2000

A Study of Integrating the Security Engineering Process into the Software Lifecycle Process Standard (IEEE/EIA 12207)

Younghwa Lee
University of Colorado at Boulder, yhlee@unlserve.unl.edu

Zoonky Lee
University of Nebraska at Lincoln, zlee@unlnotes.unl.edu

Choong Kwon Lee
University of Nebraska at Lincoln, cklee@unlserve.unl.edu

A Study of Integrating the Security Engineering Process into the Software Lifecycle Process Standard (IEEE/EIA 12207)

Younghwa Lee, College of Business and Administration, University of Colorado-Boulder
yhlee@unlserve.unl.edu
Zoonky Lee, ChoongKwon Lee, Department of Management, University of Nebraska-Lincoln
zlee@unlnotes.unl.edu, cklee@unlserve.unl.edu

Abstract

In developing an information systems (IS), most organizations have preferred a traditional add-on approach that adds commercial security products after an IS development project is finished. However, a number of recent incidents with regard to IS security indicate that this approach does not guarantee IS security because commercial products are not designed for the specific organizational IS environments. As an alternative solution, previous studies suggested that organizations integrate both the security engineering (SE) process and software development lifecycle (SDLC) process standards. Unfortunately, a few studies tried to suggest the limited integration models. In this paper, as a practical way for the development of secure IS, we suggest two SE process models. First, we develop the generalized SE model that includes all SE activities through the whole SDLC. Secondly, we suggest the process integration model that interweaves SE with IEEE/EIA 12207 through Delphi analysis.

Background

Although today's businesses highly depend on information systems, most organizations still do not consider IS security an important issue (e.g., Straub and Welke, 1998). Further, managers think that the investment in IS security is an overhead with "intangible benefit" (Piper, 1994) and including a SE process into SDLC might cause performance loss, inflexibility, and higher cost, and then they prefer the add-on approach that adds commercial security products after the system development is completed. However, this add-on approach does not guarantee to effectively protect IS, because the commercial security products developed for a general purpose are not designed to meet inherent requirements of each organization which has an inherently unique IS environment (Tettero et al., 1997). Due to this weakness of the add-on approach, many security incidents have repeatedly occurred (e.g., Shimeall and McDermott, 1999).

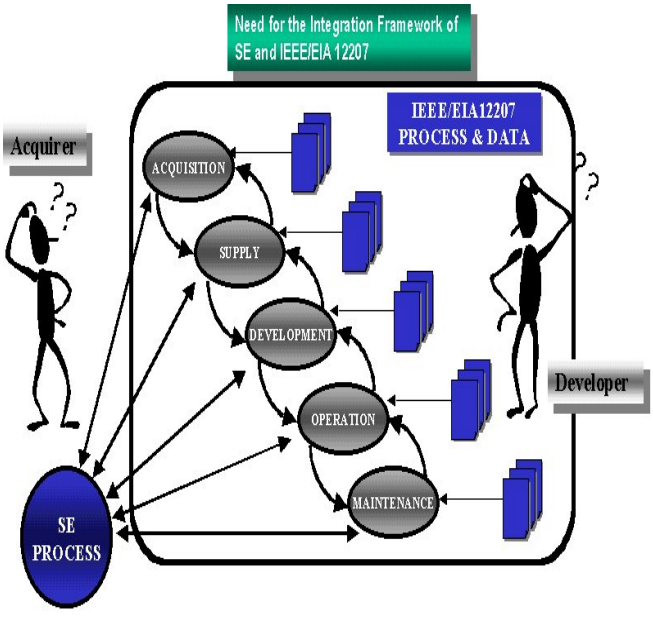
For the solution to developing a more secure system, studies have asserted that SE process be regarded as an important issue from the very beginning of system development projects and further be integrated into the whole processes of general system development (Baskerville, 1993; Booysen and Eloff, 1995; Marshall et al., 1995; Mostert and Solms, 1994). SE process is defined as "a set of activities to gain understanding of the security risks, establish a balanced set of security needs in according to identified risks, transform security needs into security functions, establish assurance in the correctness or effectiveness of security mechanism, determine that operational impacts due to residual security vulnerabilities in a system or its operation is tolerable, and integrate the efforts of all engineering disciplines"(SSECMM 1999:26). Booysen and Eloff (1995) suggested that SE activities be integrated into the initial design of an IS to achieve the better security. Baskerville (1993) also stated that the separation of security function from systems designs cause the unsecured system, because each of security designer and general function designer develops the systems based on its own focus. Mostert and Solms (1994) asserted that add-on approach costs ten times more than the SE approach that integrates SE process into software lifecycle process standard. SE process activities defined by the previous studies are summarized in Table 1.

However, the previous studies have several limitations to be generally applied in the real world. At first, they were not based on the generalized system development process in that they developed under specific application domain or specific theoretical backgrounds. For example, common criteria (CC) come from secure product evaluation, while system security engineering capability maturity model (SSE-CMM) from the evaluation of an organization's security maturity level (SEI 1997). Therefore, their activities differ from each other. Second, they generally did not consider the integration of the SE process into software lifecycle process standard, even though some studies (e.g., Tompkins and Rice, 1986, Marshall et al., 1995) attempted to consider it based on the specific standards (e.g., Mil-Std-2167A). It gives the difficulty to the acquirers because they do not have enough SE knowledge to suggest the exact security requirements and manage and control the project efficiently. Developers also experience a difficulty because they have been involved in IS projects that require a small number of security functions. This problem is shown in Figure 1.

Table. 1 The Previous Researches Dealing With SE process activities

RESEARCH	SE PROCESS ACTIVITIES
TCSEC (1985)	Audit, Trusted Path, System Architecture, System Integrity, Security Testing, Design Spec. and Verification, Covert Channel Analysis, Trusted Facility Mgt, Configuration Mgt, Trusted Recovery, Trusted Distribution, and Documentations
Tompkins & Rice (1986)	Sensitivity Determination, Security Objective, Security Risks Assessment, Security Feasibility Study, Security Requirement Analysis, Security Test Plan Development, Security Specifications Design, Security Test Procedures Development, Security Relevant Code Writing, Documentation, Security Test & Evaluation, Security Test Analysis & Certification Report
Badenhorst & Eloff (1989)	Top Manager's Computer Security Awareness and Support, SE Steering Committee Appointment, Security Policy Establishments, The Scope of Security Definition, Risk Analysis, Technical Security Measures' Installation, Detection, On-going Security Administration, Documentation and Reports, Training, Security Auditing, Change Control
Weiss (1991)	Baseline Architecture Identification, Threat Identification, Threat Analysis and Decomposition, Risk Assessment, Prioritization of Vulnerabilities, Identification of Candidate Safeguards, Safeguard Trade-off Analysis, Security Architecture Selection, Security Architecture Integration and Iteration
Bodeau (1994)	Security Requirement Analysis, Identification and Analysis of Functional Flows, Security Test, Evaluation, and Transition Plan
Marshall et.al (1995)	Security Requirements, Security Model, Security Risk and Vulnerability Analysis, Security Architecture, DTLS, FTLS, Covert Channel Analysis, Security Testing, Documentation, and Certification & Accreditation
Booysen & Eloff (1995)	Sensitivity Analysis, Security Risk Analysis, Security Prototype, Security Requirement Validation, Security Model, Information Flow Analysis, Audit, Design Security Control, Test Safeguards, Security Report, Security Documentation
CC(1996)	Security Audit, Trusted Path, Development, Testing, Vulnerability Assessment, Configuration Management, Lifecycle Support, Guidance Documents, Delivery and Operation
Tettero et al. (1997)	Security Minds, Security Policy, Security Requirement, Threat Analysis, Description of System Environments, Feasibility Analysis, System Specification, Security Framework, Security Component Building, Operation and Change Management
SSE-CMM (1997)	Admin. Sec. Controls, Assess Impact, Assess Security Risk, Assess Threat, Assess Vulnerability, Build Assurance Argument, Coordinate Security, Monitor Security Posture, Provide Security Input, Specify Security Needs, Verify and Validate Security

Figure 1. Problems Related to SE



Therefore, both of them require the general guideline for the development of secure systems.

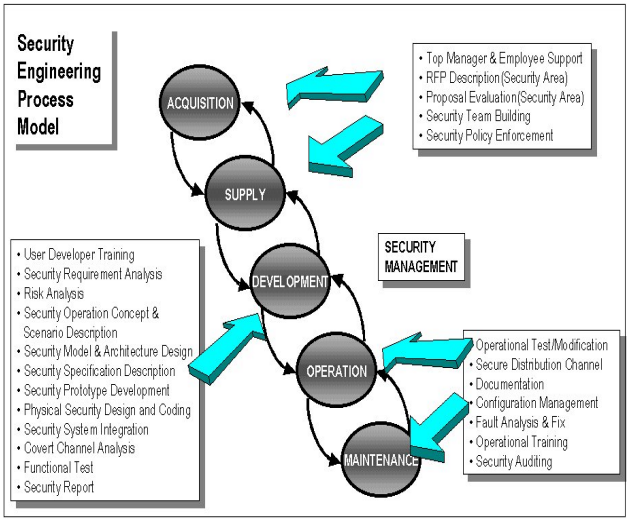
To meet this requirement, in this paper, we address two models of SE process. First, we introduce the generalized SE process model that integrates all of SE activities into the whole processes of SDLC. It is not the new one, but the result of analyzing and regrouping SE activities of previous studies and conducting the interviews with IS experts. Second, based on this generalized model, we suggest the process integration model that incorporates SE process with IEEE/EIA 12207. The model suggests the way to connect SE activities to software lifecycle process and its lifecycle data.

SE Process Model

We first developed the process model consisting of twenty-five activities based on the previous research, and then performed the interview with nine IS experts and asked for the appropriateness of the new model. There were several different opinions about the model. One of

the big issues was about the level of details related to SE process activities. Most interviewees agreed to the detailed classification, while the others wanted to reduce the number of activities. Specially, two experts wanted to reduce SE activities. Security management was pointed out by most of interviewees that consider it an important issue for the flexible communication medium between acquirers and developers during SDLC. They mentioned the building of the special team for SE to support this activity. On the contrary to our expectation, the experts mainly emphasized the managerial issues, such as security management, managerial support, and training. As a result of the interview, we modified the previous model, added four activities, merged two activities, and removed two activities. The newly added activities are managerial support, building security management team, user trainings, and fault analysis and fixing. Security model and architecture design, and security operation concept and scenario description are merged into one, while security objective and contingency planning are removed. Figure 2 shows SE process model, including the feedback mechanism, and Table 2 summarizes SE process activities.

Figure 2. SE Process Model



SE Process Integration Model

Based on SE model, we suggested the process integration model of SE process activities with IEEE/EIA 12207. For the integration, we adopt IEEE/EIA 12207 as a software lifecycle process standard since it has been used as a standard of both industry and military software development projects (IEEE 1998). It defines the role of acquirer, supplier, developer, operator and maintainer during SDLC and gives the guideline of processes and outputs for software development. Lifecycle processes of IEEE/EIA 12207 consist of five primary, eight organizational, and four supporting processes. And its lifecycle data consist of eighty-four items including thirty primary components.

We tried to integrate SE process into IEEE/EIA 12207 in two areas. One is to connect SE process activities to software lifecycle process activities and the other is to interrelate SE process to lifecycle data. The former is important in the view of combining general software development process with SE process, and the latter is important in the view of designating the right place to store outputs of SE process activities. Higginbotham and Maley (1998) suggested the purpose of the integration "by integrating security engineering process into system development, system developers can satisfy the acquirer's concern and the acquirer can satisfy about the quality of security services offered"(p. 321).

Delphi Analysis

To develop a process integration model, we performed two-stage Delphi analysis. Delphi analysis is a useful tool when judgment from experts is inevitable (Rowe et al 1991). We carefully selected the experts who have experiences on secure system development. This analysis was conducted with thirty-three IS experts consisting of five security experts, six system designers, thirteen system developers, and nine project managers. They turned out to have 5.1 years' field experience, and 2.2 times experience of secure system development in average. This analysis was a two-stage iterative process. Before we started the 1st stage analysis, we met and explained the purpose of our research and handed out a questionnaire and a form with several materials to help their understanding (i.e., summary about both SE and IEEE/EIA 12207). The form is for describing problem suggestions about the integration. In the middle of the questionnaire, we asserted the pictures that consist of SE activities, IEEE/EIA 12207's primary process activities and lifecycle data. Each expert then drew the line to show their opinions about the relationship among them, and expressed the appropriateness of connection using three-point Likert-style scales that contain one meaning a 'weak' relationship and three meaning a 'strong' relationship.

The Results of Delphi Analysis

After conducting the first stage, we calculated the weighted average of the measures. We also gathered and analyzed forms from experts. Based on these analyses, we could find three main things. One was to include the supporting and organizational process in this model. The previous questionnaire only included primary processes of IEEE/EIA 12207. Instead of drawing the line between SE activities and primary process activities, twenty-one experts suggested incorporating these two processes with primary process at the form. The other issue was security management. Security experts and project managers showed their strong interest in security management and

Table 2. Security Engineering Activities

PROCESS	PROCESS ACTIVITY	DESCRIPTION
Acquisition & Supply Process	Top manager & Employee Support and Involvement	Continuous support and active involvement on the project. It helps to raise security awareness and knowledge and the streamlined secure system development with responsibility.
	RFP Descriptions	Compose RFP about security function by security managers integrating the inf. of several sources such as security experts.
	Proposal Evaluation	Evaluate proposals in the view of meeting security requirements, economical, and technological feasibility to choose the most appropriate developer
	Security Team Building	Build the specialized security team which mainly takes a responsibility about all SE process activities during SDLC
	Security Policy Enforcement	Define the collections of rules to protect, distribute, and control the important electronic assets which will be physically implemented as security functions
Development Process	User & Developer Training	Perform user training to give information about the objective, and general views on the planned system & developer training to give the exact understanding on the user security requirements
	Security Requirement Analysis	Collect security requirements of the users about the target system and analyze them, adding security managers own security knowledge
	Risk analysis	Identify the possible threats and vulnerabilities that can affect the system's security, analyze an anticipated loss and effects due to accidents, and select appropriate countermeasures
	Security Operation Concepts& Scenario Development	Develop sec. operation concepts that explain how system is implemented to meet sec. requirements well, and develop the scenario that gives the developer tangible information about diverse threats and vulnerability of the system
	Security Model & Security Architecture Development	Analyze secure information flow by grouping objects, specifying their interdependencies, and illustrating the interactions. The top-level in that structure becomes a logical component by system architects, while the bottom-level becomes a physical component to be practically implemented
	Security Spec. Desc.	Describe the specification based on outputs of security design process activity.
	Security Prototype Development	Develop the program that consists of critical function of the completed system for verifying the appropriateness of the design for security requirements.
	Coding	Convert the physical design into programming code
	Covert Channel Anal.	Perform trials for finding secret channel
	System Integration	Integrate the developed security functions with the designated hardware device
	Functional Test	Perform functional, operational, verification, and penetration testing to evaluate initial security requirements are well implemented & worked at the real situation
	Security Report Desc.	Records the findings and results from tests, including security defects, the measures for improving them, and the results from applying the measures.
Operation & Maintenance Process	Secure Distribution Channel Plan	Make a plan to distribute to the users' sites through physical and managerial channels and maintain the continuous reliable channels
	Oper. Test & Modif.	Test the developed system at the real org. environment and find/fix the problems
	Documentation	Develop security related documents including user manual, trusted facility manual, test documentation, design documentation and security module code
	Configuration Management	Conduct configuration management which continuously observes the changes in information systems and promptly modifies the factors of changes
	Fault Analysis & Fix	Find and fix system defects that occur due to unclear procedures, invasion, and design problems.
	Operational Training	Perform the training for users and operators about how to use developed system
	Security Auditing	Perform auditing for identifying sec. policy violations that can happen in the operational processes
Security Management		Manage all of managerial problems occurred during the SDLC, and resolves them through mediating with supplier, system developer, operator and maintainer

allocated it into a number of IEEE/EIA 12207 process activities. This activity has been strongly emphasized on SE studies (e.g., James 1996). The last issue was the documentation. Project managers mainly indicated no existence of the appropriate data items in which SE activities are stored. For example, they did not mark the connection between SE process activities and lifecycle data in acquisition and supply processes and attached a comment about its inappropriateness. They also recommended the addition of four lifecycle data to the last two processes. Based on their suggestions and the analysis result, we developed the initial integration model. After that, we performed the second Delphi analysis. The analysis drew more agreements than the first one. The mean of weighted average increased from 2.34 to 2.51 in the case of the connection between both process activities, and from 2.41 to 2.49 in the case of the connection between process activities and lifecycle data. In addition, the standard deviation of weighted average decreased from 0.34 to 0.27 in the former connection, and from 0.30 to 0.26 in the latter one. However, two augmented issues in the 1st analysis still remained in disagreement (low scores) though their gap becomes narrowed. The distinguished feature of the second analysis was documentation. It mainly came from project managers. After comparing to the suggestion of the first stage that required the addition to several lifecycle data, they recommended that the addition decision of the documents remain as negotiated issues during the contract period. The detailed results of the analysis are shown in Table 3 and Figure 3, 4, and 5. The table shows that the lowest and the highest scored items in 1st and 2nd analysis. The mean and standard deviation value show that the result of 2nd stage has better homogeneity than that of 1st stage.

Table 3. Results of Delphi Analysis (1st and 2nd Analysis)

SE vs. Lifecycle process activities	1st	2nd	SE Activities vs. Lifecycle Data	1st	2nd
Lowest Scores (Below 2.0) of the 1st and 2nd Analysis			**Lowest Scores (Below 2.0) of the 1st and 2nd Analysis**		
Managerial Support-Contract Prep. Update	1.7		Managerial Support-Acquisition Plan	1.6	1.7
Sec. Team Building-Initiation	1.7		RFP Prep.-Acquisition Plan	1.8	1.9
Sec. Policy Enforcement-Initialization	1.9	2.0	RFP Prep.-Acceptance Strategy & Cond. Records	1.9	
Sec. Policy Enf.-Contract Prep.& Update	1.5	1.8	Sec. Policy Enforcement-Acquisition Plan	1.8	1.8
Sec. Mgt.- Review & Evaluation	1.9		User & Developer Training-Develop. Process Plan	2.0	
Risk Analysis-Management		2.0			
Sec. Testing-Verification		2.0			
Highest Scores (Upper 2.8) of the 1st and 2nd Analysis			**Highest Scores (Upper 2.8) of the 1st and 2nd Analysis**		
Sec. Module Coding-S/W Coding & Testing	2.9	2.9	Sec. Oper. Con. & Sce. Desc.-Con. of Oper. Desc.		2.8
Sec. System Integration-S/W Integration	2.8	2.9	Sec. Model & Arch. Design-S/W Arch. Desc.	2.8	2.8
Sec. Testing-S/W Coding & Testing	2.8		Sec. Module Coding-Source & Executable Obj. Code Records		2.8
Sec. Testing (Operational)-Validation	2.8		Sec. Sys. Integration-S/W Integration Plan	2.9	2.9
Sec. Req. Anal.-System Req. Anal.		2.9	Documentation-User Documentation Desc.		2.8
Sec. Req. Anal.-S/W Req. Anal.		2.9	Sec. Audit-Audit Agenda Record & Proc.	2.8	2.9
Secure Distribution Channel Plan-Infra.		2.9			
Documentation-Documentation		2.9			
Configuration Mgt.-Configuration Mgt.		2.9			
Operational Training-Training		3.0			
Sec. Mgt.-Mgt.		2.9			
Total Average Mean	**2.34**	**2.51**		**2.41**	**2.49**
Standard Dev.	**0.34**	**0.27**		**0.30**	**0.26**

Acquisition and Supply Process

As shown in Figure 3, although most of components in these processes incorporated with one another, there existed three problems. One is security policy. Security policy was not strongly connected with the lifecycle process activities and data of IEEE/EIA 12207. Another is security management. We connected it to too many activities of IEEE/EIA 12207 processes (i.e., supplier monitoring, acceptance and completions). The other was that three SE process activities were allocated into acquisition plan, though they are not well matched. These problems are remained as negotiation subjects of the contract for secure system development.

Figure 3 Process Integration Model- Acquisition and Supply Process

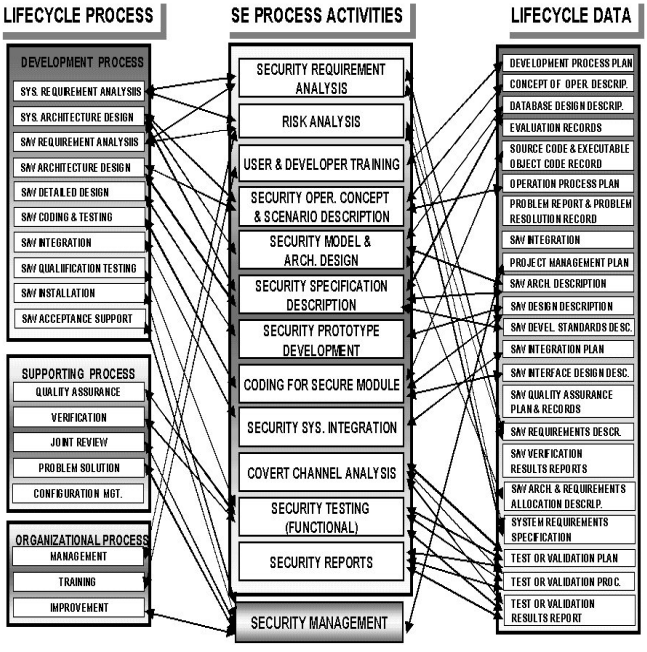
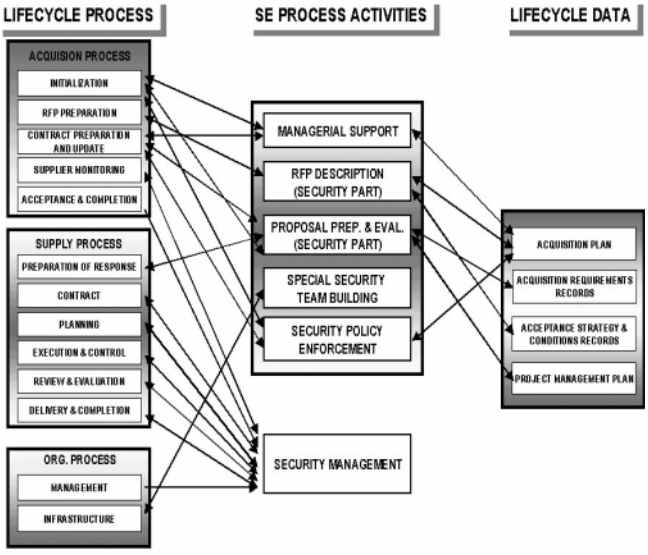


Figure 4 Process Integration Model- Development Process



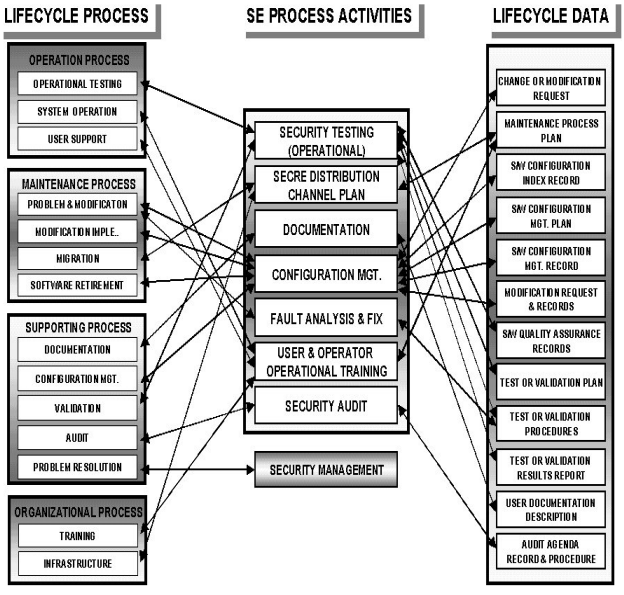
Development Process

In this process, while most components are well matched with one another, there were some components that need to be integrated with supporting and organizational process. For example, functional test was interconnected with quality assurance and verification activities, and security reports are combined with joint review, problem resolution, and improvement. Risk analysis was another issue. We connected it with system/software requirement analysis and management, and with the concept of operations and system/software requirement description, but it did not cover all of the scope of risk analysis. As an alternative, we suggest that risk analysis perform its functions with other process activities, such as management and configuration management.

Operation and Management Process

In these processes, with the primary lifecycle process activity, supporting and organizational process activities assist SE process. For example, the security documents are integrated with documentation activity in supporting process, while secure distribution channel are with infrastructure in organizational process. We incorporated four lifecycle data that are not primary data into this model. For instance, modification request and records, test or validation plan, procedures and results reports, and audit agenda record and procedure.

Figure 5 Process Integration Model- Operation and Management Process



Limitations

Although we developed the process improvement models for secure system development, they have several limitations addressed. First, the model was not yet to be applied to the real situation. Although we used Delphi analysis to preserve the objectiveness of the models, they could not prove their effectiveness in practice. Therefore, we need to perform the case study for applying these models to software development projects. Second, it does not include the tailoring guide that shows the

guideline how to tailor the model based on the size, security requirement levels, budget or periods of the project, and each industrial characteristics. And the last since we used the simple weighted average to compute the appropriateness of each mapping scheme, we could not reflect the different viewpoint of each party of Delphi analysis into the model. For example, security engineers gives high points to managerial side SE activities, while system engineers gives to the design and implementation side activities. These issues are remained as future elaboration subjects.

Conclusion

In this paper, we addressed the SE model and process integration model with IEEE/EIA 12207. We suggested a SE model that consists of twenty-five SE process activities identified by the previous researches and interviews. Also we derived the process integration model that interrelates SE process activities to IEEE/EIA 12207 based on Delphi analysis. We expect our models to contribute to showing how SE process activities can be incorporated into software lifecycle process, and providing efficient and effective process enhancement methods for the development of a secure system

Reference

Badenhorst, K.P., and Eloff, J.H.P. "Framework of a Methodology for the Lifecycle of Computer Security in an Organization," *Computer & Security* (8), 1989, pp.432-442.

Baskerville, R. "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Computing Surveys* (25:4), 1993, pp. 375-414.

Booysen, H.A.S., and Eloff, J.H.P. "A Methodology for the Development of Secure Application Systems," Proc. of IFIP Information Security, 1995, pp.255-269.

CCEB, Common Criteria for Information Technology Security Evaluation, May, 1998.

DoD, Trusted Computer System Evaluation Criteria, DoD-Std-5200.28, Dec. 1985.

Higginbotham, M.D., and Maley, J.G. "Integrating Information Security Engineering with System Engineering with System Engineering Tools," 7th IEEE Int'l Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1998, pp. 320-326.

IEEE, IEEE/EIA 12207- Industry Implementation of International Standard ISO/IEC 12207, March 1998.

Marshall D. A., Jajodia, S, and Podell, H. J. Information Security-Chap. 14-Security Engineering, IEEE Computer Society Press, 1995, pp.330-349.

Mostert, D.N.J., and Solms, S.H. " A Methodology to Include Computer Security, Safety and Resilience Requirement as Part of the User Requirement," *Computers & Security* (13), 1994, pp. 349-364.

Piper, F. "Management of Security," EDPAA Annual Conference, 1994.

Shimeall, T. J. and McDermott, J. J. "Software Security in an Internet World: An Executive Summary," *IEEE Software*, July 1999, pp.58-62.

SSECMM projects, Systems Security Engineering Capability Maturity Model-ver 2.0, January 1999.

Straub, D. W. and Welke, R. J. “Coping With Systems Risk: Security Planning Models for Management Decision Making”, *MIS Quarterly* (22:4), 1998, pp. 441-465.

Tettero, O., Out, D.J., Franken, H.M., and Schot, J. "Information Security Embedded in the Design of Telematics Systems," *Computers & Security* (16:2), 1997, pp.145-164.

Tompkins, F.G., and Rice, R. "Integrating Security Activities into the Software Development Lifecycle and the Software Quality Assurance Process," *Computer & Security* (5), 1986, pp.218-242.

Weiss, J. "A System Security Engineering Process," Proc. of 14th National Computer Security Conference, 1991, pp. 572-581.