Defining a Software Engineering Process with Cost-effective Security Requirements Implementation

Swe Zin Hlaing, Koichiro Ochimizu
University of Information Technology, Myanmar
swezin@uit.edu.mm , ochimizu@jaist.ac.jp

Abstract

Today, security problems involving computers and software are frequent, widespread, and serious. The number and variety of attacks by persons and malicious software from outside organizations, particularly via the Internet, are increasing rapidly, and the amount and consequences of insider attacks remains serious. Security is not just a question of security functionality; the properties desired must be shown to hold wherever required throughout the secure system. Because security properties are systems properties, security is an omnipresent issue throughout the software lifecycle. This paper describes the existing software development lifecycle with the integration of security engineering process. After that, we will adopt the Information System Environment in the case of the University of Information Technology (UIT). Moreover, this paper describes an Information Security Software Engineering (ISSE) process for discovering and addressing users' information protection needs based on the case study of UIT's information System Environment. Finally, the proposed system performs the quantitative risk analysis on the study of UIT Information System Environment.

Keywords- Information Security Software Engineering, Security Engineering Process, Quantitative risk analysis

1. Introduction

Security is often an afterthought during software development. A more effective approach for security requirement engineering is needed to provide a more systematic way for eliciting adequate security requirements. Information Systems Security Engineering (ISSE) is the art and science of discovering users' information protection needs and then designing and making information systems, with economy and elegance, so they can safely resist the forces to which they may be subjected. The main goal of this paper is to define the security software engineering (SSE) process with the existing software development lifecycle. In this process, the quantitative risk analysis is applied to SSE by implementing the cost-effective ways of security requirements. This paper is not intended to cover security through the entire SDLC. This paper is organized as follows. Section "Security Software Engineering Process" discusses the traditional Software Development Lifecycle (SDLC) integrates with security process and the process of Information System Security Engineering. Section "Quantitative Risk Analysis" presents the analysis of information assets quantitatively. Section "The case study of UIT's Information Environment" that explain the information system of UIT.

Section "Evaluation of the process" that shows some value after performing risk analysis on UIT's information assets. Finally, the last section describes the conclusion and future works of this paper.

2. Security Software Engineering Process

The overview of the integration of security engineering process with an ordinary System Development Lifecycle (SDLC) as shown in Figure.1.

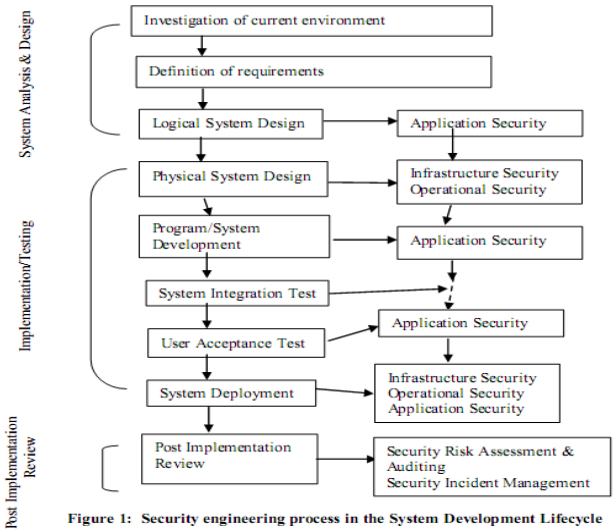

Figure 1: Security engineering process in the System Development Lifecycle

In this figure, each phase of the SDLC considers three types of security level: Application security, Infrastructure security and Operational security. Realizing security early, especially in the requirement phase, is important so that security problems can be tackled early enough before going further in the process and avoid rework. Requirement errors can be expensive

ISBN 978-99971-0-381-9

if they are not detected and fixed early in the development process.

The security engineering process proposed by Ian Sommerville is shown in Figure 2. Therefore, this paper proposed the integration of security engineering into the early phase of SDLC such as requirement definition phase and design phase.

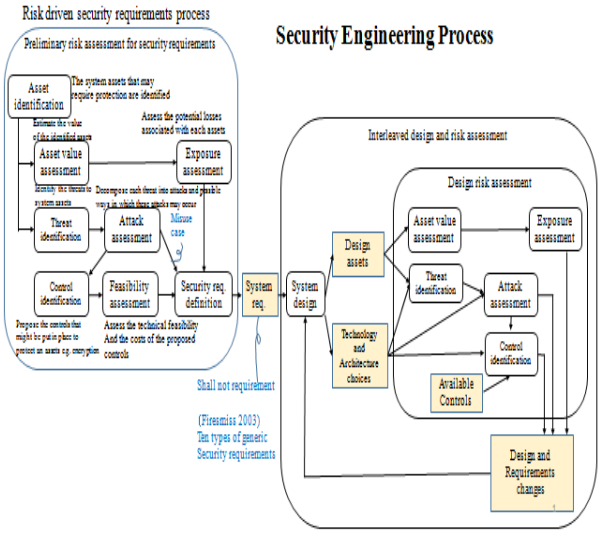

Figure 2: The security engineering process proposed by Ian Sommerville [1].

3. Quantitative Risk Analysis Process

The paper [2, 3] shows the step by step procedure of performing quantitative risk analysis. The main processes of quantitative risk analysis are as follow:

Perform risk assessment and vulnerability study: If the software development needs to consider the security, it is ensure to perform risk assessment and vulnerability study to produce risk factor matrix.

Estimate the cost of tangible/ intangible assets: During the study, we identify two types of assets such as tangible and intangible assets together with their estimated value. After that we need to determine the asset value.

Estimate the potential exposure factor (EF): We can estimate the exposure factor's value based on the identification of threats and/or survey and analyze to ask multiple questions to conduct the analysis.

Calculate Single Loss Expectancy (SLE): This process takes assets value and EF value as input parameters and produce the value of SLE.

Estimate Annualized rate of occurrence (ARO): Estimated frequency a threat will occur within a year and is characterized on an annual basis. A threat occurring once in 10 years has an ARO of 0.1; a threat occurring 10 times in a year has an ARO of 10.

Calculate Annualized Loss of Expectancy (ALE): It takes SLE and ARO as input parameters and produce ALE value.

Calculate Cost/Benefit Analysis: This process performs calculating the difference between the ALE prior to implementing the countermeasure to the ALE after implementing the countermeasures.

In this paper, we intend to integrate the security engineering process with quantitative risk analysis that emphasize on early stage of SDLC. Therefore, the proposed integration of the entire process that integrates security engineering process with quantitative cost analysis as shown in Figure 3.

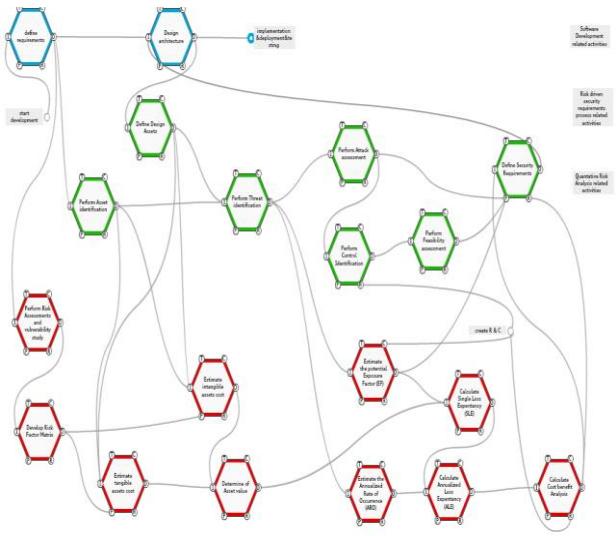

Figure 3: The entire integration process of security engineering process and quantitative risk analysis process

4. A case study of UIT's Information System Environment

By analyzing in the case of UIT Information Environment and list the following assets as shown in Table 1. To determine the cost of assets, we need to analyse the list of threats and vulnerabilities based on the case study.

In the section 4.1 describes the list of some identified threats based on our environment. And then vulnerability study on some of survey results describe in section 4.2.

Assigning values to tangible assets, the following are some typical methods for obtaining estimates for tangible assets.

Table 1. Categorization of Assets

Tangible Assets	Intangible Assets
Desktop PCs	Application Software
Laptop PCs	Technical Software
Servers	Electronic Data
Printers	Emails
Photocopiers	
Telephone	
Fax Machines	
Network Hubs and Routers	
Backup Media	
General Office Equipment	
Training Materials	
Personnel Files	

(a) Ask the IT manager for cost information regarding existing equipment, software and hardware.
(b) Conduct research on the Internet. Determine the age of current tangible assets, and calculate value by including depreciation.
There are two typical approaches for determining the valuation of intangible asset.
(a) Cost Approach – seeks to measure an asset's fair market value, with depreciation also taken into account. The cost approach does not directly consider either the amount of economic benefits that can be achieved or the time period over which they might continue. A cost approach is typically used for valuing trade secrets and know-how.
(b) Income Approach – Focuses on the income producing capability of the intellectual property. The value is measured by the present value of the net economic benefit over the life of the assets. When the economic conditions are not favorable, the income approach leads to a relative low valuation of assets. This approach is best suited for the valuations of patents, trademarks, computer software, and copyrights.

4.1 Identification of Threats

We survey and analyze the UIT's Information Environment [4] . We found out some identifiable threats and how often they occur and their impact as shown in Table 2 and Table 3.

Table 2. List of identified Threats

Ref.	Threat
1.1	Air condition failure
1.2	Damage to communication lines/ cables
1.3	Deterioration of storage media
1.4	Failure of communication services
1.5	Failure of network components
1.6	Failure of Database
1.7	Failure of power supply
1.8	Hardware failure
1.9	Illegal use of software
1.10	Maintenance error
1.11	Malicious software (eg. Viruses, worms. Trojan horses)
1.12	Software failure
1.13	Staff shortage
1.14	Theft

After identifying the possible threats of UIT's environment, assign the risk values based on occurrences of threat (likelihood) and impact (severity). Table 3 shows the estimated risk assessment value on identified threats.

Table 3. Risk assessment value of threat

Ref.	Likelihood	Severity
1.1	M	VH
1.2	L	H
1.3	L	VH
1.4	M	H
1.5	M	H
1.6	M	H
1.7	L	VH
1.8	M	H
1.9	H	H
1.10	M	H
1.11	H	H
1.12	M	VH
1.13	M	H
1.14	M	H

4.2 Identification of Vulnerabilities

From the study of vulnerability, the list of vulnerabilities, both technological and organization-related, that can affect the organization's assets as shown in Table 4.

Table 4. List of identified vulnerabilities

Ref.	Vulnerability	Ease of exploitation
2.1	Absence of personnel	M
2.2	Insufficient security training	M
2.3	Lack of monitoring mechanisms	M
2.4	Inadequate recruitment procedures	M
2.5	Inadequate or carless use of physical access control to buildings, room and offices	M
2.6	Lack of physical protection for the building doors and windows	M
2.7	Location in an area susceptible to flood	H
2.8	Insufficient maintenance	M
2.9	Lack of periodic equipment replacement schemes	M
2.10	Unstable power grid	M
2.11	Lack of identification and authentication mechanisms	H
2.12	Inadequate network management	H
2.13	No "logout" when leaving the LAN	H
2.14	Uncontrolled downloading and using software	VH

5. Evaluation

After a vulnerability assessment and threat analysis, I have proceed to quantify the risk element. After conducting the survey of the organization, it would be much simpler if it can estimate ALE directly from using the risk analysis data referenced in paper [3]. In addition, I will need to add a ranking number from 1 to 10 for quantifying severity (with 10 being the most severe, and 1 of least severity) as a correction factor for the risk estimate obtained from the data table. For UIT's Information System Environment, I may study the internet threats and issues such as uncontrolled downloading using software.

The estimated value of 78% detected students in UIT abuse of Internet access privileges (for example, downloading the video file in their classes or playing online game). So, this kind of vulnerability is very important for our environment. Conducting the risk analysis on uncontrolled downloading and using software, it has a severity ranking of 8 and we can use the corresponding adjustment factor used will be 1.1 as shown below.

Severity Ranking

10	9	8	7	6	5	4	3	2	1
1.2	1.2	1.1	1.1	10	10	0.9	0.9	0.8	0.8

Adjustment Factor

According to the data table in [5,6]
Annual revenue = $ 0.01 Million
Number of students = 1000
Size Correction (using data from CSI) = 1000 / 4700 = 0.2
ALEtable = $ 536,000
ALEcorrected = $ 536,000x 1.1 x 0.2 = $ 117920
I will study some survey data of ASIS report and estimate the ALE value of uncontrolled downloading using software in the case of UIT environment.

6. Conclusion and future works

This paper concerns the first step of integrating security engineering process and quantifying risk assessment. Then, we intend to analyze the critical security breaches concerning about our UIT environment and later on do the cost/benefit analysis on these data. After that the integration of all SDLC processes into the security engineering process should be performed. Finally, we need to evaluate our engineering approach is beneficial for financial and technological issue.

7. References

[1] Sommerville,I " Software Engineering, tenth Edition, Pearson, 2015

[2] ISO/IEC 27002:2005 Information technology- Security techniques- Code of practice for information security management , 2013

[3] Tan.D, Quantitative Risk Analysis step-by-step, 2002

[4] Exemplar_ISMS Risk Assessment Manual Version1.4.rtf , https://www.noexperiencenecessary book .com /m7V6/ isms-risk-assessment-manual-version-1-4.html

[5] ASIS International. "Trends In Proprietary Information Loss Survey Report." Septem2002. URL: http://www.asisonline.org/pdf/spi2.pdf

[6] Computer Security Institute (CSI) . "2002 CSI/ FBI Computer Crime and Security Survey." Computer Security Issues & Trends.Vol.8, No.1 Spring 2002.