A Study on Enhanced Security Monitoring in University Network Environments

[1]Mucheol Kim, [2]DaeSik Ko, *[3] Hangbae Chang

[1]Department of Multimedia, Sungkyul University, mucheol.kim@gmail.com
[2]Mokwon University, kds@mokwon.ac.kr
[3] Chung-Ang University, hangbae.chang@gmail.com

Abstract

With the rapid increase of information, security vulnerability is an emerging issue in information management. In addition, the coverage of security monitoring services in universities is so large, but they have the problem of the lack of administrative staff. This paper suggests a significant security monitoring model for university computer network environments. With comparison to company networks, we should arrange the unique characteristics of university network environments. Our suggestions are based on threat management systems, and we also deal with privacy problems, access controls, and information leakages and so on. It also considers the mobile campus environments.

***Keywords**: Security Monitoring, University Networks, Security, Intruder Detection, significant security monitoring model*

1. Introduction

As the amount of information explosively increased, security-threatening factors have also increased. In addition, systems have been exposed to cyber threats and risks more frequently. As a result, many businesses and agencies have received security monitoring and control services through professional service providers, and public organizations have established and operated a security control center in person [1-2].

Recently, cyber-attacks have evolved into a persistent and intelligent threat. As a result, conventional security systems such as vaccine and Intrusion Prevention System (IPS) have been exposed to many undetectable risks. An Advanced Persistent Threat (APT) is usually performed with the following purposes: targeted attack against a certain company, cyber spy such as stealing of national confidential data and politically/socially-purposed hacktivism [3-4].

For security monitoring and control, meanwhile, the system should be well prepared against security risk factors from diverse sources, which threaten a computer network. Otherwise, a security threat may occur because of the followings: approach to a personal computer or IT resources by unauthorized user or medium, attack of the operating system's weakness and attachment of illegal equipment. The solutions for this problem include user identification & encryption and memory device management. In addition, a network security threat can also take place because of data falsification, traffic flooding attack, DDoS and sniffing. Therefore, these problems can be fundamentally handled with an intrusion preventive or blocking system through router security, firewall, encryption and log management [5-7].

This study compares differences between the university's computer networks and company's computer network and proposes a unique integrated security monitoring and control plan in consideration of the characteristics of university.

This paper is organized as follows: Chapter 2 presents some relevant related work. Chapter 3 compares against security monitoring model of company computer networks. In Chapter 3, we present the proposed security monitoring model. In Chapter 4, discussions and conclusion are specified.

[*] Corresponding Author

Received: Sep.21, 2014, Revised: Oct. 30, 2014, Accepted: Jan. 06, 2015

2. Related Work

2.1. Intruder Detection System (IDS)

Intrusion detection system [10] is to help computer systems for preparing and dealing with the network attacks [8]. Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

The purpose of IDS is to help computer systems against various attacks, and that IDS is collecting information from several different sources within the computer systems and networks with several patterns of discrimination which are attacks or weaknesses.

There are two types of Intrusion Detection Methods. They are misuse detection and anomaly detection [9]. In misuse detection, network traffic is monitored to detect illegal access using predefined attack signatures. On the other hand, IDSs based on the anomaly detection method use normal patterns to detect abnormal activities from observed data. They should attempt to identify deviations from predefined normal patterns. Abnormal activities are regarding to the potential attacks.

2.2. Enterprise Security Management (ESM)

ESM is the integrated security solutions with several security solutions which are firewall, intruder detection system (IDS), virtual private network (VPN) and so on. ESM has showing the trend, which is including the system resource management, network management system (NMS). It establishes the consistent security policy for entire knowledge management systems which have the mutual relationships, and manages the enterprise security solutions.

In order to security monitoring for database, we should utilize the performance monitoring modules. It might improve the operation of database with managing and monitoring the performance indicators. Then they provide the DB metadata for enhanced system performance and availability when the problem occurs in database. DB should retain the integrity because they load and manage the important business data.

On the other hand, there are various virus and worm in end-point PC. Then central management system should control and supervise the end-point PC with group based monitoring. They always communicate vaccine server for synchronizations of current virus patterns. Furthermore, security agents play the role of detecting and preventing the various threats from virus.

2.3. Threat Management System (TSM)

Threat Management System (TMS) is the system for detecting, analyzing, and alarming against the cyber threats [11-12]. It should deal with the monitoring and corresponding to the illegal intruders for prevention and mitigation the intrusion damage spread. This provides the comprehensive threat management system and the efficient decision support system by analysis in conjunction of global and local threat conditions. Furthermore, they also provide abnormal traffics, vulnerabilities, malicious codes, and undefined events which are detected by analyzing the symptoms occurred between several events. TMS includes a firewall, VPN, web firewall, web content filtering, and several security tools including anti-spam software. TMS should reduce costs and comprehensive improve the management efficiency.

2.4. Security Monitoring for mitigating privacy problem

Recently, there are important security issues related to the privacy problem. It is adjusting to PC security monitoring, especially business PC. Because they have critical business data in PC of employers [13]. Then, we should consider the private data management methodology and the followed leakage prevention technology.

On the other hand, many people are utilizing various smart devices such as laptop, phone, tablet etc., company or schools need to consider to the consistent policy of access control and user authentication. Diversification of the devices connected to the system is rapidly increasing, a variety of access from each access is needed. Integrated management of user authentication and authorization should be important because of various threats that do not cover the target and data leakages.

2.5. Security Monitoring for Web Server and WAS Server

Web firewall performs the role of detections and preventions with HTTP (HyperText Transfer Protocol) Request and Response packets of web server. Their processes are come from the principle of the proxy server. They might check, detect and prevent the communication packets between web servers and web clients.

On the other hand, the amount of application’s traffic and their quality of services are important with the development of web application services [14]. Web services a new kind of information system common framework based Internet. Users should request information with remote call among various services and process the data in the TCP/IP environment. Web services communication is occurred with SOAP message. Then Web services security communication must ensure the SOAP message end-to-end security .Web Services Security should meet five basic objectives which are identity authentication, permission management, data integrity, confidentiality and anti- denial. There are many ways to protect a web application; however there is no excellent methodology that it will protect the application entirely. Then security monitoring of web applications should have the criteria to mitigate security vulnerability.

3. Comparisons against Security Monitoring Model of Company Computer Networks

According to a recent survey, the information security division in college or Computer Emergency Response Team (CERT) is still fragile. For example, even though a great number of colleges are connected with Education Cyber Security Center (ECSC) in the Ministry of Education, most of them are lack of professional staff or team that would cope with this kind of security matter. Because information security including privacy protection in college becomes more important, however, there should be a practical study on a systematic security monitoring and control.

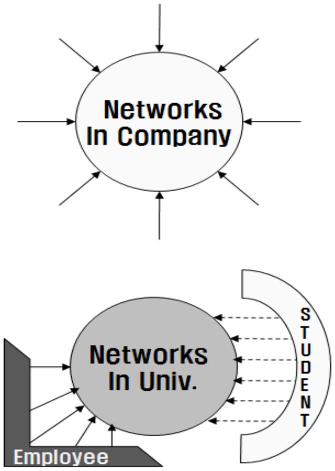

Figure 1. Structural difference of the networks in university and company

Right now, IT infrastructure is controlled through the scattered introduction of security equipment by college. However, it is still insufficient to establish a systemic security system. In addition, considering both quantitative and qualitative shortage in security monitoring and control experts and the fact that many students who are lack of security management awareness are the actual users of IT resources, it is needed to develop a security monitoring and control model which meets each college's characteristics.

In terms of a business computer network, employees get access to the network through a designated personal computer and authorized channel. A centralized control model in which a central control center can detect and handle an exceptional event when it occurs is appropriate. In a college computer network, on the contrary, faculty gets access to the network just like the business computer network. However, college students get access to the computer network through a great number of personal computers. They also attempted to approach the network using mobile devices as well as a mobile network. In terms of the scope of monitoring and control, therefore, a college computer network is greater than a business computer network. Furthermore, personal information is more useful depending on job characteristics, and the latest information technology is applied faster than the business computer network. Hence, colleges should have their own security monitoring and control framework.

4. Enhanced Security Monitoring Model for University Networks

Meanwhile, the college monitoring and control model proposed in this study further develops intrusion detection and preventive technology against the latest cyber threats by summarizing and spreading rules on new threats based on the TMS (Threat Management System) from the ECSC (Education Cyber Security Center). TMS automates the security monitoring and control process by simplifying the procedure of handling the verified detection patterns and informs the results to the malicious code and high-accuracy detection patterns in a lump sum. As a result, a cyber-threat detection technology-sharing system has been developed, applying and distributing cyber safety center's and related organization's detection technologies on a real-time basis.

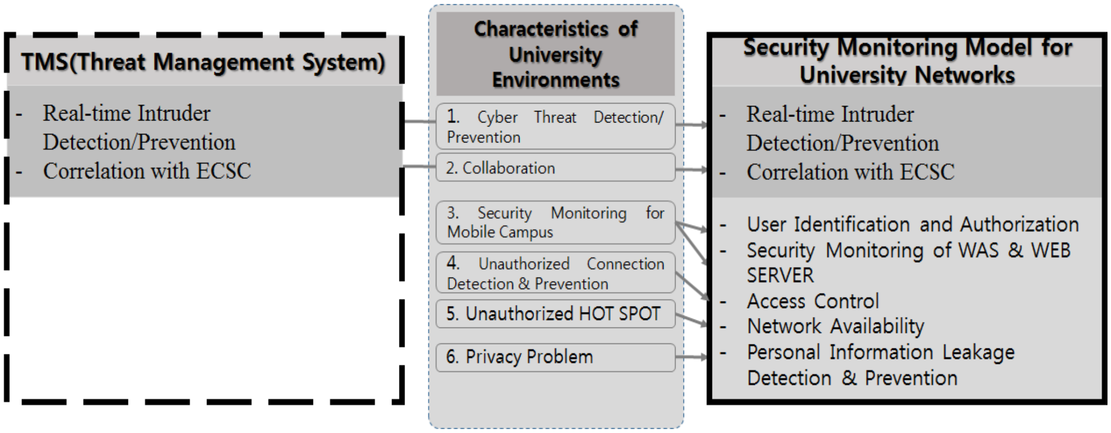
TMS(Threat Management System)
- Real-time Intruder Detection/Prevention
- Correlation with ECSC
Characteristics of University Environments
1. Cyber Threat Detection/ Prevention
2. Collaboration
3. Security Monitoring for Mobile Campus
4. Unauthorized Connection Detection & Prevention
5. Unauthorized HOT SPOT
6. Privacy Problem
Security Monitoring Model for University Networks
- Real-time Intruder Detection/Prevention
- Correlation with ECSC
- User Identification and Authorization
- Security Monitoring of WAS & WEB SERVER
- Access Control
- Network Availability
- Personal Information Leakage Detection & Prevention

Figure 2. Enhanced security monitoring model for university networks

Therefore, a real-time detection technology sharing system is established. The model proposed in this study has been developed based on the TMS provided by the ECSC. A threat management system is a management system which uses various security tools such as firewall, virtual network, instruction preventive and blocking system, web contents filtering and anti-spam software. It is a comprehensive management system improves cost reduction and management skills. When integrated security functions provided by the threat management system are all applied, poor performance may occur because of inability to handle the network traffic. Therefore, security equipment should be properly arranged even though it is still effective in terms of management and operation. For the TMS in a college security monitoring and control model, a TMS sensor is used for the collection of bad traffic.

Once bad traffic is collected through a TMS Sensor, the TMS manager carries out the followings: intrusion detection & analysis of traffic information, network monitoring, intrusion detection & analysis, analysis of abnormal climate conditions, attack pattern and traffic analysis. Based on this kind of analysis, a security policy is set, and early warning and vulnerability information is provided. Furthermore, the bad traffic information collected through the TMS is connected with Education Cyber Safety Center and National Cyber Security Center, and the latest cyber threat information is provided by these centers. Then, intrusion detection/block and related warning are provided on a real-time basis after getting the latest cyber threat information from them the centers. In order for colleges to carry out security monitoring and control suitable to IT environment, it is important to properly cope with monitoring under mobile campus environment and unauthorized accesses in addition to connection with Education Cyber Safety Center and detection & prevention of cyber threats. In addition, extreme differences in network access rates depending on major issues such as admission and enrollment should be considered. In addition, there should be security monitoring and control on the great amount of personal information on a college computer network.

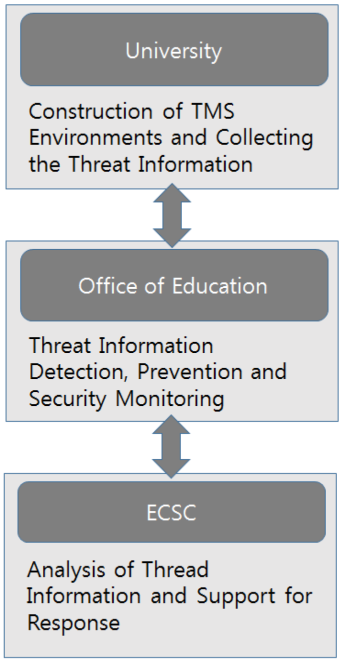
University
Construction of TMS Environments and Collecting the Threat Information
Office of Education
Threat Information Detection, Prevention and Security Monitoring
ECSC
Analysis of Thread Information and Support for Response

Figure 3. Collaboration System through TMS

To monitor and control mobile campus, the users on the college computer network should be identified, and unauthorized users should be inhibited from getting access to IT resources and college computer network through the authentication and authority management. For the effective monitoring and control on mobile campus web or app, in addition, WAS and WEB SERVER is controlled in the security monitoring and control server.

In college, there are attempts to get access to a college computer network through the IT resources which exist in dorms and research spaces as well as in lecture halls and administrative spaces. From both time and spatial aspects, there should be a solution on the detection of unauthorized access and user authority setting. Therefore, a network access control is performed, and efficiency in the use of IT resources is improved through user authentication. At the same time, security monitoring and control can be effectively carried out. In addition, an unauthorized access to the mobile network can be detected through the Intrusion Prevention System (IPS) in wireless LAN.

Furthermore, if a certain event (ex: admission, enrollment, etc.) takes place, the access to the college computer network explosively increases. To handle this effectively, network availability can be secured through a network management system, ensuring the stable operation of the network regardless of the number of network users.

Lastly, to detect and prevent information leakage on a college computer network, there should be a plan to detect and control any personal information leakage in the personal computers and IT resources and on the server. For this, the exposure and leakage of personal information should be constantly monitored.

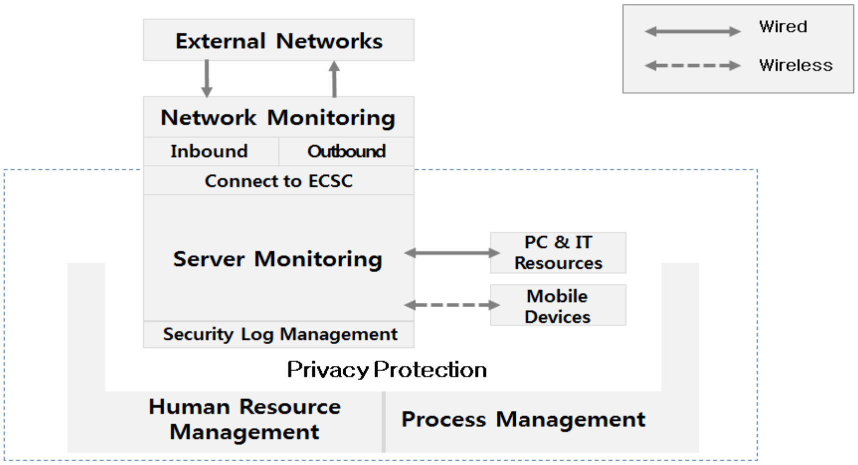

Figure 4. Proposed Security Monitoring Models

5. Discussions and Conclusions

In this study, we present a security monitoring model, taking into account a variety of university network environments.

While unspecified number of users are utilizing the PCs and IT resources of the university, the number of experts in security monitoring is lacking. In addition, the university has expanded to a mobile campus as well as a range of cloud environments. Accordingly virus and cyber-attack was revealed and the vulnerable, hence the cope for external cyber-attacks lack. The proposed security monitoring models makes several viewpoints against the weak points of university network environments. Firstly, the proposed model is based on treat management system which is provided by ECSC. It could correlate to ECSC and NCSC, then it performs the active intruder detections and preventions against the external cyber-attacks. Secondly, According to the characteristics of the university IT environment, with security control is performed with the following features:

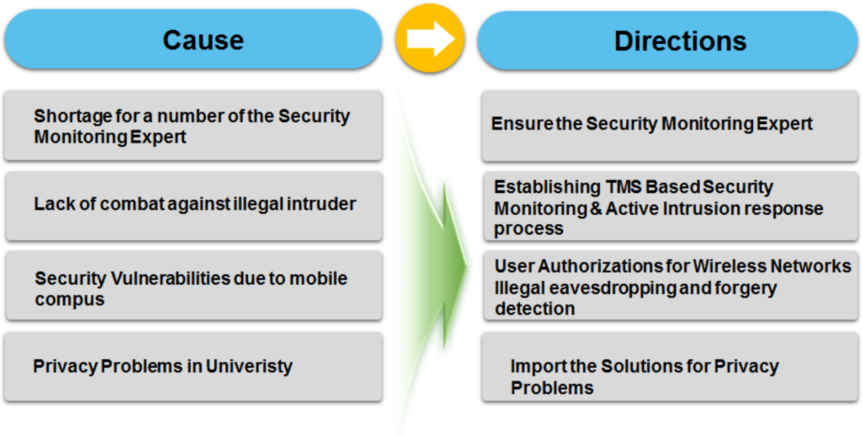
Cause
Directions
Shortage for a number of the Security Monitoring Expert
Ensure the Security Monitoring Expert
Lack of combat against illegal intruder
Establishing TMS Based Security Monitoring & Active Intrusion response process
Security Vulnerabilities due to mobile compus
User Authorizations for Wireless Networks Illegal eavesdropping and forgery detection
Privacy Problems in Univeristy
Import the Solutions for Privacy Problems

Figure 5. Directions for Security Monitoring for University Networks

In order to respond to the mobile campus to perform user identification and authentication management, and WAS & WEB SERVER monitoring. Furthermore, we should fulfill the network access control management for unauthorized connections from the place which is campus area network, but unauthorized access detection such as dormitory, graduate research laboratory and so on. When a specific event which is admission, enrollment occur, they should ensure network availability in order to prevent the rapidly increased network load. And introducing the security management agents and preparing the process for PC and IT resources management. It could realize the effectiveness with such little manpower of administrators. Lastly, we propose the customized model for preventing the private information leakage.

6. References

[1] S. Bang, S. Kang, S. Lee, and T. Kim, "A design of the DDoS defense infrastructure of a managed security service in Cloud Computing," in Proc. of the conferences of the Korean institute of communications and information sciences(KICS), Jeju, Republic of Korea, June 2011, pp. 170–171.

[2] W. Baker, A. Hutton, C. D. Hylender, J. Pamula, C. Porter, and M. Spitler, "Data breach investigations report," *Verizon RISK Team*, 1–72, 2011.

[3] B. Cho, S. Lee, and K. Dho, "A Design for Network Security System via Non-security Common Network," *Journal of the Korea institute of military science and technology*, Vol. 12, No. 5, pp. 609–614, 2009.

[4] J. Koh, T. Kim, Y. Joo, W. Kim, and K. Kang, "A Study of Asset and Risk Assessment for Established of Industrial Security Management System," *Journal of Korea Safety Management and Science*, Vol. 12, No. 4, pp. 1–11, 2010.

[5] H, Seo, J. Choi, and P. Joo, "Design of Classification Methodology of Malicious Code in Windows Environment," *Journal of the Korea institute of information security and cryptology*, Vol. 19, No. 2, pp. 83–92, 2009.

[6] Hong, N. Park, and W. Park, "Detection System Model of Zombie PC using Live Forensics Techniques," *The Journal of Society for e-Business Studies*, Vol. 17, No. 3, pp. 117–128, 2012.

[7] Y. Kim, "Sequence based Intrusion Detection using Similarity Matching of the Multiple Sequence Alignments," *Journal of the Korea institute of information security and cryptology*, Vol. 16, No. 1, pp. 115–122.

[8] A. S. Ashoor and S. Gore, "Importance of Intrusion Detection System (IDS)," *International Journal of Scientific & Engineering Research*, Vol. 2, No.1, pp. 1–4, 2011.

[9] J. Song, H. Takakura, Y. Okabe, and K. Nakao "Toward a more practical unsupervised anomaly detection system," *Information Sciences*, Vol. 231, pp. 4–14, 2013.

[10] H. J. Liao, C. H. R. Lin, Y. C. Lin, and K. Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, Vol. 36, No. 1, pp. 16–24, 2013.

[11] H. Kim, "Threat Management System for Anomaly Intrusion Detection in Internet Environment," *Journal of the Korea society of computer and information*, Vol. 11, No. 5, pp. 157–164, 2006.

[12] K. Kou, G. Mun, and D. Ryu, "A Development of AIRTMS V1.0's Security Functional Requirements based on Common Criteria Version 3.1," *Journal of Security Engineering*, Vol. 8, No. 6, pp. 645–656, 2011.

[13] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in cloud Computing," in Proc. of the International Conference on Computer Science and Electronics Engineering (ICCSEE), Hangzhou, P.R. China, March, 2012, pp. 647–651.

[14] A. Thankachan, R. Ramakrishnan, and M. Kalaiarasi, "A survey and vital analysis of various state of the art solutions for web application security," in Proc. of the International Conference on Information Communication and Embedded Systems (ICICES), CHENNAI, India, Feb 2014, pp. 1–9.