Security Requirement Engineering Issues in Risk Management

Dhirendra Pandey
Department of IT
BBA University, Lucknow

Ugrasen Suman
School for CSIT
DAVV, Indore

A. K. Ramani
School for CSIT
DAVV, Indore

ABSTRACT

Security refers the protection of software products from unauthorised access, alteration and destruction. Therefore, security requirement is a presently a major concern of software system and it is generally recommended to take care of security prior to software development process. Risk management is one of the most important aspects of security requirement engineering domain, which allows comparing security needs and costs of security measures. In this paper, we have discussed the incorporation of security issues in requirement engineering process. We have also proposed a method to match requirement engineering approaches with risk assessments approaches. The aim of this paper is to provide some models and methods to identify and include security in the early stage of software development process.

Keyword

Information System, Requirement Engineering, Security Requirements.

1. INTRODUCTION

Designing a secure software system is challenging issue for the software designers. Malicious users always try to break the systems and in response, software vendors started providing security as a necessary feature for their products and network systems [14]. As a result of years of research, many powerful techniques have been developed to solve a wide array of security problems [7]. When choosing appropriate security measures, the security system designer must consider the design of the entire system, and not incorporate security technologies at random. Designing system security is best practice, which is performing by systematic engineering approach. Systems security engineering is concerned with identifying security risks, requirements and recovery strategies [1]. In the security requirement engineering domain, risk management is one of the most efficient tools, because it permits to compare security needs and costs of security measures [14].

The Requirement engineering (RE) community has started to be aware of the problem of security and a lots of security RE approach have been developed [9]. For documenting intermediate results and for presenting the overall conclusions, we use special CORAS diagrams, which are inspired by UML. CORAS is a method for conducting security risk analysis. CORAS UML profiles are also considering security risk aspects [4]. CORAS provides a customised language for threat and risk modelling, and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis. In this respect, CORAS is model-based method. The Unified Modelling Language (UML) is typically used to model the target of the analysis. Some another security requirement engineering approach is also useful in managing risk at the early stages of software development such as problem frames decomposition and abuse frames proposal [5]. Frame decomposition and abuse frame is an approach to analyze security problems in order to determine security threats and vulnerabilities. The main objective of problem frames is to capture and bound the base system that is to be protected.

The i* framework was developed for the modelling and risk analysis of organizational environments [6]. A number of security applications framework were studied and an extension for handling risk issues was developed [7, 8]. Some researchers performed their research work in the context of risk management and particularly risk analysis, such as threat analysis, vulnerability and impact on each component of the system [2, 3]. We can cite some methods based on risk analysis such as OCTAVE [11]. It is a standard approach for a risk-driven and practice-based information security evaluation. MEHARI is another risk analysis and risk management method [12]. Some other citation is also included in this paper such as EBIOS, it allows to evaluate and act on risks relative to information systems security, and proposes a security policy adapted to the needs of an organization. [13].

The Knowledge Acquisition in automated specification approach (KAOS) was developed for security goal analysis technique to manage critical system engineering (e.g. safety for critical systems), which is adapted for securing critical business assets [9]. Another goal-oriented modelling framework is Non-Functional Requirements (NFR) framework, that handling security as a class of non-functional requirements [10]. The organisation increases their importance in the business domain. The Information system development is one of the important business activities which need more and more security requirement, due to the number of attacks. Today, security is no more a desirable quality of IT systems, but a required compliance to international regulations. A number of technical answers are available in response to IT security issues [9]. Each of these technical answers has its own level of protection and also, its own cost. Therefore, one of the challenges is to determine the most suitable compromise between the level of security achieved and its associated cost to obtain the best ROI (Return on Investment). It should be based on the correct evaluation of the IT risk, which is usually defined by a threat and vulnerability analysis, and its impact on the business assets of the organization. Therefore, it is necessary to adapt the security measures, depending on the risk and its associated components. The analysis of risks in terms of the links existing between the business assets of an organization and the technical aspects associated with its IS, seems to be best suited for the application of a security requirements engineering approach.

Security requirement is one of the most important requirements that must be used to develop secure software products. The remainder of this paper is organised as follows. We will discuss our proposed framework and problem statement related to risk management in Section 2. We then illustrate proposed framework using a case study in Section 3. Finally, we conclude with summary in Section 4.

2. RISK MANAGEMENT FRAMEWORK

Security requirement engineering is essential needs in business organisations for developing quality software products. One of the main key to a good alignment between business domain and security of IT structures is to keep the focus on the assets of the business. Assets are anything that has economic value for the organisation and that are central in the realization of business objectives. Security requirement engineering is a striking issue in software development. It can identify the threats or risks before developing software products. Security issue is also play an important role in requirement engineering. Requirements can be collected from many sources and there is possibility to get some anti-requirements. The anti-requirements are the requirement that come from malicious user. The security requirement engineering can help the software developers to handle anti-requirements. To manage anti-requirements, firstly, we identify the expected anti-requirements and then avoid the anti-requirements and try to collect only good requirements.

One view of our proposed security engineering process is shown in Figure 1. Threat modelling involves understanding the complexity of the system and identifying all possible threats to the system, regardless of whether or not they can be exploited. During the formation of security requirements, these threats are analyzed based on their criticality and likelihood, and a decision is made whether to mitigate the threat or accept the risk associated with it. System designer always attempts to find good security mechanism, and after obtaining it they must implement them into the general software engineering cycle of development, such as design, implementation, testing, and maintenance. Each stage of security engineering gives feedback to the preceding stage and through that stage to all earlier stages. Feedback allows designers to catch mistakes made in the early stages without letting their effects cascade. Threat modelling and security requirements provide the foundations upon which the rest of the security system is built. Identifying threats helps to develop realistic and meaningful security requirements. This is particularly important, for if the security requirements are faulty, the definition of security for that system will be also faulty, and thus the system cannot be secure. The proper identification of threats and appropriate selection of countermeasures reduces the ability of attackers to misuse the system.

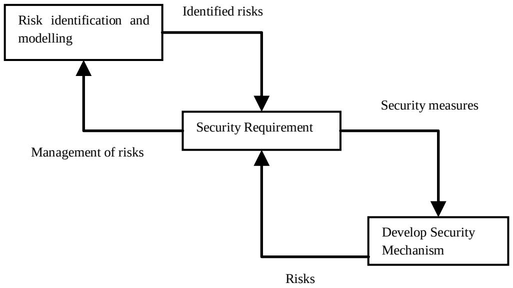

Fig 1: Security Requirement Engineering

The integration of security within software development especially during requirement engineering is considered as another research challenge. One reason for these challenges, beside technical issues, is dependence of security on organizational policy [14]. The security requirements engineering has given significant attention in recent years but it is lacking the context for operation. In Figure 2, we have also proposed a model based on the security requirement engineering framework that provide crucial link between business assets and IT assets where the risk at the core in this model. This framework melds the security requirement engineering and risk management framework. In this figure, we present different kinds of business assets in the financial domain. Also, figure 2 shows the links between risk components and assets. Vulnerability is a characteristic of the IT system and threat targets the IS, but the impact is reflected on the business of the organization.

For example, in any business organisation, account management is a core activity of that organisation. Knowledge and Information assets include customers' name, address and phone number. These assets are called IT business assets which can be hacked or stolen. People encoding data are also considered as IT assets, because they are part of the IS environment and essential in a good account management. IT assets are therefore the IS components needed to be secured, in order to ensure the achievement of the business objectives. Security designer always take care in the security measures/ mechanism assortment. Designing system security can be provided by utilizing a systematic engineering approach. Security requirements are necessary throughout the software development life cycle; for that, developers follows the general lists of security features such as password protection, firewalls, virus detection tools, etc. These are, in fact, not security requirements at all but rather implementation mechanisms that are intended to satisfy unstated requirements such as authenticated access. Security requirements are constraints on functional requirements that are derived from security goals [14].

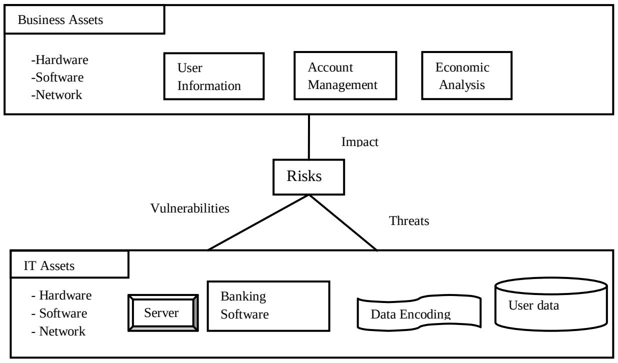

Fig. 2: Risk management framework

Assets need to be secured, as they are exposed to risks. Note that, our work only focuses on software development risks which can affect the IS development. Other risks like financial risks (investment) or organisational ones (hiring of a CEO) are out of the scope. Risk is most often defined by three components that are threat, vulnerability and impact on business organisation. We can say, risk is characterized by the opportunity of exploiting one or multiple vulnerabilities, from one or many entities, by a threatening element using a method of attack, or by causing a negative impact on business assets.

3. RISK MANAGEMENT USING SECURITY REQUIREMENT ENGINEERING

Risk management ensure the successful completion of software development. A lot of work has already been done in the risk management domain, particularly with industrial methods and norms [12]. But there is a mismatch between security methods and software system development. The proposed framework is able to handle security in the first steps of IS design and during the RE steps. Risk management methods are considered as semiformal and are often a good process for a risk assessment. But the product from these methods is informal, most often in natural language, thus creating a gap in automation, evolution, monitoring or traceability of risk management. Particularly, the aim of the research is to provide the solution of aforesaid problem and to mitigate the security requirement with the risk management.

3.1 Melding the Security Requirement Engineering with Risk Management

Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events. We have proposed a framework that associates the business assets with security engineering, which is shown in Figure 3. In this figure, we have melded the two important aspects of software engineering, which is security engineering and risk management. Security engineering generates security requirements and tools that can mitigate the risks. Basically, we have proposed two important organisational models in our framework such as business model and structural model. Business model incorporates company assets such as customer information, user account management, etc and the structural model integrates the IT assets like hardware, software, server, etc. Risk is potential problem that can come from the business process and can threaten or damage the IT assets of organisational structural model. Security engineering system plays an important role to mitigate risk by providing some security measures during the structural modelling. For example, physical security, identification of users, access control and by using encryption. This helps system engineer to built secure and good quality organisational software products.

RE is an important domain for linking business assets, driven by business goals, with the security engineering domain. On the other hand, the architectural engineering is the domain linked with IT assets, which are included in the IS architecture with security engineering. The objective of security engineering is to mitigate risks by providing security requirements. The tools used for reasoning about requirements and architectural engineering are respectively architectural and business modelling. Models provide the basis for formalisation, documentation and evolution. Our approach mainly focuses on RE domain i.e. making the link between business assets overseen by business goals and security engineering used for mitigating risks. RE approach considering security will be presented in the next section, most of them improved by modelling

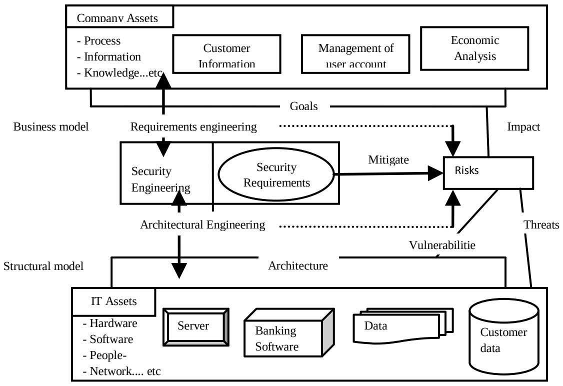

Fig. 3. Security requirements engineering with risk management

3.2 Case study

Identifying threats assists to develop realistic and meaningful security requirements. In this paper, we use the case study of health insurance information system. The aim of this case study is to design of a new Information System for health insurance. The information system should be able to store and manage requests for reimbursement. In this paper, we have considered only security aspects of the database. The database is the most sensitive IS component. It contains patient personal information (e.g. phone number and email address) in addition to the patients' healthcare treatment information. For this, the IS should protect the privacy of patients and their associated healthcare records. The confidentiality of data should be guaranteed. Moreover, the database will be available for allowing the access of patient healthcare information in case of urgent need. There is a general agreement amongst scientists and practitioners to recognize the importance of IT alignment with business. Therefore, our proposed method relies on the integration of requirements, security and architectural engineering activities. Moreover, risks are at the core of the alignment between business and IT systems. One difficulty to overcome is the rapid changes of business requirements, even during the IS development.

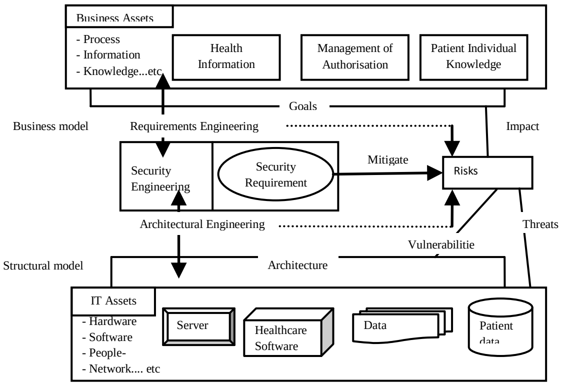

Fig.4. Security requirement engineering for healthcare system

However, keeping the focus on business assets, which seem more stable, is an opportunity for IT system development, in order to be better aligned with business. Assets are anything that has economic value to the organization and that is central in the realization of its business objectives. Securing them is essential. Figure 4 shows different kinds of business assets. In our case study, information business assets are patient personal information, a process business asset is a healthcare authorization management, and knowledge business assets are the healthcare domain knowledge.

4. CONCLUSION

In this research, we have focused on risk management and avoidance of anti-requirements. Risk management and security requirement engineering is a crucial activity in the development of secure systems. It is also recognized as a crucial activity by the RE community and new methodologies are proposed for handling security aspects. In this paper, we propose a framework that incorporate security requirement and risk management technique. Our proposal improves the iterative security engineering activity at the earliest stages of development. Also, we have concentrated on the integration of risk management in software development.

5. REFERENCES

[1] Kotonya G. and Sommerville I.: Requirements Engineering: Processes and Techniques. John Wiley & Sons, 1998.

[2] Alexander I.: Misuse Cases Help to Elicit Non- Functional Requirements, Position paper for Policy Workshop 1999, Bristol, U.K., and November 1999.

[3] McDermott J. Fox C.: Using Abuse Case Models for Security Requirements Analysis, 15th Annual Computer Security Applications Conference, Phoenix, Arizona, December 1999.

[4] Fredriksen R., Kristiansen M., Gran B., Stolen A. K., Opperud T. A. and Dimitrakos T.:The CORAS framework for a model-based risk management process, Proceedings of the 21st International Conference on Computer Safety, Reliability and Security (Safecomp 2002), LNCS 2434, pp. 94-105, Springer, 2002.

[5] Lin L., Nuseibeh B., Ince D., and Jackson M.: Using Abuse Frames to Bound the Scope of Security Problems, RE'04, Kyoto, Japan, 2004.

[6] Yu E.: Towards Modelling and Reasoning Support for Early-Phase Requirements Engineering, Proceedings of the IEEE Int. Symp. Requirements Engineering, Annapolis, Maryland, pp. 226-235, January 1997.

[7] Liu L., Yu E. and Mylopoulos J.: Analyzing Security Requirements As Relationships among Strategic Actors, 2nd Symposium on Requirements Engineering for Information Security (SREIS), Raleigh, North Carolina, 2002.

[8] Gaunard P. and E. Dubois: Using Requirements Engineering Techniques for Bridging the Gap Between Risk Analysis and Security Policies, 18th IFIP International Information Security Conference, Athens, Greece, May 2003.

[9] Dardenne A., Van Lamsweerde A. and Fickas S.: Goal-Directed Requirements Acquisition, Science of Computer Programming Vol. 20, North Holland, pp. 3-50, 1993.

[10] Chung L., Nixon B.A., Yu E. and Mylopoulos J.: Non-Functional Requirements in Software Engineering, Kluwer Academic Publishers, Boston, 2000.

[11] Sandra G. Behrens. Richard D. Pethia. William R. Wilson. :Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), Carnegie Mellon - Software Engineering Institute, June 1999.

[12] Harmonis M.: Analysis of Risks, (MEHARI), CLUSIF, Version 3, Octobre 2004.

[13] CRAMM Report, CCTA3 Risk Analysis and Management Method.

[14] Pandey Dhirendra, Suman Ugrasen, Ramani A. K.: Security Requirement Engineering Framework for Developing secure Software, International Journal of Computational Intelligence and Information Security (IJCIIS) Australia, Vol. 1 No. 8, October 2010, pp 55-65, ISSN 1837-7823.