International Journal of Computer & Information Technologies (IJOCIT)
www.ijocit.org & www.ijocit.ir
ISSN= 2345-3877

An Approach for Secure Software Development Lifecycle Based on ISO/IEC 27034

Ali Taati[1] **, Nasser Modiri**[2]

MSc, Department of Electrical, Computer & IT, Zanjan Branch, Islamic Azad University[1],

Associate Professor in Department of Electrical, Computer & IT, Zanjan Branch[2],

Islamic Azad University, Zanjan, Iran[1,2]

Ali.taati.ch@gmail.com [1] , *Nasser.modiri@yahoo.com*[2]

Abstract: In the process of software secure development it is observed that security issues are discussed more generally and the confidential level of organizations, the characteristic of each organization in the terms of the principles of the organization and the security framework of the software are not considered more in these models. This article refer to two important principle in terms of the understanding and recognition of the place of the security of software applications of each organization based on the ISO indicators27034 by concentration on the design phase and it is said that secure application should be defined based on the organizations' normative framework and the software normative framework, the targeted level of the different software security related to the field of the business and the level of importance of information get clear on that realm. This article makes it clear in addition to those software developers for common principles of software security that should be continuously controlled in each phase; they should refer to the organizations' security framework to implement during process.

Keywords: Software Security, Software Secure Development, Vulnerability, Principled Security Framework

1. Introduction

Nowadays organizations know that they must protect their information and also in the business-administrative and educational activities without using software is impossible, the main point is that their vital information are being kept in database of this software[3]. The smallest security damage in this software can destroy these companies and organizations in a competitive and sustainability environment in the business. Now the place of security in software gets clear well. Security software was not produced even in the process of security that

all the produces processes of the software included alike in figure 1.often in production of security software does not pay attention to the level of the target level of trust. Development teams run security according to the set of common standards. However a security framework seems to be crucial and essential for the safe and secure application development process. Although there are much good activities has been done in this realm but while some people are trying to penetrate in software with their knowledge and misuse its information, the software producers should increase their effort in order to improve the process of software and produce a safe software[6].

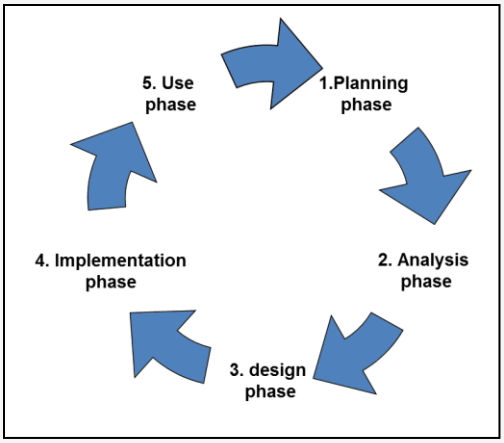

Figure 1: Software Development Process

2. Secure Software Development Lifecycle

Identification costs and management of software security risks in its cycle development are less than end of the production and software delivery, while according to figure 2 the Vulnerabilities of software increase each year. Although it is clear that without the safe software production line we can't have secure application. Also today's organizations competitive business environment depend on soft ware's which have enough accuracy in this area. According to the reported Vulnerabilities in the software area existence of secure lifecycle software, resulting in the production and development of secure application is very necessary [1].

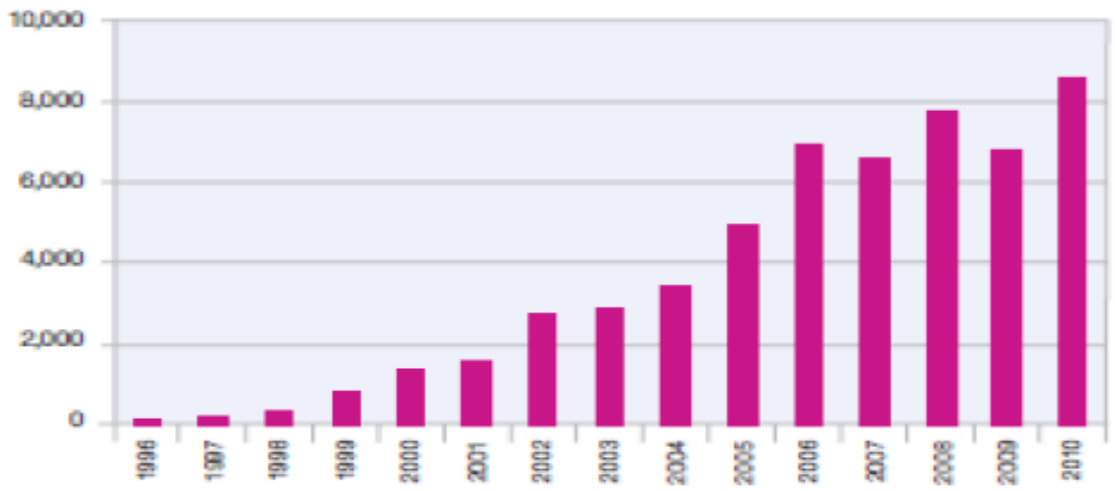

Figure 2: Software Vulnerability According to the Statistics [1]

2.1. The Security Principles of ISO/IEC 27034

The aim of the ISO 27034 is to provide guidance and a road map in order to select the best method for extended security and create a development of secure software application life cycle and better understanding of users, developers, managers and assessors of Organization Normative Framework (ONF) and applicant normative framework (ANF) and recognition needs of organization in implementation of software [6].

The Security Principles which ISO 27034 has more focuses on them are:

- Security is a necessity.
- The security of software is dependent on its application.
- Financial allocation for software security
- The security of software is an ongoing and continuing issue.

The ISO 27034 refers to the point that success in software assurance program is directly related to its executive management. All the applicants of secure software should be aware about Common principles and security threats. The creation of secure software is the result of association of all the applicants at different levels of secure lifecycle software. The applicants must learn how to create and inject security in the body of software in its all phases such as: requirements, design, development and implementation.

This standard is applicable to the organizations with a various sizes. Among the advantages of this standard is recognition of security metrics

and indicators to understand and maintain control of the security organizations.

3. Suggested Method

This approach based on sequential in each phase from the secure software development to the cycle framework security and executive rules in the organization

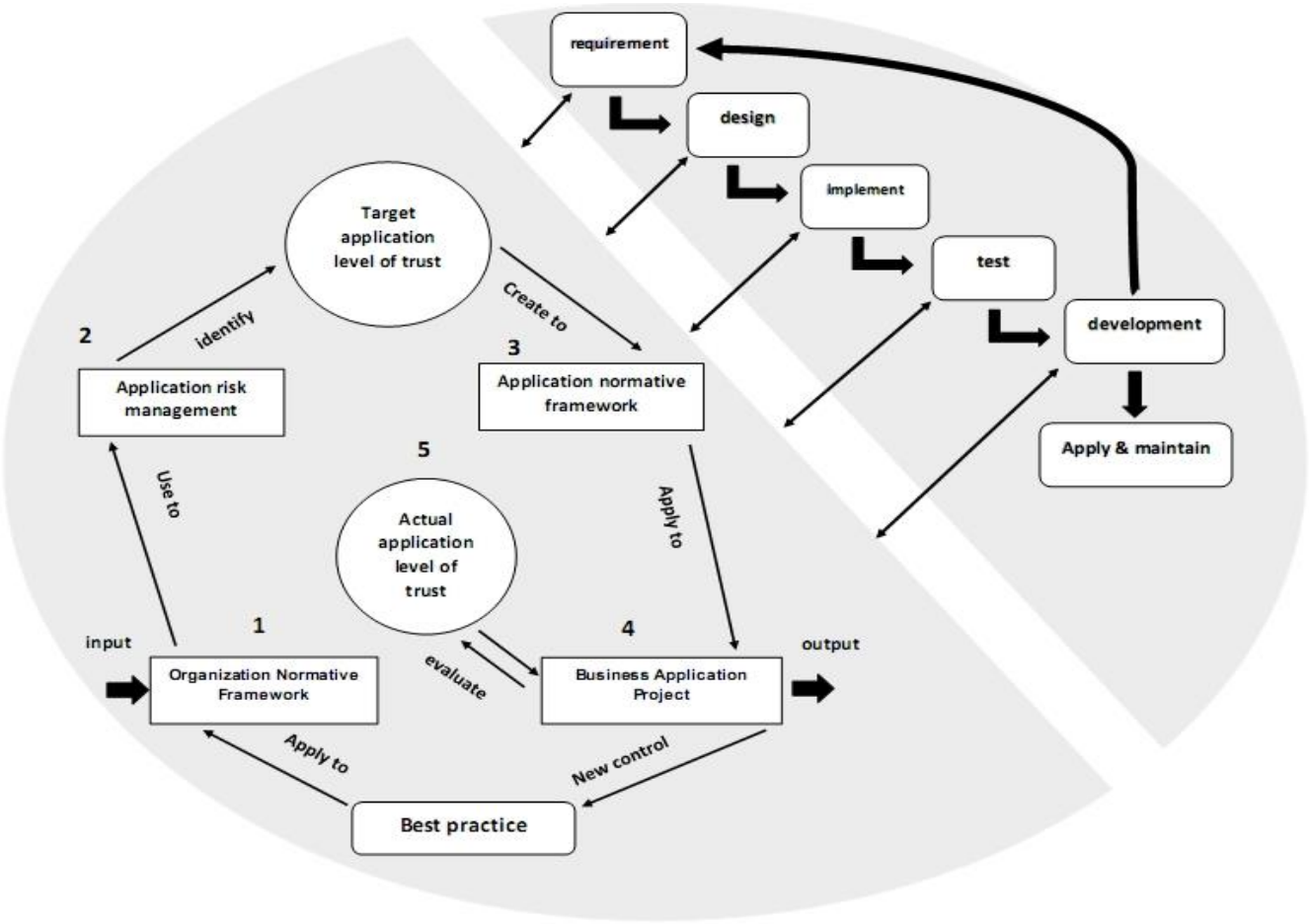

Figure 3: Secure Software Development Lifecycle

In fact this suggestion is based on two important principle in order to understand and recognize the position of the software security applicant and believes that security software should be defined based on the organization and software's principles and framework, meaning that targeted level of the different software security of organization depend on the business and the level of the information's' importance.

In this approach to development of software process the cascade model is used, that consist of these advantages:

- Have a clear process for implement than other mod
- Create prototype software
- Better connection with the project managers.
- Easier troubleshooting than other models.
- Reduce the complexity of the design.

This approach states that each organization should have a secure software design framework according to their business factor and make software developers that in the steps of software generating should follow organization's secure software management system rules.

3.1. Implementing Activities Description

- Requirements and Evaluation Phase:

At first we gather and analyze operational and functional requirements and then classified requirements and evaluate them, performance of these activities continuously enter the organizations' secure process and monitoring and refining requirements and after first completion enter the next phase.

- Design phase:

Software design is according to the determined requirements of the organizations software's frame work and then evaluated by threatening model in accordance with software features and vulnerability limited.

- Implementation Phase:

In this stage by obtained information from the requirements and design stage we start implementing; implementation should be consonant with a declared systems by a life cycle approach such as determining programming language, functions, data base and etc.

- Test phase:

In the test phase operation is according to the targeting confidence level and systems security is determined based on organizations' business security policies.

- Progress phase:

In this phase the first production of the software and the necessity survey is done. The first sample is studied in order to remove possible defects by checking the approach cycle and deliver this sample to the organization and by identification difficulties enter the second phase of software.

- The performance phase:

In this stage the software according to the general and special standard is ready to use.

3.2. The Secure Operation of the Design Phase

We can call the design phase the most important step in software creation in which all security requirements document, Production and revision of design models, threatening modeling, analysis and design of security modules are examined exactly. Named activities are based on organizations' life cycle approach, for example threatening modeling must be according to the rules, strategy and security needs of organization or designed at a higher level.

In this phase stated requirements analyzed in requirement phase and will be documentation and then enter to the organizations' software secure

lifecycle and prepared list evaluated according to the rules and security framework.

Different design model designed according to the strategy and revised in relation to the regular connection and its initial design is prepared.

In the second step that subsequent construction began after that threatening model is chosen based on design and performance. With recognizing the vulnerability of this area needed reforms is done and documented and delivered to the second phase.

3.3. Approach Anatomy

The presented approach with an effective interaction in each phase use software secure development in addition to run the general security policy and also organizations' security management, and always tries to provide the confidence level of the organization.

Security management process consists of five stages:

Organization Normative Framework (ONF): For each phase of the software development process its entrance is a reference input .this phase is a collection of the rules and strategies of the organization, that is a criteria for defining requirements, design model and identifying threats.

Risk Management Software: In this stage possible risks are identify and evaluated according to the previous step definition, these risks are analyzed with expected confidence level of the organization.

Applicant Normative Framework (ANF): Including software applications rules and confidence targeted level, that all functions and algorithms should be defined based on these strategies.

Business software project: It is using the normative framework of the organization toward summing and documentation of previous activities and evaluation of these activities with software's actual confidence level. Executive Team will be implemented security activities of previous step in this stage.

Actual confidence level of the software: This stage which may be performed by an internal or external team with criteria in step3, evaluation and necessary security controls are done.

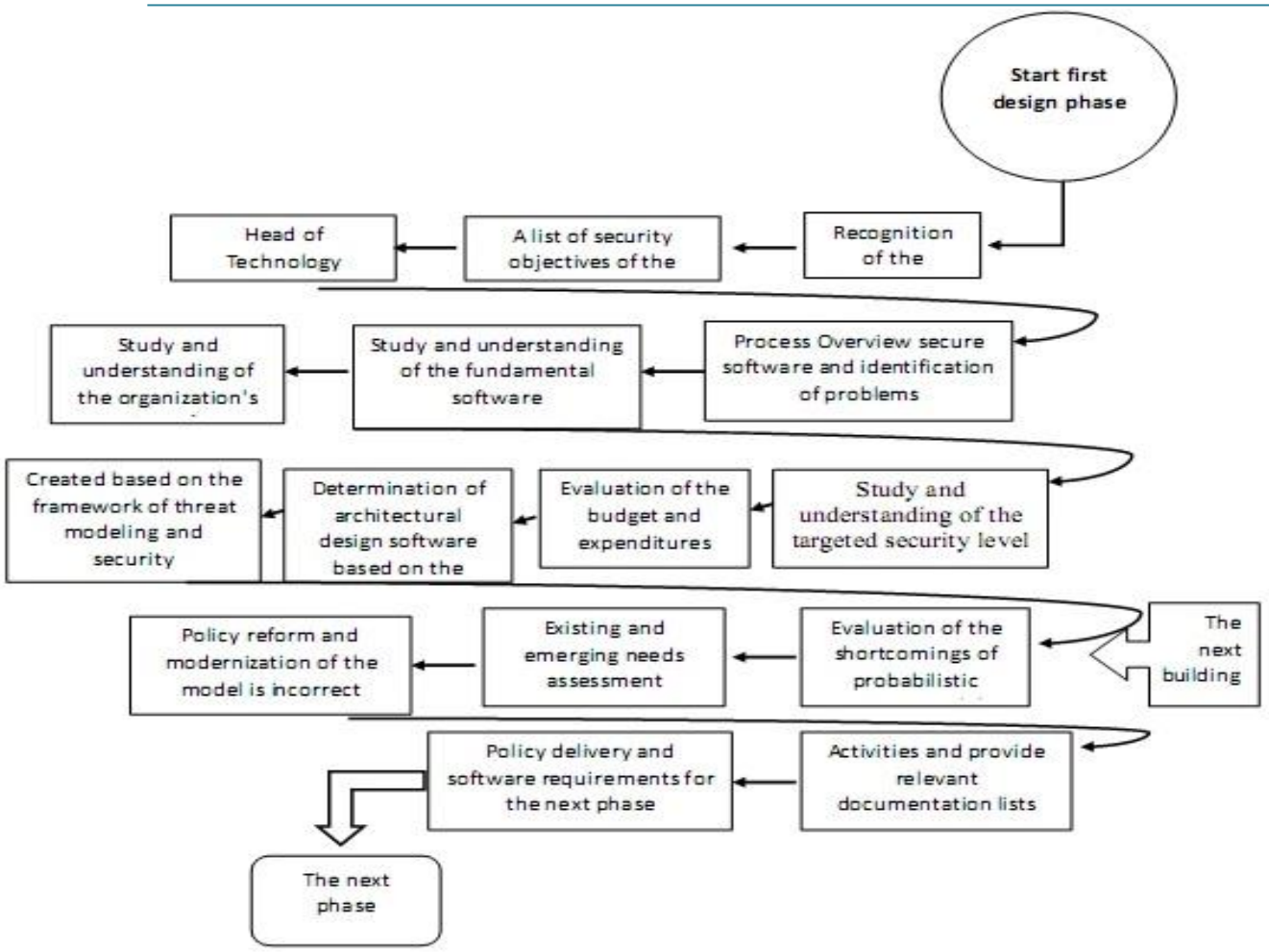

Figure 4: Security Activities of the Design Phase

4. Conclusion:

So it is important to note that software developers in addition to the common principles of software security that must be continuously controlled (in each phase), should be refer to organizations' security framework to implemented each phase. In continue we compare this approach with other models of security software development in the form of a chart based on expressed Indicators.

Table 1: Comparison of Different Models with Our Proposed Method

	Common criteria	Opensamm	Microsoft-sdl	Proposed approach
Secure configure management	√	–	–	√
Rules&policy&procedure	–	√	–	√
Risk analize	√	√	√	√
Organization-oriented process	–	–	–	√
Security education	–	√	√	–
Safe delivey	√	√	–	√
Safe regional development	–	–	–	√
Reducing the secure cost	√	–	–	√
Continuing security relationship with organization	–	–	–	√
Threat modeling	√	√	√	√
Control software compatibility	√	-	-	√
Reduce time application delivery	-	-	-	√
Compatibility with government and law	√	-	√	√
Ability to define organizational safely development cycle	-	-	-	√

As you see in the above table most of the security software models don't pay attention to the Regional development processes but also provide a general method that it will entail the following problems:

- Lack of objective criteria to ensure the organization.
- Production software with multiple vulnerabilities.
- Lack of customer satisfaction.
- Increased cost of software security.
- Lack of proper communication with those involved in the software owner.
- Failure to properly and efficiently identify vulnerabilities.
- Payment of unnecessary items and spends more time.

It can be said that for having Security Lifecycle process and security software according figure 5 the following components must be observed:

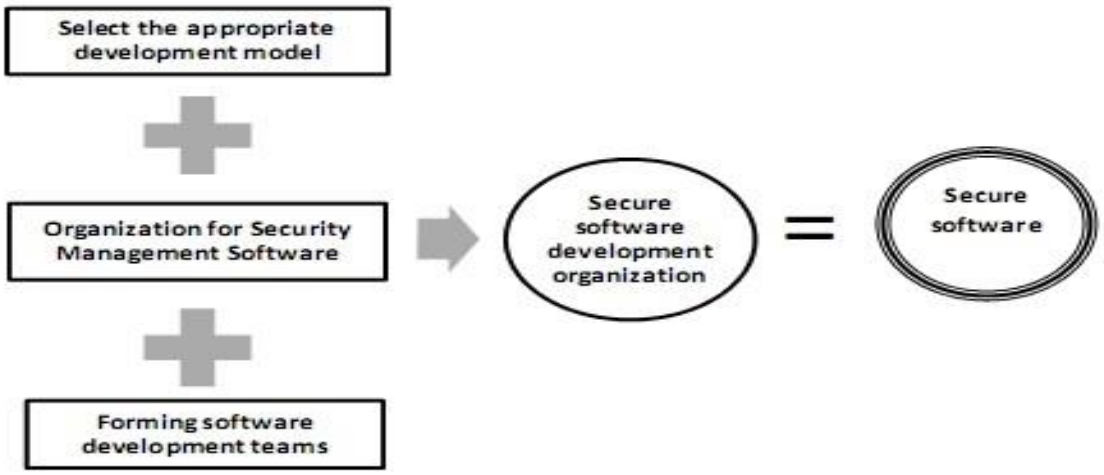

Figure 5: Secure Software Component

Thus producing secure software in an organization won't come off unless in the secure software production line and

a safe production line can't be made except recognition of the software security framework of each organization- determine the confidence range of software and adapted security policies by the employee and Create a specific internal process in which Different security requirements determined and evaluated by the threatening models and The vulnerabilities based on the confidence level of the targets are identified and controlled.

References

[1] Mehmet Kara,(2012), "Review On Common Criteria As A Secure Software Development Model", International Journal of Computer Science & Information Technology (IJCSIT) Vol 4, No 2.

[2] Muhammad Shakeel Faridi, Tasleem Mustafa and Fahad Jan,(2012)," Human Persuasion Integration in Software Development Lifecycle (SDLC)", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3.

[3] Malik Imran Daud, (2010),"Secure Software Development Model: A Guide for Secure Software Life Cycle", proceeding of the international multiconference of engineers of computer scientists IMECS hong kong.

[4] C. Banerjee, S. K. Pandey,(2009)" Software Security Rules: SDLC Perspective", (IJCSIS) International Journal of Computer Science and Information Security.

[5] A. Adebiyi, Johnnes Arreymbi and Chris Imafidon,(2012)," Security Assessment of Software Design using Neural Network",IJARAI) International Journal of Advanced Research in Artificial Intelligence.

[6] Reaves Consulting Group, LLC,(2013)" The emergence of software security standards:ISO/IEC 27034-1:2011 and your organization".

[7] Noopur Davis,(2005)," Secure Software Development Life Cycle Processes: A Technology Scouting Report",Technical Note CMU/SEI-2005-TN-024.

[8] Kakali Chatterjee • Daya Gupta • Asok De,(2013)," A framework for development of secure software''",CSIT