# Security Countermeasure Design for Information Systems by Using Block Model

**Tai-hoon Kim and Kouich Sakurai**
Dept. of Computer Science and Communication Engineering, Kyushu University
e-mail : taihoonn@empal.com and sakurai@csce.kyushu-u.ac.jp

**Abstract** Because the networks and systems become more complex, the implementation of the security countermeasures becomes more critical consideration. The designers and developers of the security policy should recognize the importance of building security countermeasures by using both technical and non-technical methods, such as personnel and operational facts. Security countermeasures may be made for formulating an effective overall security solution to address threats at all layers of the information infrastructure. This paper uses the security engineering principles for determining appropriate security countermeasures. This paper proposes a method for building security countermeasures by modeling and dividing IT systems and security components into some blocks.

**Keyword**: Block Model, Security Engineering, Security Countermeasure

## 1. Introduction

When we design general or some special IT systems, we may provide a framework for the assessment of quality or security characteristics by considering some approaches and methods. And this framework can be used by organizations involved in planning, monitoring, controlling, and improving the acquisition, supply, development, operation, evolution and support of IT systems.

In the general cases, security countermeasures for IT systems are implemented in buying and installing some security products such as Firewall, IDS and Anti-virus systems. But the scope of IT systems is being extended and the security holes are increased. Most of the threat agents' primary goals may fall into three categories: unauthorized access, unauthorized modification or destruction of important information, and denial of authorized access. Though any cases are occurred, the compromise of IT system may be connected to loss of money or job. Therefore, Security countermeasures must be implemented to prevent threat agents from successfully achieving these goals [1-4].

This paper proposes a method for building security countermeasures by modeling and dividing IT systems and security components into some blocks. In facts, IT systems are very complex and consist of very many components. So we can't help dividing IT systems into some parts. And we categorize security components into some groups.

Security countermeasures should be considered with consideration of applicable threats and security solutions deployed to support appropriate security services and objectives. Our Block model may be used to make security countermeasures in any cases. Because the size of each block expresses parts insufficient in security.

## 2. Dividing IT Systems

Implementation of any security countermeasure may require economic support. If your security countermeasures are not sufficient to prevent the threats, the existence of the countermeasures is not a real countermeasure and just considered as like waste. If your security countermeasures are built over the real risks you have, maybe you are wasting your economic resources.

First step is the division of IT systems into some parts (See Fig.1). In this paper, we divide IT systems into 4 parts. But we think this partition is not perfect one and we are now researching about that.

Each part may have three common components such as Technique, Product, and Operation and Personnel.

Next step is construction of block matrix by using the parts of IT systems and common components we mentioned above (See the Fig. 2).

Each cross point area of Fig.2 may be generalized and reduced into Block and matrix of Fig.3. Each Block may mean the area require security countermeasures or security method.

Next step is determination of security assurance level of IT systems. Security assurance level is related to the robustness. In the concept of our Block model, all cross point area should be protected by security countermeasures.

Robustness is connected to the level or strength of security countermeasures and this idea is expressed like as Fig.4. The last step may be building security countermeasures by using Block Region.

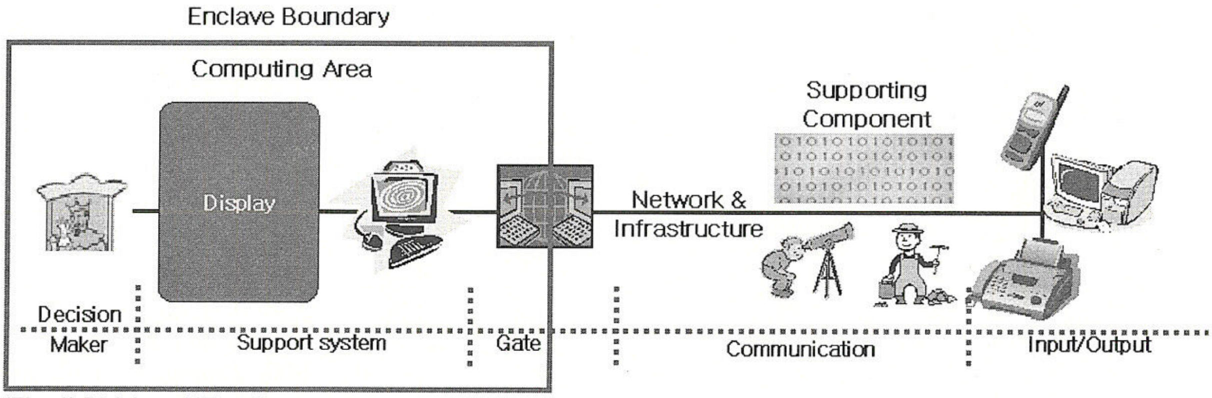
This block matrix can be applied to information engineering and system engineering. Next is the sample applied to design security countermeasures for IT systems.

## 3. Design Flow of IT Systems Security Countermeasures

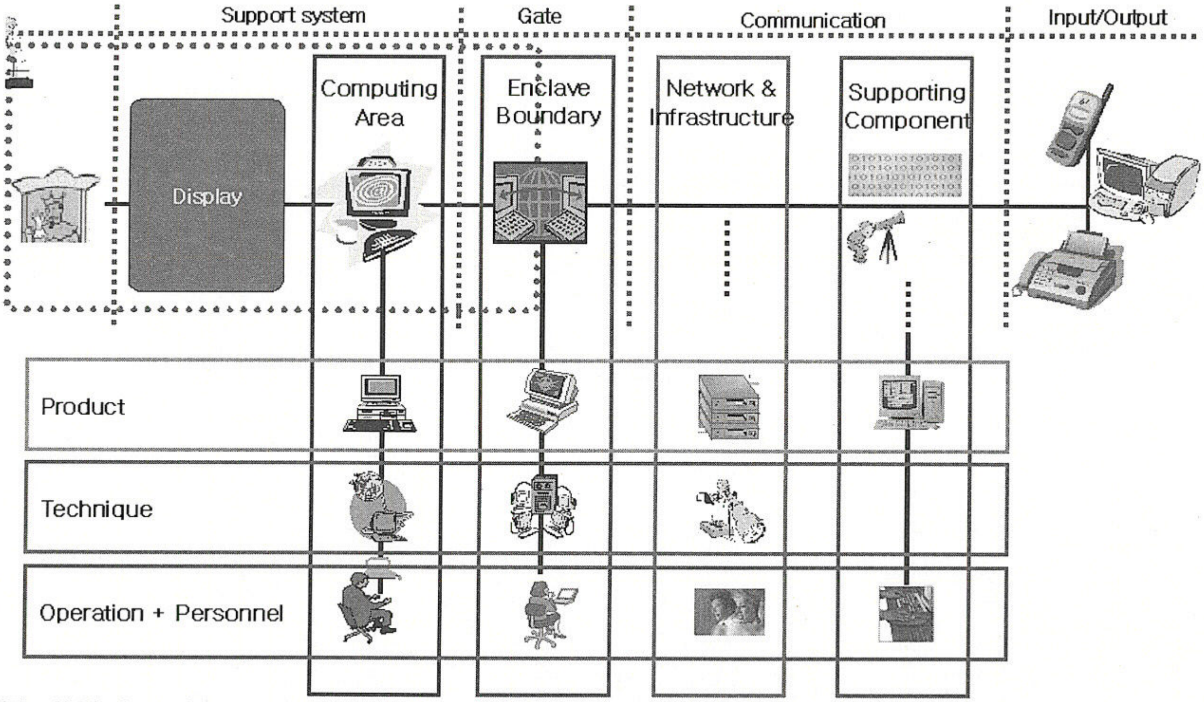
We published a design method for IT systems security countermeasures a few months ago. In that model, we identified some components we should consider for building security countermeasures. In fact, the Procedure we proposed is not perfect one yet, and the researches for improving are going on.

The discussion of the need to view strength of mechanisms from an overall system security solution perspective is also relevant to level of assurance.

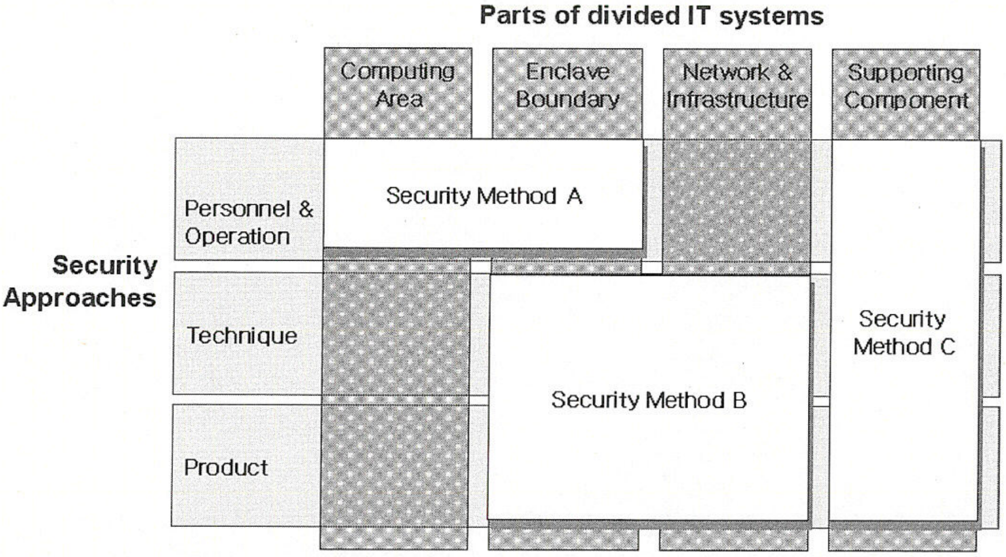
While an underlying methodology is offered by a number of ways, a real solution (or security product) can only be deemed effective after a detailed review and analysis that consider the specific operational conditions and threat situations and the system context for the solution.



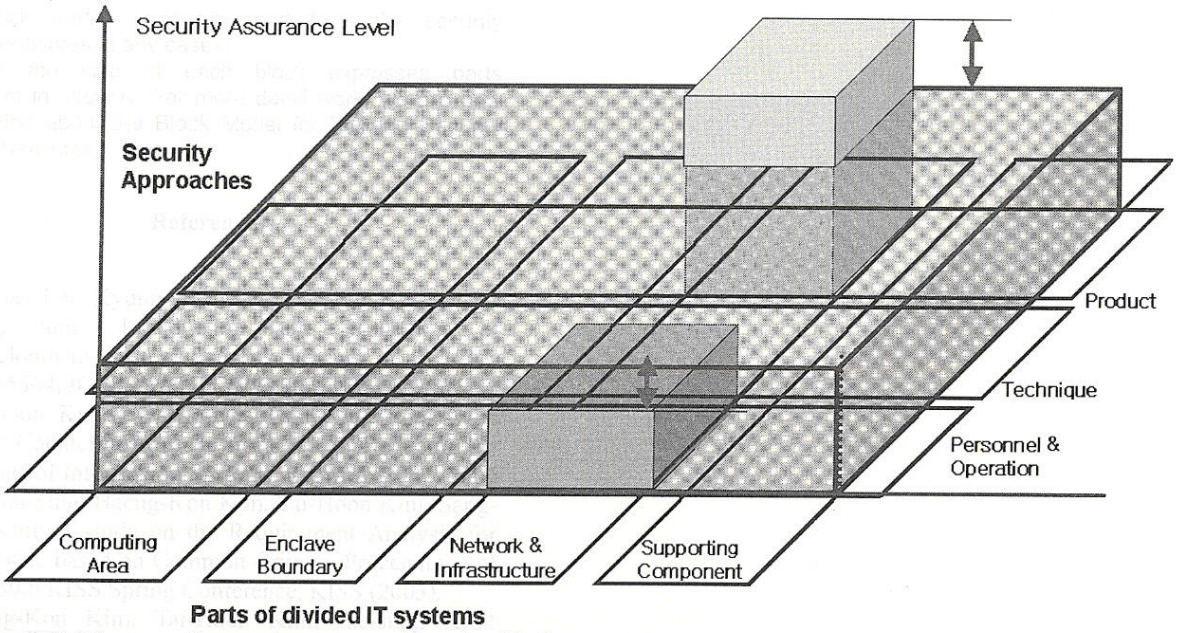
**(Fig. 1)** Division of IT systems



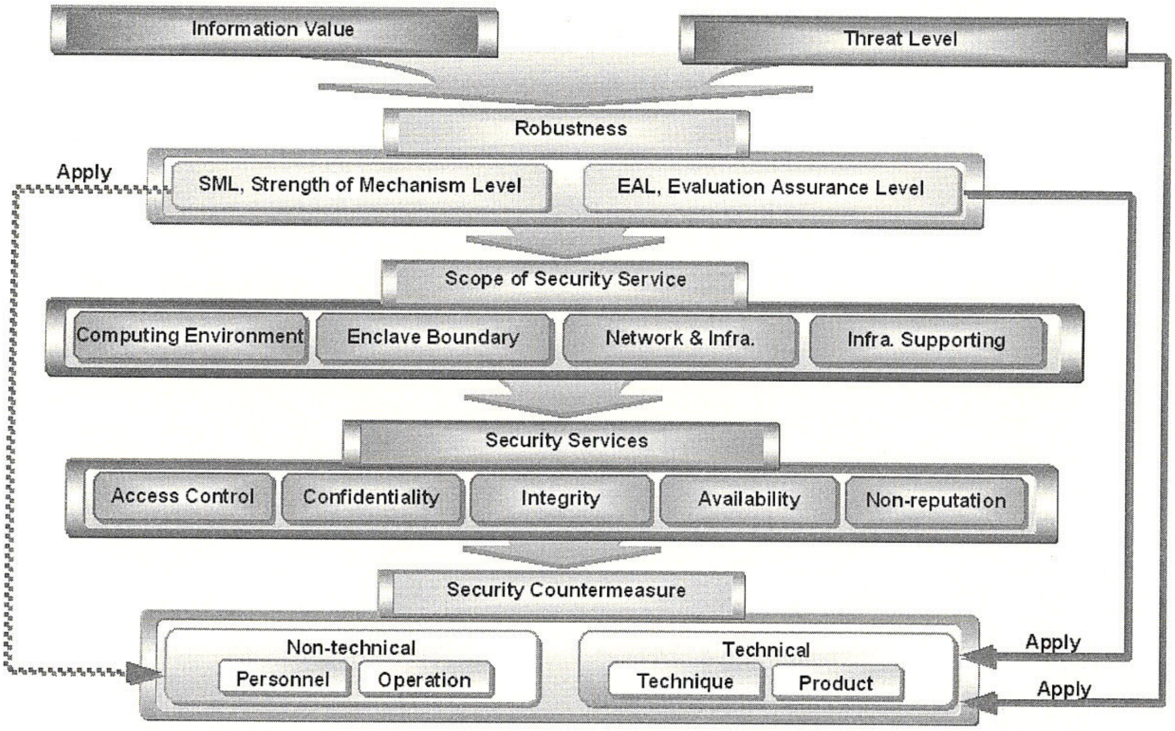
**(Fig. 2)** Block matrix.



**(Fig. 3)** Block Model for Security Countermeasures.



**(Fig. 4)** Building security countermeasures by using Block Region.



**(Fig. 5)** Security Countermeasures Design Procedure

Assurance is the measure of confidence in the ability of the security features and architecture of an automated information system to appropriately mediate access and enforce the security policy. Evaluation is the traditional method that ensures the confidence. Therefore, there are many evaluation methods and criteria exist. In these days, the ISO/IEC 15408, Common Criteria, replaces many evaluation criteria such as ITSEC and TCSEC.

The Common Criteria provide assurance through active investigation. Such investigation is an evaluation of the actual product or system to determine its actual security properties. The Common Criteria philosophy assumes that greater assurance results come from greater evaluation efforts in terms of scope, depth, and rigor.

Next figure (Fig.5) is the summarized concepts we proposed.

## 4. Conclusion

Our Block model may be used to make security countermeasures in any cases.
Because the size of each block expresses parts insufficient in security. For more detail work, we are now researching about the Block Model for Building Security Countermeasures.

## References

[1] Eun-ser Lee, Kyung-whan Lee, Tai-hoon Kim and Il-hong Jung: Introduction and Evaluation of Development System Security Process of ISO/IEC TR 15504, ICCSA 2004, LNCS 3043, Part 1, 2004

[2] Tai-hoon Kim , Chang-wha Hong and Sook-hyun Jung: Countermeasure Design Flow for Reducing the Threats of Information Systems, ICCMSE 2004, 2004.

[3] Ho-Jun Shin, Haeng-Kon Kim, Tai-Hoon Kim, Sang-Ho Kim: A study on the Requirement Analysis for Lifecycle based on Common Criteria, Proceedings of The 30th KISS Spring Conference, KISS (2003).

[4] Haeng-Kon Kim, Tai-Hoon Kim, Jae-sung Kim: Reliability Assurance in Development Process for TOE on the Common Criteria, 1st ACIS International Conference on SERA., 2003