Design of Security Management System

Seoksoo Kim*, Wooyoung Soh
Dept. of Computer & Multimedia Engineering
Hannam University, Daejeon, Korea

ABSTRACT

Enterprise security management system: Enterprise Security Management (EMS) is centralized integrated management of other kind of security solutions such as intrusion cutoff system, intrusion detection system and virtual private network. With the system, it is possible to establish security policies for entire IT system through interlocking of solutions. A security system of company network is progressing as a ESM(Enterprise Security Management) in existing security solution foundation. The establishment of the security policy is occupying very important area in ESM of the security system. We tried to analyze existing ESM system for this and designed security solution structure for enhancing the inside security. We applied implementing directly IDS system and tested. This test set the focus about inside security

Keywords: *ESM, Security, IDS, Firewall, Network*

1. INTRODUCTION

Firewall is to protect and isolate the system so that security accidents or threats to the network do not spread. This is an active defensive measure that allows permitted or authenticated traffics and blocks the incoming of illegal traffics to protect the internal network of a specific organization.
The basic purpose of firewall is to reduce the risk zone while guaranteeing transparency to network users. There are mainly five types of firewall as follows.
First, in packet filtering, the network level system is determined by the addresses and ports of the sender/receiver of IP packets and simple routers provide network level firewall. Because this has complicated rules for determining packet operation and network routes, it is hard to decide. Moreover, current network level firewall is so complicated that it can manage the state of connection, data contents, data types, etc. A distinguished point is that the network level intrusion interception system can control routers directly, allow them to use assigned IP blocks legally and guarantee fast and transparent services to users [1,2].

Second, application gateway means a machine that executes a proxy supporting the interruption ad log of direct traffics between two networks, audit function, etc. Because proxy application is a software part of firewall, it will be desirable to assign it many log and access control functions. Application level firewall is not transparent to ordinary users and requires transparency, and provides a detailed audit report and a more client setting. Recent application level IDS guarantees effective security model than network level firewall. It runs on the application layer, has separate gateway for each interpretation service, and can control packet filtering and packet data.

Third, circuit gateway exists between the 5th layer and the 7th layer of OSI network model and, different from application gateway, it has a general proxy usable to any applications. In order to connect to the internal network through firewall, a client needs a modified client program that can recognize the circuit proxy. Thus, its disadvantage is that only clients equipped with a modified client program can form a circuit.
Fourth, stateful inspection, which analyzes state information, is essential for processing new connection requests because information analysis of a single packet in existing routers is not sufficient for complicated services and high security. In new connection, the analysis of information derived from previous connections and from the corresponding applications is important in deciding the acceptance and rejection of new connection.

Fifth, there is hybrid firewall composed of various types of firewall. Functions may be assigned selectively according to the kind of services and in consideration of users' convenience and security. But this type of firewall may have difficulties in building and managing because various security policies can be applied according to the kind of service [3].
Intrusion means all actions that infringe the security elements of a computer system through unauthorized access. There are many types of intrusion including port scanning for access andactual intrusion through password hacking. Intrusion detection is to monitor a host or a network to prevent intrusions and intrusion attempts and give real-time warnings to detected intrusions. The concept of intrusion detection was introduced first by J.P Anderson in 1980 and the procedure of intrusion detection is generally composed of information collection → information processing and abstraction → intrusion analysis and detection →report and action.

* *Corresponding author. E-mail: sskim@hannam.ac.kr*
Manuscript received Sep. 16, 2005 ; accepted Oct. 18, 2005

"This work was supported by a grant No.(R12-2003-004-03003-0) from Ministry of Commerce, Industry and Energy"

IDS is a intrusion detection system that collects data from the system to be protected, filters out redundant or useless data, detects intrusions using detection techniques and gives corresponding responses. It guards the entrance of a network, inspects incoming and outcoming packets according to preset security policies, and compares them with rules to determine the passage. A difference of IDS from firewall is that IDS inspects all packets transmitted inside the network including those going out from and coming into the network.

IDS can be divided into host-based one and network-based one. Network-based IDS receives and analyzes packets for all traffic in the network and processes detected intrusions automatically. It is particularly excellent in detecting accesses unauthorized or exceeding the given authority. It can be used without additional setting of hosts and servers in the network and its failure does not cause serious damage.

On the other hand, it has difficulties in detecting attacks against threat elements with complicated information, requires the exchange of a huge amount of data through analysis and, for this, has to filter data through data abstraction for analysis.

Host-based intrusion detection system detects intrusions in a single host. It detects intrusions by inspecting host audit records, incoming packets, etc., monitors the process of logging on the host, watches over root users' behavior, and discovers intrusions through file system monitoring.

Host-based intrusion detection system is a powerful tool that can trace back attacked data through the log list on intruders' attacking, and is more effective in detection than network-based intrusion detection system. A disadvantage of host-based intrusion detection system is that, because the intrusion detection system needs to be installed in the target host, the performance of the host is lowered and setting of logging and other features for obtaining data is troublesome. In consideration of its high detect ability, this study used host-based intrusion detection system to design the enterprise security management system proposed [4].

2. DESIGN OF SECURITY MANAGEMENT SYSTEM

2.1 Concept of enterprise security management system

Enterprise security management system: Enterprise Security Management (EMS) is centralized integrated management of other kind of security solutions such as intrusion cutoff system, intrusion detection system and virtual private network. With the system, it is possible to establish security policies for entire IT system through interlocking of solutions [5].

The current level of enterprise security management technology implements a monitoring function in the same type of products but it will be developed in the future through the standardization of security protocols to have functions that monitor heterogenous security systems including other types of products, analyze collected data, report security accidents, and manage detailed policies of each security system. Representative security standard protocols for enterprise security management are OPSEC that organizes framework partners in the servers of contents security, authentication and authority management, IDS, accident analysis and reporting and directory centering on Firewall-1/VPN of Check Point Software Technology, and IDWG working group that builds IDS interlocking message standard of IETF.

According to workflow, ESM can be classified into user, policy manager, and the evaluation of vulnerability and threat [6].

2.2 Necessity of enterprise security management system and request point

With the growing importance of security management, a increasing number of companies are adopting enterprise security management (ESM) solutions. The solution is being developed toward centralized management of various heterogenous security solutions with minimizing wrong detection through analyzing interconnectivity among security solution events. It reduces the consumption of resources and improves the efficiency of centralized management.

With the activation of business, information systems are exposed to insiders and outsiders. As a result, the reliability of companies and the availability of services are being threatened.

According to the result of a survey on information protection conducted by the Ministry of Information and Communication, domestic organizations' investment in information protection is much less than those in developed countries. Particularly with regard to the pattern of security solutions, preparation against intrusive accidents such as enterprise security management and weak point analysis is quite poor. This is quite serious considering that the Internet turmoil on the 25th of January this year and many complex cyber intrusion accidents happened because the managers failed to cope with intrusions adequately.

In reality, however, it is not easy to prepare an organization and manpower exclusive for information protection that can detect abnormal symptoms through analysis of interconnectivity while operating each of different security solutions. It is because there are not many specialists in security solutions despite the increase of various specialized security solutions such as firewall, IDS, virtual private network and antivirus. Furthermore, a security manager cannot prevent and cope with all intrusions. A huge number of security events and analysis tasks processed by each security solution cannot be handled manually at all.

With the growing importance of security management, a increasing number of companies are adopting enterprise security management (ESM) solutions. The solution is being developed toward centralized management of various heterogenous security solutions with minimizing wrong detection (false positive) through analyzing interconnectivity among security solution events. In addition, it automates simple routine tasks (monitoring/log analysis, report generation, etc.) performed by company security managers so that the managers can concentrate on important tasks such as the establishment of information protection policies and guidelines and, by doing so, secure the continuity of business [6].

However, such enterprise security systems have a tree structure as in Figure 1. Thus, as mentioned earlier, security should be implemented inside and outside in this structure. However, currently available enterprise security systems are exposed to internal risks although they can establish security policies suitable for each company (network speed, the importance of security, etc.).

In order to prevent exposure to internal risks, the internal server has to have another security system. If the system is secure only from external intrusions but vulnerable to internal intrusions, hacking or a mistake by an internal member may result in the exposure of other members' computers. In such a situation, however thorough the external security is, it can be useless.

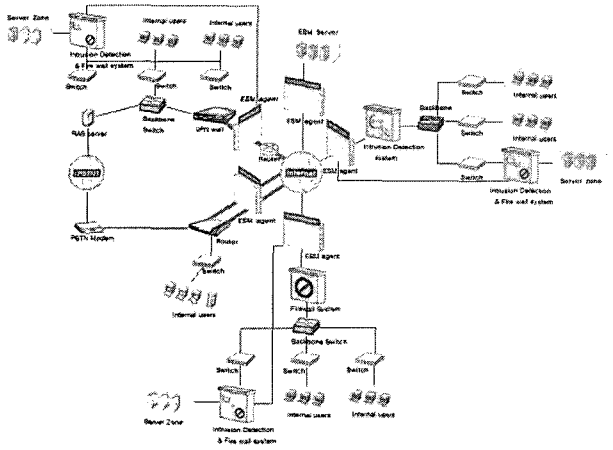


Fig. 1 Structure diagram of proposed enterprise security management system

In Figure 1, a company can choose VPN, IDS or intrusion cutoff system according to its security policy, and IDS or firewall internally according to its need, but it is internally and externally secure to establish all systems in the ESM agent. Evaluation on system security may be different according to security systems used and security policies in enterprise security management.

3. COMPARATIVE SYSTEM ANALYSIS

We tested A-system mentioned above with actual intrusions. The results are as follows.

Table 1 shows the numbers of intrusions attempted by seven computers through the Web and the numbers of attempts to connect through Telnet with six IDs in A-system. When a computer with a specific ID attempted to access, the number of data connections, data traffic and average data traffic were analyzed and, if intrusion was detected, the computer was cut off.

Table 1. A-system test list

HOST	Web log	ID	Telnet log
Total	256	*Total*	132
203.247.63.144	175	*root*	28
203.247.63.145	45	*test1*	23
203.247.63.146	7	*test2*	31
203.247.63.147	5	*test3*	17
203.247.63.148	1	*test4*	13
192.168.0.3	15	*test5*	20
192.168.0.5	8	---	---

Table 2 shows the result of real-time detection of intrusions through the Web and Telnet in A-system. The Web includes a cutoff function that can cut off hosts.

Table 2. A-system result list

HOST	Web log	ID	Telnet log
Total	233	*total*	100
203.247.63.144	175	*root*	28
203.247.63.145	45	*test1*	20
203.247.63.146	7	*test2*	12
203.247.63.147	5	*test3*	18
203.247.63.148	1	*test4*	7
192.168.0.3	No search	*test5*	15
192.168.0.5	No search		

4. CONCLUSIONS

Enterprise security management system: Enterprise Security Management (EMS) is centralized integrated management of other kind of security solutions such as intrusion cutoff system, intrusion detection system and virtual private network. With the system, it is possible to establish security policies for entire IT system through interlocking of solutions .

The present study analyzed the development process and direction of security system, which has evolved from firewall to IDS and enterprise security management system, proposed a structure of security system that is efficient in reinforcing internal security, which is the most fundamental goal of security system, and applicable to any security policies in building enterprise security management system. In addition, we implemented the structure, tested its performance and confirmed that internal security was improved. However, the addition of security system may cause the rise of cost as well as low network speed..

REFERENCES

[1] Jae-Hyeon Kim, Ja-Young Jo, "K4E Security technic of Firewall", Korea information processing society, Vol.9, No.1, 2002.1

[2] Ju-Young Li, "Design and Implementation of Network-based Intrusion Detection system for Protocol attack", master's thesis, 2002.4

[3] Sang-Hoon Lee, Goung-Hwa Do, Kyung-Won Jung, Moon-Seok Jung, "Design of packet filtering module for Firewall to prevent an inside network utility with malice ", Korea Information Science Society, Vol.29, No.2, 2002.10

[4] Hyun H. Choi ,Tai M. Chung, "A Study on Generalization of Security Policies for Enterprise Security Management System", Korea information processing society vol.9-C, NO 6, 2002.12.

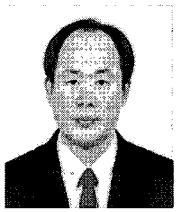
[5] Youn-seo Jeong, Bae-wook Park, Syng-won Sohn, Chang-Seok Oh, "Design of security management system for Internet of safety ", Korea computer information society Vol.7 No.3, 2002.12.

[6] Dong Young Lee, Dong Soo Kim, Tai Myoung Chung "A Study of Hierarchical PolicyModel of Policy-based Integrated Security Management for managing Heterogeneous Security Systems", Korea information processing society vol.8-C NO.5, 2001.10.

Seoksoo Kim

Received a B.S. degree in computer engineering from Kyungnam University 1989, and M.S. degree in Information engineering from Sungkyun-kwan University 1991 and Ph D. degree in Information engineering from Sungkyunkwan University 2002.

In 2003 he joined the faculty of Hannam University where he is currently a professor in Department of Computer & Multimedia Engineering. His research interests include Multimedia Communication systems, Distance learning, Multimedia Authoring, Telemedicine, Multimedia Programming, Computer Networking. Information Security. He is a Member of KCA, KICS, KIMICS, KIPS, KMS, and DCS.



Wooyoung Soh

Received a B.S. degree in Computer Science from Jung-Ang University 1979, and M.S. degree in Computer Science from Seoul National University 1981 and Ph D. degree in Computer Science from Maryland University 1991.

In 1991 he joined the faculty of Hannam University where he is currently a professor in Department of Computer & Multimedia Engineering. His research interests include Nueral Networks, Information Security, and Computer Networking. He is a Member of KIPS, KIISC, KMMS, KIAS, and DCS.