ICEB 2005 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-5-2005

Model of Information Security Engineering Based on SSE-CMM

Hong Yang

De-li Yang

Zhi Zheng

Model of Information Security Engineering Based on SSE-CMM

Hong Yang, De-li Yang, Zhi Zheng
System Engineering Research Institute
Dalian University of Technology, China, 116023
EMAIL: yh.Maggie@163.com

Abstract: On the basis of the project thought of SSE-CMM, this paper presents a kind of information security engineering model based on SSE-CMM. And it expounds the concrete work at each stage in the course of security engineering in detail.

Keywords: Information System Security, Information S ecurity Engineering, SSE-CMM

I. Introduction

I. 1 Information security engineering

With the rapid development of information technology and network technology, information system has been paid much more attention and widely used in the various aspects of our society. However, “information system security becomes a key question in the development of the global information society and gets more and more serious since there exists more problems: web attack, virus infected, wrong use by the interior stuff. People take series of measures and technology to grantee the information system security. Such as physical separation, firewall, identity certification, visiting control, identity identification, audit etc. But system security problem is dynamic and covers many aspects: security technology, products, stuff, management and so on. Therefore, information system security is not only a technological process, but a social process as well. It must be dealt with as engineering and solved by the means of system engineering. Therefore the idea of information security engineering is put forward. Information security engineering [1] is such a process that adopts concept, principle, technology and method of engineering to study, exploit, implement and maintain information and web system security in the enterprise rank. It combines engineering implementation flow, which is proved to be right by time, management technology and the best technology available now. To guarantee information system security according to the idea of information security engineering is to solve various problems in the whole security process.

I. 2 Problems existing in information security engineering

Since the idea of information system security was put forward in 1972, the evolution of the related theories and approaches has experienced several stages. It develops into LAN, Internet environment from a stand-alone environment and changes its service object from the military field to commercial organization. It takes the approaches of system engineering as a comprehensive way to tackle all the problems rather than just unitarily depend on the technology [2].

Traditional system security engineering is regarded as a special engineering activity. Its aim is to apply the information protection technology to the established system structure and design norms. It focuses on the final system and products. Furthermore, it usually does not take the investigation about the basic protection demand of the company. This kind of approach lacks of the process control of the information system security structure and makes the security engineering activity separate from the system engineering activity. This will bring about the problem about the security vulnerability and lead to the system unsteadiness. In order to solve these problems and make it well applied, the information system security must be combined with the system engineering and the information system engineering must be integrated. It should be a process going in step with the process of the integrated system engineering. If it does not run like this, it will result in the uncertainty of the measures of system security. Then the users cannot get the available risk rank of the system correctly.

I. 3 The significance of researching information security engineering

The significance of researching information security engineering is determined by the properties [3] of the information security.

(1) Information security is of sociality

The content of information security assurance is more universal and comprehensive than ever before.

(2) Information security is of comprehensiveness

Information security problems should be considered in overall aspects and the extent of the system security depends on the weakest part of the system.

(3) Information security is a process and has lifecycle

A holistic security process include at least the confirmation of security target and principle, risk analysis, requirement analysis, security strategies research, security architecture research, the confirmation of security implementation field, testing and selecting of security technology and products, security engineering implementation, security engineering implementation

Proceedings of the Fifth International Conference on Electronic Business, Hong Kong, December 5-9, 2005, pp. 518 - 521.

surveillance and management, security engineering test and running, education on security consciousness and technology training, security assessment and examination, emergency response etc. This is a lifecycle of holistic information security engineering. After security assessment and examination, a new lifecycle begins. This is a continuously to-and-fro and upward corkscrew security model.

(4) Information security is dynamic

Information technology is developing, while the level of the hacker is also improving. Security strategies, security architecture and security technology should be adjusted dynamically in order to make the security system function furthest. Then the whole security system will be in a dynamic process and keep on renewing and improving.

(5) Information security has multi-levels

Multi-level security technology and approaches should be used to remove security risk.

(6) Security is relative

Security is relative. Absolute security does not exist.

Therefore, information security engineering is complicated system engineering. It involves exploitation, integration, operation, maintenance and management of information system. It is closely linked with web integration, exploitation and application. With the dramatic increase in informatization degree of our country's national defense, government, enterprises and society, the challenge of information system security becomes more and more serious. SSE-CMM is not practical in operation; In addition, the research on information security engineering is not mature in our country. In this case, to modify and improve SSE-CMM and to conduct research on its engineering, practicability under our country's circumstances is of great realistic significance to guide the development of information security engineering in our country.

II. General Research At Home And Abroad

There are two kinds of research thoughts in the history of information security engineering approach development.

One thought is ISSE (Information System Security Engineering), based on the system engineering process approach. The idea of ISSE appears as early as 1993 in the <handbook of information system security engineering > constituted by the state security administration in the U.S.A. ISSE puts emphasis on the application system engineering of information security. Specifically speaking, information system security engineering is to apply the special security technology (communication security technology, computer security technology and internet security technology) to the each stage of the information system lifecycle in order to guarantee the demands for the information system to be satisfied by following the viable security strategies and at the same time to resist the appreciable threats. It is a methodology that demarcates the engineering elements by time-dimension. There should be many requirements running through the whole process, especially the assurance requirement of information security, but ISSE lacks of the special discussion on this issue. Besides, the content of information security is very complicated. One holistic process of information security engineering usually involves many complicated security fields, however, the time process does not show clearly in some fields [1].

The second thought is SSE-CMM (System Security Engineering Capability Maturity Model) based on the process capability maturity model. It roots in CMM, put forward by information security technicians from NSA. It was first published in Oct 1996 and renewed in Apr 1999. This model tries to make information security engineering become a mature measurable advanced subject by taking the process management.

Information security engineering has been studied for over 10 years abroad. The researchers in different countries have put forward various methods. Literature [4] puts forward an example of SLPS (Software Lifecycle Process Standard) based on IEEE/EIA12207,which is a information system security engineering model. Literature [5] discusses the viewpoint of information system security analysis and design based on BPM technology. It combines security risk analysis and organization operation process analysis. Literature [6] analyzes a series of information system security processes about how to define and transfer risks, how to integrate security to target structure and how to deal with the original system limitation when many systems are integrated to a larger one. Literature [7] shows the idea of increasing the systematic structure related to security levels. This idea aims at Web applications and is based on SSE-CMM with 3 levels. Literature [8] advances another method, which regards security as a part of the exploitation of the whole system.

The research on information security engineering theory and approaches in our country has just begins. At present, the research is mainly based on the model SSE-CMM. Literature [9] advances the thought and ways of exploitation and introduces the basic thought and architecture of this model. Literature [10] put forwards the V lifecycle model on the basis of this model. Literature [11] bring forwards the opinion that complicated information system security engineering management can be turned into a strict dependable system by SSE-CMM and demonstrates its structure, property and application. Literature [12] advances information system security lifecycle model, which centers the risk analysis. It is also based on SSE-CMM and aims at the lifecycle of information system.

III. Research Approaches

Since information security is a matter of system engineering based on process, the model SSE-CMM can be regarded as the theoretical basis of the information security engineering management and can be used to guide the specific management tasks in the process of the security engineering implementation. This model is based on the process and dynamically controlled.

III. 1 System Security Engineering Capability Maturity Model

The SSE-CMM has two dimensions, “domain” and “capability.” The domain dimension contains 11 process areas, which cover all major areas of security engineering. They are Administer Security Controls, Assess Impact, Assess Security Risk, Assess Threat, Assess Vulnerability, Build Assurance Argument, Coordinate Security, Monitor Security Posture, Provide Security Input, Specify Security Needs and Verify and Validate Security. The SSE-CMM divides security engineering into three basic areas: risk、engineering and assurance.

Among them, risk process refers to the risk analysis focusing on the system plans to implement security engineering. It analyzes all kinds of elements that probably threat the system, the vulnerability of the system itself and the influence on the system if the threatening elements play a role. Engineering process is a complicated process. According to the result of the risk analysis, some related system demands and applicable laws and policies, the engineering stuff and the clients together identify and define the system security demands. Then they found out the project after considering all the elements, such as cost, quality, technology risk and the difficult degree of use etc. This project is used to guide the exploitation and construction of the security system and test it continuously to guarantee the risk not to reach the unacceptable degree. Assurance process is to test and validate the process of security engineering and the result of the quality and consequently make sure whether the system security is credible. With the incessant implementation of these three processes, the process ability of the engineering stuff grows unceasingly.

SSE-CMM itself is not a security technology model, but it offers the key process areas of information security engineering. It can guide each part of the whole engineering and consequently turn the complicated information system security construction into a strict engineering architecture.

III. 2 Information security engineering model based on SSE-CMM

Just like above description, SSE-CMM is a security framework model. It should combine the practical circumstances to discuss the approaches when implementing security engineering. So a model of information security engineering based on SSE-CMM is produced. It combines the security process put forward by academician Shen Chang-xiang.

Figure 1 demonstrates a holistic periodicity of information security engineering. This is a continuously to-and-fro and upward corkscrew security model. It starts from confirming security target/principle, then passes security risk analysis and other series of process, at last comes to security assessment /examination. Then a new periodicity begins.

(1) Confirm security target and principle

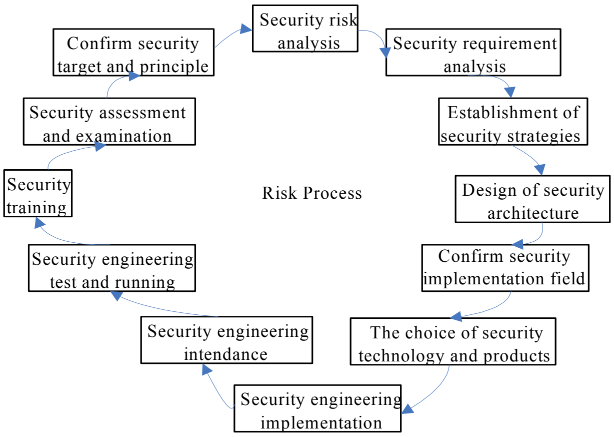
The intended security target and principles of the information system should be confirmed according to the system security requirement and the standards of the country and the same industry as well as the related policies and rules.

(2) Security risk analysis

Security risk analysis is an effective way of assessing information security. According to the confirmed security target and principle, it can focus on the unsafe elements to analyze the security risks that exist in the system, such as the system threats and vulnerability and the risks that they result in. It can assess the intending loss quantity happened to the whole system once the resource get short or is damaged.

There are many ways of doing risk analysis. They can be classified into three types: quantitative risk analysis approaches, qualitative risk analysis approaches and the hybrid risk analysis approaches of the both.

Fig. 1 Model of information security engineering based on SSE-CMM


Confirm security target and principle
Security risk analysis
Security requirement analysis
Establishment of security strategies
Design of security architecture
Confirm security implementation field
The choice of security technology and products
Security engineering implementation
Security engineering intendance
Security engineering test and running
Security training
Security assessment and examination
Risk Process

(3) Security requirement analysis

Security requirement analysis is to investigate the information system on the base of the security risk analysis. The investigation should be all-round, systematic and detailed. Its aim is to ensure the system target, collect the datum and demands for them and make sure the users' requirement. Requirement analysis is a process of further understanding and describing the object system.

(4) Establishment of security strategies

System security strategies should be put forward on the base of the result obtained by analyzing the information system risk. The establishment of them should also be combined with security target and security requirement, besides following the related information security standards and rules. System security strategies are the guidance of the further design of the security system. They are the rules and responsibility that all the departments and stuff in the organization should abide by. They provide a guide framework to guarantee the information system security.

(5) Design of security architecture

Information system security structure is to put the secure elements into the information system structure, and make a description about the relationship among the elements concerned with the fulfillment of security, that is, to describe how the system is organized to meet the security need and make the information system security be an all-around, comprehensive and multi-level holistic security framework.

(6) Confirm security implementation field

The specific implementation field of security strategies should be confirmed.

(7) The choice of security technology and products

Security technology and products should be chosen based on the security architecture. The optional security technology are like these: identity certification technology, digital signature technology, visit accredit management technology, web supervisory technology, technical segregation technology and interdiction technology etc. Security products are firewall, identity certification system, visit control system, VPN channels, and so on.

(8) Security engineering implementation

The core in the period of security engineering implementation is to establish security baseline used in the whole process management according to the property of the information system and security requirement. In the process of implementation, specific technology and management approaches should be adopted based on the different information systems.

(9) Security engineering intendance

Each part of the whole security engineering should be supervised and examined. Such as flow, rate of progress and quality.

(10) Security engineering test and running

Security engineering should be tested and run in order to find out hidden troubles and careless omission of security, and then the engineering quality can be improved.

(11) Security training

All the stuff in the organization should receive the education on the consciousness of security and get the technology training.

(12) Security assessment and examination

Security of information system should be assessed according to the assessment standards and guideline. At the same time, the implementation of information system security strategies should be also examined. The faultiness of requirement analysis should be found out timely in order to improve security strategies.

IV. Conclusion

In the face of hidden trouble and crises of the information era, information system security is not just the simple accumulation of technology and security products. It must be dealt with by means of theories and approaches of information security engineering. However, information security engineering is still faced with a great challenge since the information security engineering standards at home and abroad have just been published. Therefore, the approaches and model of information security engineering as well as the specific guidelines focusing on the different kinds of information system need further research.

References

[1] Shen Chang-xiang, information security engineering introduction (in Chinese), Electronic Industry Press, Jul 2003

[2] Wang Xing-fen, Li Yi-jun, State-of-the-art of information system security engineering: the concept and methodology(in Chinese), journal of hefei university of technology, Vol.26, No.S1, Aug 2003

[3] Shen Chang-xiang, Standardize the construction of information security with the information security engineering theory(in Chinese), Computer world, 2001

[4] Lee Y, Lee J, Lee Z. Integrating software lifecycle process standards with security engineering [J]. Computer & Security, Vol.21, No.4, 2002: 345-355.

[5] Kokolakis S A, Demopoulos A J, Kiountouzis E A. The use of business process modeling in information systems security analysis and design[J]. Information Management & Computer Security, Vol.8, No.3, 2000:107-116.

[6] Bodeau D J. System-of-systems security engineering[A]. Proceedings of 10th Computer Security Applications Conference[C] New York: Institute of Electrical & Electronics Engineers, Inc,1994: 228-235.

[7] Chan M T, Kwok L F. Integrating security design into the software development process for e-commerce system [J]. Information Management & Computer Security, Vol.9, No.3, 2001: 112-122.

[8] Haralambos Mouratidis, Paolo Giorgini, Gordon Manson, Integrating Security and Systems Engineering:Towards the Modelling of Secure Information Systems, Lecture Notes in Computer Science, 2003, 2681:63-78

[9] Li Yi-jun, Yu Yang, Cao Rong-zeng, The developing concept and method of information security engineering based on SSE-CMM(in Chinese), Information journal, Vol.21, No.5, October 2002, 21(5): 573-578

[10] Chen Jian-ming, Gong Yao-wan, Model of information system security engineering based on SSE-CMM (in Chinese), Computer Engineering, Vol.29, No.16, September 2003,29(16): 35-36

[11] Song Ru-shun, Qian Gang, Yu Leng, Information security management and control based on SSE-CMM (in Chinese), Computer Engineering and application, No.12, 2000: 128-129.

[12] Wang Xing-fen, Cui Bao-ling, Li Yi-jun, An risk analysis centric model of information system security engineering(in Chinese), Operations Research and Management Science, Vol.13, No.2, 2004:45-48

[13] Qian Gang, Da Qing-li, Management of info-security engineering based on SSE-CMM model (in Chinese), Journal of southeast university, Vol.32, No.1, Jan 2002

[14] Finne T. Information systems risk management—Key concepts and business processes [J]. Computer & Security, 2000,19:234-242.

[15] Kwok L F, Longley D. Information security management and modeling [J]. Information Management & Computer Security, Vol.7, No.1, 1999:30-39.

[16] Denis Trček, An integral framework for information systems security management, Computers & Security, Vol.22, No.4, 2003: 337-360