새로운 정보시스템 위협수준결정방법론에 대한 연구

김태훈* · 여상수** · 조성언***

A Study on the New Threat Level Decision Method for Information System

Tai-hoon Kim* · Sang-soo Yeo** · Sung-eon Cho***

요 약

정보시스템은 다양한 구성요소들을 포함하고 있으며, 이들 구성요소들은 몇 개의 유형으로 구분될 수 있다. 보안수준관리활동을 준비할 때, 관리활동의 대상을 정의하는 것이 가장 중요하며, 이들 대상을 정의한 이후 보안수준 관리활동이 시작될 수 있다. 본 논문에서는 정보시스템을 몇 개의 부분으로 나눔으로써 관리대상을 정의하고, 이들 대상은 운영 환경과 특성에 따라 다양하게 관리될 수 있음을 보여준다.

ABSTRACT

Information system contains various components, and these components can be categorized into some types. When preparing security level management activity, it is most important to define the target of management activity. And after deciding these targets, security level management activity can be started. This paper defines management targets by dividing information system into some parts, and shows these targets can be managed variously according to operation environments and characteristics.

키워드

Threat Level, Security Level Management, Division of Information System,

Ⅰ. Introduction

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 [1]-[4].

But this is a method emphasizing attacker's situation mostly, at least the analysis results of information system

* Dept. of Multimedia Engineering, Hannam University Assistant Professor(First Author)

** Dept. of Information and Systems Engineering, Kyushu University, Visiting Scholor, (Second Author)

*** Dept. of Information and Communication Engineering, Sunchon National University, Associate Professor, (Corresponding Author)

접수일자 : 2007. 8. 21

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 [5]-[6].

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 [7]-[8].

So these two activities can be considered separately, and the threat level can be decided by solving the equation (1).

$$TL=f(ID,AT) \tag{1}$$

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

Identification activity is similar to vulnerability analysis in a sense of finding weak points. 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.

But the weight of identification activity is very small when compared with that of attack activity. This is because we know many identifications can not be connected to real attack. Even though attacker know the weak points, there are many restrictions to exploit these weaknesses.

So in this paper, we will focus on real attack activity, and the equation (1) can be rewritten as like equation (2).

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

where AT is the attack activity.

Ⅱ. Considering about 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 the purpose of attack is 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 a target were the information itself, attackers will try to unauthorized access to the information or information systems, and if a target were destruction of information systems, attackers will try to cut important connection between components of IS or shut down whole systems. According to 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 facors 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 like as next equation (3).

$$Ex = f(Ai, Am, Ac, Aa, Ae, At) \tag{3}$$

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 (3) 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 IS, and he will invest more resources to get success in his attack. So some connected correlations can be formed.

Finally, to calculate equation (3), weights for not only each component but also correlation should be considered. But 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.

And it is possible to append new components into equation (3) 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 (4), 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.

$$Ex = f_{ai}(Ai) + f_{am}(Am) + f_{ac}(Ac) + f_{aa}(Aa) + f_{ae}(Ae) + f_{at}(At) + \sum_{ak=0}^{n} f_{ak}(u_{ak}) + \alpha \tag{4}$$

where, $f_{ai}(Ai)$ is a weight function for identified attacker,

$f_{am}(Am)$ is a weight function for the attacker's motivation,

$f_{ac}(Ac)$ is a weight function for attack type,

$f_{aa}(Aa)$ is a weight function for accessibility to IS,

$f_{ae}(Ae)$ is a weight function for attack tools and equipments,

$f_{at}(At)$ is a weight function for compromise time,

$f_{ak}(u_{ak})$ is a weight function for unknown components,

u_{ak} is a k-th unknown component related to attack activity

α is a weight value decided from correlation among components

2.1 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. Some attackers want to get 'the right of superuser' to use systems resource, but other attackers want to destroy the IS themselves. So when we identify attackers and weight to them, we should consider the scope of power of them.

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 superuser ID and Password.

Next Table 1 is the example of weighting for identity of attacker's capability. But when we apply this table to real IS, the weights should be corrected by checking the environment of those IS.

Table 1. Weights for identified attacker's capability

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

2.2 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, we classified attackers already and arranged them into Table 5. If an attacker's capability is included in from Trying to get inside to Paralyzing, this attacker's motivations can be thought like 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 persons who may compromise the IS accidentally. Hackers range from the inexperienced professional, college student, or novice (e.g., Script Kiddy) to the highly technical and very 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.

Next Table 2 is the example of weighting for attacker's motivations.

Table 2. Weights for attacker's motivation

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

2.3 Category of attack

In general case, IS and networks offer attractive targets to attackers. In 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.

Next Table 3 is the example of weighting for category of attacks.

Table 3. Weights for category of attacks

Item	classified	weight	result
Category of attacks	Passive	1	
	Active - getting inside	3	
	Active - denial of Service	4	
	Active - destruction	5	

2.4 Attacker's Access to IS

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

If attackers are in your office already, they may not attack your company's boundary Firewall or Intrusion Detection Systems. If attackers are in 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.

Next Table 4 is the example of weighting for access to IS.

Table 4. Weights for access

Item	classified	weight	result
Access to IS	Distribution	1	
	Close-in	3	
	Insider	5	

2.5 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.

Next Table 5 is the example of weighting for tools and equipments attackers may use.

Table 5. Weights for tools and equipments

Item	classified	weight	result
Tools and equipments	Basic or well known	1	
	Customizing	2	
	Specializing	3	
	Optimizing	4	

2.6 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 attacks.

Next Table 6 is the example of weighting for elapsed time.

Table 6. Weights for elapsed time

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

Ⅲ. 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. But 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 7 is an example of threat level.

Table 7. Threat Level Definition

Threat Level	Description
TL1	Attacks can not make any impact to IS
TL2	Attacks can disturb IS operation
TL3	Attacks can give serious harm to IS
TL4	Attacks can make IS uncontrollable
TL5	Attacks can destroy IS

Next Table 8 is the example of threat level decision.

Ⅳ. Conclusion and Future Work

Former methods for defining threat level are not elaborate and calculable but very simple and intuitive [1]-[2], [7]. Therefore, these methods can not be used to decided threat level by considering operational objectives and environments.

Table 8. Example of threat level decision

Summation of weights (SoW)	Threat Level	Description
SoW<5	TL1	Attacks can not make any impact to IS
5≦SoW<12	TL2	Attacks can disturb IS operation
12≦SoW<18	TL3	Attacks can give serious harm to IS
18≦SoW<24	TL4	Attacks can make IS uncontrollable
24≦SoW	TL5	Attacks can destroy IS

To decide a security level of information system, threat level and asset level should be decided first, and threat level can be decided by considering some components such as attacker's motivation and available tools or equipments.

This paper proposes the 5 threat levels and a method to decide threat level by using weights attached to each components related to threat. But these components are not perfect ones because each information system has their own unique operational environments and characteristics. So these variable should be researched in near future.

Reference

[1] ISO. ISO/IEC 21827 Information technology - Systems Security Engineering Capability Maturity Model (SSE-CMM)

[2] ISO. ISO/IEC 15408-1:1999 Information tech nology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[3] Sangkyun Kim, Hong Joo Lee, Choon Seong Leem "Applying the ISO17799 Baseline Controls as a Security Engineering Principle under the Sarbanes-Oxley," Act, *ICCMSE 2004*, 2004.

[4] Tai-hoon Kim and Haeng-kon Kim "The Reduction Method of Threat Phrases by Classifying Assets," *ICCSA2004, LNCS 3043*, Part 1, 2004.

[5] Tai-hoon Kim and Haeng-kon Kim "A Relationship between Security Engineering and Security Evaluation," *ICCSA2004, LNCS 3046*, Part 4, 2004.

[6] 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*.

[7] Tai-hoon Kim, Seok-soo Kim, Gil-cheol Park "Analysis of Threat Agent for Important Information Systems," *The Journal of Korea Navigation Institute*, Vol.11 No.2, 2007.

[8] Sang-soo Yeo, Tai-hoon Kim, Sung-eon Cho, Kouich Sakurai "A Study on the Development Site Security for Embedded Software," *The Journal of Korea Navigation Institute*, Vol.11 No.3, 2007.

저자소개

Tai-hoon Kim

1995 B.S. in Sungkyunkwan University
1997 M.S. in Sungkyunkwan University
2002 Ph.D. in Sungkyunkwan University

1999 Researcher in Technology Institute of SindoRicoh
2004 Senior researcher in KISA
2006 Secretary in DSC
2007 Research professor of Ewha Woman University
2007~Assistant professor of Hannam University
※Research topics: Information security and assurance, Security level management

Sang-Soo Yeo

1997 B.S. in Chungang University
1999 M.S. in Chungang University
2005 Ph.D. in Chungang University

2006 Full time lecturer of Dankook University
2007 ~ Visiting Scholor of Kyushu University
※Research topics : Ubiquitous Computing, RFID security Embedded software

Sung-Eon Cho

received the B·S degree in Communication & Information engineering from Hankuk Aviation Univ(.HAU) in 1989, M·S degree in electronic engineering from HAU in 1991, and the Ph·D. degree in electronic engineering in 1997 from HAU, respectively.

In 1997, he join the faculty member of the Sunchon national Univ., where he is currently a associate professor in the Dept. of computer & communication engineering. His research interests focus on wireless communication, wireless USN technologies.