IEICE TRANSACTIONS

on Information and Systems

VOL.E90-D
NO.4
APRIL 2007

A PUBLICATION OF THE INFORMATION AND SYSTEMS SOCIETY

The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER

A BPMN Extension for the Modeling of Security Requirements in Business Processes

Alfonso RODRÍGUEZ[†a)], *Nonmember*, **Eduardo FERNÁNDEZ-MEDINA**[††], *Member*, *and* **Mario PIATTINI**[††], *Nonmember*

SUMMARY Business Processes are considered a crucial issue by many enterprises 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 through business process modeling. We will summarize our Business Process Modeling Notation extension for modeling secure business process through Business Process Diagrams, and we will apply this approach to a typical health-care business process.

key words: *security requirement, business process, BPMN*

1. Introduction

The key to maintain competitiveness is the ability of a company 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. Business Processes, defined as a set of procedures or activities which collectively pursue a business objective or policy goal [1], 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 [2]. This security violation causes losses. For this reason, it is necessary to protect computers and their systems in the best possible way. Best possible security does not necessarily mean absolute security, but a reasonable high security level in relation to the given limitations [3].

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 [4]. The reason is mainly due to the fact that the expert in the business process domain is not an expert in security [5]. Frequently, security is considered after the definition of the system. This approach often leads to problems, which most of the times become into security vulnerabilities [6], which clearly justify the need of increasing the effort in the pre-development phases, where fixing the bugs is cheaper [7]. Moreover, most requirements engineers are not trained at all in security, and the few of them 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 [8].

If we consider that empirical studies show that it is common at the business process level that customers and end users are able to express their security needs [7], then it is possible to capture at a high level, security requirements easily identifiable by those who model business processes. Besides, requirements specification usually results in a specification of the software system which should be as exact as possible [9], since, effective business process models facilitate discussions among different stakeholders in the business, allowing them to agree on the key fundamentals as well as to work towards common goals [10].

For business process modeling, there are several languages and notations [11]. However, BPMN (Business Process Modeling Notation) and UML (Unified Modeling Language) are considered the main standards [12]. Nevertheless, we have had the opportunity to check that security aspects are not included in the Business Process Modeling either in the first version of BPMN [13] carried out by the BPMI (Business Process Management Initiative) or in the new version [14], that arised after the link [15] to the OMG (Object Management Group).

Our work considers a BPMN extension that allows us to incorporate security requirements into Business Process Diagrams from the perspective of the business analyst.

Our proposal is based on the MDA (Model Driven Architecture) approach. We will define early requirements identification using BPMN 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

Manuscript received July 6, 2006.
Manuscript revised September 29, 2006.

[†]The author is with the Departamento de Auditoría e Informática, Universidad del Bio Bio, Chillán, Chile.
[††]The authors are with the ALARCOS Research Group, UCLM-Soluziona Research and Development Institute, University of Castilla-La Mancha, Ciudad Real, Spain.
a) E-mail: alrodriguez@inf-cr.uclm.es

DOI: 10.1093/ietisy/e90–d.4.745

other associated with security experts. Thus, a system can be modeled at different levels of abstraction or from different perspectives [16]. In this paper we have deepened in the first perspective.

The remainder of this paper is structured as follows: in Sect. 2, we will summarize the main issues about security in business processes. In Sect. 3 we will put forward an overview regarding notations for business processes but we will pay special attention to BPMN. In addition, we will propose a BPMN metamodel that shows the core elements used in Business Process Diagram (BPD). In Sect. 4 we will propose a BPMN extension to represent security requirements from the business analyst's perspective. Finally, in Sect. 5, we will present an example to show our proposal and in Sect. 6 our conclusion will be drawn.

2. 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 [8]. And in the second place, security has been integrated into an application in an ad-hoc manner, often during the actual implementation process [4], during the system administration phase [16] or it has been considered like outsourcing [17].

In the review of related works, we have had the possibility to check that not only in those works directly referring to security regarding business processes [4], [5], [18]–[21] but also in those that have to do with security and information systems [6], [9], [16], [22]–[28], security specifications made by the business analyst are absent. In spite of this fact, we would like to highlight an approach to model security that takes into account several perspectives. In the work presented in [5], 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.

Concerning the security requirements that can be modeled in business processes, it is necessary to consider that security requirements in any application at the highest level of abstraction will tend to have the same basic kinds of valuable and potentially vulnerable assets [29].

Moreover, it is necessary to take into account the fact that capturing the security requirements of a system is a hard task that must be established at the initial stages of system development, and business spruces offer a view of business structure that is very suitable as a basis for the elicitation and specification of security requirements. Business process representations may in this way present in all stages of system development different levels of abstraction appropriate for each stage [7]. Consequently, we believe that business analysts can integrate their view about business security into the business process perspective and in addition 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 [29].

Finally, none of the proposals related to security specifications in business processes and/or information systems that have been analysed deal with security requirements specifications made by the business analyst. We think that this perspective will make security specifications more valuable since it allows security experts to incorporate new elements into their analysis. In addition, we consider that the improvement of the standard languages for business process representation can improve the representation of these requirements as well.

3. 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 [30]. 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 [31].

Among the techniques that have been used for business process modeling, we can highlight 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 [11], [32].

At present, and according to the state of the business process modeling industry [12], [33], it is possible to identify UML [34] and BPMN [13], [14], among the main standards.

Regarding BPMN, it is a new proposal whose notation considers a unique diagram for the representation of processes 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 Business Process Execution Language For Web Services (BPEL4WS). To do so, the notation is supported by a modeling language,

Table 1 Core modeling elements.

Element	Notation
POOL: A Pool represents a Participant in a Process. It also acts as a "swimlane" and a graphical container for partitioning a set of activities from other Pools, usually in the context of B2B situations.	
LANE: A Lane is a sub-partition within a Pool and will extend the entire length of the Pool, either vertically or horizontally. Lanes are used to organize and categorize activities.	
DATA OBJECTS: They are considered Artifacts because they do not have any direct effect on the Sequence Flow or Message Flow of the Process, but they do provide information about what activities require to be performed and/or what they produce.	Name
GROUP: A grouping of activities that does not affect the Sequence Flow. The grouping can be used for documentation or analysis purposes. Groups can also be used to identify the activities of a distributed transaction that is shown across Pools.	
TEXT ANNOTATIONS: They are a mechanism for a modeler to provide additional information for the reader of a BPMN Diagram.	Descriptive Text Here
SEQUENCE FLOW: A Sequence Flow is used to show the order that activities will be performed in a Process.	
ASSOCIATION: An Association is used to associate information with Flow Objects. Text and graphical non-Flow Objects can be associated with the Flow Objects.	
MESSAGE FLOW: A Message Flow is used to show the flow of messages between two participants that are prepared to send and receive them. In BPMN, two separate Pools in the Diagram will represent the two participants (e.g., business entities or business roles).	
EVENT: An event is something that "happens" during the course of a business process. These events affect the flow of the process and usually have a cause (trigger) or an impact (result). Events are circles with open centers to allow internal markers to differentiate different triggers or results. There are three types of Events, based on when they affect the flow: Start, Intermediate, and End.	
ACTIVITY: An activity is a generic term for work that company performs. An activity can be atomic or non-atomic (compound). The types of activities that are a part of a Process Model are: Process, Sub-Process, and Task. Tasks and Sub-Processes are rounded rectangles. Processes are either unbounded or a container within a Pool.	
GATEWAY: A Gateway is used to control the divergence and convergence of Sequence Flow. Thus, it will determine branching, forking, merging, and joining of paths. Internal Markers will indicate the type of behavior control.	

Business Process Modeling Language (BPML) and a query language, Business Process Query Language (BPQL) [35].

In this paper, we will use BPMN because we consider that, although there are several reasons to use this notation [35], 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 [14], [36].

In Table 1, we can see a description of the BPD core elements and their corresponding notations. With these elements, we have created a BPD metamodel (Fig. 1) where we have shown the main relationship between core modeling elements. To do so, we have created the class known as BusinessProcessDiagram. This class allows us to relate all BPD elements used to represent a specific business process. This metamodel will allow us to explain our proposal later on.

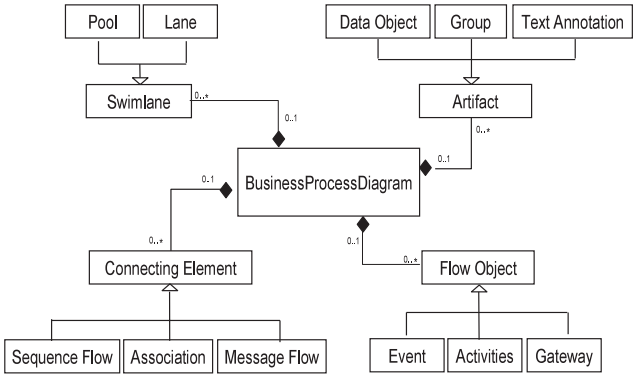

Fig. 1 Business process diagrams metamodel.

4. 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 [5]. 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 security requirements. However, among the set of symbols used for the construction of the BPD [14], *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 [36]. 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 could be used to express security requirements, mainly through Text Annotations, we consider that an explicit identification of them will facilitate modeling and will help us obtain a better interpretation by security specialists.

In order to explain our proposal we will initially show a model with the security elements (Fig. 2) that we want to incorporate into the metamodel that we have created and that is shown in Fig. 1. We have complemented the extended metamodel (Fig. 3) with security requirements. In Table 2 we will extensively show the relation between the BPD elements and the new security elements.

The mechanism of extension stated by BPMN lets us add marks or indications to the already defined graphical elements [14]. In our proposal we have associated a symbol (padlock in Fig. 2) to represent security requirements in a standard way. Each security requirement will be specified with a capital letter in the centre of the symbol (see details in Table 4). We have considered to represent security requirements (non repudiation, attack harm detection,

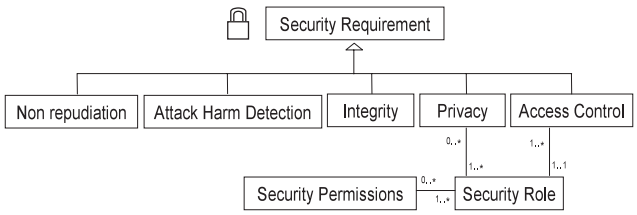

Fig. 2 Security requirement and notation associated.

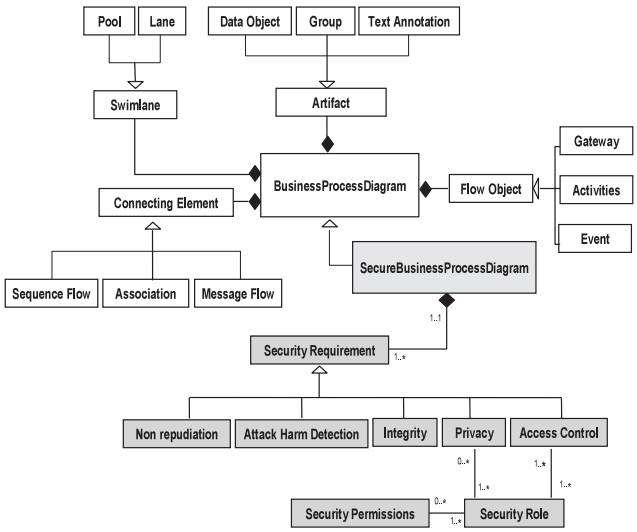

Fig. 3 BPD metamodel with security requirement.

Table 2 New security elements and element of BPD.

	Business Process Diagrams elements					
Security Elements	Pool	Lane	Group	Activity	Message Flow	Data Object
Non repudiation					✓	
AttackHarmDetection	✓	✓	✓	✓	✓	✓
Integrity					✓	✓
Privacy	✓	✓	✓			
Access Control	✓	✓	✓	✓		
Security Role	✓	✓	✓			
Security Permissions				✓	✓	✓

integrity, privacy and access control proposed in [29]), security role, associated with privacy and/or access control specification, and security permission associated with security role (see Fig. 3). The security auditing is not considered in an explicit way because it underlies each security requirement and will be explained beside each description.

In Fig. 3, we will show a BPD (core modeling elements) metamodel. This figure includes the security requirements which have been represented in the specifications of our proposal (dark-coloured). We have inherited from `BusinessProcessDiagram` the class `SecureBusinessProcessDiagram` that will be used to contain the specifications related to requirements, roles and security permissions.

In Table 2 we show the relation between security specification and BPD element. Any security requirement (non repudiation, attack harm detection, integrity, privacy, or access control) can be *added* to BPD elements.

Table 3 New data type.

Name	Description
SecReqType	It represents a type of security requirement. It must be specified for Non Repudiation (NR), Attack/Harm Detection (AD), Integrity (I), Privacy (P) or Access Control (AC).
PerOperations	It is an enumeration for possible operations over objects in activity diagrams. These operations are related to permissions granted over the object
ProtectDegree	It is an abstract level that represents criticality. This degree can be low (l), medium (m) or high (h).
PrivacyType	It consists of anonymity (a) or confidentiality (c).
AuditingValues	It represents different security events related to the security requirement specification in business processes. They will be used in later auditing

`Non repudiation` can be specified over a Message Flow. This means that the interaction cannot be denied.

≪*AttackHarmDetection*≫ specified over Pool, Lane or Group implies that all elements that these BPD elements contain must consider a mechanism that allows us to detect, register and notify an attack attempt or a successful attack. This requirement specified over Activity Message Flow or Data Object has the same meaning.

The specification of ≪*Integrity*≫ over Message Flow means that this must be protected to avoid the intentional and non-authorized corruption of its content. The meaning is the same when Integrity is specified over Data Object.

The security requirement ≪*Privacy*≫ indicated in Pool, Lane or Group implies that it must be considered a mechanism that avoids that non-authorized third parties obtain information about either the identity of Pool, Lane or Group or sensible information about them.

≪*AccessControl*≫ requirement can be specified over Pool, Lane, Group or Activity. It has always the same meaning since its aim is to express the need to avoid that non-authorized third parties access to the elements included in each one of these BPD elements.

≪*SecurityRole*≫ and ≪*SecurityPermissions*≫, in spite of the fact that they are associated with some BPD elements, cannot be directly specified over them. The described relationship for Role is indirectly obtained through the specifications of ≪*AccessControl*≫ and/or ≪*Privacy*≫. The link between ≪*SecurityPermissions*≫ and Activity, Message Flow and Data Object is derived from the ≪*AccessControl*≫ specifications.

The Security Auditing is not represented in an explicit way because this specification will be described in each security requirement (see Table 3).

In addition, we need the definitions of some data types to be used in security specification. In Table 3, we will show the data type with name, description and values associated.

In Table 4 we will show the stereotypes for secure activity specifications extensively. Each stereotype specification contains: name, description, notation, constrains and tagged values.

We have used OCL (Object Constraint Language) [37],

Table 4 Security stereotypes specifications.

Name	SecureBusinessProcessDiagram
Description	A secure activity diagram contains security specification related to requirements, role identifications and permissions
Constrains	- It must be associated at least with one SecurityRequirement **context** SecureActivityDiagram **inv**: self.SecurityRequirement–>size()>=1
Name	SecurityRole
Description	It contains a role specification. This role must be obtained from access control and/or privacy specifications
Constrains	- A security role can be derived from: Pool, Lane and/or Group. (see Table 2) - It must be associated with an access control specification and can be associated with privacy and security permissions **context** SecurityRole **inv**: self.AccessControl –> size() >= 1 **context** SecurityRole **inv**: self.Privacy –> size()>= 0 **context** SecurityRole **inv**: self.SecurityPermission –> size()>= 0
Name	SecurityPermission
Description	It contains permission specifications. A permission specification must contain details about the objects and operations involved

Constrains	- It must be associated with security role specification
	context SecurityPermission **inv**: self.SecurityRole –>size()>= 1
	- It must be associated with Activity, Message Flow or Data Object
	context SecurityPermissions **inv**:
	self.Activity.size+self.MessageFlow.size+self.DataObject.size=1
	- It must be specified such as Objects and Operations pairs.
	Context SecurityPermissions **inv**:
	if self.Activity–>size()=1 then
	self.SecPerOperations=”Execution” or
	self.SecPerOperations=”Checkexecution”
	endif
	if self.DataObject–>size()=1 then
	self.SecPerOperations=”Update” or self.operacion=”Create” or
	self.SecPerOperations=”Read” or self.operacion=”Delete”
	endif
	if self.MessageFlow–>size()=1 then
	self.SecPerOperations=”Sendreceive” or
	self.SecPerOperations=”Checksendreceive”
	endif

Tagged Values	SecurityPermissionOperation: SecPerOperations
Name	SecurityRequirement — Notation: 
Description	Abstract class containing security requirements specifications. Each security requirement type must be indicated in some of its subclasses.
Constrains	- A security requirement must be associated with a secure activity **context** SecurityRequirement **inv**: self.SecureActivity –>size()=1 - The notation must be completed for each security requirement. It must be used one security requirement type.
Tagged Values	SecurityRequirementType: SecReqType
Name	Nonrepudiation — Notation: 
Description	It establishes the need to avoid the denial of any aspect of the interaction. An auditing requirement can be indicated in Comment
Constrains	- It can be only specified in the diagram elements indicated in Table 2.
Tagged Values	AvNr: AuditingValues **context** Nonrepudiation **inv**: self.AvNr=“ElementName” or self.AvNr=“SourceName” or self.AvNr=“DestinationName” or self.AvNr=“DateTimeSend” or self.AvNr=“DateTimeReceive”
Name	AttackHarmDetection — Notation: 
Description	It indicates the degree to which the attempt or success of attacks or damages is detected, registered and notified. An auditing requirement can be indicated in Comment
Constrains	- It can be only specified in the diagram elements indicated in Table 2.
Tagged Values	AvAD: AuditingValues **context** AttackHarmDetection **inv**: self.AvAD=“ElementName” or self.AvAD=“Date” or self.AvAD=“Time”
Name	Integrity — Notation: 
Description	It establishes the degree of protection of intentional and non authorized corruption. An auditing requirement can be indicated in Comment.
Constrains	- It can be only specified in the diagram elements indicated in Table 2. - The Protection Degree must be specified by adding a lower case letter[1] according to PDI tagged value.
Tagged Values	PDI : ProtectDegree AvI: AuditingValues **context** Integrity **inv**: self.AvI=“ElementName” or self.AvI=“Date” or self.AvI=“Time”
Name	Privacy — Notation: 
Description	It indicates the degree to which non authorized parts are avoided to obtain sensitive information. An auditing requirement can be indicated in Comment.
Constrains	- It can be only specified in the diagram elements indicated in Table 2. - A privacy requirement has one security role specification **context** Privacy **inv**: self.SecurityRole –> size() = 1 - The Privacy Type must be specified adding a lower case letter[2] according to Pv tagged value. If privacy type is not specified then anonymity and confidentiality are considered.
Tagged Values	Pv: PrivacyType AvPv: AuditingValues **context** Privacy **inv**: self.AvPv=“RoleName” or self.AvPv=“Date” or self.AvPv=“Time”
Name	AccessControl — Notation: 
Description	It establishes the need to define and/or intensify the access control mechanisms (identification, authentication and authorization) to restrict access to certain components in a BPD. An auditing requirement can be indicated in Comment.
Constrains	- It can be only specified in the diagram elements indicated in Table 2. - It is valid only if it is specified at least one security requirement. **context** AccessControl **inv**: self.SecurityRole –> size() >= 1
Tagged Values	AvAC: AuditingValues **context** AccessControl **inv**: self.AvAC=“RoleName” or self.AvAC=“Date” or self.AvAC=“Time”

[1] The letter χ can be replaced by **l** for low, **m** for medium or **h** for high.

[2] The letter χ can be replaced by **a** for anonymity, **c** for confidentiality or can be omitted If Privacy Type is not specified, then both anonymity and confidentiality, are considered.

[38] to specify restrictions over the BPMN metamodel since it lets us avoid the normal ambiguity of natural language.

5. Example

Our illustrative example (see Fig. 4) describes a typical business process for the admission of patients in a health-care institution. In this case, the business analyst identified the Pool; `Patient` (individual who receives medical care and who must fill out an admission request), `Administration Area` (which is a Pool that is divided into two Lanes), where the Medical Institution records details about costs and insurances, and finally, the Pool `Medical Area` (divided into lanes `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 specification.

The business analyst has considered several aspects of security. He/she has specified Privacy (confidentiality) for `Pool Patient`, with the aim of preventing the disclosure of sensitive information about Patients. Non repudiation has been defined over the message flow that goes from the pool `Patient` to the lane `Admission` with the aim of avoiding the denial of the “Admission Request” reception. Access Control has been defined over the lane `Exams`. A Security Role can be derived from this specification. `Exams` will be a role. All objects in the lane must be considered for permissions specification (see Table 5). Access Control specification has been complemented with audit requirement. This implies that it must register role name, date and time of all events related to the lane. Integrity (high) requirement has been specified for Data Object “Clinical Information”. Finally, the business analyst has specified Attack Harm Detection for “Medical Evaluation” with audit requirement. All events related to attempt or success of attacks or damages must be registered.

Finally, the business analyst has specified Attack Harm Detection with audit requirement. All events related to attempt or success of attacks or damages are registered (names in this case are clinical information, date and time).

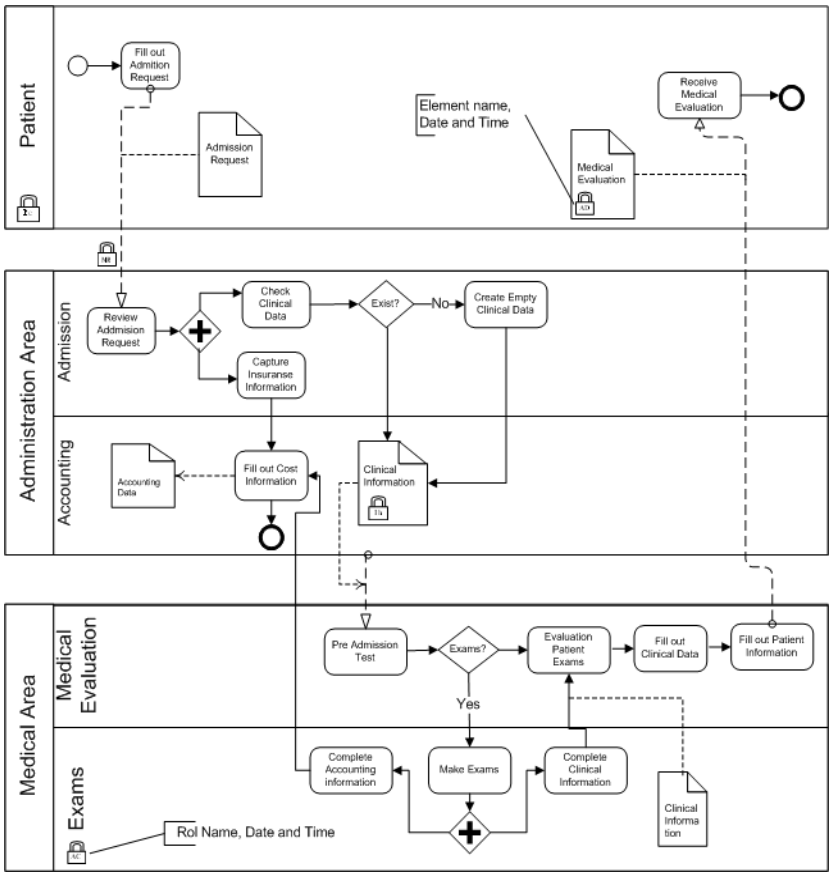

Fig. 4 Admission of patients in a medical institution.

Table 5 Security role and security permission specifications.

	Permissions		
Role	Object		Operations
Exams	Activity	Complete Accounting Information Make Exams Complete Clinical information	Execution CheckExecution Execution
	Data Object	Accounting Data	Update

6. Conclusions and Future Work

The improvement experienced in the languages for business processes modeling, especially BPMN, opens an opportunity to incorporate security requirements that allow us to improve this aspect of the systems from early stages into software development. In this paper, we have presented a BPMN metamodel with core element and extension that allows us to incorporate security requirements into Business Process Diagrams that will increase the scope of the expressive ability of business analysts. With this extension, business analysts will be able to express security requirements from their own perspective. Moreover, it will be possible to refine such requirements by security experts for software developers to be able to include them in the end product. Consequently, the next step should be that of applying an MDA approach to transform the model (including the security requirements) into most concrete models (i.e. execution models). Therefore, future work must be oriented to enrich the security requirements specifications. Furthermore, it is necessary to incorporate the viewpoint of the security expert into them in order to make implementation possible.

Acknowledgments

This research is part of the following projects: DIMENSIONS (PBC-05-012-1) and MISTICO, both supported by FEDER and the “Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha”, and COMPETISOFT granted by CYTED.

References

[1] WfMC, Workflow Management Coalition: Terminology & Glossary, 1999.
[2] G. Quirchmayr, “Survivability and business continuity management,” ACSW Frontiers 2004 Workshops, Dunedin, New Zealand, 2004.
[3] A. Zuccato, “Holistic security requirement engineering for electronic commerce,” Computers & Security, vol.23, no.1, pp.63–76, 2004.
[4] M. Backes, B. Pfitzmann, and M. Waider, “Security in business process engineering,” International Conference on Business Process Management (BPM), Eindhoven, The Netherlands, 2003.
[5] G. Herrmann and G. Pernul, “Viewing business process security from different perspectives,” 11th International Bled Electronic Commerce Conference, Slovenia, 1998.

[6] H. Mouratidis, P. Giorgini, and G.A. Manson, "When security meets software engineering: A case of modelling secure information systems," Information Systems, vol.30, no.8, pp.609–629, 2005.
[7] J. Lopez, J.A. Montenegro, J.L. Vivas, E. Okamoto, and E. Dawson, "Specification and design of advanced authentication and authorization services," Computer Standards & Interfaces, vol.27, no.5, pp.467–478, 2005.
[8] D. Firesmith, "Engineering security requirements," J. Object Technology, vol.2, no.1, Jan.-Feb., pp.53–68, 2003.
[9] C. Artelsmair and R. Wagner, "Towards a security engineering process," The 7th World Multiconference on Systemics, Cybernetics and Informatics, Orlando, Florida, USA, 2003.
[10] H.-E. Eriksson and M. Penker, Business Modeling with UML, OMG Press, 2001.
[11] G.M. Giaglis, "A taxonomy of business process modelling and information systems modelling techniques," Int. J. Flexible Manufacturing Systems, vol.13, no.2, pp.209–228, 2001.
[12] Mega, "Business process modeling and standardization," in http://www.bpmg.org/downloads/Articles/Article-MEGA-BusinessProcessModeling&StandardizationEN.pdf, 2004.
[13] BPMN, "Business process modeling notation (BPMN)," in http://www.bpmn.org/Documents/BPMN%20V1-0%20May%203%202004.pdf, 2004.
[14] BPMN, "Business process modeling notation specification," OMG Final Adopted Specification, dtc/06-02-01. In http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf, 2006.
[15] D.S. Frankel, "BPMI and OMG: The BPM merger," MDA Journal. In http://www.bptrends.com/publicationfiles/02-06%20COL%20MDA%20BPMI-OMG%20-%20Frankel1.pdf, 2006.
[16] T. Lodderstedt, D. Basin, and J. Doser, "SecureUML: A UML-based modeling language for model-driven security," The Unified Modeling Language, 5th International Conference, Dresden, Germany, 2002.
[17] A. Maña, D. Ray, F. Sánchez, and M.I. Yagüe, "Integrando la Ingeniería de Seguridad en un Proceso de Ingeniería Software," VIII Reunión Española de Criptología y Seguridad de la Información, RECSI, Leganés, Madrid, España, 2004.
[18] A.W. Röhm, G. Pernul, and G. Herrmann, "Modelling secure and fair electronic commerce," 14th Annual Computer Security Applications Conference, Scottsdale, Arizona, 1998.
[19] J.L. Vivas, J.A. Montenegro, and J. Lopez, "Towards a business process-driven framework for security engineering with the UML," Information Security: 6th International Conference, ISC, Bristol, U.K., 2003.
[20] A. Maña, J.A. Montenegro, C. Rudolph, and J.L. Vivas, "A business process-driven approach to security engineering," 14th International Workshop on Database and Expert Systems Applications (DEXA), Prague, Czech Republic, 2003.
[21] A.W. Röhm, G. Herrmann, and G. Pernul, "A language for modelling secure business transactions," 15th Annual Computer Security Applications Conference, Phoenix, Arizona, 1999.
[22] H. Abie, D.B. Aredo, T. Kristoffersen, S. Mazaher, and T. Raguin, "Integrating a security requirement language with UML," 7th International Conference, The UML: Modelling Languages and Applications, Lisbon, Portugal, 2004.
[23] J. Jürjens, "Towards development of secure systems using UMLsec," Fundamental Approaches to Software Engineering, 4th International Conference, FASE 2001 at ETAPS-2001, Genova, Italy, 2001.
[24] J. Jürjens, "Using UMLsec and goal trees for secure systems development," Proc. 2002 ACM Symposium on Applied Computing (SAC), Madrid, Spain, 2002.
[25] D. Basin, J. Doser, and T. Lodderstedt, "Model driven security for process-oriented systems," SACMAT 2003, 8th ACM Symposium on Access Control Models and Technologies, Villa Gallia, Como, Italy, 2003.
[26] H. Mouratidis, P. Giorgini, and G.A. Manson, "Integrating security and systems engineering: Towards the modelling of secure information systems," Advanced Information Systems Engineering, 15th International Conference, CAiSE 2003, Proceedings, vol.2681, pp.63–78, Klagenfurt, Austria, June 2003.
[27] M.T. Siponen, "Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods," Information and Organization, vol.15, pp.339–375, 2005.
[28] M. Zulkernine and S.I. Ahamed, "Software security engineering: Toward unifying software engineering and security engineering," in Enterprise Information Systems Assurance and Systems Security: Managerial and Technical Issues, Idea Group, ed. M. Warkentin and R. Vaughn, pp.215–232, 2006.
[29] D. Firesmith, "Specifying reusable security requirements," Journal of Object Technology, vol.3, no.1, pp.61–75, Jan.-Feb. 2004.
[30] N. Castela, J. Tribolet, A. Silva, and A. Guerra, "Business process modeling with UML," Proc. 3rd International Conference on Enterprise Information Systems, Setubal, Portugal, 2001.
[31] I. Bider, "Choosing approach to business process modeling — Practical perspective," in http://www.ibissoft.se/english/howto.pdf, 2003.
[32] T. Dufresne and J. Martin, Process Modeling for e-Business, George Mason University, 2003.
[33] A. Lonjon, "Business process modeling and standardization," BP-Trends, in http://www.bptrends.com/, 2004.
[34] OMG, "Object management group," in http://www.omg.org/, 2004.
[35] M. Owen and J. Raj, "BPMN and business process management; Introduction to the new business process modeling standard," in http://www.bpmn.org/Documents/6AD5D16960.BPMN_and_BPM.pdf, 2003.
[36] S.A. White, Introduction to BPMN, IBM Corporation, in http://www.ebpml.org/bpmn.htm, 2004.
[37] Object Management Group, "OCL 2.0 specification, version 2.0," in http://www.omg.org/docs/ptc/05-06-06.pdf, 2005.
[38] J. Warmer and A. Kleppe, The Object Constraint Language: Getting Your Models Ready for MDA, Pearson Education, 2003.

Alfonso Rodríguez is MBA from the Universidad del Bio-Bio (Chile), and a PhD student at the Escuela Superior de Informática of the Universidad de Castilla-La Mancha at Ciudad Real (Spain). He is Assistant Professor at the Departamento de Auditoría e Informática of the Universidad del Bio Bio (Chillán, Chile). His research activities are security in business process and information systems.

Eduardo Fernández-Medina is PhD and MSc in Computer Science. He is Assistant Professor at the Escuela Superior de Informática of the Universidad de Castilla-La Mancha at Ciudad Real (Spain). His research activities are security in databases, data warehouses, web services and information systems, and also in security metrics. He is the co-editor of several books and chapter books on these subjects, and has several dozens of papers in national and international conferences. He participates at the ALARCOS research group of the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain. He belongs to various professional and research associations (ATI, AEC, AENOR, IFIP WG11.3 etc.).

Mario Piattini is a professor in the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain. He has a M.Sc. and Ph.D. in Computer Science from the Politechnical University of Madrid and is a Certified Information System Auditor Manager by ISACA (Information System Audit and Control Association). Author of several books and papers on databases, software engineering and information systems, he leads the ALARCOS research group of the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain. His research interests are: advanced database design, database quality, software metrics, software maintenance and security in information systems. He has co-edited several books: 'Advanced Databases: Technology and Design,' 2000, Artech House, UK; 'Auditing Information Systems,' Idea Group Publishing, 2000, USA.