한국항행학회 논문지 제12권 제1호 2008년 2월

멀티미디어 시스템 정보보호수준 결정 기법

A Security Level Decision Method for Multimedia System

김태훈*, 이덕규**, 여상수***, 조성언****

Tai-Hoon Kim*, Deok-Gyu Lee**, Sang-Soo Yeo*** and Sung-Eon Cho****

요 약

특정 목적을 달성하기 위해서 멀티미디어 시스템을 구축하고 운영하는 조직은, 보안수준을 결정하고, 보안대책을 구현하며, 보안대책의 효과를 유지하기 위해 관리를 하여야 한다. 멀티미디어 시스템이 보안수준을 결정하고 관리하기 위해서, 첫째, 조직은 보안 수준을 결정할 수 있어야 하고, 둘째, 보안 수준에 따라 보안대책을 수립하는 절차를 확립하여야 하며, 셋째, 보안대책이 적용되어야 하는 영역을 결정할 수 있어야 하고, 마지막으로 조직은 보안대책의 효과를 평가하고 개선할 수 있어야 한다. 본 논문에서는 멀티미디어 시스템에 대한 위협의 분석, 멀티미디어 자산의 중요도 분석에 기반하여 멀티미디어 시스템의 보안수준을 결정하는 방법을 제안하였다.

Abstract

Each organization installing and operating multimedia system, to achieve the goal of organization, should decide security level, implement security countermeasure, and manage these countermeasures to keep the effects. To decide and manage security level of multimedia system, the first, organizations must be able to decide security level, and then, organizations must establish 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, and the last, organizations must be able to evaluate and improve the effect of security countermeasures. In this paper, based on the analysis of threat to multimedia system and the consideration for multimedia assets, we propose a method for deciding security level of multimedia system.

Key words : Multimedia System, Security Level, Security Level Management Model

I. Introduction

Security is concerned with the protection of assets, and assets are entities that owner places value upon. Because the concept of asset is related to the owner's mind or decision, owner is endowed with responsibilities for protection. And attackers or threat agents can think some assets are valuable, but this is because they want to abuse these assets. To protect these kinds of attack, organizations should do security level management activities [1].

Security level decision is a basic activity for

* 한남대학교 멀티미디어학부(Dept. of Multimedia, Hannam Univ.)
** 한국전자통신연구원 보네트워크보안연구팀(ETRI, HomeNetwork Security Research Team)
*** 일본 큐슈대학교 (Dept. of Computer Science and Communication engineering, Kyushu Univ.)
**** 순천대학교 정보통신공학부(Division of Iformation Communication, Sunchon National Univ.)
· 교신저자 (Corresponding Author) : 조성언

· 접수일자 : 2008년 1월 25일

developing and managing of safe multimedia systems, and core factor which can affect the investment for security countermeasures. According to the security level of multimedia system, where and how the security countermeasures are implemented, which security policies are selected, and who will manage them are able to be decided [2-4]. 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. And it is possible to change security level at each management process. But because the change of security level may affect whole security policy of multimedia system itself, operators and owners' agreement is needed essentially [5-7]. In this paper, based on the analysis of threat to multimedia system (MS) and the consideration for multimedia assets, we propose a method for deciding security level of multimedia system.

Ⅱ. Security Level Decision Method

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 formula (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 MS.

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.

But 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 formula (2).

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

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

But the weight of identification activity is very small when compared with that of attack activity, because the identification activity is not a real attack. Therefore, most TL can be effected by AT, so the formular (2) can be rewritten as like formula (3).

$$TL = f(AT) \quad (3)$$

where ID the is identification activity, and AT is the 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 MS 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 MS or shut down whole systems.

According to the importance of MS, 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 MS, tools and equipments, and compromise time estimation.

By using these factors, attack activity can be defined like as next formula (4).

$$\mathrm{Ex} = \mathrm{f}(\mathrm{Ai}, \mathrm{Am}, \mathrm{Ac}, \mathrm{Aa}, \mathrm{Ae}, \mathrm{At}) \quad (4)$$

Where, Ai : Identification of Attacker,
Am : Attacker's motivation,
Ac : Category of attack
Aa : Attacker's Access to MS,
Ae : Attacker's equipments or tools,
At : Elapsed Time of MS

Each element in formula (4) 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 MS, and he will invest more resources to get success in his attack. So some connected correlations can be formed.

Finally, to calculate formula (4), 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 MS operation. And it is possible to append new components into formula (4) according to the change of environment of MS. 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 MS. The last component of formula (5), alpha means that the weights calculated by correlation among each component. Alpha can be changed by environments and characteristics of MS, in this paper, only the estimated result is included.

$$\begin{aligned}\mathrm{Ex} = {} & \mathrm{f_{ai}}(\mathrm{Ai}) + \mathrm{f_{am}}(\mathrm{Am}) + \mathrm{f_{ac}}(\mathrm{Ac}) \quad (5)\\ & + f_{aa}(Aa) + f_{ae}(Ae)\\ & + f_{at}(At) + \sum_{ak=0}^{n} f_{ak}(u_{ak}) + \alpha\end{aligned}$$

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

$\mathrm{f_{am}}(\mathrm{Am})$ 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 MS,

$f_{ae}(Ae)$ 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

(1) Identification of Attacker

For example, if the identified attackers are terrorists, they can destroy the MS by bomb, so their power is bigger than hackers who can compromise MS 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 MS, the weights should be corrected by checking the environment of those MS.

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) Attacker's motivation

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

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	

(3) Category of attack

Attackers want to get inside, use system resources, and do something malicious. And there are very many methods for getting inside of MS not passing through the Firewall and IDS by network. 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	

(4) Attacker's Access to MS

Next [Table 4] is the example of weighting for access to MS.

Table 4. Weights for access

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

Distribution attacks are very useful, but this attack can be detected by another systems. So before many parts of IS are modified to follow attackers command, this attacks may not successful.

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

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

(5) Tools and equipments

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

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	

(6) Elapsed Time of MS

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	

We need a time to count attacks, because we should analyze the characteristics of these attacks. But we can not sure we can do this work successfully in short time. Therefore, the estimation of elapsed time is important. Initial state we may detect the attacks, we can estimate the elapsed time of the IS, and should do something to protect this systems.

(7) Definition of Threat

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 slightly
TL3	Attacks can give harm to IS
TL4	Attacks can make IS uncontrollable
TL5	Attacks can destroy IS

Next [Table 8] is the example of threat level definition.

Table 8. Example of threat level decision

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

2-2 Definition of Asset Level

Even though threat levels were decided like as [Table 8], security level of each MS is not decided yet. To decide 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 owners of MS. It is possible to reference security level managers' opinion or other specialists' suggestion, but these opinions and suggestions are not always same with owners' decision. Next [Table 9] is a basic model of AL categorized by the effect of compromise of MS.

Table 9. Example of Security Label Definition.

Asset Level	Description
AL1	Owners will not invest any more to protect these assets
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 is should be notified that higher level 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 MS were included well.

In this paper, SL is divided and described into 4 level shown in [Table 10].

Table 10. 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 continuously
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 11], but details should be decided by considering operational environments and characteristics of MS.

Table 11. 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

Ⅲ. Conclusion and Future Work

In this paper, security level decision method was proposed. But the security level decision is the first step of security level management model (SLMM).

To protect multimedia system more clearly, the SLMM architecture should be designed to provide a guide to keep the security level of information system. The goal of the SLMM architecture is to provide characteristics of the security countermeasures should be implemented to keep information system.

Acknowledgment

This paper has been supported by the 2007 Hannam University Research Fund.

References

[1] Sang-Soo Yeo, Sang-Jo Youk, Gil-cheol Park, Seok-soo Kim and Tai-hoon Kim, “Physical Threat Description of Smart Card Protection Profile in Security Level 1st,” *International Journal of Security and Its Applications,* Vol.1, No.2, October, 2007, pp.99-107

[2] Tai-Hoon Kim, Kouichi Sakurai, "A study on Security Level Management Model Description," *International Journal of Multimedia and Ubiquitous Engineering,* Vol.3 No.1 January 2008, pp.87-96

[3] Tai-Hoon Kim, Kouichi Sakurai, "Definition of Security Practices for Security Level Management Model," *International Journal of Security and Its Applications*, Vol.2, No.1, January 2008, pp.63-72

[4] Tai-Hoon Kim and Kouich Sakurai, "A Study on Security Level Features and Level Requirements in Security Level Management Model," *International Journal of Software Engineering and Its Applications,* Vol.2, No.1, January 2008, pp.109-118

[5] 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, pp.203-207

김 태 훈 (金泰勳)

1995년 성균관대학교 공학사
1997년 성균관대학교 공학석사
1999년 (주)신도리코 기술연구소 연구원
2002년 성균관대학교 공학박사
2004년 한국정보보호진흥원 선임연구원
2006년 국군기무사령부 사무관
2007년 이화여자대학교 연구교수
2007년~현재 한남대학교 멀티미디어학부 조교수
관심분야 : 유비쿼터스 및 RFID보안, 임베디드 소프트웨어

이 덕 규 (李悳揆)

2001년 순천향대학교 공학사
2003년 순천향대학교 공학석사
2006년 순천향대학교 공학박사
2006년~현재 한국전자통신연구원 정보보호연구단
관심분야 : 유비쿼터스 및 RFID보안, 임베디드 소프트웨어

여 상 수 (呂相壽)

1997년 중앙대학교 공학사
1999년 중앙대학교 공학석사
2005년 중앙대학교 공학박사
2006년 단국대학교 정보컴퓨터학부 강의전임강사
2007년~현재 Kyushu University 방문연구원
관심분야 : 유비쿼터스 및 RFID보안, 임베디드 소프트웨어

조 성 언 (趙誠彥)

1989년 한국항공대학교 항공통신정보공학과 공학사

1991년 한국항공대학교 대학원 항공통신정보공학과 공학석사
1997년 한국항공대학교 대학원 항공전자공학과 공학박사
1997년~현 재 순천대학교 정보통신공학부 부교수
관심분야 : 무선통신시스템, Wireless USN