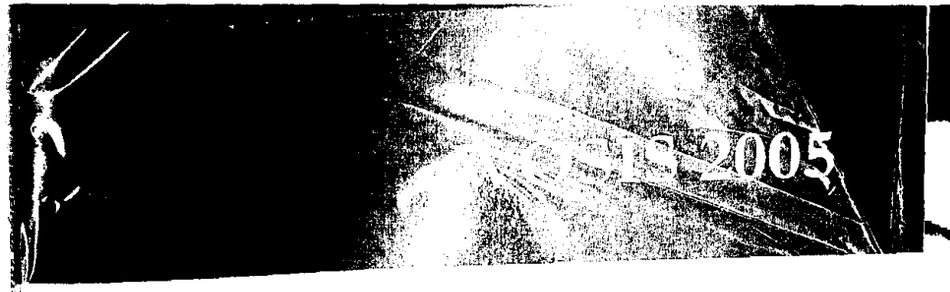


Eduardo Fernández-Medina,
Julio Hernández and
Javier Garcia (Eds.)

Security in Information Systems

Proceedings of the
3rd International Workshop on
Security in Information Systems
WOSIS 2005
In conjunction with ICEIS 2005
Miami, U.S.A., May 2005

Proceedings of the
3rd International Workshop on
Security in Information Systems WOSIS 2005
ISBN: 972-8865-25-2
http://www.iceis.org

Eduardo Fernández-Medina,
Julio César Hernández and
Luis Javier García (Eds.)

Security in Information Systems

Proceedings of the
3rd International Workshop on
Security in Information Systems,
WOSIS 2005
In conjunction with ICEIS 2005
Miami, U.S.A., May 2005

INSTICC PRESS
Portugal

Volume Editors

Eduardo Fernández-Medina
University of Castilla-La Mancha,
Spain

Julio César Hernández
Carlos III University,
Spain

and

Luis Javier García
Complutense University,
Spain

Proceedings of the 3rd International Workshop on
Security in Information Systems – (WOSIS 2005)
Miami, U.S.A., May 2005.
Eduardo Fernández-Medina
Julio César Hernández
and Luis Javier García (Eds.)

Printed in Portugal

ISBN 972-8865-25-2
Depósito Legal: 224489/05

Foreword

Obtaining a good degree of security in their Information Systems is one of the most pressing challenges facing all kind of organisations today. Although many companies have already discovered how critical information is to the success of their business operations, very few have managed to be effective in keeping their information safe, in avoiding unauthorised access, preventing intrusions, stopping secret information disclosure, etc.

Nowadays, rapid technological advances are stimulating a greater use of information systems in organisations world-wide, which handle large quantities of data, managed by huge databases and datawarehouses. In addition, information systems quite frequently manage information that can be considered sensitive, since it is related to certain intimate or personal aspects of persons (beliefs, medical data, sexual tendencies, etc.) and which must be specially protected.

Many organisations, including not only companies but also governments of several countries, are now realising how security problems can affect both business success and citizen rights, and they are proposing security policies, security planning, personal data protection laws, etc.

All of these, including technological, legislative, ethical and political factors, justifies the importance of secure information systems, and encourage us to research in new techniques, models and methodologies, which could aid designers developing and implanting safe information systems which both protect information and keep within the law. These facts, also, justifies the organization of WOSIS 2005.

The aim of this workshop is to serve as a forum to gather academics, researchers, practitioners and students in the field of Security in Information Systems by presenting new developments, lessons learned from real world cases, and providing the exchange of ideas and discussion on specific areas. From this point of view, the WOSIS 2005 workshop has been a great success, but it would be naïve and pretentious to consider that this success has only been due to their organizers. This is not the case. The organizers of the ICEIS 2005, specially Vitor Pedrosa, Slimane Hammoudi and Olivier Camp have been very helpful and proactive. The invited speaker, Professor Ernesto Damiani, has contributed a lot to increment the attractiveness and prestige of the WOSIS, helping just by joining us to bring the number of received papers to an overall maximum.

In these conditions, the review process has been specially difficult and long, (we have received 59 submissions, of which only 32 papers have been accepted) and it would have been hell if we had not the invaluable help of a very prestigious, competent and flexible Program Committee with the members we mention below. We should thank all of them.

We should thank also all the authors who submitted papers to the Workshop, being them accepted or not. The quality was quite high and we must reject some papers of value.

Additionally, the inclusion of a selection of some of the best papers of the Workshop in the "Security in Information Systems Special Collection" of the prestigious Journal of Research and Practice in Information Technology (JRPIT), has also contributed to increase the visibility and success of this year's WOSIS. Thanks very much to Sidney Morris, the editor-in-chief of the journal, it was a pleasure to work with you.

Finally, we would like to note that we will make our best to repeat this success next year.

Workshop Chairs – WOSIS 2005

Eduardo Fernández-Medina
University of Castilla-La Mancha,
Spain

Julio César Hernández
Carlos III University,
Spain

and

Luis Javier García
Complutense University,
Spain

Workshop Chairs

Eduardo Fernández-Medina
University of Castilla-La Mancha,
Spain

Julio César Hernández
Carlos III University,
Spain

and

Luis Javier García
Complutense University,
Spain

Program Committee

Vijay Atluri, Rutgers University, USA
Claudia Barenco, University of Brazilia, Brazil
Sabrina De Capitani di Vimercati, Università degli Studi di Milano, Italy
John Clark, University of York, UK
Nathan Clarke, University of Plymouth, UK
Ernesto Damiani, Università degli Studi di Milano, Italy
Ed Dawson, Information Security Research Center, Queensland, Australia
Juan Estévez, University of Granada, Spain
Csilla Farkas, University of South Carolina, USA
Eduardo B. Fernández, Florida Atlantic University, USA
Mariagrazia Fugini, Politecnico di Milano, Italy
Steven Furnell, University of Plymouth, UK
Christian Geuer-Pollmann, European Microsoft Innovation Center, Germany
Paolo Giorgini, University of Trento, Italy
Maribel González, University Rey Juan Carlos, Spain
Ehud Gudes, Ben-Gurion Univerity, Israel
Haralambos Mouratidis, University of East London, Dagenham, England
Sushil Jajodia, George Mason University, USA
Willem Jonker, University of Twente, The Netherlands
Jan Jürjens, TU Munich, Germany
Vasilis Katos, Portsmouth University, UK

Additional Reviewers:

Table of Contents

Papers

Papers

References

1. K. Alghathbar and D. Wijesekera. AuthUML: A Three-phased Framework to model Secure Use Cases. *Proc. of the Workshop on Formal Methods in Security Engineering: From Specifications to Code*, Washington D.C., 2003.
2. K. Alghathbar and D. Wijesekera. Consistent and Complete Access Control Policies in Use Cases. *Proc. of UML 2003*, San Francisco, CA, LNCS, 2003.
3. D. Bell and L. La Padula. Secure Computer Systems: Mathematical Foundations Model. *M74-244*, Mitre, 1975.
4. E. Bertino et al. A Logical Framework for Reasoning about Access Control. *ACM Trans. on Info. and System Security*, 6(1), Feb. 2003, pp. 71-127.
5. K. Biba. Integrity Considerations for Secure Computer Systems. *TR-3153*, Mitre, 1977.
6. G. Booch, et al. *The Unified Modeling Language User Guide*. Addison Wesley, 1999.
7. S. Demurjian, et al. A User Role-Based Security Model for a Distributed Environment. *Research Advances in Database and Information Systems Security*, J. Therrien (ed.), Kluwer, 2001.
8. T. Doan, et al. RBAC/MAC Security for UML. *Proc. of the 18th Annual IFIP WG 11.3 Working Conf. on Data and Applications Security*. Sitges, Spain, 2004.
9. T. Doan, et al. "MAC and UML for Secure Software Design". *Proc. of the 2nd ACM Wksp. on Formal Methods in Security Engineering* (FMSE'04). Washington D.C., 2004.
10. T. Doan, et al. UML Design with Security Integration as First Class Citizen. *Proc. of the 3rd Intl. Conf. on Computer Science, Software Engineering, Information Technology, e-Business, and Applications* (CSITeA'04). Cairo, Egypt, 2004.
11. P. Epstein and R. Sandhu. Towards A UML Based Approach to Role Engineering. *Proc. of the 4th ACM Wksp. on Role-based Access Control*, 1999.
12. D. F. Ferraiolo, et al. Proposed NIST standard for role-based access control. *ACM Trans. on Information and System Security*, 4 (3) August 2001.
13. S. Jajodia et al.. Flexible Support for Multiple Access Control Policies. *ACM Trans. on Database Systems*, 26(2) June 2001, pp. 214-260.
14. J. Jürjens. UMLsec: Extending UML for Secure Systems Development. *Proc. of UML 2002*, Dresden, LNCS, 2002.
15. T. Lodderstedt, D. Basin and J. Doser. SecureUML: A UML-Based Modeling Language for Model-Driven Security. *Proc. of UML 2002*, Dresden, LNCS, 2002.
16. OMG. *OMG-Unified Modeling Language, v.1.5*. UML Resource Page, March 2003 (www.omg.org/uml/).
17. S. Osborn, et al. Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies. *ACM Trans. on Info. and System Security*. 3(2), 2000.
18. G. Pernul, et al. The Entity-Relationship Model for Multilevel Security. *Proc. of the 12th International Conference on Entity-Relationship Approach*, Dallas, Texas, 1993.
19. G. Pernul, A M. Tjoa, W. Winiwarter. Modelling Data Secrecy and Integrity. *Data and Knowledge Engineering*, 26(3), 1998.
20. I. Ray, et al. Using Parameterized UML to Specify and Compose Access Control Models. *Proc. of the 6th IFIP Working Conf. on Integrity & Internal Control in Info. Systems*, 2003.
21. M. Shin and G. Ahn. UML-Based Representation of Role-Based Access Control. *Proc. of the 9th Intl. Wksp. on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2000.
22. G. W. Smith. Modelling Security Relevant Data Semantics. *IEEE Trans. on Software Engineering*, 17(11), 1991.
23. T.C. Ting. A User-Role Based Data Security Approach. *Database Security: Status and Prospects*, C. Landwehr (ed.), North-Holland, 1988.

Towards an integration of Security Requirements into Business Process Modeling

Alfonso Rodríguez [1], Eduardo Fernández-Medina[2], Mario Piattini[2]

[1] Universidad del Bio Bio, Departamento de Auditoría e Informática,
La Castilla S/N, Chillán Chile.
alfonso@ubiobio.cl

[2] Universidad Castilla-La Mancha, Departamento de Informática,
Paseo de la Universidad 4, Ciudad Real, España.
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Abstract: Business Processes are considered as an essential resource for companies to optimize and assure their quality by obtaining advantages with respect to their competitors. Consequently, Business Process Modeling becomes relevant since it allows us to represent the essence of the business. A notation to model businesses must be able to capture the majority of the requirements of the business. We have had the opportunity to check that security requirements have been scarcely considered in nowadays' most used notations to model business processes. In this work, we will present the security aspects that can be modelled from the business experts' dominion and that have been scarcely studied in the business process modeling, a review of the main notations used for modeling and a proposal to represent security requirements considering the knowledge of the experts in the business.

1 Introduction

Business Processes, considered as a set of procedures or activities which collectively realise a business objective or policy goal [30], form the essence of contemporary organizations' competitiveness. Each phase of the construction of business processes becomes, therefore, especially relevant. Among these phases, the requirements specification, considered as a process that effectively facilitates the necessary communication between the different parts involved in the process [20], allows us to rather ensure that the business process will be useful and functional for the objectives of the organizations.

However, the notion of security is often neglected in business process models, witch usually concentrate on modeling the process in a way that functional correctness can be show [3]. This is due to the fact that the expert in the business process dominion is not a specialist in security [14]. Furthermore, the requirements engineers are not trained at all in security and the that have been trained have only been given an overview of security architectural mechanisms such as password and encryption instead of the actual security requirements [10]. Nevertheless, many security aspects can be modelled from the user or the business analyst view since studies show that it is common that end users are able to express their security needs

at this level [18]. Consequently, during the modeling phase, the process owners should face the security requirements as well [23].

Our proposal will allow business analysts to early specify security requirements without having to deeply study implementation and/or architecture aspects. We think that an appropriate notation will facilitate this task; hence, we have extended the notation proposed by the Business Process Management Initiative (BPMI) by incorporating into it some security aspects that are comprehensible and adequate.

The paper is organized as follows: in section 2, we will present the business process security model considering the main notations used in the industry. In section 3, we will show the extension we propose for being able to represent security requirements from the business analyst perspective and finally, in section 4 we will present an example to appreciate the application of our proposal.

2 Business Process Security Model

In spite of the importance of security within business processes, business process security modeling presents two main problems. On the one hand, the modeling itself has been considered inadequate since those who specify security requirements are requirements engineers that, accidentally, have tended to replace them by specific restrictions of architecture [10]. On the other hand, security has been integrated very late, often during the actual implementation of the process [3] or even later, during the system administration phase. This can be partly explained by the fact that although security is a transversal aspect that early affects the components of an application, it is not properly understood and besides there is a lack of tools that support security engineering [17].

However, it is more or less obvious that an approach oriented to the process should also take into consideration security information in the business process management [1]. In this sense, to model security within a business process will imply to capture security requirements. This should be performed considering the following perspectives: *Static,* about the processed information security, *Functional,* from the viewpoint of the system processes, *Dynamic*, about the security requirements from the life cycle of the objects involved in the business process, *Organizational*, used to relate responsibilities to acting parties within the business process and the *Business Processes* perspective, that provides us an integrated view of all perspectives with a high degree of abstraction [14].

On the other hand, although the functional requirements of security tend to vary between applications of different types, it cannot be said the same thing about security requirements since any application at a high level of abstraction will have the same class of valuation and potentially the same vulnerability of its assets [11]. That is the reason why the most appropriate security requirements to be represented are those that are of the same type for all organizations since at this level we are not thinking about implementation. In addition, it is clear that the early identification of requirements, in this case, security requirements will allow us to save development and maintenance costs, so, it is obvious that it will be very useful to have a notation in which it is possible to specify security requirements.

Our proposal is based on two fundamental points. On the one hand, it is necessary to establish what notation will be used and on the other hand, it will be necessary to decide about the security requirements that will be considered.

2.1 Notations for Business Process Modeling

In business process modeling, the main objective is to produce a description of reality, for example, the way in which a commercial transaction is carried out to understand and eventually modify it with the aim of incorporating improvements into it. As a consequence, it is important to have a notation that allows us to model the essence of the business as clearly as possible. This notation must allow us to incorporate different perspectives giving place to different diagrams in which rules, goals, objectives of the business and not only relationships but also interactions are shown [8]. A great part of the success of the modeling has to do with the ability to express the different needs of the business as well as to have a notation in which these needs can be described. This is why when choosing an approach and/or notation, the properties of the object to be modelled must be taken into account, in other words, the business process, the environment features and the underlying reasons for the use [5].

Among the techniques that have been used for business process modeling are the following ones: flow diagrams, the family of techniques known as IDEF (Integration Definition for Function Modeling), Petri Nets, simulation, techniques based on knowledge (artificial intelligence) and Role Activity Diagrams [13].

At present, and according to the state of the business process modeling industry [19], it is possible to identify the Unified Modeling Language (UML) [21] and the Business Process Modeling Notation (BPMN) [7], among the main standards, thus, we will focus our analysis on both of them.

The use of UML is very spread in relation to business process modeling[8, 16-18, 27], since it is a consolidated language, easy to learn and it allows a fluent communication between the different actors about the model. However, UML has three problems that can undermine the business process modeling [12]; since (i) as UML has not been designed to model business processes, it may occur that some modeling aspects are not appropriately dealt with or are studied with a different orientation from the one needed by an expert in the business domain. On the other hand, (ii) UML takes it for granted an approach oriented to objects in the business process conception in which business objects should have been defined earlier, thus limiting the view of the process oriented to the business in which first of all, control and message flows are identified and then business modeling objects are implicitly defined. Finally, (iii) UML is usually more oriented to system architects and software designers due to the fact that it has been developed to facilitate the creation of software thinking of a mainly technique audience.

Regarding BPMN, it is a new proposal whose notation considers a unique diagram for the representation of processes, Business Process Diagram (BPD). This diagram was designed to facilitate its use and understanding and to offer an expressive force that allows us to model complex businesses by assigning them in a natural way to execution languages such as BPEL4WS (Business Process Execution Language For Web Services). To do so, the notation is supported by a modeling language, Business

Process Modeling Language (BPML) and a query language, Business Process Query Language (BPQL) [22].

In this paper, we will use BPMN because we consider that, although there are several reasons to use this notation [22], the most important one is that it offers us a modeling technique that is quickly understood by all users of the business, from business analysts that make drafts of the processes to technical developers that are responsible for the technological implementation of those processes and finally business people that will manage and control those processes. Moreover, it creates a standardization that connects design with implementation of business processes [7, 31].

2.2 Security requirements in the business process modeling

To model security requirements within business processes, we have to pay attention to two aspects that we think that are important. First of all, we do not have to forget that the individual who models the process is an expert in the business dominion and therefore, he/she has an idea of security without any kind of technical expression and perturbations that somebody who is thinking in the implementation or in technological solutions will have. Secondly, and for the same reason, we have to consider the part of security that is most agreed by non specialist users and whose meaning and representation is more or less standard.

The works related to security specifications developed by experts in the business dominion are: (i) scarce [3, 14, 18], (ii) oriented to security in the transaction [25] or (iii) are directly focused on information systems in general [28]. Therefore, and taking into consideration that business processes have a close relationship with workflow [24, 29], we have paid special attention to security and workflow works, [2, 6] and workflow management systems works (WfMS) [15]. We have realized that most of these works emphasize access control, defining it as identification, authentication and authorization according to the conditions specified in the taxonomy of factors and subfactors of security quality [11] through the use of access based on roles, RBAC [4, 6, 9, 26].

Consequently, and taking into account the fact that security requirements must be easy to assimilate by business analysts and have, at the same time, a clear meaning for security experts, we have considered the following ones: (i) *access control*, which must be considered as the degree to which the system limits access to its resources only to its authorized externals[1], (ii) *security auditing*, which is the degree to which the security personnel will collect, analyze and inform about the state and use of the security mechanisms and (iii) *privacy* which is the degree to which unauthorized parts are avoided from obtaining sensitive information[2] [10, 11].

1 For example; human users, programs, processes, devices or other systems
2 For example; identity of users, data or private communications

3 BPMN Extension for security modeling

To capture security requirements within the business process modeling, it is useful to have a notation that must be supported by a set of graphical concepts that allows us to represent the security semantics [14]. As we have previously indicated, BPMN offers us an orientation to the business analyst domain since it represents an opportunity to capture security requirements at a level of abstraction that, in our opinion has not been considered enough. BPMN does not explicitly consider mechanisms to represent these requirements. However, among the set of symbols used for the construction of the BPD [7], *Artifacts* can be used to express such requirements. Artifacts were designed to extend the modeling basic notation by adding them the possibility of representing specific situations [31]. They are composed of *Data Objects* that allow us to show the data required or produced by the activities, *Groups* that allow us to put together several activities in order to make analysis easier or improve documentation and *Text Annotations* that allow us to provide additional information for BPD reading. In spite of the fact that artifacts can be used to express security requirements, we consider that an explicit identification of them will facilitate modeling and will help us to obtain a better interpretation by security specialists.

The mechanism of extension stated by BPMN lets us add marks or indications to the already defined graphical elements [7]. In our proposal (see Figure 1), we have associated a symbol to represent each security requirement in a relatively standard way.

The representation of these security requirements within a business process performed by business experts will be understood as the need to incorporate (through the systems development process) the mechanisms and the technology that allow us to satisfy the intention of access control, security audit and privacy that has been specified.

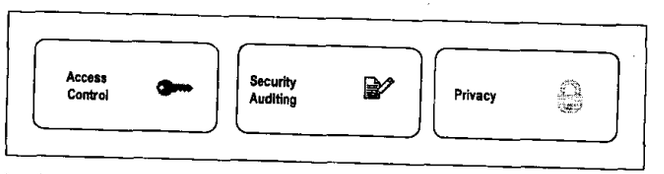
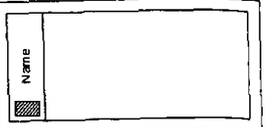
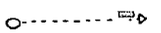
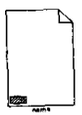
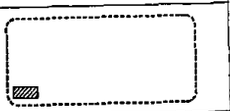


Fig. 1: Notation associated with security requirements

The BPD elements about which we propose to consider the security requirements representation are shown in Table 1. The highlighted rectangle that we have incorporated into the BPD notation indicates the place in which the security requirement must be specified.

Table 1. BPD elements incorporating security requirements.

Element		Notation
Pool: It represents an actor or a role within a business process. Graphically, it is an interval containing other BPD elements such as an Activity		
Lane: It corresponds to subdivisions of a Pool that are extended throughout this Pool in a horizontal or vertical way. Lane is used to organize and categorize Activities.		
Activity: It is the generic term used to identify the work performed by a company. This category includes processes, subprocesses and tasks.		
Message Flow: It corresponds to the information transferred during a business process between two Pools that are able to send or receive messages. A Message Flow can be represented between two activities as long as they are located in two different Participants.		
Artifact: It is used to provide additional information about a business process and it has not influence in the sequence or flow of this business process.	**Data Object:** It provides information about what the process performs. Data objects can be represented as documents, data and other objects that are used and updated by the process. Generally, they are shown associated to Activities or Sequence Flows.	
	Group: It is a visual mechanism that joins elements of a business process. Its main purpose is to highlight certain sections of the diagram with the aim of documentation and/or analysis.	

Now, we are going to describe the relationship between each one of the BPD elements (see Table 1) and the requirements of access control, security audit and privacy.

- *Pool/ Lane*: These elements will be described together since both of them specify roles. As Pool and Lane include other BPD elements in which security requirements can be also indicated, it is necessary to verify the coherence existing between the specifications performed in Pool or Lane and the elements they contain
  - *Access Control*: It indicates that, for this particular business process, the activities associated to Pool or Lane are more sensitive. Hence, it is necessary to intensify access control mechanisms. Such specification must be complemented with Text Annotation to indicate the required security degree (high, medium, low)[3].
  - *Security Auditing:* It indicates that all events related to Pool or Lane will be registered for a further analysis in relation to security auditing. If Text Annotation is used, the security auditing will be limited only to the events there indicated.
  - *Privacy:* This security requirement indicates the need to avoid that unauthorized parts obtain sensitive information (for example the identity of Pool or Lane). It is necessary to add information through the Text Annotation in which the desired degree of protection of privacy will be specified (high, medium, low).
- *Activity:* When any security requirement is specified for this BPD element, we have to pay attention to the security specifications of the elements that contain this Activity. (Pools, Lanes, Groups or other Activities). At the same time, we have to pay special attention to the specifications existing between the elements that an Activity contains (other Activities or Data Objects). Our purpose here is to maintain coherence within the security requirements specifications.
  - *Access Control:* It indicates that access to the execution of the activity must be limited. This security requirement is valid only if the Pool or the Lane that contain the Activity have not access control specification. The access control specification must be complemented with Text Annotations in which the required security level is specified (high, medium, low).
  - *Security Auditing:* It indicates that it is required to register the events taking place in the Activity. If Text Annotation artifact is used to indicate the events about which the security auditing will be performed, we will understand that the security auditing is limited only to those events that have been indicated
  - *Privacy:* This security requirement will not be represented in an Activity since we do not think it is very concrete in relation to the abstraction level in which these specifications are being carried out.
- *Message Flow:* The security requirements that are specified for this element are related to the content, origin, and destination of the Message Flow.
  - *Access Control:* The indication of this security requirement must be interpreted as the need to protect the Message Flow. This implies that Pools must be validated when the message flow is sent and received. It must be complemented with Text Annotation to indicate the required security degree (high, medium, low).
  - *Security Auditing:* The indication of this security requirement implies that we are aimed at registering all events related to Message Flow sending and reception.
  - *Privacy:* It establishes the need to protect the identity of participants and the confidentiality of the Message Flow content. It must be complemented with Text Annotation to specify the required degree of protection (high, medium ,low)

[3] Required security abstract levels that represent the higher or lower criticality noticed by the business analyst regarding access control or privacy depending on each particular case.

- *Data Object:* The security requirements for this element are related to the content of the Data Object.
  - *Access Control:* This security requirement is not directly specified on Data Object. Access Control can be extended from the specification performed in the Pool or Lane containing it through the activities that send or receive it.
  - *Security Auditing*: The indication of this security requirement implies that all events related to the sending or reception of the Data Object must be registered.
  - *Privacy:* It establishes the need to maintain the confidentiality of the Message Flow content. It must be complemented with Text Annotation to specify the required degree of protection (high, medium, low).
- *Group:* According to its definition, a Group can include any of the BPD elements described in Table 1. For this reason, the indication of security requirements performed on Group will spread to all elements involved by it. In such a case, we must consider the particular specifications of each element that it groups in order not to produce either inconsistencies or contradictions.

4 Case study using the proposal of extended BPMN

In Figure 2, it is shown an example of a BPD that has been specified using BPMN. This example describes a process of acceptance, review and preparation for the publication of papers prepared by the students of the Audit and Computer Science Department, of the Faculty of Business Science at the Bio Bio University. With these papers, every year it is edited a journal containing the best papers that have been prepared in that year. In this business process, it is described the way to carry out the process in an electronic way incorporating the security requirements into it by using the proposed extension.

The business analyst describes a process that is basically carried out by three Pools: The first one is *Student*, who prepares papers to be sent to the journal and eventually corrects the papers if it has been accepted. The second one is *Editor* who prepares the papers that will be sent to be reviewed, removes authors' information and add a guide line for evaluation, orders papers according to the obtained qualification, eventually sends papers that have been accepted to be corrected and prepares a draft with the papers that will be published. The last one is *Reviewer* who, in seven days time, will have to review the papers to complete an evaluation guide line and send them back to Editor together with the completed evaluation guide line.

The business analyst has considered it appropriate to include aspects related to security into the business process modeling. To do so, he/she uses the proposed extension, incorporating access control security requirements into the message flow generated between *Student/Editor* and *Editor/Reviewer*. This means that Pools must be validated for message flow to be sent and received. Furthermore, access control has been specified on the Activity "Review of corrections" performed by the *Student*, thus limiting the execution of this activity only to *Student* Pool. It has been specified security auditing on *Editor* Pool, thus indicating that we want to emphasize the sending/reception of message flow, the activity that this Pool has and the execution of processes "to prepare papers for review". At last, privacy has been specified on

Reviewer Pool, indicating that the degree of protection must be high, which means that his/her identity must be protected.

In spite of the fact that security requirements must have a concrete expression in the business process implementation, we think that this is a first stage that should be defined. From this definition, it will be possible to establish the correlation between specification and implementation at this level.

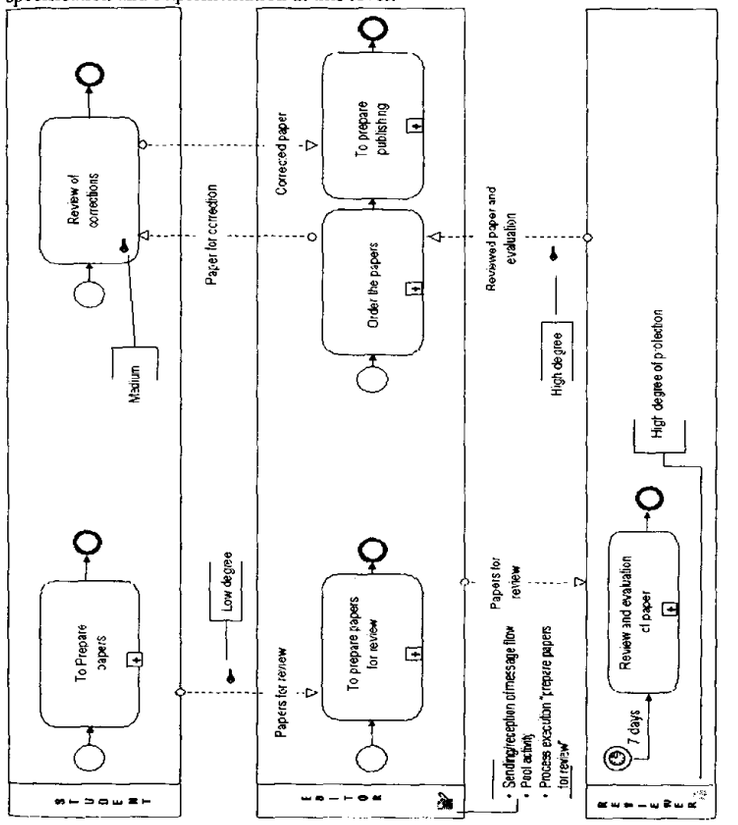


Fig. 2. Business Process for the electronic preparation of journal of the Audit and Computer Science Department.

5 Conclusions

Business process modeling is gaining importance due to the impact it can have on companies' competitiveness. Our work considers that we should pay more attention to

the business requirements specification at the high levels of abstraction because we think that the problem must not be only focused on a good solution based on IT. Security is one of the aspects that has been considered closer to the implementation of the business itself. We believe that the business process performance could be improved if security requirements are early captured. We have proposed a BPMN extension that provides business experts with an efficient vehicle to express security requirements. Future work should deeply study aspects related to use another notations (e.g. UML 2.0), and to the interpretation and implementation of security requirements by experts.

Acknowledgements

This research is part of the following projects: MESSENGER (PCC-03-003-1) financed by the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" (Spain), CALIPO (TIC2003-07804-C05-03) and RETISTIC (TIC2002-12487-E) granted by the "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (Spain).

References

1 Anttila, J., Kajava, J. and Varonen, R.; *Balanced Integration of Information Security into Business Management*, Proceedings of the 30th EUROMICRO Conference. (2004). p:558-564.

2 Atluri, V.; *Security for Workflow Systems*, Information Security Technical Report Vol. 6 (2) (2001). p:59-68.

3 Backes, M., Pfitzmann, B. and Waider, M.; *Security in Business Process Engineering*, International Conference on Business Process Management (BPM 2003) Vol. 2678 of LNCS. (2003). p:168-183.

4 Bertino, E., Ferrari, E. and Atluri, V.; *A Flexible model Supporting the Specification and Enforcement of Role-Based Authorizations in Workflow Management Systems*, Proceedings of Second ACM Workshop on Role-Based Access Control, Fairfax (Virginia). (1997). p:1-12.

5 Bider, I.; *Choosing Approach to Business Process Modeling - Practical Perspective*. In http://www.ibissoft.se/english/howto.pdf. (2003).

6 Botha, R. A. and Eloff, J. H. P.; *A framework for access control in workflow systems*, Information Management & Computer Security Vol. 9/3. (2001). p:126-133.

7 BPMN; *Business Process Modeling Notation (BPMN)*, Version 1.0 -May 3, C., BPMI.org. All Rights Reserved. In http://www.bpmi.org/. (2004).

8 Castela, N., Tribolet, J., Silva, A. and Guerra, A.; *Business Process Modeling with UML*, Proceedings of the 3st. International Conference on Enterprise Information Systems, ICEIS 2001. Vol. 2. Setubal, Portugal. (2001). p:679-685.

9 Chaari, S., Ben Amar, C., Biennier, F. and Favrel, J.; *An Authorization and Access Control Model for Workflow*, 1th International Workshop on COmputer Supported Activity Coordination CSAC 2004. Porto, Portugal. (2004). p:31-40.

10 Firesmith, D.; *Engineering Security Requirements*, Journal of Object Technology Vol. 2 N° 1 January-February 2003. (2003). p:53-68.

11 Firesmith, D.; *Specifying Reusable Security Requirements*, Journal of Object Technology Vol. 3, N° 1,January-February 2004. (2004). p:61-75.

12 Ghalimi, I.; *BPMN vs. UML*. In http://www.intalio.com/education/notes/note.xpg?id=BPMN_vs_UML. (2002).

13 Giaglis, G. M.; *A Taxonomy of Business Process Modelling and Information Systems Modelling Techniques*, International Journal of Flexible Manufacturing Systems Vol. 13 (2). (2001). p:209-228.

14 Herrmann, G. and Pernul, G.; *Viewing Business Process Security from Different Perspectives*, Proceedings of 11th International Bled Electronic Commerce Conference "Electronic Commerce in the Information Society". Slovenia. (1998). p:89-103.

15 Hung, P. and Karlapalem, K.; *A Secure Workflow Model*, Australasian Information Security Workshop (AISW2003). Vol. 21. Adelaide, Australia. (2003). p:33-41.

16 Jürjens, J., *Secure Systems Development with UML*, Springer Verlag, (2004). 309 p.

17 Lodderstedt, T., Basin, D. and Doser, J.; *SecureUML: A UML-Based Modeling Language for Model-Driven Security*, UML 2002 - The Unified Modeling Language, 5th International Conference. Vol. 2460. Dresden, Germany. (2002). p:426-441.

18 Maña, A., Montenegro, J. A., Rudolph, C. and Vivas, J. L.; *A business process-driven approach to security engineering*, 14th. International Workshop on Database and Expert Systems Applications (DEXA). Prague, Czech Republic. (2003). p:477-481.

19 Mega; *Business process Modeling and Standardization*. In http://www.bpmg.org/downloads/Articles/Article-MEGA-BusinessProcessModeling&StandardizationEN.pdf. (2004).

20 Nuseibeh, B. and Easterbrook, S. M.; *Requirements Engineering: A Roadmap*, ICSE 2000, 22nd International Conference on on Software Engineering, Future of Software Engineering Track. Limerick Ireland. ACM. (2000). p:35-46.

21 OMG; *Object Management Group*. In http://www.omg.org/. (2004).

22 Owen, M. and Raj, J.; *BPMN and Business Process Management; Introduction to the New Business Process Modeling Standard*, A Popkin Software, W. P. In http://www.bpmn.org/Documents/6AD5D16960.BPMN_and_BPM.pdf. (2003).

23 Palkovits, S., Rössler, T. and Wimmer, M.; *Process Modelling - Burden or Relief? Living Process Modelling within a Public Organisation*, ICEIS 2004, Proceedings of the 6th International Conference on Enterprise Information Systems. Porto, Portugal. (2004). p:94-102.

24 Reijers, H. A.; *Business Process Management Attempted Concepticide?*, IRMA International Conference (2004). p:128-131.

25 Röhm, A. W., Herrmann, G. and Pernul, G.; *A Language for Modelling Secure Business Transactions*, Proceedings 15th. Annual Computer Security Applications Conference. Computer Society Press., Phoenix, Arizona. (1999). p:22-31.

26 Sandhu, R. and Samarati, P.; *Authentication, Access Control, and Audit*, ACM Computing Surveys Vol. 28 N°1 March 1996. (1996). p:241-243.

27 Sparks, G.; *An Introduction to UML, The Business Process Model*. In http://www.sparxsystems.com.au/WhitePapers/The_Business_Process_Model.pdf. (2000).

28 Tryfonas, T. and Kiountouzis, E. A.; *Perceptions of Security Contributing to the Implementation of Secure IS*, Security and Privacy in the Age of Uncertainty, IFIP TC11 18th International Conference on Information Security (SEC2003) Vol. 250. Athens, Greece. (2003). p:313-324.

29 W.M.P. van der Aalst, Hofstede, A. H. M. t. and Weske, M.; *Business Process Management: A Survey*, International Conference on Business Process Management (BPM 2003) Volume 2678 (LNCS). Eindhoven, The Netherlands. (2003). p:1-12.

30 WfMC, *Workflow Management Coalition: Terminology & Glossary.*, Document Number WFMC-TC-1011, Document Number WFMC-TC-1011, (1999). 65 p.

31 White, S. A.; *Introduction to BPMN*. In http://www.ebpml.org/bpmn.htm. (2004).