Obtaining Use Cases and Security Use Cases from Secure Business Process through the MDA Approach

Alfonso Rodríguez[1] and Ignacio García-Rodríguez de Guzmán[2]

[1] Departamento de Auditoría e Informática, Universidad del Bío-Bío, Chillán, Chile

[2] ALARCOS Research Group, Information Systems and Technologies Department
UCLM-Soluziona Research and Development Institute
University of Castilla-La Mancha, Ciudad Real, Spain

Abstract: MDA is an approach based on the transformation of models for software development. It is complemented with QVT as a language for transformations specifications. This approach is being paid much attention by researchers and practitioners since it promotes the early specification of requirements at high levels of abstractions, independently of computation, that will be later part of models closer to the software solution. Taking into account this approach, we can create business process models incorporating requirements, even those of security, that will be later part of more concrete models. In our proposal, based on MDA, we start from secure business process specifications and through transformations specified with QVT, we obtain use cases and security use cases. Such artifacts complement the first stages of an ordered and systematic software development process such as UP.

1 Introduction

Business processes are important for enterprises because they allow us to obtain an advanced marketplace position, and then, these enterprises can optimize and assure the quality of their products and services. Moreover, business processes allow enterprises to describe, standardize, and adapt the way they react to certain types of business events, and how they interact with suppliers, partners, competitors, and customers [21]. At the same time, 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 [17]. This security violation causes losses. Therefore, it is necessary to protect computers and their systems with a high security level in relation to the given limitations.

A way to face security problem is that of incorporating it early into the business processes specifications. At this level, it is possible to capture security requirements that take into account the point of view of business analysts.

Nowadays, models transformation is being paid attention by the community of researchers and practitioners due to the fact that it is focused on solving the problems

Rodríguez A. and García-Rodríguez de Guzmán I. (2007).
Obtaining Use Cases and Security Use Cases from Secure Business Process through the MDA Approach.
In *Proceedings of the 5th International Workshop on Security in Information Systems*, pages 209-219
DOI: 10.5220/0002421502090219
Copyright © SciTePress

of time, cost and quality associated with software creation. The Object Management Group (OMG) proposal for this approach is composed of: Model Driven Architecture (MDA) [16]; a framework for software development that allows the creation of models independent of the technological implementation, and Query/View/Transformations (QVT) [18]; a standard for models transformation.

Our proposal is based on the MDA approach. To do so, we use a profile that allows us to specify Secure Business Processes (SBP) corresponding to Computation Independent Models (CIM). From these requirements and applying transformation rules, we can obtain UML artifacts used to describe the problem in the context of Platform Independent Models (PIM). Use cases (UC) and secure use cases are obtained. Such artifacts let us complement the requirements capture defined in the Unified Process (UP) [10].

The structure of the remainder of the paper is as follows: in Section 2, we will present a background and related works. In Section 3, we will summarize the main issues in security in business processes. In Section 4, we will present our proposal. Finally, in Section 5, we will put forward an example and in Section 6 our conclusions will be drawn.

2 Background and Related Works

In this section, we will briefly state the elements considered in our proposal and the works related to for obtaining use cases from business processes models.

UP is a software development process composed of a set of activities necessary for transforming user's requirements into a software system. Additionally, it can be understood as a methodology that provides us with generic recommendations that can be instantiated by different projects classes where not only the project itself but also the product with their different maturity levels and versions are included [15].

MDA is a framework for software development that allows the creation of models independent of the technological implementation, and QVT [18], a standard language for models transformation. In MDA approach the Computation Independent viewpoint focuses on the environment of the system, the Platform Independent viewpoint focuses on the operation of a system while hiding the details necessary for a particular platform and the Platform Specific viewpoint combines the platform independent viewpoint with an additional one focused on the details of the use of a specific platform by a system [16]. In addition, QVT offers us the possibility of manipulating models taking into consideration three factors: (i) queries that take a model as an input and select specific elements from it according to a search pattern, (ii) views corresponding to models that are derived from other models and finally, (iii) transformations that take as a reference one or more input models to obtain an output model or result.

In the works related to security and use cases (or misuse case) [2, 6, 11, 23], these are used to capture security requirements but differently of our proposal, they are not directly obtained from UML 2.0 Activity Diagrams (UML 2.0-AD) security specifications.

In the works related to for obtaining use cases from business processes specifications, we have found that in [22], it is suggested the possibility of obtaining

use cases from a business process specification made with Business Process Modeling Notation (BPMN). In [12], it is proposed the automatic for obtaining UML artifacts from a business process description that was made using BPMN. Authors extend BPMN (Extension Level-1) to add information about the sequence and the input and output flows. This allows them to apply rules from which use cases, state diagrams, sequence and collaboration are achieved. In [24], it is stated a transformation performed from a business process described with UML 2.0-AD to use cases and finally. In [4], use cases are obtained from business process models that are not represented by activity diagrams. The differences with our proposal are basically the following: (i) even in works where there are automatic transformations, previous manual intervention is required, ii) transformations are not described by using languages specially designed with this purpose iii) the result of transformations does not appear to be linked to a business process development finally, and iv) none of them is related to security aspects.

3 Security in Business Process

A business process is the combination of a set of activities within an enterprise with a structure describing their logical order and dependence whose objective is to produce a desired result. A model is a simplified view of a complex reality. It is a means by which to create abstraction, thus allowing one to eliminate irrelevant details and to focus upon one or more important aspects at a time. Business process models enable a common understanding and facilitate discussion among different stakeholders in a business [1, 5].

Those works, which are related to the specification of security requirements in business processes [3, 8, 9, 14, 20, 25], coincide in the idea that it is necessary to capture the point of view of the business expert with regard to security, and to include these specifications within the software development process.

However, at the moment is possible to capture at a high level security requirements easily identifiable by those who models business processes, because: (i) the business process representation has improved in UML 2.0 version, (ii) the security requirement will tend to have the same basic kinds of valuable and potentially vulnerable assets [7], and (iii) empirical studies show that it is common at the business process level that customers and end users are able to express their security needs [13]

Therefore, we have addressed the problem of including security in business processes [19] by extending the UML 2.0-AD to allow the security requirements specification. The proposed extension, called BPSec, basically considers the graphical representation of security requirements taking from the taxonomy proposed in [7]. We consider the following security requirement: Attack Harm Detection, Access Control, Audit Register, Integrity, Privacy and Non Repudiation. We have used a padlock, standard *de facto*, to graphical represent security requirements. The set of security requirements, not exclusive, are described in

212

Table 1.

Table 1. Security Requirement definitions.

Access Control (AC): This corresponds to the limitation of access to resources by authorized users only. The specification of this requirement by the business analyst implies the limitation of access to a set of resources that are considered important enough to be protected in a special way. From the security perspective, this specification consists of the definition of roles that may be assigned to individuals, entities, programs, devices or other systems and the definition of permission to access objects included in the field of the access control specification. In addition, this requirement may have an audit register specification
Attack Harm Detection (AD): This is defined as the detection, register and notification of an attempted attack or threat, whether it is successful or not. From the business analyst perspective, this requirement represents an attention signal covering the elements which are indicated. Furthermore, it can be interpreted as a previous step to an access control specification. From the security point of view, this specification implies the maintenance of the events register (attacks or threats) which have occurred to potentially vulnerable elements. This requirement can only be specified with an audit register
Integrity (I): This is related to the protection of components from intentional and non-authorized corruption. The integrity specification is valued as low, medium, and high. From the business analyst perspective, an integrity specification (at any degree) is related to the importance of the information contained in the data store or data flow. The integrity specification, from the perspective of the expert in security, implies the registration of the involved role and the date and time of access to the data store or data flow. Additionally, security measures are specified according to the degree of integrity. This requirement is always associated with the audit register
Non Repudiation (NR): This establishes the need to avoid the denial of any aspect of the interaction (e.g. message, transaction, transmission of data). From the business analyst perspective, Non Repudiation represents the need to protect a determined interaction so that any potential problems (e.g. legal and liability) in relation to any interaction are minimized. From the security perspective, this specification implies the generation of at least two security roles and alternatively the audit register. This requirement may additionally have an audit register specification
Privacy (P): This is related to conditions of information protection concerning a determined individual or entity, thus limiting access to sensitive information by non-authorized parties. From the point of view of the business analyst, the privacy specification implies the non-revelation (confidentiality) and non-storage (anonymity) of the information regarding a determined role. From the security viewpoint, the specification of privacy with confidentiality implies the protection of the information of a role not to be revealed to third parties. In the case of privacy with anonymity, it implies that information must not be stored either. This fact implies the creation of generic roles that expire along with the work session. Additionally, this requirement may have a specification of audit register

Such security requirements are related to UML 2.0-AD elements according to the restrictions presented in Table 2, indicating in each case if the security requirement can (✓) or cannot (–) be associated with each activity diagram element.

Table 2. Security Requirements and UML 2.0-AD Elements.

	UML 2.0 element for containment in activity diagrams				
Stereotypes for secure activity specification	Action	Activity Partition	DataStore Node	Interruptible ActivityRegion	ObjectFlow (data)
AccessControl	✓	✓	✓	✓	✓
AttackHarmDetection	–	✓	✓	✓	✓
Integrity	–	–	✓	–	✓
NonRepudiation	–	–	–	–	✓
Privacy	–	✓	–	✓	–

It is important to mention that the security specifications performed with the business processes model are very abstract. Nonetheless, as we move towards more concrete models more detailed specifications will be performed. As a result of the BPSec application, a Secure Business Process (SBP) is obtained.

4 Our proposal

A business process built by a business analyst apart from being useful in the specific business field, it is very useful in a process of software construction. From it, we can obtain system requirements, a stage taken into account by all modern development processes. In our proposal, CIM to PIM transformations (C2P) are aimed for obtaining useful artifacts in software development. The basic aspects of our proposal are shown in Figure 1. The first column (on the left) show two types of models which

conform to the MDA. In the last column we can see the UP disciplines. The central part shows our proposal and the artifacts which are derived from its application. The business process specification is made by using UML 2.0-AD and BPSec. We applied a set of transformation rules and checklists to obtain a subset of use cases and security use cases that facilitate the understanding of the problem. SBP is used in a "Business Modeling" and uses cases are used in "Requirement" and "Analysis & Design" disciplines of UP.

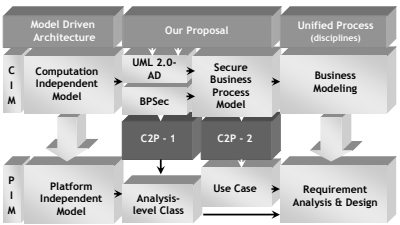

Fig. 1. An overview for our proposal.

Use cases are derived from UML 2.0-AD by applying a set of QVT rules (see Table 3), refinement rules (see Table 4) and checklists (see Table 5).

The rules that do not consider security specifications (R1, R2 and R3), are oriented to identify actors and related use cases. The rule R4 from a security requirement (AC, AD, I, NR or P) the subject (or package) name is obtained and R5 from a security requirement use case actor (Actor) that will take the name "Security Staff" it is obtained. In Table 3, all rules expressed in textual QVT are described.

Table 3. Mapping between Activity Diagrams and Use Case elements.

```
transformation ActivityDiagram2UseCaseDiagram
    top relation R1  // from Activity Partition to Actor
    {
        checkonly domain uml_ActivityDiagram ap:ActivityPartition {name = n}
        enforce domain uml_UseCaseDiagram a:Actor{name = n}
        where {
          ap.containedNode → forAll(cn:Action|R3(cn))
        }
    }
    top relation R2  // from Interruptible Activity Region to Actor
    {
        checkonly domain uml_ActivityDiagram iar:InterruptibleActivityRegion {name = n}
        enforce domain uml_UseCaseDiagram a:Actor {name = n}
        where { ap.containedNode → forAll(cn:Action|R3(cn))
        }
    }
    relation R3 // from Action to UseCase
    {
        checkonly domain uml_ActivityDiagram ac:Action {name = n, inPartition=ap}
        enforce domain uml_UseCaseDiagram uc:UseCase {name = n, subject= ACTORS: Set(Actor)};
        where { ACTORS→including (a:Actor{name=ap.name})
        }
    }
transformation BPSec2UseCaseDiagram
    top relation R4  // from Security Requirement to subject
    {
        checkonly domain bpsec_BPSec sr:SecurityRequirement {requirementtype = n}
        enforce domain uml_UseCaseDiagram c:Clasifier {name=n}
    }
    top relation R5  // from Security Requirement to subject
    {
        checkonly domain bpsec_BPSec sr:SecurityRequirement
        enforce domain uml_UseCaseDiagram a:Actor {name="Security Staff"}
    }
```

Refinement rules, described in Table 4, are focused on enriching the specifications obtained in the previous section.

Table 4. Rules to refine use cases.

RR 1:	Subject name (not related to security specification) is obtained from the business process name
RR 2:	Subject name obtained from C2P_2-R4 must be complemented with the name of the UML 2.0-AD element where security requirement has been specified
RR 3:	Region Name is obtained by linking the Activity Partition names where Interruptible Activity Region is contained
RR 4:	Main Actor corresponds to the Activity Partition or region name where Initial Node is present
RR 5:	Actor Generalization is obtained from top and middle Activity Partitions
RR 6:	Redundant specifications must be eliminated

In Table 5, a checklist that allows us to complete use cases related to security specifications is presented. For each security requirement a set of generic tasks that must be applied over a specific SBP are exposed.

Table 5. Checklist for the obtention of security use cases.

Access Control
«Preconditions» Secure Role, and Permissions over the objects in the secure role scope
«Postconditions» Secure role validated to access to resources, Permissions over the validated objects, and Audit Register (optional)
– Assign secure role to the partition, region or action
– Validate the secure role. This task is divided into: identify, authenticate and authorize the secure role
– Verify permissions over the objects in the role secure field. This implies a review of the permissions granted to the objects that are within the field of access control specification
– If audit register has been specified, then the information related to the security role, the security permissions and the objects in the access control specification field must be stored
AttackHarmDetection
«Preconditions» Secure Role
«Postconditions» Audit Register
– Assign secure role (origin and destination in the case of ObjectFlow).
– Register the type of element over which security requirements and date and time when an access to that element is produced were specified
Integrity
«Preconditions» Secure Role
«Postconditions» Audit Register
– High-integrity specification implies: ask for permissions over data store, verify permissions, make security copies (backups), and produce audit register
– Medium-integrity specification implies: send a warning message related to the data operation, make security copies, and produce audit register
– Low-integrity specification implies produce audit register
NonRepudiation
«Preconditions» Secure Roles (origin and destination)
«Postconditions» Valid roles, and Audit Register (optional)
– Assign origin and destination roles
– Validate roles: This task is divided into: identify, authenticate and authorize the secure role
Privacy
«Preconditions» Secure Role
«Postconditions» Audit Register (optional)
– Assign a secure role (if anonymity was specified, then the role is generic and expires together with the session)
– Validate roles: This task is divided into: identify, authenticate and authorize the secure role
– Verify revelation permissions (anonymity and confidentiality)
– Verify storage permissions (only anonymity)
– Verify audit register specification
– If audit register has been specified, then the information related to the security role must be stored

5 Example

Our illustrative example (see Fig. 2) 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 Partitions: Patient, Administration Area (which is a

top partition that is divided into Admission and Accounting middle partitions), and the Medical Area (divided into Medical Evaluation and Exams).

The business analyst has considered several aspects of security. He/she has specified «Nonrepudiation» has been defined over the control flow that goes from the action "Fill Admission Request" to the actions "Capture Insurance Information" and "Check Clinical Data" with the aim of avoiding the denial of the "Admission Request" reception. «Privacy» (confidentiality) and «AccessControl» has been defined over the Interruptible Activity Region. A «SecurityRole» can be derived from this specification. Admission/Accounting will be a role. All objects in an interruptible region must be considered for permissions specification. Access control specification has been complemented with an audit requirement. The audit requirement implies that it must register information about the role and permissions. Finally, the business analyst has specified Integrity (high) requirement for Data Store "Clinical Information".

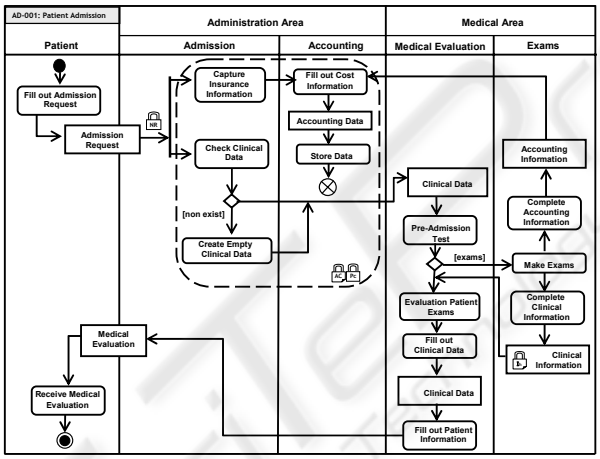

Fig. 2. Patients Admission in a Medical Institution.

In Table 6, the results of the application of the transformations defined with QVT as well as the application of refinement rules are described.

Table 6. QVT and refinement rules applied to Patient Admission Business Process.

Rule	Use case element
R1	Actors: Patient, Administration Area, Admission, Accounting, Medical Area, Medical Evaluation, and Exams
R2	Actor: Region 01
R3	Use cases: Fill out Admission Request, Receive Medical Evaluation, Capture Insurance Information, Check Clinical Data, Create Empty Clinical Data, Fill out Cost Information, Store Data, Pre-Admission Test, Evaluation Patient Exams, Fill out Clinical Data, Fill out Patient Information, Complete Accounting Information, Make Exams and Complete Clinical information
R4	Subjects: Access Control and Privacy, Non Repudiation, and Integrity
R5	Actor: Security Staff
RR1	Subject: Patient Admission
RR2	Subjects: Access Control and Privacy in AdmissionAccounting, Non Repudiation in Admission Request, and Integrity (high) in Clinical Information
RR3	Actor: AdmissionAccounting
RR4	Main Actor: Patient
RR5	Actors: Administration Area (Admission and Accounting) and Medical Area (Medical Evaluation and Exams)
RR6	Use Cases: Capture Insurance Information, Check Clinical Data and Create Empty Clinical Data in Admission Partition and AdmissionAccounting Region. Fill out Cost Information and Store Data in Accounting Partition and AdmissionAccounting Region

In Fig. 3, use cases derived from the business process specifications for the admission of patients are graphically shown. On the right side, the use case related to the security requirements "*Access Control*" and "*Privacy*" is shown. In this figure, we have omitted the tasks related to the actor "*AdmissionAccounting*" because they have already been included in the general use case (left side)

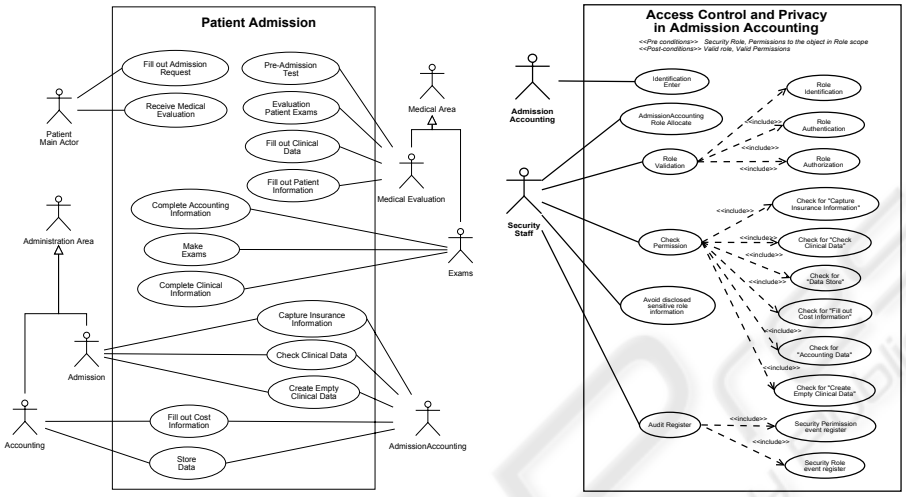

Fig. 3. Patient Admission and Access Control/Privacy use cases specification.

In Fig. 4, use cases related to the security requirements "*Integrity*" and "*Non Repudiation*" specified in the activity diagram are shown. In them, we have also omitted the use cases related to the actors "*Exams*", "*Patient*" and "*Admission*" since they have been considered in the general use case (Fig. 3).

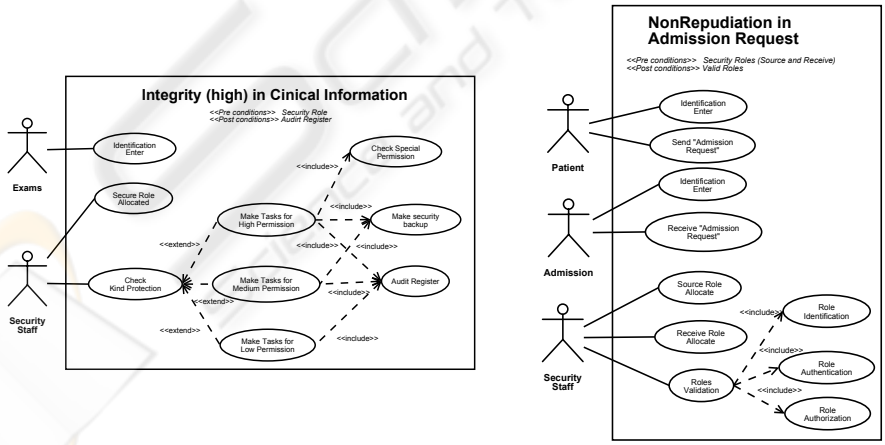

Fig. 4. *Integrity* and *Non Repudiation* security use cases specification.

6 Conclusions and Ongoing Work

The improvement presented by the UML 2.0 language related to business process specification allow us to consider such specifications as a source of requirements to be used as an input in any software development process. In previous works, we have proposed an extension to the UML 2.0 Activity Diagram through which it is possible to specify security requirements at a high level of abstraction. In this paper, we have presented a set of CIM to PIM transformations that let us obtain, from a business process built by a business analyst, use cases, without and with security, that can be used in a systematic and ordered software development process.

Ongoing work is oriented to enrich transformations to make it possible to obtain more complete use case models. Together with it, our future work has the purpose of instantiating UP with the objective of incorporating the artifacts that we have generated. Finally, our future work has the aim of optimizing the prototype that we have created to carry out the transformations necessary for improving specification reuse and documentation.

Acknowledgements

This research is part of the following projects: DIMENSIONS (PBC-05-012-1), and MISTICO (PBC06-0082) both partiality supported by FEDER and the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha", Spain, COMPETISOFT (506PI287), granted by CYTED, ENIGMAS (PIB-05-058), and FAMOSO (2006: FIT-340000-2006-67).

References

1. Aguilar-Savén, R. S.; *Business process modelling: Review and framework*, International Journal of Production Economics. Vol. 90 (2). (2004). pp.129-149.
2. Alexander, I. F.; *Misuse Cases: Use Cases with Hostile Intent*, IEEE Software. Vol. 20 (1). (2003). pp.58-66.
3. Backes, M., Pfitzmann, B. and Waider, M.; *Security in Business Process Engineering*, International Conference on Business Process Management (BPM). Vol. 2678, LNCS. Eindhoven, Netherlands. (2003). pp.168-183.
4. Dijkman, R. M. and Joosten, S. M. M.; *An Algorithm to Derive Use Cases from Business Processes*, 6th IASTED International Conference on Software Engineering and Applications (SEA). Boston, MA, USA,. (2002). pp.679-684.
5. Eriksson, H.-E. and Penker, M., *Business Modeling with UML*, OMG Press. (2001).
6. Firesmith, D.; *Security Use Case*, Journal of Object Technology. Vol. 2 (3). (2003). pp.53-64.
7. Firesmith, D.; *Specifying Reusable Security Requirements*, Journal of Object Technology. Vol. 3 (1), January-February. (2004). pp.61-75.
8. Herrmann, G. and Pernul, G.; *Viewing Business Process Security from Different Perspectives*, 11th International Bled Electronic Commerce Conference. Slovenia. (1998). pp.89-103.

9. Herrmann, P. and Herrmann, G.; *Security requirement analysis of business processes*, Electronic Commerce Research. Vol. 6 (3-4). (2006). pp.305-335.
10. Jacobson, I., Booch, G. and Rumbaugh, J., *The Unified Software Development Process*, (1999). 463 p.
11. Jürjens, J.; *Using UMLsec and goal trees for secure systems development*, Proceedings of the 2002 ACM Symposium on Applied Computing (SAC). Madrid, Spain. (2002). pp.1026-1030.
12. Liew, P., Kontogiannis, P. and Tong, T.; *A Framework for Business Model Driven Development*, 12 International Workshop on Software Technology and Engineering Practice (STEP). (2004). pp.47-56.
13. Lopez, J., Montenegro, J. A., Vivas, J. L., Okamoto, E. and Dawson, E.; *Specification and design of advanced authentication and authorization services*, Computer Standards & Interfaces. Vol. 27 (5). (2005). pp.467-478.
14. 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.
15. Monfort, V. and Kadima, H.; *Extending The Unified Process With Composition*, Electronic Notes in Theoretical Computer Science. Vol. 65 (4). (2002). pp.1-13.
16. Object Management Group; *MDA Guide Version 1.0.1*. In http://www.omg.org/docs/omg/03-06-01.pdf. (2003).
17. Quirchmayr, G.; *Survivability and Business Continuity Management*, ACSW Frontiers 2004 Workshops. Dunedin, New Zealand. (2004). pp.3-6.
18. QVT, *Meta Object Facility (MOF) 2.0 Query/View/Transformation Specification*, OMG Adopted Specification ptc/05-11-01, (2005). 204 p.
19. Rodríguez, A., Fernández-Medina, E. and Piattini, M.; *Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes*, 3rd International Conference on Trust, Privacy and Security in Digital Business (TrustBus). Vol. 4083. Krakow-Poland. (2006). pp.51-61.
20. Röhm, A. W., Pernul, G. and Herrmann, G.; *Modelling Secure and Fair Electronic Commerce*, 14th. Annual Computer Security Applications Conference. Scottsdale, Arizona. (1998). pp.155-164.
21. 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.
22. Rungworawut, W. and Senivongse, T.; *A Guideline to Mapping Business Processes to UML Class Diagrams*, WSEAS Transactions on Computers. Vol. 4 (11). (2005). pp.1526-1533.
23. Sindre, G. and Opdahl, A.; *Capturing Security Requirements through Misuse Cases*, Proceedings of Norsk informatikkonferanse (NIK). Trondheim, Norway. (2001). pp.219-230.
24. Štolfa, S. and Vondrák, I.; *A Description of Business Process Modeling as a Tool for Definition of Requirements Specification*, Systems Integration 12th Annual International Conference. Prague, Czech Republic. (2004). pp.463-469.
25. Vivas, J. L., Montenegro, J. A. and Lopez, J.; *Towards a Business Process-Driven Framework for security Engineering with the UML*, Information Security: 6th International Conference, ISC. Bristol, U.K. (2003). pp.381-395.