



## Inside this issue:

- ✂ **Abstract Review, Excerpts – A Reference Monitor for Workflow Systems with Constrained Task Execution – Part I**
- ✂ **RBAC Taskforce – Meeting Update**
- ✂ **Upcoming Meetings**

### VHA/IHS RBAC TF Chair

Robert O'Hara, MD  
[Robert.Ohara@med.va.gov](mailto:Robert.Ohara@med.va.gov)

### VHA Deputy Chief Architect

RBAC Project Manager  
Steve Wagner  
[Steve.Wagner@med.va.gov](mailto:Steve.Wagner@med.va.gov)

### VHA Security Architect

RBAC Architect  
Mike Davis, CISSP  
[Mike.Davis@med.va.gov](mailto:Mike.Davis@med.va.gov)

### VHA Security Architect

RBAC Architect  
Ed Coyne, PhD  
[Ed.Coyne@med.va.gov](mailto:Ed.Coyne@med.va.gov)

### VHA Software Security Architect

Amy Page  
[Amy.Page@med.va.gov](mailto:Amy.Page@med.va.gov)

### RBAC Project Lead

Suzanne Webb  
[Suzanne.Gonzales-Webb@va.gov](mailto:Suzanne.Gonzales-Webb@va.gov)

## Abstract Review, Excerpts - A Reference Monitor for Workflow Systems with Constrained Task Execution

**Jason Crampton<sup>1</sup>, Information Security Group  
Royal Holloway, University of London**

### Abstract

Constraints in access control in general and separation of duty constraints in particular are an important area of research per Jason Crampton. There are two important issues relating to constraints: their specification and their enforcement. His studies lead him to believe that existing separation of duty specification schemes are rather complicated and that the few enforcement models that exist are unlikely to scale well. This abstract examines the assumptions behind existing approaches to separation of duty and present a combined specification and implementation model for a class of constraints that includes separation of duty constraints. The specification model is set-based and has a simpler syntax than existing approaches. We discuss the enforcement of constraints and the relationship between static, dynamic and historical separation of duty constraints. Mr. Crampton's abstract also proposes a model for a scalable role-based reference monitor, based on dynamic access control structures that can be used to enforce constraints in an efficient manner.

### Introduction

Separation of duty is an important control principle in management whereby sensitive combinations of duties are partitioned between different individuals in order to prevent the violation of business rules. Based on this description, a very simple example of this is that narcotics may require two different signatures, as in an RN signing out narcotics from the inpatient pharmacy cannot be the same RN entering (receiving) narcotic count on the floor.

A paper written on separation of duty in role-based systems [1] proposed a rule-based specification scheme for separation of duty constraints and a history-based implementation to enforce those constraints. Several authors have since identified increasingly complex separation of duty requirements and specification schemes to express them [2, 3, 4, 5]. However, none of these papers have suggested a model for implementing such constraints. Per Mr.

<sup>1</sup> Use of this article was by permission of the author.



## Upcoming Meetings

- ✂ **HL7 20<sup>th</sup> Annual Plenary & Working Group**  
September 10-15, 2006  
Boca Raton, FL
- ✂ **Infosec CD '06**  
2006 Information Security Curriculum Development Conference  
September 22-23, 2006  
Kennesaw, GA
- ✂ **INCITS/CS1**  
Roles Based Access Controls Task Group  
October 2, 2006  
Atlanta, GA
- ✂ **INCITS/CS1**  
Cyber Security Task Group  
October 3-4, 2006  
Atlanta, GA
- ✂ **ONC (ONCHIT)**  
American Health Information Community Meeting  
October 7, 2006  
Washington, DC 20201
- ✂ **OASIS Adoption Forum**  
October 28-29, 2006  
London, United Kingdom
- ✂ **HL7 Educational Summit**  
November 7-9, 2006  
Lynnwood, WA
- ✂ **ASTM Committees E31**  
November 12-14, 2006  
Atlanta, GA

Crampton's abstract, separation of duty requirements is an important issue in workflow management systems. It has been suggested [6] that such requirements can be enforced using logic programming techniques to compute all valid execution paths for a workflow (in the presence of constraints) and permitting an access request to proceed only if it belongs to a valid execution path [6]. It is our belief that this approach will not scale well to large-scale applications.

In this paper he proposes a simple specification scheme for separation of duty constraints. In fact, Mr. Crampton supports a definition for constraints that are not separation of duty constraints in the traditional sense which is why in this paper he uses the term authorization constraint [6]. Unlike most existing specification schemes, we do not explicitly specify the conditions that must be preserved if the constraint is to be satisfied. This is for two reasons: firstly, we believe that this approach places an unnecessary burden on the syntax of the specification scheme; and secondly, that the constraints should be enforced by the reference monitor. Therefore, we also propose a simple implementation model that can be used to enforce a restricted set of the authorization constraints supported by our specification scheme. This model is based on the idea of dynamic access control structures that are updated when constraint-relevant events occur.

## BACKGROUND

This abstract introduces a role-based access control model which provides a context for the specification scheme and enforcement model. It contains a discussion of constraints in role-based models and workflow systems and issues related to constraint specification in a role-based model. In the latter discussion he hopes to provide the motivation for support of the presented specification scheme and for certain aspects of the enforcement model.

## RBAC constraints

The existence of a role hierarchy facilitates the specification of separation of duty constraints because of its ability to model organizational structures. Using healthcare roles as an example, a billing clerk and a pharmacist role will typically be incomparable roles in the role hierarchy, and it may well be an organizational requirement that no user be assigned to both roles.

In a workflow environment, it may be that when co-signing for narcotics, the dispensing 'approve' action must be co-signed (Mr. Crampton uses the terminology 'invoked' twice) by not only a different user, but by a role that is more senior than the role that



## RBAC Newsletter Editor

ATTN: Suzanne Webb  
RBAC Project Lead  
10260 Campus Point MS-B1E  
La Jolla, CA 92121

Or e-mail:

[Suzanne.Gonzales-Webb@va.gov](mailto:Suzanne.Gonzales-Webb@va.gov)

invoked the raise action [6], such as an RN and a supervisory RN. Alternatively, we may have a ‘dispensing approve’ action and insist that the permissions (narcotic pull from stock, approve) and (narcotic dispense, raise) are not assigned to the same role.

The literature has long recognized that there are three different “flavors” of separation of duty constraint. Static separation of duty typically constrains the assignment of users and permissions to roles. Dynamic separation of duty typically constrains the activation of roles and invocation of permissions in the run-time environment. Historical separation of duty typically constrains the invocation of permissions over the course of time; for example, we may require that no user can receive narcotics from the pharmacy and log the narcotics to floor stock.

In many cases, a constraint will apply to the same object, as in the transfer of narcotics example above. Several papers have distinguished between order-dependent and order-independent constraints [1, 5]. In the former case, the constraint would require that narcotics are logged into floor stock before they are issued or dispensed. In the latter case, no such requirement would be made.

[Abstract review will continue in next month’s newsletter.]

- [1] Simon, R., and Zurko, M. Separation of duty in role-based environments. In Proceedings of 10<sup>th</sup> IEEE Computer Security Foundations Workshop (Rockport, Massachusetts, 1997), pp. 183–194.
- [2] Ahn, G.-J., and Sandhu, R. Role-based authorization constraints specification. ACM Transactions on Information and System Security 3, 4 (2000), 207–226.
- [3] Gavrilu, S., and Barkley, J. Formal specification for role based access control user/role and role/role relationship management. In Proceedings of Third ACM Workshop on Role-Based Access Control (Fairfax, Virginia, 1998), pp. 81–90.
- [4] Gligor, V., Gavrilu, S., and Ferraiolo, D. On the formal definition of separation-of-duty policies and their composition. In Proceedings of 1998 IEEE Symposium on Research in Security and Privacy (Oakland, California, 1998), pp. 172–183.
- [5] Jaeger, T., and Tidswell, J. Practical safety in flexible access control models. ACM Transactions on Information and System Security 4, 2 (2001), 158–190.
- [6] Bertino, E., Ferrari, E., and Atluri, V. The specification and enforcement of authorization constraints in workflow management



## RBAC Newsletter Editor

ATTN: Suzanne Webb  
RBAC Project Lead  
10260 Campus Point MS-B1E  
La Jolla, CA 92121

Or e-mail:

[Suzanne.Gonzales-Webb@va.gov](mailto:Suzanne.Gonzales-Webb@va.gov)

systems. ACM Transactions on Information and System Security 2, 1 (1999), 65–104.

[7] Clark, D., and Wilson, D. A comparison of commercial and military computer security policies. In Proceedings of 1987 IEEE Symposium on Security and Privacy (Oakland, California, 1987), pp. 184–194.

[8] Sandhu, R., Coyne, E., Feinstein, H., and Youman, C. Role-based access control models. IEEE Computer 29, 2 (1996), 38–47.

## RBAC Taskforce – Update

The next RBAC Taskforce meeting call will be held tentatively September 6, 2006 - Wednesday at 1100PST / 1200MT / 1300CT / 1400EST.

The RBAC Taskforce will focus on completing the Healthcare Roadmap for both the Licensed and Non-Licensed portions that were submitted. Permissions developed by the Non-Licensed group will be added to the Licensed Practitioners and the roadmap spreadsheet will be completed. The discussion of constraints to the current Permission Catalog and Roles may also occur as well as an update on the initiation of RBAC incorporation into the VA re-engineering projects. Members will be contacted with additional materials in preparation for the meeting. If you would like to be a part of the Task Force please contact Suzanne Gonzales-Webb for more information. Thank You.

~

Role-Based Access Control is critically important to the security aspects of the VA and other healthcare organizations. There is a growing management and security demand for RBAC to be implemented in healthcare systems.

RBAC grants rights and permissions to roles rather than individual users. Users then acquire the rights and permissions by being assigned to appropriate roles. By grouping individuals with other individuals who have similar access rights, RBAC can provide significant security management efficiencies.

The latest RBAC Documentation additions and prior RBAC Newsletters can be found on the RBAC Website.

~