Access Control for Business Processes

Todays business environment is undergoing dramatic change. Competitive pressure from traditional and non-traditional sources, the rapid emergence and growth of new channels, increasing pressure to outsource selected business processes, and demands for compliance with a plethora of new regulatory and legal requirements are all contributing to an ever growing demand for change. Traditionally, many organizations have struggled to manage change. In order to survive and prosper in the coming years, these organizations will need to develop a capability to sustain a state of change and evolution. The ability of an organizations IT systems to cope with this level of change will be a significant factor in the organizations success in adapting to this increasingly dynamic business environment. Organizations are addressing this by adopting service-oriented architecture (SOA) principles. Service orientation (and SOA in general) is increasingly being viewed as a means to better align business and IT objectives and to better support the levels of flexibility and change required by the business. Business processes or workflows can be built by combining Web services through the use of a process specification language. Such languages basically allow one to specify which tasks have to be executed and the order in which they should be executed. Because of their importance, process specification languages have been widely investigated and a number of languages have been developed. One such language is WS-BPEL (Web services Business Process Execution Language), which has became the de facto standard to implement business processes based on Web services [10]. WS-BPEL resulted from the combination of two different workflow languages, WSFL [162] and XLANG [253], and adopts the best features of these language. WS-BPEL is layered on top of several XML standards, including WSDL 1.1[67], XML Schema 1.0 [258], and XPath 1.0 [71], but of these, WSDL has had the most influence on WS-BPEL. Despite significant progress toward the development of an expressive language for business processes, significant challenges still need to be addressed before business processes management systems can be widely used in distributed computer systems and Web services. Even if WS-BPEL has been developed to specify automated business processes that
orchestrate activities of multiple Web services, there are cases in which people must be considered as additional participants who can influence the execution of a process. Recently, a WS-BPEL extension to handle person-to-person processes has been proposed called BPEL4People [5]. In BPEL4People, users who have to perform the activities of a WS-BPEL business process are directly specified in the process by user identifiers or by groups of people names. No assumption is made on how the assignment is done or on how it is possible to enforce constraints like separation of duties.

WS-BPEL does not provide any support for the specification of authorization policies or of authorization constraints on the execution of activities composing a business process. We believe, however, that it is important to extend WS-BPEL to include the specification of human activities and an access control model able to support the specification and enforcement of authorizations to users for the execution of human tasks within a business process while enforcing constraints, such as separation of duty, on the execution of those tasks [43, 81, 65, 270].

This chapter presents RBAC-WS-BPEL [216], an authorization model for WS-BPEL business processes that also supports the specification of a large number of different types of constraints. Role-based access control (RBAC) (see Appendix A) is a natural paradigm for the specification and enforcement of authorization in workflow systems because of the correspondence between tasks and permissions. In recent years, several extensions to RBAC have been proposed with the goal of supporting access control for workflow systems [7, 43, 270]. However, a role-based model alone is not sufficient to meet all the authorization requirements of workflow systems, such as separation of duty constraints, and binding of duty constraints. Separation of duty exists to prevent conflicts of interest and to make fraudulent acts more difficult to commit. A simple example of a separation of duty constraint is to require two different signatures on a check. Binding of duty constraints require that if a certain user executes a particular task, then this user must also execute a second task in the workflow. This chapter introduces BPCL (Business Process Constraint Language), which can be used to specify authorization constraints for business processes.

The chapter is organized as follow. The next section presents the main proposals about access control for workflow and business process systems. Then, Section 8.2 introduces WS-BPEL and a loan approval business process that will be used throughout the chapter to illustrate the discussion. Section 8.3 defines the components of RBAC-WS-BPEL, including authorization policies and authorization constraints. Section 8.4 discusses how authorization information can be represented in RBAC-XACML. Section 8.5 describes the BPCL language and how it implements the authorization constraints described in Section 8.3. Section 8.6 describes how WS-BPEL can be extended to support the specification of human activities and authorizations and authorization constraints. Section 8.7 introduces an algorithm to evaluate whether a request by a user to execute an activity in a WS-BPEL process can be granted.