ABSTRACT

The authors propose a business-oriented approach to support accurate and dynamic user-role assignments for the Role Based Access Control (RBAC) model. Their model, called Business-Driven Role Based Access Control (BD-RBAC), is composed of three layers. The first layer extends the RBAC model with the concepts of business roles, system roles, credentials, and users’ capabilities. The second layer dynamically assigns users to business and system roles, and filters outdated (abnormal) user-role assignments. The third layer supports exception handling and partial authorization. The novel aspect of the work is the adaptation of RBAC-based access control systems to changes in organizational needs, while reducing the burden of security administration. To this end, the authors have developed (1) a series of algorithms to compute internal and external user-role assignments based on organizational policies, users’ requests and capabilities, (2) and shown that their outputs are permissible, i.e., a legitimate user is authorized to activate the role, complete, i.e., a legitimate user can activate the roles necessary to perform all the requested tasks, and minimal, i.e., a legitimate user does not receive any non-authorized or not-needed privileges.

Keywords: Business-Driven, Capabilities, Exception Handling, Role Assignment, Role Based Access Control (RBAC)

1. INTRODUCTION

The Role-Based Access Control (RBAC) model (Sandhu, Ferraiolo, & Kuhn, 2000; Vincent, Ferraiolo, & Kuhn, 2006; Sandhu & Coyne, 1996) has been widely used in many commercial systems to enforce security. The central idea behind this model is that users in an organization or domain are mapped to roles. Access rights are associated with the roles, thereby assigning appropriate permissions to the users belonging to these roles. RBAC provides intui-
tive and powerful access control capabilities. An essential but costly component of RBAC is to engineer roles. This process, also known as role engineering, consists of defining optimal and persistent sets of roles, permissions, and role-permission assignments that meet organizational requirements such as adherence to compliance standards while limiting the system administration cost.

However, as organizations evolve, new business tasks arise, existing ones are revised or eliminated. In order to support these changes, the system administrators of the organizations must generally manage large collections of different objects, processes, and user-role assignments across diverse organizational boundaries, and possibly over a long period of time. The business changes require to periodically repeat the costly role engineering process or to depend on outdated user-role assignments. Outdated assignments may however provide unneeded privileges to the users (employees) or block them from completing their assigned tasks, thus causing security risks. As new business tasks are also introduced or existing ones are updated, the employees must adapt to the continually changing circumstances and organizational responsibilities. Unfortunately, the capabilities of the employees, that is their aptitude to precisely adapt to these circumstances and to perform their assigned tasks without causing harm to the resources or security systems of the organizations, also change. Thus, as the organizations evolve, it is important to ensure that the security systems of the organizations enable the employees to accommodate to the new requirements without the need for substantial changes in the structure of these security systems.

We believe that organizations deploy security systems in order to control the current and future usage of their resources by ensuring, regardless of the changes that could occur in their business processes, that the actions of their users or employees on their resources are aligned with their security requirements (Dunlop, Indulska, & Raymond, 2001). RBAC-based access control systems, however, cannot accommodate efficiently these changes. For example, the skills and capabilities of the employees of an organization play a crucial role in influencing organizational decisions. As new business needs appear, the organization must determine whether its employees have the necessary skills and capabilities to satisfy its needs or to rely on more qualified external users. In RBAC-based access control systems, users that are unknown within or external to an organization security domain are however generally mapped to default roles such as guest or customer with limited privileges, or simply discarded. Another non-trivial challenge is assessing the employees’ competences. RBAC offers only limited options to model users’ skills, experiences and qualifications. Although RBAC provides a hierarchical representation of roles, this reflects more an organization line of authority and responsibility than the qualifications, skills and experience of its employees. Thus, little of an employee’s capabilities may be dynamically inferred from the roles to which the employee is assigned. Organizing RBAC roles according to the employees’ capabilities would require frequent and manual updates as employees acquire new skills and gain experience over time, and manually adding and removing employees in the assigned roles based on their capabilities is however costly and error prone.

We propose in this paper to supplement RBAC with the concepts of capabilities and credentials. The capabilities denote the competences of the users, their qualifications and skills. The credentials denote roles membership requirements. Extending RBAC with these concepts enables our model to dynamically adjust RBAC-based security systems according to changes in the business requirements. Sandhu et al. (Al-Kahtani & Sandhu, 2002) have described a similar approach in which they supplement RBAC with rules and assign users to roles based on predefined attribute expressions and constraints. However, their approach requires the attribute expressions to be updated when new roles are created or existing roles are modified. Moreover, they assume the number of roles to be relatively small. As it increases to
Related Content

Computational Complexity Analysis for a Class of Symmetric Cryptosystems Using Simple Arithmetic Operations and Memory Access Time
[www.irma-international.org/article/computational-complexity-analysis-class-symmetric/78530/](www.irma-international.org/article/computational-complexity-analysis-class-symmetric/78530/)

Health IT: A Framework for Managing Privacy Impact Assessment of Personally Identifiable Data
[www.irma-international.org/chapter/health-it/123536/](www.irma-international.org/chapter/health-it/123536/)

Privacy-Preserving Data Mining and the Need for Confluence of Research and Practice
[www.irma-international.org/chapter/privacy-preserving-data-mining-need/30098/](www.irma-international.org/chapter/privacy-preserving-data-mining-need/30098/)

Observations on Genderwise Differences among University Students in Information Security Awareness
[www.irma-international.org/article/observations-on-genderwise-differences-among-university-students-in-information-security-awareness/148066/](www.irma-international.org/article/observations-on-genderwise-differences-among-university-students-in-information-security-awareness/148066/)
The Moral Status of Information and Information Technologies: A Relational Theory of Moral Status
www.irma-international.org/chapter/moral-status-information-information-technologies/23331/