Activity based security in intranet and internet workflows

Thomas A. Kindler

Institute of Parallel and Distributed High-Performance Systems (IPVR)
University of Stuttgart, Breitwiesenstr. 20-22, D-70565 Stuttgart, Germany
e-mail: kindler@informatik.uni-stuttgart.de

Abstract - *This paper deals with a model to support security requirements of intra-/ internet based workflows. The model is emerged from deficiencies of today's security models in the context of workflows. The basic idea is the consideration of time that extends subject-object based or role based access control models. Access control should be modeled in the context of workflows and their activities and is leading to activity based access control (ABAC). As a result access control will be defined in conjunction with workflows instead of defining them implicitly in enterprise policies.*

1. Introduction

Due to the increasing effort of large organizations, like international companies and public administration, in business process reengineering, the introduction of intranet solutions and workflow management systems becomes more and more attractive. It is very important to ensure the security requirements which result from business processes in those distributed environments. In small organizations it is feasible to ensure security requirements due to homogeneous security environments. In larger and more heterogeneous environments or in case of inter-enterprise business processes via the internet, however, administration and maintance of security is complex, costly, and susceptible to attacks.

This paper presents a solution based on activity based access control (ABAC). The next section introduces security requirements from the business process point of view. Section 3 discusses the suitability of common access control models for these requirements. Section 4 proposes the activity based access control model. Finally, in section 5 a conclusion is given.

2. Security requirements of workflows

Workflow management [3] [9] is not a baseline technology but a high-level application that integrates and coordinates different business applications or business objects [2]. During enactment of workflow instances the workflow system schedules distinct activities in a sequential and/or parallel order to make the business processes go on. An activity is made up of three parts: a job, an actor to execute the job, and an execution context. The job describes what should be done. The actor is not necessarily a single person, it can also be an application, or groups of them. The execution context specifies which data is relevant for the activity, which resources ought to be used etc. Which impact do workflow systems have on access control? Two important aspects should be examined closer:

Aspect of time: Due to dynamic resource assignment in workflow management systems, it must be guaranteed that during lifetime of an activity appropriate access permissions are granted to the actor. It should be considered that the actor and the objects in an activity context are not known in advance. They will be assigned by the workflow management system while scheduling the activity.

Aspect of domains: Real world business processes and related resource access do not end at boundaries of intranets, enterprises or security domains. They demand continuous workflow support across boundaries. Not only process instances must be able to cross such boundaries, also access to objects must be possible across those boundaries in the context of workflow instances. Of course, this access must be well defined and controlled. In the next section common access control models will be reviewed under consideration of both aspects.

3. Access control models

The purpose of access control [1] [5] [8] is to limit operations that authorized users of computer systems can perform. Access control constrains the actions a user can do directly, as well as what programs executing on behalf of the user are allowed to do. In this way access control tries to protect enterprises from operations that break security policies.

3.1. Subject-Object based access control

The subject-object based access control model was introduced in [4] as an access control matrix. The model introduces three terms: subjects, objects and an access function (see figure 1). The access function is enforced via a reference monitor. How does subject-object based access control fit into the requirements of section 2?

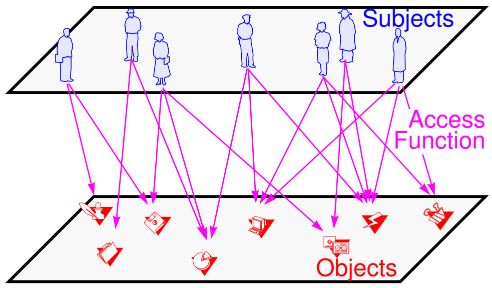

Figure 1: Access paths and abstraction layers in subject-object based access control

Aspect of time: The permissions in subject-object based access control are defined in context of the subjects and/or objects without considering any other context like activities or other dynamic time constraints.

Aspect of domains: Due to very close attachment of access control information to subjects and objects, subject-object based access control is not independent from security domains and the access control mechanisms used. Therefore it cannot be used to model access control in inter-enterprise workflows.

Hence subject-object based access control seems to be inappropriate for workflow relevant requirements.

3.2. Role based access control

Role based access control (RBAC) extends subject-object based access control by an additional abstraction layer: *roles* (see figure 2). A role defines the authority, responsibility and/or competency of subjects concerning objects. The relationships which subjects belong to a role and which permissions these subjects have on objects are independent and can be changed over time. A more detailed discussion on role based access control models and their advanced features can be found in [6] and [7]. How does role based access control fit into the requirements of section 2?

Aspect of time: Roles are improving and simplifying the administration of access control. But the role concept cannot be applied to realize the time dependent requirements of workflow activities without counteracting the basic ideas of role based access control.

Aspect of domains: Workflow enactment between different security domains can be supported by the additional abstraction layer of roles in RBAC. There must be an agreement on a set of roles which can be used between the cooperating security domains. The agreement must include a common understanding of the roles' semantics, but it does not depend on the access control mechanisms used in each security domain.

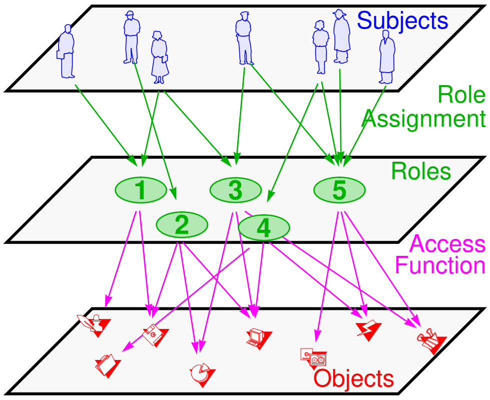

Figure 2: Access paths and abstraction layers in role based access control

4. Activity based access control

On account of deficiencies of other access control models, a model of activity based access control (ABAC) is proposed in this paper. The model introduces an additional abstraction layer: *activities* (see figure 3).

4.1. ABAC model

In the ABAC model an activity A is based on the following four components. An activity consists of many more components, but these four are the relevant components for ABAC:

- t_{start} : Time when the activity is scheduled by the workflow management system.
- $actor$: A subject, a group of subjects, or an application which is assigned to the activity.
- P : A set of permissions for the object O which is in the context of activity A.
- t_{end} : Time when the activity is completed by the $actor$ or terminated by the workflow management system.

In figure 3 the activity based access control model is shown. Roles are not mandatory to the ABAC model. An access from the subject S_x to an object O_y is valid in ABAC if the following conditions are fulfilled: 1. S_x must be an valid $actor$ of activity A_z and O_y must be in the activity context of activity A_z. 2. For access time t_{access} the equation: $t_{start}(A_z) \le t_{access} \le t_{end}(A_z)$ must be valid. 3. The permissions in $P(A_z)$ must grant the requested access of S_x to O_y. If all conditions are fulfilled the access from subject S_x to object O_y will be granted by ABAC. In figure 3 you can see that S_i only can access O_j within the time beginning at $t_{start}(A_b)$ and ends in $t_{end}(A_b)$.

How does ABAC fit into the requirements of section 2? *Aspect of time:* The activity concept in ABAC fits into the aspect of time of workflow management systems. Only necessary access to the objects in the activity context will be granted to actors of scheduled activities. Delegation and vacation replacement can be supported by ABAC as well. If ABAC is integrated with workflow management systems no additional effort is needed to manage access control.

Aspect of domains: ABAC can support inter-domain workflows. Between cooperating domains a mutual agreement must exist on workflows and the relevant security specification. The agreement must include a common understanding of workflow definitions, activity definitions and security specifications but it does not matter which activity implementations and security mechanisms are used in each domain. Finally, ABAC fits best to the workflow requirements compared to other access control models.

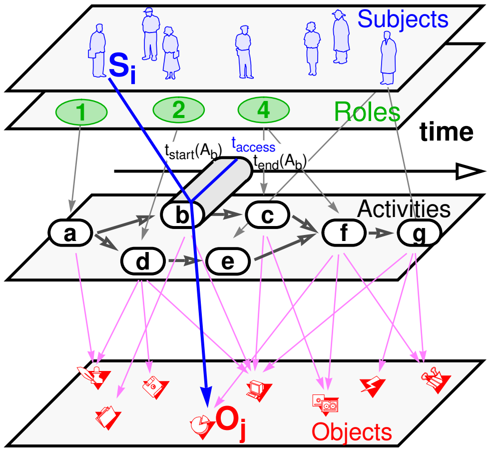

Figure 3: Access paths and abstraction layers in activity based access control

4.2. Implementation details

To use ABAC in a real world workflow environment, the following workflow management system and security domain components must be adapted:

Workflow language - A security extension of the workflow definition language is necessary to define workflow related security. The language extension must be independent of security domain specific access control mechanisms. This independence offers the opportunity to define workflow security without considering the runtime environment, which can differ between distinct workflow instances of the same workflow definition. The workflow definition language of the current prototype implementation is extended by security attributes. Security attributes are used to express security from the business process point of view. An attribute consists of a name, a security semantics and a range of workflow definition elements to which it can be applied.

Workflow management system - The workflow management system must be enabled to enforce security attributes of the extended workflow definition language. The workflow system must check and enforce the security attributes against the security domain where the activity is scheduled: 1. Does the security domain support the security attributes? 2. Is the selected *actor* authorized for the activity? 3. Setup (at t_{start}) the security domain specific access mechanisms and access rights between the actor and context objects. 4. Set (at t_{end}) the access rights depending on the security attributes.

Security domain - Each security domain where ABAC is used needs security brokers which manages security attributes and convert them to appropriate access control mechanisms. For security attributes in workflow definitions, the security broker needs to know how to interpret the semantics of these attributes. The definition of security attributes in the workflow environment and the mapping between these definitions and access control mechanisms can be seen as a contract between the workflow environment and the security domain. Based on such contracts, workflow instances or parts of them can be executed with appropriate security in those security domains.

5. Conclusion

The model outlined satisfies fundamental requirements of activity driven environments. Two important aspects, the aspect of time and the aspect of domains, are addressed by this model. ABAC extends conventional access control models and simplifies the modeling of access control in activity and process driven environments. Activity based access control introduces an additional abstraction layer and a new dimension in access control. The new abstraction layer is the consideration of activities as entities in access control and the new dimension is time. The proposed model is a step towards activity based access control in workflow environments for large enterprises, intranets and the internet. Currently a prototype implementation based on the SWATS-PoliFlow workflow system [9] is realized to validate the applicability of ABAC.

I acknowledge financial support from the project PoliFlow which was funded by the German Secretary for Education, Science, Research, and Technology (BMBF). I also acknowledge the contribution of my colleagues to the work discussed in this paper.

References

[1] Abadi, M., Burrows, M., Lampson, B., and Plotkin, G. (1993). A Calculus for Access Control in Distributed Systems. *ACM Transactions on Programming Languages and Systems*, 15(4):706–734.

[2] Curtis, B., Kellner, M. I., and Jim, O. (1992). Process Modeling. *Communications of the ACM*, 35(9):75–89.

[3] Georgakopolulos, D., Hornick, M., and Sheth, A. (1995). An Overview of Workflow Management: From Process Modeling to Workflow Automation Infrastructure. *Distributed and Parallel Databases*, pp. 119–153.

[4] Lampson (1971). Protection. Proc. *Fifth Princeton Symposium on Information Sciences and Systems,* March 1971. Reprinted in Operating Systems Review, 8,1, January 1974, pp. 18-24

[5] Lin, P. and Lin, L. (1996). Security in Enterprise Networking: A Quick Tour. *IEEE Communications Magazine*

[6] Lupu, E. C., Marriott, D., Sloman, M. S., and Yialelis, N. (1995). A Policy Based Role Framework For Access Control. In *First ACM/NIST Role Based Access Control Workshop*.

[7] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). Role-Based Access Control Models. *IEEE Computer*, February:38–47.

[8] Sandhu, R. S. and Samarati, P. (1994). Access Control: Principles and Practice. *IEEE Communications Magazine*

[9] Siebert, R., Kindler, T., and Soyez, T. (1997). Integrated Workflow and Telecooperation Support for the German Government. In *12th Annual Symposium on Applied Computing (SAC'97)*