2012 International Conference on Information and Computer Applications (ICICA 2012)
IPCSIT vol. 24 (2012) © (2012) IACSIT Press, Singapore

A Novel Framework to Model a Secure Information System (IS)

Youseef Alotaibi and Fei Liu [+]

[1] Department of Computer Science and Computer Engineering, La Trobe University, Bundoora, VIC, 3086, Australia,

Abstract. The existing information system (IS) developments methods are not met the requirements to resolve the security related Information System (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.

Keywords: Information System; Software Development Process; Requirement Engineering; Security Goals

1. Introduction

Information system (IS) has been used almost in all aspect of human society, such as military, health science, telecommunication companies, e-commerce etc. Since using the IS has been arise, the concept of security to secure these systems requires to be arise. Because many systems may contain a private data to be available only to authorized people, the security concepts have to be added into the IS. For example, the mobile phone order management process in a telecommunication company contains the customers' personal information and their credit card information and thus this system must to be secured to save the customers' privacy.

The security is considered as a non-functional requirement by the software engineering [4]. Although, the non-functional requirement introduces the quality features, it represents the constraints, such as authorized and unauthorized accesses where the systems must be operated [7][20]. Therefore, the security requirements must be defined after identifying the system. However, there are several challenges to have a better support for the security engineering. Firstly, the security requirements are commonly complicated to be analyzed and modelled. There is one main problem in analyzing the non-functional requirements which is the requirement of separate the functional and non-functional requirements while 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 correspondence between them cannot be seen easily. Secondly, the IS developers may have lack knowledge to develop and model a secure system [3][12].

The security has to be considered through all business development process and identified with the requirements specification. If the security only considers in the certain stages of the development process, the security requirements will conflict within the system functional requirements. Therefore, the security requires to be taken into account within the functional requirement during the system development stages in

[+] Corresponding author.
E-mail address: yaalotaibi@students. , f.liu@]latrobe.edu.au

order to limit the conflict cases and that can be done by defining them in the early stages of the system development and trying to overcome them. However, when the security only adds in the late stages of the system developments, the chance of having more conflicts could be increased and it may require a lot of money to overcome them.

Literature shows that there are many commercial methods, such as ITBPM, OCTAVE, CRAMM, EBIOS, MEHARI, etc available to IT security officers in the organizations to be used to perform the risk analysis of the security problems and define the security solutions [2][11][13]. However, these existing methods of the IS developments are not met the requirements to resolve the security related IS problems and they fail to provide a successful integration security during all development process stages.

Thus, we propose an integrated security and IS engineering approach in the all development process stages by using i^* language. There are four stages of the software developments to have a secure IS in our proposed framework approach: (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 2 describes the related work of modeling secure IS; section 3 presents our proposed framework approach; the conclusion and future research directions are presented in section 4.

2. Related Work

Literature shows that there are only a few approaches considered the security requirements as a primary part of all software development processes. For example, in [4], the authors applied the process oriented approach to represent the security requirement as harmonious goals and used them throughout the software system development. This non-functional requirements proposed framework is represented and used the security requirements as the classes of the non-functional requirements and it permits the system developers to consider the design decisions which are related into the represented non-functional requirements.

In [16], 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 constructs security objectives, such as actors, (3) examining whether these specifications are consistent or not, and (4) creating the list of the essential security measures for every business process component.

In [11] and [18], the authors proposed the requirements engineering approach to model and map the IS security goals at the early stage of the software development process in the context of the alignment between the business and IS. These approaches contain five major steps: (1) identifying organization 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.

In [8], the extension of the Unified Modelling Language (UML) which calls UMLsec was proposed to contain the model of the security features, such as access control and confidentiality. There are four different UML diagrams used in [8]: (1) class diagrams to guarantee that exchanging of data obeys the security levels, (2) state chart diagrams to avoid the indirect information flow from the high to low values with the object, (3) interaction diagrams to guarantee the accuracy of the important security interactions between the objects and (4) deployment diagrams to guarantee that the physical layer can meet the security requirement on communication. Moreover, in [10] the UML was extended to model security and the authors presented the security modelling language called the SecureUML. The authors described how the UML could be used to identify the access control related information in the whole application design and used this information to create a complete access control infrastructures automatically.

In [12], the authors adapted the use cases to propose an abuse case model which used to capture and analyze the security requirements. This model identified as the specification of complete interaction type between the system and one or set of actors and this interaction can negatively affect the system. The misuse case concept which describes the non allowed function by the system defined in [17]. Furthermore, the mis-actor concept defined as someone who accidentally or intentionally starts the misuse case. In this approach, the security is considered by analyzing the security related misuse case.

In [5], the obstacle concept was used in the KAOS framework to capture undesired system properties, identify and relate the security requirements into other system requirements. There are two set of techniques which bases on the temporal logic formalization utilized because of obstacle goals satisfaction and requirements.

Tab.1 Related Work of Existing Software Development Process Stages.

Reference	Year	Software Development Process Stages			
		Early Requirement	Late Requirement	Architecture Design	Detail Design
[12]	1999	√			
[8]	2001			√	
[9]	2002	√		√	
[16]	2002	√			
[10]	2002			√	
[11]	2007	√			
[6]	2008			√	
[19]	2009	√		√	
[18]	2011	√			
[15]	2011			√	√

All of pervious mentioned approaches above provide the first step to integrate the security concept within the software engineering and they are useful in modelling security requirements. However, these approaches has some drawbacks since they only have a guide about how can the security handled during the certain stage of software development process. For example, the approach in [8] is applicable throughout the design stage while the approach in [12] is used throughout the early requirements analysis. Hence, we will propose a security approach covering all software development process which can help limiting the conflict cases by defining them at the early stage in the system development and trying to overcome them. Table 1 summarizes the literature of existing software development process stages.

3. Proposed FrameWork

There are many IS security problems happened when the origination assets require to be protected from the threats and attacks. However, it is a complex task to protect organization assets since the business environment has been changed rapidly. The business organizations contain complex business structures that are evaluated and updated within the customer structures and demands which consist of processes, models, strategies and set of activities which work together to achieve the business goals. To better alignment between IS and business, the IS security problems have to be addressed by managing the security in the form of defining, analyzing, modelling and mapping the IS attacks and identifying the suitable security requirements in order to respond to these attacks in four different IS development stages: early requirements stage, late requirements stage, architecture design stage and detail design stage.

This paper aims to present a requirement engineering-based approach for the business and IS analysts to better understand the security problems and define their associated security goals and detecting the security requirements and constraints from the goals. We have categorized our proposed framework into three separate parts: modelling business environment part, modelling information technology system part and modelling information system security part as shown in figure 1. Part 1 divides 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 the business goals, the business rules, the rules measurement and the 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 behaviour, the

business process, the system behaviour analysis, and the use case. Part 1 and 2 are not in the scope of this paper and for more details please refer to [1].

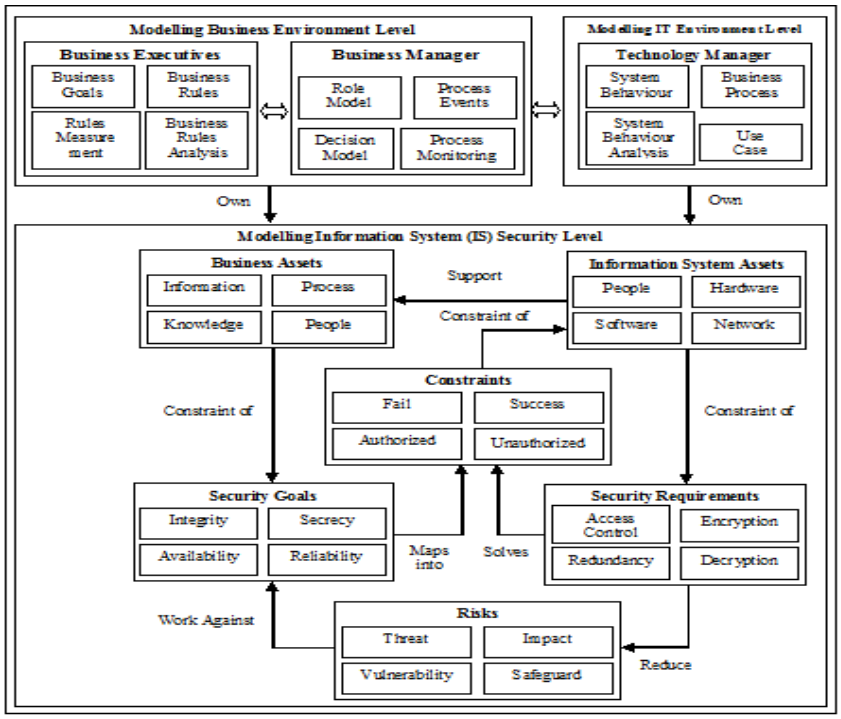

Fig.1 Proposed Framework Approach

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

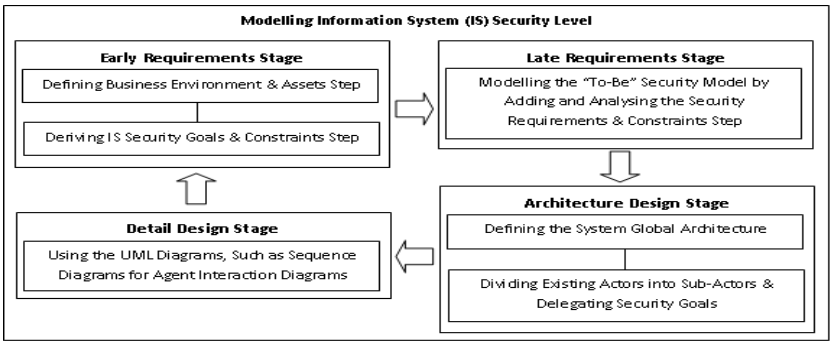

Fig.2 Modelling Information System (IS) Security Level.

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

The early requirements stage focuses on understanding the problems by studying the setting of existing organizations. In this stage, the business environments and assets are identified and the IS security goals and constraints are derived. Therefore, the organization model is the output of this stage. However, the late requirements stage focuses on modelling the "to-be" security model by adding and analyzing the security requirement and constraints. Furthermore, the architectural design stage focuses on defining the system global architecture, such as mobile agent and client and server in subsystems that interconnect to each other throughout the data and control flows. Next, 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 has been defined in the previous stages in more details in inputs, outputs, controls and security aspects by using the UML sequence diagram for the agent interaction diagram [14].

4. Conclusion & Implications

The security has to be considered through all business development process and identified with the requirements specification. Thus, in this paper, we presents an integrated security and IS engineering approach in whole software development process stages by using i^* language. Our proposed framework is categorized into three separate parts: modelling business environment part, modelling information technology system part and modelling information system security part where modelling IS security part contains four major stages: (1) early requirements stage, (2) late requirements stage, (3) architectural design stage and (4) details design stage. 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 validate our proposed framework within any existing business process as a case study.

5. References

[1] 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.

[2] Anderson, R.J., Security Engineering: A guide to building dependable distributed systems. 2008.

[3] Backes, M., B. Pfitzmann, and M. Waidner, Security in business process engineering. Business Process Management, Springer Berlin / Heidelberg, 2003: p. 1019-1019.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] Jürjens, J., Towards Development of Secure Systems Using UMLsec Fundamental Approaches to Software Engineering, H. Hussmann, Editor. 2001, Springer Berlin / Heidelberg. p. 187-200.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] Object, M.G., OMG Unified Modeling Language (OMG UML), Superstructure, V2. 1.2. November 2007.

[15] 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.

[16] 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.

[17] Sindre, G. and A.L. Opdahl, Eliciting security requirements with misuse cases. Requirements Engineering, 2005. 10(1): p. 34-44.

[18] 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.

[19] Wolter, C., et al., Model-driven business process security requirement specification. Journal of Systems Architecture, 2009. 55(4): p. 211-223.

[20] 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.