Design of the Convergence Security Platform for Smart Universities

[1]Seongho Park, *[2] Daesik Ko
[1]*Computer center, Mokwon University, shpark23@mokwon.ac.kr*
[2]*Dept. of Electronic Engineering, Mokwon University, kds@mokwon.ac.kr*

Abstract

In this study, we proposed a futuristic model of the convergence security system consisted of the security system of universities, performance disability management, and the facility security system. The proposed convergence security system model for universities is composed of the security system, performance and disability management, facility security system, and applied with the IOT live sensing technology and Big-data analyzing technology. In addition, the proposed model has been designed to support remote security systems of small universities by operating a professional security control center based in universities in the region. The results of this study can be utilized to present a direction that universities can introduce security control system or build a organized security control service system.

Keywords: *Network security, IT performance monitoring, security system design, convergence security model, total security design*

1. Introduction

Not only the large- scale domestic cyber attacks like 3.20 and 6.25, hacking incidents over the Internet are steadily increasing. Hacked system is often exploited as a pathway to spread malware or an attack tool to attack or exploit another system. In addition, an attacker who successfully hack the system will inflict great loss by destroying the system or stealing important assets from the system. In order to cope with this constantly increasing hacking incident, in addition to essential information communication system for country management such as administration, energy, and finance, the government is building and operating a security control center to take complete charge of information protection activities such as prevention activities, security system, and violation incident response at the national level [1, 2].

However, in the case of universities, only small number of universities have their own security control center with minimal standard of security personnel employment, and most universities do not introduce performance disability control center for IT resources.

In the case of universities, explosive traffic increases during the enrollment and admissions season, and most students are using mart pads and mobile devices, but the universities lack appropriate responses.

Fortunately, the Ministry of Education recently is supporting remote security system by operating Educational Cyber Security Center (ECSC).

In this study, we proposed futuristic model of convergence security system compounded of the security system of university, performance disability management, and facility security system. For this, we analyzed the current introduction situation of security solution and integrated security control system of the existing universities. The proposed convergence security control model considered the physical integrating connection of integrated security system, performance, disability management of IT resources, and facility system, moreover, it applied the IOT live sensing technology and Big-data analyzing technology. In addition, this proposed model has included the concept of expanding the cyber security center facilities and new and existing remote security control services in regional universities.

* Corresponding Author

Received: Mar. 09, 2015, Revised Mar.30, Accepted: Jul .08, 2015

2. Analysis of Current Security Control system of Universities

Recently, universities are on the trend of introducing security solution due to the increasing complexity of the IT infrastructure, and this reflect the expanding trend of ESM Solution demand with the integrated infrastructure management and security management service market by causing interest in security service. Upon this background, it is expected that the domestic SVM market led mainly by the domestic security control service providers and the local vendors through ESM, TMS (Threat Management System), PMS (Patch Management System) will be expanded with the opportunities of industrial security and convergence security market that is combined with physical security and information security management technology such as RMS (Risk Management System), SIEM (Security Information & Event Management), cyber forensics, compliance, RFID, CCTV, biometric devices, and etc.

There are four main computer security attributes. They were mentioned before in a slightly different form, but are restated for convenience and emphasis. These security attributes are confidentiality, integrity, privacy, and availability.

Confidentiality and integrity still hold to the same definition. Availability means the computer assets can be accessed by authorized people. Privacy is the right to protect personal secrets. Various attack methods relate to these four security attributes. Table 1 shows the attack methods and solutions [3].

In general, integrated security management that universities apply is the efficiency and security of integrated security management system that is used for the purpose of maximizing the improvement of security management by unified security management and operations. The integrated security system for the information system, not only has generally known as managerial security measures, but includes operational security and security incident management activities that must be performed daily, and also requires strong information security program in order to perform the infrastructure role in the physical and operational security measures and administration.

Table 1. Attack methods and security technology [4]

Computer Security attributes	*Attack Methods*	*Technology for Internet Security*
Confidentiality	Eavesdropping lacking Phishing, DoS and IP Spoofing	IDS, Firewall Cryptographic Systems, IPSec and SSL
Integrity	Viruses, Worms, Trojans. Eavesdropping, DoS and IP Spoofing	IDS, Firewall, Anti-Malware Software, IPSec and SSL
Privacy	Email bombing, Spamming, Hacking, DoS and Cookies	IDS, Firewall, Anti-Malware Software, IPSec and SSL
Availability	DoS, Email bombing, Spamming and Systems Boot Record Infectors	IDS, Anti-Malware Software and Firewall

Technically, each classified sections (network, server and systems, applications, PC security) includes its necessary information security system, and synthetically, the integrated security system that performs security management and threat management is consist of the information from these individual information security systems. In addition, recently, it includes the operations such as facility protection, physical security measures like access control, protected areas, equipment protection, power equipment, access control system, monitoring system, management tips and the collection and disposal of private information from lifecycle perspective.

However, the reality of the security services of universities is on the basic level, limited by operation of network security system and limited by merely monitoring various events that occur on the devices. The hacking techniques such as homepage change, major information leaks, and etc has been specialized and advanced over time. Although, by many private information leak incidents, the private information security is recognized as significant point of security, these issues are not reflected and operated in the service.

3. Convergence Security System Platform Design for Universities

3.1. PC Security Control Model Design of Universities

In this study, we design a security control system model for PC, which the members of universities, particularly majority of students use.

Majority security problems that occur in school network are mostly started by security trespass of universities' network connecting devices, but the reality is that it is difficult for small number of IT supervisors to manage a broad number of devices. Therefore, this document proposes a guide that focuses on the needs of device centralized security management solution to minimize the device security incidents by applying compulsory security solution.

Due to the special feature of university, before designing the objective model, we classified students' training PC from faculties' business use, and the following is the network configuration of information system for universities designed for PC security control purpose [5, 6].

In university, the proposed solutions for PC security control are the NAC sensors, NAC Policy Server, DLP PMS wireless confirm, personal information leakage protection, HOST DRM, DLP keyboard security, antivirus, USB security, and my PC protector. Since many students share the school PC lab, it is difficult to verify the identity of the users and manage the install software and patches. However, since PCs for training do not contain major tasks or data, we proposed to secure a plan to block simple OS management and IP arbitrary modifications without installation of document security solution [7, 8].

3.2. Convergence Security Platform Design for University

In this study, we proposed futuristic model of convergence security system compounded of the security system of university, performance disability management of IT resources, and facility security system. The proposed convergence security control model synthetically connects the performance and disability of the security system and information system, and the facility security control of the entire university. Moreover, the proposed model has included the system that predicts security incidents by analyzing the data collected by the IOT live sensing technology and Big-data analyzing technology. Also, it has included the concept of improving the system and expanding the cyber security center facilities and new and existing remote security control services in the Ministry of Education and the regional universities by applying professional system and security experts [9].

First of all, the purpose of convergence integrated control model we propose in this study is to build a system, in which the security issues, resources/physical control issues collected from the regional universities convergence control center and connect, share, and response effectively based on the information. On the other hand, in the case of a security issue, through the convergence control center in each regional universities, connected with Educational Cyber Security Center (ECSC), perform security control, information sharing and cooperation, and the information about the events are transmitted to National Cyber Security Center(NCSC), which is the upper institution of ECSC, and receives the security instructions and infringement recovery support. In addition, future security threats will be prepared by sharing security threats information through the connection with domestic and international CERT. Figure 1 shows the model that universities in Daejeon area, including Mokwon University, are connected with the regional convergence control center and again they are connected to other convergence control center in different regions.

Secondly, the proposed model collects events from security equipment, threatening information from TMS sensor, and events or log information from infra-equipment for information collection, and transmit them to analysis server. At this point, when cyber threat from outside is detected, it is reported to Educational Cyber Security Center (ECSC) and National Cyber Security Center (NCSC) through regional universities cyber security center, and operates violation response. Moreover, in case of disability of performance of IT resources, it is also reported to regional universities, and operates a response. By sharing the control history with other regional universities, it is possible to realize highly-sophisticated security control performance and performance disability response.

In Convergence Security Control System, facility security control refers to protecting facilities and assets containing information from illegal trespasses by using f ICT technologies and human resources, such as CCTV and security guards.

Recently, it is utilizing the parking control, fence detection, intelligent CCTV systems using ICT technologies.

Finally, the proposed model does not limit its control range to IT resources, but the entire facilities of the university. For this purpose, it collects the events and logs from the entire university facilities and networks them. Moreover, this model ensures the efficiency of the next-generational system by installing the Big-data analyzing service in order to process increased quantity and various types of data by the control range expansion. Through this proposed model, the analyzed data will be used to perform IT resource ability control and security system through a variety of procedures.

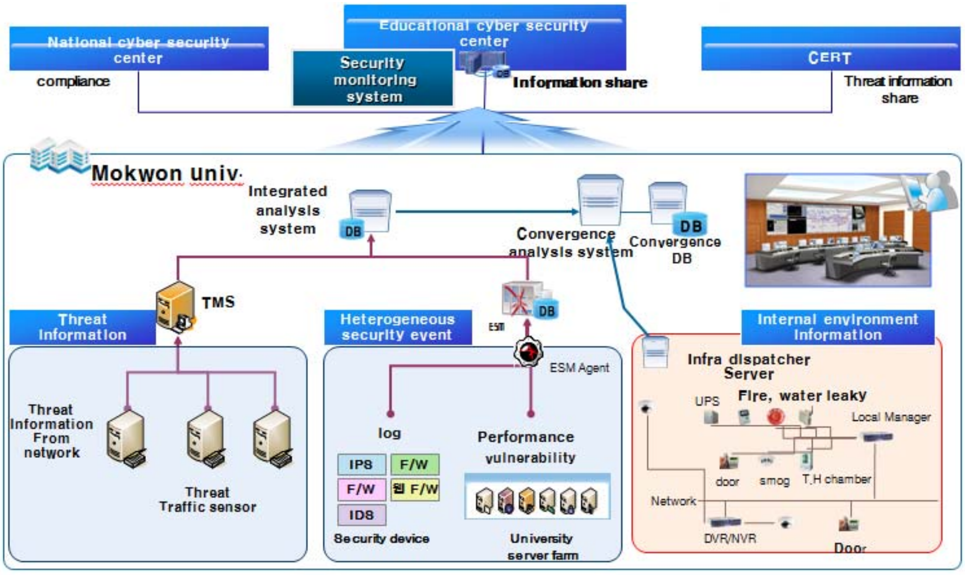

Figure 1. Convergence security for University network

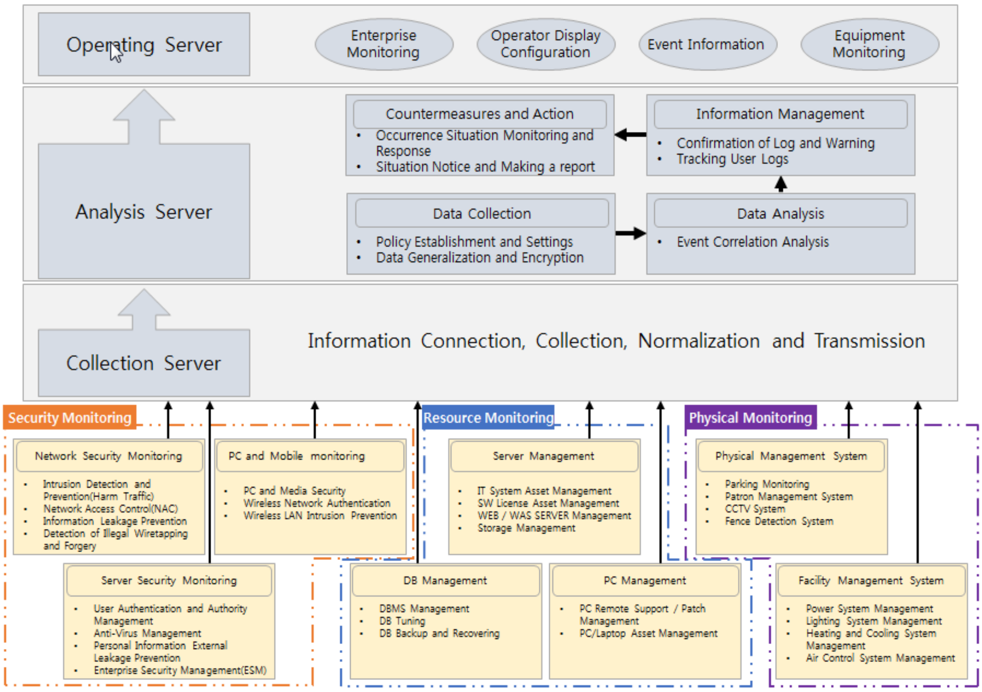
Operating Server
Enterprise Monitoring
Operator Display Configuration
Event Information
Equipment Monitoring
Analysis Server
Countermeasures and Action
Occurrence Situation Monitoring and Response
Situation Notice and Making a report
Information Management
Confirmation of Log and Warning
Tracking User Logs
Data Collection
Policy Establishment and Settings
Data Generalization and Encryption
Data Analysis
Event Correlation Analysis
Collection Server
Information Connection, Collection, Normalization and Transmission
Security Monitoring
Network Security Monitoring
Intrusion Detection and Prevention(Harm Traffic)
Network Access Control(NAC)
Information Leakage Prevention
Detection of Illegal Wiretapping and Forgery
PC and Mobile monitoring
PC and Media Security
Wireless Network Authentication
Wireless LAN Intrusion Prevention
Server Security Monitoring
User Authentication and Authority Management
Anti-Virus Management
Personal Information External Leakage Prevention
Enterprise Security Management(ESM)
Resource Monitoring
Server Management
IT System Asset Management
SW License Asset Management
WEB / WAS SERVER Management
Storage Management
DB Management
DBMS Management
DB Tuning
DB Backup and Recovering
PC Management
PC Remote Support / Patch Management
PC/Laptop Asset Management
Physical Monitoring
Physical Management System
Parking Monitoring
Patron Management System
CCTV System
Fence Detection System
Facility Management System
Power System Management
Lighting System Management
Heating and Cooling System Management
Air Control System Management

Figure 2. Logical constitution of convergence security system model

The Figure 2 shows the logical structure of the proposed Convergence Security Control System Model. The controlling system of each university is consists of security control, IT resource control, and physical control. The security control divided into network traffic control, traffic control server, PC, and mobile control, and collects data. The resource control is divided into server management, DB management, PC management. Lastly, the physical control is divided into physical management system, facility management system, and collects information. The information collect by each control systems are analyzed at convergence integrated control system, and hold operating server to assist the convenience of the administrator. The collecting server performs connection, collection, and normalization and analyzation, and transmission of the collected information from each system to the analyzing server. The analysis server performs analyzation, management of collected data, and prepares problem solving measures. Also, the operation server performs integrated control and a user interface service, event information management, and performs the monitoring equipment.

4. Conclusion

In this study, we proposed futuristic model of convergence security system compounded of the security system of university, facility security system, and performance disability management of IT infrastructure.

Due to the special feature of university, before designing the objective model, we classified students' training PC from faculties' business use, and proposed the network configuration of information system designed for PC security control purpose. Since many students share the school PC lab, it is difficult to verify the identity of the users and manage the install software and patches. However, since Lab PCs for training do not contain major tasks or data, we proposed to secure a plan to block simple OS management and IP arbitrary modifications without installation of document security solution.

The proposed model collects events from security equipment, threatening information from TMS sensor, and events or log information from infra-equipment for information collection, and transmit them to analysis server. At this point, when cyber threat from outside is detected, it is reported to Educational Cyber Security Center (ECSC) and National Cyber Security Center (NCSC) through regional universities cyber security center, and operates violation response. Moreover, in case of disability of performance of IT resources, it is also reported to regional universities, and operates a response. By sharing the control history with other regional universities, it is possible to realize highly-sophisticated security control performance and performance disability response.

The results of this study can be utilized to present a direction that universities can introduce security control system or build a organized security control service system.

5. References

[1] J. Y. Ahn, “A New Model for Fostering Security Capability by Vulnerability Reporting Center Operation”, Proceedings of KIIT Summer Conference, May 2014, pp. 500-504.

[2] Almgren, M., & Lindqvist, “U. Application-integrated data collection for security monitoring”, *In Recent Advances in Intrusion Detection*, pp. 22-36, 2001.

[3] Bhavya Daya, “Network Security: History, Importance, and Future”, http://web.mit.edu/~bdaya/www/ Network%20Security.pdf

[4] Adeyinka, O., “Internet Attack Methods and Internet Security Technology”, Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, Kuala Lumpur, 13-15 May 2008, pp.77-82.

[5] Igloo security report 2014.

[6] Jini networks report 2014.

[7] wwwjunipernet/us/en/local/pdf/whitepapers/2000384-enpdf, Defining Characteristics of QFabric by Pradeep Sindhu.

[8] wwwjunipernet/us/en/local/pdf/whitepapers/2000483-enpdf, Understanding Big Data and the Fabric System: Fabric System Enables a High-Performance, Scalable Big Data Infrastructure with Simplicity.

[9] Lee, H., and Song, J., “An Advanced Incident Response Methodology Based on Correlation Analysis of Polymorphic Security Events”, *IEICE Transactions on Communications*, Vol. 96, No. 7, pp. 1803-1813, July 2013.