An approach to Cost-effective Software Development Strategy for Secure Information Systems

Kyawt Kyawt San, Swe Zin Hlaing, Koichiro Ochimizu
University of Information Technology (UIT), Myanmar
kyawtkyawtsan@uit.edu.mm, swezin@uit.edu.mm, ochimizu@jaist.ac.jp

***Abstract*— Software security attacks such as misuse of hardware resources, steal confidential data, or denial of services, are frequently occurred to software systems. A larger percentage is caused by software design defects. Most of the organizations completely depend on software systems for their day-to-day operations, and hence, it is important to produce secure software products on cost-effective way. This paper proposes a security engineering process in the system development lifecycle processes that help to develop secure systems on University of Information Technology (UIT) in cost-effective way by using cost/benefit analysis. A Secure Software Development Model that integrates security engineering with software engineering is proposed so that it ensures the developed software system is secure within given budget and usability constraints. In this proposed model, estimating techniques for assets value and their risk factors will help to present a cost effective approach for security engineering process. Security policies and guidelines in forms of laws are also supported to guide developers throughout the development process. The proposed secure system aims to help in developing a secure software systems based on UIT's Information Environment concerning with security requirement document including cost effective approach.**

Keywords—Security Attacks, cost/benefit analysis, Security Policies and guidelines

I. Introduction

As more and more systems are connected to the Internet, a variety of different external attacks such as misuse of hardware resources, steal confidential data, or denial of services are frequently occurred to these systems. Software engineers should be aware of the security threats and should implement proper degree of security mechanisms that meet the security requirements. Everyone knows, however, that building secure system is expensive. We need to have security engineering processes that help us to develop secure systems in cost-effective way. Cost-effective way means that we should be concerned with designing a system so that it is as secure as possible, given budget and usability constraints. We should pay attention on how much cost spent on the security failures and what level of security mechanisms we must ascertain in advance. In this proposal, we consider three kinds of security such as infrastructure security, application security and operational security. For designing the application software, software engineers should ensure the application security that the software system is designed to prevent the attacks. While setting up the infrastructure, system engineers makes the most effective way of designing infrastructure security to consider the variety of potential security vulnerabilities and holes. Moreover, the application engineer is concerned with designing a system so that it is as secure as possible, given budget and usability constraints. So, application security requirements may be implemented through the infrastructure or the application itself. Operational security may concern with human and social issue (cyber security, equipment failure, etc).

II. Research Background

A. Background Theory

The security engineering process should be merged into an ordinary System Development Lifecycle (SDLC) as shown in Figure.1.

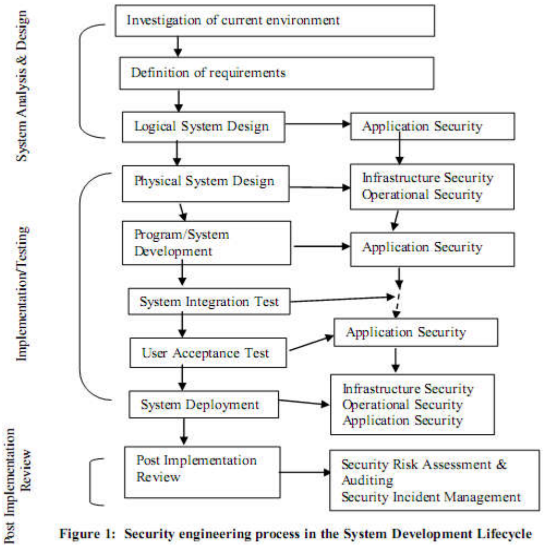


Figure 1: Security engineering process in the System Development Lifecycle

B. *Cost-Effective Security Engineering Process*

Cost-effective security engineering process heavily relates to the system analysis and design phase of SDLC in Fig. 1. An example of security engineering process proposed by Ian Sommerville is shown in Figure.2.

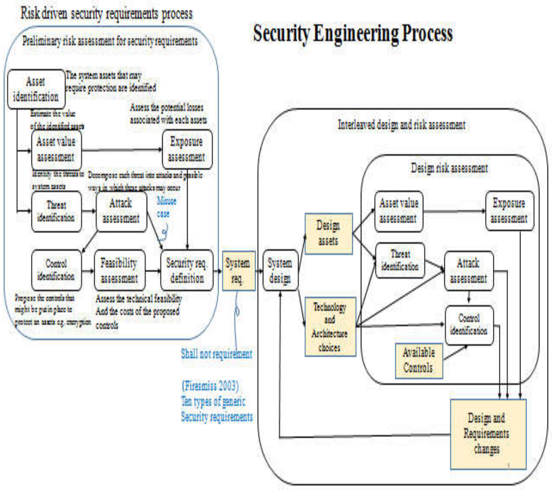

Risk driven security requirements process
Preliminary risk assessment for security requirements
Security Engineering Process
Asset identification
The system assets that may require protection are identified
Estimate the value of the identified assets
Assess the potential losses associated with each assets
Asset value assessment
Exposure assessment
Identify the threats to system assets
Decompose each threat into attacks and possible ways in which these attacks may occur
Threat identification
Attack assessment
Misuse case
Control identification
Feasibility assessment
Security req. definition
System req.
Propose the controls that might be put in place to protect an assets e.g. encryption
Assess the technical feasibility And the costs of the proposed controls
Shall not requirement
(Firesmiss 2003) Ten types of generic Security requirements
Interleaved design and risk assessment
Design risk assessment
System design
Design assets
Technology and Architecture choices
Asset value assessment
Exposure assessment
Threat identification
Attack assessment
Control identification
Available Controls
Design and Requirements changes

Figure 2: Risk Assessment Process

The process shown in Figure.2 help us to define two types of security requirement. One is system requirements and the other is design requirements. Major activities included in the process are:

(1) Asset Identification
(2) Asset value assessment and Exposure assessment
(3) Threat identification and attack assessment
(4) Control identification and Feasibility assessment
(5) Security requirement definition

We are going to improve the above procedure to get security requirements list with the order of priority within the budget which we can spend. We call the improved procedure cost-effective security engineering process.

III. Proposed System

We adopted the Information System Environment of the University of Information Technology. Figure.3 shows the UIT's Information System Environment. This environment has system of systems of software systems that contains different user type such as management, staff, student and citizen and so on. Security policies set out information access strategies that applied across the university. Firesmith (Firesmith 2003) identified 10 types of security requirements and we may consider on three types of security design issues such as infrastructure security, application security and operational security.

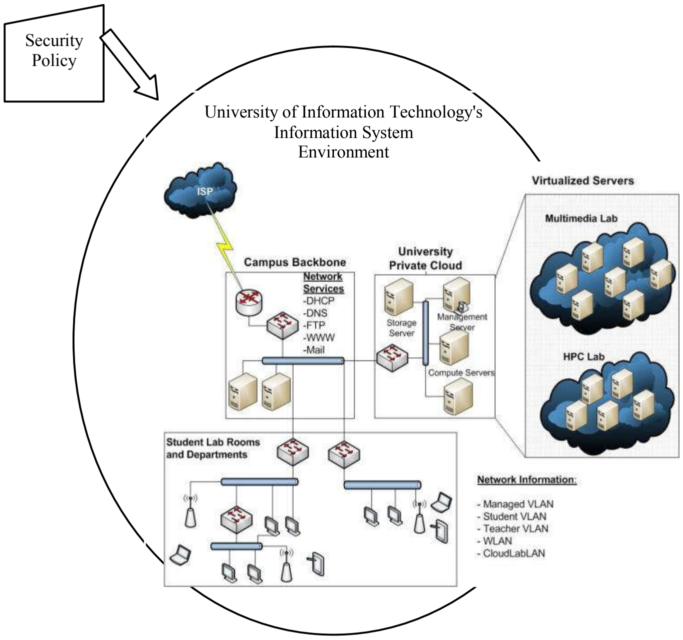
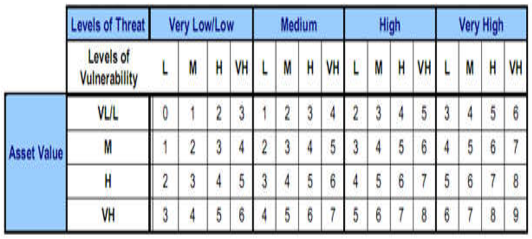


Figure 3. Proposed System Design for UIT's Environment

In this section, the Risk Assessment Analysis of UIT information Environment is presented.

Table 1 : A matrix for measure of risk



	Levels of Threat	Very Low/Low				Medium				High				Very High			
	Levels of Vulnerability	L	M	H	VH	L	M	H	VH	L	M	H	VH	L	M	H	VH
Asset Value	VL/L	0	1	2	3	1	2	3	4	2	3	4	5	3	4	5	6
	M	1	2	3	4	2	3	4	5	3	4	5	6	4	5	6	7
	H	2	3	4	5	3	4	5	6	4	5	6	7	5	6	7	8
	VH	3	4	5	6	4	5	6	7	5	6	7	8	6	7	8	9

The matrix shown above has been used to determine the 'Measure of Risk'. The matrix is 3 dimensional taking into account Threats, Vulnerabilities and Asset Value resulting in an overall 'Measure of Risk' in the range 0 (no risk) to 9 (very high risk) [5].

A. Assets identification & value assessment

We analyze the current UIT Information Environment and list the following information assets as shown in Table 2 according to the value of above matrix in Table 1.

B. Quantitative Risk Analysis

The following is a step-by-step breakdown of the quantitative risk analysis [4].

(1) Conduct a risk assessment and vulnerability study to determine the risk factors shown in Table 1.

Table 2 : Type of assets and its value

Assets	Value (VH, H, M,L)
Paper Documents	
Training Materials	M
Personnel Files	VH
Emails	H
Physical Assets	
Desktop PCs	L
Laptop PCs	L
Servers	M
Printers	L
Photocopiers	L
Telephone	L
Fax Machines	L
Network Hubs and Routers	VH
Backup Media	VH
General Office Equipment	L
Logical Assets	
Application Software	L
Technical Software	L
Electronic Data	VH
People	VH

(2) Based on the matrix , determine the value of assets under risk factor. Determine the assets value regards to the UIT information Environment. Use the data in Table 2 to make quantitative estimates for risk analysis.

(3) Estimate the Annualized Rate of Occurrence (**ARO**) for each risk factor according to the following equation.

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.

(4) Before Determining the Annualized Loss Expectancy (ALE) for each risk factor , we need to calculate firstly Exposure Factor (EF) and Single Loss Expectancy (SLE).

Exposure Factor (EF) = Percentage of asset loss caused by identified threat, ranges from 0 to 100%.

Estimating the Potential Exposure Factor

Here is a method for estimating the exposure factor for use in conducting risk analysis.

Start off with 100% for the starting exposure factor and answer each of the following questions…

1. Does the system under attack have any redundancies/backups/copies?
   Subtract 30% if the answer is YES
2. Is the system under attack behind a firewall?
   Subtract 10% if the answer is YES
3. Is the attack from outside?
   Subtract 20% if the answer is YES
4. What is the potential rate of attack? (10% damage /hour vs. 10% damage/min)

Subtract 20% if the answer is less than 20% damage/hr

Subtract 40% if the answer is less than 2% damage/hr

5. What is the likelihood that the attack will go under-detected in time for a full recovery?

Subtract 10% if the probability of being undetected is less than 20%

Subtract 30% if the probability of being undetected is less than 10%

6. How soon can a counter measure can be implemented in time if at all?

Subtract 30% if the countermeasure can be implemented within ½ hour

Subtract 20% if the countermeasure can be implemented within 1 hour

Subtract 10% if the countermeasure can be implemented within 2 hour

Single Loss Expectancy (SLE) = *Asset Value * Exposure Factor;*

1,000,000@ 20% likelihood = $200,000

(5) Before estimating cost/benefit analysis, we need to calculate Annualized Loss Expectancy (ALE).

Annualized Loss Expectency(ALE) = *Single Loss Expectancy * Annualized Rate of Occurrence*

ALE can sometimes be extrapolated from existing comparable data.

(6) Conduct the safeguard cost/benefit analysis by calculating the difference between the ALE prior to implementing the countermeasure to the ALE after implementing the countermeasures.

Safeguard cost/benefit analysis = *(ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard)*

After applying the step (1) to (5), the table 3 shows the initial result of quantitative risk analysis regards to the UIT's Information Environment.

IV. Conclusion

In this research proposal, estimating techniques for assets value and their risk factors will help to present a cost incentive approach for security engineering process. A discussion of methods for the risk analysis will help to quantify the information environment in the University of Information Technology (UIT). The initial result shown in this paper has the standard factor of analysis and later on it is needed to calculate the cost/benefit analysis. We have to incorporate with information security management committee from UIT and define the potential countermeasure and their costs. Finally, we will determine the return on investment using Internal Rate of Return (IRR) based on the quantitative analysis. This proposal aims to help in developing a secure software systems based on UIT's Information Environment concerning with security requirement document including cost effective approach.

References

[1] Ian Sommerville, Software Engineering, tenth Edition, Pearson (2015)

[2] Donald Firesmith and Didar Zowghi: Requirements Engineering: AFramework-Based Handbook, 2003.

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

[4] Ding Tan, Quantitative Risk Analysis step-by-step (2002)

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

Table 3 : Quantitative Risk Analysis for UIT's Information Environment

Assets	**Value (VH, H, M,L)**	**Exposure Factor**	**Single Loss Expectancy (A.V*EF)**	**Annualized Rate of Occurrence (ARO)**	**Annualized Loss Expectancy SLE*ARO**
Paper Documents					
Training Materials	M (5)	30%	5*0.3=1.5	0.1	1.5*0.1=0.15
Personnel Files	VH (9)	30%	9*0.3=2.7	0.1	0.27
Emails	H (7)	10%	7*0.1=0.7	0.1	0.07
Physical Assets					
Desktop PCs	L (3)	20%	3*0.2=0.6	0.1	0.06
Laptop PCs	L (3)	20%	3*0.2=0.6	0.1	0.06
Servers	M (5)	40%	5*0.4=2	0.1	0.02
Printers	L (1)	20%	1*0.2=0.2	0.1	0.02
Photocopiers	L (1)	20%	1*0.2=0.2	0.1	0.02
Telephone	L (1)	20%	1*0.2=0.2	0.1	0.02
Fax Machines	L (1)	20%	1*0.2=0.2	0.1	0.02
Network Hubs and Routers	VH (9)	40%	9*0.4=3.6	0.1	0.36
Backup Media	VH (9)	30%	9*0.3=2.7	0.1	0.27
General Office Equipment	L (1)	20%	1*0.2=0.2	0.1	0.02
Logical Assets					
Application Software	L (1)	10%	1*0.1=0.1	0.1	0.01
Technical Software	L (1)	10%	1*0.1=0.1	0.1	0.01
Electronic Data	VH (9)	30%	9*0.3=2.7	0.1	0.27
People	VH (9)	10%	9*0.1=0.9	0.1	0.09