Modelling Security for Integrated Enterprise Workflow and Telecooperation Systems

T. Kindler, T. Soyez

Institute of Parallel and Distributed
High-Performance Systems (IPVR)
University of Stuttgart
Breitwiesenstr. 20-22, D-70565 Stuttgart, Germany
Email {kindler,soyez}@informatik.uni-stuttgart.de
Fax +49 711 7816 424

Abstract - *Inside and between widely distributed (parts of) organizations is a growing need for integrated solutions of workflow management systems and telecooperation tools to support business processes overall in an efficient way. In this paper we discuss two important aspects, concerning the security in such an environment. One problem is the heterogeneity of security platforms with different mechanisms and policies. The second problem we want to talk about are security aspects when using teleconferencing in the context of business processes. We present a first approach for a platform independent security model, based on the idea of dynamic mapping of security requirements of a business process to real world security environments.*

Key Words - *Enterprise Security, Security Models, Telecooperation, Workflow, Teleconferencing*

1. Introduction

The IPVR is involved in a project of the research program POLIKOM which was funded by the german secretary for education, science, research, and technology (BMBF). The research program has been initiated after the decision of the government to move parts of the administration from the former capital Bonn to the new capital Berlin. The mission of the POLIKOM projects is to close the arising gap between the departments of the german government, as in the future they are spatial widely distributed over both cities.

Our POLIKOM project is called PoliFlow and one of its aims is to develop an integrated telecooperation infrastructure which supports workflow management across heterogeneous (security) platforms as well as teleconferencing between Bonn and Berlin.

Workflow management is necessary to hold control over the intra and inter department business processes. Teleconferencing is necessary to improve the quality of the workflow processes through the possibilities of enabling spontaneous checkbacks and planned meetings directly from the desktop.

One major research issue we found out during the investigation of user requirements is the problem to guarantee confidence and access control rights to users who are working in the integrated and widely distributed workflow and teleconferencing environment.

2. Security Requirements

In this paper we want to consider two aspects of security. On one side we look at requirements resulting from asynchronous workflow management across multiple security environments. On the other side we want to focus on requirements which arise by integrating synchronous telecooperation in workflow management systems.

Workflow driven requirements for enterprise business processes

If we want to model workflows which have impact on several departments or other organizational units, we have seen that a lot of entities have their own security domain and all the different domains have also different security mechanisms and policies. For that reason the usage of domain specific security mechanisms in a process definition would make the workflow definition inflexible. If the underlying security environment changes, such process definitions could not be initiated anymore and would have to be adapted to the new security environment.

Teleconferencing driven requirements for business processes

Today most teleconferencing systems do not support possibilities to realize any confidence status or security policies within a conference context, e.g. if application sharing is supported by the teleconferencing system every participant can share any application to everybody and grant data access via input control.
This behavior is unsuitable for intra and inter enterprise teleconferencing in the context of business processes, especially in confidential parts of a workflow instance. If access rights are only granted to specific persons or roles these persons are not necessarily allowed to share this access rights via teleconferencing to arbitrary persons inside or outside the own organization.
This means that on the one hand teleconferencing tools must be enabled to consider the requirements from the security environment. On the other hand the business process definition has to be extended by the possibility of modelling the special aspects of integrated teleconferencing.

3. Solution Approach

Our approach is based on the idea of a platform independent security model. Therefore the process definition (activities, roles, documents, ...) has to be extended by elements for the description of security aspects associated with workflow activities, documents etc.
Furthermore for each security environment there has to be a mapping of these security constraints into mechanisms of the given platform. In cases where the target environment does not fit the needs for security, an exception handling is necessary. One way of handling exceptions is the generation of an event to notify responsible persons. Another way is to integrate exception actions already in the process definition. In this case, the system has the possibility to avoid manual interaction by using predefined alternatives for the further processing of the workflow.
During the runtime of a business process instance the mapping of the security constraints of the workflow definition will be done dynamically step by step.

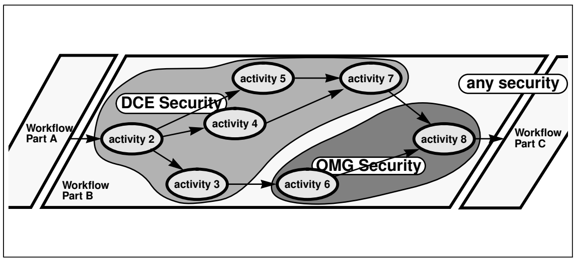

Fig. 1: Example of a workflow which was processed within different security environments

This concept supports also security requirements when using synchronous telecooperation tools in the context of workflow processing. The idea is to define security relations for teleconferencing (e.g. „x is allowed to share doc1 with y“) between the roles in a business process definition.

4. Conclusion

The growing number of computers in industry and administration and the distribution of organizations all over the world lead to a lot of challenges in supporting business processes across multiple locations in an user-friendly and efficient manner. In this paper we have talked about some of these challenges concerning intra and inter enterprise security aspects. We explained problems arising from the existence of different security environments and we discussed security requirements driven by the integration of tools for synchronous telecooperation with workflow management systems. Finally we outlined a possible approach how these both problems can be solved. Currently we are working on the definition of the abstract security layer and the runtime mapping into workflow environments based on DCE and CORBA.