On the Configuration and Improvement of Security Control Systems

Seung Jae Yoo*

ABSTRACT

Due to the advanced IT environment, the role of Security Monitoring & Control becomes more important as the cyber-crime is becoming intelligent, diversified, and advanced.

In contrast to the way it relied solely on security devices such as Firewall and IDS in the past, Security Monitoring & Control tasks responding to cyber attacks through real-time monitoring have become wide spread and their role is also important. In response to current cyber threats, since security equipment alone can not be guaranteed a stable defense, the task of Security Monitoring & Control became essential to operate and monitor security equipment and to respond in real time.

In this study, we will discuss how to configure network security system effectively and how to improve the real-time Security Monitor & Control.

보안관제시스템 구성 및 개선방안 연구

유 승 재*

요 약

IT시대의 고도화로 인한 사이버 범죄는 지능화, 다양화, 고도화 되고 있는 가운데 보안 관제의 역할은 더욱 중요해졌다. 과거 방화벽이나 IDS 등 보안 장비에만 의존하던 방식과는 달리 실시간 감시를 통해 사이버 공격에 대한 대응을 하는 보안 관제 업무가 광범위해지고 그 역할 또한 중요하게 되었다. 현재의 사이버 위협에 대해 보안 장비만으로는 안정적인 방어를 할 수 없기 때문에 보안 장비를 운영 및 감시하고 실시간적인 대응을 할 수 있는 보안 관제의 업무가 필수 요소가 된 것이다. 본 연구에서는 네트워크 보안시스템을 효율적으로 구성하는 방법과 보안시스템을 실시간 운영하는 보안관제의 현황과 개선방안에 대해 다루고자 한다.

Key words : Security Monitoring & Control System, Behavior-based Detection, Security Countermeasure

접수일(2017년 6월 15일), 게재확정일(2017년 6월 26일)

* 중부대학교 정보보호학과

1. Introduction

Due to the rapid expansion of advanced information communication networks such as computer networks and the Internet, it is spreading to all areas including individuals, organizations, institutions and facilities so that there is no place that does not use the communication network. At the same time, illegal infringement technologies using various communications have been developed and illegal activities are increasing.

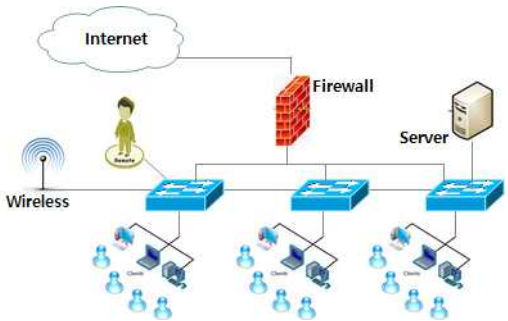
The establishment of a security system suitable for the advancement of information and communication technology is strongly emphasized as a realistic issue. In order to prevent these risks and respond in real time, security system monitor & control is being performed which is composed of Firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Virtual Private Network (VPN) in the network. However, various illegal activities that threaten information security are becoming more intelligent and diversified day by day, and so there are limits to security by simply relying on security devices. Therefore, there is a steady increase in demand for security HW / SW technology and security services.

In this study, we analyze the status of security equipment operation and Security Monitor & Control operation and analyze the pros and cons for each case of how these security devices are configured on a real network. Also we suggest more effective construction method and Security Monitor & Control operation method[11].

2. Network security equipment and Interconnectivity

2.1 Network Security Summary

Due to the structural nature of the network connection of multiple networks, the unauthorized access attempts of some networks can cause catastrophic damage to the system as well as to other networks or the entire system. Therefore, it is the most basic network security to protect internal system from external access by using network security system as well as basic user's authority and policy.



[Fig.1] Typical network configuration diagram

Hacking, unauthorized access to someone's computer for the purpose of intercepting information or deleting data and program, is basically a network-based behavior, so the network security system is at the forefront of responding to hacking intrusion. In other words, the network is the basic object of information security and, conversely, is the basic object of the hacking attack.

Therefore, it is very important to understand the network and apply security policy and system according to the purpose, size and environment of the network, and to have a thorough security consciousness by the network administrator.

2.2 Network security equipment interconnection

(1) Network security equipment function

A firewall that blocks intrusion from the outside to the inside performs Access control by ACL based on IP and Port to protect the network from external illegal access, and performs the Identification and Authentication function for (internal/external) users and the integrity checking of data, Also it performs the functions as an audit trail function as well as Network Address Translation (NAT) function, es such as VPN, PPTP, L2TP, IPsec, SSL, and NMS, etc. As such, the firewall protects the internal information and resources by protecting the network from unauthorized access, blocking unknown intentional or unintentional traffic, and isolating the internal and external networks. However, on the other hand, it has a limitation that it can not appropriately respond to detour attempts using detour access or allowed services[2][4].

In order to minimize such limitations, It is necessary to select and apply appropriate equipment considering the environment and conditions of the network in adopting firewall as follows;

- Performance, including throughput, connections per second, concurrent sessions, and encryption throughput
- Compatibility with other equipment, upgrade and service stability and operability
- Logging method, Fail-Over method, Load Balancing function, Administrator's management tool and approach, VPN function support etc.

In addition, in terms of operational management, it is very important to pay attention to design ruleset order to inspect both detailed policy and comprehensive policy in application of security policy with increasing log collection. IDS performs the functions of Detection, Notification, Connection Termination, and Session Recording, and the former implementation requirements are constant vigilance, stealth design, infrastructure, and adversary belief.

Currently, IDS uses the classification scheme of Computer Operations Audit and Security Technology (COAST). Then COAST classification is classified into the data source based (construction type) such as H-IDS(Single-Host based IDS,), MH-IDS(Multi-Host based IDS) and N-IDS(Network based IDS), and the intrusion detection model such as Misuse Detection and Anomaly Detection[1,5]. Intrusion Prevention System(IPS), a device to overcome the limitation of passive operation of firewalls and IDS, is an intelligent blocking system that protects the network from viruses, worms and DDoS by detecting harmful traffic in the network and blocking access in advance. IPS is classified into Signature Based and Heuristics based on Intrusion Detection

Model and classified as Firewall-based IPS, IDS-based IPS, switch-based IPS, and application IPS depending on the type of infrastructure solution.

VPNs built using encryption protocols provide data confidentiality, data integrity, dat origin authentication, and access control on the network. This is categorized by implementation location, configuration type, and implementation layer as shown in [Table1] below[3].

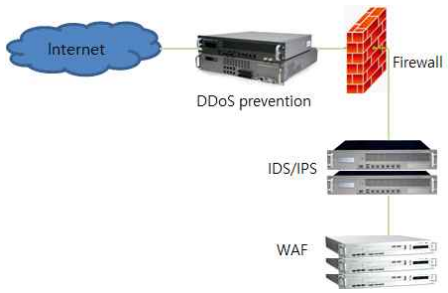
[Table. 1] VPN Classification Table

Classification by configuration type	
Application Model	Configuration type
Intranet VPN	Host/Gateway to Gateway
Extranet VPN	Host/Gateway to Gateway
Remote Access VPN	Host to Gateway
Classification by implementation location	
Equipment classification	Complex function
Firewall based VPN	Firewall + VPN (Encryption+Authentication)
Router based VPN	Router + VPN (Encryption +Authentication)
Dedicated VPN	Dedicated VPN HW/SW
Classification by implementation layer	
OSI Layer	Tunneling Protocol
Layer2 ; G2C	L2F, PPTP, L2TP
Layer3 : G2G	IPSec, VTP, ATMP
Layer4,5	SOCKS V5, SSL, TLS

The DDoS-enabled equipment which is implemented to monitor traffic on the network to block DDoS attacks (Distributed Denial of Service Attacks) and block the abnormally increased network traffic is usually configured at the top level in the network configuration. The Threat Management System (TMS) which is implemented to perform real-time cyber threat monitoring & control functions performs comprehensive threat analysis, based on traffic analysis and correlation analysis as well as detection of cyber attacks such as worms, viruses and hacking. The Unified Threat Management (UTM), which is designed to integrate the functions of each security system and solution that have been independently acting as a single device, practically manages both intra-network errors and external threats at the same time. An integrated security management system (ESM) is implemented for integrated management of solutions such as firewalls, IDS, and VPNs in one screen, and is expanding the scope of its operations, such as managing system and network resources. It is a device that plays a very important role in integrating heterogeneous devices in recent trends.

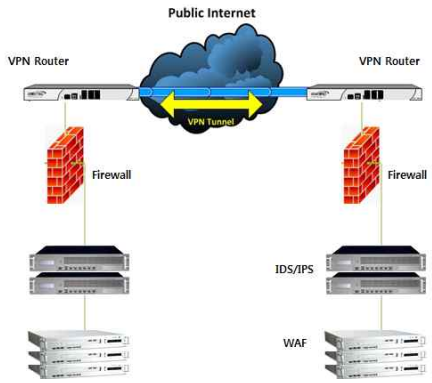
(2) Establishment of linkage considering characteristics of security equipment

In order to maximize security through the introduction of various devices like the above, it is necessary to identify the advantages and disadvantages of each equipment, and to complement each other. Since hacking attacks are changing in a variety of ways, it is necessary to build them appropriately. We compare the problems of establishing security equipment in one private network and connecting multiple private networks.



[Fig.2] Configuring security devices in a network

[Fig.2] shows the security device configuration in one network. In the case of an outside illegal intrusion attempt, first it must pass the DDoS response system with an approach that does not exceed a certain threshold. Then it should not be restricted by the firewall, not by violating the unacceptable policy, and to the next, it should not be considered an intrusion by IDS/IPS. Finally, it is necessary to pass other security devices such as a web firewall to hack the server or user PC. Therefore it is more efficient to construct multiple levels of security to utilize the role of multiple security devices, rather than relying on a single device such as UTM.



[Fig.3] Configuration using private network

[Fig.3] is a configuration diagram of private network A and private network B using VPN equipment. When the user of the private network A transmits data to the server of the private network B, since the packet is encrypted and transmitted through the VPN device, there is less concern that the content is leaked by the sniffing. The linkage of security equipment is an important process that not only complements the weak points of security equipment, but also maximizes its original functions. And to enhance the security strength and stability by making maximum use of the functions of each device. Despite the development of superior security equipment such as the next-generation intelligent IPS, the existing firewall, IDS / IPS, etc. are supplemented to establish enhanced security through linkage in many cases.

3. Security equipment configuration and Security Monitoring & Control

3.1 Security Monitoring & Control operation

Security Monitoring & Control is the task of detecting and responding to Illegal access from outside or unusual behavior inside the network to protect the information system. In this case, it is important to configure and deploy the best security equipment, by the considering the size of the various systems, equipment, PCs, etc. in operation and the level of security requirements of the organization.

The security control personnel comply with the five steps of the work procedure [(a)event detection - (b)initial analysis and action- (c)accident investigation - (d)recovery assistance - (e)report results] to take appropriate action against unusual traffic and unauthorized access from outside.

In step (a), while detecting events that occur to the controlling system, if an abnormal traffic to the network is detected, such as a web hacking attempt of the homepage or an infection signal of the malicious code from the internal user PC, immediately after that, the attacking IP is blocked and the initial action is taken (b). At the same time, additional attention should be paid to the control work because additional attacks can occur on other attack sites and other systems. (c) is the process of carrying out an accident investigation for a system when an attack is actually successful and damage occurs. The subject of the action, the target system, the time of occurrence, and the content of the damage are examined in detail from the event. (d) provides recovery measures or quick recovery guides to restart the affected system as soon as possible. Finally, at (e), everything from event detection to recovery is documented and reported. In addition, security control needs to be mandatory. Organizations need not only to operate security control mandatory but also to perform super security management for senior and lower level organizations.[9]

In security control, if each task is shared by stage and sector and is carried out nested, and if the information is shared with each other, the efficiency of security controls will be very high in response to cyber attacks.

3.2 Security Equipment Configuration Examples

In order to construct a security system optimized for the environment of the enterprise, it is necessary to consider not only a sufficient understanding of security equipment and network configuration in advance, but also the following points.

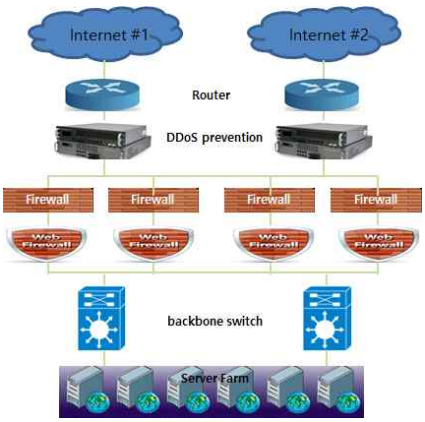
- Budget of security equipment
- Size of system accessible from outside such as web server
- Separation of the internal business network and internet network
- Scale of construction of the facility system
- Connection with other local facilities

The cost of configuring security equipment varies depending on the size of the facility. Therefore, in order to maintain security stability, basically, it is important to budget appropriately considering maintenance and ongoing update of physical parts of security equipments. Systems that are accessible from the outside or that provide external Web services are exposed to external threats, so it is necessary to thoroughly prepare against external attacks such as denial-of-service attacks, direct website hacking and website defacement. If the network is not separated, even if the server for the business file is backed up and managed separately, the risk of leakage of the internal data or failure of the system is increased when the Internet user's PC is infected with malicious code or the like.

It is necessary to accurately identify and

investigate the size, quantity and importance of the system in the facility, and so establish and manage a systematic and gradual security system suitable for the system. If the system is connected with facilities in other regions, virtual private networking is an essential component. Security Monitoring & Control and its operations are classified according to whether the security control and operation are to be carried out individually or in a centralized manner.

Next, we look at some examples of network security configurations in operation actually, and look for their pros and cons and improvement. And so, by comparing the pros and cons of each security system, it is possible to select the appropriate security system for the organization.

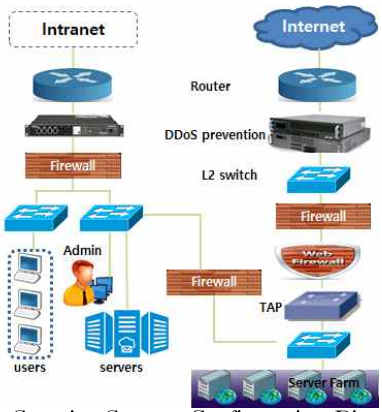


[Fig.4] Security System Configuration Diagram1

In Figure 4, Internet#1 and #2 are considered to be internal networks. The DDoS protection system is located in the area where the router passes and touches to enter the network through the Internet. The DDoS prevention system is to place the top of the network in order to prevent an overload attack by blocking the illegal traffic access at the beginning. Among the traffic that is judged normally, there is an attempt to illegally or abnormally access the internal system from the outside, and the firewall blocks them based on the IP and Port.

Next, the web firewall (WAF) detects and blocks abnormal attempts for SQL injection or other web hacking on the web through signature or other pattern detection. This configuration is analyzed as a structure to protect the server farm, and it is identified as some structure method used in facilities or institutions.

In [Fig.5], the internal network and the Internet network are distinguished, and it can be understood that the system is an overall configuration diagram.

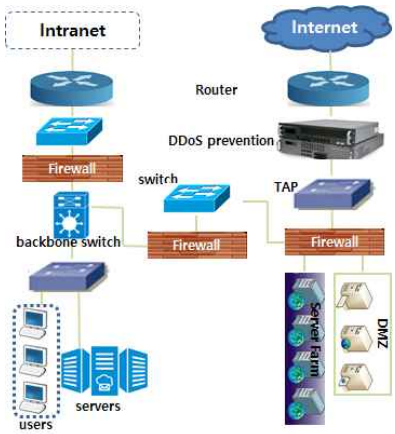


[Fig.5] Security System Configuration Diagram2

While it comes down from the top of the internal network, it reaches the firewall system via router and L2 switch. It goes through the internal network's firewall and into the user's PC and the administrator or internal server. Here, it can be seen that the L2 switch

has been installed at the top of the user and the administrator, so it is separated from the inside by itself. The use of firewall in the connection between the internal network and the Internet network is used for the security policy for the internal network administrator to use servers and devices in the Internet network. Only the administrator of the internal network can manage the server of the Internet network through the access control of the firewall. Looking at the composition of the Internet network, DDoS prevention equipment is essential since most server farm configurations provide external services. [Fig.5] differs from [Fig.4] in that it is the arrangement of the TAP equipment. The TAP is a device that handles network traffic and access log, and transfers traffic to the console server by mirroring the traffic. In other words, it performs console or remote monitoring of all traffic passing through the web firewall.

In [Fig.6], the TAP equipment is located at the bottom of the DDoS prevention system and collects packet information about the traffic that normally passes through the DDoS protection system. Also the TAP is located at the top of the firewall. In fact, if the system is sensitive to external access records, it is meaningful to collect more access information by placing TAP equipment at the top of the firewall.



[Fig.6] Security System Configuration Diagram3

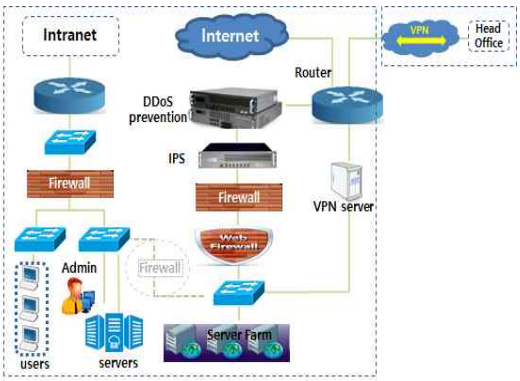
But, if it is not sensitive to external access, it is also possible to place TAP at the bottom of the firewall so that internal users and servers can be monitored with certainty, even though it is not possible to collect packet information about external illegal access.

[Fig.7] Security System Configuration Diagram4

In [Fig.7], IPS can be detected and blocked by signature, pattern detection, and so on which is a step up from the firewall. Inbound packets coming from the outside come down to the firewall through the first DDoS prevention equipment, secondarily pass through the firewall, and deploy IPS to detect and

block specific attacks. Only packets passing through the IPS are collected in the TAP log, which can reduce the collection and improve the accuracy of the detection.

In [Fig.8], the internal network and the Internet network are separated, and the user and the administrator/internal server are separated in the internal network. The Internet network consists of DDoS prevention devices, a firewall, a web firewall, and a server farm in that order. The VPN can be connected to the main office VPN through a VPN under the configuration through the security devices.



[Fig.8] Security System Configuration Diagram5

In addition, the administrator in the internal network can manage the server farm of the Internet network through the additional connection (dotted line in the middle) between the internal network and the firewall of the Internet network.

3.3 Configuration Problems and Solutions

Configuration Diagram2[Fig.5] shows that the internal network and the Internet are separated, and there is a TAP equipment at the bottom of all security devices in the Internet Network. This means detection only for packets that pass through security devices, and it is also a way to increase TPR(True Positive Rate). However, there is a problem that the outbound packet can not be properly monitored because there is no real-time detection device in addition to the security device in the internal network. For example, due to a PC infected with malware, the infected signal transmitted to the malicious code route or the data transmitted to the server of the hacker are all outbound packets. Therefore, it is necessary to monitor the packet information of the user PC or another internal system in real time by placing TAP equipment on the top or bottom of the internal network firewall.

In Configuration Diagram3[Fig.6], the TAP equipment of the Internet network collects all the packets before being filtered by the firewall, so the amount of packet log collection on the Internet network increases sharply. Therefore, although the load on the TAP equipment can occur, there is an advantage that the false accept rate (FAR) can be significantly reduced and the initial response to illegal access is easy. In addition, in the internal network, an additional TAP device is placed directly above the user, which is a very effective configuration for malicious code.

In Configuration Diagram5[Fig.8], it is difficult to detect in real time because the TAP equipment is not configured. Therefore, it is necessary to construct TAP equipment at the bottom of the firewall of the internal network and the Internet network, respectively, to perform real-time monitoring. It is not possible to

completely detect the illegal access attempts with security equipment and it is the same for malicious code infected signal, so it is necessary to monitor directly by administrator using TAP equipment. In the internet network, IPS is located at the top of the firewall. IPS is designed to perform detailed and specific detection and blocking with detection patterns and detection rules for all packets received through DDoS equipment. Therefore, in order to maximize the cost effectiveness of the IPS, it is desirable to switch the IPS to the bottom of the firewall to improve its performance.

However, the number of IDS and TAP equipment that can be constructed in actual system configuration is limited. In many cases, there are multiple distribution points at optimal locations for building TAP equipment, such as the bottom of a firewall or switch. Therefore, in these cases, in order to monitor the entire system, even if the FRR (false rejection) increases, it is inevitable to consider the construction of the TAP location on the firewall or the switch.

3.4 Recent Trends of Security Control System

As a global security threat, mobile security, ransomware attack, sandbox bypass attack, distribution of SNS malicious code and big data security analysis for APT are suggested.[7]

However, monitoring using existing security devices is limited to traditional security control areas such as intrusion prevention by firewall, Web based attack detection through web firewall, DDoS defense through DDoS countermeasures, signature based intrusion detection and defense through IDS / IPS. And so, there is a serious problem that it is impossible to cope with such an intelligent attack only by monitoring the existing security equipment.

[Table2] Existing Security Countermeasures

Attack target	Attack type	Countermeasures
Network·System attack	IP/Port/Packet forgery, Web shell	F/W, IPS Web Shell detection
Service blocking attack	DoS/DDoS	Anti-DDoS
User-directed attack	Phishing, Ransomware	User security education, Sandbox

As shown in [Table2], these countermeasures are based on the provision of signature solutions, and behavior-based threat countermeasures are emerging as measures to overcome such limitations.

The security management system event classification and comprehensive analysis are summarized as follows;

- Security events : Various log security events from F/W, IPS, IDS, VPN, WAF, server, DB, etc.
- Harmful traffic event : Traffic threat event, Signature-based intrusion detection event,
- Forgiven Events
- Logs collected by EMS : Threat informations, logs generated from information protection products,
- Logs collected by TMS : Signature based

detection, intrusion threats, harmful traffic threat information

[Table3] Comparing Signature and Behavior Based Methods [6]

	Signature-based method	Behavior-based method
Detection method	malicious code signature comparison	abnormal/malicious behavior analysis
Target of detection	endpoint & network information	endpoint/network behavior
Malicious behavior detection	△	○
Detour attempt Response	×	○
Operator response Needs	No	Necessary
Main Products	Vaccine, DPL, F/W, IPS, etc	ERD, NTA, SIEM, etc

IP, port-based network layer detection, or malicious IP (known attack-based) detection and analysis are not possible for unknown attack detection and application detection. It is impossible to respond to APT attacks. And it is difficult to analyze the association between attacks in an integrated security environment. The difference between the signature method and the behavior based method is summarized as [Table3].

Therefore, it has become necessary to extend monitoring to traffic / packet and host event areas to detect not only the old traditional security control area, but also the symptom of signature- based attacks. In order to expand the monitoring area, a new method such as a mathematical analysis or a behavior analysis method should be applied to create a ruleset capable of detecting an unknown attack, which is not possible with the existing analysis method. By doing so, profiling of intelligent attacks will become possible, and further predictions and preemptive responses to attacks will become possible.[8]

4. Conclusions

With the expansion of the advanced IT era, cyber crimes become more intelligent, diversified and advanced, and the role of security control becomes more important. In contrast to the previous method that relied solely on security devices such as firewall and IDS in the past, the security control task of responding to cyber attacks through real-time monitoring has become widespread and its role becomes important. Since the current cyber threats can not be reliably protected by security equipment alone, it is essential for the security control to be able to operate and monitor security equipment and to respond in real time. Beyond monitoring, which is simply a concept of security management consultation, the primary cyber infringement countermeasure task are performed in the security control area.

In order to safeguard the communication network, the institution or the facility must prepare the security control measures and must fulfill them mandatory, and establish the institutional system to supervise the security control. An important part to be equipped after

such institutional systems are provided is the way of building security devices and the ability to control them.

It will be necessary to construct systematic and stabilized security equipment. And, in order to control it, it is required the new knowledge on changing network environment, security equipment, system configuration and periodical education for job capacity enhancement. As the number of new or variant attacks increases, the control personnel need to develop and specialize accordingly. In addition, there should be continuous development of security systems to detect and block various unknown cyber attacks. It will be continuous to develope the additional technologies such as data inference, statistical analysis, modeling for which improve detection accuracy. And using these results, it can respond to intelligent attacks properly, and then it will be a trend of next generation security control.

References

[1] Park, Si-Jang; Park, Jong-Hoon, “Current Status and Analysis of Domestic Security Monitoring Systems”, The Journal of the Korea institute of electronic communication sciences, Volume 9, Issue 2, 2014, pp.261-266

[2] Eric Cole, Ronald L. Krutz and James Conley, Network Security Bible, John Wiley & Sons Inc., 2005

[3] John R. Vacca, Computer and Information Security Handbook, Elsevier, 2013

[4] Michael E Whiteman and Herbert J. Mattord, Principle of Information Security, Thomson, 2003.

[5] Paul Campbell, Ben Calvert, Steven Boswell, Security+Guide to Network Security, Thomson, 2003.

[6] Next Generation Behavior-based Threat Detection, http://blog.lgcns.com/1221

[7] McAfee Labs Threat s Report, 2014

[8] 곽희선, “진화하는 APT 공격에 대응한 보안관제의 진화 방안”, IDG Summary, 2015

[9] 김귀남 외1명, “데이터 마이닝 기반 보안관제 시스템”, 정보보안논문지 제11권 6호, 3-8, 2011.

[10] 신휴근, 김기철, “보안관제 기술동향 조사 및 차세대 보안관제 프레임워크 연구”, 정보보호학회지 제23권 제6호, 2013.

[11]이동휘, 하옥현 “융합보안관제시스템 개선에 관한 연구”, 융합보안논문지 제11권 제5호 pp.3-12, 2011

[저자소개]

유 승 재 (Seung-jae Yoo)
1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교 정보보호학과 교수
email : sjyoo@joongbu.ac.kr