Title: A Study on Security Level Management Model for Information System

by

Tai-hoon Kim

Submitted in fulfilment of the

Requirements for the Degree of

Doctor of Philosophy

University of Tasmania

March 25, 2011

STATEMENT OF ORIGINALITY

This thesis contains no material which has been accepted for a degree or diploma by the University or any other institution, except by way of background information and duly acknowledged in the thesis. To the best of my knowledge and belief, this thesis contains no material previously published or written by another person except where due acknowledgement is made in the text of the thesis, nor does the thesis contain any material that infringes copyright.

Tai-hoon Kim
March 25, 2011

AUTHORITY OF ACCESS

This thesis may be made available for loan. Copying of any part of this thesis is prohibited for two years from the date this statement was signed; after that time limited copying is permitted in accordance with the Copyright Act 1968.

ABSTRACT

The attempts to protect information and Information System (IS) from the threats are progressing variously and systematically, and the necessity to build security countermeasures by considering the characteristics of IS is gathering strength. In fact, to satisfy the proposition of information security, we don't have to invest excessive budget.

Needless to say, it is important to protect information and IS, but it is not desirable to build uniform security countermeasures regardless of degree of importance. Depending on the purpose of building or operation, IS may have different degree of importance, meaning an IS may have higher degree of importance than other IS.

Systems in same office can even have different degree of importance. In other words, some systems should be protected from the attack, even though some systems can be compromised from the same attack.

In agreement with the degree of importance of IS, the strength of security countermeasure should be changed. For important systems, stronger security countermeasures should be selected, and stronger verification processes should be executed properly.

As we can reduce unnecessary budget for IS which has a lower degree of importance, we can increase investment to IS which has higher degree of importance with the budget saved from other IS.

Therefore, the most important factor is the decision of degree of importance of IS. From now on, this degree of importance will be called required security level or security level briefly. Depending on the selected security level, strength of security countermeasures should be decided. Security countermeasures can be formed after deciding the security level.

In this thesis, after analysing previous research results, the author proposes some essential elements for security level definition and management of IS. After classifying, proper level was granted to threats and assets, and weights were assigned to each level. By summating these weights, the security level of an IS can be decided.

After deciding the security level, basic technical and non-technical requirements for security level management are proposed in detail. Some items needed to ensure basic security state of IS are listed in this requirements.

After this, level requirements to ensure security level required for each IS are proposed in detail. These level requirements should be applied differently for both technical and non-technical parts. Level requirements are designed by using step-model for technical areas, and continuous-model for non-technical areas.

DEDICATION

I dedicate this thesis to Loving God.

Your endless love and grace allowed me to endure all obstacles.
Thank you for your companionship in moments of uncertainty, anxiety, and conflict
during all my long journeys.

Table of Contents

LIST OF TABLES

Number *Page*

LIST OF FIGURES

Number *Page*

1. INTRODUCTION

1.1 BACKGROUND AND MOTIVATION

Information system (IS) and the information processed by IS are very important to maintain all functions and keep the duty of organization. The problems derived from unauthorized disclosure, modification, and destruction of important information or compromise of IS should be considered very carefully because these can be connected to economical loss or the collapse of organizations.

IS carries out a critical role in the aspects of promptitude and exactitude, and most organizations rely on IS to sustain their existence. Therefore, in a competitive environment, a fatal error or compromise of IS can lead to a dangerous situation. To avoid this, most organizations invest a great amount of money and effort in security areas to protect their IS.

The most common investment in IT security is buying and installing of security systems made by others. Security systems are a type of system designed to perform security functions. This kind of investment is a very simple and relatively easy method. If the owners of IS have more budget, they can buy and install more products as much as they want. This behavior is based on the concept 'the more they install security products, the more IS can be secure.' Firewall systems, IDS (Intrusion Detection Systems), and anti-virus systems are representative security products. Installation and operation of these products are very useful if IS contains many legacy systems.

In these days, because security functions like as intrusion detection or prevention are embedded into general IT products, the investment style for security is changing from former days. In other words, by purchasing and installing some products which contain security functions, indirect investment for security are going on generally. However the establishment of security countermeasure by using security products takes a major portion of the investment [1-5].

The weak point of security countermeasure materialized technically by using security functions is that it is very difficult to manage this countermeasure as the newest one. Trials for incapacitation of IS or depredation of information are always in existence and on the increase.

The keeping of security functions made by security products as a newest one is a very difficult decision because this requires additional investments. For example, the IDS designed to work in 10Mbps network environments may not protect 100Mbps network improved by using optical cable. In this case, to protect improved environments, new products should be bought and installed. To do like this, additional investments are needed.

Fortunately, this kind of investment can be easily decided if the IS is very important. Owners will invest additionally to overcome technical problems. Unfortunately, even though they improve the security countermeasures to protect IS by using some products containing security functions, security accidents will not be reduced under regular level.

To find the reason there were many researches, and most research-results pointed out that many security functions were not generated or managed properly. For example, many security accidents are originated from mis-configuration of IS or lack of update of important components. These are the problems not included in the information system itself, but arose from compound components like operation policy, culture, operator's mind, and work procedure of organization.

Therefore, the security concept for IS was expanded from physical aspect to manage mental aspect. The research for overall processes which can operate and manage various security countermeasures continuously is getting persuasive power.

To cope with the new security problems occurring in every second, it is not a good idea to buy and install security products. This is because much time is needed to make decision for buying products, and the life-cycle of products is not long.

It is more important to build strategies and procedures can be used when a new threat is detected. By following these strategies and procedures, operators can manage IS optimally and encounter to the threat systematically. Since then implementation of security countermeasures and management systems were merged to be used together [6-7].

Here related works for protecting an IS safely from attacks are summarized.

1.2 RELATED WORKS

The concept of information system can be confused because the term 'system' is able to be defined in many different ways. This thesis used the concept of information system that "Information system is an aggregate of humans, procedures, and resources that gather, process, and transfer information for organization." [8][22]

Therefore, not only physical configuration consists of individual products, all sorts of policies, laws and procedures for operating and managing physical components but also human operators who operate system practically should be included in the systems.

When an organization sets up a special goal and wants to achieve this goal by using an IS, the organization should configure a trustable IS according to the importance of its goal. Security level management concept considering whole scope of IS can guarantee the construction and operation of proper security countermeasures.

As an IS can be present as various forms in real environments, it is very critical to define the parts that should be managed by security level management program. As well as this general IS are too big to be managed by integrated style, after classifying security level management activities into some parts, requirements needed for each part should be derived and applied.

Security level management for IS will be accomplished by following 2 steps. The first step is a verification if security requirements needed for IS are truly implemented. Second step is a confirmation if the implementation of security requirements can meet the security level needed for IS. This concept is the same as ISO/IEC 15504 (SPICE, Software Process Improvement Capability determination) and ISO/IEC 21827 (SSE-CMM, System Security Engineering-Capability Maturity Model).

1.2.1 SECURITY EVALUATION FOR IT PRODUCTS

Basically an IS consists of various IT products and their combination. So the security level of IS is seriously affected directly by the security level of each product included in the IS. To make the whole IS secure, security level of all products included in IS should be checked.

Security evaluation of IT products was enforced for a long time, and each country has their own security evaluation systems and criteria commensurate with their environments. By using these systems and criteria, each country evaluates and certificates the security and trust of IT products, and opens evaluation results to the public for free use.

The fact that the security evaluation results of IT products may affect the security level management of IS cannot be ignored. So the evaluation results should be used fully to manage security level of IS effectively.

The method evaluating security by checking the existence and nonexistence of security functions was used for the TCSEC (Trusted Computer Security Evaluation Criteria) [22-23].

The TCSEC is a United States Government Department of Defense (DoD) standard 5200.28-STD that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. The TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information.

The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications. Initially issued by the National Computer Security Center (NCSC) an arm of the National Security Agency in 1983 and then updated in 1985, TCSEC was replaced with the development of the Common Criteria international standard originally published in 2005.

The TCSEC defines four divisions: D, C, B and A where division A has the highest security. Each division represents a significant difference in the trust an individual or organization can place on the evaluated system. Additionally divisions C, B and A are broken into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and A1.

Next Table 1 shows the requirements of the immediately prior division or class.

Table 1 Security Requirements of TCSEC

Class	Division	Description
D (Minimal Protection)		- Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.
C (Discretionary Protection)	C1 (Discretionary Security Protection)	- separation of users and data - DAC capable of enforcing access limitations on an individual basis
	C2 (Controlled Access Protection)	- more finely grained DAC - individual accountability through login procedures - audit trails - resource isolation
B	B1	- informal statement of the security policy model

(Mandatory Protection)	(Labeled Security Protection)	data sensitivity labels - MAC over select subjects and objects - label exportation capabilities - all discovered flaws must be removed or otherwise mitigated
	B2 (Structured Protection)	- clearly defined and documented formal security policy model - discretionary and mandatory access control enforcement be extended to all subjects and objects - covert storage channels are analyzed for occurrence and bandwidth - carefully structured into protection-critical and non-protection-critical elements - design and implementation enable more comprehensive testing and review - authentication mechanisms are strengthened - trusted facility management is provided administrator and operator segregation - strict configuration management controls are imposed
	B3 (Security Domains)	- satisfies reference monitor requirements - structured to exclude code not essential to security policy enforcement - significant system engineering directed toward minimizing complexity - a security administrator is supported - audit security-relevant events - automated imminent intrusion detection, notification, and response - trusted system recovery procedures - covert timing channels are analyzed for occurrence and bandwidth
A (Verified Protection)	A1 (Verified Design)	- functionally identical to B3 formal design and verification techniques including a formal top-level specification formal management and distribution procedures

In May 1990, France, Germany, the Netherlands and the United Kingdom published the Information Technology Security Evaluation Criteria (ITSEC) based on existing work in their respective countries [23-24]. Following extensive international review, Version 1.2

was subsequently published in June 1991 by the Commission of the European Communities for operational use within evaluation and certification schemes.

The ITSEC is a structured set of criteria for evaluating computer security within products and systems. The product or system being evaluated, called the target of evaluation, is subjected to a detailed examination of its security features culminating in comprehensive and informed functional and penetration testing.

The degree of examination depends upon the level of confidence desired in the target. To provide different levels of confidence, the ITSEC defines evaluation levels, denoted E0 through E6. Higher evaluation levels involve more extensive examination and testing of the target.

Unlike the earlier criteria, notably the TCSEC developed by the US defense establishment, the ITSEC did not require evaluated targets to contain specific technical features in order to achieve a particular assurance level. For example, an ITSEC target might provide authentication or integrity features without providing confidentiality or availability. A given target's security features were documented in a Security Target document, whose contents had to be evaluated and approved before the target itself was evaluated. Each ITSEC evaluation was based exclusively on verifying the security features identified in the Security Target.

Since the launch of the ITSEC in 1990, a number of other European countries have agreed to recognize the validity of ITSEC evaluations.

The ITSEC has been largely replaced by Common Criteria, which provides similarly-defined evaluation levels and implements the target of evaluation concept and the Security Target document [22-24].

The Common Criteria (CC) is an international standard (ISO/IEC 15408) for computer security. Unlike standards such as FIPS 140, Common Criteria does not provide a list of product security requirements or features that products must contain. Instead, it describes a framework in which computer system users can specify their security requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.

CC is composed of 3 parts. Detail specification of security functions is included in part 2, so the user of developer can use or recommend these functions [1-3]. When the security evaluation with CC and Common Evaluation Methodology (CEM, ISO/IEC 18045) is going on, security functions requested or certificated by users should be included. This is because there are some choices selected by users.

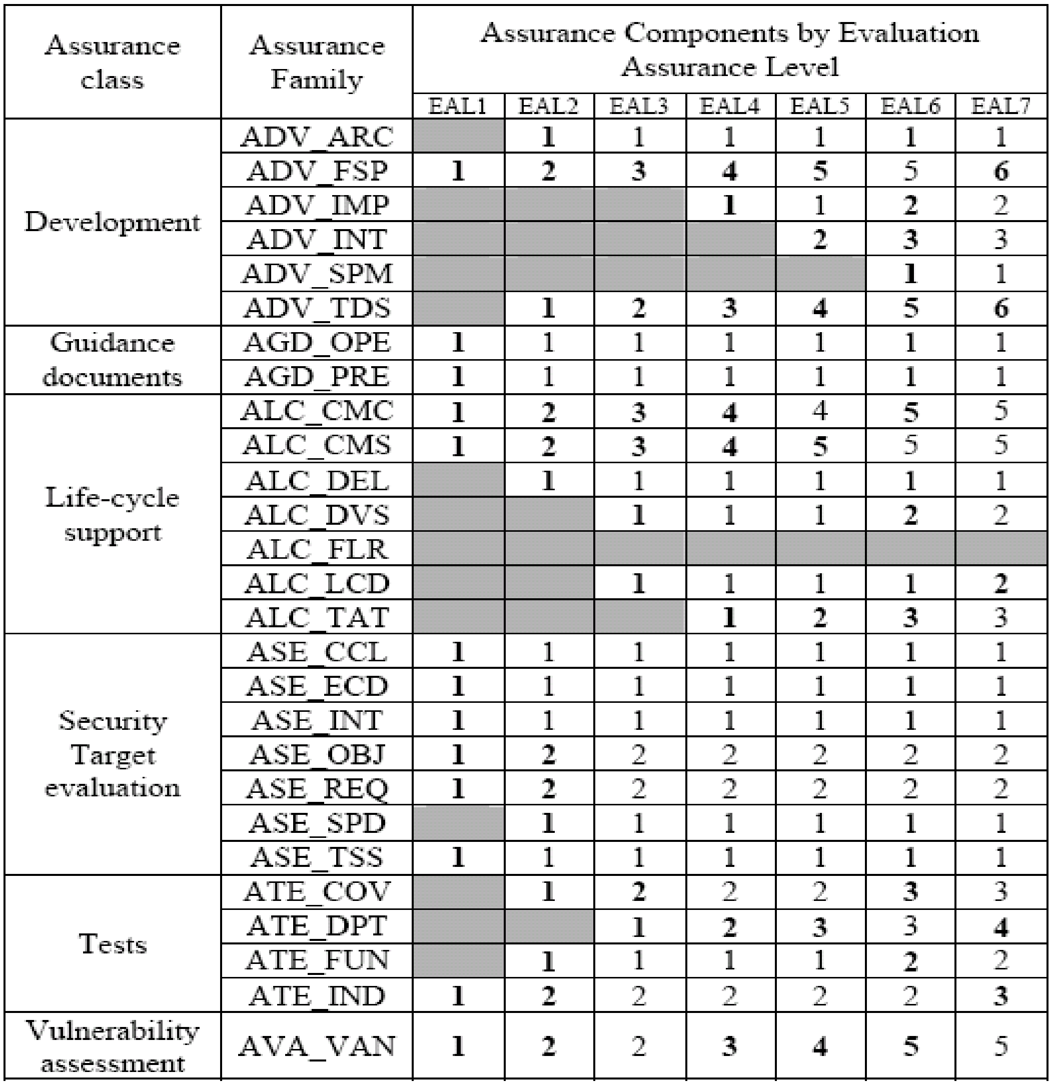
Important thing is that all security functions requested by users should be selected as the target of evaluation. After checking the implementation of security functions, evaluators should validate if these functions are enough to satisfy the level requested by IS.

The evaluation processes by using CC and CEM may satisfy these two considerations, but it cannot be sure. This is because the evaluation with CC and CEM focuses on not the implementation of security functions but level requirements. In other words, CC and CEM focus on the quality of implemented security functions not the existence of necessary security functions.

Evaluation Assurance Level (EAL) is recognized as security evaluation results of IT products. However there is a problem. Sometimes evaluation target is not the security functions requested by users but the functions implemented by developer. Therefore, if necessary security functions are not included in evaluation targets, this evaluation result cannot be used valuably.

Next Table 2 depicts EAL and requirements specified in CC.

Table 2. Evaluation Assurance Level Summary



Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

It is not good idea to try to satisfy security level of IS by only using IT products. By increasing some investments for IT products, organizations will get some effects, but this is not enough. So organizations should prepare and operate systematic and manageable rules to complete insufficiencies.

For example, even though security functions included in IT products are not sufficient, operators who have enough knowledge and capability can compensate this weakness.

The basic concept of the evaluation of security functions in IS is very similar to that of security level management of IS. The concept that first is the checking of the existence and nonexistence of security functions and second is the validation of security level management is the same as that of security level management.

1.2.2 CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

The CMVP was established by the U.S. National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of the Government of Canada in July 1995.

The Cryptographic Module Validation Program (CMVP) is a joint American and Canadian security accreditation program for cryptographic modules. The program is available to any vendors who seek to have their products certified for use by the U.S. Government and regulated industries (such as financial and health-care institutions) that collect, store, transfer, share and disseminate "sensitive, but not classified" information.

All of the tests under the CMVP are handled by third-party laboratories that are accredited as Cryptographic Module Testing Laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). Product certifications under the CMVP are performed in accordance with the requirements of FIPS 140-2.

NVLAP accredited Cryptographic Modules Testing (CMT) laboratories perform validation testing of cryptographic modules. Cryptographic modules are tested against requirements found in FIPS PUB 140-2, Security Requirements for Cryptographic Modules.

Security requirements cover 11 areas related to the design and implementation of a cryptographic module Within most areas, a cryptographic module receives a security level rating (1-4, from lowest to highest), depending on what requirements are met. For other areas that do not provide for different levels of security, a cryptographic module receives a rating that reflects fulfilment of all of the requirements for that area.

An overall rating is issued for the cryptographic module, which indicates (1) the minimum of the independent ratings received in the areas with levels, and (2) fulfilment of all the requirements in the other areas.

On a vendor's validation certificate, individual ratings are listed, as well as the overall rating. It is important for vendors and users of cryptographic modules to realize that the overall rating of a cryptographic module is not necessarily the most important rating. The rating of an individual area may be more important than the overall rating, depending on the environment in which the cryptographic module will be implemented (this includes understanding what risks the cryptographic module is intended to address) [25-26].

FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.

o Level 1 : The lowest which imposes very limited requirements. Loosely, all components must be "production-grade" and various egregious kinds of insecurity must be absent.

o Level 2 : Adds requirements for physical tamper-evidence and role-based authentication.

o Level 3 : Adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.

o Level 4 : This level makes the physical security requirements more stringent, and requires robustness against environmental attacks.

For Levels 2 and higher, the operating platform upon which the validation is applicable is also listed. Vendors do not always maintain their baseline validations.

1.2.3 DEVELOPING PROCESS

It is not proper to discuss security level management after constructing an IS because an IS is a complex consists of many components. A vulnerability included in a component can be a security hole of an IS, and it is common that vulnerabilities are implicated in the products.

Even though a research to observe the development process and make up for insufficiency by applying software engineering is going on, this research was derived from the attempt to make more complete software by reducing the errors occurred when programmers wrote the codes.

However the purpose of this research is not to guarantee the integrity and completeness of software itself but to reduce the unnecessary budget and prevent the possibility of careless errors by controlling the whole development processes. All the researches were merged into CMMI (Capability Maturity Model Integration) and ISO/IEC 15504 (SPICE, Software Process Improvement Capability determination) [27-28].

The reason why the research related to the software area is going on actively is because the software development is more difficult than other things and software has a very special characteristic, "intangible."

Developers have some difficulties when they develop a software because the substantials of software may be not visible. These difficulties are connected to users' hardships because they cannot predict where and when the flaws will be found. To overcome these problems, process improvement tools such as CMMI and SPICE were developed.

SEI (Software Engineering Institute) already developed and distributed various CMM-base models like SW-CMM (Capability Maturity Model for Software), SE-CMM

(The System Engineering Capability Model), and IPD-CMM (The Integrated Product Development Capability Maturity Model).

CMMI is the successor of the CMM. In 2002 version 1.1 of the CMMI was released: v1.2 followed in August 2006. The goal of the CMMI project is to improve usability of maturity models for software engineering and other disciplines, by integrating many different models into one framework. It was created by members of industry, government and the SEI. The main sponsors included the Office of the Secretary of Defense (OSD) and the National Defense Industrial Association (NDIA) Systems Engineering Committee [29-30].

The CMMI comes with two different representations - staged and continuous. The staged model, which groups process areas into 5 maturity levels, was also used in the ancestor software development CMM, and is the representation used to achieve a "CMMI Level Rating" from a SCAMPI (Standard CMMI Appraisal Method for Process Improvement) appraisal. The continuous representation, which was used in the ancestor systems engineering CMM, defines capability levels within each profile. The differences in the representations are solely organizational; the content is equivalent.

The CMMI uses a common structure to describe each of the 22 process areas (PAs). A process area has 1 to 4 goals, and each goal is comprised of practices. Within the 22 PAs these are called specific goals and practices, as they describe activities that are specific to a single PA. There is one additional set of goals and practices that apply in common across all of the PAs; these are called generic goals and practices.

Next [Table 3] represents the model types of CMMI.

Table 3 Model Types of CMMI

Classification	Continuous model presentation	Staged model presentation

Process Area	Grouping by Capability Level	Grouping by Maturity Level
Similar CMM model	SE-CMM	SW-CMM
Maturity	0 ~ 5 Level	1 ~ 5 Level

The CMMI rated maturity as 5 or 6 level, and this rating is similar to those of SPICE.

A working group was formed in 1993 to draft the international standard SPICE. SPICE initially stood for "Software Process Improvement and Capability Evaluation", but the French concerns over the meaning of the last word meant that SPICE now means "Software Process Improvement and Capability Determination".

Even though the formal ISO standards number, ISO 15504, is now the correct reference, SPICE is still used for the user group of the standard, and the title for the annual conference. The first SPICE was held in Limerick, Ireland in 2000, "SPICE 2003" was hosted by ESA in Netherlands, "SPICE 2004" was hosted in Portugal, "SPICE 2005" was hosted in Austria, and "SPICE 2006" was hosted in Luxembourg.

The first versions of the standard were focused exclusively on software development processes. This was expanded to cover all related processes in a software business, for example, project management, configuration management, quality assurance, and so on. The list of processes covered, grew to cover six business areas such as organizational, management, engineering, acquisition supply, support, and operations.

In a major revision to the draft standard in 2004, the process reference model was removed and is now related to the ISO 12207 (Software Life-cycle Processes). The issued standard now specifies the measurement framework and can use different process reference models.

There are five general and industry models in use [31-32].

o Level 0: Incomplete, The process is not implemented or fails to achieve its purpose

o Level 1: Performed, The process is implemented and achieves its process purpose

o Level 2: Managed, The process is managed and work products are established, controlled and maintained.

o Level 3: Established, A defined process is used a standard process.

o Level 4: Predictable, The process is enacted consistently within defined limits.

o Level 5: Optimizing, The process is continuously improved to meet relevant current and projected business goals

It is a pity that CMMI and SPICE do not mention the security-related contents independently. So organizations should decide how they will manage security problems which can be included during the development processes of IT products or IS.

In a general way, for the evaluation with CC and CEM, all proofs related to development processes were documented and submitted to be checked. By evaluating these deliverables, evaluator can guess the development processes. Alternately, evaluators are used to visiting the development site and interviewing developers or engineers.

However to increase the trust about development processes and get valid conclusion, organizations can use the international standard ISO/IEC 21827, SSE-CMM (System Security Engineering-Capability Maturity Model) [9].

The SSE-CMM describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The model is intended to be used as a:

o Tool for engineering organizations to evaluate security engineering practices and define improvements to them.

o Standard mechanism for customers to evaluate a provider's security engineering capability.

o Basis for security engineering evaluation organization (e.g., system certifiers and product evaluators) to establish organization capability-based confidences (as an ingredient to system or project security assurance).

The SSE-CMM addresses security engineering activities that span the entire trusted product or secure system life cycle, including concept definition, requirements analysis, design, development, integration, installation, operations, maintenance, and decommissioning.

The SSE-CMM applies secure product developers, secure system developers and integrators, and organizations that provide security services and security engineering. The SSE-CMM applies to all types and sizes of security engineering organizations, such a commercial, government, and academic.

1.2.4 Information Security Management Systems

After it was proven that the security countermeasures implemented by only technical materials could not encounter the rapid change of environments properly, researches about the comprehensive process for managing and operating various security countermeasures started to gain popularity.

To properly encounter the new security problems occurring in every short time, systematic strategies and procedures were requested. These are included in ISO/IEC 17799 (Information Technology - Code of Practice for Information Security Management) and ISMS (Information Security Management System) [33].

BS 7799 Part 1 was a standard originally published as BS 7799 by the British Standards Institute (BSI) in 1995. It was written by the United Kingdom Government's Department of Trade and Industry (DTI), and after several revisions, was eventually adopted by ISO as ISO/IEC 17799, "Information Technology - Code of practice for information security management" in 2000. ISO 17799 was most recently revised in June 2005 and is expected to be renamed ISO/IEC 27002 during 2007.

The second part to BS7799 was first published by BSI in 1999, known as BS 7799 Part 2, titled "Information Security Management Systems - Specification with guidance for use." BS 7799-2 focused on how to implement an Information security management system (ISMS), referring to the information security management structure and controls identified in ISO 17799. The 2002 version of BS 7799-2 introduced the Plan-Do-Check-Act (PDCA), aligning it with quality standards such as ISO 9000. BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005. BS7799 Part 3 was published in 2005, covering risk analysis and management. It aligns with ISO 27001.

An Information Security Management System (ISMS) is, as the name suggests, a system of management concerned with information security. The idiom arises primarily out of ISO/IEC 17799, a code of practice for information security management published by the International Organization for Standardization in 2000 [34].

The best known ISMS is ISO/IEC 27001, published by the ISO, complementary to ISO/IEC 17799 (developed from BS 7799-1). A system for certification against BS-7799-2:2002 is well established.

ISM3 (pronounced ISM-cubed, Information Security Management Maturity Model) is the only other ISMS that is accreditable. ISM3 was developed from ITIL (Information Technology Infrastructure Library), ISO 9001, CMM and ISO 27001 and Information Governance concepts. ISM3 can be used as a template to make ISO 9001 compliant information security management systems. While ISO27001 is controls based, ISM3 is process based [35].

Using SSE-CMM own words, SSE-CMM is "A tool for engineering organizations to evaluate their security engineering practices, a method by which security engineering evaluation organizations can establish confidence in the organizational capability; A standard mechanism for customers to evaluate a provider's security engineering capability", while ISM3 is a standard for security management (how to achieve the organization's mission despite of errors, attacks and accidents with a given budget). They do not have the same subject matter.

1.3 CHALLENGING ISSUES

Combination of the security countermeasures and management systems is a good solution but is not perfect. Many vulnerabilities are included in IS as ever. These vulnerabilities can be found from either the sub-systems or the process for combination of sub-systems into whole systems.

Even though security countermeasures are designed and managed well, these vulnerabilities included in somewhere can be the cause of compromise of IS.

A new method that considers security from the initial concept design step was proposed to reduce potential vulnerabilities. By applying this method, we can derive and append security requirements when developing IS. By implementing these security requirements into development processes, we can complement security-related materials in the whole life-cycle of IS [8-9].

From related research results, this new method considering security requirements from the initial step of development process is better than the other method used considering security after finishing development process. In the aspect of economics, new method can reduce budget.

The attempts to protect information and IS from the threats are progressing variously and systematically, and the necessity to build security countermeasures by considering the characteristics of IS is gathering strength. In fact, to satisfy the proposition of information security, we don't have to invest excessive budget.

Needless to say, it is important to protect information and IS, but it is not desirable to build uniform security countermeasures regardless of degree of importance. Depending on the purpose of building or operation, IS may have different degree of importance, meaning an IS may have higher degree of importance than other IS.

Systems in same office can even have different degree of importance. In other words, some systems should be protected from the attack, even though some systems can be compromised from the same attack.

In agreement with the degree of importance of IS, the strength of security countermeasure should be changed. For important systems, stronger security countermeasures should be selected, and stronger verification processes should be executed properly.

As we can reduce unnecessary budget for IS which has a lower degree of importance, we can increase investment to IS which has higher degree of importance with the budget saved from other IS.

Therefore, the most important factor is the decision of degree of importance of IS. From now on, this degree of importance will be called required security level or security level briefly. Depending on the selected security level, strength of security countermeasures should be decided.

Security countermeasures can be formed after deciding the security level. Where and how the security countermeasures should be built is decided by considering the characteristics of IS. Security countermeasures may be focused on network, server, or maintenance of management systems [10-13].

Security can be achieved after securing all areas to the same level. This is the only method for attaining and managing security level continuously for IS. As the only vulnerability included in a component of IS can comprise of whole IS, partial security countermeasures for a part in IS cannot protect whole IS.

So each organization installing and operating IS, to achieve the goal of organization, should decide on a security level, implement security countermeasure, and manage these countermeasures to maintain the effects [14-16].

To manage the security level of IS, organizations must be able to decide on a security level, then they must have procedures for building security countermeasures according to security level. For the next step, organizations must be able to select areas where security countermeasures should be applied. Last of all, organizations must be able to evaluate and improve the effect of security countermeasures [17-20].

Some methods for deciding the strength of security of IT products have already been proposed [21].

However, research for developing a method for deciding the security level has not been proposed actively yet. This is because too many unpredictable variables are contained in an IS.

1.4 OUR CONTRIBUTIONS

In this thesis, after analyzing previous research results, the author proposes some essential elements for security level definition and management of IS. After classifying, proper level was granted to threats and assets, and weights were assigned to each level. By summating these weights, the security level of an IS can be decided.

After deciding the security level, basic technical and non-technical requirements for security level management are proposed in detail. Some items needed to ensure basic security state of IS are listed in this requirements.

After this, level requirements to ensure security level required for each IS are proposed in detail. These level requirements should be applied differently for both technical and non-technical parts. Level requirements are designed by using step-model for technical areas, and continuous-model for non-technical areas.

1.4.1 THREAT LEVEL DEFINITION METHOD

Threat level is intimately associated with the possibility of potential attack and vulnerabilities included in IS. According to ISO/IEC 18045, CEM (Common Evaluation Methodology), threat level is able to be decided by the level of potential possibility of attacker's success, and this possibility can be analogized by solving the function constructed by the attacker's motivation, speciality, and available resource.

However, this is a method emphasizing attacker's situation mostly. Therefore, at least the analysis results of information system characteristics should be considered to decide the threat level at the same time.

There are many kinds of attack methods and purposes. General purpose of hacking is to get the administrator's privilege, but other purposes of attack are more serious. Some attacks tries to destroy the IS itself.

Unfortunately, CEM considers only electrical attacks, but in this thesis, the author extends the concept of attack to all possibilities of real attack. So the physical destruction should be considered as one of attack type.

Finally, the author appended more factors to decide threat level. To categorize and decide the level of attack, next factors should be considered: identification of attacker, attacker's motivation, category of attack, access to IS, equipments or tools and elapsed time of IS.

1.4.2 ASSET LEVEL DEFINITION METHOD

In risk management researches, 'impact analysis' or other expressions are used instead of 'asset level'.

The impact analysis in risk management area means the calculation of possible losses when attacks are successful. This calculation result will be connected to the implementation of some countermeasure to prevent these losses.

However, there are some problems in general impact analysis processes :

The first, to do correct and effective impact analysis, specialists should have enough information. So, most or all important information of the organization should be opened to them.

The second, most of risk management specialists have enough knowledge about security, but they may not know about major market and competition environment of the organization. Therefore, it may be difficult to judge correct value of assets.

And the last, there can be the differences between the judgements of specialists and owners. Only owners can identify all assets, and know the correct and exact value of their assets, so owners must decide the asset value.

The author propose next four asset levels as the sample, and in SLMM (Security Level Management Level), asset level decided by owners is used instead of impact factor analysis. But the decision of asset level is a very subjective concept and will be made by the owners of IS. It is possible to reference SLMM consultants' opinion or other specialists' suggestion, but these opinions and suggestions are not always the same as owners' decision. The four levels are expressed as qualitative expression, but SLMM consultants can change them as quantitative expression by considering the environments of the organization.

1.4.3 Security Level Definition Method

The author proposes SL (Security Level) definition method by considering 2 factors, threat level and asset level defined above. About the security level, it should be notified that higher level threat level does not mean higher security level, and conversely, higher security level does not mean higher threat level.

Security Level should be decided by correct analysis of threat level and asset level, and should be changed by considering the changes of threat level and asset level.

Security level can be decided by using metrics in [Table 20], but details should be decided by considering operational environments and characteristics of IS.

1.4.4 Security Level Management Model

The author designed SLMM architecture to provide a guide to keep the security level of information system. The goal of the architecture is to provide characteristics of the security countermeasures should be implemented to keep information system. And the goal of this architecture is to clearly separate basic characteristics from its institutionalization characteristics. In order to ensure this separation, the model has two dimensions, called "area" and "level" as like many international models such as SSE-CMM [9] and CMM [14].

Importantly, the SLMM does not imply that any particular group or role within an organization must do any of the security practices described in the model. Nor does it require that the latest and greatest security related technique or methodology be used. The model does require, however, that an organization have a policy that includes the basic security practices described in the model. The organization is free to create their own policy and organizational structure in any way that meets their business objectives.

1.4.4.1 Level Dimension in Security Level Management Model

The author designed the level dimension which represents some “level features” as they apply across a wide range of security areas by modifying SSE-CMM. The level features represent activities that should be checked and confirmed as a part of implementing security practices. Each level feature contains some level requirements. There are five levels in SSE-CMM, but four levels are enough for security level management, so level features of 5th level in SSE-CMM were merged to 4th level.

Design flow is listed below:

1. Characteristics of each level in six levels of SPICE were analyzed.

2. Characteristics of each level in five levels of CMMI were analyzed.

3. Characteristics of each level in five levels of SSE-CMM were analyzed.

4. Map between security level and analyzed level was made. To obtain a higher level, owners should invest more resources including financial investment.

5. As a result, each level requirement was selected and assigned to security levels

1.4.4.2 Area Dimension in Security Level Management Model

The author designed the area dimension, too. As like the CMM and SPICE, the area dimension is perhaps the easier of the two dimensions to understand. This dimension simply consists of all the security areas that can construct security countermeasure.

To design security areas, the author used area division form in SPICE, ISO/IEC 15504 and SSE-CMM, ISO/IEC 21827.

Design flow is listed below:

1. From SSE-CMM, totally 128 base practices in 22 practice areas were analyzed, and only the practices related to security were selected.

2. From SSE-CMM, all work products were analyzed, and only the work products related to security were selected.

3. From SPICE, all processes in five process dimension (customer-supplier, engineering, supporting, management, organization) were analyzed, and only the processes related to security were selected.

4. From the IATF, all technical items were analyzed, and only the items can be realized were selected.

5. From the ISMS, all controls were analyzed and selected.

6. All factors selected were grouped in 26 categories according to the characteristics.

7. Common expression and name can represent each category was decided, and each category was re-named as a security practice.

8. All security practices were grouped in 8 groups according to the characteristics.

9. Common expression and name can represent each group was decided, and each group was re-named as a security area.

10. All security areas were grouped in two parts according to the characteristics: management part and technology part.

1.4.4.3 **Continuous Model and Staged Model**: In SLMM, security management part is continuous style, and security technology part is staged style. Staged model was used in CMM. In staged model, to upgrade to higher level, all processes or basic practices should be satisfied with level requirements without exception. In other words, all security practices in technology part should be satisfied to get the target level.

Continuous model is being used in SSE-CMM and SPICE, etc. In continuous model, to upgrade to higher level, only selected processes or basic practices should be satisfied with level requirements. In other words, only selected security practices in management part should be satisfied to get the target level.

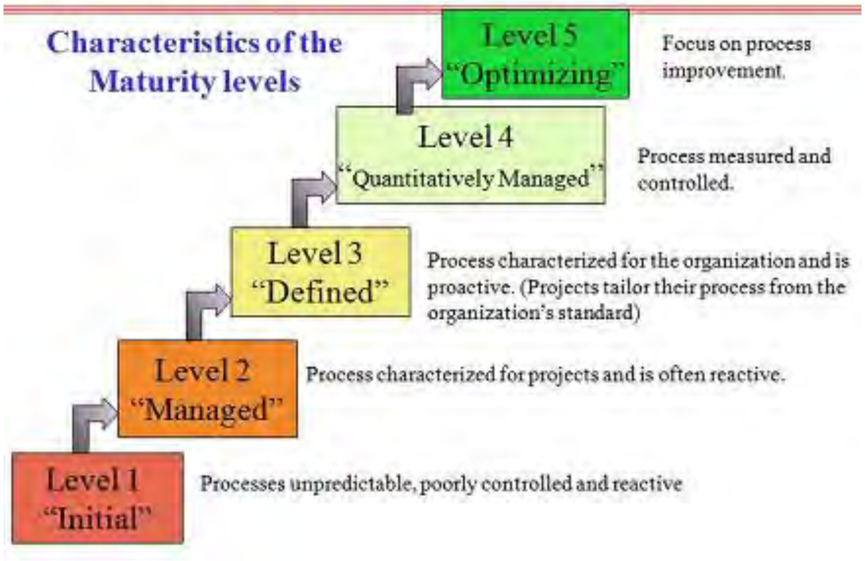

Characteristics of the Maturity levels
Level 5 "Optimizing"
Focus on process improvement.
Level 4 "Quantitatively Managed"
Process measured and controlled.
Level 3 "Defined"
Process characterized for the organization and is proactive. (Projects tailor their process from the organization's standard)
Level 2 "Managed"
Process characterized for projects and is often reactive.
Level 1 "Initial"
Processes unpredictable, poorly controlled and reactive

Figure 1 Example of Staged Model

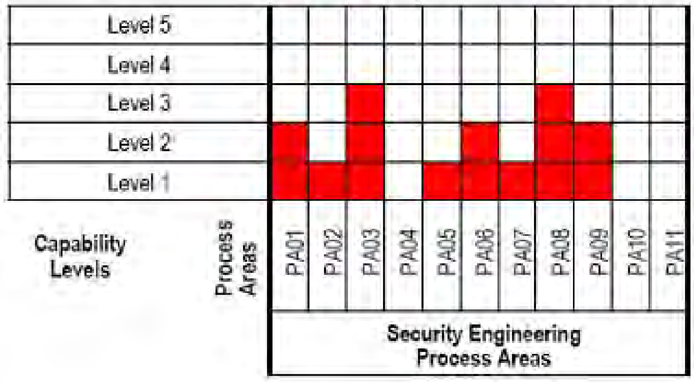


Figure 2 Example of Continuous Model

1.5 COMPARISON WITH EXISTING WORKS.

Current standards approaches to information security and management can be classified as [23-59]:

- Process oriented: ISM3, CMMI, Cobit 4.0, ISO9001:2000, ISO20000, ITIL/ITSM, SSE-CMM, CMM, SPICE
- Controls oriented: BSI-ITBPM, ISO27001:2005, ISO13335-4, ISMS
- Product oriented: CC/ISO15408, CEM/ISO18045, ITSEC, TCSEC
- Risk management oriented: AS/NZS 4360, CRAMM, EBIOS, ISO 27005, MAGERIT, MEHARI, OCTAVE, SP800-30, SOMAP
- Best practice oriented: ISO/IEC 17799:2005, Cobit, ISF-SoGP

Here the [Table 4] expresses the differences among SLMM and some existing works.

Table 4 Differences Among SLMM and Some Existing Works

Characteristic **Research Works**	**Level Definition**	**Security Level**	**Threat Level**	**Asset Level**	**Management**	**Technology**	**Continuous Type**	**Staged Type**
SLMM	⊙	⊙	⊙	⊙	⊙	⊙	◎	◎
CMM	⊙	△	×	×	⊙	△	×	⊙
CMMI	⊙	△	×	×	⊙	△	⊙	×
SSE-CMM	⊙	◎	△	△	⊙	◎	⊙	×
SPICE	⊙	△	×	×	⊙	△	⊙	×
ISMS	×	×	○	△	◎	⊙	×	×
ISM^3	×	×	×	×	⊙	○	×	×
IATF	⊙	◎	⊙	◎	◎	⊙	×	◎
CMVP	⊙	○	○	△	△	⊙	×	×
CC/CEM	⊙	○	◎	△	△	⊙	◎	×

※ Relationship: ⊙ Very much, ◎ Much, ○ Medium, △ Little, × None

2. SECURITY LEVEL DECISION METHOD

Security level decision is a basic activity for developing and managing safe information systems, and core factor which can affect the investment for security countermeasures.

According to the security level of IS, important decisions such as where and how the security countermeasures are implemented, which security policies are selected, and who will manage them are able to be decided.

Security Level can be decided at the initial step of management processes and can be changed according to the change of environments at the later steps. It is possible to change security level at each management process, but the change of security level may affect whole security policy of IS itself, thus operators and owners' agreement is needed.

Security is concerned with the protection of assets, and assets are entities that owner places value upon. As the concept of asset is related to the owner's mind or decision, owner is endowed with responsibilities for protection.

This concept is described in 'common criteria' very well [1-3].

Many assets are in the form of information that is stored, processed and transmitted by IT products to meet requirements laid down by owners of the information. Information owners may require that availability, dissemination and modification of any such information is strictly controlled and that the assets are protected from threats by countermeasures. [Figure 3] illustrates these high level concepts and relationships.

Safeguarding assets of interest is the responsibility of owners who place value on those assets. Actual or presumed threat agents may also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner. Examples of threat agents include hackers, malicious users, non-malicious users (who sometimes make errors), computer processes and accidents.

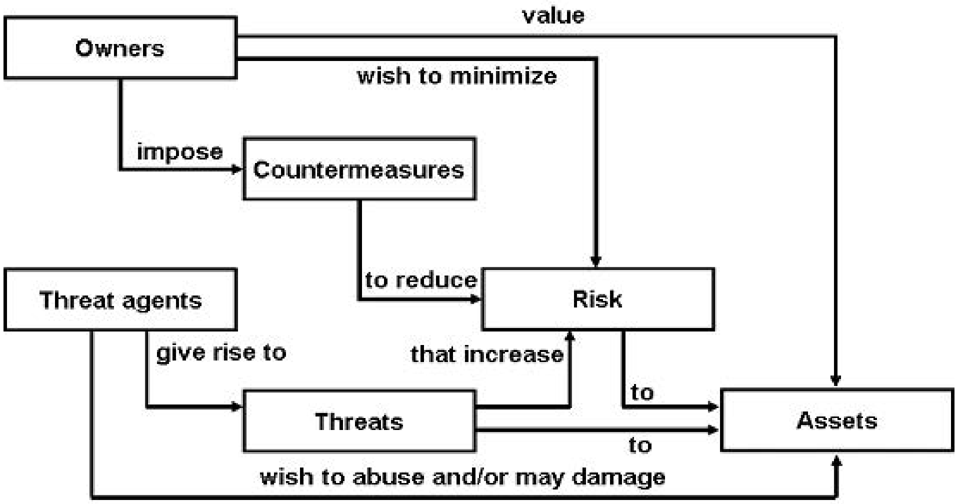


Figure 3 Security Concepts and Relationships

The owners of the assets will perceive such threats as potential for impairment of the assets such that the value of the assets to the owners would be reduced. Security-specific impairment commonly includes, but is not limited to: loss of asset confidentiality, loss of asset integrity and loss of asset availability.

These threats therefore give rise to risks to the assets, based on the likelihood of a threat being realised and the impact on the assets when that threat is realised. Subsequently countermeasures are imposed to reduce the risks to assets. These countermeasures may consist of IT countermeasures (such as firewalls and smart cards) and non-IT countermeasures (such as guards and procedures).

In Figure 3, threat and asset are the more important factors that should be considered to decide security level of IS. Others are connected mutually and affect to security level indirectly.

Security level (SL) is decided by calculating the value of information and information systems protected and the strength of threat, and can be depicted as like next equation (1).

$$SL=f(TL,AL) \tag{1}$$

where, TL is the threat level and AL is the asset level.

When organizations decide the SL, threat level and asset level should considered as two important factors. Threat level can be decided by cooperation of owners, operators, and developers, but asset level should be decided by owner of IS and information.

In general case, the assets value can be analyzed and decided by the size, scope, or economic merits, but it is not easy to say this general analysis or counsel may be same with owner's opinion. This is because even though an asset seems to be unimportant to analyzers, this asset can be grouped as one of very important assets.

2.1 DEFINITION OF THREAT LEVEL

Threat level is intimately associated with the possibility of potential attack and vulnerabilities included in IS. According to ISO/IEC 18045, CEM (Common Evaluation Methodology), threat level is able to be decided by the level of potential possibility of attacker's success, and this possibility can be analogized by solving the function constructed by the attacker's motivation, speciality, and available resource.

On the other hand, this is a method emphasizing attacker's situation mostly, at least the analysis results of information system characteristics should be considered to decide the threat level.

Threat can be divided into two parts: identification activity to find attackable points of IS for future attack, and attack activity to do real assail.

This classification is very reasonable. For example, let's consider a vulnerability opened to the public. In the aspect of identification activity, this is very dangerous because this vulnerability is opened and everybody can exploit it. But in the aspect of attack activity, this may not a dangerous one because it is possible that the method to exploit this vulnerability is very difficult or the development of attack tool needs too many resources and times or detection and defense method are already known.

So these two activities can be considered separately, and the threat level can be decided by solving the equation (2).

$$TL=f\,(ID,AT) \tag{2}$$

where ID the is identification activity and AT is the attack activity.

2.1.1 Identification Activity

Identification activity is similar to vulnerability analysis in a sense of finding weak points. But Identification activity is more related to real attack and this an activity to find potential attackable point. A subject, motivation, tool & equipment, and time are the factors can affect to identification activity, so these factors should be considered to decide the depth of identification activity. And other factors can be included according to the environments or importance of IS.

Identification activity can be decided by solving next equation (3) with basic 4 factors.

$$ID=f\,(SoI, MoI, EoI, ToI) \tag{3}$$

Where, SoI is the subject of identification, MoI is the motive of identification, EoI is the equipments or tools for identification, and ToI is the time needed to identify.

Factors of equation (3) may have correlation with one another, but this correlation may not be derived as a formal equation. For example, even though someone has strong motive, this cannot be connected to the reduction of activity time.

The easiest way to solve the equation (3) is to give the weight value to each factor and sum these values. Weight value can be changed by considering environments if necessary.

According to the circumstances, new factors are able to be appended because environments or importance of IS can be changed. In this case, new factors can be inserted to equation (3).

If only four factors mentioned above are considered, the equation (3) is can be depicted like as equation (4). But the correlation function is omitted.

$$ID = f\_SoI\ (SoI) + f\_MoI\ (MoI) + f\_EoI\ (EoI) + f\_ToI\ (ToI) \qquad (4)$$

where, f_SoI (SoI) is a function of SoI,

f_MoI (MoI) is a function of MoI,

f_EoI (EoI) is a function of EoI, and

f_ToI (ToI) is a function of ToI.

As described earlier, threat level can be decided by identification activity and attack activity. But the weight of identification activity is very small when compared with that of attack activity. The equation (2) can be rewritten as like equation (5).

$$TL=f\ (AT) \qquad (5)$$

where AT is the attack activity.

2.1.2 Attack Activity

Attack activity means various and realistic attacks are approaching or will be started in near future. There are many kinds of attack methods and purposes. General purpose of hacking is to get the administrator's privilege, but other purposes of attack are more serious. Some attacks tries to destroy the IS itself.

In this paper, the concept of attack contains all possibilities of real attack, so the physical destruction should be considered as one of attack type.

The goal of attack can be divided into two parts: access to information and compromise or destruction of information systems. If the target were the information itself, attackers will try to obtain unauthorized access to the information or information systems, and if the target were destruction of information systems, attackers will try to cut important connection between components of IS or shut down whole systems. Depending on the importance of IS, potential attacks will be realized differently.

Attack activity is a real attack to the information and information system to compromise or destroy them. To categorize and decide the level of attack, after identifying potential attackers, assessors should consider some factors such as motivation and type of attack, accessibility to IS, tools and equipments, and compromise time estimation.

By using these factors, attack activity can be defined as the next equation (6).

$$Ex = f\,(Ai, Am, Ac, Aa, Ae, At) \qquad (6)$$

Where, Ai : Identification of Attacker,

Am : Attacker's motivation,

Ac : Category of attack

Aa : Attacker's Access to IS,

Ae : Attacker's equipments or tools,

At : Elapsed Time of IS

Each element in equation (6) may have correlation or not. This correlation can not be induced as a formal type. But the possibility of correlation among the elements of attack activity is higher than that of identification activity. For example, if an attacker were the cyber-terrorist, he would have higher motivation for attack to destroy an IS, and he will invest more resources to get success in his attack. So some connected correlations can be formed.

Finally, to calculate equation (6), weights for not only each component but also correlation should be considered. However it is very difficult to say that this correlation can be applied fixedly. Therefore, the weights for correlation among each component should be considered according to the real environments of IS operation. It is possible to append new components into equation (6) according to the change of environment of IS. In this case, not only new components but also correlation among old components should be considered together.

In this paper, weights are given to each component by integer, but these value can be modified by considering real environments and characteristics of IS. The last component of equation (7), alpha means that the weights calculated by correlation among each component. Alpha can be changed by environments and characteristics of IS, in this paper, only the estimated result is included.

$$Ex = fai(Ai) + fam(Am) + fac(Ac) + faa(Aa) + fae(Ae) + fat(At) + \sum fak(Uak) + \alpha \quad (7)$$

where, fai(Ai) is a weight function for identified attacker,

fam(Am) is a weight function for the attacker's motivation,

fac(Ac) is a weight function for attack type,

faa(Aa) is a weight function for accessibility to IS,

fae(Ae) is a weight function for attack tools and equipments, fat(At) is a weight function for compromise time,

fak(Uak) is a weight function for unknown components,

Uak is a k-th unknown component related to attack activity

α is a weight value decided from correlation among components

(1) Identification of Attacker

Generally speaking, attackers are thought of as having malicious intent. However, in the context of system and information security and protection, it is also important to consider the threat posed by those without malicious intent.

Next [Table 5] shows examples of individuals and organizations in both of these categories. Because attackers of [Table 5] did not categorized by the 'Target of attack', [Table 5] can not express the weights of each attacker. Some attackers want to get 'the right of superuser' to use systems resource, but other attackers want to destroy the IS themselves [36].

So when we identify attackers and weight them, we should consider their scope of power.

Table 5 Potential Attacker

Attacker	Description
Malicious	
Nation States	Well-organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having economic, military, or political advantage.
Hackers	A group or individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws.

Terrorists/ Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organized Crime	Coordinated criminal activities, including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.
Other Criminal Elements	Another facet of the criminal community, but one that is normally not very well organized or financed. Usually consists of very few individuals or of one individual acting alone.
International Press	Organizations that gather and distribute news, at times illegally, selling their services to both print and entertainment media. Involved in gathering information on everything and anyone at any given time.
Industrial Competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments through corporate espionage.
Disgruntled Employees	Angry, dissatisfied individuals who can inflict harm on the local network or system. Can represent an insider threat depending on the current state of the individual's employment and access to the system.
Nonmalicious	
Careless or Poorly Trained Employees	Users who, through lack of training, lack of concern, or lack of attentiveness, pose a threat to information and IS. This is another example of an insider threat or attacker.

For example, if the identified attackers are terrorists, they can destroy the IS by bomb, so their power is bigger than hackers who can compromise IS by getting super user ID and Password. Next [Table 6] is the example of weights for identity of attacker's capability. When we apply this table to real IS, the weights should be corrected by checking the environment of those IS.

Table 6 Weights for Identified Attacker's Capability

Item	classified	weight	result
Attackers capability	Trying to get inside	1	
	Infiltration	3	
	Paralyzation	5	
	Destruction	7	

(2) Attacker's motivation

Individual motivations to attack are many and varied. In general case, because we think only the information processed by IS, attacker's motivation is defined like as 'Getting Inside'.

In this paper, attackers were classified and arranged into [Table 6]. If an attacker's capability is included in from Trying to get inside to Paralyzing, this attacker's motivations can be thought as getting inside. In this case, attackers with malicious intent who wish to achieve commercial, military, or personal gain are known as crackers or hackers.

At the opposite end side of the spectrum are people who may compromise the IS accidentally. Hackers range from inexperienced professional, college student, or novice (e.g., script kiddy) to the highly technical and capable. Most hackers pride themselves on their skill and seek, not to destroy, but simply to gain access so that the computer or network can be used for later experimentation. Hackers often believe that by exposing a hole or 'back-door' in a computer system, they are actually helping the organization to close the holes, providing a benefit to the Internet and a needed resource. Other hackers have less benign motives for getting inside.

The following are some common reasons why an attacker might want to exploit a particular target:

o Gain access to classified or sensitive information. (Note: What is of high value to one person or organization might be of no value to another.)

o Track or monitor the target's operations (traffic analysis).

o Disrupt the target's operations.

o Steal money, products, or services.

o Obtain free use of resources (e.g., computing resources or free use of networks).

o Embarrass the target.

o Overcome the technical challenge of defeating security mechanisms.

From an information system standpoint, these motivations can express themselves in three basic goals: access to information, modification or destruction of information or system processes, or denial of access to information. In attacking an information processing system, an attacker accepts a certain amount of risk. This risk may be time dependent. The risk of loss to the attacker may far exceed the expected gain. Risk factors include

o Revealing the attacker's ability to perform other types of attacks.

o Triggering responses that might prevent the success of a future attack, especially when the gain is much greater.

o Incurring penalties (e.g., fines, imprisonment, embarrassment).

o Endangering human life.

The level of risk that an attacker is willing to accept depends on the attacker's motivation. If certain terrorists decide to destroy other organization's IS, they may not be afraid of being exposed to risks. This can be another kind of motivation, and most significant case. Next [Table 7] is the example of weighting for attacker's motivations.

Attackers' capability and motivation is not the same concept. Even though an attacker has high capability, it is very difficult to say that attacker has strong motivation to attack an IS. Therefore, when we apply this table to a real IS, the weights should be corrected by checking the environment of IS and expected attackers' motivation.

Table 7 Weights for Attacker's Motivation

Item	Classified	weight	result
Attacker's motivation	Embarrassing	1	
Attacker's motivation	Obtaining of Resource	2	
Attacker's motivation	Stealing	3	
Attacker's motivation	Denial of service	4	
Attacker's motivation	Destruction	5	

(3) Category of attack

In general case, IS and networks offer attractive targets to attackers. In an ideal case, IS should be resistant to attack from the full range of threat-agents from hackers to nation states. Moreover, they must limit potential damage and recover rapidly when attacks do occur. But in real case, it is very difficult to resistant to strong attacks, especially physical attacks. If attackers may use bombs to destroy the IS, there are few methods to protect them. Therefore, in this paper, physical destruction of IS are not considered.

In this thesis, attacks divided into two categories such as Passive and Active. The key aspects of each category of attack can be summarized like as next description.

o Passive

Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information (e.g., passwords). Passive intercept of network operations can give adversaries indications and warnings of impending actions.

Passive attacks can result in the disclosure of information or data files to an attacker without the consent or knowledge of the user. Examples include the disclosure of personal information such as credit card numbers and medical files.

Passive attacks involve passive monitoring of communications sent over public media (e.g., radio, satellite, microwave, and public switched networks). Countermeasures used against passive attacks include virtual private networks (VPN), cryptographically protected networks, and protected distribution networks (e.g., physically protected or alarmed wireline distribution network).

Next [Table 8] provides examples of attacks characteristic of this class. But these are not the all kinds of passive attacks but only examples.

But passive attacks are not limited to physical areas. Attackers can gather significant information about the target not only intercepting traffic but also hearing talk of administrators.

o Active

Active attacks include attempts to circumvent or break protection features, introduce malicious code, and steal or modify information. These include attacks mounted against a network backbone, exploitation of information in transit, electronic penetrations into an enclave, or attacks on an authorized remote user when attempting to connect to an enclave. Active attacks can result in the disclosure or dissemination of data files, denial of service, or modification of data.

Table 8 Examples of Passive Attacks

Attack	Description
Monitoring Plaintext	An attacker monitoring the network could capture user or enclave data that is not otherwise protected from disclosure.
Decrypting Weakly Encrypted Traffic	Cryptoanalytic capability is available in the public domain, as witnessed by the June 1997 collaborative breaking of the 56-bit-strength Data Encryption Standard. While the near-term potential for attack on large volumes of traffic is questionable given the number of machines and hours involved, breaking of DES does show the vulnerability of any single transaction.
Password Sniffing	This type of attack involves use of protocol analyzers to capture passwords for unauthorized reuse.
Traffic Analysis	Observation of external traffic patterns can give critical information to adversaries even without decryption of the underlying information. For example, extension of a network into a tactical theater of operations may indicate the imminence of offensive operations thereby removing the element of surprise.

Typical countermeasures include strong enclave boundary protection (e.g., firewalls and guards), access control based on authenticated identities (ID) for network management interactions, protected remote access, quality security administration, automated virus detection tools, auditing, and intrusion detection.

Next [Table 9] provides examples of active attacks characteristic of this class. But these are not the all kinds of active attacks but only examples.

Table 9 Examples of Active Attacks

Attack	Description
Modifying Data in Transit	In the financial community, it would be disastrous if electronic transactions could be modified to change the amount of the transaction or redirect the transaction to another account.
Replaying (Insertion of Data)	Reinsertion of previous messages could delay timely actions. Bellovin shows how the ability to splice messages together can be used to change information in transit.

Session Hijacking	This attack involves unauthorized use of an established communications session.
Masquerading as Authorized User/Server	This attack involves an attacker's identifying himself or herself as someone else, thereby gaining unauthorized access to resources and information. An attacker first gets user or administrator information by employing sniffers or other means, then uses that information to log in as an authorized user. This class of attack also includes use of rogue servers to obtain sensitive information after establishing what is believed to be a trusted service relationship with the unsuspecting user.
Exploiting System-Application and Operating System Software	An attacker exploits vulnerabilities in software that runs with system privileges. Well-known attacks involve sendmail and X-Windows server vulnerabilities. Recently, there has been an increase in alerts regarding Windows 95 and Windows NT vulnerabilities. New vulnerabilities for various software and hardware platforms are discovered almost daily. Attacks, vulnerabilities, and patches are reported through the various computer emergency response alerts and bulletins.
Exploiting Host or Network Trust	An attacker exploits transitive trust by manipulating files that facilitate the provision of services on virtual/remote machines. Well-known attacks involve UNIX commands, .rhosts and .rlogin, which facilitate workstation's sharing of files and services across an enterprise network.
Exploiting Data Execution	An attacker can get the user to execute malicious code by including the code in seemingly innocent software or e-mail for downloading. The malicious code might be used to destroy or modify files, especially files that contain privilege parameters or values. Well-known attacks have involved PostScript, Active-X, and MS Word macro viruses.
Inserting and Exploiting Malicious Code (Trojan horse, trap door, virus, worm)	An attacker can gain execution access to a user's system commands through one of the vulnerabilities previously identified and use that access to accomplish his or her objectives. This could include implanting software to be executed based on the occurrence of some future event. Hacker tools are available on the Internet. These tools have turnkey capabilities, including an insertion script, root grabbing, Ethernet sniffing, and track hiding to mask the presence of a hacker.
Exploiting Protocols or Infrastructure Bugs	An attacker exploits weaknesses in protocols to spoof users or reroute traffic. Well-known attacks of this type include spoofing domain name servers to gain unauthorized remote login, and bombing using Internet Control Message Protocol (ICMP) to knock a machine off the air. Other well-known attacks are source routing to impersonate a trusted host source, Transmission

	Control Protocol (TCP) sequence guessing to gain access, and TCP splicing to hijack a legitimate connection. Malicious code can exfiltrate information through a lower level tunnel within a VPN. At least one published paper points out potential security concerns revolving around use of Internet Protocol Security default security mechanisms. In addition, Bellovin points out occasions on which the integrity functions of Data Encryption Standard in Cipher Block Chaining mode can be circumvented, with the right applications, by splicing of packets.
Denial of Service	An attacker has many alternatives in this category, including ICMP bombs to effectively get a router off the network, flooding the network with garbage packets, and flooding mail hubs with junk mail.

Similar to passive attack, active attacks are not limited to physical areas. Attackers want to get inside, use system resources, and do something malicious. There are very many methods for getting inside of IS not passing through the Firewall and IDS by network.

Next [Table 10] is the example of weighting for category of attacks.

Table 10 Weights for Category of Attacks

Item	Classified	weight	result
Category of attacks	Passive	3	
Category of attacks	Active	5	

(4) Attacker's Access to IS

In general case, if the IS can be accessed physically, compromise becomes easier. The status of 'physical access to IS' means, in most case, that the attacker has already bypassed the security countermeasure of boundary area.

If the attackers are in your office already, they may not attack your company's boundary Firewall or Intrusion Detection Systems. If attackers are in the mainframe room already, they will attack mainframe or critical server systems directly.

Attackers know well about the penalties they should bear when their malicious actions are detected. But the IS and networks offer attractive targets to attackers. So they will find more easy and safe methods to compromise IS, and indeed, physical access to IS, if attackers can do so, is the easiest way.

There are too many methods to access information systems. So it is impossible to describe all methods. In this paper, methods of access to IS are divided into three categories: distribution, close-in, and insider. The key aspects of each category of access can be summarized like in the next description.

o Distribution

The term "distribution" refers to the potential for malicious modification of hardware or software between the time of its production by a developer and its installation, or when it is in transit from one site to another. Distributions can be connected to attack. So it is possible to call this class 'distribution attack.'

Vulnerability at the factory can be minimized by strong in-process configuration control. International standard ISO/IEC 21827, System Security Engineering Capability Maturity Model (SSE-CMM), can provide basic concept about this work. However SSE-CMM can not cover all production and development processes deeply enough.

Vulnerability to distribution can be addressed by use of controlled distribution or by signed software and access control that is verified at the final user site. This work is related to acquisition capability and process of international standard ISO/IEC 15504, but this is not complete one. Next [Table 11] contains examples of attacks characteristic of this class.

Table 11 Examples of Distribution Attacks

Attack	Description
Modification of Software/Hardware at Manufacturer's Facility	These attacks can involve modifying of the configuration of software or hardware while it is cycling through the production process. Countermeasures for attacks during this phase include rigid integrity controls, including high-assurance configuration control and cryptographic signatures on tested software products.
Modification of Software/Hardware during Distribution	These attacks can involve modifying of the configuration of software or hardware during its distribution (e.g., embedding of listening devices during shipment). Countermeasures for attacks during this phase include use of tamper detection technologies during packaging, use of authorized couriers and approved carriers, and use of blind-buy techniques.

o Close-in

Close-in means that outsiders or attackers physical access to IS. So we can call this such as 'Close-in attack.'

Close-in attacks are attacks in which an unauthorized individual gains close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Gaining such proximity is accomplished through surreptitious entry, open access, or both.

Next [Table 12] provides examples of specific attacks characteristic of this class.

Table 12 Examples of Close-In Attacks

Attack	Description
Modification of Data/Informati on Gathering	This results from an individual gaining physical access to the local system and modifying or stealing information, such as, Internet Protocol addresses, login ID schemes, and passwords.

System Tampering	This type of attack results from an individual in close proximity gaining access to and tampering with the system (e.g., bugging, degrading).
Physical Destruction	This type of attack results from an individual in close proximity gaining physical access, and causing the physical destruction of a local system.

o Insider

Insider attacks are performed by a person who either is authorized to be within the physical boundaries of the information security processing system or have direct access to the information security processing system.

There are two types of insider attacks: malicious and non-malicious (the latter involving carelessness or ignorance of the user). The non-malicious case is considered an attack because of the security consequences of the user's action.

- Malicious Insider Attacks.

Federal Bureau of Investigation (FBI) estimates indicate that 80 percent of attacks and intrusions come from within organizations [61]. An insider knows the layout of the system, where the valuable data is, and what security precautions are in place.

Insider attacks originate from within the enclave and are often the most difficult to detect and to defend against. Sources of insider attacks can include uncleared cleaning crews (with after-hours physical access), authorized (privileged to login) system users, and system administrators with malicious intent. Often it is difficult to prevent individuals who have legitimate access to a system from accessing into more private areas to which they do not have authorized access.

Insider attacks may focus on compromise of data or access and can include modification of system protection measures. A malicious insider may use covert channels to signal private information outside of an otherwise protected network. However, there are many other avenues by which a malicious insider can damage an information system.

- No malicious Insider Attacks.

These attacks are caused by authorized persons who have no intent to cause damage to the information or to the information processing system but may unintentionally do so.

The damage in this case is caused by lack of knowledge or by carelessness.

Typical countermeasures include security awareness and training, auditing and intrusion detection, security policy and enforcement, specialized access control for critical data, servers, local area networks (LAN), etc., implemented by trust technology in computer and network elements, and a strong identification and authentication (I&A) capability. Next [Table 13] contains examples of attacks characteristic of this class.

Table 13 Examples of Insider Attacks

Attack	Description
Malicious	
Modification of Data or Security Mechanisms	Insiders often have access to information due to commonality of shared networks. This access can, allow manipulation or destruction of information without authorization.
Establishment of Unauthorized Network Connections	This results when users with physical access to a classified network create an unauthorized connection to a lower classification level or lower sensitivity network. Typically this connection is in direct violation of the classified network's security policy or user directives and procedures.
Covert Channels	Covert channels are unauthorized communication paths used for transferring misappropriated information from the local enclave to a remote site.
Physical Damage/ Destruction	This is intentional damage to, or destruction of, a local system resulting from the physical access afforded the insider.
Nonmalicious	
Modification of Data	This type of attack results when insiders, either through lack of training, lack of concern, or lack of attentiveness, modify or destroy information located on the system.

Physical Damage/ Destruction	This type of attack is listed under malicious as well. As a nonmalicious attack, it can result from carelessness on the part of the insider, for instance, failure to obey posted guidance and regulations, resulting in accidental damage to or destruction of, a system.

Next [Table 14] is the example of weighting for access to IS.

Table 14 Weights for Access

Item	classified	weight	result
Access to IS	Unauthorized access	3	
Access to IS	Establishment of unauthorized connection	4	
Access to IS	Disability	5	

Distribution attacks are very useful, but this type of attack can be detected by another systems. So before many parts of IS are modified to follow attackers command, this attack may be stopped.

Close-in attacks are also very useful, but if physical protection guard systems are well developed and implemented already, this attack may not be successful.

Insider attack may not be detectable, because an insider knows well about the security policies and security systems. So this type of attack is the most dangerous.

(5) Tools and equipments

Possibility of attacks is dependent on the resources, tools and equipments attackers may use. For example, if attacker can use the super computer to analysis crypto systems, they may have higher possibility than the case they use only personal computers.

Indeed, most attackers knows very well about the penalty they may overcome when their malicious actions are detected or captured. So if they want to get more valuable assets, they will use more expensive and high-tech tools and equipments.

When calculating the weights about the tools and equipment, we should consider who the attackers are. If attackers are script kiddies or non-malicious users, they may not have excellent tools or expensive equipments. But if attackers are nations or cyber-terrorists have sufficient budget and malicious intent, they will develop very elaborate tools and buy very expensive equipments to achieve their final goals.

And because good tools and equipments can compensate for the lack of expertise and knowledge, weights for the tools and equipments are important.

Next [Table 15] is the example of weighting for tools and equipments attackers may use.

Table 15 Weights for Tools and Equipments

Item	classified	weight	result
Tools and equipments	Basic or well known	2	
Tools and equipments	Specializing	4	
Tools and equipments	Optimizing	5	

(6) Elapsed Time of IS

It is very difficult to calculate the elapsed time of IS. There are too many methods to attack the IS, and nobody can identify all of these methods.

But this "Elapsed time" is very important, because elapsed time means that the permitted time to us to count the attack. Unfortunately, we have no much time to count attacks if attackers may do a concentrated attack.

In fact, concentrated attacks are dependent on the tools and equipments attackers may use. Tools and equipments of attackers are dependent on accessibility to the target systems, and trying to access the target systems is dependent on the type of attacks the attackers want to do. The category of attack is dependent on the attackers' motivation, and finally, this motivation is dependent on who the attackers is.

Operators need time to counter attacks, because they should analyze the characteristics of these attacks. However they may not sure they can do this work successfully in a short time. Therefore, the estimation of elapsed time is important. At the initial state when operators may detect the attacks, they can estimate the elapsed time of the IS, and should do something to protect this systems.

Next [Table 16] is the example of weighting for elapsed time.

Table 16 Weights for Elapsed Time

Item	classified	weight	result
Elapsed time	some months	1	
Elapsed time	some days	3	
Elapsed time	some hours	5	

2.1.3 THREAT LEVEL DECISION BY SUM OF WEIGHTS

Threat Level can be decided by summation of weights of all components listed above. Working environment of each information system is different, and therefore, sometimes relationships among some components should be considered. However these relationships are very dependent on the characteristics of each information system, and unfortunately, we can not consider all cases. Characteristics of each information system should be considered after selecting target system. Easiest way to decide threat level is disregarding the correlation among the components. And this method can be extended easily to specific systems. From the weight tables proposed above, summation of weights can be changed variously. And this is enough to make a threat level decision table.

Before construction threat level decision table, threat levels should be defined. When we consider binary communication signal, 'On', 'Off' and 'Undecided' signals can be defined. For example, 5[V] can be defined 'On', and 0[V] 'Off'. But how about 4.5[V]? Most systems consider this signal as 'On'. Then how about 3.5[V]? Some systems consider this signal as 'On', too. Here is a problem. 3.5[V] and 5[V] are the same value?

In this case, we can use make a rule. If the systems are very sensitive, we can define only 4.5[V] or higher signal should be considered as 'On'. If the systems are not sensitive, we can define 3.5 [V] or higher signal can be considered 'On'. Next [Table 17] is an example of threat level.

Table 17 Threat Level Definition

Threat Level	Description
TL1	Attackers can check current security countermeasures
TL2	Attackers can disturb IS operation slightly, Attackers may achieve some IS information
TL3	Attackers can give little harm to IS, Attackers may access to IS with low privilege
TL4	Attackers can give much harm to IS, Attackers may access to IS with low privilege
TL5	Attackers can destroy IS, Attackers can control IS

Next [Table 18] is the example of threat level definition.

Table 18 Example of Threat Level Decision

Summation of weights (SoW)	Threat Level
SoW < 6	TL1
6 ≦ SoW < 12	TL2
12 ≦ SoW < 18	TL3
18 ≦ SoW < 24	TL4
24 ≦ SoW	TL5

2.2 DEFINITION OF ASSET LEVEL

Even though threat levels are decided like in [Table 18], security level of each IS has not been decided yet. To decide the security level, AL (Asset Level) defined by user or owner should be considered together. Estimation for AL is related to the evaluation of the effect occurred by compromise to assets. But the decision of AL is a very subjective concept and will be made by the owners of IS. It is possible to reference security level managers' opinion or other specialists' suggestion, but these opinions and suggestions are not always the same as owners' decision. Next [Table 19] is a basic model of AL categorized by the effect of compromise of IS.

Table 19 Example of Security Label Definition

Asset Level	Description
AL1	Owners will maintain current status
AL2	Owners will invest a little more resources to protect these assets
AL3	Owners will invest a lot of resources to protect these assets
AL4	Owners will do everything to protect these assets

2.3 DEFINITION OF SECURITY LEVEL

SL (Security Level) can be decided by considering 2 factors, threat level and asset level defined above. About the security level, it should be notified that higher threat level does not mean higher security level, and conversely, higher level security level does not mean higher threat level.

Security level is related to the concept of IA (Information Assurance), and the definition of security level can be the proof that security requirements for IS were included well.

In this paper, SL is divided and described into 4 level shown in [Table 20].

Table 20 Security Level Definition

Security Level	Description
SL1	Executed Basically - Security countermeasures are executed informally
SL2	Verified and Tracked - Security countermeasures should be verified and tracked
SL3	Quantitatively Controlled - Security countermeasures should be measured and managed
SL4	Monitored and Improved - Security countermeasures should be monitored and optimized

Security Level should be decided by correct analysis of threat level and asset level, and should be changed by considering the changes of threat level and asset level.

Security level can be decided by using next metrics in [Table 21], but details should be decided by considering operational environments and characteristics of IS.

Table 21 Decision of Security Level

Asset level	Threat Level				
	TL1	TL2	TL3	TL4	TL5
AL1	**SL1**	**SL1**	**SL1**	**SL1**	**SL1**
AL2	**SL1**	**SL1**	**SL1**	**SL2**	**SL2**
AL3	**SL1**	**SL1**	**SL2**	**SL3**	**SL3**
AL4	**SL1**	**SL2**	**SL3**	**SL3**	**SL4**

3. SECURITY LEVEL MANAGEMENT MODEL DESCRIPTION

SLM2 or SLMM (Security Level Management Model) is a compilation of some engineering theories related to security. To understand this model, some backgrounds in security engineering and software engineering are required.

3.1 SLMM ARCHITECTURE DESCRIPTION

The SLMM architecture is designed to provide a guide to keep the security level of information system. The goal of the architecture is to provide characteristics of the security countermeasures should be implemented to keep information system.

And the goal of this architecture is to clearly separate basic characteristics from its institutionalization characteristics. In order to ensure this separation, the model has two dimensions, called “area” and “level”.

Importantly, the SLMM does not imply that any particular group or role within an organization must do any of the security practices described in the model. Nor does it require that the latest and greatest security related technique or methodology be used. The model does require, however, that an organization have a policy that includes the basic security practices described in the model. The organization is free to create their own policy and organizational structure in any way that meets their business objectives.

3.2 THE BASIC MODEL

The SLMM has two dimensions, “area" and “level.”

The area dimension is perhaps the easier of the two dimensions to understand. This dimension simply consists of all the practices that can construct security countermeasure.

These practices are called “security practices”, and can be categorized into 8 security areas in 2 parts.

The structure and content of these security practices are discussed below.

The level dimension represents some “level features” as they apply across a wide range of security areas. The level features represent activities that should be checked and confirmed as a part of implementing security practices. Each level feature contains some level practices.

Figure 4 illustrates the relationship between security practices and level requirements. This figure represents similar concept with SSE-CMM but not same. The biggest difference is that SSE-CMM has the only continuous model but SLMM has not only continuous model but also staged model. In other words, security management part is continuous style, but security technology part is staged style.

Putting the security practice and level requirements together provides security requirements that should be implemented to keep an organization’s security level.

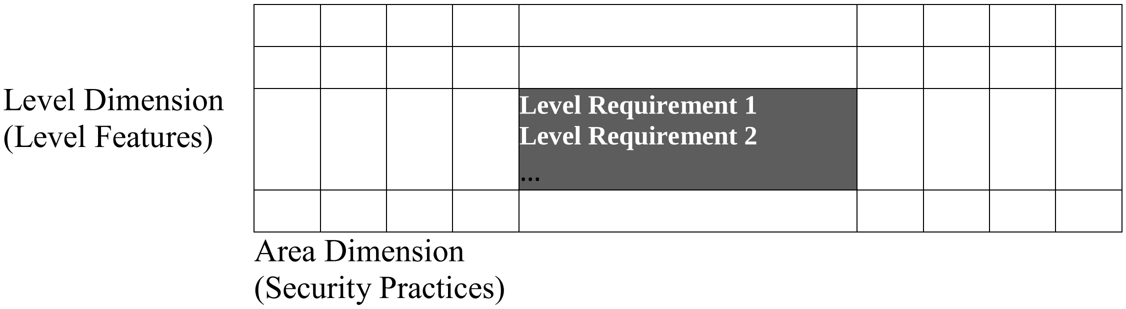


Figure 4 Relationships between Security Practice and Level Requirements

After deciding on a security level, some practices should be selected by considering characteristics and environments of information systems. Implementing all the requirements raised by combining all the security practices with all the level requirements will provide a good picture of the security countermeasures of the organization in question.

3.3 THE SECURITY PRACTICES

The SLMM contains 26 security practices, organized in 8 areas. These security practices cover all major areas of security countermeasures. Additionally, more security practices organized in additional areas can be appended, and these additional practices can be drawn from the other systems engineering or security engineering areas.

The security practices were gathered from a wide range of existing materials, practices, and expertises. The practices selected represent the best existing practice of the security community, but these practices are not static and can be modified by considering characteristics and environments of information system.

Identifying security practices is complicated by the many different names for activities that are essentially the same. These activities occur anytime in the life cycle, at a different level of abstraction, or are typically performed by individuals in different roles.

An organization cannot be considered to have achieved a security practice if it is only performed during the design phase or at a single level of abstraction. SLMM does not ignore these distinctions because these can be a candidate practice organizations can select. But SLMM does not contain these practices, so security level manager should decide if they want to include these practices.

It is recommended that each security practice has some characteristics like as:

- Practice should be able to be applied across the lifecycle of the organization.

- Practice does not overlap with other practices.

- Practice represents a “best practice” of the security community.

- Practice does not simply reflect a state-of-the-art technique.

- Practice is applicable using multiple methods in multiple business contexts.

- Practice does not specify a particular method or tool.

The security practices have been organized into security areas in a way that meets a broad spectrum of security organizations. There are many ways to divide the security domain into areas.

Each security area has a set of goals that represent the expected state of an organization that is successfully implementing the security area. An organization that performs the security practices of the security area should also achieve its goals.

It is recommended that each security area has some characteristics such as:

- Security area assembles related activities in one area for ease of use

- Security area relates to valuable security services

- Security area applies across the life cycle

- Security area includes all security practices that are required to meet the goals of the security area

In SLMM, there are 8 security areas and these areas are grouped into 2 parts. The 8 security areas of the SLMM are listed below. Note that they are listed in alphabetical order to discourage the notion that the security areas are ordered by lifecycle phase. These security areas and the security practices that define them are described in Chapter 4.

Part 1: Security Management Part (SMP)

- SA01 Human Resource

- SA02 Operation and Administration

- SA03 Physical Protection

Part 2: Security Technology Part (STP)

- SA04 Access Control Technology

- SA05 Cryptography Technology

- SA06 Identification and Authentication Technology

- SA07 Service Assurance Technology

- SA08 Shielding Technology

3.4 THE LEVEL REQUIREMENTS

Level requirements are activities that apply to areas. They can address the management, measurement, and institutionalization aspects of each area. In general, they provide guide for security countermeasure and are used during an appraisal to determine if an organization keeps the guide well.

Level requirements are grouped into logical areas called “level features” which are organized into four “Security Levels” which represent increasing organizational requirements. Unlike the security practices of the area dimension, the level features of the level dimension are ordered according to level, and contains process concept partially.

Subsequent level features have level requirements that help to determine how well an organization manages and improves each security area as a whole. The level features below represent the attributes of level requirements to achieve each level, and each level feature contains some level requirements.

And each security level contains two kinds of level features, one for security management part, and the other for security technology part.

Security Level 1: Executed Basically

- 1.1 Security Practices in SMP are Performed Informally

- 1.2 Security Practices in STP are Installed and Managed Properly

Security Level 2: Verified and Tracked

- 2.1 Security Practices in SMP are Verified and Tracked

- 2.2 Security Practices in STP are Installed and Managed Properly

Security Level 3: Quantitatively Controlled

- 3.1 Security Practices in SMP are Measured and Controlled

- 3.2 Security Practices in STP are Installed and Managed Properly

Security Level 4: Monitored and Improved

- 4.1 Security Practices in SMP are Monitored and Improved

- 4.2 Security Practices in STP are Installed and Managed Properly

An organization is generally free to plan, track, define, control, and improve their security level in any way or sequence they choose. However, because some higher level requirements are dependent on lower level requirements, organizations are encouraged to work on the lower level requirements before attempting to achieve higher levels.

4. SECURITY PRACTICES

Security level management is the activity to sustain the security level (decided by owners) by considering operational environments of information systems. So security level management is not the checking of temporary status in a short time but the continuous observation of the variable environment.

To perform security level management, all factors related to the operation of information system should be considered, and by doing so, security of the whole information system can be managed. However due to the limitation occurred by some reasons, all factors can not be managed as the same level. To overcome this problem, selection of important factors should be done first.

4.1 SECURITY MANAGEMENT PART

In this paper, security areas in security management part are divided into 3 groups such as human resource, operation and administration, and physical protection.

Part 1: Security Management Part (SMP)

- SA01 Human Resource
- SA02 Operation and Administration
- SA03 Physical Protection

4.1.1 SA01 Human Resource

Many practices are needed to do security level management. But some practices related to people are very important. Even though some technologies are developed very carefully, these will not be operated in best conditions if operators do not generate or operate them. Even though an organization established a good security process, these will not be kept properly if employees do not follow or stick to them.

Due to hiring, training and education, disposition, and retirement of human resource are being rotated continuously, the level of individual resource can be changed variously. Therefore, the security level of each organization can not be fixed and has the possibility of changing.

By hiring the people of proper level, sustaining their level before retirement, and replacing them with new employees of same capability, organization can manage its security level. This is the objective of this security area.

In SA01 Human Resource, there are 4 security practices

- SP.01.01 Personnel Management
- SP.01.02 Clearance Level
- SP.01.03 Monitoring of Suspicious Action
- SP.01.04 Training and Education

SP.01.01 Personnel Management

Establish personnel management process.

Description

Personnel are managed in accordance with the personnel management plan and operational requirements.

Related Work Products

- personnel management plan
- operational requirements specification
- hired personnel
- record of hire and retirement

Notes

Hire the personnel with proper capability in a timely manner (just-in-time hire). Even though some people move to another position or retire from the organization, security level of the organization should be sustained.

- Procedures of hire, move and retirement should exist to keep the skill level of the employee.
- Personnel management plan can be modified by considering the change of system and environment.
- Before making changes in personnel disposition, security level should be considered.

SP.01.02 Clearance level

Assign and manage required clearance level.

Description

Organization should assign proper clearance level to each position or person. Clearance level is not same with the skill level of employee, and furthermore, has no relationship with position level.

Related Work Products

- personnel management plan

- operational requirements specification

- record of hire and retirement

- clearance level assignment record

Notes

Clearance level is the basic factor of security level management. Based on clearance level, persons can access not only to physical facilities but also to information systems and information.

- Organization doesn't have to build complex clearance level, but should support clearance level system in all areas.

- Clearance level should be assigned to all employees, and can be changed by personnel management plan.

- Change condition and procedure of clearance level should be prepared.

- Organization should keep the clearance level assignment and change records.

SP.01.03 Monitoring of Suspicious Action

Monitor suspicious actions.

Description

Monitor all suspicious or abnormal actions made by personnel. Sometimes a small violation can be connected to harmful situation, even though personnel break the regulation by mistake.

Related Work Products

- record of hire and retirement
- clearance level assignment record
- monitoring report
- sample list of suspicious actions

Notes

Personnel can violate rule or procedure by intention or by mistake, and these unusual behaviors are classified into suspicious actions.

- All kinds of suspicious actions, for example, access to important data or oral disclosure of information should be considered.
- Some suspicious actions are not real threat. But all actions regarded as suspicious can give lesson to organization.
- Organization can adjust clearance level based on suspicious action record.
- By analyzing the trend of suspicious actions, organization can analogize weak point or vulnerability.

SP.01.04 Training and Education

Educate and train personnel to have the skill, knowledge, and sense of responsibility needed to perform their assigned roles.

Description

Personnel are educated and trained in accordance with the education and training plan in personnel management plan.

Related Work Products

- trained personnel
- education and training plan
- personnel management plan
- operational requirements specification

Notes

Offer the education and training in a timely manner to ensure optimal retention and the highest possible skill level.

- A procedure should exist to determine the skill level of the employee prior to receiving the training to determine if the training is appropriate (i.e., if a trainer waiver or equivalent should be administered to the employee).
- A process exists to provide incentives and motivate the personnel to participate in the education and training.
- If it is possible, organization provides online education/training/customized instruction modules.

4.1.2 SA02 OPERATION AND ADMINISTRATION

Small organization can make decision by simple discussion or intuitive estimation. However as the organization becomes bigger, operation or administration by using proper procedure becomes even more important.

It is very difficult to predict when or how security incidents may occur. Therefore, organization should prepare rules and procedures to encounter with incidents, and force employees to follow these. Most incidents may not be solved by physical system only, so organization should consider management system together.

In SA02 Operation and Administration, there are 9 security practices

- SP.02.01 Establishment of Security Role
- SP.02.02 Configuration Management of Security Controls
- SP.02.03 Incident Identification
- SP.02.04 Incident Management
- SP.02.05 Monitoring of Change
- SP.02.06 Security Control Management
- SP.02.07 Common Use of Security Constrains and Considerations
- SP.02.08 Guidance
- SP.02.09 Identification of Laws, Policies, Standards, and External Influences

SP.02.01 Establishment of Security Role

Establish responsibilities and accountability for security roles.

Description

Responsibilities and accountability will be imposed to each security role.

Some aspects of security can be managed within the normal management structure, while others require more specialized management.

The procedures should ensure that those charged with responsibility are made accountable and empowered to act. It should also ensure that whatever security controls are adopted are clear and consistently applied.

Related Work Products

- personnel management plan
- role of position
- education and training plan
- definition and description of security role
- requirements of each security role
- security policy
- incident response procedure

Notes

Management of security role is more efficient than management of each person, because the person in charge (for example, operators or administrator) can be changed more frequently than the role.

- Organization should define and divide security roles and impose responsibilities to them to sustain durability of security even though the person of a role is changed.

- Security role can be modified by considering the change of system and environment.

- Security role should be specified in security policy and incident response procedure.

SP.02.02 Configuration Management of Security Controls

Manage the configuration of security controls.

Description

Security controls are managed by proper procedure, and organization can check the change of controls.

Related Work Products

- security control configuration list
- security control configuration management procedure
- security control implementation
- role of position
- definition and description of security role

Notes

Security controls are base of security level management. Selection and management of security control should be done very carefully. Organization can recommend other documents or standards to select security controls.

Selection, change, and remove of security controls should be recorded and managed.

- Organization selects, change, or remove security controls by proper procedure.
- Security control configuration list can be connected to security role and responsibilities.

SP.02.03 Incident Identification

Identify security relevant incidents.

Description

Determine if a security relevant incident has occurred, identify the details, and make a report if necessary. Security relevant incidents may be detected using not only system information such as historical event data, configuration data, or other system information but also changed environment such as rapid drop of stock value, sudden similar product development of competitor.

Related Work Products

- definition and description of incidents
- history of incident and response
- incident reports
- periodic incident summaries
- security control configuration list
- security control configuration management procedure
- security control implementation
- role of position

Notes

Security incidents can occur in both the system and management environment.

In technical aspect, deliberate technical attacks by hackers or malicious code (viruses, worms, etc.) necessitate a different approach than protection against random events. Analysis of the system configuration and state is required to detect technical attacks.

In managemental aspect, it is more difficult to detect attacks because they are caused by and related to personnel.

Appropriate response plans should be prepared, evaluated and put into action. In many cases uncoordinated responses can make the situation worse.

SP.02.04 Incident Management

Manage the response to security relevant incidents.

Description

Many events cannot be prevented, thus the ability to respond to disruption is essential. A contingency plan requires the identification of the maximum period of non-functionality of the system; the identification of the essential elements of the system for functionality; the identification and development of a recovery strategy and plan; testing of the plan; the maintenance of the plan.

Related Work Products

- periodic evaluation schedule and procedure
- recovery strategy and plan
- definition and description of incidents
- history of incident and response
- incident reports
- security control configuration list
- security control configuration management procedure
- security control implementation
- role of position

Notes

Future events can not be pre-determined, but, unless they are to cause chaos, they must be managed. If the situation falls outside the pre-identified scenarios, it is elevated to the appropriate business management decision level.

SP.02.05 Monitoring of Change

Monitor changes in the environments

Description

Monitor changes that may give any impact to the current security status, regardless of positive or negative.

Security controls should be in relation to the threats, vulnerabilities, impacts and risks as they relate to its environment both internal and external. None of these are static and changes influence both the effectiveness and appropriateness of the security controls.

All must be monitored for change, and the changes analyzed to assess their significance with regard to the effectiveness of the security controls.

Related Work Products

- report of changes
- history of change and countermeasure
- periodic assessment of changes and their impact
- security control configuration list
- security control configuration management procedure
- security control implementation
- role of position

Notes

Changes in systems can be monitored, but changes in management area can be omitted by personnel by mistake or by intention. So it is important to force employees to follow proper procedures correctly.

Both internal and external environments should be examined because they can be connected in many cases. And whenever changes are noted at least one response should be triggered.

SP.02.06 Security Control Management

Manage the security controls to cover necessary changes.

Description

The security status of a organization is subject to change based on the threat environment, operational requirements, and system configuration. Changes are occurred as a necessity, with the consequence that the environment considered is changed, too. Therefore, security controls should be changed to cover necessary changes to sustain security level.

Related Work Products

- history of change and countermeasure
- security control configuration list
- security control configuration management procedure
- security control implementation
- evaluation report of the current security risk environment

Notes

A evaluation of the security status should be conducted in the light of the current operational environment and changes that have occurred. If other events, such as changes, have not triggered a complete evaluation of security, a evaluation should be triggered based on the time since the last evaluation. Time triggered evaluation should be in compliance with appropriate policy and regulations.

The evaluation should lead to a reassessment of the adequacy of current security and the appropriateness of the current level of risk acceptance.

SP.02.07 Common Use of Security Constrains and Considerations

Search, analyze, and share the security constrains and considerations.

Description

The purpose of this practice is to search, analyze, identify, and share all the security constraints and considerations needed to make informed choices. The security engineering group performs analysis to determine any security constraints and considerations on the requirements, design, implementation, configuration, operation, management, and documentation. Constraints may be identified at all times during organization's life. They may be identified at many different levels of abstraction, and can be either positive or negative.

Related Work Products

- list of security constrains and considerations
- analysis report of constrains and considerations
- security implementation rules for security constraints and considerations
- administrator manual
- user manual
- security related guidance

Notes

A major source of the constraints and considerations is the security relevant requirements. These constraints and considerations are used to identify and build security alternatives, and to provide security engineering guidance.

SP.02.08 Guidance

Provide security related guidance.

Description

The purpose of this practice is to develop security related guidance and provide it to the employees. Guidance can be divided into many small ones.

Related Work Products

- administrator manual
- user manual
- security policy
- incident response procedure
- education and train course

Notes

The amount of guidance required and the level of detail depends on the knowledge, experience and familiarity of the other security disciplines. In many cases much of the guidance may relate to the environment rather than the system.

SP.02.09 Identification of Laws, Policies, Standards, and External Influences

Identify the laws, policies, standards, external influences and constraints.

Description

The purpose of this practice is to gather all external influences which affect the security of the organization. Determination of applicability should identify the laws, regulations, policies and standards which govern the target environment of the organization. Determination of precedence between global and local policies should also be performed. Requirements for security placed on the organization must be identified and the security implications extracted.

Related Work Products

- list of security constrains and considerations
- analysis report of constrains and considerations
- security implementation rules for security constraints and considerations
- security environment
- security objectives

Notes

Conflict may occur between laws and regulations that are applicable in different countries and different types of business. As part of the identification process, conflicts should be at a minimum, identified and resolved if possible.

4.1.3 SA03 Physical Protection

This security area, physical protection, contains security practices related to not only the protection of physical space but also protection by using physical resource.

Space used by organization may be divided into several sub-spaces, and each sub-space may be assigned by different security level. Only the person who has the permission can enter the space.

Physical resource does not mean only digital device or equipments should be used. However the history of entrance and exit should be recorded.

In SA03 Physical Protection, there are 3 security practices

- SP.03.01 Secure Zone
- SP.03.02 Physical Security Perimeter Management
- SP.03.03 Classified Materials Storing

SP.03.01 Secure Zone

Establish a secure zone, and manage entrance and exit.

Description

Establish a secure zone, and allow entrance and exit to whom has permission only.

Related Work Products

- secure zone list and map
- entrance and exit procedure
- security level of secure zones
- role of position
- clearance level assignment record

Notes

Regardless of physical area, organization can establish secure zone and assign security level.

To enter the secure zone, personnel should follow entrance and exit procedure, and the personnel or role list related to permission should be prepared.

SP.03.02 Physical Security Perimeter Management

Manage the physical security perimeter.

Description

To check the entrance and exit status, physical security perimeters are prepared and managed.

Related Work Products

- secure zone list and map
- entrance and exit procedure
- security level of secure zones
- role of position
- record of clearance level assignment
- physical security perimeter
- security perimeter passage record

Notes

Only the personnel who have permission can pass physical security perimeter, and to assure this, physical security perimeters should be installed and managed properly. For the secure zone, multiple physical security perimeters can be used. Passage record of physical security perimeter should be managed. This record provides accountability.

- Passage record of physical security perimeter doesn't have to be digital one.
- Physical security perimeter doesn't have to be a digital device.

SP.03.03 Classified Materials Storing

Protect classified materials by securing facilities.

Description

Classified materials should be protected by securing facilities. Organization can select facilities by considering the importance of materials and change of environment.

Related Work Products

- securing facilities
- list of facilities and equipments
- security level of each space
- secure zone list and map
- security level of secure zones
- record of clearance level assignment
- physical security perimeter

Notes

Classified materials are not only digital data but also physical materials. It is better to use securing facilities in secure zone. All facilities should be checked periodically, and can be used as a multi-layer style depending on the importance of materials.

- Classified materials should be stored in security zone, and protected by securing facilities.
- Securing facility doesn't have to be a digital device.

4.2 SECURITY TECHNOLOGY PART

In this paper, security areas in security technology part are divided into 5 groups, such as access control, cryptography, identification and authentication, service assurance, and shielding.

Part 2: Security Technology Part (STP)

- SA04 Access Control Technology
- SA05 Cryptography Technology
- SA06 Identification and Authentication technology
- SA07 Service Assurance Technology
- SA08 Shielding Technology

4.2.1 SA04 ACCESS CONTROL TECHNOLOGY

Access control can be thought of as a "super service" encompassing all security services.

The primary goal of this security area is to prevent unauthorized use, unauthorized disclosure, or modification of data by unauthorized entities. Security practices of this secure area can be used to support other security mechanism.

In SA04 Access Control Technology, there are 2 security practices

- SP.04.01 Access Control
- SP.04.02 Audit

SP.04.01 Access Control

Establish and manage access control technology.

Description

Access control techniques are sometimes categorized as either discretionary or non-discretionary. The three most widely recognized models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC).

DAC is an access policy determined by the owner of an object. The owner decides who is allowed to access the object and what privileges they have.

MAC is an access policy determined by the system, not the owner. MAC is used in multilevel systems that process highly sensitive data, such as classified information.

Role-based access control (RBAC) is an access policy determined by the system, not the owner. RBAC is used in commercial applications and also in military systems, where multi-level security requirements may also exist.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- Discretionary Access Control: Comparable to UNIX permission bits

Notes

RBAC differs from DAC in that DAC allows users to control access to their resources, while in RBAC, access is controlled at the system level, outside of the user's control. Although RBAC is non-discretionary, it can be distinguished from MAC primarily in the way permissions are handled. MAC controls read and write permissions based on a user's clearance level and additional labels. RBAC controls collections of permissions that may include complex operations such as an e-commerce transaction, or may be as simple as read or write. A role in RBAC can be viewed as a set of permissions [62].

SP.04.02 Audit

Implement and manage audit mechanism.

Description

Audit trails (records) and logs can be checked to associate a subject with its actions. The information recorded should be sufficient to map the subject to a controlling user. Audit trails and logs are important for

- Detecting security violations

- Re-creating security incidents

Base Requirements

- Informal reaction mechanism

Notes

If no one is regularly reviewing your logs and they are not maintained in a secure and consistent manner, they may not be admissible as evidence.

When implementing the audit mechanism, the following components should be considered.

- What is being audited and what relevant events are detected.

- How the audit (detected) data is protected, analyzed, and reported.

- What the reaction strategy is to the audit data analysis and reporting.

4.2.2 SA05 Cryptography Technology

This security area contains practices relate to cryptography technology.

Cryptography is the translation of information (known as plaintext) into a coded form (known as cypertext) using a key. Cryptography is mostly used to protect the information (i.e. limit who can access the information).

In a strong cryptosystem, the original information (plaintext) can only be recovered by the use of the decryption key. So the plaintext information is protected from "prying eyes" [63].

Security practices in this area can be considered as the basic requirements.

In SA05 Cryptography Technology, there are 2 security practices

- SP.05.01 Key Length
- SP.05.02 Key Management

SP.05.01 Key Length

Select effective key length to protect information.

Description

After deciding cryptographic algorithm, the effective length of the key should be decided by considering security level. If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- public Key 512 bits

- shared (or symmetric) key 40 bits

Notes

It is recommended to use encryption even though that is a weak one. Because it is better to use weak encryption than not to protect data at all. However it should be notified that a weak encryption system is that it can give organization a false sense of security [64].

SP.05.02 Key Management

Establish and manage key management infrastructure (KMI).

Description

A key management infrastructure is a set of information technology components. In this practice, the KMI performs a set of operations for internal infrastructure needs (allocation of operations, identification and authentication of operators, etc.) and may provide complementary services for users (such as generation of authentication dual keys, or reissue of keys on behalf of users, issuing confidence dates, etc.).

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- SMI Cat X,

- 80+ exponent 512+ modulus public key length,

- 80+ hash key length

Notes

The fact that the KMI complies with documents formalizing a security level according to recognised evaluation criteria (i.e. protection profiles).

Possibly, the legal system used by the infrastructure, if there are any KMI accreditation schemes (for example such as the accreditation of banking certification authorities) [65].

4.2.3 SA06 IDENTIFICATION AND AUTHENTICATION TECHNOLOGY

The security practices in this security area are related to identification and authentication technology.

Identification and authentication technology is required for effective access control. This technology usually includes a process for enabling recognition of an entity and a security measure for establishing the validity of a transmission, message, or originator or verifying an individual's eligibility to receive specific categories of information.

Identification and authentication (I&A) is the process of verifying that an identity is bound to the entity that asserts it. The I&A process assumes that there was an initial vetting of the identity, during which an authenticator was established. Subsequently, the entity asserts an identity together with an authenticator as a means for validation. The only requirements for the identifier is that it must be unique within its security domain. [60][66]

In SA06 Identification and authentication technology, there are 2 security practices

- SP.06.01 Identification

- SP.06.02 Authentication

SP.06.01 Identification

Install and manage identification mechanism.

Description

Identification, or system identification (SID) in particular, is one way in which a system might recognize the entity (which may be a person) requesting authentication.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- unique system identifier (or ID)

Notes

The function of Identification is to map a known quantity to an unknown entity so as to make it known. The known quantity is called the ID and the unknown entity is what needs identification [66].

A basic requirement for identification is that the ID be unique. IDs may be scoped, that is, they are unique only within a particular scope. IDs may also be built out of a collection of quantities such that they are unique on the collective [60].

Biometrics can be used to identify a living person.

SP.06.02 Authentication

Install and manage authentication mechanism.

Description

Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true. Authenticating an object may mean confirming its provenance, whereas authenticating a person often consists of verifying their identity.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- passwords or personal identification numbers (PIN), or challenge/response exchanges

Notes

Human-to-machine authentication could use alphanumeric phrases, like passwords, personal identification numbers (PIN), or challenge, response exchanges that are memorized by a human or used with a token calculator. Physical devices, such as hardware tokens also provide such authentication (e.g., a credit card-type physical entity) [60].

Peer-to-peer authentication can use certificates to identify and authenticate entities. Such certificates are bound to the entity by a cryptographic algorithm, with a digital signature [60].

4.2.4 SA07 SERVICE ASSURANCE TECHNOLOGY

Service assurance has the same mean with availability. To ensure availability of data, the system must employ both preventive and recovery mechanisms.

This security area contains practices related to recovery mechanism, and other security areas contain practices related to preventive mechanism.

Availability is defined as a measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at a random point in time [67].

In SA07 Service Assurance Technology, there are 2 security practices

- SP.07.01 Redundancy

- SP.07.02 Data Recovery

SP.07.01 Redundancy

Consider and implement mechanism to support redundancy.

Description

Redundancy in engineering is the duplication of critical components of a system with the intention of increasing reliability of the system, usually in the case of a backup or fail-safe.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- Bypass channel available

Notes

Redundancy or redundant paths should be available to allow information flow without violating the site security policy. Such information flow might include bypassing any problem areas, including congested servers, hubs, cryptography, and so on [60][68-71].

SP.07.02 Data Recovery

Consider and implement mechanism to provide data recovery.

Description

Data recovery is the process of salvaging data from damaged, failed, corrupted or inaccessible primary storage media when it cannot be accessed normally.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- manual backup system

Notes

Often the data are being salvaged from storage media formats such as hard disk drive, storage tapes, CDs, DVDs, and other electronics [72].

4.2.5 SA08 SHIELDING TECHNOLOGY

This security area contains practices related to physical and electronical shielding technology.

Tampering is the unauthorized modification that alters the proper functioning of an information security device or system in a manner that degrades the security or functionality it provides. Anti-tamper mechanisms detect such alterations [73].

TEMPEST is the investigation, study, and control of compromising emanations from telecommunications and automated information system (AIS) equipment [74].

In SA08 Shielding Technology, there are 2 security practices

- SP.08.01 Anti-tamper
- SP.08.02 TEMPEST

SP.08.01 Anti-tamper

Impede unapproved technology transfer, alteration of system capability, or countermeasure development.

Description

Anti-tamper encompasses the systems engineering activities intended to prevent and/or delay exploitation of critical technologies. These activities involve the entire life-cycle of systems.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- FIPS PUB 140-1 level 2

- ISO/IEC 15408 level 2

Notes

Properly employed, anti-tamper will add longevity to a critical technology by deterring efforts to reverse-engineer, exploit, or develop countermeasures against a system or system component [74].

Anti-tamper is not intended to completely defeat hostile attempts, but it should discourage exploitation, reverse-engineering or make such efforts so time-consuming, difficult, and expensive.

SP.08.02 TEMPEST

Consider and implement mechanism to prevent compromising emanations.

Description

Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose the information transmitted, received, handled, or otherwise processed by any information processing equipment.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- NATO SDIP-27 Level A (formerly AMSG 720B)

- USA NSTISSAM Level I

Notes

Compromising emanations consist of electrical or acoustical energy unintentionally emitted by any of a great number of sources within equipment/systems which process information. This energy may relate to the original message, or information being processed, in such a way that it can lead to recovery of the plaintext [75-76].

5. LEVEL REQUIREMENTS

This chapter contains the level requirements, that is, the requirements should be met to achieve each level, and these requirements can be grouped for SMP and STP. These level requirements are used in a area appraisal to determine the level of any security area. The level requirements are grouped according to level feature and security level. The level requirements are divided into the following security levels, each of which has several level features:

- Security Level 1 - Executed Basically
- Security Level 2 - Verified and Tracked
- Security Level 3 - Quantitatively Controlled
- Security Level 4 - Monitored and Improved

Each level is decomposed into a set of level features that consist of a set of level requirements.

Level requirements are activities that apply to areas, and can address the management, measurement, and institutionalization aspects of each area. In general, level requirements provide guide for security countermeasure and are used during an appraisal to determine if an organization is keeping the guide well.

An organization is generally free to plan, track, define, control, and improve their security level in any way or sequence they choose. However, because some higher level requirements are dependent on lower level requirements, organizations are encouraged to work on the lower level requirements before attempting to achieve higher levels.

5.1 REQUIREMENT OF LEVEL 1 EXECUTED BASICALLY

Security practices of the security area are basically performed. Work products of the security area testify to their performance. Individuals within the organization recognize that an action should be executed, and there is general agreement that this action is executed when required.

This security level comprises the following level features:

- Level feature 1.1 Security Practices in SMP are Performed Informally

- Level feature 1.2 Security Practices in STP are Installed and Managed Properly

5.1.1 Level Feature 1.1 Security Practices in SMP are Performed Informally

The level requirements of this level feature simply ensure that the security practices of the security management part are being performed in some manner. And this level feature can not be applied to the security practices of the security technology part.

Even though formal or well-defined documents are not required, the consistency or performance and the quality of the work products produced are likely to be highly variable. All these materials can be used to upgrade security level.

This level feature comprises the following level requirement (LR):

- LR 1.1.1 Perform Selected Practices

LR 1.1.1 Perform Selected Practices

Description

Perform selected security practices in security management part.

Notes

This level feature may be termed the “informal performance." The customer(s) of the security area may be internal or external to the organization.

5.1.2 Level Feature 1.2 Security Practices in STP are Installed and Managed Properly

The level requirements of this level feature ensure that the security practices of the security technology part are being installed and managed. This level feature can not be applied to the security practices of the security management part.

This level feature comprises the following level requirement:

- LR 1.2.1 Install and manage selected security practices

LR 1.2.1 Install and manage selected security practices

Description

Install and manage selected security practices in security technology part.

Notes

Organization can select proper security practices. But if a practice were selected, this practice should be installed and managed.

5.2 REQUIREMENT OF LEVEL 2 VERIFIED AND TRACKED

In security level 1, informal and basic performance of security practice is enough. However in security level 2, performance of the selected security practices should be verified and tracked according to specified procedures.

Measurement is used to track the performance, thus enabling the organization to manage its activities based on actual performance. The primary distinction from Level 1, Executed Basically, is that the performance is planned, verified, and tracked.

This security level comprises the following level features:

- 2.1 Security Practices in SMP are Verified and Tracked
- 2.2 Security Practices in STP are Installed and Managed Properly

5.2.1 LEVEL FEATURE 2.1 PRACTICES IN SMP ARE VERIFIED AND TRACKED

This level feature is applied to only SMP, and comprises the following level requirements (LR):

- LR 2.1.1 Make a plan
- LR 2.1.2 Follow a plan
- LR 2.1.3 Verify the Performance
- LR 2.1.4 Track the Performance

LR 2.1.1 Make a Plan

Description

This level requirement focuses on the aspects of planning to perform the security practices. Thus the documentation of the security practice, provision of appropriate tools to perform the security practice, planning of the performance of the security practice, training in the performance of the security practice, allocation of resources to the security practice and the assignment of responsibility for the performance of the security practice are all addressed. This level requirement forms an essential foundation for disciplined performance of the security practice.

Action needed

- Allocate adequate resources (including people) to perform the security practice.

- Assign responsibilities to develop the work products and/or provide the services of the security practice.

- Plan the performance of the security area and document it.

Notes

- Participation of the people who perform a security practice (its owners) is essential to creating a usable practice description.

- The resources required can be varied depending upon the practice being performed.

- Plans for security areas in the engineering and project categories may be in the form of a project plan, whereas plans for the organization category may be at the organizational level.

LR 2.1.2 Follow a Plan

Description

This level requirement focuses on the amount of control exercised over the practice. Thus the use of plans for the performance of the security practice, performing the security practice according to standards and procedures, and placing the work products produced by the security practice under configuration management are all addressed. This level requirement forms an important foundation for being able to verify the performance of the security practice.

Action needed

- Use documented plans, standards, and/or procedures in implementing the security area.

- Place work products of the security area under version control or configuration management, as appropriate.

Notes

- Practice measures should be defined in the standards, procedures, and plans.

LR 2.1.3 Verify the Performance

Description

This level requirement focuses on confirming that the security practice has been performed as intended. Thus verification that the security practice was performed in compliance with the applicable standards and procedures, and the auditing of the work products are addressed. This level requirement forms an important foundation for the ability to track the performance of the security practice.

Action needed

- Verify compliance of the security practice with the applicable standards and/or procedures.

- Verify compliance of the work products with the applicable standards and/or requirements.

Notes

- Verification should be done by using the standards, procedures, and plans.

LR 2.1.4 Track the Performance

Description

This level requirement focuses on the ability to control the security practice. Thus tracking the performance of the security practice against a measurable plan, and taking corrective action when the performance of the security practice deviates significantly from that plan are addressed.

Action needed

- Track the status of the security area against the plan using measurement.

- Take corrective action as appropriate when progress varies significantly from that planned.

Notes

- Building a history of measures is a foundation for managing by data, and is begun here.

- Progress may vary because estimates were inaccurate, performance was affected by external factors, or the requirements, on which the plan was based, have changed.

5.2.2 SECURITY PRACTICES IN STP ARE INSTALLED AND MANAGED PROPERLY

This level feature is applied to only STP, and comprises the following level requirement (LR):

- LR 2.2.1 Install and manage security technology requirements

LR 2.2.1 Install and manage security technology requirements

Description

Install and manage selected security practices in security technology part.

Action needed

• Key length [64]:

- Public Key 1,024 bits
- Shared key 40 bits

• Key Management [60][75-77]:

- SMI Cat X
- 80+ exponent 512+ modulus public key length,
- 80+ hash key length

• Anti-tamper [71]:

- FIPS PUB 140-1 level 2
- ISO/IEC 15408 level 2

• TEMPEST [73-74]:

- NATO SDIP-27 Level A
- USA NSTISSAM Level I

• Redundancy [60][78]:

- Backup data path

• Data Recovery [60][78]:

- Formal archive system

- Central backup system

• Identification [60][66]:

- unique system identifier changed periodically

• Authentication [60][66]:

- passwords or personal identification numbers (PIN), or challenge/response exchanges with minimum effective length

- badge, key static token

• Access Control [60]:

- Discretionary access control with access control lists

• Audit [1-3]:

- Semi-automatic reaction mechanism

Notes

• Organization can select proper security practices. But if a practice were selected, this practice should be installed and managed correctly.

5.3 REQUIREMENT OF LEVEL 3 QUANTITATIVELY CONTROLLED

In security level 2, it is enough that performance of the selected security practices are verified and tracked according to specified procedures. But in security level 3, performance of the selected security practices should be quantitatively controlled, according to process.

By collecting and analyzing the evidences of performance, organization can get a quantitative understanding of security level and an improved ability to predict performance [79].

This security level comprises the following level features:

- 3.1 Security Practices in SMP are Measured and Controlled
- 3.2 Security Practices in STP are Installed and Managed Properly

5.3.1 LEVEL FEATURE 3.1 PRACTICES IN SMP ARE MEASURED AND CONTROLLED

This level feature is applied to only SMP, and comprises the following level requirements (LR):

- LR 3.1.1 Define and Perform a Standard Process
- LR 3.1.2 Coordinate Security Practices
- LR 3.1.3 Establish Measurable Goals and Manage Performance

LR 3.1.1 Define and Perform a Standard Process

Description

This level requirement focuses on the institutionalization of a standard process and the repeatable performance of a defined process. Thus the use of the institutionalized process, the review of the results of the process, work products, for defects, and use of data on the performance and results of the process are addressed. This level requirement forms an important foundation to the coordination of security practices.

Action needed

- Document and use a standard process or family of processes for the organization, that describes how to implement the security practices of the security area.

- Perform defect reviews of appropriate work products of the security area.

Notes

- A process can be tailored from the organization's standard process definition.

LR 3.1.2 Coordinate Security Practices

Description

This level requirement focuses on the coordination of activities throughout the organization. Many significant activities are performed by disparate groups within the organization and cooperative groups of outside organizations, therefore, a lack of coordination can cause delays or incomparable results. Thus the coordination of intra-group, inter-group, and external activities are addressed. This level requirement forms an essential foundation to having the ability to quantitatively control processes.

Action needed

- Coordinate communication among the various groups within the organization.

- Coordinate communication with external groups.

Notes

- A coordination among the various groups within the organization addresses the need for an engineering discipline to ensure that decisions with regard to technical issues (e.g. Access Controls) are arrived at through consensus. The commitments, expectations, and responsibilities of the appropriate engineers are documented and agreed upon among those involved. Engineering issues are tracked and resolved.

- A coordination with external groups addresses the needs of external entities that request or require engineering results (e.g., consumers, certification activities, evaluators). A relationship between external groups (e.g., customer, systems security certifier, user) is established via a common understanding of the commitments, expectations, and responsibilities of each activity within an organization.

LR 3.1.3 Establish Measurable Goals and Manage Performance

Description

This level requirement focuses on the establishment of measurable targets for the work products developed by the organization's processes, and determining quantitative measures and making use of them to manage the process.

In this level requirement, the establishing of measurable goals and the using the quantitative measures as a basis for corrective action is addressed. This level requirement forms an essential foundation to having the ability to achieve continuous improvement.

Action needed

- Establish measurable goals for the work products of the organization's standard process family.

- Take corrective action as appropriate when the process is not performing as expected.

Notes

- Special causes of variation, identified based on an understanding of security level, are used to understand when and what kind of corrective action is appropriate.

5.3.2 Security Practices in STP are Installed and Managed Properly

This level feature is applied to only STP, and comprises the following level requirement (LR):

- LR 3.2.1 Install and manage security technology requirements

LR 3.2.1 Install and manage security technology requirements

Description

Install and manage selected security practices in security technology part.

Action needed

- Key length:
  - Public Key 1,568 bits
  - Shared key 90 bits
- Key Management:
  - SMI Cat Y
  - 160+ exponent 1,024+ modulus public key length,
  - 160+ hash key length
- Anti-tamper:
  - FIPS PUB 140-1 level 3
  - ISO/IEC 15408 level 3

- TEMPEST:
  - NATO SDIP-27 Level B
  - USA NSTISSAM Level II
- Redundancy:
  - Hot spare
- Data Recovery:
  - Formal archive system
  - Central backup system
- Identification:
  - Unique and minimum character length system identifier
- Authentication:
  - Memory device
- Access Control:
  - Discretionary access control with access control lists
- Audit:
  - Semi-automatic reaction mechanism

Notes

- Organization can select proper security practices. But if a practice were selected, this practice should be installed and managed correctly.

5.4 REQUIREMENT OF LEVEL 4 MONITORED AND IMPROVED

In security level 3, it is enough that performance of the selected security practices is quantitatively controlled. But in security level 4, performance of the selected security practices should be monitored and improved continuously.

Based on the business goals of the organization, quantitative performance goals for level effectiveness and efficiency are established. And continuous endeavor of improvement against these goals should be enabled by quantitative feedback.

This security level comprises the following level features:

- 4.1 Security Practices in SMP are Monitored and Improved
- 4.2 Security Practices in STP are Installed and Managed Properly

5.4.1 LEVEL FEATURE 4.1 PRACTICES IN SMP ARE MONITORED AND IMPROVED

This level feature is applied to only SMP, and comprises the following level requirements (LR):

- LR 4.1.1 Monitor and Improve Organizational Capability
- LR 4.1.2 Monitor and Improve Effectiveness

LR 4.1.1 Monitor and Improve Organizational Capability

Description

This level requirement focuses on monitoring and improving the use of the standard process throughout the organization. As the process is used, opportunities are sought for enhancing the standard process, and defects produced are analyzed to identify other potential enhancements to the standard process. Thus goals for process effectiveness are established and monitored, improvements to the standard process are identified, and are analyzed for potential changes to the standard process. This level requirement forms an essential foundation to improving process effectiveness.

Action needed

- Establish quantitative goals for monitoring and improving process effectiveness of the standard process family, based on the business goals of the organization and the current capability.

- Continuously improve the process by changing the organization's standard process family to increase its effectiveness.

Notes

- Changes to the organization's standard process family may come from innovations or incremental improvements in technology or the turning of environment.

LR 4.1.2 Monitor and Improve Process Effectiveness

Description

This level requirement focuses making the standard process one that is in a continual state of controlled improvement. Thus eliminating the cause of defects produced by the standard process, and continuously improving the standard process are addressed.

Action needed

- Monitor, analyze, and eliminate the causes of defects in the defined process selectively.

- Continuously improve process performance by changing the defined process to increase its effectiveness.

Notes

- Those who perform the process are typically participants in this analysis. This is a pro-active causal analysis activity as well as re-active.

- Both common causes and special causes of variation are implied in this level requirement, and each type of defect may result in different action.

5.4.2 Security Practices in STP are Installed and Managed Properly

This level feature is applied to only STP, and comprises the following level requirement (LR):

- LR 4.2.1 Install and manage security technology requirements

LR 4.2.1 Install and manage security technology requirements

Description

Install and manage selected security practices in security technology part.

Action needed

- Key length:
  - Stronger than public key 1,568 bits
  - Stronger than shared key 90 bits
- Key Management:
  - SMI Cat Y
  - 160+ exponent 1,024+ modulus public key length,
  - 160+ hash key length
- Anti-tamper:
  - FIPS PUB 140-1 level 4
  - ISO/IEC 15408 level 4
- TEMPEST:
  - NATO SDIP-27 Level C
  - USA NSTISSAM Level III
- Redundancy:
  - Multiple data path

  - Multiple hot spare

- Data Recovery:

  - off-side backup

- Identification:

  - Unique, minimum character length, and minimum distance system identifier

- Authentication:

  - Updated everytime

- Access Control:

  - Mandatory access control system

- Audit:

  - Automatic reaction mechanism

Notes

- Organization can select proper security practices. But if a practice were selected, this practice should be installed and managed correctly.

6. CASE STUDY

In this chapter, application of SLMM to a case was described. Because SLMM consultants considered the target of SLMM as a virtual laboratory and commercial company, it may be difficult to say this result can be applied to real one in same way. But this case study will give enough information about the real application of SLMM to real company, and many people can understand how to use SLMM according to their own environment.

The size of commercial company describe in the case study below may not proper to be considered as real one, but it is enough to provide a guide for SLMM application.

The virtual commercial company considered in this paper is a small size one, and the information related to this company is assumed as like below:

General information of company:

- The company named 'Computer Technology' was established 10 years ago, and is listed in middle standing.

- The total value of assets is about $20,000,000 USD, the total sales per year is about $50,000,000 USD, and the clear profit per year is about $5,000,000 USD.

- The average price of stock in this year is about $20 USD.

- About 200 staffs and employees are working at the department of manage, sales and AS, and research.

- A annex research institute is composed of 2 parts, and 20 researchers are working at each part.

- There are 5~6 competitors in the domestic market, and 30 competitors in the world.

- Domestic market size is about $300,000,000 USD per year, and world market size is about $5,000,000,000 billion USD.

- Total market size is extended rapidly about 10% per year.

- Recently, many large companies are preparing to be included in this market.

- Main target of SLMM is an annex research institute located in external building separately.

Business situation:

- this company threw the news that the success of new projects is coming to the public taking account stock prices.

- Because the possibility of success in the market was estimated very high, so the company got may investment proposals.

- Recently company recognized accidently that competitors organized research teams to develop similar products.

- This company decided to hire more researchers to finish the project as soon as possible and invest more money to marketing aggressively.

- Location of research institute:

- The research institute is located at the center of 6 floor in the 12 storied building.

- At each story, there are 30 research rooms, sized 900 ㎡ (30 meters long and 30 meters wide, and height is 3 meters).

- Back side of research room is blocked by double windows (a thickness of 5 mm), and the distance to nearest building is about 70 meters.

- Windows were fixed, and automatic blinds were installed.

- The wall of each research room is 15 cm cement.

- In the fore side, there is a door sized width 1.5 m and height 2 m. Door is made of wood and divided into 2 pieces.

- Wood door has a thickness of 10 cm.

- At the door, there are two locks and one smart card lock.

Inside of research room:

- In the window side, there are spaces for 2 team leaders, and their spaces are divided by partitions (a thickness of 7 cm).

- In front of the spaces for team leaders, there are spaces for 20 researchers divided by partitions.

- There is one personal computer and 19 inches LCD monitor set on the desk of each researcher.

- There are 5 server systems: 2 servers for projects management, 1 server for printer control, 1 server for DBMS, and 1 server for testing.

- There are 5 CRT monitors connected to each server.

- 2 color laser printers, 1 ink-jet color printer (combined use as like scanner and fax.)

were installed.

- Wire network speed is 100Mbps, and wireless network speed is 54Mbps.

- In research room, 2 switching hubs are working.

- 1 firewall system and 1 IDS system have EAL were connected in the network.

- Anti-virus software was installed in all PCs for researchers.

- Host IDS system was installed in each server.

- Anti-virus system is updating every 1 week, and firewall system and IDS system are updating every 2 weeks.

- 64bit-base crypto technology is applied to the research room.

In/Out information of researchers:

- All researchers including team leaders are working from 9 a.m. to 6 p.m.

- All researchers including two team leaders (A and B) keep their own desk except meetings, holidays and business trips.

- Each researcher has his/her own smart card for the identification, and this card is used as a key, too.

- Each researcher has 2 keys for 2 locks.

- For emergency case, additional keys and smart card key is kept in the guardrooms.

Working information:

- Two software development projects are going on.

- One team leader and 9 researchers are assigned to each project.

- Computer systems of each researcher are in operation during working time.

- Two server systems for project management are working 24 hours.

- One server system for testing is connected to external network and working 24 hours. And some researchers connect to this server at night to check the testing status.

- One database server works 24 hours to provide some data to other system and stores testing results.

- In the morning, researchers start their work after getting data from server systems.

- Some researchers installed remote access control software in their PC to work at outside (when business trip or holiday)

Project information:

- The name of projects developed in these days are January and February.

- At least 3 years are needed to finish each project.

- Project January is in the second year development progress, and project February is in the first year development progress.

- The price of each software developed will be at least $5,000 USD per copy.

- Commercial version of each software is expected to be sold at least 10,000 copies.

- Life cycle of each commercial version is expected as 2 years.

- January is the project to development a software which can build internet shopping site automatically regardless of operating system and database management system.

- February is the project to development a software which can analyze network traffic to provide the expectation about customers' purchase. And in this software, load balancing function is included, too.

- Potential value of technology is expected at least $5,000,000 USD.

- In the market, these technologies are evaluated as upgraded one at least two or more levels

Researchers' information:

- Totally 20 researchers are working at this research room including 2 team leaders.

- Team leader A became a member of this research team after graduating university (his major is related to computer engineering) 9 years ago, and was promoted to team leader last year. There is no problem in home background and personal relationship. He is usually a man of a few words and has a strong sense of responsibility.

- Team leader B moved to this research team after working at marketing team for 8 years. Because her major was business administration, her major roles as a team leader is the analysis of user requirements and quality assurance.

- Each researcher's personal data was managed by managing department.

- All researchers joined this company after graduating university, but some researchers' major is not related to computer or programming area.

- Researcher C is a veteran programmer of 12 years career, and he was formerly a team leader at this research room (before new leader A). He has great capability in program development, but he used to miss the deadlines because he is obsessed with perfect.

- Researcher D is a programmer of 9 years career, joined this company with A together. Because D likes drinking and has very active and free character, he often makes a pleasant atmosphere.

- Researcher E is a programmer of 8 years career, he likes gambling like as a horse race and card game.

- Researcher F is a programmer of 8 years career. Because she is sometimes careless, she used to make some errors ih her source codes.

- Researcher G is a programmer of 7 years career. She is very silent, so she does not make any problem.

- Researcher H is a programmer of 7 years career, and moved to this company 3 years ago from other company. H has great capability in programming, and all his colleagues admit it.

- Researcher I is a programmer of 6 years career, and moved to this company last year because of bankrupt of his own company he established when he graduate university.

- Researcher J is a programmer of 5 years career, and has interesting to investment in stocks and funds.

- Researcher K is a programmer of 4 years career, but other researchers think K needs more career.

- Researcher L is a programmer of 4 years career, and he has no interesting to other things except the works assigned to himself. He dislikes night duty and special duty.

- Researcher M is a designer of 4 years career. Because of a traffic accident, he is wearing a cast in right foot. He likes a baseball very much, sometimes makes a bet at baseball game.

- Researcher N is a designer of 4 years career. Because of a traffic accident with M together, he is wearing a cast in left arm. New baby was born a few weeks ago, so he is trying to move to other company to get more money.

- Researcher O is a tester of 3 years career. He is worrying about the shortage of time for testing.

- Researcher P is a tester of 3 years career. He manifests dissatisfaction about insufficient investment to testing environment construction.

- Researcher Q is a tester of 3 years career. He moved to this company 1 year ago because of bankrupt of former company.

- Researcher R is a tester of 2 years career. His major in university was the fine arts. But he studied computer program at a graduate school.

- Researcher S is a manual writer of 4 years career. He checks development processes always.

- Researcher T is a manual writer of 2 years career. After getting opinions from past users, she is trying to make easy manuals.

6.1 SECURITY LEVEL DECISION

6.1.1 DEFINITION OF THREAT LEVEL

(1) Who is the potential threat agent and what is his capability?

This middle size commercial company develops and sells commercial softwares. The security level management target is a research room located separately in the external building. Potential users of the commercial software developed by this company are other companies or people who are preparing internet based company establishment.

Potential threat agents who can attack this research room can be identified based on [Table 5] like this:

- Nation states: It is rarely possible to apply the softwares developed in this research room to military or political areas. So it is difficult to consider nation states as the potential attacker.

- Hackers: Even though there are 5 servers and 20 PCs in this research room, there are many more easy targets in the world. So it is possible to consider well trained hacker as the attacker, but it is hard to say this hacker will attack this research room to get more computer resources.

- Terrorists/Cyber-terrorists: It is hard to say that the physical attack to destroy system or electronic attack to disable system will be forced to this research room.

- Organized crime/Other Criminal Elements: It is possible some criminals will try to steal the software from the research room and sell it to another company.

- International Press: It is hard to say that international presses have interest to this software. If the presses want it, company will provide enough information about the software to advertise it.

- Industrial Competitors: Industrial Competitors can try to steal this software to extend market share or sustain the competitive power in the market. It is possible industrial competitors will buy the stolen software from criminals or cooperate with criminals to get the software.

- Disgruntled Employees: It is possible some researchers discontented with his position, promotion or salary try to steal the softwares.

- Careless or Poorly Trained Employees: Because of careless actions or conversations, some critical information related to software development project can be drained away.

Therefore, SLMM consultants can consider Organized crime/Other Criminal Elements, Industrial Competitors, Disgruntled Employees, and Careless or Poorly Trained Employees as the potential attackers.

Next stage is capability estimation of potential attackers based on [Table 6]. Some criminals can destroy or disable the research room itself, but this possibility is very low because their objective is stealing the softwares.

Since SLMM consultants can expect easily that potential attackers have the capability to slip in the research room, meaning attackers can steal important information, the SLMM consultants can decide the weight for threat agent and capability identification is 3.

(2) What is the attackers' motivation?

In this case, attackers' motivation is very clear. Motivation is to steal softwares developed in the research room. So SLMM consultants can decide the weight for attackers' motivation is 3.

(3) What is the attack type?

Potential attackers are Organized crime/Other Criminal Elements, Industrial Competitors, Disgruntled Employees, and Careless or Poorly Trained Employees.

- There is no special security countermeasure at the main door of 12 storied building (research room is 6 floor in this building). If someone want to visit research room, security men call any researchers to notify visitors are coming. CCTV cameras are installed at main door, entrance of elevators (between 2 elevators), and the gate of each emergency staircases. Stored CCTV data deleted every 1 SLMM week, and new data are stored again. As there is no restaurant in this building, external food service men deliver dishes to each room in the building frequently. So security men don't control their entrance. Therefore, it is possible attackers slip in the building.

- The back side of research room is walled in from behind by a wide glass; it is possible to spy upon the researchers' monitors. (Because the distance from near building is only 70 meters, highly efficient cameras can capture monitor screens. And electromagnetic signals are leaking out to outside, it is possible to restore data by analyzing these signals.

- There are two locks and one smart card lock at the door, but because all researchers have their own keys, someone may miss their keys.

- Because there is no separate space for visitors, visitors can enter to research room freely and connect to internal wireless networks. Therefore, visitors can send some internal information or data.

- There is no CCTV camera at the door, and there is no camera in the research room. So it is impossible to monitor internal researchers' action.

- Each researcher can see other researchers' monitors and works easily because the height of partitions is too low. And each researcher can check other researchers' work from the server.

- Each researcher can make domestic and international phone call freely, and the conversations by telephone are not monitored. Each researcher can send fax messages to anyone (domestic and international) freely without any restriction. Some researchers installed and use messenger program on their own PC. All researchers have cell phone and use it freely in the room (can send MMS and photos, access to web for finding or sending information). Researchers can access internet mail system and send or receive a attachment maximum 10 megabyte. So it is possible to send out important information.

- According to the rule, researchers' working time is from 9 a.m. to 6 p.m. but some researchers come to office at 8 a.m. and stay by 9 p.m. to do internet surfing. All researchers' PCs are connected to internet, it is possible attackers access to researchers PCs or servers passing through researchers' PCs to steal critical information.

- Some researchers are discontented with their position, omission from promotion, or wage-freeze policy. As some researchers think their wages are too small, it is possible to yield to temptations of scout proposal and divulgement of secret.

- USB drive ports and DVD R/W are attached in each PC, and DVD disks are distributed to each researcher for back-up freely. However, there is no method to control the leakage of DVD and USB from the research room.

- Some researchers installed a remote control program in their PC to work on vacation or business trip. Accesses from external terminal like this are accepted to provide work convenience.

As there are many attack methods SLMM consultants can not expect, SLMM consultants are able to assume attackers have capability to infiltrate into research room (physically or electronically).

Important thing is that SLMM consultants have deeply identified the attackers' motivation is to steal softwares. So SLMM consultants can expect attackers will do something active. Therefore, weight for attack type can be decided based on [Table 10] as 5.

(4) Can attackers access to information systems?

SLMM consultants should consider about the access to information system not information itself. This is because, in these days, information is managed and stored by information systems as a digital file, not physical documents.

Important information consists of many data. So even if someone may flow out the data he knows, these data are just fragments. On the other hand, if someone has access to information systems and find data, these can be really important data.

- Unauthorized access: If an attacker accessed an information system, according to the privilege of the account cracked, the attacker can obtain information. Access means not physical but electronic, so even though attacker entered into the research room, this does not mean access for the attacker if attacker can not log-on to the system.

- Establishment of unauthorized connection: A temporary unauthorized access to information system and establishment of unauthorized connection path are not the same. The latter means attacker can access the system again later when he want, and will steal the information continuously.

- Disability: After stealing important information, attackers can disable the system.

Attackers may intrude into the research room or examine the inside of the room or access to the system via networks. If the attacker is a insider, he will access to the systems directly. In any case, if attackers try to compromise information system actively with obvious motivation, the risk will be increased.

Since insufficient amount of security countermeasures are implemented (only firewall systems, IDS, and anti-virus software), and the update cycles of these security products are too slow, attackers can establish unauthorized access channel to information system via networks.

If attackers have access to physical system directly or insiders may be changed to attackers, it will be more easy to install malicious softwares. By using these softwares, attackers will access to information systems continuously and freely.

Therefore, the weight for access is 4 based on [Table 14].

(5) What are the tools and equipments can be used?

Performance of tools and equipments improved in proportion to price. It is a problem if someone download hacking tool from the web and use it carelessly, but it will be bigger problem if someone modify this tool according to the characteristics of the targets.

Fortunately, it is very difficult to optimize hacking tools and prepare expensive computer equipments because much money and high technology will be needed to meet these requirements.

Originally tools and equipments are different things. But in these days, well trained hackers can make and control many zombies systems and thus overcome the lack of high performance equipments.

- Basic or well known: Many tools, books and knowledge sources are available already. Someone may attack the system by using these well known materials.

- Specializing: Someone may merge tools well known to make their own specialized methods, tools and equipments. It is possible to use zombie systems to maximize the effect.

- Optimizing: Someone may modify the source code of tools and optimize it according to the characteristics of target. They will use sufficient equipment.

Based on this classification, SLMM consultants can expect attackers may have at least specialized tools and equipments. So the weight for tools and equipments can be 4 from [Table 15].

(6) How long will the security countermeasures withstand an attack?

Information systems contain important information can be attacked, and if there may be no proper countermove, systems will be compromised.

Regardless of physical access or network access, final countermeasure about these attacks is the security mechanisms. The total time before all security mechanisms are disabled is the 'elapsed time'. If the elapsed time is short, this means there may be no enough time to cope with the situation; otherwise long elapsed time means the security mechanisms implemented are strong enough to defend information systems.

- Because the update cycle of firewall and IDS which are protect networks of research room is too long, it is impossible to say these systems can protect information systems well.

- Because crypto systems were established by using 64 bit, it is very hard to say this is enough to protect information systems well.

- Because some researchers play online games, messenger and investment in stocks by using their business PC, softwares that have no relationship with research are installed. Therefore, it is possible malicious codes are downloaded and installed.

- Test server connected to external network has the function of bypassing security systems to provide high performance. So this test server can be in a defenseless state.

- Researchers have some problems (did not be promoted, discontented for their low salary, were in dept) may try to access information systems to steal important information.

If attackers attack the information system in this research room by using modified tools and nice equipments, it will be compromised in a few hours because of weak security countermeasures. So the weight can be 5 from [Table 6].

(7) Additional weight for interrelation

When SLMM consultants calculate the security level, after considering current environments and correlation between weight factors, they can append some more weights.

- Potential value of softwares developed in this research room may be over ten million dollars by considering market size, competition status, stock prices and research investment.

- Therefore attackers will invest millions dollars to steal these softwares.

- Attackers have clear motivation, and will prepare good tools and equipments by using enough funds. Alternately, attackers can find assistants among the inside researchers.

- So 2 can be appended as the additional weights.

(8) Decision of threat level

From the equation (7), threat level can be decided:

Ex = 3 for threat agent and capability identification

+ 3 for attackers' motivation

+ 5 for attack type

+ 4 for access to information system

+ 4 for tools and equipments

+ 5 for elapsed time

+ 2 for correlation

= 26

Based on the total value 26, threat level can be decided as TL5 from [Table 18].

Threat level 5 has the meanings: first, attackers can destroy IS, and second, attackers can control IS.

The former one means attackers can destroy information systems itself (not only physical destruction but also electrical disability are included in this scope). And this means attackers can paralyze the whole business continuity by making information systems disable after stealing important information.

The latter one means attackers make information systems as zombie. This means attackers can control information systems freely and will steal information continuously without any problem.

In any case, TL5 means information systems are in the serious status immediate complementary measures are needed.

6.1.2 DEFINITION OF ASSET LEVEL

In risk management process, an estimation method of the impact of successful attack has been used. However the information the SLMM consultants can provide is related only to security, so the information related to economics should be provided by economists. In other words, SLMM consultants do not evaluate the asset value or level.

It is not good idea to open business information to economists to evaluate asset value. The only subject who can grasp the point about business loss is the owner of assets.

If SLMM consultants have enough knowledge about economics, there may be no problem, but it is better to get assistance from specialists to decide the asset level.

Let's consider next items as the data provided by economic specialists:

- The softwares developed in this research room have similar value to annual sales of this company, and after development it is expect to wide a technical gap among competitors.

- Based on the success, it is expected the domestic market shares can be extended to about 30%, and international market shares can be extended to about 10%.

- Based on the success, it is expected this company can monopolize a market at least a year.

- Based on the success, it is expected stock prices go up rapidly and net profits increase to double.

- If the core technology were leaked, financial loss can be estimated as millions of dollars including three years' amount invested. In particular, if a competitor obtains this technology and launches similar products to the market at an early stage, this company will be at a crisis.

- Because this company is having a conference with investors after announcing the final release is near at hand, leakage of core information may break all agreements

Owners should consider all information collectively before making decision. As a matter of course, SLMM consultants are able to provide the information about security countermeasures they should implement after deciding asset levels.

Let's consider that owner decided asset level:

- Level 1: This is a level selected when owners think the threat level is not critical and their assets can be protected by current security countermeasures, or owners think the company will not be damaged by theft of information.

But this level is not applicable at the current state.

- Level 2: This is a level owners decide to invest some money to upgrade security countermeasures: security education or training for researchers, upgrade of some security products, making up for the weak points in access control.

- Level 3: This is a level owners can invest much money to upgrade security countermeasures: hiring security specialists, installing additional CCTV, attaching bio-metric access control devices, replacement of old type security products, getting a separate space for visitors, prohibition of private phone or network access, blocking of electromagnetic signal leakage, control of portable storage, changing of crypto mechanism to 128 bit base.

- To keep the assets, owners will do everything. However company is trying to hire new researchers to finish the projects on time, and advertising these new softwares on a large scale by mass media. So now the financial state is not good enough to invest much money.

According to this basis for judgment, owners select AL3 from the [Table 19] first, and will upgrade to AL4 next time.

6.1.3 Definition of Security Level

Because threat level and asset level were decided, it is possible to decide security level from [Table 21]. Security level needed in this research room is SL3 like [Table 22].

Table 22 Security Level for Research Room

Asset level	Threat Level				
	TL1	TL2	TL3	TL4	**TL5**
AL1	**SL1**	**SL1**	**SL1**	**SL1**	**SL1**
AL2	**SL1**	**SL1**	**SL1**	**SL2**	**SL2**
AL3	**SL1**	**SL1**	**SL2**	**SL3**	**SL3**
AL4	**SL1**	**SL2**	**SL3**	**SL3**	**SL4**

In SL3, there are two kinds of level features, one for security management part, and the other for security technology part:

Security Level 3: Quantitatively Controlled

• 3.1 Security Practices in SMP are Measured and Controlled

• 3.2 Security Practices in STP are Installed and Managed Properly

6.2 SELECTION OF SECURITY PRACTICES

6.2.1 SECURITY MANAGEMENT PART

SLMM consultants can summarize some possible security management practices as like next [Table 23].

To perform the security level management for SL3, all managemental practices related to the operation of information system should be considered. All the practices in [Table 23] can be selected.

However in this case study, only one SA, 'Human Resource' will be selected, and only one SP 'Personnel Management' from this SA will be selected for explanation.

Table 23 Summary of Security Management Practices

Security Area	Security Practice
Human Resource	Personnel Management
	Clearance Level
	Monitoring of Suspicious Action
	Training and Education
Operation & Administration	Establishment of Security Role
	Configuration Management of Security Controls
	Incident Identification

	Incident Management
	Monitoring of Change
	Security Control Management
	Common Use of Security Constrains and Considerations
	Guidance
	Identification of Laws, Policies, Standards, and External Influences
Physical Protection	Secure Zone
	Physical Security Perimeter Management
	Classified Materials Storing

The reason why SLMM consultants selected this SP is because this practice is related to researchers themselves. Researchers are the main target of security level management. Researchers should get security clearance according to their position and role, and complete security education and training. Researchers' doubtful actions should be monitored continuously.

6.2.2 Security Technology Part

SLMM consultants can summarize some possible security technology practices as like next [Table 24].

Table 24 Summary of Security Technology Practices

SA	SP
Access Control Technology	Access Control
	Audit
Cryptography Technology	Key Length
	Key Management
Identification and Authentication technology	Identification
	Authentication
Service Assurance Technology	Redundancy
	Data Recovery
Shielding Technology	Anti-tamper
	TEMPEST

Originally, all security practices in [Table 24] should be selected, but in this case study, only one SA, 'Cryptography Technology' will be selected. Therefore, 3 security practices will be selected as like [Table 25].

Table 25 Selected Security Practice

SA	SP
Human Resource	Personnel Management
Cryptography Technology	Key Length
	Key Management

6.3 CHECKING OF SL3 REQUIREMENTS

In security level 3, performance of the selected security practices should be quantitatively controlled. By collecting and analyzing the evidences of performance, organization can acquire the quantitative understanding of security level and an improved ability to predict performance.

This security level contains the following level features:

- Security Practices in SMP are Measured and Controlled

- Security Practices in STP are Installed and Managed Properly

To be SL3, all selected security practices should satisfy LP 3.1 and LP 3.2. To satisfy LP 3.1, all selected security practices should satisfy LR 3.1.1, LR 3.1.2, and LR 3.1.3.

And to satisfy LP 3.2, all selected security practices should satisfy LR 3.2.1. Next [Figure 5] is the summary of these things. To be SL3, 5 areas in [Figure 5] should be satisfied (1, 2, and 3 for management part, 4 and 5 for technology part).

Satisfying LR does not mean 100% perfect satisfaction. To satisfy LR more clearly, owners should invest additional money. So the LR is the final objective of investment, and can be satisfied gradually.

SLMM consultants should provide the information which part is not enough yet, but they cannot force owners to invest their money.

<table>
<tr><td rowspan="3">LF 3.1</td><td>LR 3.1.1</td><td>1</td><td>...</td><td>...</td><td>...</td><td></td><td></td></tr>
<tr><td>LR 3.1.2</td><td>2</td><td>...</td><td>...</td><td>...</td><td></td><td></td></tr>
<tr><td>LR 3.1.3</td><td>3</td><td>...</td><td>...</td><td>...</td><td></td><td></td></tr>
<tr><td>LF 3.2</td><td>LR 3.2.1</td><td></td><td></td><td></td><td></td><td>4</td><td>5</td></tr>
<tr><td colspan="2" rowspan="4">Level Dimension
(Level Features of SL3)</td><td>SP.01.01</td><td>SP.01.02</td><td>SP.01.03</td><td>SP.01.04</td><td>SP.05.01</td><td>SP.05.02</td></tr>
<tr><td colspan="4">SA01</td><td colspan="2">SA05</td></tr>
<tr><td colspan="4">SMP</td><td colspan="2">STP</td></tr>
<tr><td colspan="6">Area Dimension - (Security Practices Selected)</td></tr>
</table>

Figure 5 Security Practices and Level Requirements

6.3.1 Level Feature for Management Part

Management level feature is applied to only SMP, and contains the following level requirements (LR):

- LR 3.1.1 Define and Perform a Standard Process

- LR 3.1.2 Coordinate Security Practices
- LR 3.1.3 Establish Measurable Goals and Manage Performance

To be SL3, all these LRs should be satisfied.

6.3.1.1 SP.01.01 - LR 3.1.1

Core actions to satisfy LR 3.1.1 are documentation and usage of standard process or family of processes. By documentation and standardization, staffs react in the same way about the same event.

At the former stage of documentation and standardization, reactions to the events are different and intuitive. So the consistent management is very difficult, and it is hard to expect easily how the people will react.

Security practice SP.01.01 is related to personnel management, and contains the next 4 main work products.

- personnel management plan
- operational requirements specification
- hired personnel
- record of hire and retirement

There are many kinds of work products (sometimes a memo, an order or an incorporeity). Even though work product is an incorporeity, this is not a big problem. However the management will be hard, obviously.

'Record of hire and retirement' contains history of hire and retire, and 'personnel management plan' expresses where a person worked at any department, what education and training courses he passed, and what his examination mark was.

Brief record, for example, he joined the company on Dec. 1, 2008 and moved to another company on Jan. 15, 2009 can be a kind of work product. But this brief record may not give enough information about his relation to security incidents.

To meet the requirement of LR 3.1.1 for SP.01.01, whole things related to personnel management should be documented and standardized. In other words, all things mentioned in SP.01.01 should be documented, standardized, and managed.

For example, let's consider new researcher employment processes of a company.

In the processes, next things may be included: request for new researchers from research team, confirmation of finance team, announcement for new employment, evaluation from management team, education and training for new researchers, work assignment to new researchers, and so on. These all processes should be documented, standardized, and managed.

By checking all information about the researchers (where a researcher worked, what his characteristics are, what his interesting is, what his work is, and so on), it is possible to predict potential security incidents related to this person.

6.3.1.2 SP.01.01 - LR 3.1.2

Core actions to satisfy LR 3.1.2 are the coordination of activities throughout the organization. Many significant activities are performed by disparate groups within the organization and cooperative groups of outside organizations, therefore, a lack of coordination can cause delays or incomparable results. Thus the coordination of intra-group, inter-group, and external activities should be addressed.

To meet the requirement of LR 3.1.2 for SP.01.01, communication among the various groups within the organization and communication with external groups should be coordinated.

Because the focus is related to personnel management, the coordination of intra-group, inter-group, and external activities for personnel management should be addressed. If it is enough to meet the requirement of LR 3.1.2 only, any kind of coordination is acceptable, for example, oral contract or agreement is possible.

On the other hand as previously stated, to meet the requirements of LR 3.1.1, all things related to personal management should be documented, standardized, and managed. To meet the requirements of LR 3.1.1 and LR 3.1.2 together, communication among the various groups within the organization and communication with external groups for personnel management should be documented, standardized, and managed, too.

Let's consider the new researcher employment processes again.

In the employment processes, many kinds of coordination of intra-group, inter-group, and external activities should be addressed: coordination between research team and finance team, coordination between advertising team and finance team, coordination among training team, research team, finance team, external review team, and external education team, and so on.

All these things should be documented, standardized, and managed, too.

6.3.1.3 SP.01.01 - LR 3.1.3

Core actions to satisfy LR 3.1.3 are establishment of measurable goals for the work products and taking of correct action as appropriate.

It is possible to evaluate and correct objectives only in the case of using quantitative objectives. So the objective "all researchers should get CISA certificate" is better than "all researchers should have enough knowledge about security". To achieve objectives, standard processes can be modified.

Let's consider the new researcher employment processes one more time.

To meet the requirements of LR 3.1.1, LR 3.1.2, and LR 3.1.3 together, for example, it is possible to make objective as like: Based on the documented and standardized process, training team, research team, finance team, external review team, and external education team should cooperate to make all researchers be able to obtain CISA certificate in one year.

This is an example. So SLMM consultants should provide proper guidelines by considering the environment of the company.

6.3.2 Level Feature for Technology Part

This level feature related to technology contains only one level requirement (LR):

- LR 3.2.1 Install and manage security technology requirements

To meet the technical requirements of SL3, only LR 3.2.1 should be satisfied.

Because two security practices (key length and key management) were selected, next requirements should be satisfied.

- Key length:
  - Public Key 1,568 bits
  - Shared key 90 bits
- Key Management:
  - SMI Cat Y
  - 160+ exponent 1,024+ modulus public key length,
  - 160+ hash key length

6.4 SUMMARY OF CASE STUDY

In this case study, small size research room was considered to apply SLMM.

All information related to research room, researchers and projects developed are assumed, and general level security countermeasures were assumed, too.

However to apply SLMM to real company, more detail information should be checked.

In this case study, only basic information was considered to decide threat level. To decide threat level in a real situation, all information from personnel to whole systems should be checked.

Asset level definition should be done by owners. SLMM consultants should provide threat information to owners, and after getting the result of asset level from owners, the decision about the security level should be made with the owner's input.

After deciding the security level, SAs and SPs should be selected. It is not a good idea to select too many SPs. To implement SP, owners should invest money. So SLMM must consultants provide enough information to owners to select proper SPs (Owners can append more SPs later).

After deciding security practices, LPs should be implemented. As each LP is described as a general purpose expression, SLMM consultant should modify it.

The most important factor is continuous management; because many factors in security environment are changed continuously, threat level and asset level will also be changed. Therefore, security level should be managed continuously.

7. FUTURE WORK

In this thesis, security level decision method and security level management model were proposed. This approach is different from other international standard such as SPICE and SSE-CMM, and applicable to most information system environments.

The SLMM architecture is designed to provide a guide to maintain the security level of information system. The goal of the architecture is to provide characteristics of the security countermeasures that should be implemented to keep information system.

However to apply this SLMM to information systems, employees of organization should first be educated to know the basic principles of security engineering and software engineering. This is a very difficult pre-condition to meet, since all employees are always very busy.

To avoid this problem, even though an organization forms a team to take full charge in security level management, it is still important to make all team members have knowledge in similar level.

To help the organizations that wish to use the SLMM, resources such as manuals, guidances, procedures, appraisal methodologies and training programs, and so on, are needed. By using these materials, organizations can use and apply SLMM easily to protect their information systems.

So in the near future, researches related to SLMM manuals, guidances, procedures, appraisal methodologies, training programs should be started.

To apply SLMM to real system, it is better to follow the method ISO/IEC 15408 (CC, Common Criteria) used. Because CC contains very specialized knowledge, the staffs in charge of each company are confronted by difficulties for misunderstanding. So each country operates education center and publishes some handbooks for employees, university students, and common people.

The scope of SLMM is wider than CC, we will try to draw up many kinds of guidances, methodologies, and case studies. And finally, we will develop education programs and automatic tools. By using these tools, the staffs in company can get their security level and necessary security countermeasures automatically after inserting some information.

REFERENCES

[1] ISO/IEC 15408, Common Criteria, Part 1, version 3.1, http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

[2] ISO/IEC 15408, Common Criteria, Part 2, version 3.1, http://www.commoncriteriaportal.org/public/files/CCPART2V3.1R1.pdf

[3] ISO/IEC 15408, Common Criteria, Part 3, version 3.1, http://www.commoncriteriaportal.org/public/files/CCPART3V3.1R1.pdf

[4] ITU-T X.1051, "Information Security Management Systems - Requirements for Telecommunications", 2004

[5] ISO 14001, "Environmental Management Systems - Specification with Guidance for Use", 1996

[6] ISO/IEC 17799, "Information Technology - Code of Practice for Information Security Management", 2000

[7] BS7799-2, "Information Security Management Systems - Specification with Guidance for Use", 2002

[8] ISO/IEC TR 19791, "Information Technology - Security Techniques - Security Assessment of Operational Systems", 2005

[9] ISO/IEC 21827 SSE-CMM, http://www.sse-cmm.org/index.html

[10] Tai-Hoon Kim, Myong-chul Shin, Sang-ho Kim, Jae Sang Cha: Security Requirements for Software Development. KES (Knowledge-Based Intelligent Information and Engineering Systems) 2004: LNAI 3215, 116-122

[11] Tai-Hoon Kim, Seung-youn Lee: Design Procedure of IT Systems Security Countermeasures. ICCSA (Computational Science and Its Applications) 2005: LNCS 3481, 468-473

[12] Tai-Hoon Kim, Seung-youn Lee: Intelligent Method for Building Security Countermeasures by Applying Dr. T.H. Kim's Block Model. KES (Knowledge-Based Intelligent Information and Engineering Systems) 2005: LNCS 3682, 1069-1075

[13] Tai-Hoon Kim, Seung-youn Lee: A Relationship Between Products Evaluation and IT Systems Assurance. KES (Knowledge-Based Intelligent Information and Engineering Systems) 2005: LNCS 3681, 1125-1130

[14] http://www.sei.cmu.edu/cmm/

[15] DoD Directive 5000.1, "The Defense Acquisition System", 2000

[16] DoD Directive 5200.40, "DoD IT Security Certification and Accreditation Process (DITSCAP), 1997

[17] DoD Directive 8500.1, "Information Assurance", 2002

[18] DoD Directive 8500.2, "Information Assurance Implementation", 2003

[19] Tai-Hoon Kim, Seung-youn Lee: Security Evaluation Targets for Enhancement of IT Systems Assurance. ICCSA (Computational Science and Its Applications) 2005: LNCS 3481, 491-498

[20] Tai-Hoon Kim, Chang-hwa Hong, Myoung-sub Kim: Towards New Areas of Security Engineering. RSFDGrC (Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing) 2005: LNCS 3642, 568-574

[21] http://www.commoncriteriaportal.org/public/files/CEMV3.1R1.pdf

[22] National Security Institute - 5200.28-STD Trusted Computer System Evaluation Criteria (TCSEC)

[23] AEDI CAYSER http://www.aedi.es/asp/ACYS-0001.asp

[24] AICPA Generally Accepted Privacy Principles, http://infotech.aicpa.org/Resources/Privacy/Generally+

[25] AS/NZS 4360, http://www.riskmanagement.com.au/

[26] Business Process Improvement, http://en.wikipedia.org/wiki/Business_Process_

[27] CERT OCTAVE, http://www.cert.org/octave/

[28] CIS, http://www.cisecurity.org/

[29] CLUSIF MEHARI http://www.clusif.asso.fr

[30] CRAMM, http://www.cramm.com/

[31] EBIOS, http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html

[32] ISACA CISA, http://www.isaca.org/

[33] ISACA CISM, http://www.isaca.org

[34] ISECOM OSSTMM, http://www.isecom.org/

[35] ISC2 CISSP, http://www.isc2.org/

[36] ISO 544R, http://www.iso.org/

[37] ISO 15228, http://www.iso.org/

[38] ISSA GAISP

[39] MAP MAGERIT, http://www.csi.map.es/csi/pg5m20.htm

[40] NIST RBAC, http://csrc.nist.gov/rbac/

[41] NSA, http://www.nsa.gov/snac

[42] Motorola Six Sigma http://www.motorola.com/motorolauniversity.jsp

[43] OIS SVRRP, http://www.oisafety.org/

[44] OWASP, http://www.owasp.org/

[45] SEI P-CMM, http://www.sei.cmu.edu/cmm-p/

[46] http://en.wikipedia.org/wiki/TCSEC

[47] "Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonised Criteria". Document COM(90) 314, Version 1.2. Commission of the European Communities, June 1991

[48] http://en.wikipedia.org/wiki/ITSEC

[49] http://csrc.nist.gov/cryptval/

[50] http://csrc.nist.gov/cryptval/140-2.htm

[51] http://www.sei.cmu.edu/cmmi/faq/his-faq.html

[52] http://www.isospice.com/

[53] http://www.sei.cmu.edu/cmmi/general/general.html

[54] http://www.automotivespice.com/

[55] http://www.12207.com

[56] ISO/IEC 12207:1995, Information technology - Software life cycle processes

[57] http://iso-17799.safemode.org/

[58] http://en.wikipedia.org/wiki/ISMS

[59] http://www.ism3.com/index.php

[60] http://www.iatf.net

[61] http://www.cs.purdue.edu/coast/intrusion-detection/

[62] http://en.wikipedia.org/wiki/Access_Control#Access_Control_Techniques

[63] http://www.boran.com/security/IT1x-7.html#Heading86

[64] http://www.boran.com/security/IT1x-7.html#Heading90

[65] http://www.ssi.gouv.fr/en/faq/faq_igc.html#1161

[66] http://www.boran.com/security/IT1x-7.html#Heading111

[67] DOD3235.1H Test & Evaluation of System Reliability, Availability, and Maintainability—A Primer , March 1982. 287 Pages

[68]http://www.eventhelix.com/RealtimeMantra/FaultHandling/reliability_availability_basics.htm

[69]http://www.ev60enthelix.com/RealtimeMantra/FaultHandling/system_reliability_availability.htm

[70] http://www.barringer1.com/mil_files/DOD3235.1-H.pdf

[71] UK-DefStan00-43-Part1-Issue1, Reliability And Maintainability Assurance Activity Part 1: In-Service Reliability Demonstrations, January 1993

[72] http://www.at.dod.mil/index.htm

[73] http://en.wikipedia.org/wiki/TEMPEST#TEMPEST_measurement_standards

[74] http://web.archive.org/web/20070408221244/cryptome.org/tempest-2-95.htm

[75] FIPS PUB 171, Key Management Using ANSI X9.17

[76] FIPS PUB 140-1, Security Requirements for Cryptographic Modules

[77] http://www.ssi.gouv.fr/en/faq/faq_igc.html#1180

[78] http://www.boran.com/security/IT1x-7.html#Heading130

[79] http://www.antimoon.com/forum/2004/5487.htm

APPENDIX KEY ABBREVIATION LIST

AIS	Automated Information System
AL	Asset Level
BSI	British Standards Institute
CC	Common Criteria
CEM	Common Evaluation Methodology
CMMI	Capability Maturity Model Integration
CMT	Cryptographic Modules Testing
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
DAC	Discretionary Access Control
DoD	Department of Defense
DTI	Department of Trade and Industry
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
I&A	Identification and Authentication
IA	Information Assurance
IDS	Intrusion Detection Systems

IPD-CMM	The Integrated Product Development Capability Maturity Model
IS	Information System
ISM3	Information Security Management Maturity Model
ISMS	Information Security Management System
ITSEC	Information Technology Security Evaluation Criteria
KMI	Key Management Infrastructure
LAN	Local Area Networks
LF	Level Feature
LR	Level Requirement
MAC	Mandatory Access Control
NCSC	National Computer Security Center
NDIA	National Defense Industrial Association
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
SoD	Secretary of Defense
PA	Process Areas
PDCA	Plan-Do-Check-Act
PIN	Personal Identification Numbers
RBAC	Role Based Access Control

SA	Security Area
SE-CMM	The System Engineering Capability Model
SEI	Software Engineering Institute
SID	System Identification
SL	Security Level
SLM2	Security Level Management Model
SLMM	Security Level Management Model
SMP	Security Management Part
SP	Security Practices
SPICE	Software Process Improvement Capability dEtermination
SSE-CMM	System Security Engineering-Capability Maturity Model
STP	Security Technology Part
SW-CMM	Capability Maturity Model for Software
TCSEC	Trusted Computer Security Evaluation Criteria
TL	Threat Level

ACKNOWLEDGEMENT

I should express my appreciation to many people, and hope I have not missed anyone in this brief acknowledgement message. First and foremost, I would like to express my special thanks to my supervisor, Professor B. H. Kang. Without his patience and encouragement, I could not finish this thesis.

I also owe a great deal of appreciation to Professor Byung-joo Park, Seok-soo Kim, and all other Professors of Hannam University, Professor Dae-sik Ko, Yun-ho Kim and Hea-jou Kang of Mokwon University, Professor Haeng-kon Kim of Catholic University of Daegu, and Prof. Yang-sun Lee of Seokyeong University.

Finally, I must also thank my families for providing the motivation and encouragement over the course of my researching.

PUBLISHED PAPERS

Aneel Rahim, Fahad T. Bin Muhaya, Muhammad Sher and Tai-hoon Kim: Validation of Secure Broadcast Framework using VANETs. Information, Vol.14, No.1, January, 2011, pp.151-156. (SCIE, Corresponding Author)

Debnath Bhattacharyya, Tai-hoon Kim, Kheyali Mitra and Samir K Bandyopadhyay: Information Management in Wireless Mobile Sensor Network. Information, Vol.14, No.1, January, 2011, pp.167-178. (SCIE, Corresponding Author)

Tai-Hoon Kim, Debnath Bhattacharyya, Samir Kumar Bandyopadhyay: Supervised chromosome clustering and image classification. Future Generation Comp. Syst. 27(4): 372-376 (2011) (SCIE, Corresponding Author)

(Editorial) Ruay-Shiung Chang, Tai-Hoon Kim: Special Section: Future Generation Information Technology. Future Generation Comp. Syst. 27(4): 370-371 (2011) (SCIE, Corresponding Author)

Tai-hoon Kim: A Non-Secure Information Systems and the Isolation Solution. INTERNATIONAL JOURNAL OF COMPUTERS: Vol.5 No.1, 50-57, 2011

Debnath Bhattacharyya, Tai-hoon Kim: Vehicle Track Control. INTERNATIONAL JOURNAL OF COMPUTERS: Vol.5 No.1, 123-131, 2011

Debnath Bhattacharyya, Tai-hoon Kim and Subhajit Pal: A Comparative Study of Wireless Sensor Networks and Their Routing Protocols, Sensors, Volume 10, Issue 10 (October 2010), Pages 10507-10523 (SCIE, Corresponding Author)

Aneel Rahim, Zeeshan Shafi Khan, Fahad T. Bin Muhaya, Muhammad Sher and Tai-Hoon Kim: Sensor Based Framework for Secure Multimedia Communication in

VANET, Sensors, Volume 10, Issue 10 (October 2010), Pages 10146-10154 (SCIE, Corresponding Author)

Shivali Goel, Jemal H. Abawajy and Tai-hoon Kim: Performance Analysis of Receive Diversity in Wireless Sensor Networks over GBSBE Models. Sensors, Volume 10, Issue 10 (October 2010), Pages 11021-11037 (SCIE, Corresponding Author)

Hak-Man Kim, Tetsuo Kinoshita, Yujin Lim and Tai-Hoon Kim: A Bankruptcy Problem Approach to Load-shedding in Multiagent-based Microgrid Operation, Sensors, Volume 10, Issue 10 (October 2010), Pages 8888-8898 (SCIE, Co-author)

Zhao Wu, Naixue Xiong, Jong Hyuk Park, Tai-Hoon Kim, Lei Yuan: A Simulation Model Supporting Time and Non-time Metrics for Web Service Composition. Comput. J. 53(2): 219-233 (2010) (SCIE, Co-author)

Naixue Xiong, Jing He, Yan Yang, Yanxiang He, Tai-Hoon Kim, Chuan Lin: A Survey on Decentralized Flocking Schemes for a Set of Autonomous Mobile Robots (Invited Paper). JCM 5(1): 31-38 (2010) (SCIE, Co-author)

Tai-hoon Kim: Diffusing RFID-Sensor Networks and Security Threats. WSEAS TRANSACTIONS on SIGNAL PROCESSING, Issue 4, Volume 6, 133-144, October 2010 (SCOPUS, Corresponding Author)

Tai-hoon Kim: Dissolving Active Networks Privacy Threats and Vulnerabilities. WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 8, Volume 9, 473-484, August 2010 (SCOPUS, Corresponding Author)

Farkhod Alsiherov, Taihoon Kim: Research Trend on Secure SCADA Network Technology and Methods. WSEAS TRANSACTIONS on SYSTEMS and CONTROL, Issue 8, Volume 5, 635-645, August 2010 (SCOPUS, Corresponding Author)

Tai-hoon Kim: SCADA Architecture with Mobile Remote Components. WSEAS TRANSACTIONS on SYSTEMS and CONTROL, Issue 8, Volume 5, 611-622, August 2010 (SCOPUS, Corresponding Author)

Tai-hoon Kim: Weather Condition Double Checking in Internet SCADA Environment. WSEAS TRANSACTIONS on SYSTEMS and CONTROL, Issue 8, Volume 5, 623-634, August 2010 (SCOPUS, Corresponding Author)

Rosslin John Robles and Tai-hoon Kim: Review: Context Aware Tools for Smart Home Development. International Journal of Smart Home, Vol.4, No.1, 11-11, January, 2010

Randy S. Tolentino and Tai-hoon Kim: Review: Distributed System Network Architecture for Securing SCADA system. International Journal of Smart Home, Vol.4, No.1, 13-22, January, 2010

Maricel O. Balitanas and Taihoon Kim: Review: Security Threats for RFID-Sensor Network Anti-Collision Protocol. International Journal of Smart Home, Vol.4, No.1, 23-36, January, 2010

Uttam Kumar Dash, Debnath Bhattacharyya, Tai-hoon Kim: Advisory for Securing Different Assets of an Organization. International Journal of Smart Home, Vol.4, No.1, 37-56, January, 2010

Maricel O. Balitanas and Taihoon Kim: Architecture for Automatic Management of ParcTab Ubiquitous Computing. International Journal of Advanced Science and Technology, Vol. 15, 1-12, February, 2010

Rosslin John Robles and Tai-hoon Kim: A Review on Security in Smart Home Development. International Journal of Advanced Science and Technology, Vol. 15, 13-22, February, 2010

Maricel O. Balitanas and Taihoon Kim: Using Incentives for Heterogeneous peer-to-peer Network. International Journal of Advanced Science and Technology, Vol. 15, 23-36, February, 2010

Rosslin John Robles and Tai-hoon Kim: Applications, Systems and Methods in Smart Home Technology: A Review. International Journal of Advanced Science and Technology, Vol. 15, 37-47, February, 2010

Sumana Barman, Amit Kumar Samanta, Tai-hoon Kim and Debnath Bhattacharyya: International Journal of Advanced Science and Technology, Vol. 15, 49-62, February, 2010

T K Ghosh, Debnath Bhattacharyya, Tai-hoon Kim: Gas Hold-up Characteristics of an External Loop Airlift Contactor. International Journal of Hybrid Information Technology, 25-32, Vol.3, No.2, April, 2010

Debnath Bhattacharyya, Susmita Biswas, Tai-hoon Kim: Emerging Approach of Natural Language Processing in Opinion Mining: A Review. International Journal of Multimedia and Ubiquitous Engineering, Vol. 5, No. 2, 39-45, April, 2010

Jayanta Kumar Basu, Debnath Bhattacharyya, Tai-hoon Kim: Use of Artificial Neural Network in Pattern Recognition. International Journal of Software Engineering and Its Applications, Vol. 4, No. 2, 23-33, April 2010

Debnath Bhattacharyya, Susmita Biswas, Tai-hoon Kim: A Review on Natural Language Processing in Opinion Mining. International Journal of Smart Home, Vol.4, No.2, 31-38, April, 2010

Hoon Ko, Jongmyung Choi, Maricel O. Balitanas, Tai-hoon Kim and Carlos Ramos: A Study on Secure Contents Using in Intelligent Urban Computing. International Journal of Smart Home, Vol.4, No.2, 39-48, April, 2010

Timir Maitra, Anindya J Pal, Debnath Bhattacharyya and Tai-hoon Kim: Noise Reduction in VLSI Circuits using Modified GA Based Graph Coloring. International Journal of Control and Automation, Vol. 3, No. 2, 37-44, June, 2010

Biman Ray, Anindya J Pal, Debnath Bhattacharyya and Tai-hoon Kim: An Efficient GA with Multipoint Guided Mutation for Graph Coloring Problems. International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 3, No. 2, 51-58, June, 2010

Shilpi Saha, Debnath Bhattacharyya, Tai-hoon Kim and Samir Kumar Bandyopadhyay: Model Based Threat and Vulnerability Analysis of E-Governance Systems. International Journal of u- and e- Service, Science and Technology, Vol. 3, No. 2, June, 2010

Debnath Bhattacharyya, Pallabi Chakraborty, Farkhod Alisherov, Tai-hoon Kim: Quantum Watermarking: A Review. International Journal of Security and Its Applications, Vol. 4, No. 3, 46-54, July, 2010

Debashis Ganguly, Srabonti Chakraborty, Tai-hoon Kim: A Cognitive Study on Medical Imaging. International Journal of Bio-Science and Bio-Technology, Vol. 3, No. 3, 1-18, September, 2010

T.K. Ghosh, Shounak Banerjee, C.B. Majumder and Tai-hoon Kim: Comparison of modified airlift reactor with conventional airlift reactor. International Journal of Control and Automation, Vol. 3, No. 3, 25-39, September, 2010

Timir Maitra, Anindya J. Pal, Tai-hoon Kim, Debnath Bhattacharyya: Hybridization of Genetic Algorithm with Bitstream Neurons for Graph Coloring. International Journal of u- and e- Service, Science and Technology, Vol. 3, No. 3, 37-53, September, 2010

Samit Biswas, Tai-hoon Kim, Debnath Bhattacharyya: Features Extraction and Verification of Signature Image using Clustering Technique. International Journal of Smart Home, Vol.4, No.3, 43-55, July, 2010

(Editorial) Tai-Hoon Kim, Wai-Chi Fang: Special section: Grid/distributed computing systems security. Future Generation Comp. Syst. 25(3): 351 (2009) (SCIE, Corresponding Author)

Chuan Lin, Naixue Xiong, Jong Hyuk Park, Tai-Hoon Kim: Dynamic power management in new architecture of wireless sensor networks. Int. J. Communication Systems 22(6): 671-693 (2009) (SCIE, Co-author)

Binod Vaidya, Tai-Hoon Kim, Jong Hyuk Park, Young Jae Lee: Secure ubiquitous connectivity in hybrid multipath wireless ad hoc network. Int. J. Communication Systems 22(9): 1153-1176 (2009) (SCIE, Co-author)

Rodrigo Fernandes de Mello, Rudinei Goularte, Evgueni Dodonov, Laurence Tianruo Yang, Jong Hyuk Park, Tai-Hoon Kim: On modeling and evaluating multicomputer transcoding architectures for live-video streams. Multimedia Tools Appl. 43(2): 109-129 (2009) (SCIE, Co-author)

Tai-hoon Kim and Kouichi Sakurai: Case Study - SLMM Application. International Journal of Advanced Science and Technology, Vol. 2, 1-16, January, 2009

Rosslin John Robles, Min-kyu Choi, Sung-Eon Cho, Yang-seon Lee, Tai-hoon Kim: SOX and its effects on IT Security Governance. International Journal of Smart Home, Vol. 3, No. 1, 81-87, January, 2009

Poulami Das, Debnath Bhattacharyya, Samir Kumar Bandyopadhyay, Tai-hoon Kim: Person Identification through IRIS Recognition. International Journal of Security and its Applications, Vol. 3, No. 1, 129-147, January, 2009

Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay and Tai-hoon Kim: Text Steganography: A Novel Approach. International Journal of Advanced Science and Technology, Vol. 3, 79-86, February, 2009

P. Calduwel Newton, Dr. L. Arockiam, Dr. E. George Dharma Prakash Raj, R. Hari Prasath and Tai-hoon Kim: A Refined Algorithm for Efficient Route Identification in Future Generation Networks, International Journal of Advanced Science and Technology, Vol. 3, 49-57, February, 2009

P. Calduwel Newton, L. Arockiam, Tai-hoon Kim: An Efficient Hybrid Path Selection Algorithm for an Integrated Network Environment. International Journal of Database Theory and Application, Vol. 3, No. 1, 31-38, March, 2009

Manpreet Singh, Manjeet Singh Patterh, Tai-hoon Kim: A Formal Policy Oriented Access Control Model for Secure Enterprise Network Environment. International Journal of Security and Its Applications, Vol. 3, No. 2, 1-14, April, 2009

Debnath Bhattacharyya, Arpita Roy, Pranab Roy and Tai-hoon Kim: Receiver Compatible Data Hiding in Color Image. International Journal of Advanced Science and Technology, Volume 6, 15-23, May, 2009

Poulami Dutta, Debnath Bhattacharyya and Tai-hoon Kim: Data Hiding in Audio Signal: A Review. International Journal of Database Theory and Application, Vol. 2, No. 2, 1-8, June 2009

Poulami Das, Debnath Bhattacharyya, Samir K. Bandyopadhyay and Tai-hoon Kim: Analysis and Diagnosis of Breast Cancer. International Journal of u- and e- Service, Science and Technology, Vol. 2, No. 3, 1-12, September, 2009

Kheyali Mitra, Debnath Bhattacharyya, Sattarova Feruza Y. and Tai-hoon Kim: A Heuristic Approach for Mobile Phone Bases Information Management System in Wireless Sensor Network. International Journal of of Grid and Distributed Computing, Vol.2, No.3, 1-11, September, 2009

Praveen Ranjan Srivastava and Tai-hoon Kim: Application of Genetic Algorithm in Software Testing. International Journal of Software Engineering and Its Applications, Vol. 3, No.4, 87-96, October 2009

Sattarova Feruza Y. and Tai-hoon Kim: Review on YCrCb color space optimization, TV images compression, Algorithm of Signals Sources Isolation and Optical Fiber. International Journal of Smart Home, Vol.3, No.4, 43-62, October, 2009

Govardhanan Kousalya, P. Narayanasamy, Jong Hyuk Park, Tai-Hoon Kim: Predictive handoff mechanism with real-time mobility tracking in a campus wide wireless network considering ITS. Computer Communications 31(12): 2781-2789 (2008) (SCIE, Co-author)

Deok-Gyu Lee, Jong Hyuk Park, Tai-Hoon Kim, Laurence Tianruo Yang: U-multimedia framework: a secure and intelligent multimedia service framework based on context information in U-home. The Journal of Supercomputing 45(1): 88-104 (2008) (SCIE, Co-author)

Dong-Joo Kanga, Balho H. Kimb and Tai-hoon Kim: GAME THEORY APPLICATION TO PROBLEM SOLVING IN ELECTRIC POWER INDUSTRY – STRATEGIC BIDDING IN ELECTRICITY MARKET AND CYBER SECURITY OF SCADA COMMUNICATION. International Journal of Mathematics, Volume 18, Number 2, pp. 63-93, 2008

LI Hong-qi, LI Li, XIE Shao-long, Tai-hoon Kim: An Improved PSO-based of Harmony Search for Complicated Optimization Problems. International Journal of Hybrid Information Technology, Vol.1, No.3, 91-98, July, 2008

DUSART Pierre, SAUVERON Damien, Tai-hoon Kim: Some limits of Common Criteria certification, International Journal of Security and Its Applications, Vol.2, No.4, 11-19, October, 2008

Tai-Hoon Kim, Hojjat Adeli: Advances in Computer Science and Information Technology, AST/UCMA/ISA/ACN 2010 Conferences, Miyazaki, Japan, June 23-25, 2010. Joint Proceedings Springer 2010

Tai-Hoon Kim, Young-Hoon Lee, Byeong Ho Kang, Dominik Slezak: Future Generation Information Technology - Second International Conference, FGIT 2010, Jeju Island, Korea, December 13-15, 2010. Proceedings Springer 2010

Debnath Bhattacharyya, Arup Kumar Bhaumik, Minkyu Choi, Tai-Hoon Kim: Directed Graph Pattern Synthesis in LSB Technique on Video Steganography. AST/UCMA/ISA/ACN 2010: 61-69

Gladys Benigni, Osvaldo Gervasi, Francesco Luca Passeri, Tai-Hoon Kim: USABAGILE_Web: A Web Agile Usability Approach for Web Site Design. ICCSA (2) 2010: 422-431

Jong Hyuk Park, Hsiao-Hwa Chen, Mohammed Atiquzzaman, Changhoon Lee, Tai-Hoon Kim, Sang-Soo Yeo: Advances in Information Security and Assurance, Third International Conference and Workshops, ISA 2009, Seoul, Korea, June 25-27, 2009. Proceedings Springer 2009

Young-Hoon Lee, Tai-Hoon Kim, Wai-Chi Fang, Dominik Slezak: Future Generation Information Technology, First International Conference, FGIT 2009, Jeju Island, Korea, December 10-12, 2009. Proceedings Springer 2009

Maricel O. Balitanas, Rosslin John Robles, Nayoun Kim, Tai-Hoon Kim: Crossed Crypto-Scheme in WPA PSK Mode. BLISS 2009: 102-106

Feruza Sattarova Yusufovna, Farkhod Alisherov Alisherovich, Minkyu Choi, Eun-suk Cho, Furkhat Tadjibayev Abdurashidovich, Tai-Hoon Kim: Research on Critical Infrastructures and Critical Information Infrastructures. BLISS 2009: 97-101

Debnath Bhattacharyya, Debasri Chakraborty, Tai-Hoon Kim: Effective GIS Mobile Query System. FGIT 2009: 129-137

Debnath Bhattacharyya, Jhuma Dutta, Poulami Das, Rathit Bandyopadhyay, Samir Kumar Bandyopadhyay, Tai-Hoon Kim: Discrete Fourier Transformation based Image Authentication technique. IEEE ICCI 2009: 196-200

Yuanyuan Zeng, Naixue Xiong, Tai-Hoon Kim: Channel assignment and scheduling in multichannel wireless sensor networks. LCN 2008: 512-513

Deqing Zou, Jong Hyuk Park, Laurence Tianruo Yang, Zhensong Liao, Tai-Hoon Kim: A Formal Framework for Expressing Trust Negotiation in the Ubiquitous Computing Environment. UIC 2008: 35-45

Naixue Xiong, Hongyan Li, Tai-Hoon Kim, Laurence Tianruo Yang: An Approach on Adaptive Time-Delay Estimate and Compensation Control in Internet-Based Control Systems. FGCN (1) 2008: 116-121

INDEX