Available online at www.sciencedirect.com
ScienceDirect
Information and Software Technology 00 (2012) 1–4
IST

A Systematic Literature Review on Role-Based Access Control

Abstract

Role-based access control (RBAC) has become an increasingly popular access control for various applications such as web applications and database applications. RBAC restricts access to resources based on identity of subjects and/or groups called roles. Since RBAC is introduced in 1998, researchers have proposed various extended models of RBAC. For example, they define additional constraints among roles (e.g., temporal constraints or location constraints) or hierarchy relationship of roles. Our goal of this work is to study extended models of RBAC and analyze their extended features and claimed research contributions to find limitations of current RBAC models and what extent of extended features that can be used for future RBAC. We conduct a systematic literature review by collecting and synthesizing relevant research papers. We initially collect XXXX papers from various sources such as IEEE and ACM websites and selected 26 papers systemically. We perform a comparative analysis to find relationships among extended models and RBAC. [TBD: Result] [TBD: Conclusion]

Keywords:

1. Introduction

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.

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.

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 is:

- Google Scholar - ttp://scholar.google.com
- IEEExplore - http://ieeexplore.ieee.org
- ACM Portal - http://dl.acm.org

For each of the criteria below, a search was performed on each of the search engines for a total of 9 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. For each criteria for each search engine, the results were captured until a stopping criteria was met. For a given run was done 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 any of the search criteria words within the title. After gathering all 9 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.

The results of the searches was as follows:

	RBAC	role based access control	role-based access control
Google Scholar	261	581	391
ACM Portal	321	281	261
IEEExplore	171	221	201

We collect papers on extended role-based access control [1].

2.1. Research Questions

We have following research questions.

- RQ1. What are problems in current RBAC model to propose extended RBAC models?
- RQ2. What are reasons to propose RBAC extensions?
- RQ3. Which extended features of RBAC model are proposed?
- RQ4. How they provide evidence to show that their model work in practice? For example, they provide a prototype to run a real example.
- RQ5. What is criteria for evaluation? We investigate how they evaluate their research work.

For RQ1-RQ3, we compare of proposed extended models. For RQ4, we compare quality of completeness of the proposed models. Beyond modeling of extended RBAC models, an prototype shows that their models work in practice and improves the quality of the completeness of research papers. For RQ5, we compare criteria for evaluation of extended RBAC models.

2.2. Categorization

This section describes categorization of papers based on specific extended features as follows.

- Temporal-related-constraints [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
- Inheritance [13]
- Location [7]
- Delegation [14]
- General constraints [15, 16]
- Context [17, 18, 19, 20, 21, 22]
- General extension [23, 24]
- Combination with other access control models such as Task-based access control [16, 25, 26, 27] and Agent-based access control [28]

References

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

[2] T. Mossakowski, M. Drouineaud, K. Sohr, A temporal-logic extension of role-based access control covering dynamic separation of duties, in: Temporal Representation and Reasoning, 2003 and Fourth International Conference on Temporal Logic. Proceedings. 10th International Symposium on, 2003, pp. 83 – 90.

[3] 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.

[4] M. Kumar, R. E. Newman, Strbac - an approach towards spatio-temporal role-based access control, in: Communication, Network, and Information Security'06, 2006, pp. 150–155.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] E. Bertino, P. A. Bonatti, E. Ferrari, Trbac: A temporal role-based access control model, ACM Trans. Inf. Syst. Secur. 4 (3) (2001) 191–233.

[10] J.-Q. Li, X.-Y. Li, S.-X. Xie, C. Chen, H.-S. Yu, G.-L. Liu, A fine-grained time-constraint role-based access control using ocl, in: Digital Information Management, 2008. ICDIM 2008. Third International Conference on, 2008, pp. 81 –86.

[11] 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.

[12] 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.

[13] C.-L. Ren, X.-H. Zuo, Z.-X. Li, X.-X. Niu, Y.-X. Yang, Towards hierarchical-user RBAC model, in: Machine Learning and Cybernetics (ICMLC), 2010 International Conference on, Vol. 6, 2010, pp. 2870 –2874.

[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] 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] L. Yao, X. Kong, Z. Xu, A task-role based access control model with multi-constraints, in: Proceedings of the 2008 Fourth International Conference on Networked Computing and Advanced Information Management - Volume 01, NCM '08, 2008, pp. 137–143.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] S. Oh, S. Park, Task-role-based access control model, Inf. Syst. 28 (6) (2003) 533–562.

[26] W. Zhou, C. Meinel, Team and task based RBAC access control model, in: Network Operations and Management Symposium, 2007. LANOMS 2007. Latin American, 2007, pp. 84 –94.

[27] S. Oh, S. Park, Task-role based access control (T-RBAC): An improved access control model for enterprise environment, in: Proceedings of the 11th International Conference on Database and Expert Systems Applications, DEXA '00, 2000, pp. 264–273.

[28] W. Yamazaki, H. Hiraishi, F. Mizoguchi, Designing an Agent-Based RBAC system for dynamic security policy, in: Proceedings of the 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE '04, 2004, pp. 199–204.