A Systematic Literature Review on Role-Based Access Control

Eric D. Helms, JeeHyun Hwang

North Carolina State University

Department of Computer Science

890 Oval Drive, Box 8206

Raleigh, NC 27695-2858

Abstract

Since the introduction of the Role-based access control (RBAC) standard in the late 1990's, RBAC has become an increasingly popular access control mechanism for enterprises such as web applications, mobile computing and databases. RBAC restricts access to resources based on the identity of subjects connected to logical groupings of permissions called roles. The introduction of computing into new domains has led to proposals for extensions to the standard RBAC model; for example, defining additional constraints among roles, adding context or defining new hierarchy relationships. *The goal of this work is to provide practioners an assessment of the state of extended models of RBAC and researchers with insights into the lack of robust evaluation of RBAC extension models.* We conducted a systematic literature review by collecting and synthesizing relevant research papers in the area of RBAC extensions. We initially collect XXXX papers from sources such as IEEE and ACM websites and selected X primary sources. We performed a comparative analysis of the primary sources to find relationships among extended models and analyze the state of RBAC extension evaluations.

Keywords: RBAC, access control, systematic literature review

1. Introduction

Role based access control (RBAC) was first introduced in the 1990s when the National Instittute for Standards and Technology (NIST) requested that a unified standard be created by combining the Ferraiolo and Kuhn model [1] with the framework proposed by Sandhu, et al [2]. In an RBAC model, roles represent a group of users who are involved in a specific job function in an organization. RBAC assigns permissions of specific actions on resources to roles instead of individual users. Therefore, in order to gain roles' permission on specific resources, users acquire appropriate roles first. RBAC is a generalized access control approach used for various applications including web services, database applications, and healthcare applications. RBAC has advantages in maintaining and managing organization's security policies. For example, if a user is to access manager role's resources within a given

organization, security policy administrators simply add the user to be associated with the manager role.

Since the introduction of the standardized RBAC model, innovation and the spread of software engineering into new domains has led to scenarios that, by some accounts, the standard RBAC model cannot handle. For example, RBAC is ill-equipped to handle the additional entities that need to be taken into consideration during authorization with the introduction of privacy concerns in domains such as healthcare Thus, a series of extensions to the standard RBAC model have appeared in the literature, each adding one or more features. However, as researchers often develop their own specialized extended models of RBAC, their research cannot be generalized or compared with other research work appropriately.

The goal of this work is to provide practioners an assessment of the state of extended models of RBAC and researchers with insights into the lack of robust evaluation of RBAC extension models.

A systematic literature review is designed to yield quanitfiable results across a body of research in order to draw out similarities, trends and defiencies in an area as a whole. The review we performed yielded 1716, of which XX were deemed primary sources for inclusion as model extensions to the RBAC standard model. This review is intended to serve as a starting place for researcher's looking to tackle new problems in the realm of authorization and prevent re-invention of the wheel. For developer's looking to find a model to fit their seemingly unique access control needs, this review will provide a basis for comparison and easy look-up for what extension based model to use. Further, the review provides insight into the state of evaluation, or lack thereof, within the RBAC extension model community.

Our research provides contributions to the community in the following ways:

- Summarizes current extended RBAC research work and its contributions
- Guides a direction for a standard of extended RBAC. Understanding the categorization and the motivation of the existing research results helps decide a standard of extended RBAC.
- Our work shows a criteria in comparison among research results.
- Identify the research challenges in the areas of security policies and suggest a future extension of RBAC
- Identify the deficiencies in RBAC extension evaluation

The rest of the paper is organized as follows. Section 2 covers background and the core RBAC model. Section 3 lays out the process used in conducting the review. Section 4 provides the results of the search. Section 5 tackles the research questions and analyzes the results. Section 6 contains the final conclusions.

- TODO: Add some references to the prevalence of RBAC in industry
- TODO: Add link to RBAC standard documents
- TODO: List research questions here or in process

2. Core Role Based Access Control

Since the basis for our review is extensions to the core model, we will describe the core model, associated entities and other terminology encountered across the space of our review. The NIST RBAC model proposed by Ferraiolo et al. and later adopted as the official standard for RBAC by the International Committee for Information Technology Standards (INCITS) consists of four basic entities:

- a set of users *Users*: A user can be a person or an agent.
- a set of roles *Roles*: A role is a collection of permissions to perform a specific job function in an organization.
- a set of permissions *Permissions*: A permission refers to an access mode that can be exercised on an object in the system and a session relates a user to possibly many roles.
- a set of sessions *Sessions*: In each session, a user can be assigned to some of the roles, only when the corresponding role is enabled for activation for that time.

In the RBAC, a user can exercise a permission only if the user are assigned to a role. In addition to the four basic components, two functions are defined: the user role assignment (UA) and the role permission assignment (PA) functions. UA models assignment of users to roles. PA models assignment of permissions to roles.

P1: Describe RBAC entities
P2: Note the 4 levels of RBAC
P3: Concisely describe level 1
P4: Concisely describe level 2
P5: COncisely describe level 3
P6: Concisely describe level 4

3. Process

The systematic literature review process was developed in whole prior to application and agreed upon by the researchers following recommendations from Kitchenham's suggested processes [3]. The systematic literature review process was broken down in to four stages and the rest of this section is broken down by each stage. The stages were:

- Development of a search strategy
- Elimination of papers based on title
- Elimination of papers based on abstract
- Elimination of papers based on content and matching to elimination criteria

3.1. Search Strategy

For the first phase of our systematic literature review, a search strategy for finding papers was developed. The search strategy was executed by an automated comprehensive search taking as input a set of academic search engines and a list of search criteria. The search performed was done in an automated way using a set of scripts to query and collect data from each search engine with the criteria string as input. For each criteria for each search engine, the results were captured until a stopping criteria was met. The search algorithm was performed as follows:

1. Remote call to search engine with current search start position and the current search criteria.
2. Parse results and extract paper title, authors and year of publication.
3. Compare results against stopping criteria.
    - If stopping criteria met, stop search.
    - If stopping criteria not met, increase search position by number of results and return to step 1.

The stopping criteria used was either after the first 1000 results, a limitation imposed by some of the search engines, or if ten consecutive results did not contain the search criteria phrase within the title. After gathering all 12 data sets, the data was combined into a master list by systematically comparing the bibliographic information for each. After producing a master list, a series of elimination rounds were performed to narrow the list of papers and identify primary sources.

3.2. Elimination Rounds

The elimination rounds were performed based on reading of the title, abstract and finally the paper itself. While each elimination stage had a unique set of criteria for elimination the general procedure for elimination for the researchers was as follows.

- Each reviewer independently classified papers as relevant, irrelevant or uncertain based off elimination criteria
- Those papers marked as relevant by both reviewers were kept and those marked irrelevant by both were thrown out.
- Papers marked as relevant, or irrelevant by a single reviewer were combined with all papers marked as uncertain and discussed by both reviewers. From this discussion, papers were either thrown out or kept until the next round of the review. Ties were broken by an indepedent party.

3.2.1. Title Elimination

The first round of elimination was performed by strict examination of the title. Each researcher was tasked with deciding on elimination by answering the following questions:

- Did the title contain a reference to 'role based access control' or 'RBAC'?
- Did the title contain a reference to 'model'?

3.2.2. Abstract Elimination

The second round of elimination was based on strict reading of the abstracts of papers that survived title elimination. Researchers read each abstract and evaluated relevancy based off:

- Does the abstract mention a proposed model?
- Does the abstract mention extension of role-based access control?
- Does the abstract mention either an implementation, evaluation or domain for their model?

3.2.3. Content Elimination

The final elimination round involved taking the entire paper into consideration and answering five questions that would serve as the basis for elimination. The data collected by answering these questions served as the basis towards answering the research questions. The questions each reviewer attempted to answer based on the content of the paper was:

- Does this model extend the core model?
- What reasons and evidence do researchers give that RBAC needs extension?
- Was the paper and subsequent model inspired by a real world example?
- Is there any evaluation of the proposed model? If yes, how did they do one? If no, why?
- Did the authors implement their model?

4. Results

4.1. Search

For our systematic literature review, the search strategy was applied to four search engines and three search strings based on popularity and database size. This produced 12 different data sets that are combining for overlapping papers resulted in 1716 candidates. The paper count for each search engine and criteria are shown in Table 1.

TODO: Add metrics for each portion of the elimination

4.2. Extraction

After selection of primary sources, the next step was to extract data from each paper that pertained to our research questions in order to look for trends. The first step was to take the individual data generated from the final elimination round and organize this information around the research questions. During the paper reading round, and resulting data, the fact that the papers were logically falling into a number of categorizations became evident. Thus, the first step undertaken was to answer the question of what categories exist

Search Engines	**RBAC**	**role based access control**	**role-based access control**	**Total**
Google Scholar	651	213	435	1299
ACM Portal	500	20	720	1240
IEEExplore	200	40	230	470
CiteSeerX	100	100	150	350
Totals	1451	373	1535	3359
Combined				**1716**

Table 1: Paper counts after applying search strategy

for the RBAC model extensions and what papers feel into what categories. Each paper deemed a primary source and the papers associated categorization are shown in Table 2.

Given that there were multiple papers for some categories, the researchers decided to tackle all further research questions by first analyzing the research question on a per category basis and then looking across all categories for generalization and trends.

5. Category Definitions

We found that different definitions for the same terms. Therefore, we next describe terms and definitions.

- Task-Based Access Control:
- Agent-Based Access Control:
- Obligations: obligations are requirements, which should be fulfilled before or after authorization decision is enforced. Consider that a user has permission to access specific resources. For example, obligation is that the user should complete her/his office duty before accessing the resources.
- Inheritance: Inheritance defines an inheritance relationship among attributes such as roles. For example, the role structure for a company use employee role for employees. Department manager may inherit all permissions of the employee role. (Role-Based Access Control by F. Ferrailolo et al.)
- Static Separation of Duty (SSoD): SSoD restricts the conflicting-role assignments statically that are associated with a user. On situations where multiple roles can be associated with a single user and roles $Role_A$ and $Role_B$ are conflicting each other, no permission is given to a user who is assigned to both $Role_A$ and $Role_B$. SSoD is known to be too rigid for practical use in cases where a user should have permissions as either $Role_A$ and $Role_B$. (Role-Based Access Control by F. Ferrailolo et al.)

Paper	**Category**
Alam, M. and Hafner, M. and Breu, R. 2006 [4]	Constraint
Tzelepi, Sofia K. and Koukopoulos, Dimitrios K. and Pangalos, George 2001 [5]	Context
Haibo, SHEN and Fan, HONG 2005 [6]	Context
Damian G. Cholewka and Reinhardt A. Botha and Jan H. P. Eloff 2000 [7]	Context
Huang, X. and Wang, H. and Chen, Z. and Lin, J. 2006 [8]	Context
Motta, G.H.M.B. and Furuie, S.S. 2003 [9]	Context
Bao, Y. and Song, J. and Wang, D. and Shen, D. and Yu, G. 2008 [10]	Context
Yamazaki, W. and Hiraishi, H. and Mizoguchi, F. 2004 [**?**]	Context
Jian-min, H. and Xi-yu, L. and Hui-qun, Y. and Jun, T. 2008 [11]	Context
Thein, N. and others 2011 [12]	Context
Zou, D. and He, L. and Jin, H. and Chen, X. 2009 [13]	Context
Hasebe, K. and Mabuchi, M. and Matsushita, A. 2010 [14]	Delegation
Zhang, Z. and Zhang, X. and Sandhu, R. 2006 [15]	Organizational
Ni, Q. and Trombetta, A. and Bertino, E. and Lobo, J. 2007 [16]	Privacy
Masoumzadeh, A. and Joshi, J. 2008 [17]	Privacy
Zhao, Y. and Zhao, Y. and Lu, H. 2008 [18]	Resource
Bertino, E. and Catania, B. and Damiani, M.L. and Perlasca, P. 2005 [**?**]	Spatial
Ray, I. and Kumar, M. and Yu, L. 2006 [19]	Spatial
Hansen, F. and Oleshchuk, V. 2003 [20]	Spatial
Aich, S. and Sural, S. and Majumdar, A. 2007 [21]	Spatio-Temporal
Chen, L. and Crampton, J. 2008 [22]	Spatio-Temporal
Samuel, A. and Ghafoor, A. and Bertino, E. 2007 [23]	Spatio-Temporal
Chandran, S. and Joshi, J. 2005 [24]	Spatio-Temporal
Ray, I. and Toahchoodee, M. 2007 [19]	Spatio-Temporal
Aich, S. and Mondal, S. and Sural, S. and Majumdar, A. 2009 [25]	Spatio-Temporal
Yao, L. and Kong, X. and Xu, Z. 2008 [26]	Task
ZHANG, S. and CHEN, X. and HOU, G. 2009 [27]	Task
Oh, S. and Park, S. 2003 [28]	Task
Joshi, J.B.D. and Bertino, E. and Latif, U. and Ghafoor, A. 2005 [29]	Temporal

Table 2: Primary sources grouped by categorization

- Dynamic Separation of Duty: Dynamic SoD (DSD) is known to be more flexible than SSD. DSD restricts the conflicting-role assignments dynamically that are associated with a user. On situations where multiple roles can be associated with a single user and , given a context, roles $Role_A$ and $Role_B$ are conflicting each other dynamically, no permission is given to a user. (Role-Based Access Control by F. Ferrailolo et al.)

We define temporal and spatial constraints as follows:

- Temporal Constraints: Temporal constraints are time-based constraints in specifying access control policies. For example, in organizations, periodic temporal durations are enforced while a specific role is permitted to conduct an action. Consider that part-time employee works only from 9:00 a.m. to 3:00 p.m. In such cases, the part-time employee role should access required resources during the interval. Temporal constraints can incorporate either on roles, user-role assignments, or role-permission assignments. (Role-Based Access Control by F. Ferrailolo et al.)

- Spatial Constraints: Spatial constraints are location-based constraints in specifying access control policies. For example, in organizations, locations are enforced while a specific role is permitted to conduct an action. Consider that part-time employee works only in specific location. In such cases, the part-time employee role should access required resources only when the user is in the location. Spatial constraints can incorporate either on roles, user-role assignments, or role-permission assignments.

6. Analysis

6.1. Research Question 1

What are the deficiencies in the current RBAC model?

6.2. Research Question 2

What are the motivations behind RBAC extensions?

6.3. Research Question 3

Do the extension models have corresponding implementations in practice?

When designing and proposing a model targeted at a feature that is rooted in practical usage by real software systems, bringing the model to life is strong evidence that the proposed model can work in practice. The concept of authorization, and access control is rooted in a business need. Thus, any access control model needs to be feasible in the real world not just on paper. We analyzed the primary sources to see how many proposed models actually had implmenetations associated with them. And quantified the type of implementation. Whether the implementation was for a real system, for a prototype and/or used in a production environment.

Of the 29 papers surveyed, there was a significant lack of implementation with 21 of the paper providing no mention of a implementation or prototype. Of the remianing 8 papers that did mention an implementation, half were simply prototypes developed by the authors while the other half were claimed to be implemented within a real system.

6.4. Research Question 4

How are extended RBAC models evaluated in theory and in practice?

Providing evaluation of a proposed model is a key component in establishing the models validity. The papers were examined for evidence of evaluations ranging from performance to mathematical accuracy to application to real world scenarios. Further, for each proposed model, the reviewers looked for evidence that the authors made comparisons between their own model and the base model as they pertained to claims made by the authors of why their model is needed. The quantifiable evaluations looked for were:

- Time-based Performance
- Complexity analysis
- Comparison to standard RBAC
- Mathematical accuracy
- Example scenarios of the model in action
- Experimental analysis of the model
- Case study of the model in practice

Based on the diverse evaluation criteria, 12 models presented no evidence of an evaluation. 8 models presented example scenarios and how application of their model would apply and resolve the situation. 6 of the models provided some form of performance or complexity analysis of their model. This included graphs of the model's time to determine authorization as the number of entities grew, and the size of the role space for the extension model compared to standard RBAC. 4 models provided mathematical descriptions and analsysis as a way to provide evaluation in the form of completeness.

The most widely used evaluation method was providing sample scenarios with accompanying workflows of how the extension model would tackle those scenarios. Much is left to the reader to assume of these types of evaluations, as the authors do not explicitly state or show how the standard model is deficient in tackling said scenarios.

6.5. Research Question 5

What domains or scenarios serve as inspiration for these extensions?

Business needs have historically driven RBAC research and development. The primary mode of evaluation for model extensions has been the presentation of business scenarios in various domains and how the model uniquely handles those particular scenarios. Thus, looking for trends in the domains used in the example scenarios might serve to illuminate a trend worth further examination into the reason for the explosion of RBAC extensions.

Upon examination of the primary sources, the most prevalent domains were:

- What domains or scenarios serve as inspiration for these extensions?
- Medical domain
- Pervasive computing environments
- Mobile devices
- Large-scale organizations with many sub-departments
- Enterprise, organization workflows

6.6. Research Question 6

What commonalities or generalizations exist across all categorizations?

7. Conclusion

P1: Mention core RBAC, note specific results for each research question
P2: Mention bigger results that cut across and any other peritentn information

References

[1] D. Ferraiolo, D. Kuhn, Role based access control, in: 15th National Computer Security Conference, Oct 13-16, 1992, pp. 554–563.

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

[3] B. Kitchenham, S. Charters, Guidelines for performing systematic literature reviews in software engineering.

[4] M. Alam, M. Hafner, R. Breu, A constraint based role based access control in the sectet a model-driven approach, in: Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services, PST '06, 2006, pp. 13:1–13:13.

[5] S. K. Tzelepi, D. K. Koukopoulos, G. Pangalos, A flexible content and context-based access control model for multimedia medical image database systems, in: Proceedings of the 2001 workshop on Multimedia and security: new challenges, Sec '01, 2001, pp. 52–55.

[6] S. Haibo, H. Fan, A context-aware role-based access control model for web services, in: Proceedings of the IEEE International Conference on e-Business Engineering, ICEBE '05, 2005, pp. 220–223.

[7] D. G. Cholewka, R. A. Botha, J. H. P. Eloff, A context-sensitive access control model and prototype implementation, in: In: Information Security for Global Information Infrastructures: IFIP TC 11 Sixteenth Annual Working Conference on Information Security, Kluwer Academic Publishers, 2000, pp. 341–350.

[8] X. Huang, H. Wang, Z. Chen, J. Lin, A context, rule and role-based access control model in enterprise pervasive computing environment, in: Pervasive Computing and Applications, 2006 1st International Symposium on, 2006, pp. 497 –502.

[9] G. Motta, S. Furuie, A contextual role-based access control authorization model for electronic patient record, Information Technology in Biomedicine, IEEE Transactions on 7 (3) (2003) 202 –207.

[10] Y. Bao, J. Song, D. Wang, D. Shen, G. Yu, A role and context based access control model with uml, in: Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for, 2008, pp. 1175 –1180.

[11] H. Jian-min, L. Xi-yu, Y. Hui-qun, T. Jun, An extended RBAC model based on granular logic, in: Granular Computing, 2008. GrC 2008. IEEE International Conference on, 2008, pp. 261 –264.

[12] N. Thein, et al., Leveraging access control mechanism of android smartphone using context-related role-based access control model, in: Networked Computing and Advanced Information Management (NCM), 2011 7th International Conference on, IEEE, 2011, pp. 54–61.

[13] D. Zou, L. He, H. Jin, X. Chen, Crbac: Imposing multi-grained constraints on the rbac model in the multi-application environment, Journal of Network and Computer Applications 32 (2) (2009) 402–411.

[14] K. Hasebe, M. Mabuchi, A. Matsushita, Capability-based delegation model in RBAC, in: Proceedings of the 15th ACM symposium on Access control models and technologies, SACMAT '10, 2010, pp. 109–118.

[15] Z. Zhang, X. Zhang, R. Sandhu, Robac: Scalable role and organization based access control models, in: Collaborative Computing: Networking, Applications and Worksharing, 2006. CollaborateCom 2006. International Conference on, 2006, pp. 1 –9.

[16] Q. Ni, E. Bertino, J. Lobo, C. Brodie, C. Karat, J. Karat, A. Trombeta, Privacy-aware role-based access control, ACM Transactions on Information and System Security (TISSEC) 13 (3) (2010) 24.

[17] A. Masoumzadeh, J. Joshi, Purbac: Purpose-aware role-based access control, On the Move to Meaningful Internet Systems: OTM 2008 (2008) 1104–1121.

[18] Y. Zhao, Y. Zhao, H. Lu, A flexible role-and resource-based access control model, in: Computing, Communication, Control, and Management, 2008. CCCM'08. ISECS International Colloquium on, Vol. 2, IEEE, 2008, pp. 75–79.

[19] I. Ray, M. Toahchoodee, A spatio-temporal role-based access control model, in: Proceedings of the 21st annual IFIP WG 11.3 working conference on Data and applications security, 2007, pp. 211–226.

[20] F. Hansen, V. Oleshchuk, Spatial role-based access control model for wireless networks, in: Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th, Vol. 3, IEEE, 2003, pp. 2093–2097.

[21] S. Aich, S. Sural, A. K. Majumdar, Starbac: spatiotemporal role based access control, in: Proceedings of the 2007 OTM confederated international conference on On the move to meaningful internet systems: CoopIS, DOA, ODBASE, GADA, and IS - Volume Part II, OTM'07, 2007, pp. 1567–1582.

[22] L. Chen, J. Crampton, On spatio-temporal constraints and inheritance in role-based access control, in: ASIACCS: ACM Symposium on InformAtion, Computer and Communications Security, 2008, pp. 205–216.

[23] E. B. Arjmand Samuel, Arif Ghafoor, A framework for specification and verification of generalized spatio-temporal role based access control model, Tech. Rep. CERIAS Tech Report 2007-08.

[24] S. M. Chandran, J. B. D. Joshi, Lot-rbac: a location and time-based RBAC model, in: Proceedings of the 6th international conference on Web Information Systems Engineering, WISE'05, 2005, pp. 361–375.

[25] S. Aich, S. Mondal, S. Sural, A. K. Majumdar, Transactions on computational science iv, 2009, Ch. Role Based Access Control with Spatiotemporal Context for Mobile Applications, pp. 177–199.

[26] L. Yao, X. Kong, Z. Xu, A task-role based access control model with multi-constraints, in: Networked Computing and Advanced Information Management, 2008. NCM'08. Fourth International Conference on, Vol. 1, IEEE, 2008, pp. 137–143.

[27] W. Zhou, C. Meinel, Team and task based rbac access control model, in: Network Operations and Management Symposium, 2007. LANOMS 2007. Latin American, IEEE, 2007, pp. 84–94.
[28] S. Oh, S. Park, Task–role-based access control model, Information Systems 28 (6) (2003) 533–562.
[29] J. Joshi, E. Bertino, U. Latif, A. Ghafoor, A generalized temporal role-based access control model, Knowledge and Data Engineering, IEEE Transactions on 17 (1) (2005) 4 – 23.

8. Outline

1. Introduction
   - RBAC history, RBAC as a standard
   - Audience that should care about our review
   - Brief explanation of what has led to extensions cropping up
   - Paper organization
2. Background
   - What is RBAC
   - Core RBAC and it's entities, and what it tries to solve
3. Process
4. Results
   - Data used in process, results of process for paper count
   - Categorization that came out applying process (based on word usage)
   - Results for each research question (raw data)
5. Analysis
   - Explanation and definitions of categories based on results
   - Examination of results in relation to each research question and larger trends drawn from data
   - Examination of cross research question concerns an
6. Conclusion