# Role Based Access Control (RBAC): Potential & Limitations Reading List

Ioannis G. Pagkalos
*MSc Web Technology, University of Southampton*
*ip1w07@ecs.soton.ac.uk*

## Abstract

*Role Based Access Control (RBAC) is the way forward for modern Access Control implementations. This reading list provides an introduction to RBAC, followed by a list of References (Journal Articles, Conference Papers) and relevant Bibliography (Textbooks, Web Links). The selection of each of the above resources is explained in the section preceding the list (section 2: Further Reading).*

## 1. Introduction

Initial research in the area of Access Control (the means by which the ability to access a computer resource is granted or revoked) resulted in two fundamental policies: MAC (Mandatory Access Control) and DAC (Discretionary Access Control). Both model definitions can be found in U.S. Department of Defense's Trusted Computer Security Evaluation Criteria (TCSEC) – also known as "The Orange Book" [17]

DAC gives users the ability to define permissions on objects that they own, whereas MAC assigns security clearance levels to individual objects. As defined in the DoD's TCSEC, MAC is "A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e. clearance) of subjects to access information of such sensitivity."

Both of these policies are not well suited to the security requirements of a modern organisation, where access should be based on the role(s) that the user has as part of the organisation, rather than being object-based. For this reason, Role Based Access Control (also called Role Based Security), as formalized in 1992 by David Ferraiolo and Rick Kuhn, [1] has become the predominant model for advanced access control because it reduces the complexity and cost of security administration.

RBAC is a flexible and policy-neutral model that resembles an organisation's hierarchy. Permission to perform a specific operation is assigned to a role within the organisational structure. Users of the system are then assigned roles and thus acquire the permission to perform these operations. This provides a system where permissions are assigned indirectly, making the process of managing user rights easy & simple. With RBAC, it is also not necessary to translate the organisation's structure into another view to accommodate for an access control mechanism.

## 2. Further Reading

### 2.1. Pre-RBAC and generic resources

Bishop [15] differentiates security policies into two groups: military security policies and commercial security policies. His book on Computer Security provides a good view on why developing an all-purpose security model is difficult (and is an excellent computer security resource in general)

MAC & DAC are defined in the DoD's Trusted Computer Security Evaluation Criteria (TCSEC) [17], an important resource in the history of Access Control.

### 2.2. The RBAC Model

RBAC was first presented by D.F. Ferraiolo and D.R. Kuhn in 1992 [1]. This paper, along with a paper from R. S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman in 1996 [2] provide the basis for the RBAC Framework.

RBAC was standardized in 2004 by ANSI INCITS. The original authors have published a paper [3] describing the process towards this unified standard.

With the growing success of RBAC, the original team produced a book [16] which is now considered an excellent resource for RBAC study.

Further information can be obtained by reading W.A. Jansen's [4],[5] papers on RBAC (specifically role hierarchies and the revised version of the RBAC model)

### 2.3. The potential in RBAC

This Web Link [18] provides links to a number of RBAC case studies and experience reports from NIST (the National Institute of Standards and Technology is an Agency of the U.S. Department of Commerce)

NIST has also studied the economic impact of RBAC in U.S. businesses and published a report [19]

A paper discussing the overall effectiveness of RBAC was published on 1997 [6]

### 2.4. Limitations of RBAC & Solutions / Extensions

RBAC has become a very popular access control model and is now extensively used in industry, government and commercial organizations [18]. Research is currently under way to solve problems related to the model and/or its applications, or to extend the model and adapt it to a multitude of varied environments. A few examples follow:

The original RBAC model cannot manage permissions on a sequence of operations. This is discussed on the original RBAC model paper [2] and solutions are proposed in these papers [9],[10] (TBAC – Task Based Access Control is specified here as well)

RBAC must take into consideration the vast security issues of the World Wide Web. RBAC/Web[7] is an extension of RBAC for the World Wide Web. A study around its implementation on Corporate Intranets can be found in this paper [8].

RBAC also exists for web services: Web applications can use RBAC services defined by the OASIS XACML Technical Committee. The XACML specification [20] describes building blocks from which an RBAC solution is constructed [21]. XACML 2.0 and all the associated profiles were approved as OASIS Standards on 1 February 2005.

Another interesting topic is making the model capable of handling the dynamic and ever-changing environment of real - life organizations [11]. Examples include adding a 'dynamic' dimension to the model (e.g. DARBAC) [12],[14] and making the model capable of handling collaborative environments and applications (when a decision to allow access depends on more than one user) [13]

## 3. References


[1] D.F. Ferraiolo and D.R. Kuhn, "Role Based Access Control", *15th National Computer Security Conference*, Oct, 1992

[2] R. S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, "Role-Based Access Control Models", *IEEE Computer 29(2): 38-47*, IEEE Press, 1996.

[3] R. Sandhu, D.F. Ferraiolo, D, R. Kuhn, "The NIST Model for Role Based Access Control: Towards a Unified Standard," *Proceedings, 5th ACM Workshop on Role Based Access Control*, July 26-27, 2000

[4] W.A. Jansen, "Inheritance Properties of Role Hierarchies," *21st National Information Systems Security Conference*, October 6-9, 1998, Crystal City, Virginia

[5] W.A. Jansen, "A Revised Model for Role Based Access Control", *NIST-IR 6192*, July 9, 1998

[6] D. Ferraiolo and J.F. Barkley, "Comparing Administrative Cost for Hierarchical and Non-hierarchical Role Representations", *Second ACM Workshop on Role-Based Access Control*, Nov 6-7, 1997

[7] J. Barkley, A.V. Cincotta, D.F. Ferraiolo, S. Gavrila, , D.R. Kuhn, "Role Based Access Control for the World Wide Web", *20th National Computer Security Conference*, 1997

[8] D.F. Ferraiolo, J. Barkley, "Specifying and Managing Role-Based Access Control within a Corporate Intranet", *Second ACM Workshop on Role-Based Access Control, 1997*

[9] Imtiaz Mohammed and David M. Dilts, "Design for dynamic user-role-based security", *Computers & Security, 13(8):661-671*, 1994.

[10] Roshan Thomas and Ravi S. Sandhu, "Conceptual foundations for a model of task-based authorizations", *IEEE Computer Security Foundations Workshop (7):66-79*, Franconia, NH, June 1994.

[11] Dimitrios Baltatzis, Christos K. Georgiadis and G. Pangalos, "Dynamic authorizations: an important security aspect in distributed systems", *International Conference on Mobile Data Management*, 2005

[12] Andreas K. Mattas, Ioannis Mavridis, G. Pangalos, "Towards Dynamically Administered Role-Based Access Control", *14th International Workshop on Database and*

*Expert Systems Applications (DEXA'03)*, September 1-5, 2003

[13] A. Mattas, I. Mavridis, C. Ilioudis, I. Pagkalos, "Dynamic Access Control Administration for Collaborative Applications", Proceedings of 10th WSEAS International Conference on COMPUTERS, Greece, July 2006.

[14] A. Mattas, I. Mavridis and I. Pagkalos, "An Implementation of Dynamically Administered Role-based Access Control on the Web", *International Review on Computers and Software Journal*, 2007

# 4. Bibliography

## 4.1. Textbooks & Standards

[15] Bishop, M., *Computer Security: Art and Science*, Addison-Wesley Publishing Company, Boston, Massachusetts, 2004.

[16] David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli, *Role-Based Access Control*, Artech House, 2003

[17] Department of Defense, *Trusted Computer Security Evaluation Criteria, DoD 5200.28-STD*, 1985.

## 4.2. Web Links

[18] NIST RBAC Case Studies – http://csrc.nist.gov/groups/SNS/rbac/case_studies.html

[19] NIST RBAC economic impact report summary – http://csrc.nist.gov/groups/SNS/rbac/documents/rbac-impact-summary.doc

[20] OASIS group – XACML Introduction, http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html

[21] OASIS group - Core and hierarchical role based access control (RBAC) profile *of XACML v2.0*, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf