International Journal of Multimedia and Ubiquitous Engineering
Vol. 3, No. 1, January 2008

A study on Security Level Management Model Description

Tai-Hoon Kim
Dept. of Multimedia, Hannam University, Daejeon, Korea
taihoonn@hnu.ac.kr

Kouichi Sakurai
Dept. of Computer Science & Communication Engineering, Kyushu University, Japan
sakurai@csce.kyushu-u.ac.jp

Abstract

Security level decision is a basic activity for developing and managing of safe information systems, and core factor which can affect the investment for security countermeasures. According to the security level of IS, where and how the security countermeasures are implemented, which security policies are selected, and who will manage them are able to be decided. But more important thing than level decision is the management of level decided. And in this model, we proposed a new model to manage security level of IS.

1. SLMM Architecture Description

SLM^2 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.

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.

In this paper, we proposed SLMM to manage security level of IS efficiently and effectively.

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 1 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 should be implemented to keep an organization's security level.

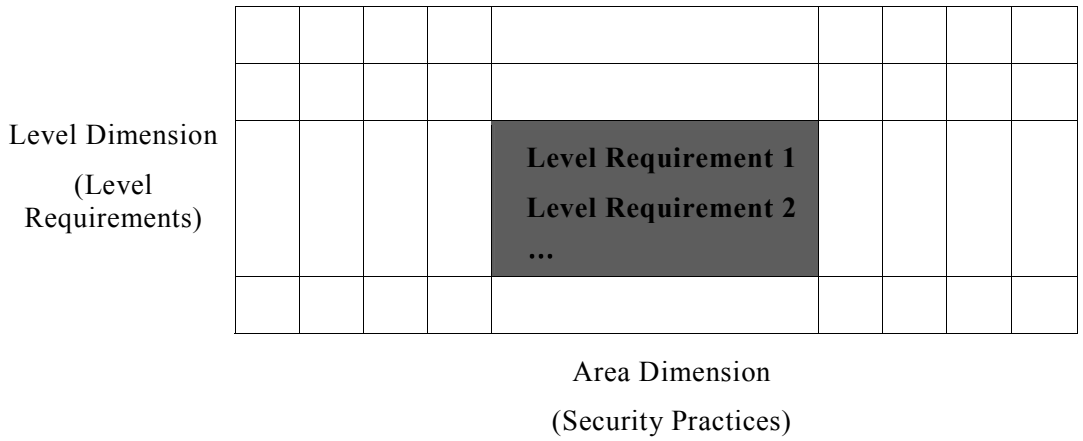

Fig.1 Relationship between security practices and level requirements

After deciding 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. 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 like 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 there the security areas are ordered by lifecycle phase.

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

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.

5. Security Practices

Security level management is the activity to sustain the security level which defined as an essential one by considering operational environments of information systems [1-4]. So security level management is not the check of temporary status in short time but the continuous observation to the variable environment.

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

5.1. 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

5.2. 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

6. 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 keeps 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.

6.1. 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 as and 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

6.2. Requirement of Level 2 Verified and Tracked

In security level 1, informal and basic performance of security practice is enough. But 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

6.3. 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 [5].

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

6.4. Requirement of Level 4 Monitored and Improved

In security level 3, it is enough that performance of the selected security practices are 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

7. Conclusion and Future Work

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.

But to apply this SLMM to information system, employees of organization should be educated to know basic principles of security engineering and software engineering first.

Because this is a very difficult pre-condition to meet, because all employees are very busy always.

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

In this paper, unfortunately, we could not propose the list of security practices and level requirements. But the list of core security practices and level requirements will be published in near future.

8. References

[1] FIPS PUB 171, Key Management Using ANSI X9.17
[2] FIPS PUB 140-1, Security Requirements for Cryptographic Modules
[3] http://www.ssi.gouv.fr/en/faq/faq_igc.html#1180
[4] http://www.boran.com/security/IT1x-7.html#Heading130
[5] http://www.antimoon.com/forum/2004/5487.htm
[6] Jones, C.D., A.B. Smith, and E.F. Roberts, Book Title, Publisher, Location, Date.
[7] http://www.cs.purdue.edu/coast/intrusion-detection/
[8] http://en.wikipedia.org/wiki/Access_Control#Access_Control_Techniques