ELSEVIER

Decision Support Systems 29 (2000) 357–369

Decision Support Systems

www.elsevier.com/locate/dsw

An object-oriented organizational model to support dynamic role-based access control in electronic commerce ☆

Edward C. Cheng

OCT Research Laboratory, Birkbeck College, University of London, Three Waters Park, MS 215, San Mateo, CA 94403, USA

Abstract

Role-based access control (RBAC) provides flexibility to security management over the traditional approach of using user and group identifiers. In RBAC, access privileges are given to roles rather than to individual users. Users acquire the corresponding permissions when playing different roles. Roles can be defined simply as a label, but such an approach lacks the support to allow users to automatically change roles under different contexts; using static method also adds administrative overheads in role assignment. In electronic commerce (E-Commerce) and other cooperative computing environments, access to shared resources has to be controlled in the context of the entire business process; it is therefore necessary to model dynamic roles as a function of resource attributes and contextual information.

In this paper, an object-oriented organizational model, Organization Modeling and Management (OMM), is presented as an underlying model to support dynamic role definition and role resolution in E-Commerce solution. The paper describes the OMM reference model and shows how it can be applied flexibly to capture the different classes of resources within a corporation, and to maintain the complex and dynamic roles and relationships between the resource objects. Administrative tools use the role model in OMM to define security policies for role definition and role assignment. At runtime, the E-Commerce application and the underlying resource manager queries the OMM system to resolve roles in order to authorize any access attempts. Contrary to traditional approaches, OMM separates the organization model from the applications; thus, it allows independent and flexible role modeling to support realistically the dynamic authorization requirements in a rapidly changing business world.

Keywords: Electronic commerce; Role-based access control; Organization modeling; Role resolution; Business process management; Workflow

1. Introduction

Electronic Commerce (E-Commerce) applications aim to conduct business over the electronic network. Although electronic business transactions evolved from EDI protocols will continue to play a major role in E-Commerce, the rapid growth of the Internet (in 1998, more than 2 million new users are added to the Internet every quarter [20]) has pushed companies to expand the scope of E-Commerce applications to cover the full range of business activities [3]. These activities may include marketing, negotiation, fulfillment and follow up, all perform over the Internet. This trend creates new business opportunities and posts new technical challenges. It pushes E-

☆ An invited paper. A shorter version of the paper was presented at HICSS 1999.

E-mail address: edwardc@octlab.com (E.C. Cheng).

0167-9236/00/$ - see front matter
PII: S0167-9236(00)00083-X

Commerce to go beyond simple short-lived transactions but become a business process that includes outside customers, business partners, and a number of resources within a company. As more people are involved in the transaction circle, security and authorization control become one of the biggest concerns.

Current E-Commerce solutions are primarily developed as applications on top of Resource Managers (RM) or database management system (DBMS). Unfortunately, resource manager implementations have historically focused on technologies around access methods, concurrency control, and logging and recovery [7,8,16]. The security model and access control usually assume a simple and static model, which are based on user and group identifiers. As E-Commerce applications are implemented over the DBMS, they simply adopt the user and security model of a relational database management system (RDBMS) as their access control model. However, the user model in RDBMS is designed primarily to support access control in processing isolated transactional operations rather than integrated process activities [17]. It is thus not adequate to model the flexible resource relationship that is required to support cooperative works in the E-Commerce context.

The introduction of workflow technology allows E-Commerce applications to cover the full range of business activities over the network. As the work-process flows across multiple organizations, it is important to identify the different resources involved in the process. However, current workflow deployment practically focuses on departmental level; many of these systems simply ignore the role issue. Others though expand their scope to cover workflow across departmental boundaries, they still assumed a static organization and role model within a single corporation [2,13].

This paper discusses an organizational and role model to support dynamic access control in E-Commerce. The model is called Organization Modeling and Management (OMM). The OMM methodology supports both the conceptual design and the design implementation phases of the enterprise modeling cycle [1]. It serves as an underlying system for applications and resource managers to control resource accesses and job assignment. The next section covers the related research work in role-based access control (RBAC) and organization modeling. Section 3 describes the OMM conceptual and reference model for enterprise modeling. OMM does not assume a particular process or application architecture. With this generic approach, OMM is able to map its object types to other organizational data schemes and to present an integrated multidimensional view of different organizational resources. Section 4 presents the role resolution concept in E-Commerce and discusses a Java-based prototype, OMM, which is used to implement an RBAC system to enable the E-Commerce strategy in a hi-tech company. Section 5 discusses the OMM system architecture. The paper will conclude in Section 6 by a summary and by sharing our practical experience of applying the OMM methodology to a hi-tech firm to support their E-Commerce strategy.

2. Related work

Role-based security has been applied in various areas of computer systems security [32]. Osborn [28] and Kuhn [21] proposed formal models for RBAC. These works provide a basis for separation of duty based on role names. Access privileges are granted to different roles. A user can play multiple roles by binding with a number of role names. Although this approach gives more flexibility to access control than the simple granting to user identifier method, it is still a static approach and ignores entirely the organization model.

Others have proposed specific role models and methodologies for concurrent engineering, such as M*-OBJECT [12], SAM* [33], and ObjectFlow [18,19]. They all start from the process view and tightly couple the organization model with the role model, and some even with the process model.

Other researchers have proposed visual and programming languages for organizational and office systems, such as Officeaid-VPE [11], HI-VISUAL [15], M*-OBJECT [12] and Regatta VPL [34]. Officeaid-VPE and HI-VISUAL were limited to the description of single office tasks. They are therefore not adequate for the integration and collaboration across multiple offices, let alone to include external customers and business partners as required in E-Commerce. M*-OBJECT and Regatta VPL have a comprehensive process model and an abstract view