Chapter VI
Towards a Scalable Role and Organization Based Access Control Model with Decentralized Security Administration

Zhixiong Zhang
The College Board, USA

Xinwen Zhang
Samsung Information System America, USA

Ravi Sandhu
University of Texas at San Antonio, USA
TriCipher Inc., USA

ABSTRACT
This chapter addresses the problem that traditional role-base access control (RBAC) models do not scale up well for modeling security policies spanning multiple organizations. After reviewing recently proposed Role and Organization Based Access Control (ROBAC) models, an administrative ROBAC model called AROBAC07 is presented and formalized in this chapter. Two examples are used to motivate and demonstrate the usefulness of ROBAC. Comparison between AROBAC07 and other administrative RBAC models are given. We show that ROBAC/AROBAC07 can significantly reduce administration complexity for applications involving a large number of organizational units. Finally, an application compartment-based delegation model is introduced, which provides a method to construct administrative role hierarchy in AROBAC07. We show that the AROBAC07 model provides convenient ways to decentralize administrative tasks for ROBAC systems and scales up well for role-based systems involving a large number of organizational units.
**INTRODUCTION**

With the wide Internet usage in our society, the security and privacy issues become more important than ever. In the last decade, role-based access control (RBAC) had been generating considerable interests among the researchers and practitioners. In RBAC, roles are defined based on job functions, permissions are associated with roles, and users are made members of appropriate roles, thereby acquiring the roles’ permissions. This indirect association between users and permissions greatly simplifies users’ permission management. RBAC has several attractive features, such as policy neutrality, principle of least privilege, and ease of management. Several well-known RBAC models, such as RBAC96 (Sandhu et al, 1996), the role graph model (Nyanchama & Osborn, 1999), and NIST model (Ferraiolo et al., 2001), have been developed during the last decade. Those models form the basis for the ANSI RBAC standard (ANSI INCITS 359-2004). As a powerful alternative to traditional discretionary and mandatory access control, the adoption of RBAC in commercial software and enterprises has rapidly increased in recent years (RTI International, 2002).

The complexity of an RBAC system can be defined on the basis of the number of roles, the number of permissions, the size of the role hierarchy, the constraints on user-role and permission-role assignments, etc. (Sandhu et al, 2000). For existing large-scale RBAC systems, the number of roles and the number of permissions are in the order of 1000s. Beyond that magnitude, the performance of RBAC may degrade and its management becomes too difficult to handle correctly. Several approaches (Giuri & Iglio, 1997; Thomas, 1997; Perwaiz & Sommerville, 2001; Park et al, 2004) have been proposed to scale up RBAC systems by extending the RBAC model from various perspectives. To achieve decentralized administration of RBAC, some role-based administrative models have been proposed (Sandhu et al, 1999; Crampton & Loizou, 2003; Oh et al, 2006; Bhatti et al, 2004). Most of the previous work address RBAC in the context of a single organization and are mainly motivated by B2E (Business to Employee) applications. On the other hand, B2B (Business to Business) and B2C (Business to Consumer) applications often involve a large number of organizations such as corporations, schools, families, etc. Typically, users from different organizations with the same role name have slightly different access privileges due to privacy consideration. For example, a user with parent role in family A has permission to view the progress records of Family A’s kids but not the progress recodes of other families’ kids. Using standard RBAC naively in these situations can result in an enormous number of roles and permissions, well into the order of millions.

This chapter tries to address the scalability problem when applying RBAC to applications involving many organizational units. The rest of this chapter is organized as follows. Section 2 gives background and two motivating examples. Section 3 reviews Role and Organization Based Access Control (ROBAC) models. Section 4 presents a decentralized administrative ROBAC model called AROBAC07 (administrative ROBAC ’07) to control administrative tasks in ROBAC systems. Section 5 discusses the implementation perspective of ROBAC. Section 6 concludes the chapter.

**BACKGROUND**

ANSI RBAC reference model includes core RBAC (no role hierarchy), hierarchy RBAC (has role hierarchy), and constrained RBAC (has Separation of Duty constraints). Figure 1 shows a classic (standard) RBAC which is based on the well-known RBAC96 and permission definition from ANSI RBAC.

Here we use the term classic RBAC to refer the typical RBAC models proposed in (Sandhu et al, 1996; Nyanchama & Osborn, 1999; Ferraiolo et al,