Future Directions in Role-Based Access Control Models

Ravi Sandhu

Chief Scientist, SingleSignOn.Net Inc.
11417 Sunset Hills Road, Reston, VA 20190, USA
rsandhu@singlesignon.net, www.singlesignon.net
&
Professor of Information Technology and Engineering
George Mason University, Fairfax, VA 22030, USA
sandhu@gmu.edu, www.list.gmu.edu

Abstract. In the past five years there has been tremendous activity in role-based access control (RBAC) models. Consensus has been achieved on a standard core RBAC model that is in process of publication by the US National Institute of Standards and Technology (NIST). An early insight was that RBAC cannot be encompassed by a single model since RBAC concepts range from very simple to very sophisticated. Hence a family of models is more appropriate than a single model. The NIST model reflects this approach. In fact RBAC is an open-ended concept which can be extended in many different directions as new applications and systems arise. The consensus embodied in the NIST model is a substantial achievement. All the same it just a starting point. There are important aspects of RBAC models, such as administration of RBAC, on which consensus remains to be reached. Recent RBAC models have studied newer concepts such as delegation and personalization, which are not captured in the NIST model. Applications of RBAC in workflow management systems have been investigated by several researchers. Research on RBAC systems that cross organizational boundaries has also been initiated. Thus RBAC models remain a fertile area for future research. In this paper we discuss some of the directions which we feel are likely to result in practically useful enhancements to the current state of art in RBAC models.

Introduction

Research on access control models was started in the 1960s and 1970s by the two thrusts of mandatory and discretionary access control. Mandatory access control (MAC) came from the military and national security arenas whereas discretionary access control (DAC) had its roots in academic and commercial research laboratories. These two thrusts were dominant through the 1970s and 1980s almost to exclusion of any other approach to access control models. In the 1990s we have seen a dramatic shift towards pragmatism.

The dominant access-control model of the 1990s is role-based access control (RBAC). In this paper we make the case that RBAC will continue to be dominant for the next decade.

Current State of RBAC Models

To my knowledge the first use of the term RBAC is due to Ferraiolo and Kuhn [FK92] although there has been prior mention in the security literature of "roles" and "role-based security." Sandhu et al [SAN96] subsequently published a seminal paper defining a family of models that has since come to be called RBAC96. A crucial insight of RBA96 was the realization that RBAC can range from very simple to very sophisticated so we need a family of models rather than a single model. A single model is too complex for some needs and simple for others. A graded family of models enables selection of the "correct" model for a particular situation. Publication of RBAC96 was followed by a flurry of research that has clearly established RBAC as the dominant access control model. Remarkably the basic concepts of RBAC96 have proved to be robust and no significant omissions have been identified. In many years of research following publication of RBAC96 we have had occasion to introduce only one new concept (role activation hierarchies [SAN98]) which was not already present in RBAC96.

Let us now briefly review important achievements in recent RBAC research. The perspective given here is necessarily a personal one. As such the papers cited are those with greatest direct impact on our own understanding of RBAC models. There simply is not enough room to cite many other papers of considerable significance.

We feel that RBAC models have advanced in at least three respects in recent years, discussed below in turn.

Firstly, an important recent development is emergence of a **consensus standard model** which is supported by a major standards organization (the US National Institute of Standards and Technology or NIST). Following the publication of RBAC96 it became clear that many authors were pursuing very similar ideas but with differences in detail leading to confusion about the nature of RBAC. RBAC96 was unique in proposing the concept of a graded family of models. Once this family notion was accepted by the RBAC community consensus on a core set of RBAC concepts became feasible. To this end an initial attempt at a family of standard models was presented at the Berlin RBAC Workshop by Sandhu et al [SFK00]. Workshop attendees reacted to this proposal with heated discussion [JT00]. The current proposal is to be published soon [FER01] and will then evolve into NIST publications. Deployment and use of RBAC in commercial products and systems will be facilitated by the NIST standard model.

Another important development is a **deeper theoretical understanding of RBAC** and particularly its relationship to MAC and DAC. There has been much confusion with some authors claiming that RBAC is a form of MAC while others arguing it is a form of DAC. Osborn et al [OSM00] show that RBAC96 can be configured to do MAC or DAC as one chooses. So RBAC transcends the MAC-DAC distinction. Fundamentally it turns out that both MAC and DAC are just special cases of RBAC. For historic reasons MAC and DAC gained early dominance in the research community. MAC and DAC are easily unified within the framework of RBAC. This unification is more than coexistence. MAC systems also usually implement DAC but in these systems MAC and DAC simply coexist. The RBAC viewpoint is that MAC and DAC are just examples of policies to configure in a policy-neutral RBAC model.

The third significant development is a **contextual understanding of the practical purpose of RBAC models**. Sandhu [SAN00] argues that the purpose of RBAC models is two-fold. On hand they help us articulate access-control objectives in a mathematical and rigorous framework. On the other hand they help us understand how to actually architect a system with attendant trust, liability and authority responsibilities and obligations. The clear separation of a model from objectives (or policy) and architecture (and even deeper mechanism) is captured in the four layer OM-AM (for objectives, models, architecture, mechanism) framework of [SAN00]. RBAC models are designed to be objective (or policy) neutral but can be configured to achieve a wide range of policies (including the extreme cases of MAC and DAC discussed above). In this paper our focus is on models and OM-AM allows us to clearly understand the two-faced nature of RBAC models. On one side models help us understand and articulate policy. On the other side a given model can be implemented in many different architectures (and with many different mechanisms).

Future Directions for RBAC Models

Now we consider aspects of RBAC models that need further research. Some of these have already been explored. Some are even rather mature but consensus in the community has not yet been achieved. Others have only been hinted at in the literature or only preliminary exploratory work has been published. So we can divide our discussion roughly into two categories: areas in which strong progress has been made but consensus needs to be developed to reach maturity such as embodied in standards, and areas in which only preliminary work has been accomplished.

One of the main omissions in the NIST standard model [FER01] is the authorization of administration of RBAC. Access control is basically simple so long as the permissions do not change. However a static model of access control is not very realistic. Sandhu et al [SAN98] have argued that administration of RBAC in large scale systems must itself be decentralized and can profitably be managed using administrative roles. The ARBAC97 model shows how this can be done using RBAC96 as the underlying model. It would be desirable to develop standards in this arena because administration is often the place where security breaks. Moreover, the ARBAC97 model addresses RBAC administration from one point of view and one administrative paradigm.

Alternate administrative paradigms for RBAC have been recently discussed in the literature. Hildmann and Barholdt [HB99] and Herzberg et al [HER00] consider some issues in assigning roles to users in systems that cross organizational boundaries. Barka and Sandhu [BS00] have proposed a framework for modeling delegation of roles from one user to another. Huang and Atluri [HA99] discuss the dynamics of RBAC in workflow systems. Damianou et al [DDLS01] and Hitchens and Varadharajan [HV01] have proposed languages for specifying RBAC policy. Thomas and Sandhu [TS98] have argues the need for active authorization models which are self-adminstering. These papers present specific perspectives and viewpoints on adminstration of RBAC. However, we are far short of an integrated model around which community consensus can be developed.

Most RBAC research to date has been based on a single organization's point of view. This is a natural consequence of the initial motivation for RBAC which is concerned with managing access rights in large-scale systems. In the future we are likely to see greater interest in applications of RBAC to Business-to-Business and Business-to-Consumer electronic commerce. RBAC is a natural technology for separating responsibilities in cross-organization systems. User-role assignment can be handled by one organization while permission-role assignment is handled by another.

Another consequence of the organizational emphasis in past RBAC research is that assigning a role to a user is generally considered an administrative act of some other user (or administrator). In the digital economy we can conceive of roles that are acquired due to payment, such as membership in a club or society, or as a reward or bonus, such as frequent flyer status. We can also have roles that are traded between users for some kind of a fee. Developing a comprehensive RBAC administrative model to cover this scope is a challenging research task.

While role hierarchies are well understood RBAC constraints have only received attention in recent years. Classically separation of duty has been seen as the main motivation for constraints in RBAC models. More recently their importance beyond separation of duties has been recognized in the literature [JAE99, BBF00]. Ahn and Sandhu [AS00] have proposed the RCL2000 language for specifying RBAC constraints and have argued that prohibition and obligation constraints are both required with separation constraints being an example of prohibition.

Conclusion

We hope to have convinced the reader that research on RBAC models has just begun and much interesting and challenging work remains to be done. The RBAC arena is intrinsically dominated by practical considerations and offers an opportunity for good theoretical research to be translated into practical impact on products and practice.

Acknowledgement

The work of Ravi Sandhu is partially supported by the National Science Foundation.

References

[AS00] Gail Ahn and Ravi Sandhu. "Role-Based Authorization Constraints Specification." *ACM Trans. on Information and System Security*, Volume 3, Number 4, November 2000.

[BS00] Ezedin Barka and Ravi Sandhu, "Framework for Role-Based Delegation Models." *Proc. 16th Annual Computer Security Applications Conference*, New Orleans, Dec., 2000.

[BBF00] E. Bertino, P. Bonatti, and E. Ferrari. "TRBAC: A Temporal Role-Based Access Control Model." *ACM Transactions on Info. and System Security*, 4:3, Aug. 2001, to appear.

[DDLS01] N. Damianou, N, Dulay, E. Lupu, and M. Sloman. "The Ponder Policy *Int. Workshop on Policy*, Jan. 2001, Springer LNCS 1995.

[FK92] D. Ferraiolo and R. Kuhn. Role-Based Access Control. In *Proc. of the NIST-NSA National Computer Security Conference*, pp 554-563, 1992.

[FER01] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn and Ramaswamy Chandramouli. "A Proposed Standard for Role-Based Access Control." *ACM Transactions on Information and System Security*, Volume 4, Number 3, August 2001, to appear.

[HER00] A. Herzberg, Y. Mass , J. Mihaeli, D. Naor and Y. Ravid. "Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers." *IEEE Symposium on Security and Privacy*, Oakland, May 2000.

[HB99] Thomas Hildmann and Jörg Barholdt. "Managing trust between collaborating companies using outsourced role based access control." In *Proc. of 4th ACM Workshop on Role-Based Access Control*, pp. 105-111, 1999.

[HV01] M. Hitchens and V. Varadharajan. "Tower: A Language for Role Based Access Control." *Int. Workshop on Policy*, Bristol, UK, January 2001, Springer LNCS 1995.

[HA99] W. Huang and V. Atluri. A secure web-based workflow management system. In *Proc. of 4th ACM Workshop on Role-Based Access Control*. 1999.

[JAE99] Trent Jaeger. "On the Increasing Importance of Constraints." *Proc. 4th ACM Workshop on Role-Based Access Control*, Fairfax, Virginia, Oct. 28-29, 1999, pages 33-42

[JT00] T. Jaeger and J. Tidswell. Rebuttal to the NIST RBAC model proposal. *Proc. 5th ACM Workshop on Role-Based Access Control*, Berlin, Germany, July 26-28, 2000, pages 65-66.

[OSM00] S. Osborn, R. Sandhu and Q. Munawer. "Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies." *ACM Trans. on Information and System Security*, Volume 3, Number 2, May 2000, pages 85-106.

[SAN96] Ravi Sandhu, Edward Coyne, Hal Feinstein and Charles Youman, "Role-Based Access Control Models." *IEEE Computer*, Volume 29, Number 2, Feb. 1996, pages 38-47.

[SAN98] Ravi Sandhu, "Role Activation Hierarchies." *Proc. 3rd ACM Workshop on Role-Based Access Control*, Fairfax, Virginia, October 22-23, 1998, pages 33-40.

[SBM99] R. Sandhu, V. Bhamidipati and Q. Munawer. "The ARBAC97 Model for Role-Based Administration of Roles." *ACM Trans. on Info. and System Security*, 2:1, Feb. 99, 105-135.

[SAN00] Ravi Sandhu, "Engineering Authority and Trust in Cyberspace: The OM-AM and RBAC Way." *Proc. 5th ACM Workshop on RBAC*, Berlin, July 26-28, 2000, pages 111-119.

[SFK00] R. Sandhu, D. Ferraiolo and R. Kuhn, "The NIST Model for Role-Based Access Control: Towards A Unified Standard." *Proc. 5th ACM Workshop on RBAC*, ages 47-63.

[TS98] Roshan Thomas and Ravi Sandhu, "Task-based Authorization Controls (TBAC): Models for Active and Enterprise-Oriented Authorization Management." In *Database Security XI: Status and Prospects*, Chapman & Hall 1998, pages 262-275.