A Systematic Literature Review on Extensions to Role Based Access Control

Eric D. Helms, JeeHyun Hwang, Tao Xie, Laurie Williams

North Carolina State University

Department of Computer Science

890 Oval Drive, Box 8206

Raleigh, NC 27695-2858

Abstract

Context: 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 applications 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 heirarchy relationships.

Aim: *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.*

Method: 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.

Results:

Conclusions: 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 Institute 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 practitioners 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 quantifiable results across a body of research in order to draw out similarities, trends and deficiencies 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 authors adopted and applied a systematic literature review 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:

- Step 1: Development of a search strategy
- Step 2: Elimination of papers based on title criteria
- Step 3: Elimination of papers based on abstract criteria
- Step 4: Elimination of papers based on content and matching to elimination criteria

3.1. Step 1: Search Strategy

For the first phase of our systematic literature review, the authors developed a search strategy for finding papers. The search strategy was executed by an automated comprehensive search taking as input a set of academic search engines and a list of search terms. The search was performed by applying each search term to each engine incrementally until a stopping criteria was met. Table 1 lists the four search engines along the left most column with the three search term across the top row along with the papers for each criteria and engine combination. The search algorithm was performed as follows:

1. Call to search engine with current search position and current search term.
2. Parse results and extract paper title, authors and year of publication.
3. Compare results against stopping criteria:
   - If the size of the result set is greater than or equal to 1000 then stop.
   - If the last ten results did not contain the search term phrase within the tite then stop.
4. If stopping criteria not met, increment search position and go back to step one.

The result set size stopping criteria was chosen due to a technical limitation of some search engines. The stopping criteria related to the last ten titles is meant to stop after relevant results are no longer being returned by the search engine. After gathering all 12 data sets, the authors combined the papers into a master list by systematically comparing the bibliographic information for each. The master list of 1716 papers was used to perform a series of elimination rounds to narrow the list of papers and identify primary sources.

TODO: Add elimination stats.

	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

3.2. Steps 2-4: 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.

- The two first authors 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.

3.2.1. Step 2: 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. Step 3: 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. Step 4: 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:

1. Does this model extend the core model? (Exclusion)
2. Do the researchers give evidence that RBAC needs extension? (Inclusion)
3. Was the paper and subsequent model inspired by a real world example? (Conditional Inclusion)
4. Did the researchers offer any evaluation of the proposed model? If yes, how did they do one? If no, why? (Conditional Inclusion)
5. Did the authors implement their model? (Inclusion)

Question 1 was a definitive exclusion criteria as any paper that failed in the affirmative was rejected. Questions 3 and 4 were marked as conditional includes given that they were connected in making a decision. A paper that met Question 3 but not 4, or met 4 but not 3 would be included since in some cases the real world examples served as research evaluations and without this conditional include the paper list size would be too small to be significant.

4. Analysis

4.1. Research Question 1

What categorizations exist within RBAC extensions?

- Constraint:
- Context:
- Organizational:
- Privacy:
- Resource:
- Spatial: 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.
- Spatio-Temporal:

- Task: A task is a fundamental unit of a business activity. Different from core RBAC, in task-role-based access control model, roles are not directly associated with permissions. Roles are first associated with tasks, which are associated permissions. For example, the employee role is associated with a task, which is to write a report. Then, this task is associated with a permission.
- Temporal: 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.

4.2. Research Question 2

What are the motivations behind RBAC extensions?

Core RBAC model provides an abstraction of authorization model based on user role assignment (UA) and the role permission assignment (PA). Since this simple model may not provide a fine-grained access control for sophisticated security mechanism, a variety of extended RBAC models have been proposed over the years to meet security requirements. When administrators design a model, it is important to capture an important abstraction to help the model to be enforced in a system.

- Core RBAC model needs additional contextual information and constraints to develop fine-grained policies in practice.
- Core RBAC does not incorporate context. Therefore, RBAC belongs to static access control model, which may not capture changes in environments.
- Core RBAC does not support for various constraints such as temporal and spatial constraints to design sophisticated policies on demand.
- Core RBAC does not provide an abstraction to additional user-defined attributes (e.g., task and team) and their association with existing attributes.
- Core RBAC has limitation on delegation and role hierarchy. For example, partial inheritance in role hierarchy needs to be developed.
- Model needs to incorporate additional contextual information and constraints to develop fine-grained policies in practice.
- Model needs to incorporate additional attributes such as task, team, purpose, organizational roles and collaborative activities over existing attributes. Moreover, new association between attributes are introduced.
- Model needs to improve existing features such delegation and role hierarchy to meet fine-grained access control.

4.3. Research Question 3

Do the extension models have corresponding implementations?

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 implementations 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 remaining 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.

4.4. Research Question 4

How are extension to RBAC evaluated theoritically 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 [4], [5]
- Complexity analysis [6], [7], [8], [5]
- Comparison to standard RBAC [6], [9], [7], [10], [11]
- Mathematical modeling [**?**], [12], [13], [8], [14]
- Example scenarios of the model in action [15], [16], [17], [18], [6], [19], [**?**], [9], [11], [20], [11], [14], [21], [22], [23]
- Experimental analysis of the model
- Case study of the model in practice [24]

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 analysis 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.

TODO: Add references to list above.

4.5. Research Question 5

What domains have RBAC extensions been created for?

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

4.6. Research Question 6

What commonalities or generalizations exist across all categorizations?

5. 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] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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, IEEE, 2008, pp. 261–264.

[20] 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.

[21] 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.

[22] 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.

[23] S. Oh, S. Park, Task–role-based access control model, Information Systems 28 (6) (2003) 533–562.

[24] 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.

[25] 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.

[26] 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.

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

[28] 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.

6. 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

7. Appendix

Paper	**Category**
A constraint based role based access control in the SECTET a model-driven approach, 2006 [15]	Constraint
A flexible content and context-based access control model for multimedia medical image database systems, 2001 [16]	Context
A context-sensitive access control model and prototype implementation, 2000 [17]	Context
A Context, Rule and Role-Based Access Control Model In Enterprise Pervasive Computing Environment, 2006 [18]	Context
A contextual role-based access control authorization model for electronic patient record Motta, 2003 [24]	Context
A Role and Context Based Access Control Model with UML, 2008 [6]	Context
An extended RBAC model based on granular logic, 2008 [19]	Context
Designing an agent-based RBAC system for dynamic security policy, 2004 [**?**]	Context
An extended RBAC model based on granular logic, 2008 [25]	Context
Leveraging Access Control Mechanism of Android Smartphone Using Context-Related Role-Based Access Control Model, 2011 [26]	Context
CRBAC: Imposing multi-grained constraints on the RBAC model in the multi-application environment, 2009 [9]	Context
ROBAC: Scalable Role and Organization Based Access Control Models, 2006 [7]	Organizational
Privacy-aware role-based access control, 2007 [4]	Privacy
PuRBAC: Purpose-Aware Role-Based Access Control, 2008 [27]	Privacy
A Flexible Role- and Resource-Based Access Control Model, 2008 [10]	Resource
GEO-RBAC: a spatially aware RBAC, 2005 [**?**]	Spatial
LRBAC: A location-aware role-based access control model, 2006 [11]	Spatial
Spatial role-based access control model for wireless networks, 2003 [12]	Spatial
STARBAC: Spatiotemporal role based access control, 2007 [13]	Spatio-Temporal
On spatio-temporal constraints and inheritance in role-based access control, 2008 [8]	Spatio-Temporal
A framework for specification and verification of generalized spatio-temporal role based access control model, 2007 [20]	Spatio-Temporal
LoT-RBAC: A Location and Time-Based RBAC Model, 2005 [28]	Spatio-Temporal
A Spatio-temporal Role-Based Access Control Model, 2007 [11]	Spatio-Temporal
Role Based Access Control with Spatiotemporal Context for Mobile Applications, 2009 [5]	Spatio-Temporal
A Task-Role Based Access Control Model with Multi-Constraints, 2008 [21]	Task
Team and Task Based RBAC Access Control Model, 2009 [22]	Task
Task-role-based access control model, 2003 [23]	Task
A generalized temporal role-based access control model, 2005 [14]	Temporal

Table 2: Primary sources grouped by categorization