Chapter 10
On Ontology of Integration Between Access Control and Business Process Deep Structure

Sérgio Luís Guerreiro
Instituto Superior Técnico, Universidade de Lisboa, Portugal & Instituto de Engenharia de Sistemas e Computadores – Investigação e Desenvolvimento, Portugal

ABSTRACT

Access control models (ACM) offers the guarantee that only the qualified users can gain access to the artifacts contained in business processes. Business processes are designed, implemented, and operated using many industrial standards that challenge the interoperation with access control standards. Enterprise engineering (EE) introduces rigorous capabilities to design and implement the essential concepts related with the dynamic of business processes. ACM deals with the systematic design and implementation of dynamic and static access control concepts to qualify the access of the users to the artifacts. This chapter proposes an ontological integration between EE and ACM concepts in order to enable the discussion of access control in the deep structure of the business processes. ACM integrated with EE allow the run-time qualification of the actors while they perform all the business process steps and not only at invocation time. The proposal encompasses business process designed with DEMO ontology and role-based access control concepts using a mathematical model logic description.

DOI: 10.4018/978-1-7998-2975-1.ch010
1. INTRODUCTION

Authorization is present in every form of information technology today and is concerned with the ways which users can access resources in computer systems or, informally speaking, with *who can do what*. Role-based access control (RBAC) (Ravi et al., 1996) models the classical concepts for access control encompassing: *user, role, permission, constraint* and *session*. It represents an evolution from Discretionary Access Control (DAC), Mandatory Access Control (MAC) and other policies due to less provisioning effort needed. In RBAC users are assigned to a role; each role has a set of associated permissions and changing the permissions only affects the users associated with each role. Some well-known RBAC constraints are: separation of duties (SoD), conflict of interest (CoI), delegation of duties (DoD), binding of duties (BoD), history-based separation of duties (HsD) or newly identified constraints in social networks such as context constraints, *e.g.*, (Carminati et al., 2011). RBAC is applicable to organizational silos, however, it is limited to only one kind of organizational artifact at a single time. It is broadly used in a single architectural layer such as applications or databases (Ferraiolo, Kuhn, & Chandramouli, 2007). This limitation is identified as a first problem which demands a large effort to manage the configuration of accesses in business processes performed by an organization over time (Gaaloul, Guerreiro, & Proper, 2014; Guerreiro, Vasconcelos, & Tribolet, 2011).

Besides this limitation, Hung and Karlapalem (2003) point to the problem of how to enforce access control in workflow management systems (WfMS). To solve this problem, Bertino, Ferrari, and Atluri (1999, 1997) propose a combination of static, dynamic and hybrid constraints to split the enforcement of RBAC in WfMS: the static constraints are processed offline and the dynamic constraints requires an execution engine to monitor the workflow sessions. It is a computationally intensive process that cannot get in the way with the WfMS execution itself.

Developments in attribute-based access control (ABAC) approaches such as the one proposed by Wang, Wijesekera, and Jajodia (2004) extend the RBAC capability, granting access to the artifacts based on the attributes possessed by the requester. The advantage when compared with RBAC is that management of the roles and permissions is not needed. The access configuration is specified by a set of rules that uses the attributes that are issued in the client request. A change in the access policy is performed by a simple change in the rules. In this context, Kuhn, Coyne, and Weil (2010) add that ABAC approach is still evolving from the previous definition of RBAC and not emerging from previous unknown. Moreover, the distributed nature of the web services and the service-oriented architecture (SOA) environments are identified as a potential application area for the development of the ABAC concepts (Shen & Hong, 2006).
Related Content

Measuring Models
[www.igi-global.com/chapter/measuring-models/26829?camid=4v1a](www.igi-global.com/chapter/measuring-models/26829?camid=4v1a)

Designing Secure and Privacy-Aware Information Systems
[www.igi-global.com/article/designing-secure-and-privacy-aware-information-systems/190419?camid=4v1a](www.igi-global.com/article/designing-secure-and-privacy-aware-information-systems/190419?camid=4v1a)

Volumetric Estimation of the Damaged Area in the Human Brain from 2D MR Image
Non-Monotonic Modeling for Personalized Services Retrieval and Selection
[www.igi-global.com/article/non-monotonic-modeling-personalized-services/44686?camid=4v1a](www.igi-global.com/article/non-monotonic-modeling-personalized-services/44686?camid=4v1a)