Towards Security Semantics in Workflow Management

Gaby Herrmann, Günther Pernul
University of Essen, Department of Information Systems, Germany
{herrmann|pernul}@wi-inf.uni-essen.de

Abstract

In the past few years workflow management has become an important topic both, for the research community as well as for the commercial arena. One important topic which has been treated at less detail so far is providing security and integrity in workflow management. The main goal of this paper is to study what kind of security requirements need to be enforced during workflow management and which components of a workflow are effected by appropriate security measures.

1. Introduction

Most work about security and integrity in workflow management use a very narrow definition of security and integrity. They try to adapt authorization and access control methods as used in operating or database systems to the special need of workflow management. An example is [6]. At least in the opinion of the authors of [3] such models are only partially applicable to workflow management. One step forward in the development of a security and integrity model for workflow management is given by [1], [2] and [5]. [2] has developed the Policy Resolution Model, which main emphasis is on authorization and access controls, too. [1] describes possible dependencies of tasks with different security levels and a method of their execution. In [5] special concern is devoted to acitivity management only. The work discussed above focuses on specific areas of workflow security only while a general discussion and a broader coverage is still missing. In our ongoing research we are developing an architecture to realize all possible security and integrity requirements in workflow management. The architecture covers the whole range of workflow security - from modelling security semantics of applications to suggesting appropriate software modules for their realization.

2. Architecture

Security semantics are defined as all security relevant knowledge of the application domain. A domain expert will analyse business processes of the application domain and specify its informational, functional, dynamic, organizational, and workflow aspects by following a methodology and using certain modelling tools. Analysing, modelling, and realization of the security semantics of a business process is supported by the following framework [4]: The framework consists of a three-layered architecture. The top layer contains well-defined concepts used to represent the security semantics of the real world. The domain expert may use these concepts to express the security requirements of the business process under consideration in one of the five different perspectives. In a real world application domain experts are not necessarily security experts and therefore the understanding of the security requirements may be very vague and at a high level of abstraction. To transform the specified security requirements to an executable form additional work is necessary. For that, detailed knowledge of security and integrity is necessary and a security administrator must be consulted. The security administrator takes the high-level security specifications of the workflow model as input and transforms them in a more detailed representation (intermediate language) by using guidelines located at layer 2 of the architecture. This leads to detailed specifications of security requirements of business processes. Security experts may either be human or computerized agents and during transformation cooperation with the domain expert may be necessary. The guidelines consist of a repository with information about dividing individual security requirements into basic building blocks. Layer 1 of the framework offers a repository of hardware and software components which are needed to realize the building blocks.

3. Security and Integrity Requirements

A business process is an often complex and in many cases relates to already existing models and procedures. A model of a business process may be viewed at least from the following perspectives: informational, functional, dynamic, organizational, and workflow specific perspective.

1060-3425/98 $10.00 (c) 1998 IEEE

Requirements on business processes are expressed in terms of these five perspectives. There are different types of requirements which influence the different perspectives at different intensity. An important class of requirements refers to security and integrity of business processes. These requirements apply to protect parts of a business process against certain threats. Examples of such requirements are requirements as they occur in any information system, such as confidentiality, integrity, and availability but also requirements which are more specific to workflow management (e.g. non-repudiation of the receipt of an electronic document), anonymity (e.g. of an agent performing a decision), legal requirements (such as privacy or copyright laws), legal bindings or mutual dependencies on agreements). Security and integrity requirements are complicate to handle because they influence all five perspectives of a business process. For example, confidentiality of a construction plan influences the data structuring of the plan (informational perspective), the handling of the construction plan within the organization (functional perspective), different versions of the construction plan (dynamic perspective), who is allowed to access the plan (organizational perspective), and the processing of the plan within the workflow (workflow perspective).

Security and integrity requirements result from different facts. They may result from facts internal to the enterprise or from facts coming from the environment the enterprise is acting in. External security requirements reflect the opinion of society and may be formed by laws and official regulations or reflect the informal view of the majority of people. The following components of a business process may be target of protection:

- *Information entities*
- *Processing agents* and *commissioning agents*
- *Procedures*
- *Final products*
- *Information flow*

The following table shows the relationship of targets of protection to security requirements. A "x" denotes that the corresponding requirement may occur for the business process component. "-" denotes that the security requirement may not be required for this component.

4. Conclusion

This extended abstract proposes a general framework for security and integrity and contains an enumeration of types of security semantics which need to be represented in a workflow. The ideas presented are part of a larger project with the goal to develop a security infrastructure for interorganizational workflow management.

5. References

[1] Atluri, V., Huang, W.-K., and Bertino, E. (1997). An Execution Model for Multilevel Secure Workflows. *Proc. IFIP 11.3 Workshop on Database Security*.

[2] Bußler, Ch.: Access Control in Workflow Management Systems. Proceedings of *IT Security'94*, Oldenbourg-Verlag, 1995, pp. 165-179.

[3] Ellmer, E.; Pernul, G.; Quirchmayr, G.; Tjoa, A M.: Access Controls in Cooperative Workflow Environments. *ACM SIGOIS Bulletin*, Vol. 15, No. 2, 1994, pp. 24-27.

[4] Herrmann, G., Pernul, G. (1997). A General Framework for Security and Integrity in Interorganizational Workflows. Proceedings of *10th International Bled Electronic Commerce Conference*, pp. 300-315.

[5] Karlapalem, K., Hung, P. (1997). Security Enforcement in Activity Management Systems. *Proc. NATO-ASI on Workflow Systems and Interoperability*, Turkey, Aug. 1997.

[6] Shen, H.; Dewan, P.: Access Control for Collaborative Environments. Proceedings of *CSCW´92*, ACM Press, 1992.

targets of protection / security req.	confidentiality	authenticity	integrity	availability	originality	anonymity	pseudo anonymity	authorized use	non-repudiation	ownership	authorship	copyright	legal binding	mutual dependencies	hiding activities
information	x	x	x	x	x	-	-	x	-	x	x	x	x	-	-
processing component	x	x	-	x	-	x	x	x	x	x	x	-	-	x	x
commissioning component	x	x	-	-	-	x	x	x	x	x	-	-	-	x	x
procedure	x	-	x	x	-	-	-	x	x	x	x	x	-	x	x
final product	x	x	x	x	x	-	-	x	-	x	x	x	-	-	-
information flow	x	-	x	-	-	-	-	-	x	-	-	-	-	x	x