r_6\}$, in the local domain D_0, and there are five roles, $\{r_7, r_8, r_9, r_{10}, r_{11}\}$, in the foreign domain D_1. Role hierarchy of the IRBAC 2000 model is very clear. There are two users, u_1 and u_2. User u_1 is assigned to role r_9 and r_{11} and user u_2 is assigned to role r_9. There are also three role associations, $r_8 \to r_3$, $r_{10} \to r_6$, $r_9 \to r_2$. Suppose that there exists a SMER constraint $(\{r_2, r_3\}, 2)$. According to the construction algorithm of CPN model in Table 1, the CPN model is shown in Figure 5.

We define color sets for the corresponding CPN model for Figure 4 as follows:

colset s= with r2|r3;

The mutual exclusive roles in Figure 4 are r_2 and r_3, so we only define a color set containing r_2 and r_3.

 Copyright ⓒ 2014 SERSC

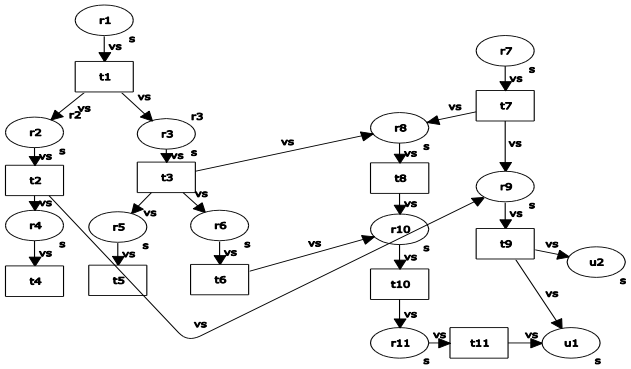

Figure 5. The Corresponding Model for Figure 4

For each place in Figure 5, $C(p)$ is a color set that is "s". We also define a variant, "vs", of the colors set "s" as follows:

var vs : s;

So each arc expression function in Figure5 is "vs".

The three arcs, t3 $\rightarrow$ r8, t6ment r10, t2 $\rightarrow$ r10, represent the three corresponding role associations, $r_8 \rightarrow r_3$, $r_{10} \rightarrow r_6$, $r_9 \rightarrow r_2$ respectively. According to the algorithm in Table 1, the initialization function of the CPN in Figure 5, i.e., the initial colored tokens in each place are that there is a colored token "r_2" in place r_2, there is a colored token "r_3" in place r_3, and there is not any token in others.

We can simulate the CPN and the reachability graph can be calculated by CPN tools. But the reachability graph for the case is complex. In fact, we can know that there must not exists post-set of place u_1 and u_2, so the Best Upper Multi-set Bounds of place u_1 and u_2 can be used to verify whether there exists SMER constraints violation. And then we use CPN tools to simulate the CPN model with an initial marking $M_0(r_2) = r_2$ and $M_0(r_3) = r_3$. When we have generated the state space for a CPN, we can get a standard report providing information about the Best Upper Multi-set Bounds of place. The results are listed as follows in Table 2.

We can see that $\exists u_1$ such that *length* (*remdupl* ($M(u_1)) \cap \{r_2, r_3\}$) =*length* (*remdupl*($\{r_2, 2 \cdot r_3\}$) $\cap \{r_2, r_3\}$) =*length* ($\{r_2, r_3\}$) =2.

Table 2. A Part of Output Standard Report by CPN Tools

Best Upper Multi-set Bounds
NewPage'r10 1 2'r3
NewPage'r1 1 empty
NewPage'r11 1 2'r3
NewPage'r2 1 1'r2
NewPage'r3 1 1'r3
NewPage'r4 1 1'r2
NewPage'r5 1 1'r3
NewPage'r6 1 1'r3
NewPage'r7 1 empty
NewPage'r8 1 1'r3
NewPage'r9 1 1'r2
NewPage'u1 1 1'r2++2'r3
NewPage'u2 1 1'r2

Copyright ⓒ 2014 SERSC

According to Theorem 1, we can determine that u_1 can acquire all permissions of r_2 and r_3 and DRTS violates the SMER constraint $(\{r_2, r_3\}, 2)$.

Let us continue to discuss about the Best Upper Multi-set Bounds of place u_1. What means the value 1‘r2++2‘r3?

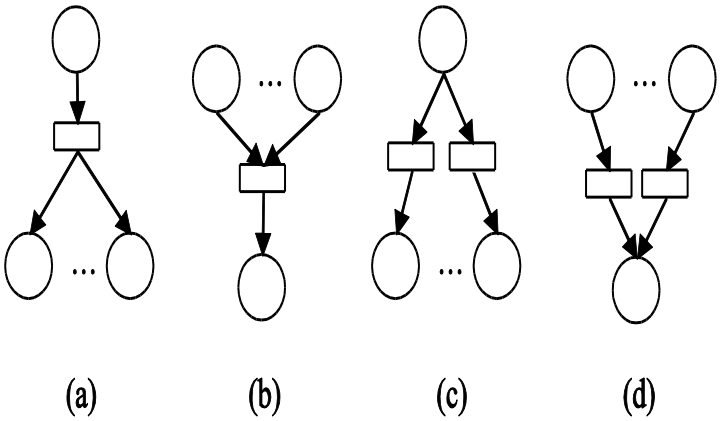

Figure 6. 4 Kinds of Basic Petri Net Structure

There are four kinds of basic Petri net structure in Figure 6. According to the construction algorithm of CPN model in Table 1, we know that there are only two cases in Figure 6(a) and Figure 6(d) to appear in the built CPN model. 1‘r2 means that there exists a transition sequence in CPN model that can reach the marking M such that $M(u_1) =$ 1‘r2++2‘r3. Similarly, 2‘r3 means that there exist two transition sequences in CPN model that can reach the marking M such that $M(u_1) =$ 1‘r2++2‘r3. These three key transition sequences are t2 t9, t3 t6 t10 t11 and t3 t8 t10 t11 respectively.

4. Prerequisite

In the environment of interoperation between two domains, role association and user-role assignment are usual managerial practices, where SMER constraints violation can occur. So it is important and necessary that some prerequisites can be used to decide whether these management operations can violation SMER constraints. We can present two formal denotations to express the prerequisites.

The first kind of denotation is defined as follows.

Theorem 2. SMER constraint $(\{r_1, r_2, ..., r_n\}, m)$ is not violated in an IRBAC2000 model, which still keeps a safe state if and only if $\forall u \in U$, $\neg\exists M \in R(M_0)$ such that *length* (*remdupl* $(M(u)) \cap (r_1, r_2, ..., r_n)) \geq m$ for the new CPN model after adding dynamic role translation (role association) $(y, x)(y \in R_1, x \in R_0)$ or a user-role assignment (u, y).

Obviously, Theorem 2 can be proofed easily according to Theorem 1 and so we omit proof. But there exists a considerable flaw while using Theorem 2. Every time when administrators add a new dynamic role translation (role association) or a user-role assignment, the CPN model must be re-simulated and may take a long time.

After the CPN model simulate, some statistics information, e.g., size of state space and state space graph, are stored. We can use these statistics information to provide prerequisites.

 Copyright ⓒ 2014 SERSC

So the CPN model need not be re-simulated. We will use the Best Upper Multi-set Bounds of one place.

Definition 15. The Best Upper Multi-set Bounds of one place p is denoted by $BUMB(p)$.

Definition 16. a CPN, $post-set(x:P\cup T)=x^{\bullet}$, then

$$super-post-set(x:P\cup T)=\{y\,|\,(y\in P\cup T)\wedge(x\cup\bigcup_{y\in post-set(x)}super-post-set(y))\}.$$

Theorem 3. SMER constraint $(\{r_1,r_2,...,r_n\},m)$ is not violated in an IRBAC2000 model, which still keeps a safe state after adding dynamic role translation (role association) $(y,x)(y\in R_1,x\in R_0)$ if and only if for the former CPN model, $\forall u\in U$ such that either

(1) $length(remdupl(BUMB(x)\cup BUMB(u))\cap\{r_1,r_2,...,r_n\})<m$.

(2) $u\notin super-post-set(y)$.

Proof 2 For the "if" part.

(1) If $\forall u\in U$ such that $length(remdupl(BUMB(x)\cup BUMB(u))\cap\{r_1,r_2,...,r_n\})<m$, then after adding dynamic role translation (role association) $(y,x)(y\in R_1,x\in R_0)$, we can simulate the new CPN model. According to the construction algorithm of CPN model in Table 1 such that $\forall u\in U$, $\neg\exists M\in R(M_0)$ such that $length\ (remdupl\ (M(u))\cap\{r_1,r_2,...,r_n\})\geq m.$ So the IRBAC2000 model still keeps a safe state according to theorem 2.

(2) if $\forall u\in U$ such that $u\notin super-post-set(y)$, we can simulate the new CPN model. Obviously, according to the construction algorithm of CPN model in Table 1 such that $\forall u\in U$, $\neg\exists M\in R(M_0)$ such that $length\ (remdupl\ (M(u))\cap\{r_1,r_2,...,r_n\})\geq m.$ So the IRBAC2000 model still keeps a safe state.

For the "only if" part. We proof by contradiction.

Suppose if $\exists u\in U$ such that

$(length(remdupl(BUMB(x)\cup BUMB(u))\cap\{r_1,r_2,...,r_n\})\geq m)\wedge u\in super-post-set(y)$, then we can simulate the new CPN model. According to the construction algorithm of CPN model in Table 1 such that $\exists u\in U$, such that $length\ (remdupl\ (M(u))\cap\{r_1,r_2,...,r_n\})\geq m.$ So the IRBAC2000 model cannot still keep a safe state, which is a contradiction.

Let us illustrate Theorem 3 by a case study. A modified CPN model is shown in Figure 7 and there are not any SMER constraint violations.

Now $BUMB(r4)=\{r2\}$, $BUMB(u1)=\{r2\}$ and $BUMB(u2)=\{r2\}$. Some role associations can be added, e.g., $r_8\rightarrow r_4$, which means that an new arc, t4 $\rightarrow$ r8, will add into the CPN model. According to Theorem 3, because $length(remdupl(BUMB(r4)\cup BUMB(u1))\cap\{r_1,r_2\})=1$ and $length(remdupl(BUMB(r4)\cup BUMB(u2))\cap\{r_1,r_2\})=1$, the first condition can still be satisfied. So there are still not any SMER constraints violation for user u_1 and u_2 and adding a role association $r_8\rightarrow r_4$ is still safe.

Copyright ⓒ 2014 SERSC

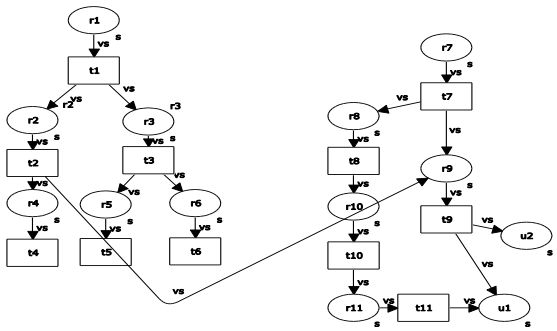

Figure 7. The CPN Model of a Safe IRBAC 2000 Model

For the CPN model in Figure 7, we can also know that $BUMB(r3)=\{r3\}$, $BUMB(u1)=\{r2\}$ and $BUMB(u2)=\{r2\}$ now. If a role association $r_8 \to r_3$. is added, a new arc t3 → r8 will be added into it. Now $length(remdupl(BUMB(r3)\cup BUMB(u2))\cap\{r_1,r_2\})=2$, so the first conditions in theorem 3 will not be satisfied for user u_2. But $u2 \notin super-post-set(r8)$ and the second condition is still satisfied for user u_2, so there are still not any SMER constraints violations for user u_2. However, for the user u_1, both of the two conditions are not satisfied, so adding a role association $r_8 \to r_3$ is not safe.

Theorem 4. SMER constraint $(\{r_1,r_2,...,r_n,m\})$ is not violated in an IRBAC2000 model, which still keeps a safe state after adding a user-role assignment (u,y) if and only if for the former CPN model such that

$\forall u \in U$ such that $length(remdupl(BUMB(y)\cup BUMB(u))\cap\{r_1,r_2,...,r_n\})<m$.

Because the proof for theorem 4 is similar with theorem 3, we omit proof.

We use another case study to illustrate theorem 4 in Figure 8.

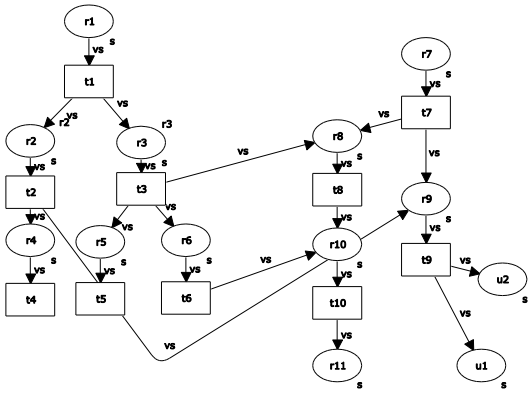

Figure 8. Another CPN Model of a Safe IRBAC 2000 Model for Theorem 4

The new CPN in Figure 8 can be simulated and we know $BUMB$(r11)= $\{2\cdot r_3\}$ and $BUMB(u1)=\{r_2\}$. Suppose adding a user-role assignment (u_1,r_{11}), after a new transition t11 and a new arc t11 → u1 into Figure 8 is added, the new CPN model is the same in Figure 5. So *length* (*remdupl* ($BUMB$($r11)\cup BUMB(u1)) \cap\{r_2,r_3\}$) =2. According to theorem 4, there exists SMER constraint violation for user u_1. Furthermore, according to theorem 1 we can

 Copyright ⓒ 2014 SERSC

also know if the CPN model in Figure 8 is added an user-role assignment (u_1, r_{11}), the new CPN model is violate SMER constraint for user u_1.

It should be noted that mentioned theorems are all discussed based on one SMER constraint. Because every token in the CPN model is different color, the case that there are several SMER constraints does not affect the result. After the CPN model is simulated, these SMER constraints can be verified one by one.

5. Conclusions

This paper continue to discuss and analyze the SMER constraints violation problem due to dynamic role translation in the IRBAC2000 model based on [3,6,7]. And a new approach based on CPN is proposed to be used to model and analyze the SMER constraints violation problem. So SMER constraints violation problem is translated into analyzing the reachable marking or reachability graphs of a CPN. It can be analyzed by some powerful and mature Petri net analysis tool, which is very easy and visualized. A construction algorithm of CPN model from an IRBAC2000 model is presented, and then we proof the sufficient and necessary conditions to satisfy the CPN model not to violation SEMR constraints. Then a case study is used to illustrate the efficiency of the proposed model and detection method. To guarantee the security and decide whether these usual managerial practices, e.g., role association and user-role assignment, can violation SMER constraints in the IRBAC2000 mode we present two formal denotations to express prerequisites and verify their effectiveness by proof and case study. Future work includes the further performance analysis of the detection algorithm in other situations, and the research of other better detection algorithm.

References

[1] R. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, “Role-based access control models”, IEEE Computer, vol. 29, no. 2, **(1996)**, pp. 38-47.
[2] D. F. Ferraiolo, R. S. Sandhu, S. I. Gavrila, D. R. Kuhn and R. Chandramouli, “Proposed nist standard for role-based access control”, ACM Trans. Inf. Syst. Secur., vol. 4, no. 3, **(2001)**, pp. 224-274.
[3] A. Kapadia, J. AlMuhtadi, R. H. Campbell and D. Mickunas, “I-RBAC 2000: Secure Interoperability Using Dynamic Role Translation”, Proceedings of The 1st International Conference on Internet Computing (IC ’00), **(2000)**, pp. 231-238.
[4] L. Gong and X. Qian, “Computational Issues in Secure Interoperation”, IEEE Trans on Software Engineering, vol. 22, no. 1, **(1996)**, pp. 43-052.
[5] N. Li, Z. Bizri and M. V. Tripunitara, “On mutually-exclusive roles and separation of duty”, Proceedings of the ACM Conference on Computer and Communications Security 2004, (**2004**), pp. 42-51.
[6] J. Liao, F. Hong, X. Zhu and H. Xiao, “Separation of duty in dynamic role translations between administrative domains”, Journal of Computer Research and Development, vol. 43, no. 6, **(2006)**, pp. 1065-1070.
[7] Z. Zhai, Z. Xu and D. Feng, “Violation of Static Mutual Exclusive Role Constraints in Dynamic Role Transition”, Journal of Computer Research and Development, vol. 45, no. 04, **(2008)**, pp. 677-683.
[8] T. Murata and P. Nets, “Properties, Analysis and Applications, an invited survey paper”, Proceedings of the IEEE, vol. 77, no. 4, **(1989)**, pp. 541-580.
[9] K. Jensen, “Coloured Petri Nets”, Springer, Heidelberg, vol. 1, **(1992)**.

Copyright ⓒ 2014 SERSC

Authors

Meng Liu received his Master's degree in Computer Sciences from the School of Computer Science and Technology, Shandong University, China, in 2004. Currently, he is working toward the Ph.D. degree in Computer Science at the Computer Application Research Center, Harbin Institute of Technology Shenzhen Graduate School, China and is a lecturer in the School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai, China. His main research interests include network and information security.

Xuan Wang received his M.S. and Ph.D. degrees in Computer Sciences from Harbin Institute of Technology, Harbin, China, in 1994 and 1997 respectively. He is a professor and Ph.D. supervisor in the Computer Application Research Center, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China. His main research interests include artificial intelligence, computer vision, computer network security and computational linguistics. He is a member of the IEEE.

Copyright ⓒ 2014 SERSC