Towards a UML 2.0 Profile for RBAC Modeling in Activity Diagrams

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

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

[2] ALARCOS Research Group
Information Systems and Technologies Department
UCLM-Soluziona Research and Development Institute
University of Castilla-La Mancha
Paseo de la Universidad 4, – 13071, Ciudad Real, Spain.

Abstract. Business Processes are a crucial issue for many companies because they are the key to maintain competitiveness. Moreover, business processes are important for software developers, since they can capture from them the necessary requirements for software design and creation. Besides, business process modeling is the center for conducting and improving how the business is operated. Security is important for business performance, but traditionally, it is considered after the business processes definition. Empirical studies show that, at the business process level, customers, end users, and business analysts are able to express their security needs. In this work, we will present a proposal aimed at integrating security requirements and role identification for RBAC, through business process modeling. We will summarize our UML 2.0 profile for modeling secure business process through activity diagrams, and we will apply this approach to a typical health-care business process.

1 Introduction

The key to maintain competitiveness is the ability of an enterprise to describe, standardize, and adapt the way it reacts to certain types of business events, and how it interacts with suppliers, partners, competitors, and customers [29]. Business Processes, defined as a set of procedures or activities which collectively pursue a business objective or policy goal [36], are a good answer to the environment complexity, the speed required by new products and the growing number of involved actors in the activities of the organization.

The new business scene, where there are many participants and an intensive use of communications and information technologies, implies that enterprises not only expand their businesses but also increase their vulnerability. As a consequence, with the increase of the number of attacks on systems, it is highly probable that sooner or later an intrusion can be successful [26]. This security violation causes losses. For this reason, it is necessary to protect computers and their systems in the best possible way.

Rodríguez A., Fernández-Medina E. and Piattini M. (2006).
Towards a UML 2.0 Profile for RBAC Modeling in Activity Diagrams.
In *Proceedings of the 4th International Workshop on Security in Information Systems*, pages 174-184

Best possible security does not necessarily mean absolute security, but a reasonable high security level in relation to the given limitations [37].

The notion of security is often neglected in business process models, which usually concentrate on modeling the process in a way that functional correctness can be shown [3] mainly due to the fact that the expert in the business process domain is not an expert in security [16]. Usually, security is considered after the definition of the system. This approach often leads to problems, which most of the times are translated into security vulnerabilities [24]. Moreover, most requirements engineers are not trained at all in security, and the few that have been trained have been only given an overview of security architectural mechanisms such as passwords and encryption rather than a proper training in actual security requirements [13].

Requirements specification usually results in a specification of the software system which should be as exact as possible [1]. Moreover, an early consideration of the security properties of the business process is positive for the development of secure systems. On the other hand, adding security as an afterthought not only increases the chances of a security conflict to exist, but also requires a huge amount of money and valuable time to overcome it, once the problem has been identified [24]

Best practices in software security include a manageable number of simple activities that should be applied throughout any software development process. These lightweight activities should start at the earliest stages of software development and then continue throughout the development process and into deployment and operations [34]. We believe that security should be considered during the business process definition because it is a good point to start software development.

In the same way, access control is an important requirement of information systems. RBAC [4, 12, 31] was found to be the most attractive solution for providing security features in multidomain digital government infrastructure. RBAC is characterized by the notion that permissions are assigned to roles, and not directly to users. Users are assigned appropriate roles according to their job functions, and hence indirectly acquire the permissions associated with those roles [19]. Moreover, due to the fact that roles represent organizational functions, an RBAC mechanism can directly support the specification of the access control policies of the organization [4].

On the other hand, effective business process models facilitate discussions among different stakeholders in the business, allowing them to agree on the key fundamentals and to work towards common goals. In order to create the best software, the businesses in which the software systems operate must be also modeled, understood, and sometimes improved [11].

For business process modeling, there are several languages and notations [15]. However, BPMN (Business Process Modeling Notation) and UML (Unified Modeling Language) are considered the main standards [23]. The most important change of UML 2.0 version with respect to the previous ones has been that of the activity diagrams which improve the business process representation. Our work considers a UML 2.0 profile that allows us to incorporate security requirements into the activity diagrams from the perspective of the business analyst. Business analysts will be able to specify access control, among other security requirements identified in the taxonomy proposed in [14]. The access control specification will give origin to an identification of roles and permissions over some activity diagram elements that have been used to describe a business process.

Our proposal is based on the MDA (Model Driven Architecture) approach. We will define early requirements identification using UML and this will make it possible to perform independent specifications of the implementation. Moreover, we believe that it is possible to have two different perspectives about security requirements at a high level of abstraction. One of them related to business analysts and the other associated with security experts. In this paper we have deepened in the first perspective.

The remainder of this paper is structured as follows: in next Section, we will summarize the background and related works. In Section 3 we will propose a UML 2.0 profile to represent security requirements from the business analyst's perspective. This profile will allow roles and permissions identification oriented to implement RBAC approach. Finally, in Section 4, we will present an example to show our proposal and in Section 5 our conclusion will be drawn.

2 Background and Related Work

In this section we will summarize the fundamental topics about security in business process, Role-based access control, and UML 2.0 activity diagrams and profiles. Related works are considered in each sub-section.

2.1 Security in Business Process

In spite of the importance of security for business processes, we have found out two problems. The first one is that modeling has not been adequate since, generally, those who specify security requirements are requirements engineers that have accidentally tended to use architecture specific restrictions instead of security requirements [13]. And in the second place, security has been integrated into an application in an ad-hoc manner, often during the actual implementation process [3], during the system administration phase [20] or it has been considered like outsourcing [22].

An approach to model security considering several perspectives is presented in [16]. Authors take into consideration 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 with an integrated view of all perspectives with a high degree of abstraction. We believe that from the business process perspective business analysts can integrate their view about business security.

On the other hand, functional security requirements tend to vary depending on the kind of application. This cannot be said about security requirements since any application at the highest level of abstraction will tend to have the same basic kinds of valuable and potentially vulnerable assets [14].

The research works related to security specifications carried out by business domain experts are; (i) scarce [3, 16, 21], (ii) oriented to transaction security [28], (iii) directly oriented to information systems in general [33] or (iv) thought for security and software engineers. [22]. Therefore, and taking into consideration that business processes have a close relationship with workflow[35], we have paid special attention to security and workflow works [2, 8]. We have proved that most of these works emphasize access control through the use of access based on roles, RBAC [5, 8, 30].

2.2 Role-based Access Control (RBAC)

The basic concept of RBAC (see Figure 1) is that users are assigned to roles, permissions are assigned to roles and users acquire permissions by being members of roles. A user in this model is a human being or other autonomous agent such as a process or a computer. A role is a job function or job title within the organization that describes the authority and responsibility of the user assigned to the role. A permission is a right granted to an individual acting on behalf of the user, that enables the holder of those rights to act in the system within the bounds of those rights [1].

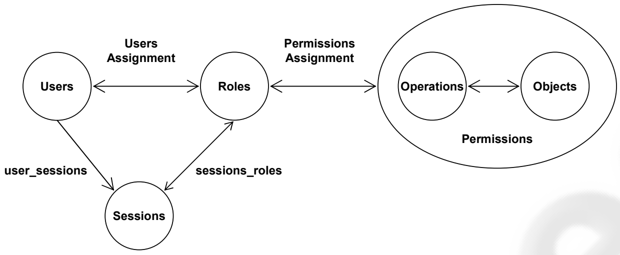

Fig. 1. Core RBAC [12].

RBAC is well suited as a foundation for the modeling of access control for several reasons. The concept of role-based permissions is close to the domain vocabulary used to define security in organizations. Therefore, it can ease the expression of requirements relevant for access control during analysis as well as promote their realization in the design [20].

Research works related to Role-based and business process modeling are presented in [9] and [10]. Authors show the fundamental concept for building a role based business process model. This approach presents two distinct models: the business object model and the role model. The first one focuses on the description of business objects, i.e. the components of a business. It represents the type of each business object, its intrinsic behavior and properties but it does not address the representation of the object's collaboration-related features. The role model specifies roles as types that can be specialized and aggregated. Role reuse is possible whenever the semantics of the interaction pattern is the same. The role model depicts the collaborative behavior between roles and the constraints that regulate them. Roles are bound to business objects in a specific business object model that defines their usage context.

Our proposal considers RBAC like an integral part of the security requirement about access control. This security requirement specified into activity diagrams with the UML 2.0 profile is fundamental to RBAC specification.

2.3 UML 2.0 Activity Diagrams and UML 2.0 Profiles

Activity diagrams are the UML 2.0 elements used to represent business processes and workflows [17]. In UML previous versions, expressivity was limited and this fact confused users that did not use the orientation to objects as an approach for modeling. Now, it is possible to support flow modeling across a wide variety of domains [6].

UML 2.0 is divided into structural and behavioral specifications, that is, models of the static and dynamic aspects of a system. Behavior models specify how the structural aspects of a system change over time. UML has three behavior models: activities, state machines, and interactions. Activities focus on the sequence, conditions, and inputs and outputs for invoking other behaviors, state machines show how events cause changes of object state and invoke other behaviors, and interactions describe message-passing between objects that causes invocation of other behaviors [7]. An activity specifies the coordination of executions of subordinate behaviors, using a control and data flow model. The graphical notation of an activity is a combination of nodes and connectors that allow us to form a complete flow. In Figure 2 we show a UML 2.0 meta-model for Activity Diagrams.

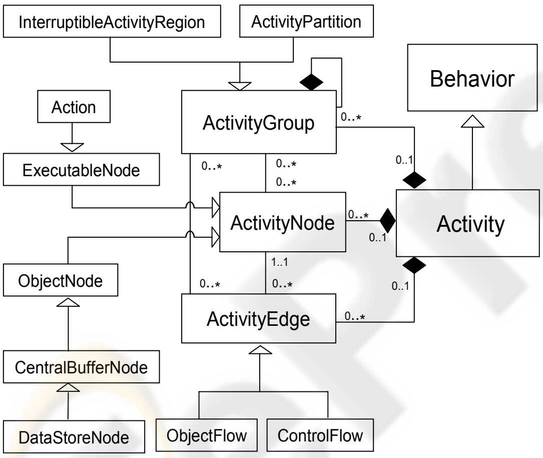

Fig. 2. UML 2.0 Activity Diagrams meta-model.

On the other hand, the Profiles package contains mechanisms that allow to adapt the meta-model for different purposes, for example, different platforms (such as J2EE or .NET) or domains (such as real-time or business process modeling). The profiles mechanism is consistent with the OMG Meta Object Facility (MOF) [25]. UML profiles consist of Stereotypes, Constraints and Tagged Values. A stereotype is a model element defined by its name and by the base class to which it is assigned. Constraints are applied to the stereotype with the purpose of indicating limitations (e.g. pre or post conditions, invariants). They can be expressed in natural language, programming language or through OCL (Object Constraint Language). Tagged values are additional meta-attributes assigned to a stereotype, specified as name-value pairs.

Research works related to UML 2.0 profiles and business processes refer to aspects of the business such as Customer, kind of Business Process, Goal, Deliverable and Measure [18], Data Warehouse and its relation to business process dynamic structures [32] or they add semantics to the activities considering organizational aspects that allow us to express resource restrictions during the execution of an activity [17]. Nevertheless, none of them is not related to security specifications.

3 UML 2.0 Profile for RBAC Modeling in Activity Diagrams

Our proposal allows business analysts to specify security requirements in the business process by using activity diagrams. From the Control Access requirement specification, it is possible to obtain a role identification and permissions oriented to RBAC specification. Later on, these requirements will be transformed, by the security experts, into technical specifications including all necessary details for their implementation. In this paper, we will only study the first part.

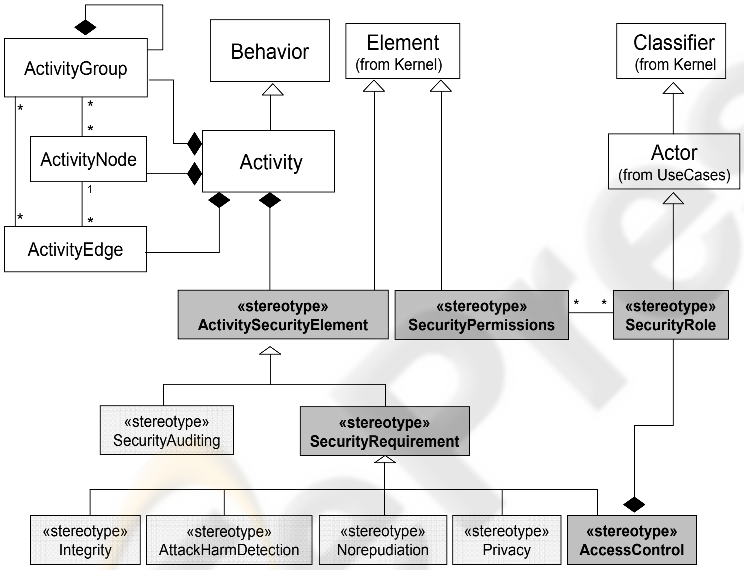

Fig. 3. Stereotype for security element and role identification.

We have proposed a UML 2.0 profile that allows us to define security requirements. Figure 3 show us the stereotype related to security requirement specification in activity diagrams (gray-coloured). For details about «*SecurityRequirement*», and its classes derived, see [27]. In this work we will study in depth the stereotypes about access control and the role and permissions identification (dark-gray- coloured).

The stereotype *«ActivitySecurityElement»* (see Table 1) is an abstract class created to contain security specifications obtained from the taxonomy proposed in [14]. The stereotype *«SecurityRole»* is an abstract class, derived from Actor (from UseCase), created to contain role specifications (see Table 1). *«SecurityRole»* has a composition relationship with *«AccessControl»* class. The stereotype *«SecurityPermission»* (see Table 1) is an abstract class derived from Element (from Kernel) created to contain permission specifications. These permissions must be specified for each object (activity diagram elements) that was used in the activity diagram that describes a business process.

Table 1. Security stereotypes specifications.

Name	ActivitySecurityElement	
Base Class	Element (from Kernel)	
Description	Abstract class containing audit specifications and security requirements	
Name	SecurityRequirement	Notation 🔒
Base Class	ActivitySecurityElement	
Description	It can contain business process security requirements specifications. It must be specialized to indicate the required security type.	
Constrains	It must be specified for Integrity (I), Access Control (AC), Non Repudiation (NR), Privacy (P) and Attack/Harm Detection (AD).	
Name	AccessControl	Notation 🔒 AC
Base Class	SecurityRequirement	
Description	It establishes the need to define and/or intensify the access control mechanisms to restrict access to specific components in an activity diagram.	
Constrains	It can be only specified in the following activity diagram elements: Activity, ActivityPartition and/or InterruptibleActivityRegion.	
Name	SecurityRole	
Base Class	Actor (from UseCases)	
Description	Abstract class containing role specifications.	
Constrains	– «*SecurityRole*» has only associations to «AccessControl» stereotype. – «*SecurityRole*» must have a name. – The *Role* in «*SecurityRole*» must be derived from: Activity, ActivityPartition or InterruptibleActivityRegion	
Name	SecurityPermission	
Base Class	Element (from Kernel)	
Description	Abstract class containing permission specifications.	
Constrains	– «*SecurityPermission*» has only associations to «*SecurityRole*» stereotype. – «*SecurityPermission*» must be specified such as *Objects-Operations* pairs – *Objects* could be related to: Action, DataStore and ObjectFlow – Each Object must be associated to Operations, according to: – *Actions {Execution, CheckExecution}* *Execution* is a default value. CheckExecution is specified when the Role must be verified once again. – *DataStore {Update, Create, Read, Delete}* *Update* is a default value. Create, Read and Delete are the classical operations for data store. – *ObjectFlow {SendReceive , CheckSendReceive}* *SendReceive* is a default value. CheckSendReceive is specified when the Role must be verified once again for operation to be carried out.	

4 Example

Our illustrative example (see Figure 4) describes a typical business process for the admission of patients in a health-care institution. In this case, the business analyst identified the following Activity Partition: Patient (individual who receives medical care and who must fill out an admission request), Administration Area (which is a top partition that is divided into two middle partitions), where the Medical Institution records details about costs and insurances, and finally, the Medical Area (divided into Medical Evaluation and Exams) where pre-admission tests, exams, evaluations and complete clinical data collecting are carried out. Security requirements are included in this business process. The business analyst has considered several aspects of security.

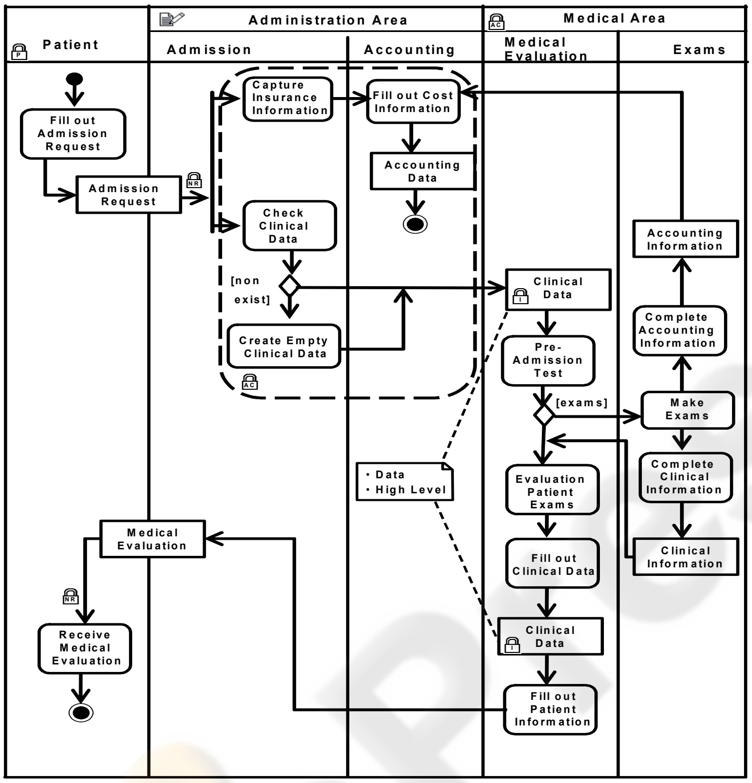

Fig. 4. Business Process: Admission of Patients in a Medical Institution.

We are to going pay special attention into Access Control specifications. *«AccessControl»* has been defined over the Interruptible Activity Region. This specification involves Actions (Capture Insurance Information, Check Clinical Data, Create Empty Clinical Data and Fill out Cost Information) and Data Store (Accounting Data). Access Control has been also specified over the Activity Partition "Medical Area" which implies that Access Control is applicable to all objects (Actions, Data store and object flow) in "Medical Evaluation" and "Exams" middle activity partitions.

In Table 2, we will show details about the specification. The first column contains the role. It has been extracted from Activity, ActivityPartition or InterruptibleActivityRegion. The second column shows the objects within the scope of the access control specification. The last column contains information about operations over objects in relation to access control constrains.

Table 2. «*SecurityRole*» and «*SecurityPermission*» specifications.

	Permissions		
Role	**Objects**		**Operations**
Admission/Accounting	Action	Capture Insurance Information Fill out Cost information Check Clinical Data Create Empty Clinical Data	Execution CheckExecution Execution Execution
	DataStore	Accounting Data	Update
Medical Evaluation	Action	Pre-Admission Test Evaluation Patient Exams Fill out Clinical Data Fill out Patient Information	Execution Execution Execution Execution
	DataStore	Clinical Data	Update
Exams	Action	Complete Accounting Information Make Exams Complete Clinical Information	CheckExecution Execution CheckExecution
	DataStore	Accounting Information Clinical Information	Read, Create Read, Create

5 Conclusions and Ongoing Work

The improvement experienced in the languages for business processes modeling, especially UML 2.0 activity diagrams, opens an opportunity to incorporate security requirement that allow us to improve this aspect of the systems from early stages in software development. In this paper, we have presented a UML 2.0 profile that allows us to incorporate security requirements into activity diagrams that will increase the scope of the expressive ability of business analysts. We have placed particular emphasis on Access Control requirement. From this specification, it is possible to identify roles for RBAC specifications and permissions specifications that consider objects and operations over this object.

The next step should be that of apply an MDA approach to transform the model (including the security requirements) into most concrete models (i.e. execution models). Therefore, the future work must be oriented to enrich the security requirements specifications, improving the UML profile specification to complement it with Well-Formedness Rules and OCL. Furthermore, it is necessary to incorporate the viewpoint of the security expert into them in order to make implementation possible.

Acknowledgements

This research is part of the following projects: DIMENSIONS (PBC-05-012-1), supported by FEDER and the “Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha”, COMPETISOFT (granted by CYTED) and RETISTIC (TIC2002-12487-E) granted by the “Dirección General de Investigación del Ministerio de Ciencia y Tecnología” (Spain).

References

1. Artelsmair, C. and Wagner, R.; Towards a Security Engineering Process, The 7th World Multiconference on Systemics, Cybernetics and Informatics. Vol. VI. Orlando, Florida, USA. (2003). pp.22-27.
2. Atluri, V.; Security for Workflow Systems, Information Security Technical Report. Vol. 6 (2). (2001). pp.59-68.
3. Backes, M., Pfitzmann, B. and Waider, M.; Security in Business Process Engineering, International Conference on Business Process Management. Vol. 2678, LNCS. Eindhoven, The Netherlands. (2003). pp.168-183.
4. Bertino, E.; RBAC models – concepts and trends, Computers and Security. Vol. 22 (6). (2003). pp.511-514.
5. Bertino, E., Ferrari, E. and Atluri, V.; A Flexible model Supporting the Specification and Enforcement of Role-Based Authorizations in Workflow Management Systems, Second ACM Workshop on Role-Based Access Control, Fairfax (Virginia). (1997). pp.1-12.
6. Bock, C.; UML 2 Activity and Action Models, Journal of Object Technology. Vol. 2 (4), July-August. (2003). pp.43-53.
7. Bock, C.; UML 2 Activity and Action Models, Part 2: Actions, Journal of Object Technology. Vol. 2 (5), September-October. (2003). pp.41-56.
8. Botha, R. A. and Eloff, J. H. P.; A framework for access control in workflow systems, Information Management & Computer Security. Vol. 9/3. (2001). pp.126-133.
9. Caetano, A., Rito Silva, A. and Tribolet, J.; Business Process Modeling with Objects and Roles, 6th International Conference on Enterprise Information Systems (ICEIS 2004). Porto, Portugal. (2004). pp.109-114.
10. Caetano, A., Zacarias, M., Rito Silva, A. and Tribolet, J.; A Role-Based Framework for Business Process Modeling, 38th Hawaii International Conference on System Sciences (HICSS-38 2005). Big Island, HI, USA. (2005). pp.130-136.
11. Eriksson, H.-E. and Penker, M., Business Modeling with UML, OMG Press. (2001).
12. Ferraiolo, D. F., Sandhu, R., Gavrila, S. I., Kuhn, D. R. and Chandramouli, R.; Proposed NIST standard for role-based access control, ACM Transactions on Information and System Security (TISSEC). Vol. 4 (3). (2001). pp.224-274.
13. Firesmith, D.; Engineering Security Requirements, Journal of Object Technology. Vol. 2 (1), January-February. (2003). pp.53-68.
14. Firesmith, D.; Specifying Reusable Security Requirements, Journal of Object Technology. Vol. 3 (1), January-February. (2004). pp.61-75.
15. Giaglis, G. M.; A Taxonomy of Business Process Modelling and Information Systems Modelling Techniques, International Journal of Flexible Manufacturing Systems. Vol. 13 (2). (2001). pp.209-228.
16. Herrmann, G. and Pernul, G.; Viewing Business Process Security from Different Perspectives, 11th International Bled Electronic Commerce Conference. Slovenia. (1998). pp.89-103.
17. Kalnins, A., Barzdins, J. and Celms, E.; UML Business Modeling Profile, Thirteenth International Conference on Information Systems Development, Advances in Theory, Practice and Education. Vilnius, Lithuania. (2004). pp.182-194.
18. List, B. and Korherr, B.; A UML 2 Profile for Business Process Modelling, 1st International Workshop on Best Practices of UML (BP-UML 2005) at ER-2005. Klagenfurt, Austria. (2005).
19. Liu, P. and Chen, Z.; An Extended RBAC Model for Web Services in Business Process, IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04). (2004). pp.100-107.
20. 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). pp.426-441.

21. 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). pp.477-481.
22. Maña, A., Ray, D., Sánchez, F. and Yagüe, M. I.; Integrando la Ingeniería de Seguridad en un Proceso de Ingeniería Software, VIII Reunión Española de Criptología y Seguridad de la Información, RECSI'04. Leganés, Madrid. España. (2004). pp.383-392.
23. Mega; Business process Modeling and Standardization. In http://www.bpmg.org/downloads/-Articles/Article-MEGA-BusinessProcessModeling&StandardizationEN.pdf. (2004).
24. Mouratidis, H., Giorgini, P. and Manson, G. A.; When security meets software engineering: a case of modelling secure information systems, Information Systems. Vol. 30 (8). (2005). pp.609-629.
25. Object Management Group; Unified Modeling Language: Superstructure, version 2.0, formal/05-07-04. In http://www.omg.org/docs/formal/05-07-04.pdf. (2005).
26. Quirchmayr, G.; Survivability and Business Continuity Management, ACSW Frontiers 2004 Workshops. Dunedin, New Zealand. (2004). pp.3-6.
27. Rodríguez, A., Fernández-Medina, E. and Piattini, M.; Integrating Security Requirement with a UML 2.0 Profile, International Symposium on Frontiers in Availability, Reliability and Security in conjunction with ARES 2006. Accepted. Vienna, Austria. (2006).
28. Röhm, A. W., Herrmann, G. and Pernul, G.; A Language for Modelling Secure Business Transactions, 15th. Annual Computer Security Applications Conference. Phoenix, Arizona. (1999). pp.22-31.
29. Roser, S. and Bauer, B.; A Categorization of Collaborative Business Process Modeling Techniques, 7th IEEE International Conference on E-Commerce Technology Workshops (CEC 2005). Munchen, Germany. (2005). pp.43-54.
30. Sandhu, R. and Samarati, P.; Authentication, Access Control, and Audit, ACM Computing Surveys. Vol. 28 Nº1 March 1996. (1996). pp.241-243.
31. Sandhu, R. S.; Future Directions in Role-Based Access Control Models, International Workshop on Information Assurance in Computer Networks: Methods, Models, and Architectures for Network Security. Vol. 2052. St. Petersburg, Russia. (2001). pp.22-26.
32. Stefanov, V., List, B. and Korherr, B.; Extending UML 2 Activity Diagrams with Business Intelligence Objects, 7th International Conference on Data Warehousing and Knowledge Discovery (DaWaK2005). Copenhagen, Denmark. (2005).
33. 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). pp.313-324.
34. van Wyk, K. R. and McGraw, G.; Bridging the Gap between Software Development and Information Security, IEEE Security and Privacy. Vol. 3 (5). (2005). pp.75-79.
35. 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). pp.1-12.
36. WfMC, Workflow Management Coalition: Terminology & Glossary., (1999). p.65.
37. Zuccato, A.; Holistic security requirement engineering for electronic commerce, Computers & Security. Vol. 23 (1). (2004). pp.63-76.