멀티미디어 시스템 정보보호수준관리를 위한 관리형 프랙티스에 관한 연구

A Study on The Managing Practices in SLM for Multimedia System

김태훈[*], 조성언[**]

Tai-Hoon Kim[*] and Sung-Eon Cho[**]

요 약

멀티미디어 시스템의 보안은 멀티미디어 자산 자체를 보호하는 것과 시스템을 보호하는 것, 두 가지 측면으로 나누어 생각할 수 있는데, 이들 두 가지 측면을 별도로 고려한다고 하여도 보안관리의 중요성은 결코 떨어지지 않는다. 본 논문에서는 멀티미디어 시스템의 정보보호수준을 관리하기 위한 관리적 측면에서의 프랙티스들을 도출하고, 이를 적용하기 위해 그룹화하였다.

Abstract

Multimedia system security can be categorized into groups such as protection of multimedia asset itself and protection of multimedia systems which can process multimedia asset. Divided consideration for these two factors will not hurt the importance of security management. In this paper, managing practices for keeping security level of multimedia systems are induced and categorized.

Key words : Security level management, Management practices

I. Introduction

Security level management is the activity to sustain the security level which defined as an essential one by considering operational environments of information systems. 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 [1].

* 한남대학교 멀티미디어학부(Division of Multimedia, Hannam Univ.)
** 순천대학교 정보통신공학부(Division of Information Communication engineering, Sunchon National Univ.)
· 교신저자 (Corresponding Author) : 조성언

· 투고일자 : 2008년 11월 3일
· 심사(수정)일자 : 2008년 11월 5일 (수정일자 : 2008년 12월 19일)
· 게재일자 : 2008년 12월 30일

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.

In this paper, managing practices for keeping security level of multimedia systems were induced and categorized.

Ⅱ. Multimedia and Multimedia System

Multimedia is media that uses multiple forms of information content and information processing, e.g. text, audio, graphics, animation, video, interactivity to inform or entertain the (user) audience. Multimedia also refers to the use of (but not limited to) electronic media to store and experience multimedia content.

In fine art it is a synonym for traditional mixed media as well as technological new media. The term "rich media" is also synonymous for interactive multimedia.

Multimedia may be broadly divided into linear and non-linear categories. Linear active content progresses without any navigation control for the viewer such as a cinema presentation. Non-linear content offers user interactivity to control progress as used with a computer game or used in self-paced computer based training. Non-linear content is also known as hypermedia content.

Multimedia presentations can be live or recorded. A recorded presentation may allow interactivity via a navigation system. A live multimedia presentation may allow interactivity via interaction with the presenter or performer.

Multimedia presentations may be viewed in person on stage, projected, transmitted, or played locally with a media player. A broadcast may be a live or recorded multimedia presentation. Broadcasts and recordings can be either analog or digital electronic media technology. Digital online multimedia may be downloaded or streamed. Streaming multimedia may be live or on-demand. Multimedia games may be played in person in an arena with special effects, with multiple users in an online network, or locally with an offline computer or game system.

The various formats of technological or digital multimedia may be intended to enhance the users experience, for example to make it easier and faster to convey information. Or in entertainment or art, to transcend everyday experience. Enhanced levels of interactivity are made possible by combining multiple forms of media content. Online multimedia is increasingly becoming object-oriented and data-driven, enabling applications with collaborative end-user innovation and personalization on multiple forms of content over time. Examples of these range from multiple forms of content of web sites like photo galleries with both images (pictures) and title (text) user-updated, to simulations whose coefficients, events, illustrations, animations or videos are modifiable, allowing the multimedia "experience" to be altered without reprogramming.

Multimedia finds its application in various areas including, but not limited to, art, education, entertainment, engineering, medicine, mathematics, business, and scientific research.

Below are the several examples as follows:

- **Engineering**: In Engineering, especially in mechanical and automobile engineering, multimedia is primarily used for designing a machine or an automobile. This lets an Engineer view a product from various perspectives, zoom in on critical parts and do other manipulations, before actually producing it. This is known as computer-aided design (CAD) or computer-aided engineering (CAE).

- **Medicine**: In Medicine, doctors can get trained by looking at a virtual surgery or they can simulate how the human body is affected by diseases spread by viruses and bacteria and then develop techniques to prevent it.

- **Mathematical and Scientific Research**: In Mathematical and Scientific Research, multimedia are mainly used for modeling and simulation. For example, a scientist can look at a molecular model of a particular substance and manipulate it to arrive at a new substance.

- **Education**: In Education, multimedia is used to produce computer-based training courses (popularly called CBTs) and reference books like encyclopedia and almanacs. A CBT lets the user go through a series of presentations, text about a particular topic, and associated illustrations in various information formats. Edutainment is an informal term used to describe combining education with entertainment, especially multimedia entertainment.

- **Industry**: In the Industrial sector, multimedia is used as a way to help present information to shareholders, superiors and coworkers. Multimedia is also helpful for providing employee training, advertising and selling products all over the world via virtually unlimited web-based technologies.

- **Multimedia Messaging System:** The Multimedia Messaging System, or MMS, is an application that allows one to send and receive messages containing Multimedia - related content. MMS is a common feature of most cell phones. An electronic multimedia encyclopedia can present information in better ways than traditional encyclopaedia, so the user has more fun and learns more quickly.

Generally speaking, computer engineering is progressed in 2 ways. First is virtual reality and second is ubiquitous. For virtual reality systems, because we should go into the virtual space with the aid of computer and some devices, all scenes we can see is the artificial materials and these are generally constructed by Multimedia.

Ⅲ. Multimedia Assets and Security

In business and accounting by asset is meant economic resources controlled by an entity as a result of past transactions or events and from which future economic benefits may be obtained.

In these days, it is very common to get economic benefits by using Multimedia. Physical assets management is an accounting process that seeks to track fixed assets for the purposes of financial accounting, preventive maintenance, and theft deterrence.

Many organizations face a significant challenge

-to track the location, quantity, condition, maintenance and depreciation status of their fixed assets.

-a popular approach to tracking fixed assets utilizes

-serial numbered Asset Tags, often with bar codes for easy and accurate reading.

-periodically, the owner of the assets can take inventory with a mobile barcode reader and then produce a report.

And Multimedia is one of the Digital Assets. Digital Asset is any form of content and/or media that have been formatted into a binary source which include the right to use it. A digital file without the right to use it is not an asset.

Digital assets are categorized in three major groups which may be defined as textual content, images and multimedia. Based on the agreement that Multimedia is a kind of Digital Assets, we should consider about security.

Figure 1 is a diagram depicts the concept of threat to Multimedia and Multimedia systems. Multimedia systems are the systems support successful Multimedia interactivities. From now on, when I mention about the Multimedia, please think it contains Multimedia systems.

Most important thing is an our asset, Multimedia. For example, please consider we have very helpful AVI file contains the investment trend of 10 major companies.

In this case, someone want to abuse this file with their own, and they will generate threat to our asset and find vulnerabilities to get this file. All these action of someone who can use our asset without agreement will increase Risk to our assets.

If we are the owner of this file, and if we detect or acknowledge these threats, we may take or buy technical and non-technical methods to protect our file. This is a countermeasure for our assets and this can be a start point of security concept.

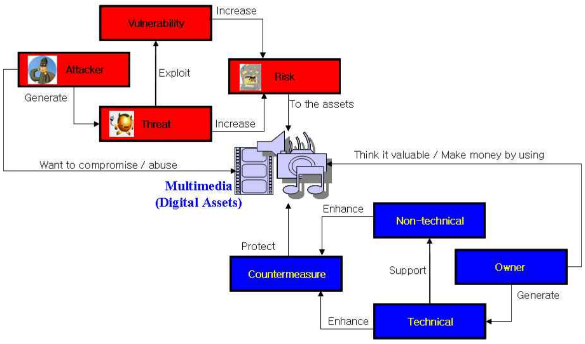

Fig. 1. Concept of Multimedia Security

Ⅳ. Managing Practices in Security Level Management (SLM)

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

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

4-1 Human Resource

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

Because hiring, training and education, disposition, and retirement of human resources are being rotated continuously, the level of individual resource can be changed variously. And 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 other new employees of same capability, organization can manage its security level. And 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

4-1-1 SP.01.01 Personnel Management

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

4-1-2 SP.01.02 Clearance level

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

4-1-3 SP.01.03 Monitoring of Suspicious Action

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

4-1-4 SP.01.04 Training and Education

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

4-2 Operation and Administration

Small organization can make decision by simple discussion or intuitive estimation. But the bigger organization is, the more important operation or administration by using proper procedure is. Especially, in the case that security related incidents are happen or the possibility of incidents are very high, it is possible to reduce the damage by confronting efficiently and actively.

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 be not 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

4-2-1 SP.02.01 Establishment of Security Role

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 alsoensure 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

4-2-2 SP.02.02 Configuration Management of Security Controls

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

4-2-3 SP.02.03 Incident Identification

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

4-2-4 SP.02.04 Incident Management

Many events can not 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

4-2-5 SP.02.05 Monitoring of Change

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

4-2-6 SP.02.06 Security Control Management

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

4-2-7 SP.02.07 Common Use of Security Constrains and Considerations

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

4-2-8 SP.02.08 Guidance

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

4-2-9 SP.02.09 Identification of Laws, Policies, Standards, and External Influences

The purpose of this practice is to gather all external influences which affect the security of the organization. A determination of applicability should identify the laws, regulations, policies and standards which govern thetarget environment of the organization. A determination of precedence between global and local policies should 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

4-3 Physical Protection

This security area, physical protection, contains security practices related to not only the protection of physical space but also the 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. And only the person who has the permission can enter the space.

Physical resource does not mean only digital device or equipments should be used. But 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

4-3-1 SP.03.01 Secure Zone

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

4-3-2 SP.03.02 Physical Security Perimeter Management

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

4-3-3 SP.03.03 Classified Materials Storing

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

Ⅴ. Conclusion and Future Work

SLM can be divided into 2 groups, managing part and technical part. By considering these 2 parts together, security level management of mulitmedia system can be achieved.

But in this paper, only 16 security practices, organized in 3 areas for the MP (Managing Part) in SLM (Security Level Management). These security practices can cover major areas of security countermeasures in management area, but are not able to be applied to technology area. Therefore, security practices related to TP (Technical Part) should be defined and listed in near future.

Acknowledgement

This paper has been supported by the 2008 Hannam University Research Fund.

References

[1] Tai-hoon Kim, Gil-cheol Park and Kouichi Sakurai, "A study on Security Level Management Model Description", *International Journal of Multimedia and Ubiquitous Engineering*, Vol.3 No.1, January 2008, pp.87-94

[2] ISO 14001, "Environmental Management Systems - Specification with Guidance for Use", 1996

[3] ISO/IEC 17799, "Information Technology - Code of Practice for Information Security Management", 2000

[4] BS7799-2, "Information Security Management Systems - Specification with Guidance for Use", 2002

[5] ISO/IEC TR 19791, "Information Technology - Security Techniques - Security Assessment of Operational Systems", 2005

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 : 대규모 시스템 보안, 정보보증, SCADA 보안

조 성 언 (趙誠彦)

1989년 한국항공대학교 항공통신정보공학과 공학사
1991년 한국항공대학교 대학원 항공통신정보공학과 공학석사
1997년 한국항공대학교 대학원 항공전자공학과 공학박사
1997년~현재 순천대학교 정보통신공학부 부교수
관심분야 : 무선통신시스템, Wireless USN