RBAC-SLR Documentation

Release 0.1

Eric D. Helms

February 02, 2013

CONTENTS

Contents:

CHAPTER

ONE

1. INTRODUCTION

Why is the base model of RBAC extended by newer models?

Role-based access control (RBAC) models [1] become popularly used to govern access to critical resources. 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.

RBAC is first introduced in 1990s, NIST proposed standard RBAC model [1] Standard RBAC model considers only role-user association and role hierarchy. Since standard RBAC model has limitations such as specifying environmental constraints or context information Researchers developed extended models of RBAC to overcome the limitations. However, as researchers often develop their own specialized extended models of RBAC, their research cannot be generalized or compared with other research work appropriately. As a result, researchers could take time on reinventing the wheel. But how do we, as a community, ensure that a metric is suitable and acceptable for its intended purpose?

The goal of this work is to synthesize available research results on extended models of RBAC. We analyze their extended features and claimed research contributions to find limitations of current RBAC models and what extent of extended features by comparing with similar research work. We conducted a systematic literature review (SLR) to evaluate and interpret all available research relevant to a particular research question or topic area of interest.

Our research give benefits to a community as follows:

- Our work summarizes current extended RBAC research work and its contributions. By synthesizing the current results, our work shows a roadmap of current extended RBAC research.
- Our work 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.
- Our work helps identify the research challenges in the ares of security policies and suggest a future extension of RBAC.

CHAPTER

TWO

2. METHODOLOGY AND PROCESS

For the first phase of our systematic literature review, an automated comprehensive search of multiple academic search engines was performed. The list of search engines were:

- Google Scholar - http://scholar.google.com
- IEEExplore - http://ieeexplore.ieee.org
- ACM Portal - http://dl.acm.org
- CiteSeerX - http://http://citeseerx.ist.psu.edu/index

For each of the criteria below, a search was performed on each of the search engines for a total of 12 data sets. The criteria used were:

- role based access control
- RBAC
- role-based access control

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. Each run 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 assessment rounds were performed to narrow the paper list and identify primary sources.

There were a total of three elimination rounds. The first round was based solely on title, the second on reading of the abstract and the last round was based on a full read of the paper and comparison to the research questions outlined. Each round was performed as follows:

- Each reviewer independently classified papers as relevant, irrelevant or uncertain.
- 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.

The results of the searches is summarised below:

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**

2.1 Research Questions

Based on our intial intent for the systematic literature review, and notes taken during the third phase of elimination, we have identified the following research questions:

- RQ1. What are the deficiencies in current RBAC model to propose extended RBAC models?
- RQ2. What are the motivations behind RBAC extensions?
- RQ3. What are the categorizations of RBAC model proposed?
- RQ4. For each categorization, what are the extended features of RBAC model proposed?
- RQ5. Do these models have corresponding implementations in practice?
- RQ6. How are extended RBAC models evaluated in theory and in practice?
- RQ7. Are there any commonalties or generalizations across all categorizations?
- RQ8. What domains or scenarios serve as inspiration for these extensions?

CHAPTER

THREE

RQ1: WHAT ARE THE DEFICIENCIES IN CURRENT RBAC MODEL?

3.1 Common Themes

-

3.2 By Category

Constraint

- no support for partial inheritance
- inability to support permission assignment constraints

Context

- Missing ability to apply constraints between role and permissions and enforce
- Missing context that defines if a role can be activated at execution time
- Role activation on a per object or process execution rather than session based
- No allowance for context to check permission at execution moment based on context
- activation of roles based on current context rather than session intiation
- conflict resolution
- RBAC cannot handle dynamic authorization and entities
- Role cannot be resource dependent
- RBAC is too simple
- Missing granularity
- Inability to handle dynamic nature of multiple projects with multiple resources
- Too simple
- Lacks context
- Handling authorization between applications and within can be different

Organizational

- RBAC cannot handle cross-organizational roles and access in an administratively easy way

Privacy

- Privacy regulations are complex, with many entities, RBAC lacks ability to handle all of these
- Context, conflict detection and resolution
- RBAC lacks ability to define purpose

Resource

- No support for multiple security domains
- No support for same security, different applications
- Lack of flexibility

Spatial

- Lack of contextual information
- Role needs a defined schema
- Role activation based on context
- Giving a permission an operation

Spatio/Temporal

-

Task

- Needs an entity to represent a task and connect a role and a permission through it
- Need for team and tasks
- Need for entity between permission and roles to hold constraint and allow for dynamic situations and entities

Temporal

- RBAC can't handle time based constraints for role enablement

CHAPTER

FOUR

RQ2: WHAT ARE THE MOTIVATIONS BEHIND RBAC EXTENSIONS?

4.1 Common Themes

- Roles, users and permissions need context associations
- Location and time constraints as well as contexts needed
- RBAC lacks ability to link in objects
- RBAC does not handle single user base and multiple organizations/applications
- Role enablement based on context
- User granting/revoking of roles based on context

4.2 By Category

Constraint

- No support for partial inheritance
- Permission assignment constraints

Context

- Relationship between object and viewer can’t be represented
- Object content matters
- Location and time constraints on the user
- Departmental context around access
- RBAC does not handle many small services to wrap around them
- RBAC lacks security principle enforcement
- Lack of specifying context, and permission checks of dynamic evaluation time rules
- RBAC is static and lacks ability to handle dynamic authorization and definitions
- RBAC ignores context
- Role granulatiry not well controlled

- Roles should depend on the resources
- RBAC cannot handle multiple projects with multiple tasks and differing roles in each system but the same user
- Lack of context support
- Too simple for dynamic environments

Delegation

- Support cross-domain delegation

Organizational

- Reduce administrative complexity of RBAC for multi-organizational

Privacy

- Lack of components, purpose binding, conditions, obligations to handle privacy needs

Resource

- Need to support multiple securtiy domains
- Need to support same security with different applications
- Role heirarchy adds complexity and reduces flexibility

Spatial

- Lack of contextual information with roles, users and permissions
- Role needs a schema to allow specification of attributes
- Location based security scenarios
- Role activation based on location
- Support physical and logical locations
- Attaching operations to permissions

Spatio/Temporal

- RBAC doesn't inherently support location and time constraints
- Spatial and temporal awareness of roles, inheritance and permissions
- Context mechanisms needed
- Physical and logical locations, hybrids
- Role assignment based off time and space, as well as permissions
-

Task

- RBAC can't handle large enterprises with multiple applications and single user base
- Security requirements for enterprises (look up these)

Temporal

- Workflow based organizations need time base constraint for role enablement

CHAPTER

FIVE

RQ3: WHAT ARE THE CATEGORIZATIONS OF PROPOSED RBAC EXTENSIONS?

Across the papers found, a number of higher level categories emerged that each proposed model fell in to. Some of these categories had singular primary papers, while others had multiple extension models proposed that were deemed independent of one another.

For each category, the breakdown of the papers for each category is:

Paper	Category
Alam, M. and Hafner, M. and Breu, R. 2006	Constraint
Tzelepi, Sofia K. and Koukopoulos, Dimitrios K. and Pangalos, George 2001	Context
Haibo, SHEN and Fan, HONG 2005	Context
Damian G. Cholewka and Reinhardt A. Botha and Jan H. P. Eloff 2000	Context
Huang, X. and Wang, H. and Chen, Z. and Lin, J. 2006	Context
Motta, G.H.M.B. and Furuie, S.S. 2003	Context
Bao, Y. and Song, J. and Wang, D. and Shen, D. and Yu, G. 2008	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	Context
Thein, N. and others 2011	Context
Zou, D. and He, L. and Jin, H. and Chen, X. 2009	Context
Hasebe, K. and Mabuchi, M. and Matsushita, A. 2010	Delegation
Zhang, Z. and Zhang, X. and Sandhu, R. 2006	Organizational
Ni, Q. and Trombetta, A. and Bertino, E. and Lobo, J. 2007	Privacy
Masoumzadeh, A. and Joshi, J. 2008	Privacy
Zhao, Y. and Zhao, Y. and Lu, H. 2008	Resource
Bertino, E. and Catania, B. and Damiani, M.L. and Perlasca, P. 2005	Spatial
Ray, I. and Kumar, M. and Yu, L. 2006	Spatial
Hansen, F. and Oleshchuk, V. 2003	Spatial
Aich, S. and Sural, S. and Majumdar, A. 2007	Spatio-Temporal
Chen, L. and Crampton, J. 2008	Spatio-Temporal
Samuel, A. and Ghafoor, A. and Bertino, E. 2007	Spatio-Temporal
Chandran, S. and Joshi, J. 2005	Spatio-Temporal
Ray, I. and Toahchoodee, M. 2007	Spatio-Temporal
Aich, S. and Mondal, S. and Sural, S. and Majumdar, A. 2009	Spatio-Temporal
Yao, L. and Kong, X. and Xu, Z. 2008	Task
ZHANG, S. and CHEN, X. and HOU, G. 2009	Task
Oh, S. and Park, S. 2003	Task
Joshi, J.B.D. and Bertino, E. and Latif, U. and Ghafoor, A. 2005	Temporal

5.1 By Category

Constraint (1) a limitation or restriction

Context (8) circumstances in which an event occurs

Delegation (1) the act of empowering to act for another

Organizational (1) of or relating to an organization

Privacy (1) freedom from unauthorized intrusion

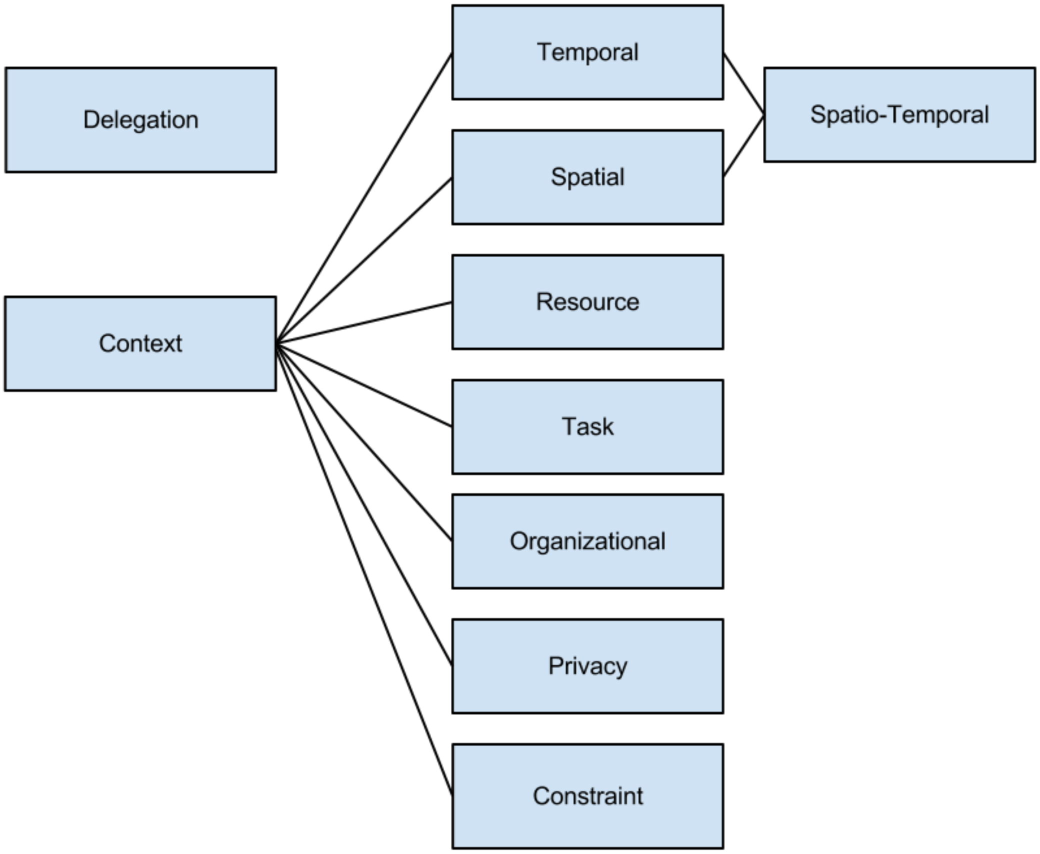
Resource (1) an available supply than be drawn on when needed

Spatial (3) of or relating to facility in percieving relations in space

Spatio/Temporal (6) combining space and time

Task (3) a usually assigned piece of work often to be finished within a certain time

Temporal (1) of or relating to the sequence of time or to a particular time


Delegation
Temporal
Spatio-Temporal
Spatial
Context
Resource
Task
Organizational
Privacy
Constraint

CHAPTER

SIX

RQ4: FOR EACH CATEGORIZATION, WHAT ARE THE EXTENDED FEATURES OF RBAC PROPOSED?

Is this the same as RQ_1 ?

6.1 Common Themes

-

6.2 By Category

Constraint

-

Context

-

Delegation

-

Organizational

-

Privacy

-

Resource

-

Spatial

-

Spatio/Temporal

-

Task

-

Temporal

-

CHAPTER

SEVEN

RQ5. DO THESE 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.

7.1 Common Themes

- 21 No's
- 8 Yes's
- Half the implementation's were prototypes

7.2 By Category

Constraint

- No

Context

- No - system architecture provided
- No
- Yes - prototype with VB6 and MS Access97
- Yes - prototype system, system architecture, algorithms implemented, simulation scenarios
- Yes - on an EHR system
- Yes - prototype using XML container
- Yes - web based API agent
- No

- No
- No

Delegation

- No

Organizational

- No

Privacy

- No
- No

Resource

- No

Spatial

- No
- No
- No

Spatio/Temporal

- No
- No
- No
- No
- No
- Yes - integrated with telemedicine application, web based

Task

- Yes - mentions of systems that exist using the model
- Yes - prototype system
- No

Temporal

- No

CHAPTER

EIGHT

RQ6. HOW ARE EXTENDED RBAC MODELS EVALUATED IN THEORY AND IN PRACTICE?

8.1 Common Themes

- 12 had no evaluation whatsoever
- 8 present example scenarios and how their model would apply
- 6 presented performance and time complexity analysis

8.2 By Category

Constraint

- No evaluation

Context

- Present hospital scenarios and explanation of how new model would handle
- No
- No
- No
- No
- Scenarios with how model affects, performance test of the model vs. traditional RBAC
- Description of a fake project management system that the model is designed for
- Applied to conceptual situation
- No
- Example scenario comparing their model vs other models

Delegation

- No

Organizational

- Comparison caluclation for number of roles vs standard model, numerical size comparisons against other proposed models

Privacy

- Evaluate the performance of permission assignment and authorization checks for various sizes and context variables
- No

Resource

- Model comparison from a qualitative standpoint

Spatial

- Algorithm and Big-O performance evaluation
- No except minor scenarios and how the model handles
- No other than mathematical specification

Spatio/Temporal

- Mathematical description
- Mathematical analysis of role graph, complexity comparisons across different models
- Pseudo example scenario
- No
- Detailed scenario with examination of how model handles situation
- Discuess difference btween their model and other models, time-complexity analysis to show no performance impact with standard model

Task

- No
- No
- No

Temporal

- Mathematical modeling and graphs to detail usage and interactions, explanation of example scenarios

CHAPTER

NINE

RQ7. ARE THERE ANY COMMONALTIES OR GENERALIZATIONS ACROSS ALL CATEGORIZATIONS?

9.1 Common Themes

-

9.2 By Category

Constraint

-

Context

-

Delegation

-

Organizational

-

Privacy

-

Resource

-

Spatial

-

Spatio/Temporal

-

Task

-

Temporal

-

CHAPTER

TEN

RQ8. WHAT DOMAINS OR SCENARIOS SERVE AS INSPIRATION FOR THESE EXTENSIONS?

10.1 Common Themes

- Medical domain
- Pervasive computing environments
- Mobile devices
- Large-scale organizations with many sub-departments
- Enterprise, organization workflows

10.2 By Category

Constraint

- Medical domain
- Service Oriented Architecture

Context

- Medical imaging database
- Handling an insurance claim workflow
- Pervasive computing environments
- Medical emergency overrides
- Electronic health records
- Supermarket
- Project management system with large project, task and user base
- Power load forecasting system (multi-level user environment)

Delegation

- Large-scale electronic health record systems

Organizational

- Online tutoring system
- State education system with schools, districts, etc.

Privacy

- Privacy within the medical domain, HIPAA

Resource

- N/A

Spatial

- Hospital with multi-floors, departments

Spatio/Temporal

- Pervasive computing environments
- Hospital using mobile devices with multiple user types on a single floor, departments
- Mobile, peer-to-peer
- Doctor out in the world needing access during a random medical emergency
- Students at a university

Task

- Large enterprises with multiple applications and a single user base
- Hospital needs
- Complex enterprise environments

Temporal

- General organizational needs for time constraints

CHAPTER

ELEVEN

CONSTRAINT

Definition a limitation or restriction

Papers

- A constraint based role based access control in the SECTET a model-driven approach

---

A constraint based role based access control in the SECTET a model-driven approach

Inspired by a real example? SECTECT is a framework that provides workflow for Service oriented Architectures and is the primary target.

Scenarios or examples. Presented generic scenarios from the medical domain as examples to describe how mechanisms worked.

What reasons and evidence do researchers claim RBAC needs extension?

- The claim is that with respect to Service Oriented Architecture, and the execution of web services, RBAC lacks needed features.
- RBAC does not support partial inheritance
- "total inheritance of permissions in RBAC is against the principle of least privilege"
- ability for some sub-role permissions not be available to super role
- "permission assignment constraints"

Did they implement the model? No evidence of use in a real system.

Is there an evaluation? If yes, how did they do one? If not, why? No.

Does this model extend the core model?

- Presents a modification to a core aspect of RBAC
- Allow partial inheritance at the permission level by a superrole instead of treating the role as an atomic entity

Notes. Apply a restricted status to a permission which prevents a superrole from inheriting that permission

CHAPTER

TWELVE

CONTEXT

Definition. circumstances in which an event occurs

Papers

- A flexible content and context-based access control model for multimedia medical image database systems
- A Context-Aware Role-Based Access Control Model for Web Services
- A context-sensitive access control model and prototype implementation
- A Context, Rule and Role-Based Access Control Model In Enterprise Pervasive Computing Environment
- A contextual role-based access control authorization model for electronic patient record
- A Role and Context Based Access Control Model with UML
- Designing an agent-based RBAC system for dynamic security policy
- An extended RBAC model based on granular logic
- Leveraging Access Control Mechanism of Android Smartphone Using Context-Related Role-Based Access Control Model
- CRBAC: Imposing multi-grained constraints on the RBAC model in the multi-application environment

---

A flexible content and context-based access control model for multimedia medical image database systems

Inspired by a real example? Scenarios or examples. Real world inspiration based upon medical image database. One simple scenario shown where the model is applicable.

What reasons and evidence do researchers claim RBAC needs extension?

- What the image is of is important to who can view
- Domain governs who can see a particular image (e.g. departments in a hospital)
- Location for determining if user is accessing from secure location or location of importance (e.g. emergency room)
- Time constraints for validity periods
- Relationship between images and viewer

Did they implement the model? Provided system architecture for entire medical imaging database with access control system. No implied implementation of model.

Is there an evaluation? If yes, how did they do one? If no, why? No evaluation. Present proposed situation and hospital structure with scenario where new model would be applicable. No reason for lack of evaluation given.

Does this model extend the core model?

- Proposes adding of constraints between the Role-Permission relationship which must be satisfied in order for the holder of said role to be able to use those permissions

This appears to be an active mechanism during enforcement not assignment

- Adds user attributes (e.g. company position, location, user name)
- Adds a decision rule to role-permission relationship
- Role-perm relationship contains 5 attributes: identifier, subject/role, action, target objects, constraints

Notes.

A Context-Aware Role-Based Access Control Model for Web Services

Inspired by a real example? Scenarios or examples. No.

What reasons and evidence do researchers claim RBAC needs extension?

- claim is that RBAC can not handle many small services that need roles/perms wrapped around them

Did they implement the model? No.

Is there an evaluation? If yes, how did they do one? If no, why? No.

Does this model extend the core model?

- services replace objects/actions
- adds contexts that must be satisfied
- splits roles into local and global, where local is reflective of actions within a service/domain and global roles are reflective of the permissions to access the service
- roles are activated based on context at execution time

Notes.

- context oriented, provides what appears to be a different spin or implementation of heirarchies

---

Context-sensitive access control model and prototype implementation

Inspired by a real example? Scenarios or examples. Initiates the paper with case scenario “handle an insurance claim” workflow.

What reasons and evidence do researchers claim RBAC needs extension?

- points out contrasts between base RBAC and improvements clearly
- claims that RBAC supports security principles but does not enforce the use of

Did they implement the model? Prototype created using VB6 and MS Access97.

Is there an evaluation? If yes, how did they do one? If no, why? No.

Does this model extend the core model?

- largely using mechanisms prescribed by RBAC specifically SoD and LP see note about how RBAC provides for but not the use of the previous security practices

- roles are activated whenever a tasks is chosen to be performed and checked if the user can have said role
- provides more implementation of SoD and LP than additions to model

Notes.

- context oriented, provides what appears to be a different spin or implementation of heirarchies

---

A Context, Rule and Role-Based Access Control Model In Enterprise Pervasive Computing Environment

Inspired by a real example? Scenarios or examples.

- Inspired by the needs of access control in pervasive computing environments

What reasons and evidence do researchers claim RBAC needs extension?

- "static method of management user-role-permissions"

Did they implement the model?

- Created prototype system to verify model correctness and system architecture
- Implemented the algorithms proposed by their model
- Simulated scenarios but the details of the simulations are not in the paper, nor are the results in a consumable manner

Is there an evaluation? If yes, how did they do one? If no, why? No.

Does this model extend the core model?

- Claim to be an extension and follow the standard RBAC execution model except by adding two different checks where permissions are re-evaluated by the context of the current user according to the already specific rules
- context aware rules that dynamically determine permissions
- constraining the permissions based on a users location
- assignment/removal of a role based on context information
- connection of roles, granting a user certain role permissions when another user/role is present
- Provide mechanism to deal with conflicts

Notes.

A contextual role-based access control authorization model for electronic patient record

Inspired by a real example? Scenarios or examples.

- Traditional RBAC does not support emergency overrides based on the situation
- Inspired by the needs of an EHR application in practice

What reasons and evidence do researchers claim RBAC needs extension? Claim RBAC is static and cannot handle the dynamic authorization and definitions needed by EHR application complexity

Did they implement the model?

- Implemented using Java and LDAP on InCor EHR system
- They quote number of users and rules, but provide no evidence of comparison or any observation data of the system in use

Is there an evaluation? If yes, how did they do one? If no, why? Showed some discussion evidence for the requirement for these extensions to RBAC, and they implemented it, however, they provided little evidence as to the effectiveness

Does this model extend the core model?

- Claim to be a context based extension
- Focused on the authorization aspect of permissions for a given role
- Contains both positive and negative permission authorizations
- Provides for overriding of authorizations based on inheritance

Notes.

A Role and Context Based Access Control Model with UML

Inspired by a real example? Scenarios or examples.

- Describes a scenario whereby a supermarket could not effectively use RBAC to encapsulate all the various access scenarios they need
- Propose a model that adds attributes and system context

What reasons and evidence do researchers claim RBAC needs extension?

- RBAC ignores context
- RBAC is too simple and unilateral and does not align with real world
- Role granularity is not well controlled
- Roles should depend on the resources not vice-versa
- Roles should e assigned to one resource instead of resources being assigned to one role

Did they implement the model?

- Prototype system created using XML container to contain roles and conditionals

Is there an evaluation? If yes, how did they do one? If no, why?

- No evidence as to the comparison of the model in terms of the need over traditional RBAC other than conjecture around a scenario
- The performance test is really only valid for their implementation and shows no grounded re-worldness
- performed a performance analysis of traditional RBAC and C-RBAC based off their prototype

Does this model extend the core model? Extension of the traditional model adding context and maps roles to context and contex to resources with authorization and verification mixed in

Notes.

Designing an agent-based RBAC system for dynamic security policy

Inspired by a real example? Scenarios or examples.

- users and application sbecoming larger
- many applications have dynamic attributes and defining scenarios for all of them is difficult

What reasons and evidence do researchers claim RBAC needs extension?

- For their project manage system, traditional RBAC cannot handle the dynamic nature of multiple projects with multiple tasks that different users may be managing in one and not in another

Did they implement the model? Talks about some weird web based API for the agent

Is there an evaluation? If yes, how did they do one? If no, why? Discuss a fake project management system claiming this type of system is the target for this type of access control

Does this model extend the core model? Defines model clearly Extension that defines an Abstract Role, Context Rules and Context Information and the actual role is decided upon based off the context inputs and the rules

Notes.

An extended RBAC model based on granular logic

Inspired by a real example? Scenarios or examples. Inspired by a muli-level user environment with a complicated authorization management - power load forecasting system

What reasons and evidence do researchers claim RBAC needs extension?

- traditional RBAC does not provide context
- RBAC is too simple for large dyanmic environments

Did they implement the model? No.

Is there an evaluation? If yes, how did they do one? If no, why? No evidence, applied in theory to a conceptual situation, no comparison

Does this model extend the core model? Additions to specification, and rules around whether a user is authorized to perform an action based on their role and the context within the role

Notes.

Leveraging Access Control Mechanism of Android Smartphone Using Context-Related Role-Based Access Control Model

Inspired by a real example? Scenarios or examples.

- Access control needs of smart phones
- Installation of third party applications that a user needs to trust
- User must grant device privileges to the application
- Parents want to limit the amount of time kids use phone
- User might can to limit accessbility to friends and admins
- Companies want to limit data access by employee phones
- User loses company phone in admin mode, context to prevent leakage

What reasons and evidence do researchers claim RBAC needs extension?

- smartphone is centralized, user-centric system where identities are known in advance
- smartphone has lots of contextual info
-

Did they implement the model? No.

Is there an evaluation? If yes, how did they do one? If no, why? No.

Does this model extend the core model?

- Adds objects, environmental context, policies and decisions to model
- Object is an accessible entity
- a property of the system at the moment of interaction
- policy is the formal specification of the access control

Notes.

- precedential order of access privileges to prvent policy bugs

---

CRBAC: Imposing multi-grained constraints on the RBAC model in the multi-application environment

Inspired by a real example? Scenarios or examples.

- proliferation of distributed applications
- example of limited disk space when a database read and update are performed to resolve which operation to give preference to

What reasons and evidence do researchers claim RBAC needs extension?

- need flexible and dynamic authorization constraints
- authorization differs between and within applications
- Users may be granted access to the application and entities or may be granted access to objects with the application depending on context
- role and permission constraints are also possible

Did they implement the model? No.

Is there an evaluation? If yes, how did they do one? If no, why?

- analysis of example scenario, comparison of constraint vs other models,

Does this model extend the core model?

- adds object sets, entities, status and set of authorization attributes
- permissions on objects with constraints
- user and user constraints mapped to roles with permission attribute constraints

Notes.

- classification of constraints as either users eligibility to to use a resource/service or constraints on the users actual use of a resource (limiting what they can do)

CHAPTER

THIRTEEN

HISTORICAL

Definition. based on or reconstructed from an event, custom, style, etc., in the past

Papers

- HRBAC: Historical Role-Based Access Control

HRBAC: Historical Role-Based Access Control

Inspired by a real example? Scenarios or examples.

- a need to incorporate information of the past to make access control decisions
- for example, ensuring a user had a set of previous roles before being granted a higher responsibility role (e.g. “chief” role needs to have once had a manager role)

What reasons and evidence do researchers claim RBAC needs extension?

- in order to store and express historical entities of each base entity in order to apply constraints of current assignments and roles and permissions based off the past

Did they implement the model?

- No

Is there an evaluation? If yes, how did they do one? If no, why?

- No, only examples of mechanisms

Does this model extend the core model?

- Yes, extends each of the 4 levels of RBAC
- incorporates new entities to represent historical version of each core entity
- provides various historical constraints
- provides algorithms for performing constraint resolution
- highly defined model and entities

Notes.

CHAPTER

FOURTEEN

ORGANIZATIONAL

Definition. of or relating to an organization

Papers

- ROBAC: Scalable Role and Organization Based Access Control Models

---

ROBAC: Scalable Role and Organization Based Access Control Models

Inspired by a real example? Scenarios or examples.

- inspired by context from business-to-business and business-to-consumer context
- a theoritical web based report delivery system e.g. a set of educational professionals from schools, districts, and states
- also provide example of an online tutoring system

What reasons and evidence do researchers claim RBAC needs extension?

- claim that their model can significantly reduce administrative complexity for multi-organization
- more succint and intuitive than RBAC
- same expressive power

Did they implement the model?

Is there an evaluation? If yes, how did they do one? If no, why?

- present comparison calculations for the number of roles that must be generated between their model and standard
- provide numerical size comparisons with other proposed models (Role Templates, Team-based Access Control, Organizational Units

Does this model extend the core model?

- extension of RBAC to consider organization and role (a.k.a. context)
- an organization must own the object, and the role must give permission on the type for a user to access

Notes.

CHAPTER

FIFTEEN

PRIVACY

Definition. freedom from unauthorized intrusion

Papers

- Privacy-aware role-based access control
- PuRBAC: Purpose-Aware Role-Based Access Control

Privacy-aware role-based access control

Inspired by a real example? Scenarios or examples.

- inspired by conventional RBAC's inability to handle privacy
- extra attributes are needed to support the intricacies of privacy

What reasons and evidence do researchers claim RBAC needs extension? due to the lack of basic components required by privacy regulations, especially purpose binding (i.e., data collected for one purpose should not used for another purpose without user consent), conditions, and obligations. Despite its limitations, existing access control technology can be used as a starting point for managing personal identifiable information

Did they implement the model? No.

Is there an evaluation? If yes, how did they do one? If no, why? Evaluated the performance of assigning permissions and checking authorization for various permission size bases as well as variety in number of context variables

Does this model extend the core model?

- Defines additions to each level of the base RBAC model
- Adds objects, purposes, actions, obligations and conditions to core
- Includs context variables that can be very general, from space to time to other
- Conflict detection and resolution mechanisms

Notes.

PuRBAC: Purpose-Aware Role-Based Access Control

Inspired by a real example? Scenarios or examples.

- Web and companies with privacy policies make it harder to follow said policies and protect user data

What reasons and evidence do researchers claim RBAC needs extension?

- privacy policies include purposes under which collected data can be used
- current RBAC model does not include a entity or relationships to incorporate purpose
- authorization requests should include a purpose for performing the intended action

Did they implement the model?

- No.

Is there an evaluation? If yes, how did they do one? If no, why?

- No evaluation, conclusion includes note that further analysis needs to be done
- Discusses entities added by this model, the way they were added and why this method is the best way to add purpose and support privacy

Does this model extend the core model?

- extends the base and heirarchy portion of the model, adds in a hybrid heirarchy
- connects purposes to permissions

Notes.

- claim to reduce policy complexity by associating a purpose with only a permission and not with roles and users as well
- locks down the users ability to declare purpose, by putting authorization controls around the purposes

CHAPTER

SIXTEEN

RESOURCE

Definition. an available supply that can be drawn on when needed

Papers

- A Flexible Role- and Resource-Based Access Control Model

A Flexible Role- and Resource-Based Access Control Model

Inspired by a real example? Scenarios or examples. No.

What reasons and evidence do researchers claim RBAC needs extension?

- RBAC cannot support multiple security domains
- cannot support same security with different applications
- lack of flexibility in authorization
- discard role heirarchy for directory structure to reduce complexity and increase flexibility

Did they implement the model? No.

Is there an evaluation? If yes, how did they do one? If no, why? Comparison of the two models from a qualitative standpoint

Does this model extend the core model?

- Not an extension
- Re-imagining of the hierarchy aspect and adding a resources entity

Notes.

CHAPTER

SEVENTEEN

SPATIAL

Definition. of or relating to facility in perceiving relations in space

Papers

- GEO-RBAC: a spatially aware RBAC
- LRBAC: A location-aware role-based access control model
- Spatial role-based access control model for wireless networks

---

GEO-RBAC: a spatially aware RBAC

Inspired by a real example? Scenarios or examples. Hospital based examples of activating roles, allowing doctors to only see patient records while in the department of the patient Extended example section that discusses how a hospital setting with some typical actors would perform simple patient access

What reasons and evidence do researchers claim RBAC needs extension? Lack of contextual information with roles, users and permissions Role needs a schema which allows specification of more attributes of the role

Did they implement the model? No.

Is there an evaluation? If yes, how did they do one? If no, why? Shows that this model can be be represented by first-order logic and that they can be evaluated in PTIME ?

Does this model extend the core model?

- Introduces the concept of a spatial role
- Extends the base model at each of the 4 levels
- Specify mutual exclusion constraint for separation of duty
- Split model into a model without constraints and an extensive model with constraints

Notes.

LRBAC: A location-aware role-based access control model

Inspired by a real example? Scenarios or examples. Some brief real world concepts with regards to intricate security scenarios based on location of user or object

What reasons and evidence do researchers claim RBAC needs extension?

- Allowing for different security scenarios based on location

- Role activation based on location of object or user
- Add objects to define physical or logical with location data
- Attaches an operation to a permission

Did they implement the model? No.

Is there an evaluation? If yes, how did they do one? If no, why? Describes in full definition each object and it's role in the graph Describes a number of specific operations that would be performed and how the model handles them with respect to locations Description of how the core RBAC is related to each piece of their model No evaluation Minor scenarios

Does this model extend the core model?

- Extension adding operation, object and role enabling based on a constraint

Notes.

Spatial role-based access control model for wireless networks

Inspired by a real example? Scenarios or examples. Provide an application scenario of where this would be needed and used

What reasons and evidence do researchers claim RBAC needs extension?

- standard RBAC cannot handle location based constraints and attributes

Did they implement the model? No.

Is there an evaluation? If yes, how did they do one? If no, why? Mathematical specification of each aspect Definitions of each element in their model

Does this model extend the core model?

- extension at every level of RBAC
- includes separation of duty and heiarchry concerns specifically

Notes.

CHAPTER

EIGHTEEN

SPATIO-TEMPORAL

Definition. combining space and time

Papers

- STARBAC: Spatiotemporal role based access control
- On spatio-temporal constraints and inheritance in role-based access control
- A framework for specification and verification of generalized spatio-temporal role based access control model
- LoT-RBAC: A Location and Time-Based RBAC Model
- A spatio-temporal role-based access control model
- Role Based Access Control with Spatiotemporal Context for Mobile Applications

---

STARBAC: Spatiotemporal role based access control

Inspired by a real example? Scenarios or examples. Similar reasoning as other location based models, No formal evaluation, scenarios or real world examples.

What reasons and evidence do researchers claim RBAC needs extension? Extension of RBAC and of SRBAC by combining spatial and temporal

Did they implement the model?

Is there an evaluation? If yes, how did they do one? If no, why? Mathematical explanations, definitions Includes descriptions and math behind the semantics

Does this model extend the core model?

Notes.

On spatio-temporal constraints and inheritance in role-based access control

Inspired by a real example? Scenarios or examples. Believe that previous models focus on syntax and not semantics

What reasons and evidence do researchers claim RBAC needs extension?

- pervasive computing environments requirement for spatial and temporal awareness
- previous spatio-temporal do nt address interaction between these constraints and inheritance
- makes 4 claims about how existing models do not handle the above

- trusted entities to override restrictions
- attempt to show compatibility with standard model and claim others do not

Did they implement the model?

Is there an evaluation? If yes, how did they do one? If no, why?

- Examine previous models and point out deficiencies, use of graphs to show off relationships
- Evaluation includes a mathematical examination of the role graphs, and ordering
- authors note that there is added complexity in their method, but that is the price to pay to get user and user-role application constraints
- trade-off between complexity of policies and complexity of constraints
- authors do comparisons of complexity for the various models
- authors note that SoD should be considered in the future

Does this model extend the core model? Additions to the specification for constraints with a specific look at how to do spatial and temporal

Notes.

A framework for specification and verification of generalized spatio-temporal role based access control model

Inspired by a real example? Scenarios or examples. Based off hospital example with mobile devices inspiring combining location and time based models Provides an example hospital access control policy that requires space and time - based on the layout of the floor of a hospital and the various users and entitie sthat might exist such as nurse, doctor and surgeons

What reasons and evidence do researchers claim RBAC needs extension? Need to be able to handle add attributes that location and spatial specification requires Add context mechanisms

Did they implement the model? No

Is there an evaluation? If yes, how did they do one? If no, why? To some degree, an example, and some analysis of developing policy and how to deal with conflicts

Does this model extend the core model? Builds on GTRBAC, extends at all 4 levels Adds role activation/deactivation Provides conflict resolution Includes a GSTRBAC policy specification model using Alloy

Notes.

LoT-RBAC: A Location and Time-Based RBAC Model

Inspired by a real example? Scenarios or examples. Inspired by growing needs of mobile, peer-to-peer devices with regards to activating and specifying permissions and roles based on time and location Detailed scenario of a person having a medical emergency, and a doctor on site needing to request patient data, as well as the progression through the ambulance, to hospital and citing such location based clues to help know if the doctor should be granted privileges such as being in or near his own car

What reasons and evidence do researchers claim RBAC needs extension? Previous location and time based RBAC models did not incorporate location for both the user and role In-depth, detailed location heirarchies and specifications are needed Physical, logical, and hybrid location

Did they implement the model? No

Is there an evaluation? If yes, how did they do one? If no, why? No

Does this model extend the core model?

Notes.

A Spatio-temporal Role-Based Access Control Model

Inspired by a real example? Scenarios or examples. Growth of wireless networks, mobile devices, the move towards pervasive computing

What reasons and evidence do researchers claim RBAC needs extension? Claim that previously examined models of spatial, temporal, or spatio-temporal lack needed aspects Role assignment should be dependent on space and time Permissions need to be dependent on space and time not just roles

Did they implement the model? No. Authors acknowledge need to implement.

Is there an evaluation? If yes, how did they do one? If no, why? No. Best they do is provide a detailed scenario with an examination of how such a scenario would be represented in their model. Author acknowledge detailed analysis is needed.

Does this model extend the core model? Defines for Space - physical location, logical location and mapping functions and relationship definitions Defines for Time - time instant, time interval Adds objects to Core model, object can be physical or logical (computer or files e.g.) Defines a number of potential role hierarchy strategies Examines impact on both static and dynamic separation of duties for new attributes and mechanisms

Notes.

Role Based Access Control with Spatiotemporal Context for Mobile Applications

Inspired by a real example? Scenarios or examples. Need and desire to put spatio-temporal context and constraint on roles and permissions - such as students at a university or hospital facilities

What reasons and evidence do researchers claim RBAC needs extension? Needs enhancements to be able to handle space and time attributes on roles and permissions

Did they implement the model? Yes. Integrated an access control system into iMedik - a telemedicine application in India that is web-based and allows mobile access Their implementation is a bolt-on solution, that intercepts calls and verifies their authorization Provide detailed architecture and implementation details

Is there an evaluation? If yes, how did they do one? If no, why? Include section that discusses differences between their model and STRBAC and STARBAC Incorporate algorithms for determining whether a particular authorization is granted and use time-complexity arguments to discuss the effectiveness of each algorithm and to attempt to display that the added complexity of their model over traditional RBAC does not impace performance significantly

Does this model extend the core model? Extends at all 4 levels Adds “extents” which are design to extend the base entities such as a role, multiple RoleExtents can belong to a single role based off constraint or context

Notes.

CHAPTER

NINETEEN

TASK

Definition. a usually assigned piece of work often to be finished within a certain time

Papers

- A Task-Role Based Access Control Model with Multi-Constraints
- Team and Task Based RBAC Access Control Model
- Task–role-based access control model

A Task-Role Based Access Control Model with Multi-Constraints

Inspired by a real example? Scenarios or examples. Not much reasoning or evidence as to the 'why'

What reasons and evidence do researchers claim RBAC needs extension? RBAC can't handle large enterprises with multiple applications and a single user base

Did they implement the model?

- Discussion of the applications of the model, mentions of real companies using the implementation, and a mention of a system that exists

Is there an evaluation? If yes, how did they do one? If no, why?

- Unclear, as their examples and applications didn't contain much data

Does this model extend the core model?

- rigorous constraints definitions, mathematical specification of additional model elements
- Attempts to combine TBAC and RBAC by placing a task between a role and a permission
- not really extending the base RBAC model

Notes.

Team and Task Based RBAC Access Control Model

Inspired by a real example? Scenarios or examples.

- Real world scenarios - hospital
- Applications of TT-RBAC in an imaginary hospital scenario

What reasons and evidence do researchers claim RBAC needs extension?

Did they implement the model?

- Prototype system

Is there an evaluation? If yes, how did they do one? If no, why?

Does this model extend the core model?

- Covers all 4 levels of RBAC, provides mathematical definitions of entities
- Extension to RBAC at all four levels
- Introduces teams that map to users, roles and tasks
- Introduces tasks that map to teams and permissions

Notes.

Task–role-based access control model

Inspired by a real example? Scenarios or examples. Define a set of security requirements for access control in an enterprise environment

What reasons and evidence do researchers claim RBAC needs extension? 8 security requirements for enterprise environments

Did they implement the model? No.

Is there an evaluation? If yes, how did they do one? If no, why?

- No implementation, not enough envidence other than the security requirements, the requirements are based off a few thought scenarios that seem based on a ‘typical’ enterprise organizational setup

Does this model extend the core model?

- extension by adding Task notion to connect with roles and users

Notes. Task has constraints, task sits between permission and roles, tasks used to compose workflows, and are more mutable than roles - task can be used for defining set of actions and help when the specific data objects are less known at creation time

CHAPTER

TWENTY

TEMPORAL

Definition. of or relating to the sequence of time or to a particular time

Papers

- A generalized temporal role-based access control model

A generalized temporal role-based access control model

Inspired by a real example? Scenarios or examples. In many organizations, processes and functions may have limited time spans or have periodic temporal durations

What reasons and evidence do researchers claim RBAC needs extension?

- Workflow based organizations need a time based constraint for disabling/enabling roles

Did they implement the model? No.

Is there an evaluation? If yes, how did they do one? If no, why?

- Model is limited to enabling/disabling of roles based on time constraints only
- model is fully described from entities, to constraints, to conflict resolution to execution in pseudo-code
- Evaluation lies in the construction of mathematical modeling and graphs to detail the usage and interaction of the model pieces
- A few example scenarios are explained

Does this model extend the core model?

- Extension of the base RBAC model
- adds periodicity and duration constraints for role enabling
- provides for conflict resolution of constraints

Notes.

BIBLIOGRAPHY

[1] David F. Ferraiolo, Ravi S. Sandhu, Serban I. Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3):224–274, 2001.