International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:6, No:2, 2012

A New Framework to Model a Secure E-Commerce System

A. Youseef, F. Liu

***Abstract*—**The existing information system (IS) developments methods are not met the requirements to resolve the security related IS problems and they fail to provide a successful integration of security and systems engineering during all development process stages. Hence, the security should be considered during the whole software development process and identified with the requirements specification. This paper aims to propose an integrated security and IS engineering approach in all software development process stages by using *i** language. This proposed framework categorizes into three separate parts: modelling business environment part, modelling information technology system part and modelling IS security part. The results show that considering security IS goals in the whole system development process can have a positive influence on system implementation and better meet business expectations.

***Keywords*—**Business Process Modelling (BPM), Information System Security, Software Development Process, Requirement Engineering.

I. Introduction

INFORMATION SYSTEMS (IS) are used in almost every area of life, for example, in the military, health sciences, telecommunication, e-commerce etc, hence there is a need to ensure that these systems are secure as many systems contain private data which should only be available to authorized parties. For example, the mobile phone order management process in a telecommunication company contains the customers' personal information and credit card information, thus this system must be secure to ensure the customers' privacy.

Security is considered a non-functional requirement by the software engineering community [1]. Non-functional requirements represent constraints, such as authorized and unauthorized accesses where the systems are operating [2] [3]. Therefore, security requirements must be defined after identifying the system. However, there are many challenges in implementing security into IS. Firstly, security requirements are often complicated to analyze and model. The requirement of separate the functional and non-functional requirements is one main problem in analyzing the non-functional requirements whereas the non-functional requirements could be related to one or set of the functional requirements at the same time. However, when the non-functional requirements are stated separately from the functional requirements, the relationship between them cannot be seen easily. Secondly, IS developers may lack knowledge on developing and modelling a secure system [4] [5].

A. Y. Author is with Umm Alquri University, Makkah, Saudi Arabia (phone: +966 504519903; e-mail: yaalotaibi@students.latrobe.edu.au).
F. L. Author is with La Trobe University, Bundoora,VIC, 3086, Australia. (phone +61 3 9479 1949; e-mail: f.liu@latrobe.edu.au).

Security should be considered throughout the entire business development process and requirements specifications should be identified. If security is only considered in certain stages of the development process, the security requirements will conflict with the system's functional requirements. Therefore, the issue of security must be taken into account with functional requirements during the system development stages in order to limit conflict. This can be done by defining them in the early stages of system development and making attempts to overcome them. However, when security is only added in the late stages of system development, the chance of more conflicts occurring is increased, which may require a lot of money to overcome.

The literature shows that there are many commercial methods, such as ITBPM, OCTAVE, CRAMM, EBIOS, MEHARI, etc available to IT security officers to perform a risk analysis of the security problems and define the security solutions [6] [7] [8]. However, these existing methods do not meet the requirements to resolve security-related IS problems and they fail to facilitate the successful integration of security during all development process stages. Thus, we propose an integrated security and IS engineering approach in all development process stages by using the *i** language. In our proposed framework, there are four stages in software development to create a secure IS: (1) early requirements stage; (2) late requirements stage; (3) architectural design stage; and (4) details design stage.

The remainder of this paper is organized as follows: section II describes the related work of modeling secure IS; section III presents our proposed framework approach; and the conclusion and future research directions are presented in section IV.

II. Related Work

The literature shows that only a few approaches consider security requirements as a primary part of all software development processes. For example, in [1], the authors applied the process-oriented approach to represent security requirements as harmonious goals and used them throughout the software system development. This non-functional requirements proposed framework uses security requirements and permits the system developers to consider design decisions which are related into the represented non-functional requirements.

In [9], the authors proposed an approach to reuse the existing descriptions of the business process to analyze the security requirements and derive the essential security measures. This proposed approach contained four major steps: (1) identifying the general security objectives of the business

process; (2) examining the constructed security objectives, such as actors; (3) examining whether these specifications are consistent or not; and (4) creating a list of essential security measures for every business process component.

In [7] and [10], the authors proposed the requirements engineering approach to model and map IS security goals at an early stage of the software development process in the context of alignment between the business and IS. These approaches consist of five major steps: (1) identifying organizational environments; (2) derivation of information security goals; (3) detecting security requirements from goals; (4) detecting constraint and security requirements; and (5) analyzing risks at the architectural level.

TABLE I
RELATED WORK ON EXISTING SOFTWARE DEVELOPMENT PROCESS STAGES

Reference	Year	Software Development Process Stages			
		Early Requirement	Late Requirement	Architectural Design	Detail Design
[5]	1999	√			
[11]	2001			√	
[12]	2002	√		√	
[9]	2002	√			
[13]	2002			√	
[14]	2003	√			
[7]	2007	√			
[15]	2007			√	
[16]	2008			√	
[17]	2008	√			
[18]	2008	√			
[19]	2009	√		√	
[10]	2011	√			
[20]	2011			√	√

In [11], an extension of the Unified Modelling Language (UML), called UMLsec, was proposed to contain security features in UML model, such as access control and confidentiality. There are four different UML diagrams used in [11]: (1) class diagrams to guarantee that the exchange of data conforms to the security levels; (2) state chart diagrams to avoid the indirect flow of information from high to low values with the object; (3) interaction diagrams to guarantee the accuracy of important security interactions between the objects; and (4) deployment diagrams to guarantee that the physical layer can meet the security requirements in communication. Moreover, in [13], the UML was extended to model security and the authors presented a security modelling language called SecureUML. The authors described how UML could be used to identify access control-related information in the whole application design and they used this information to automatically create a complete access control infrastructure.

In [5], the authors adapted use cases to propose an abuse case model which captured and analyzed security requirements. This model identified the specifications of every interaction between the system and one or a set of actors as this interaction can negatively affect the system. The misuse case concept describes functions which the system should not allow, as defined in [21] and [22]. Furthermore, the miss-actor concept is defined as someone who accidentally or intentionally starts the misuse case. In this approach, security is considered by analyzing a security-related misuse case.

In [23], the obstacle concept was used in the KAOS framework to capture undesirable system properties, and to identify and relate security requirements to other system requirements. There are two sets of techniques based on the temporal logic formalization utilizing because of obstacle goals satisfaction and requirements.

TABLE II
RELATED WORK ON EXISTING SECURITY GOALS

Reference	Year	Security Goal					
		Integrity	Confidentiality	Availability	Reliability	Privacy	Access Control
[5]	1999						
[11]	2001		√	√			
[12]	2002	√	√			√	
[9]	2002	√	√	√			
[13]	2002						√
[14]	2003	√	√				
[7]	2007	√	√	√			
[15]	2007	√				√	√
[16]	2008			√			√
[17]	2008						√
[18]	2008			√			√
[19]	2009	√	√	√			
[10]	2011		√	√	√		
[20]	2011	√				√	√

All these previously mentioned approaches provide the first step in integrating security in the software engineering and they are useful in modelling security requirements. However, these approaches have several drawbacks since they only provide guidance as to how security can be handled during certain stages of the software development process. For example, the approach in [11] is applicable throughout the design stage while the approach in [5] is used throughout early

requirements analysis. We will propose a security approach covering all software development processes which can help to limit the number of conflicts by defining them at an early stage in system development and taking steps to overcome them. Table 1 summarizes the literature on existing software development process stages.

Some of the previously mentioned approaches only deal with specific security requirements, goals and constraints. For example, UMLsec proposed in [11] focuses on access control security requirements and integrates this into the model driven software development process. However, we will propose a security approach which considers all security requirements, such as access control and encryption, security goals, such as integrity and secrecy, and security constraints, such as authorized and unauthorized access. Table 2 summarizes the literature on existing security goals.

III. PROPOSED FRAMEWORK

Business Process Modelling (BPM) is a well accepted method within the business organization sector for structuring business processes. It provides support to the organization's processes using different methods, techniques and software tools to control and analyze organizational processes and activities, which includes people, organizations, applications, documents and other related information. A successful BPM method contains three important components: model, strategy, and operations. A business model includes knowledge of the creation of the organization, delivers values, and how to capture the business goals and objectives. Strategies carry rules and guidelines that fulfill all model-related elements. Operations in the business are the combination of several elements, such as people, processes and technology, whereas a different group of people worked together to complete organizational required goals with the help of information system services.

Many IS security problems can occur when an organization's assets need to be protected from threats and attacks. However, it is a complex task to protect these assets since the business environment changes rapidly. Business organizations comprise complex business structures that are evaluated and updated within the customer structures and demands which consist of processes, models, strategies and set of activities worked together to achieve the business goals. For better alignment between IS and business, IS security problems have to be addressed by managing security in the form of defining, analyzing, modelling and mapping the IS attacks and identifying suitable security requirements in order to respond to these attacks in four different IS development stages: the early requirements stage, late requirements stage, architecture design stage and detail design stage.

This paper aims to present a requirement engineering-based approach for business and IS analysts to better understand security problems and define their associated security goals and to detect security requirements and constraints from the goals. We have divided our proposed framework into three parts: modelling the business environment, modelling the information technology system and modelling the information system security, as shown in figure 1. Part 1 is divided into two levels: the business decision level and the business process modelling level where each level is made up of four business components. The business decision level consists of business goals, business rules, rules measurement and business rules analysis. The business process modelling level consists of the role model, the process events, the decision model and process monitoring. Part 2 consists of the system behavior, the business process, system behavior analysis, and the use case.

Part 1 and 2 describe the specifications of the business organization environment and IT environment respectively, in relation to infrastructure and assets, based on the already accepted business process modelling methodology known as business process modelling towards the derivation of information technology goals, as proposed in [24]. Business assets are anything that the business organization owns and has an economic value to the business organization. For example, the business assets in our case study are the mobile phone order management process in a telecommunication company, the personal information of the company's consumers and staff and the company's data and knowledge management. IS assets are anything that is part of the IT department which provides support to the business assets. For example, the IS assets in our case study are the hardware, software, people and the network etc. Protection of these assets is essential for the continued existence of the business organization.

Part 3 describes how to define, model and analyze the attacks on IS and the business organization, as security is the major element in IS in this proposed approach. It identifies the qualities expected from IS, such as reliability, safety, usability etc. Part 3 is divided into four different IS development stages: early requirements stage, late requirements stage, architecture design stage and detail design stage, as shown in figure 2.

The early requirements stage focuses on understanding the problems by studying the setting of the existing organizations. In this stage, the business environment and assets are identified and the IS security goals and constraints are derived. Therefore, the organization model is the output of this stage. The late requirements stage focuses on modelling the "to-be" security model by adding and analyzing security requirements and constraints. The architectural design stage focuses on defining the system's global architecture, such as the mobile agents, clients and servers in the subsystems that connect to each other throughout data and control flows. The existing actors are divided into sub-actors and the security goals are delegated as the second level in this stage. The detail design stage focuses on defining the architecture elements that have been defined in the previous stages in more detail in inputs, outputs, controls and security aspects by using the UML sequence diagram for the agent interaction diagram [25].

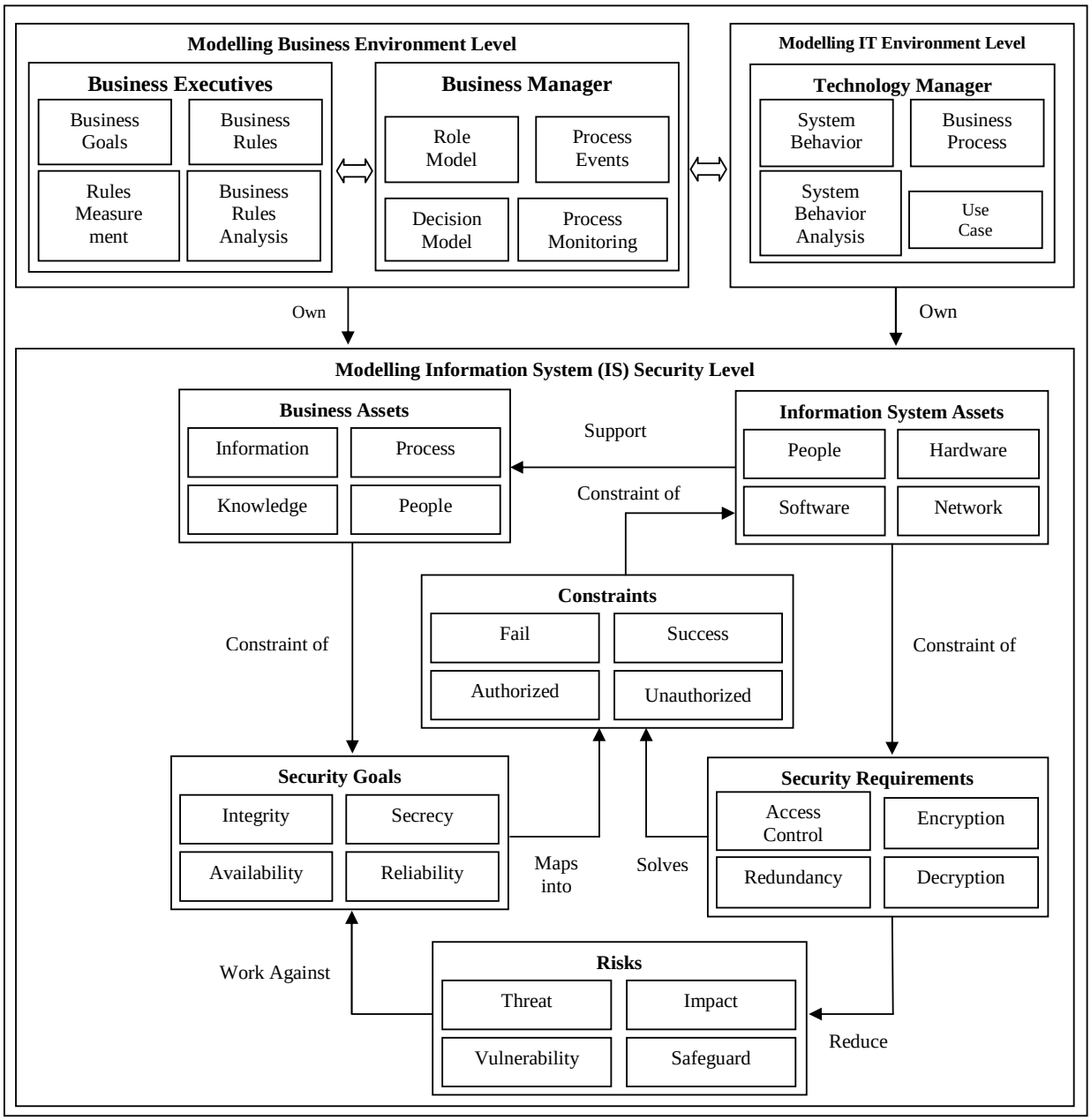

Fig. 1 Proposed Framework Approach

A. Modelling Business Environment

The modelling business environment contains two parts: the business decision and the business process modelling.

1. Modelling Business Decision

Modelling business decisions consist of the business goals, the business rules, the rules measurement and the business rules analysis. Business goals are used to represent why business processes exist and how to fulfill the organization's mission statement. Business rules refer to the statement that how to control the overall business behavior. It defines the operations, business constraints and definitions that apply to an organization. The business rules could be applied to people, business processes, behavior and the information system in the organization and are put in place in order to assist organizations achieve their goals and objectives [11]. The measurement of business rules depicts the detailed analysis of business rules. Business rule analysis is a procedure to define rules and refine their meaning.

2. Business Process Modelling

Business process modelling consists of the role model, the process events, the decision model and the process monitoring. The business role model is used to capture the business organizational value. Events in the process are things in the business that affect the sequence of the process, including activities. The decision model is a unique logical representation for business logic showing how and where it is executed. Business logic, which is the logic proposed by the business rules, represents how the business intends to make significant decisions. The decision model is used to perceive, manage and organize the business rules and logic. Business process monitoring is a method used to identify how business people can provide real-time information on the significant indicators of the business performance in order to improve the speed and effectiveness of business operations. In the process monitoring, each individual activity is tracked and thus information on the state of the process can easily be seen and statistics on the performance of the process can be presented. In this proposed paper, we model business decisions and business processes using well accepted modelling techniques, namely *i** and the UML goal tree.

B. Modelling IT Environment

The term "IT modelling environment" became popular in the mid 1990s and refers to a set of shared IT resources that work together to achieve common goals. The IT environment normally comprises two major parts: "technical" and "human", where technical includes software, hardware, network, telecommunication, etc, and human refers to the technical skills (persons) and knowledge that is required to maintain the IT resources. In the context of organizations, business processes are increasingly becoming more and more complex every day and their goals and objectives are changing rapidly.In this situation, the IT environment needs to be flexible so that rapid changes in business goals and objectives can be managed. In this paper, we propose to model the IT environment in relation to four different components: system behavior, the business process, system behavior analysis and use case.

System behavior refers to how the system should behave when the customer places a query. The business process is a set of internal organizational procedures or activities that work together to achieve an organization's goals and objectives to meet the consumers' expectations. It is the key element of the business where other business components, such as goals, strategies, policies etc are based. System behavior analysis is used to identify errors in the system's behavior; for example are all the system's functions working well or not? Use Case Analysis is a technique used to identify the high level requirements of a system. We begin by identifying the actors involved in using the system. We then identify all the functions each actor will be performing with the system. Each function an actor is intended to carry out with the system is a use case.

Two important elements are necessary for a complete use case diagram: actor and use case, where an actor is a person, system or other external entity that interacts with the system in question and a use case is a description of a system's intended behavior, given an external request by an actor. A use case identifies the type of interaction with a system and the actor involved. Use cases are a fundamental feature of the UML notation for describing system models.

C. Modelling Information System Security

Part 3 describes how to define, model and analyze the attacks on IS and the business organization, as security is the major element in IS in this proposed approach. It identifies the qualities expected from IS, such as reliability, safety, usability etc. Part 3 is divided into four different IS development stages: early requirements stage, late requirements stage, architecture design stage and detail design stage.

The early requirements stage focuses on understanding the problems by studying the setting of existing organizations. There are two main levels in this stage. In the first level, the business environments and assets are identified while the IS security goals and constraints are derived in the second level. In other words, level 1 is where the business processes can be modelled by using the *i** language and thus the security requirements can be linked within it whereas level 2 defines the information system security goals and how to link them within the business processes. Therefore, the organization model is the output of this stage.

The functional, non-functional and security requirements of the system "to-be" are described in the late requirements stage. The "to-be" system introduces one or a set of actors that have a set of dependencies with other organizational actors identified in the early requirements stage.

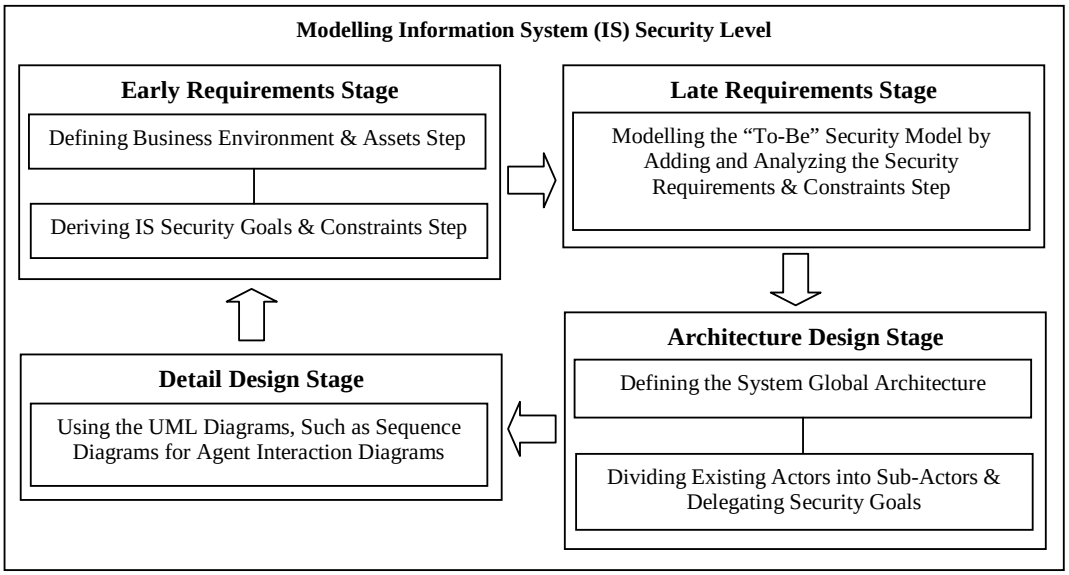

Fig. 2 Modelling Information System (IS) Security Level

Thus, the late requirements stage focuses on modelling the "to-be" security model by adding and analyzing the security requirements and constraints.There are two main steps in the architectural design stage. In the first level, the system's global architecture, such as the mobile agent and the client/server, is defined in subsystems which interconnect to each other throughout the data and control flows. Thus, the Architectural Style Selection Diagram (ASSD) proposed in [18] is used to model these architecture styles and system security requirements and goals. In the second level, the existing actors are divided into sub-actors and the security goals are delegated.The detail design stage focuses on defining the architecture elements that have been defined in the previous stages in more detail in relation to inputs, outputs, controls and security. In other words, the system developers identify the actors' interactions in detail throughout the detail design stage, taking the security-related aspects derived from previous stages into account. In this stage, the UML sequence diagram is used to model the agent interaction between the system actors [20] [21].

IV. CONCLUSION AND IMPLICATIONS

Security can play a crucial role in business processes and e-commerce. However, the literature shows that it is quite challenging to add security into business processes for several reasons. Firstly, the integration of security into a developed business process is not very well understood. Secondly, security properties are complicated and error-prone when integrated by hand. Furthermore, the lack of experience of IS developers can lead to security leaks. Therefore, IS developers need to have concrete guidelines and appropriate tools to develop secure applications.

Security must be considered throughout the entire business development process and requirements specifications should be identified. In this paper, we present an integrated security and IS engineering approach throughout all the software development process stages by using the *i** language. We have divided our proposed framework into three separate parts: modelling the business environment, modelling the information technology system and modelling the information system security.

Modelling IS security consists of four major stages: (1) early requirements stage; (2) late requirements stage; (3) architectural design stage; and (4) details design stage. In the early requirements stage, the business environment and assets are identified and the IS security goals and constraints are derived, whereas in the late requirements stage, the "to-be" security model is modelled by adding and analyzing the security requirements and constraints. Furthermore, in the architectural design stage, the existing actors are divided into sub-actors and the security goals are delegated while in the detail design stage, the architecture elements are defined in more detail by using the UML sequence diagram for the agent interaction diagram.

Two major implications can be derived from the study for information system developers and business organizations. First, for developers, the study shows how system security goals can be derived from the business environment and defined during the whole system development process which leads them to better improve their system. Second, for the business organization, it can increase the customer confidante and trust which can lead to increase the companies' profit. However, the paper has one limitation; we have not validated our proposed framework within any existing business process as a case study.

REFERENCES

[1] Chung, L. and B.A. Nixon, Dealing with non-functional requirements: three experimental studies of a process-oriented approach, in Proceedings of the 17th international conference on Software engineering. 1995, ACM: Seattle, Washington, United States. p. 25-37.
[2] Haley, C.B., et al., A framework for security requirements engineering, in Proceedings of the 2006 international workshop on Software engineering for secure systems. 2006, ACM: Shanghai, China. p. 35-42.
[3] Yu, E. and L. Cysneiros. Designing for privacy and other competing requirements. in 2nd Symposium on Requirements Engineering for Information Security (SREIS' 02). 2002. Raleigh, North Carolina.
[4] Backes, M., B. Pfitzmann, and M. Waidner, Security in business process engineering. Business Process Management, Springer Berlin / Heidelberg, 2003: p. 1019-1019.
[5] McDermott, J. and C. Fox. Using abuse case models for security requirements analysis. in Computer Security Applications Conference, 1999. (ACSAC '99) Proceedings. 15th Annual. 1999.
[6] Anderson, R.J., Security Engineering: A guide to building dependable distributed systems. 2008.
[7] Mayer, N., E. Dubois, and A. Rifaut, Requirements Engineering for Improving Business/IT Alignment in Security Risk Management Methods Enterprise Interoperability II, R.J. Gonçalves, et al., Editors. 2007, Springer London. p. 15-26.
[8] Mouratidis, H. and J. Jurjens, From goal-driven security requirements engineering to secure design. International Journal of Intelligent Systems, 2010. 25(8): p. 813-840.
[9] Rohrig, S. and S.S. Ag, Using process models to analyze health care security requirements, in International Conference Advances in Infrastructure for e-Business, e-Education, e-Science, and e-Medicine on the Internet. 2002: Italy.
[10] Ullah, A. and R. Lai, Managing Security Requirements: Towards Better Alignment Between Information Systems And Business, in 15th Pacific Asia Conference on Information System (15th PACIS) 2011: Queensland University of Technology (QUT) in Brisbane, Australia.
[11] Jürjens, J., Towards Development of Secure Systems Using UMLsec Fundamental Approaches to Software Engineering, H. Hussmann, Editor. 2001, Springer Berlin / Heidelberg. p. 187-200.
[12] Liu, L., E. Yu, and J. Mylopoulos. Security and privacy requirements analysis within a social setting. in Proceedings on 11th IEEE International Requirements Engineering Conference, . 2003.
[13] Lodderstedt, T., D. Basin, and J. Doser, SecureUML: A UML-Based Modeling Language for Model-Driven Security, in the Proceedings of the 5th International Conference on the Unified Modeling Language, J.-M. Jézéquel, H. Hussmann, and S. Cook, Editors. 2002, Springer Berlin / Heidelberg. p. 426-441.
[14] Mana, A., et al. A business process-driven approach to security engineering. in Proceedings on 14th International Workshop on Database and Expert Systems Applications, . 2003.
[15] Rodríguez, A., E. Fernández-Medina, and M. Piattini, A bpmn extension for the modeling of security requirements in business processes. IEICE transactions on information and systems, 2007. 90(4): p. 745-752.
[16] Goluch, G., et al. Integration of an Ontological Information Security Concept in Risk-Aware Business Process Management. in Proceedings of the 41st Annual Hawaii International Conference on System Sciences, 2008.
[17] Mayer, N., et al. Towards a measurement framework for security risk management. 2008.
[18] Matulevicius, R., N. Mayer, and P. Heymans. Alignment of Misuse Cases with Security Risk Management. in Third International Conference on Availability, Reliability and Security (ARES 08) 2008.
[19] Wolter, C., et al., Model-driven business process security requirement specification. Journal of Systems Architecture, 2009. 55(4): p. 211-223.
[20] Rodríguez, A., et al., Secure business process model specification through a UML 2.0 activity diagram profile. Decision Support Systems, 2011. 51(3): p. 446-465.
[21] Sindre, G. and A.L. Opdahl. Eliciting security requirements by misuse cases. in Proceedings of 37th International Conference on Technology of Object-Oriented Languages and Systems, TOOLS-Pacific 2000.
[22] Sindre, G. and A.L. Opdahl, Eliciting security requirements with misuse cases. Requirements Engineering, 2005. 10(1): p. 34-44.
[23] Dardenne, A., S. Fickas, and A.v. Lamsweerde, Goal-directed concept acquisition in requirements elicitation, in Proceedings of the 6th international workshop on Software specification and design. 1991, IEEE Computer Society Press: Como, Italy. p. 14-21.
[24] Alotaibi, Y. and F. Liu, Business Process Modelling Towards Derivation of Information Technology Goals, in Proceedings of the 45st Annual Hawaii International Conference on System Sciences. 2012: Maui, Hawaii, US.
[25] Object, M.G., OMG Unified Modeling Language (OMG UML), Superstructure, V2. 1.2. November 2007.