A framework for access control in workflow systems

Reinhardt A. Botha
Port Elizabeth Technikon, Port Elizabeth, South Africa
Jan H.P. Eloff
Rand Afrikaans University, Johannesburg, South Africa

Keywords
Access control, BPR, Computer software

Abstract
Workflow systems are often associated with business process re-engineering (BPR). This paper argues that the functional access control requirements in workflow systems are rooted in the scope of a BPR project. A framework for access control in workflow systems is developed. The framework suggests that existing role-based access control mechanisms can be used as a foundation in workflow systems. The framework separates the administration-time and the run-time aspects. Key areas that must be investigated to meet the functional requirements imposed by workflow systems on access control services are identified.

Introduction

The increase of workflow systems in the last decade was largely fuelled by the perceived advantages of streamlining of processes. This is taunted by business process re-engineering (BPR) practitioners in the wake of a global, networked economy. The increased reliance on electronic information, specifically in open environments such as the Internet, has caused information security research to rapidly increase over the past decade. One of the aspects of information security that received increased attention is access control. Several researchers recognized the functional difference required of access control in the workflow environment (Atluri and Huang, 1996; Bertino *et al.*, 1999; Long *et al.*, 1999). The solutions proposed by them cover technical implementation aspects or provide formal models. It neglects, however, to provide a holistic framework for discussing access control in workflow systems.

This paper proposes a framework wherein access control in workflow systems can be studied. The framework addresses not only the technical enforcement aspects, but also the administration and operational aspects of access control in workflow systems. Figure 1 graphically depicts two spheres, an access control and a workflow sphere, evident in the proposed framework.

Both the workflow and access control spheres consist of a conceptual design requirement level and a technical enforcement level relating concepts within the fields of workflow and access control respectively. This paper will investigate the interaction of the access control sphere and the workflow sphere. In Figure 1 the interaction of the workflow and access control spheres is depicted by an arrow marked with a question mark. We first examine each of the spheres. Thereafter a framework for addressing access control within the workflow environment is presented by exploring the interaction between the various components identified in the two spheres.

Spheres in the framework

The workflow sphere

Developments such as the Internet have a profound impact on the way that organizations do business. Companies embrace such challenges in different ways, but ultimately it results in a strategic alignment phase (Garber, 1999). In this phase organizations are likely to redefine or reinvent their business (Brandau *et al.*, 1999). This will entail the redefinition of existing business processes, the introduction of new business processes and the general revamp of procedures and policies. These activities are often referred to as BPR (Davidson, 1993).

Business process re-engineering projects can be approached from various perspectives (Earl *et al.*, 1995). From an information technology perspective, two approaches are of interest. A "systems" strategy refers to an approach where systems analysis is central to the BPR exercise. An "engineering" strategy emphasizes the optimization of flows of work through the coordination and scheduling of interdependent tasks. The interrelation of these two approaches is interesting. Information systems present the core mechanism for facilitating information flow in organizations. Although the emphasis may differ according to the approach, it is inevitable that certain activities in the "systems" strategy and the "engineering" strategy are inseparable. A "systems" strategy will require the identification of the

Information Management & Computer Security
9/3 [2001] 126–133

[ISSN 0968-5227]

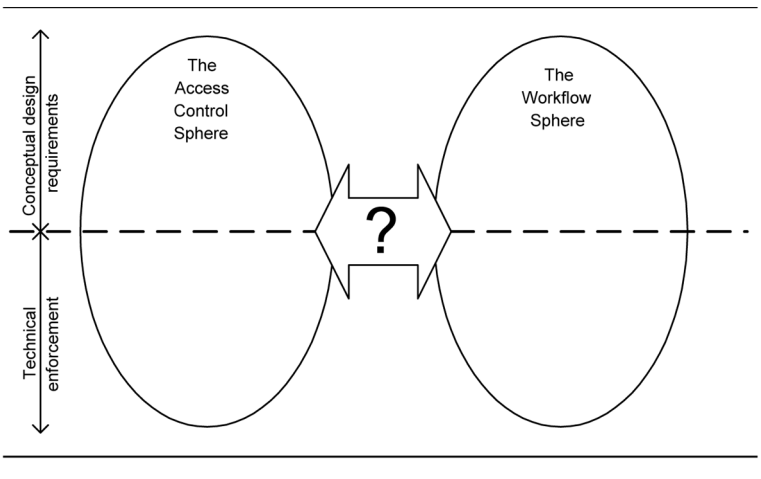
Information Management &
Computer Security
9/3 [2001] 126–133

user's activities (an integral part of the "engineering" strategy), whilst the "engineering" strategy will also investigate the development of systems (the core of the "systems" strategy) that support the coordination of the activities. This paper adopts a middle-of-the-road approach by emphasizing the interrelation of these two approaches.

Against this backdrop, the existence of a magnitude of methodologies, tools and techniques in BPR (Kettinger *et al.*, 1997) is not surprising. Application of these methodologies, tools and techniques in BPR allows us an extended scope to traditional industrial engineering (Evans *et al.*, 1999). The "width" scope of a BPR project is concerned with the flow of products, information and other resources. Its prime objective is to identify the enablers that speed up the flow. The "breadth" scope of BPR determines how far reaching the impact is: across work processes, business processes, supply chains and holonic networks (Evans *et al.*, 1999). The "depth" scope of the BPR project considers the impact on the roles and responsibilities, the measurements and incentives, the organizational structure, the shared values, the workforce skills and the information technology influencing the people in the business. This three-dimensional scope of BPR is represented in Figure 2 by the three sides of the cube.

Workflow systems provide an information technology solution particularly aimed at the "computerized facilitation or automation of a business process, in whole or part" (Hollingsworth, 1995). This definition of workflow systems captures the correspondence between the classic concept of "workflow" which is understood to be "the set of sequences of activities which represent the functioning of an organization" (Khandwalla, 1977) and that of business processes, that is, of "a structured set of activities designed to produce a specific output for a specific market" (Davenport, 1995). Business process re-engineering can thus be seen as the conceptual reconstruction of an organization to be more efficient. Workflow systems, in turn, provide part of the technology infrastructure required for the implementing and facilitation of this move towards greater efficiency in the business. In Figure 2 the arrow between the information technology depth scope of BPR and the technical enforcement level of the workflow sphere depicts this relationship.

Figure 1
Spheres of interest



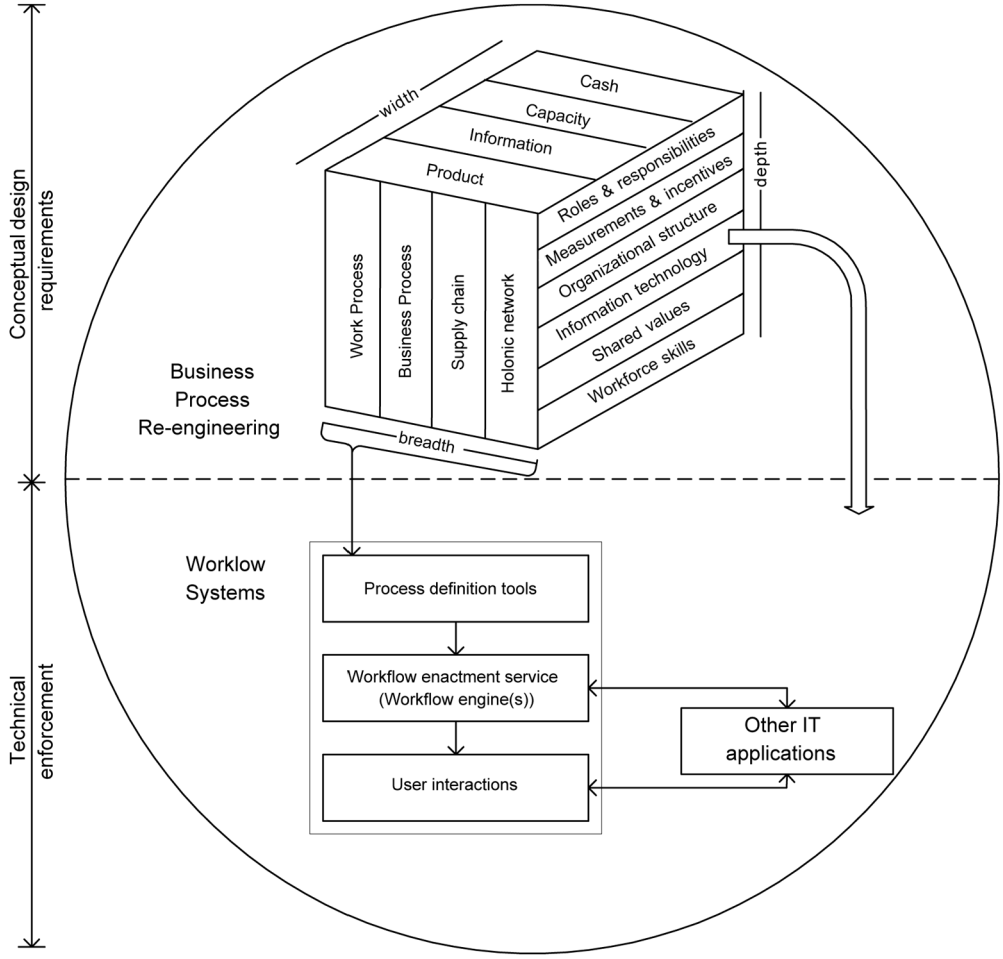
The components of a workflow system are depicted on the technology level of the workflow sphere in Figure 2. The following components can be observed:

- *Process definition tools* are concerned with the defining and modeling of the business process and its constituent tasks. The computerized representation of the business process is called the process definition. A process definition consists of task definitions linked together by business rules. These process definitions may span the entire breadth of the BPR impact, i.e. it may cover internal processes or business processes that span a supply chain.
- *The workflow enactment service*, consisting of one or more workflow engines, is concerned with the management of the business processes in an operational environment. At run-time, the process definition is interpreted by the workflow engine, which is responsible for creating and maintaining process instances. Task instances will be maintained for the tasks that are created based on the process definition and interpretation of the business rules. Tasks will be allocated to users or applications.
- *User interaction* typically occurs through a worklist. The instantiated tasks are communicated to the relevant end-user through a worklist. Other IT applications may be invoked in order to complete the task.

The access control sphere

BPR is likely to emphasize the importance of an organization's information resources. This results in a greater awareness of information security. Information security objectives are not only attained through technical controls, but also through operational controls (von Solms, 1999). As far

Figure 2
The workflow sphere



as technical controls are concerned information security relies on five essential services: identification and authentication; access control; integrity; confidentiality; and non-repudiation (ISO, 1989). Identification and authentication, confidentiality and non-repudiation are implemented in ways similar to non-workflow systems. The access control and integrity services require special attention. Semantic integrity, in particular, refers to the consistency of the information with business rules. This is often achieved with the assistance of the access control service. For example, the business rule that states, "a person may not approve his own purchase order" requires the access control service to deny "approve" access to the initiator of the purchase order. The access control service was therefore chosen as focus area for this paper.

The access control sphere depicted in Figure 3 represents the concepts and components related to the access control service.

Access control is concerned with controlling the access permissions of a user to an object. Users may be actual people or the processes and agents acting on their behalf. Objects represent anything of value that requires protection and forms part of an information system. Documents, directories and database records are examples of objects. The access permissions may be specified according to the semantics of the objects that it relates to. For example, the access permissions associated with an account object may be debit and credit, whilst the access permissions associated with file may be read, write and delete. Unique user and object identifiers represent the minimum information that is required before a technical enforcement strategy can be discussed. An access matrix maps access permissions between users and objects.

The allocation of access permissions to users is governed by organizational policy. The organizational policy describes "how things are done around here". It will

determine whether a discretionary or mandatory access control administration paradigm will be used. Organizational policy will typically dictate permissions be granted according to the least privilege principle, i.e. a user will receive the minimum permissions to perform his job. A manager, for example, may only view the salaries of staff reporting to him. Separation of duty is another example of organizational policy. A typical separation of duty policy may state that a user may not approve his own purchase order. Organizational policies are expressed at the conceptual level. The abstractions used on the organizational policy level and the information available on the information level, however, may not match. For this purpose, access control mechanisms often use additional information that corresponds more closely to the policies that must be supported. Multi-level models typically classify the information and users, using this classification information to base their access decisions on. Role-based access control (RBAC) introduces the abstract notion of a role to facilitate access control.

RBAC is fast becoming a *de facto* standard in industry and as such is implemented in various commercial applications. RBAC users are associated with roles, while roles are associated with permissions. A user thus receives access permissions based on the roles that he may assume. The session concept in RBAC allows a user to activate only a required subset of his roles, and thus a subset of permissions, at a given time.

The technical enforcement can only be seen as effective if the necessary operational controls are in place. Operational controls can be seen as procedures that must be enforced. It may, for example, describe the steps to be followed when a user resigns from his current position, or when he is promoted. Such controls may depend on the behavior of users and thus cannot totally be enforced technically.

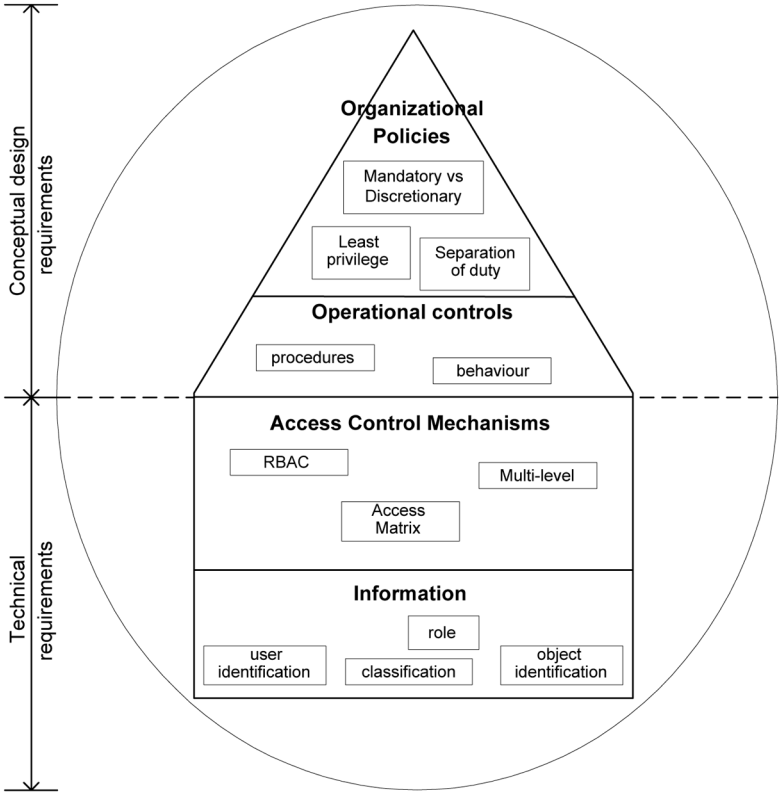
Figure 3 depicts that the policies and operational controls fall within the conceptual design level of the sphere, whereas the mechanisms and information is situated on a technical enforcement level.

If the influence of BPR is not considered the access decision is static in the sense that it always yields the same result for a specific user and a specific object. This would imply that a user who may approve a purchase order could do so regardless of who initiated such purchase order. This leads to the following questions:

- Can a user approve the order before quotes have been obtained?
- Can a user, who may approve orders, approve an order while he/she is busy generating the order?
- Can a user approve the order of a family member?

When the access control decision is static, the answers to the above questions are yes. This is, however, undesirable. The following paragraph discusses how this situation can be rectified by considering the interaction between the two spheres.

Figure 3
The access control sphere



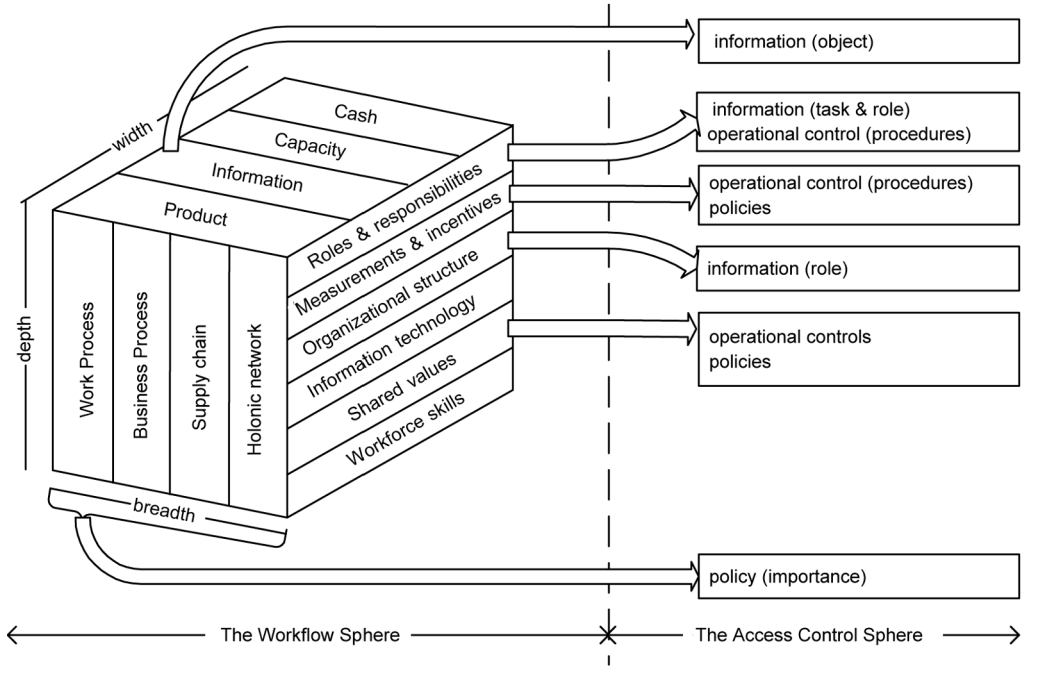
Interaction between spheres

Figure 4 depicts the interaction of BPR as positioned in the workflow sphere on the access control sphere.

First, consider the width scope of a BPR project. Information technology will primarily be used for facilitating the flow of information. Optimizing information flow could aid in radical changes as far as the utilization of the other resources in the breadth dimension is concerned. A BPR project will therefore have to identify the information that requires protection.

Second, the breadth scope of a PBR project would determine the importance of access control within the environment. The importance of access control increases

Figure 4
BPR impact on access control sphere



proportionally to the number of communicating partners in the business processes. The process's constituent tasks are performed by different people. Each task requires different access permissions to complete. The importance of access control increases proportionally to the number of communicating partners in the business process. When the process involves the complete supply chain, access control is likely to be found more important than when considering a process involving a small internal group of people. The perceived importance of access control will determine the extent to which it is governed by organizational policy.

Finally, consider the depth dimension of the BPR project. As previously mentioned, the effective technical enforcement of access control is reliant on operational controls. The effectiveness of these operational controls is largely a human issue. It is thus important that the people involved must commit to make the controls work. The BPR project must therefore address the "shared values" that must be instilled in the people participating in the business processes. These "shared values" are mainly communicated through organizational policies and procedures. In order to determine the success of the newly established policies and procedures the "measurements and incentives" aspects of the depth dimension of the scope of a BPR project must be considered. On a more practical note, the example of an employee resigning can be cited. The revocation of access permissions from the resigning employee thus needs to be controlled and managed by any number of systems administrators. This could, however, also be seen as an impact of access control on the BPR project. It may require the definition of a workflow that facilitates or coordinates the actions required by whichever employees. In the cited example, certain of the activities that currently are performed manually could even be automated.

BPR projects will impact on the jobs of people, i.e. their "Roles and responsibilities" in the organization. A person's responsibility will directly reflect on his access permissions. The concept of least privilege requires that no user should receive more access permissions than what is necessary to do his/her job. This will thus have an operational impact on the security administrators who will have to ensure that the information is kept up to date and in line with job descriptions. It also has a significant impact on the technical enforcement of access control. RBAC, for example, has proven popular, particularly in workflow systems. This is due to the close correspondence of the abstractions used in RBAC mechanisms to the concepts of "roles and responsibilities" and "organizational structure".

If the influence of the three dimensions of BPR is carefully considered, three conceptual design requirements that distinguish access control in workflow systems from access control in non-workflow systems can be identified. These are: strict least privilege, order of events and separation of duty. For the purpose of this paper these three requirements are collectively called context-sensitive access control.

1 *Strict least privilege*. The concept of least privilege acknowledges that a user should only receive access permissions that are in line with his or her job responsibilities. It does not however, recognize that those permissions may at specific times be inappropriate and unnecessary. For example, a manager who initializes a purchase order should not receive, at the initialization stage, the permission to approve the purchase order. Strict least privilege is proposed as a strengthening of the least privilege concept in that it distinguishes between a person's job and the tasks that a person must fulfill as part of his job. Strict least privilege therefore states that a user should receive the smallest possible set of permissions for the current task within the business process.
2 *Order of events*. Order of events is mentioned in current literature as a shortcoming of pure RBAC models (Sandhu *et al.*, 1996; Nyanchama and Osborn, 1999). Certain permissions can only be granted once others have been exercised. For example, an order cannot be approved until filled out completely; similarly, once the order has been approved, it may not be edited again.
3 *Separation of duty*. Although there will always be a human element involved with the enforcement of policies and procedures, technical enforcement should be attempted as far as possible. One such example is the well-known separation of duty policy requirement. Separation of duty has as its primary objective the prevention of fraud and errors, thus ensuring the semantic integrity of business information. Separation of duty requirements are often formulated as business rules such as "a person may not approve his own purchase order" or "a cheque requires two different signatures". In this case, the access control service should be sensitive to the access history of the relevant objects and appropriately disallow access.

This paragraph showed that the interaction of the workflow sphere and the access control sphere warrants special attention. The next paragraph presents a framework wherein the identified access control requirements can further be studied.

The framework

Figure 5 depicts the context-sensitive access control in workflow environments (CoSAWoE) framework. This framework uses the conceptual design requirements identified in the previous paragraph and information regarding the organizational structure and the business processes identified in BPR as inputs. This represents the conceptual design requirements for an access control service.

The CoSAWoE framework is positioned so as to provide an environment for the technical enforcement of access control. Due to its popularity in both industry and research, RBAC has been chosen as the foundational access control mechanism in the CoSAWoE framework. Figure 5 shows that this framework has an impact on the RBAC mechanism, as well as on the workflow system.

The CoSAWoE framework is depicted as consisting of two parts. The administration time part considers impacts when the administrative tasks in the environment are performed, whilst the run-time part suggests concerns while the business process is facilitated by the workflow system. Consider each of the CoSAWoE parts in turn.

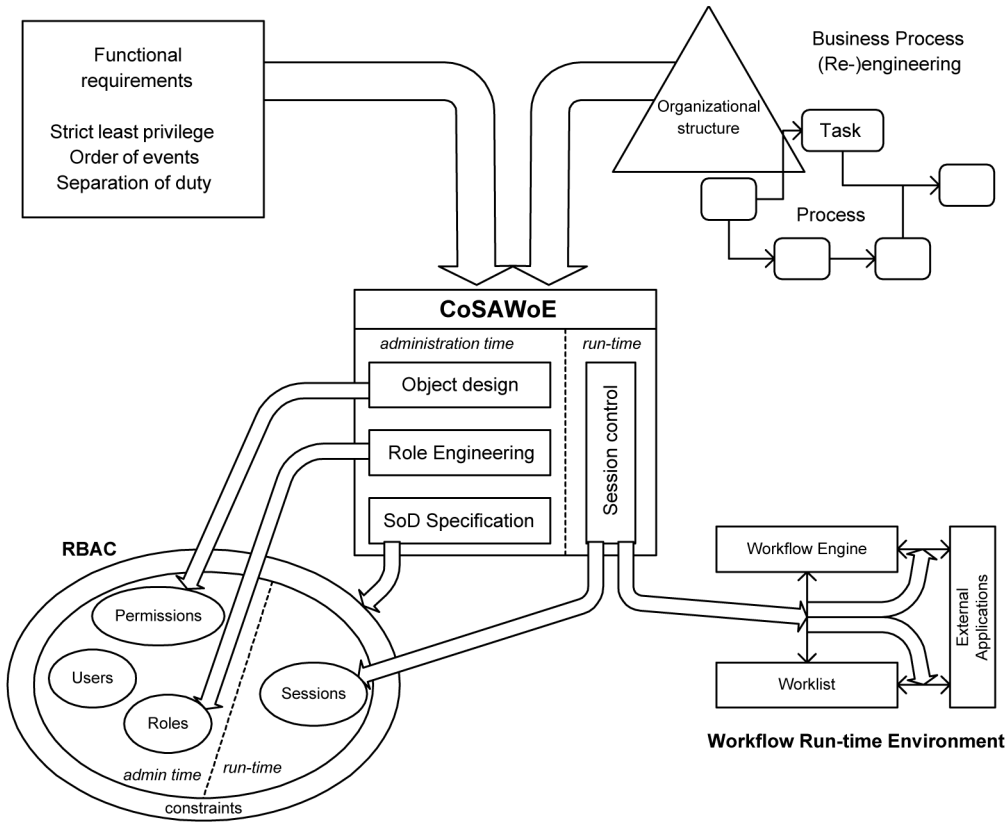
Administration time

The administration time aspect is concerned with ensuring that the environment is susceptible to the technical enforcements that are suggested. In terms of the design of the framework three aspects need attention. In the first place, it needs to be established what needs to be protected (the objects) and to what degree protection should occur. The second aspect specifies from whom the objects must be protected. This protection is often described in terms of the organizational positions, which relate to the role-concept in role-based access control models. This aspect is described as role engineering. Finally, an aspect relating to the expression and formulation of SoD requirements is described.

Object design

In order to achieve strict least privilege protection must occur at a detail level within the object. This results in abstract permissions that are tied to the semantics of the object. For example, the approve permission for a purchase order document

Figure 5
CoSAWoE framework



would require view permission on a certain part of the document, whilst the write permission is permitted on other portions of the document. These permissions would for administration purposes not be granted as read and write of specific parts of the object. Instead, the abstract permission, "approve purchase order" will be granted. For effective administration, a balance between the level of detail (administration effort) and the level of abstraction (administration ease) must be found. The design of objects and their related permissions (which equates to the available methods) must therefore receive attention.

Role engineering
The concept of a role relates to the typical hierarchical structure of an organization. Role hierarchies, as part of RBAC, do not directly support concepts such as reporting structure. A senior clerk role may be superior to a junior clerk role. This, however, only reflects on the responsibilities of users associated with those roles and does not necessarily reflect the reporting structure. Junior clerks, for example, may report to the same manager as senior clerks. The proposed framework thus needs to reflect the design of role structures to allow for the specification of more complex relations between organizational positions than only inheritance of access permissions.

SoD specification
In order to enforce SoD policies, abstractions that can be used by the technical enforcement environment need to be introduced. Moreover, the consistency of these policies should be checked against each other. For example, the requirement that at least two users must be involved in a business process requires that the process definition be examined to determine the roles and the possible users that can perform the task. Further enforcement can then be applied in the run-time environment.

Run-time
At run-time the access control mechanism is concerned with two aspects: the enforcement of strict least privilege and the enforcement of policies. This is achieved by controlling the user's sessions. In a session a user is associated with a specific subset of the roles that may be granted to him. The user thus receives only a subset of the permissions associated with roles that he may assume. In order to ensure strict least privilege, the user must not be granted privileges outside of the context of the task that he currently works

on. An application, for example, must not be launched to view a document with no relevance to the task. The enforcement of access control policies, such as separation of duty, will furthermore require the workflow engine to interpret the access history of objects during that instance of the process. This would require the worklists to correctly reflect who may perform the activity.

Conclusion

This paper argued that the scope of a BPR project provides a foundation for determining the effect of workflow on access control. Three properties that summarized the functional access control requirements in workflow systems were presented. A framework based on RBAC was presented. The administration-time and run-time aspects that must be considered in order to meet the access control requirements of workflow systems were highlighted. The proposed framework showed that workflow systems require special interpretation of RBAC concepts. The framework also suggests an influence on the run-time components of the workflow system.

The framework allows for discussion of existing work from a more holistic perspective. The framework furthermore provides the opportunity to identify the inter-relation between work which, at first sight, may seem to have nothing in common.

References

Atluri, V. and Huang, W-K. (1996), "An authorization model for workflows", *Proceedings of the Fifth European Symposium on Research in Computer Security*, Rome, pp. 44-64.

Bertino, E., Ferrari, E. and Atluri, V. (1999), "Specification and enforcement of authorization constraints in workflow management systems", *ACM Transactions on Information and System Security*, Vol. 2 No. 1, pp. 65-104.

Brandau, R., Confrey, T., D'Silva, A., Matheus, C.J. and Weihmayer, R. (1999), "Reinventing GTE with information technology", *IEEE Computer*, Vol. 32 No. 3, pp. 50-8.

Davenport, T.H. (1995), *Process Innovation: Re-engineering Work through Information technology*, Harvard Business School Press, Boston, MA.

Davidson, W.H. (1993), "Beyond re-engineering: the three phases of business transformation", *IBM Systems Journal*, Vol. 38 Nos 2 and 3, pp. 485-99.

Earl, M.J., Sampler, J.L. and Short, J.E. (1995), "Strategies for business process reengineering: evidence from field studies", *Journal of Management Information Systems*, Vol. 12 No. 1, pp. 31-56.

Evans, G.N., Mason-Jones, R. and Towill, D.R. (1999), "The scope paradigm of business process re-engineering", *Business Process Management Journal*, Vol. 5 No. 2, pp. 121-35.

Garber, L. (1999), "IT must focus on transforming business for e-commerce", *IT Professional*, Vol. 1 No. 6, p. 88.

Hollingsworth, D. (1995), *The Workflow Reference Model*, Document Number TC-00-1003. Issue 1.1. Available from www.wfmc.org

ISO (1989) *ISO 7498-2: Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

Kettinger, W.J., Teng, J.T.C. and Guha, S. (1997), "Business process change: a study of methodologies, techniques, and tools", *MIS Quarterly*, Vol. 21 No. 1, pp. 55-80.

Khandwalla, P.N. (1977), *The Design of Organizations*, Harcourt Brace Jovanovich Publishers, New York, NY.

Long, D.L., Baker, J. and Fung, F. (1999), "A prototype secure workflow server", *Proceedings of the 15th Annual Computer Security Applications Conference*, Radisson Resort Scottsdale, Phoenix, AZ, pp. 129-38.

Nyanchama, M. and Osborn, S. (1999), "The role-graph model and conflict of interest", *ACM Transactions on Information and Systems Security*, Vol. 2 No. 1, pp. 3-33.

Sandhu, R.S., Coyne, E.J., Fenstein, H.L. and Youman, C.E. (1996), "Role-based access control models", *IEEE Computer*, Vol. 29 No. 2, pp. 38-47.

von Solms, R. (1999), "Information security management: why standards are important", *Information Management and Computer Security*, Vol. 7 No. 1, pp. 50-7.