A Role-driven Security and Access Control Model for Secured Business Process Management Systems

Jae-Kang Won[1] and Kwang-Hoon Kim[2]
Collaboration Technology Research Lab.
Department of Computer Science
KYONGGI UNIVERSITY
San 94-6 Yiuidong Youngtongku Suwonsi Kyonggido, 442-760, South Korea
http://ctrl.kyonggi.ac.kr
Phone:+82-31-249-9679
Fax:+82-31-249-9673
e-Mail:{jkwon, kwang}@kyonggi.ac.kr

Abstract

This paper formally defines a role-driven security and access control model of a business process in order eventually to provide a theoretical basis for realizing the secured business process management systems. That is, we propose a graphical representation and formal description of the mechanism that generates a set of role-driven security and access control models from a business process modeled by the information control net(ICN) modeling methodology that is a typical business process modeling approach for defining and specifying business processes. Based upon the mechanism, we are able to design and accomplish a secured business process management system that provides an unified resource access control mechanism of the business process management engine domain's and the application domain's. Finally, we strongly believe that the secured access control policies from the role-driven security and access control model can be easily transformed into the RBAC(Role-based Access Control) model that is a standardized security technology for computer and communications systems of commercial and civilian government organizations.

Keywords. *Access control, security policy, discretionary access control, integrity, mandatory access control, role-based access control, secured business process management*

1. Introduction

There exist a lot of technologies which appear and disappear in our society. Among them, we can easily recognize that convergence of those technologies surviving recently has appeared to bring the world closer together, physically and conceptually. Groupware is a meaningful technology with great promise of bringing people closer together conceptually. Whether people are in the same place or scattered around the world, groupware is able to support them to coordinate, collaborate, and cooperate. In this paper, particularly we are concerned about the coordinative groupware technology – workflow and business process management technology – with respect to the topic of security control mechanism.

In the business process management literature, the current set of security policies, access control guidelines, and mechanisms has little grown out of research and development efforts. But, according to the growths of the business process management market, the security issue is taking the immediate attention in the literature. Today the best known computer-related security standard is the Role-Based Access Control(RBAC) [1,2,3] that has been accepted as a secured access control model being appropriate and central to the secure processing needs within industry and civilian government. However, without any modifications and extensions, it is unreasonable for the role-based access control model to be directly applied in order to realize a secured business process management system. Therefore, for realizing the secured business process management, in this paper we propose a new business process management security control model, which is called a role-driven BPM security control model, by analyzing and reflecting the properties of business processes, and the security control model will be possibly extended to the role-based access control standard in the future.

In the next section, we introduce the motivation of the paper, and summarize its related works that have been done on the topic of security issue in the business process management literature. We next describe the basic structure of the role-driven BPM security control model and its mechanism and algorithm that automatically generates a set of role-driven security control models from a business process modeled by the information control net modeling methodology [4,5,6,7]. Finally, we explain the mechanism's applicability through an example of business process model – the hiring business process model [8,9].

2. Motivation and Related Work

The conceptual part, i.e. the logical foundation of workflow management system, is called workflow model. It

contains all objects and relationships available to describe a particular workflow. The expressiveness of a workflow management system is decided by the content of this model. Thus, the workflow model is mainly influenced by requirements stemming from the application areas. Not only current application requirements but also future application requirements determine the workflow model. These requirements differ dramatically on several dimensions such as structure, predictability, number of users, etc. One important measure of workflow models is the ability to fully describe the wide range of application types. Another critical measure is the amount of programming needed to implement a workflow. Almost any workflow can be coded with enough programming effort, but a "good" workflow model will minimize custom development. There have been several workflow models such as the information control net model of FlowPath workflow system, the conversational model of Action workflow system, and the object oriented model of ViewStar workflow system. However, anything of these workflow models is not a "good" workflow model to be adapted for the recent working behaviors and environments – the any-cast and the multi-cast – without any modifications on it. workflow models have to provide abilities to define the interface for the user and developer. Basically, they include fields which are maintained in a database: types of objects such as forms, documents, activities, users, etc.; access permissions; route identification (through graphic drawing or field specification); route decision points; and so on. The primary question for the user is, "Does the model allow me to specify all that is necessary for the work to flow?" A robust mode will permit all the exigencies of the work process to be efficiently captured. The secondary question is, "How much work do I have to invest in modeling the workflow?" There are tradeoffs between the programming required and the amount of workflow already "programmed." Based on the comparison results for the traditional workflow models done by, the ICN model is closer to an ideal model for workflow. But, we would argue that the ICN model should be insufficient to model all that is necessary for a completely effective workflow implementation accommodating the new trends of working behaviors such as the any-cast and the multi-cast workflow. As a conclusion, in terms of the user's perspective we use the ICN model to define a workflow procedure. And, in terms of the developer's perspective we also construct a role-based workflow model from the ICN model for the sake of the design and implementation of workflow architectures embedding the new working behaviors.

Recently, there have been considerable attentions on researching and addressing the security reeds of commercial and civilian government organizations. It is apparent that significant and broad sweeping security requirements exist not only civilian government and corporations but also rely heavily on information processing systems to meet their individual operational, financial, and information technology requirements imposed of databases, data networks, and key software systems. Especially, in spite of that the workflow/business process management systems have been swiftly catching the public attentions and the market growth, making and realizing a secured business process management accomplishment issue is still on the stage of unawareness. In Fig. 1, we illustrate a reasonable solution for the security problem of the current business process management systems. As shown in the figure, a business process management system definitely needs a certain type of interconnections and interactions with the application domain. However, the business process management arena and the application arena separately have their own security and access control mechanisms and policies. Without further explanation, we are able to imagine what the problems are on the current business process management systems. Conclusively speaking, we need an unified security and access control mechanism to resolve the problems, and we would be positive on that the role-driven security control model proposed in this paper be a reasonable solution to provide the unified security and access control services to both BPM users and application users in an uniform fashion.

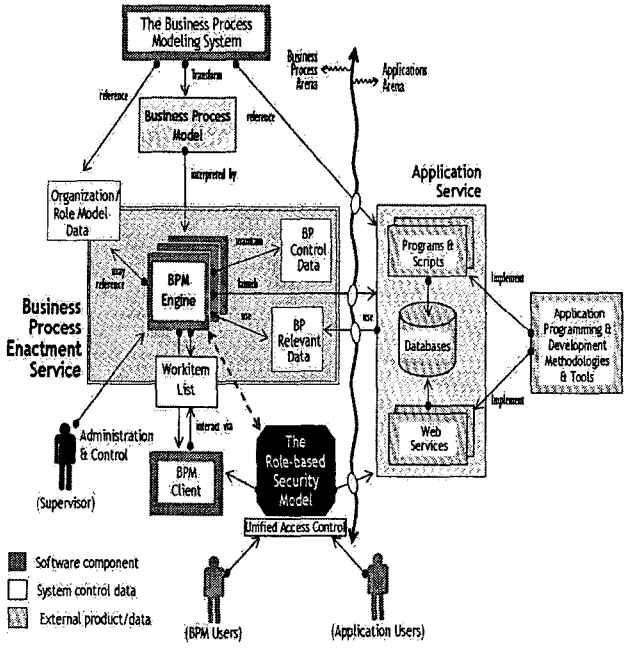


Figure 1. The Secured BPM Realization Using the Role-driven Security Control Model

So far, in terms of the security criteria, standards, and guidelines in commercial and civilian government organizations, the Trusted Computer System Evaluation Criteria(TCSEC) must be the best known standard [1]. The TCSEC specifies three types of access controls: Discretionary Access Controls(DAC), Mandatory Access Controls(MAC), and Role-Based Access Control(RBAC) [1,2,3]. DAC requirements have been perceived as being technically correct for commercial and civilian government security needs, as well as for single-level military systems.

MAC is used for multi-level secure military systems, but its use in other applications is rare. And, as stated in [1,2,3], the Role-Based Access Control(RBAC) is more appropriate and central to the secure processing needs within industry and civilian government than that of DAC. On the web site [10], we can find a lot of documents and materials about the RBAC model and its technologies. Especially, the site reads that there is a patent of workflow management employing RBAC [10], which seems to be surely related with this paper's approach. Even though we couldn't read the contents of the patent through the web site, it is manifest that the approach is completely difference from our approach because our approach is based upon not the RBAC model but our own model that is automatically generated from a business process model. In the next section, we define our own model – the role-driven BPM security control model.

3. Role-driven BPM Security Control Model

In this section, we formally define the role-driven business process management security control model(RDBPSCM) and propose an algorithm that automatically generates a set of the underlining role-driven security control models from a business process model.

3.1. Nomenclature

In this paper, we use the information control net methodology [6] to represent business processes and workflows. The information control net was originally developed in order to describe and analyze information flow within offices. It has been used within actual as well as hypothetical automated offices to yield a comprehensive description of activities, to test the underlying office information flow, and to suggest possible office restructuring permutations. The ICN model defines an office as a set of related procedures. Each procedure consists of a set of activities connected by temporal orderings called procedure constraints. In order for an activity to be accomplished, it may need information from repositories, such as files, forms, and some data structures.

As shown in Fig. 2, ICN captures these notations of business processes, activities, roles, actors, precedence, applications, and repositories. A business process is a predefined set of work steps, called activities, and a partial ordering of these activities. Activities can be related to each other by conjunctive logic (after activity A, do activities B and C) or by disjunctive logic (after activity A, do activity B or C) with predicates attached. An activity is either a compound activity containing another subprocess, or a basic unit of work called an elementary activity. An elementary activity can be executed in one of three modes: manual, automatic, or hybrid. Typically one or more actors are associated with each activity via roles. A role is a named designator for one or more actors (or groups) which conveniently acts as the basis for partitioning of work skills, access controls, execution controls, and authority / responsibility. An actor is a person, program, or entity that can fulfill roles to execute, to be responsible for, or to be associated in some way with activities and business processes. The following is the formal description of ICN:

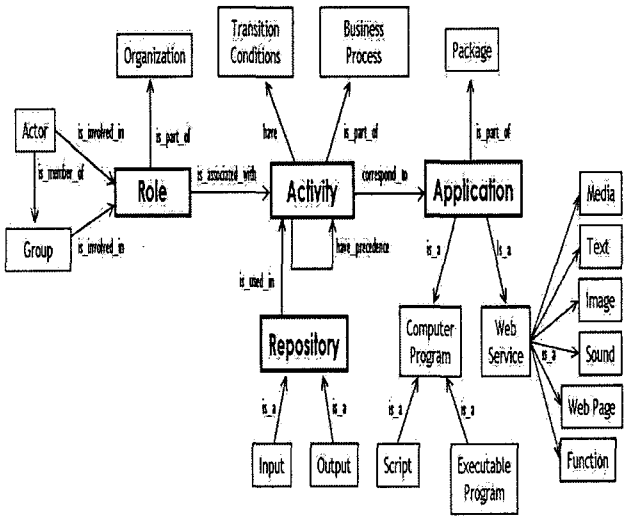


Figure 2. Entities and Relationships of Business Process Model

Formal Description of the Information Control Net

A basic ICN is 8 tuple $\Gamma = (\delta, \gamma, \chi, \varepsilon, \pi, \kappa, \mathbf{I}, \mathbf{O})$ over a set of **A** activities (including a set of group activities), a set **T** of transition conditions, a set **R** of repositories, a set **G** of invoked application programs, a set **P** of roles, and a set **C** of actors (including a set of actor groups), where

- **I** is a finite set of initial input repositories, assumed to be loaded with information by some external process before execution of the ICN;
- **O** is a finite set of final output repositories, perhaps containing information used by some external process after execution of the ICN;
- $\delta = \delta i \cup \delta o$
  where $\delta o : \mathbf{A} \rightarrow \wp(\alpha \in \mathbf{A})$ is a multi-valued mapping function of an activity to its sets of (immediate) successors, and $\delta i : \mathbf{A} \rightarrow \wp(\alpha \in \mathbf{A})$ is a multi-valued mapping function of an activity to its sets of (immediate) predecessors;
- $\gamma = \gamma i \cup \gamma o$
  where $\gamma o : \mathbf{R} \rightarrow \wp(\alpha \in \mathbf{A})$ is a multi-valued mapping function of an activity to its sets of output repositories, and $\gamma i : \mathbf{R} \rightarrow \wp(\alpha \in \mathbf{A})$ is a multi-valued mapping function of an activity to its of input repositories;
- $\chi = \chi a \cup \chi p$
  where $\chi p : \mathbf{G} \rightarrow \wp(\alpha \in \mathbf{A})$ is a single-valued mapping function of an activity to its invoked application program, and $\chi a : \mathbf{A} \rightarrow \wp(\tau \in \mathbf{G})$ is a multi-valued

mapping function of an invoked application program to its set of associated activities;

- $\varepsilon = \varepsilon a \cup \varepsilon p$
  where $\varepsilon p : \mathbf{P} \rightarrow \wp(\alpha \in \mathbf{A})$ is a single-valued mapping function of an activity to one of the roles, and $\varepsilon a : \mathbf{A} \rightarrow \wp(\eta \in \mathbf{P})$ is a multi-valued mapping function of a role to its sets of associated activities;
- $\pi = \pi p \cup \pi c$
  where $\pi c : \mathbf{C} \rightarrow \wp(\eta \in \mathbf{P})$ is a multi-valued mapping function of a role to its set of associated actors, and $\pi p : \mathbf{P} \rightarrow \wp(o \in \mathbf{C})$ is a multi-valued mapping function of an actor to its sets of associated roles;
- $\kappa = \kappa i \cup \kappa o$
  where κi : sets of control-transition conditions, **T**, on each arc, $(\delta i(\alpha),\alpha),\alpha \in \mathbf{A}$; and κo : sets of control-transition conditions, **T**, on each arc, $(\alpha,\delta o(\alpha)),\alpha \in \mathbf{A}$; where the set **T** = {default, or(conditions), and(conditions)}.

3.2. Graphical Representation and Formal Description

Based upon the ICN-based business process model in the previous section, we define and clarify the notion of RDBPSCM by giving a graphical representation as well as a simple formal description. The graphical representation of RDBPSCM is shown in Fig. 3. As seen in the figure, each role defined in the business process model is associated with a set of subjects that is assigned into the corresponding role through its assigned activities, and it also has a set of member actors reflecting the organizational structure. Finally, a set of objects with permission modes (read or / and write) is assigned into the role. Note that the notion of the subject is same to the application entity in the ICN-based business process model, and the object is same to the notion of the relevant data entity. Also, as you can intuitively guess, the number of role-driven security control models to be generated from a business process model is exactly same to the number of roles in it.

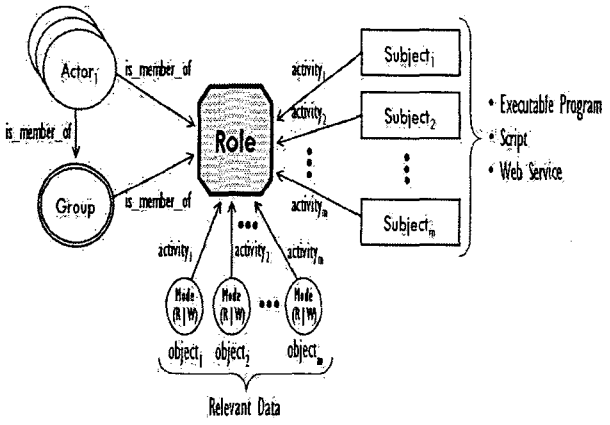


Figure 3. Graphical Representation of the Role-driven Security Control Model

Formal Description of RDBPSCM

In order to clarify the graphical representation of the role-driven business process management security control model, we give a formal notation of the model and also a set of formal descriptions of the operations that are able to be executed on the model as followings:

3.2.1. Formal Description of Role-driven BPM Security Control Model

A role-driven BPM security control model is formally defined as $\Re = (\xi,\vartheta,\gamma,\chi,\pi,\mathbf{S},\mathbf{E})$, over a set **P** of roles, a set **O** of Objects, a set **P** of actors, a set **G** of subjects and a set **A** of activities, where,

- **S** is a finite set of the initial activities, assumption to be loaded by some external procedures;
- **E** is a finite set of the final activities, perhaps containing activities of some external procedures. A role dependent net is constructed from a procedure driven model through the following simple algorithm;
- $\xi = \xi i \cup \xi o$
  where $\xi o : \mathbf{P} \rightarrow \wp(\alpha \in \mathbf{P})$ is a multi-valued mapping function of a role to its set of (immediate) successors, and $\delta i : \mathbf{P} \rightarrow \wp(\alpha \in \mathbf{P})$ is a multi-valued mapping function of a role to its sets of (immediate) predecessors;
- $\vartheta = \vartheta i \cup \vartheta o$
  where ϑo : a set of activities, $\mathbf{J} \subseteq \mathbf{A}$, on each arc, $(\xi i(\eta),\eta),\eta \in \mathbf{P}$; and ϑi: a set of activities, $\mathbf{J} \subseteq \mathbf{A}$, on each arc, $(\eta,\xi o(\eta)),\eta \in \mathbf{P}$;
- $\gamma = \gamma i \cup \gamma o$
  where $\gamma o : \mathbf{O} \rightarrow \wp(\alpha \in \mathbf{A})$ is a multi-valued mapping function of an activity to its set of output Objects with R/W, and $\gamma i : \mathbf{O} \rightarrow \wp(\alpha \in \mathbf{A})$ is a multi-valued mapping function of an activity to its set of input Objects with R/W;
- $\chi = \chi a \cup \chi p$
  where $\chi p : \mathbf{G} \rightarrow \wp(\alpha \in \mathbf{A})$ is a single-valued mapping function of an activity to Subjects, and $\chi a : \mathbf{A} \rightarrow \wp(\tau \in \mathbf{G})$ is a multi-valued mapping function of a Subject to its set of associated activities;
- $\pi = \pi p \cup \pi c$
  where $\pi c : \mathbf{C} \rightarrow \wp(\eta \in \mathbf{P})$ is a multi-valued mapping function of a role to its sets of associated actors, and $\pi p : \mathbf{P} \rightarrow \wp(o \in \mathbf{C})$ is a multi-valued mapping function of an actor to its sets of associated roles;

3.2.2. Formal Description of Operations

- For each activity, the active role is the one that the activity is currently using:

AR(a : activity) = {the active role for activity a}.

- Each activity may be authorized to perform one or more roles:
  RA(a : activity) = {the authorized roles for activity a}.

- Each role may be assigned to one or more activities:
  AA(r : role) = {the authorized activities for role r}.

- Each activity may be authorized to perform one or more subjects:
  AS(a : activity) = {the authorized subjects for activity a}.

- Each role may be assigned to one or more actors (or groups):
  RC(r : role) = {the authorized actors for role r}.

- Each activity may be authorized to read-access or write-access to one or more objects:
  AO(a : activity) = {the authorized objects for activity a}.

- For each activity, the active actor (or group) is the one that is currently performing the activity:
  AC(a : activity) = {the active actor or group for activity a}.

- Activities may execute subjects. The predicate exec(a,s) is true if activity a can execute subject s at the current time, otherwise it is false:
  exec(a : activity, s : subject) = {true iff activity a can execute subject s}.

Also, four basic rules are required in the rule-based business process management security control model as followings:

- Role assignment: An activity can execute a subject only if the activity has selected or been assigned a role:
  $\forall$ a : activity, s : subject(exec(a,s) $\Rightarrow$ AR(a) = $\varnothing$).
  Like in the RBAC model, the identification and authentication process (e.g. login) is not considered an activity. All other user activities on the business process management system are conducted through subjects. Thus all active actors are required to have some active role.

- Role authorization: An activity's active role must be authorized for the activity:
  $\forall$ a : activity(AR(a) $\subseteq$ RA(a)).
  With (1) above, this rule ensures that actors can take on only roles for which they are authorized.

- Subject authorization: An activity can execute a subject only if the subject is authorized for the activity's active role:
  $\forall$ a : activity, s : subject(exec(a,s) $\Rightarrow$ s $\in$ AS(AA(AR(a)))).

  With (1) and (2), this rule ensures that actors can execute only subjects for which they are authorized. Note that, because the conditional is "only if", this rule allows the possibility that additional restrictions may be placed on subject execution. That is, the rule does not guarantee a subject to be executable just because it is in AS(AA(AR(a))), the set of subjects potentially executable by the activity's active role.

- Object authorization: A subject can access objects only if the subject is authorized for the objects with access modes:
  $\forall$ a : activity, s : subject, o : object(exec(a,s) $\Rightarrow$ access(AR(a), s, AO(a),x).

  This rule is defined using a subject to object access function access(r,s,o,x) which indicates if it is permissible for a subject in role r to access object o is mode x using subject s, where x is taken from some set of modes such as read and write.

  Like the RBAC model [1], access control decisions of RDBPSCM, such as duties, responsibilities, and qualification, are determined by the roles. But the difference is on the way of determination. That is, in the business process management it is determined at the build-time of business processes. A RBAC policy bases access control decisions on the functions of organization-specific protection guidelines within an organization, while a RDBPSCM policy is based upon access control decisions on the functions of business process-specific authorization within an organization. This is a fundamental difference between RBAC and RDBPSCM.

3.3. Application of the Role-driven BPM Security Control Model

In order to clarify the role-driven BPM security control model described in the previous section, we show how a business process model is transformed into a set of role-driven security control models through an example of the hiring business process model [8].

The hiring business process model consists of 17 activities having precedence with each other, seven roles – applicant, hiring clerk, personnel clerk, security clerk, medical clerk, hiring manager, and computer – and four relevant data – applicant information, decision result, checking results, and review results – as depicted in Fig. 4.

The detailed description of the components are the followings:

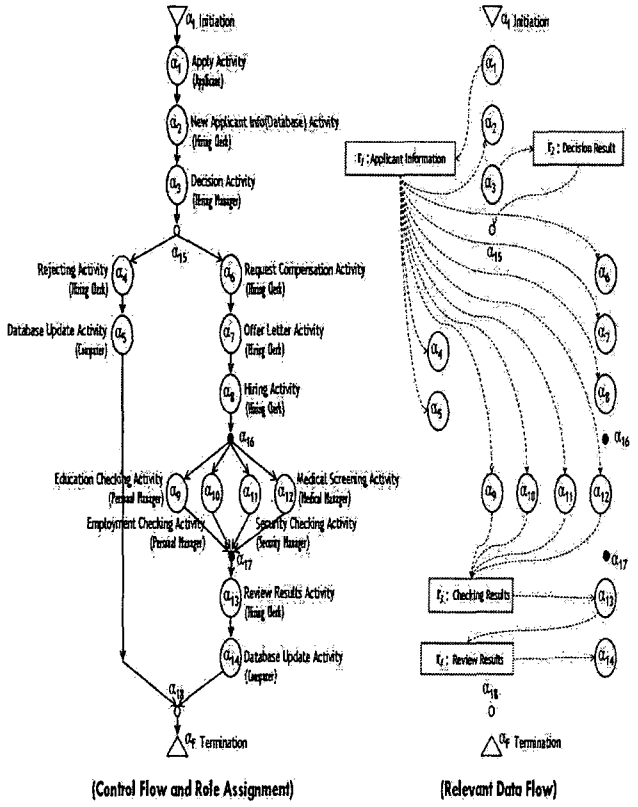


Figure 4. The Hiring Business Process Model

3.3.1. Activities

- The APPLY activity is accessed by an applicant. The applicant fills out an application form through the employment page on the World Wide Web or the employment interfaces. This entails creating a workcase of the hiring procedure and starting the workcase. Applicants should give the following information: personnel data, security data, affirmative action data including working preference, education, employment experience, etc.

- The NEW APPLICANT INFO activity validates the application information written by an applicant, stores it in the database, and prepares and distributes the information for the medical screening, the security checking, and the background checking activities.

- The DECISION activity reviews and evaluates the applicant's information and decides whether the applicant is eligible and appropriate for the requirements of an open position.

- The REJECTING activity receives the applicants who failed in the employment procedure, composes a rejection letter, and sends it to them.

- The HIRING activity physically consists of three activities: request compensation, offer letter, and hiring activity. It receives the applicants who passed in the employment procedure, composes a job offer letter, and sends it to them after deciding on salary.

- The DATABASE UPDATE activity updates the employment database automatically.

- The BACKGROUND CHECKING activity validates the background information, such as educational background and employment background, submitted by the applicants. After checking the information, the actors prepare the checking results with some comments.

- The MEDICAL SCREENING activity does some medical tests, such as for drugs, venereal diseases, and geriatric diseases. After testing, the actors prepare the test results with some comments, and send them to the personal department.

- The SECURITY CHECKING activity validates the security information written by the applicants. After checking the information, the actors write the checking results with comments.

- The REVIEWA PPLICANT INFO activity reviews the results sent by the previous activities, and decides whether the applicant should be failed or passed, based on the organization's employment policy. If the results satisfy the policy, then the actors prepare and inform so that the clerks can proceed continuously to the internal hiring procedure.

3.3.2. Actors and Roles

There are seven roles, applicant, hiring clerk, hiring manager, personnel manager, medical manager, security manager, and computer; nine actors; and two actor groups in the hiring business process model. Each actor is involved in a role. The left-hand side of Fig.4 presents the hiring business process and its role and actor assignments through the ICN modeling methodology.

3.3.3. Relevant Data

There are typically four relevant data within the hiring business process model: application information, decision result, checking results, and review results. In fact, there are other relevant data for processing applications, but we do not specify the details here to simplify the model. The right-hand side of Fig.4 depicts the relevant data flows and assignments (access mode: read or write) on each of the activities.

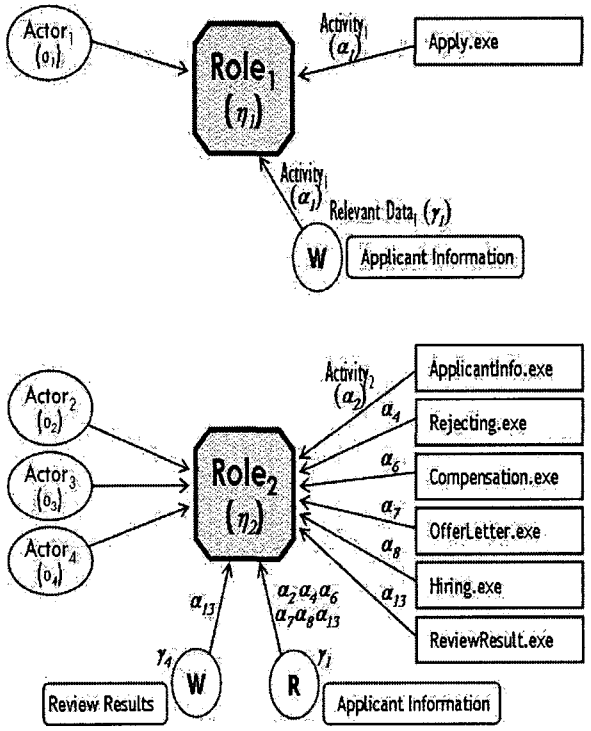


Figure 5. $Role_1$ and $Role_2$ Security Control Models of the Hiring Business Process Model

After applying the notion of the role-driven BPM security control model into a business process model, we are able to gain a set of role-driven security control models, the number of which is exactly same to the number of roles in the corresponding business process. Fig.5 is to present two role-driven security control models that are corresponding to $Role_1$ and $Role_2$, respectively, after applying to the hiring business process model.

4. Conclusions

In recent, many organizations in industry and civilian government start deploying business process management technology and systems with expecting the dramatic operational efficiency improvement on their business and administrative environments. With these atmospheres, the security issue is becoming a much more important challenge in the business process management literature.

So far, the role-based access control model has been accepted as a promise solution and standard that is able to accomplish the central administration of an organizational specific security policy and to meet the secure processing needs of many commercial and civilian government organizations. In spite of these facts, the RBAC model should be inapplicable to the business process management systems without further modifications and extensions. So, we proposed the role-driven BPM security control model that is directly applicable to the business process management system. We defined a graphical representation and formal description of the model, and demonstrated its feasibility through applying the model to the hiring business process model. As future research issues, there might be several extensions that we should investigate how the concept of the role-driven security control model is incorporated into the other families of coordination models and systems. Additionally, we expect that, in the near future, the role-driven business process security control model be taken into consideration as a methodology to design and implementation of secured business process management systems.

Notes and Comments. The research was conducted by supports of the research funds of Kyonggi University.

References

[1] David F. Ferraiolo and D. Richard Kuhn, "Role-Based Access Controls," Proceedings of the 15th NIST-NSA National Computer Security Conference, Baltimore, Maryland, October 13-16, 1992.

[2] David F. Ferraiolo and et al., "AN INTRODUCTION TO ROLE-BASED ACCESS CONTROL", NIST/ITL Bulletin December, 1995.

[3] David F. Ferraiolo, Janet A. Cugini, and D. Richard Kuhn, "Role-Based Access Control (RBAC): Features and Motivations," Proceedings of the 11th Annual Computer Security Applications, 1995.

[4] Clarence A. Ellis, Gary J. Nutt, "Office Information Systems and Computer Science", ACM Computing Surveys, Vol. 12, No. 1, 1980.

[5] Clarence A. Ellis, Gary J. Nutt, "The Modeling and Analysis of Coordination Systems", University of Colorado/Dept. of Computer Science Technical Report, CU-CS-639-93, 1993.

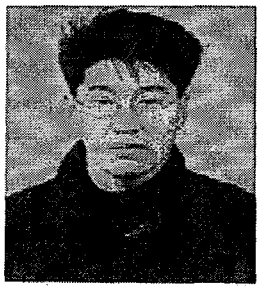
[6] Clarence A. Ellis, "Formal and Informal Models of Office Activity", Proceedings of the 1983 Would Computer Congress, Paris, France, 1983.

[7] James H. Bair, "Contrasting Workflow Models: Getting to the Roots of Three Vendors", Proceedings of International CSCW Conference, 1990.

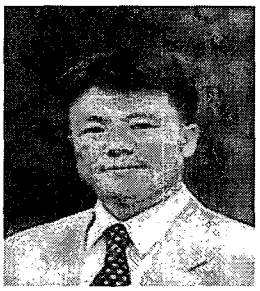
[8] Kwang-Hoon Kim, "Practical Experience on Workflow: Hiring Process Automation by FlowMark", IBM Internship Report, IBM/ISSC Boulder Colorado, 1996.

[9] Kwang-Hoon Kim and Su-Ki Paik, "Practical Experiences and Requirements on Workflow", Lecture Notes Asian '96 Post-Conference Workshop: Coordination Technology for Collaborative Applications, The 2nd Asian Computer Science Conference, Singapore, 1996.

[10] http://csrc.nist.gov/rbac



Jae Kang Won is a student of doctoral course in the department of Computer Science and member of the Collaboration Technology Research Laboratory at Kyonggi University, South Korea. Mr. Won's research focus is workflow systems, groupware, Business Process Management (BPM), workflow mining, database systems, computer networks, and Roll-based Access Control (RBAC). He received the B.S. degree in biology from the kangnung University in 1999. And he received the M.S. degree in computer science from the kyonggi University in 2002.



Kwang-Hoon Kim is an Associate Professor of Computer Science Department and Director of the Collaboration Technology Research Laboratory at the Kyonggi University, South Korea. At Kyonggi, he is involved in research and teaching of workflow, groupware, coordination theory, computer networks, software architectures, and database systems. He received the B.S. degree in computer science from the Kyonggi University in 1984. And he received the M.S. degree in computer science from the Chungang University in 1986. He also received the M.S. and Ph.D. degree from the computer science department of the University of Colorado at Boulder, in 1994 and 1998, respectively. He had worked as a researcher and developer at Aztek Engineering, American Educational Products Inc., IBM, and ETRI. In present, he is a vice-chair of the BPM Korea Forum, a chair of the Workflow Project Group in TTA, and a vice-chair of the Workflow Management Coalition. He has also been on the editorial board of the journal of KSII, and the committee member of the several conferences and workshops. His research interests include groupware, workflow systems, BPM, CSCW, collaboration theory, distributed systems, data warehousing and mining, software architecture modeling and simulation, e-commerce, and computer networks.