Computing and Informatics, Vol. 24, 2005, 109–121

DEVELOPMENT OF THREAT EVALUATION TOOL FOR DISTRIBUTED NETWORK ENVIRONMENT

Keun-Hee Han, Il-Gon Kim
Kang-Won Lee, Jin-Young Choi*

Department of Computer Science and Engineering
Korea University, Seoul, Korea
e-mail: {khhan, igkim, kwlee, choi}@formal.korea.ac.kr

Sang-Hun Jeon

Infosec Co., Ltd.
Seoul, Korea
e-mail: winsnort@securityindepth.net

Manuscript received 10 May 2004; revised 6 April 2005
Communicated by Jiří Šafařík

Abstract. Current information protection systems only detect and warn against individual intrusion, and are not able to provide a collective and synthesized alert message. In this paper, we propose a new Meta-IDS system which is called "SIA System". The SIA system can filter redundant alert messages, analyze mixed attacks using correlation alert messages from each sensor and respond to security threats quickly, after classifying them into one of four different statuses. Then we implement the SIA system and test the efficiency of it in the managed networks. Thus we confirm that the SIA system enables security managers to deal with security threats efficiently.

Keywords: ESM (Enterprise Security Management), SIM (Security Information Management), SIA (Security Information Alert), IDS (Intrusion Detection System)

[*] Corresponding author: Jin-Young Choi

1 INTRODUCTION

Security systems such as IDS (Intrusion Detection System) and Firewalls have been developed to detect and protect these systems in both wired and wireless networks. However, along with the changes that have occurred in the patterns of attack and the increasing use of variant methods, more and more attacks are now using diverse and mixed techniques rather than being limited to a single attack technique or making use of multiple exploits [4]. Unfortunately, current information protection systems only detect and warn against individual intrusion, and are not able to provide a collective and synthesized alert message.

Therefore, it is very difficult to detect and react effectively against variant exploits. It not only takes a lot of time to analyze and determine practical vulnerabilities from the huge amounts of collected data in order to detect potential information and protect the system, but also requires a lot of manpower, skilled in such security issues.

Various methods have been used in order to solve these problems. References [2] and [11] proposed the translation of security information from IDS log to Hybrid format. Papers [11] and [10] were concerned with reducing false alerts by correlating intrusion alerts and limiting the scope of redundant alert data. Studies [10] and [1] proposed a methodology for identifying complex attacks using the data warehousing and data mining methods.

In this paper, we propose a method of correlating the alerts provided by IDS systems and Firewalls, and demonstrate the contribution of this method to the detection of DDoS (Distributed Denial of Service) attacks, and test and implement a new algorithm and security model which can be used to tackle security problems quickly through the support of background data. Our approach facilitates the creation of the information necessary to evaluate the degree of danger, together with the attack status of the managed network environment.

The remainder of this paper is organized as follows. Section 2 explains related works of the SIA (Security Information Alert) system, and current security system status levels. Section 3 explains the evaluation criterion used in the SIA system. Section 4 shows the implementation of the proposed model, along with the experimental results. Finally, Section 5 concludes this paper.

2 RELATED WORKS

There are several approaches which have been taken in order to extract useful information from alerts or events gathered from Multisensor (Firewall, IDS, Network Scanner, Syslog, etc.) [6, 8, 9, 12, 13]. These methods originated from the requirement to integrate and analyze the data from the various established security solutions, and have evolved so as to interface with systems that offer a higher degree of security, as the information systems themselves have grown. The format in which alerts and events are stored varies from one vendors' product to another, and this inconsistency in the event format poses a problem when it comes to analyzing log data synthetically and may confuse the information security manager, with the result that it is difficult for him or her to recognize an attack.

To solve this problem, several different approaches have been used in an attempt to obtain a uniform result from the sensors' alerts and events. Meta-IDS [7] is a management system that can track alert data flowing from a Host-IDS to a Network-IDS. There have been two approaches to constructing Meta-IDS systems. In the first approach, the log data is converted to a standard format just before it is displayed on the console. In the second approach, the security alerts are translated into a format which is suitable for storing the data from each vendor's product. The current ESM (Meta-IDS) model supports message integration by means of an agent. However, it is difficult to integrate different vendors' agent alert data.

To solve this problem, for which there is no uniform guideline, the Intrusion Detection Exchange Format working group (IDWG) of the IETF (Internet Engineering Task Force) is currently working on standards that will enable different IDS systems to communicate with each other, as well as with security consoles. However, due to the lack of interest on the part of the security system companies about IDMEF (Intrusion Detection Message Exchange Format) [5, 3], IAP (Intrusion Alert Protocol), CIDF (Common Intrusion Detection Framework) and IDXP (Intrusion Detection Exchange Protocol) in developing a standard format, and their reluctance to abandon their own event representation, the current ESM (Enterprise Security Management) or SIM (Security Information Management) system provides just simple event format translation.

3 SIA SYSTEM

3.1 Overview

In the ESM systems, there are two approaches to unify the log data for an evaluation of a security threat. One approach involves converting the log data from each security product into a standard format, while the other involves translating the log data from one security product's format to another's. The ESM can extract the essential information from the bulk log data using a standard format. There are several advantages to the SIA System's logic, including the possibility of combining the logs from various security systems, integrating the messages from IDS and Firewalls, and analyzing a large amount of raw data.

However, the particular benefit of the SIA system is that it can reduce the number of false alarms that occur in large distributed networks and systems, recognize the security threats more easily, and facilitate the establishment of a contingency plan to deal with these threats.

The SIA System can notify the system administrator of security threats to information systems, by applying problem finding logic after storing the information obtained from the different security products in a common database. This application of such logic is useful for identifying the overall threat, but not for individual, specific threats. It is possible to determine the level of the security threat based on the source IP and the destination IP.

3.2 Proposed Differentiated Intrusion Alert Model

The intention of an attack can be summarized as consisting of four different statuses. The categories of the attack statuses are determined according to the method of attack used against the managed network assets. The attack types can be divided into four levels, namely 1:1, 1:N, N:1 and N:N. Because the current IDS and ESM systems generally evaluate network intrusion traces in managed networks as being individual attacks, it is very difficult to generalize security threats. Therefore, classifying the attack types syntactically facilitates the identification of security threats.

In order to accomplish this, it is first necessary to survey the attack status of managed network assets and to analyze the detailed alert information. This means that the existing IDS and ESM systems concentrate on detecting the individual attacks, whereas the SIA system focuses on evaluating the overall security threats including a mixed attack. The four attack statuses recognized by the SIA system are as follows:

1. an attack by multiple attackers on one target host,
2. vulnerability scanning and an attack in a managed network,
3. an attack on a specific destination host in an information network, and
4. large scale scanning multiple hosts.

Most information security systems generate alerts and events in the case of a specific attack, with the result that they can create false alarms and have difficulty handling an individual alert message. For example, the Nimda worm includes mixed threats with an attack pattern consisting of the Unicode attack and the CodeRed backdoor attack. In general, security systems' sensors (Multisensor) cannot easily detect these types of attacks.

Therefore, this paper proposes a new intrusion detection model that can better evaluate the overall attack flow, rather than being concentrated on one individual attack, by sorting the security threats according to the four different statuses defined above, based on the intruder IP and the destination IP.

Figure 1 shows the four different security threat statuses. The threshold value is referred to as the value used to determine the threat status by using the intruder IP and the destination IP. The status is determined according to this threshold value. The threshold value can differ depending on the scope of the managed network system. More precisely, each status is determined according to the intruder host count and the destination host count in the distributed network environment. The threshold value can be varied, by taking into consideration the managed network status. For example, if the intruder host count is small and the destination host count is large, the potential security threats are the network subnet scanning, the

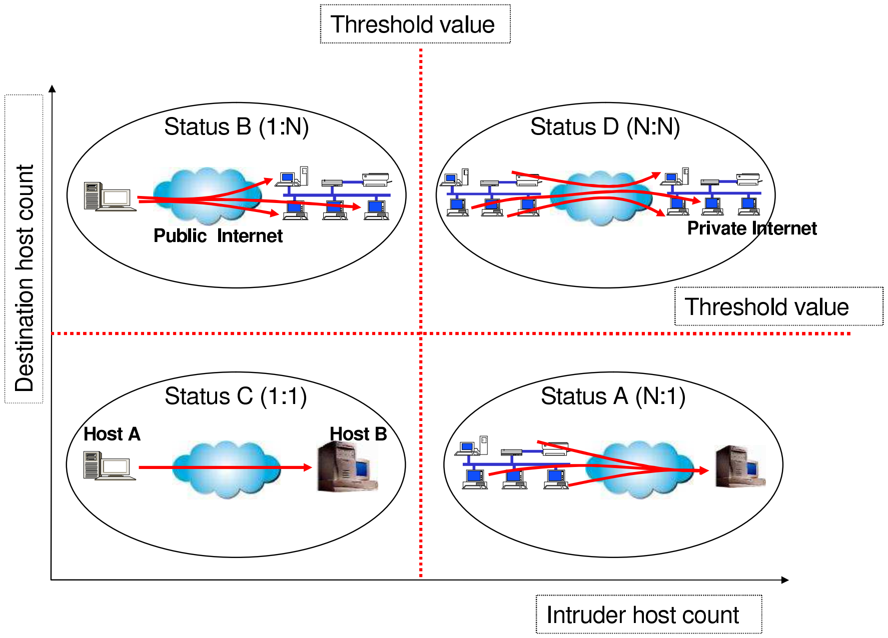

Fig. 1. New analysis method of SIA

full scanning of a single host or a DDoS attack from multiple hosts on a few target hosts. The basis for evaluating the attack as being Status A, B, C or D is not just dependant on the alert messages from the sensor, but is also dependent on whether the attack is on the target resource or is a general threat to the network system. Furthermore, the information concerning the intruder IP address and destination IP address is used to discriminate the security threat in a managed network. The status values for security threats in a managed network can be summarized as follows;

Status A: N:1 attack type (many hosts attack a single host)

Status B: 1:N attack type (a single host attacks many hosts)

Status C: 1:1 attack type (a single host attacks a single host)

Status D: N:N attack type (many hosts attack many hosts).

The advantages of the use of these four statuses are as follows;

- the ability to evaluate the security threat from a large amount of data obtained from multisensor
- the ability to detect a security threat based on data from multisensor in a managed network
- the ability to identify a security threat in a managed network
- a reduction in the number of false alarms and the creation of valuable data.

4 IMPLEMENTATION

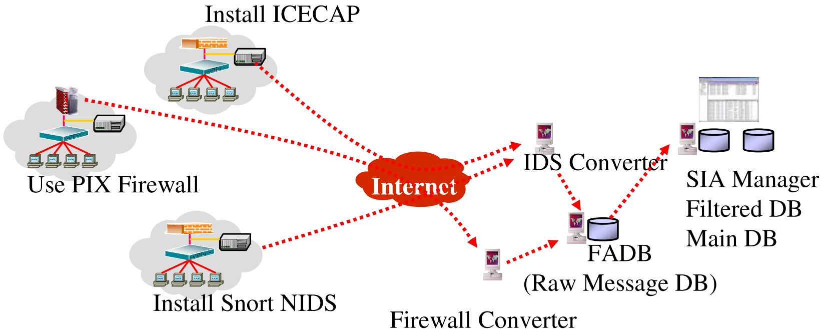

Fig. 2. Network roadmap

The SIA System architecture consists of a manager and a converter. Among the multiple sensors, we implemented the interface with IDS, focusing on the ISS ICECAP (BlackIce Manager) 2.6 and 3.0, SNORT 1.7 and 1.8, and that with the Firewall focused on the PIX. We installed two servers which have Pentium III 800 MHz processors and 256 MB of RAM as the converter servers, and a second server with Zeon dual processors and 512 MB RAM as the manager server. For the implementation of the DB server, we used MS SQL 2000, the C programming language, Visual C++ 6 and Visual Basic 6. In the Firewall converter design, we limited our support to the Syslog in the current implementation. The Firewall converter can change the Syslog raw message saved in the DB into standard format. The IDS converter has a separate DB for the data from each vendor's product. It reads the raw messages saved in the DB, and then saves this data in standard format in a high level DB. Figure 2 shows network roadmap in the SIA system.

4.1 Experimental Results

We collected the test data of the SIA system in an ISP (Internet Service Provider) infra-network. In our experiment, we researched the relationship between the interval time and threshold value. We were mainly interested in comparing our SIA system with IDS systems. Before explaining our experimental results, two terminologies need to be defined, as follows.

Interval time: the time from the first raw alert occurrence to the last raw alert occurrence. It is used for evaluating the attack status.

Threshold value: This provides the basis for the 'N' value, as referred to in the 1:N, N:1 and N:N statuses.

The interval time can be set to a different value, depending on the network environment. However, in our test cases, we set it to 3 minutes, because it takes at least

3 minutes to integrate and generalize alert messages concerning the Nimda, Codered and Welchia viruses more effectively than that which is possible with existing IDS systems. If the interval time is set to less than 3 minutes, then the SIA system's experimental results are not different from those of general IDS systems. Likewise, changing of the threshold value may give rise to different results. If the threshold value is set to 1 or 2, the experimental results are not different from those of existing IDS systems. In other words, if the threshold value is less than 2, it is possible to distinguish 1:1, 1:N, N:1 and N:N attack statuses. In our test results, we confirmed that minimum setting of 3 was required for the threshold value, in order to be able to classify the attack status correctly. The relationships between interval time and threshold value for attack statues are shown in Figures 3, 4, 5 and 6.

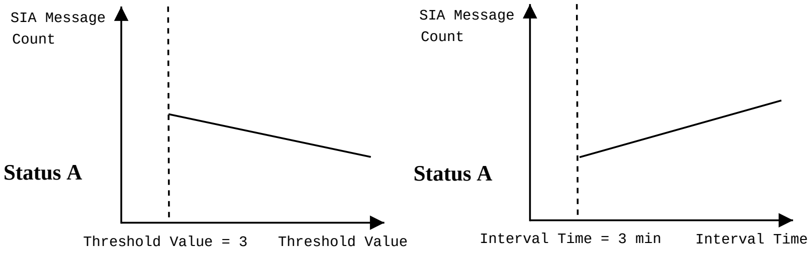

Fig. 3. Status A – evaluation chart

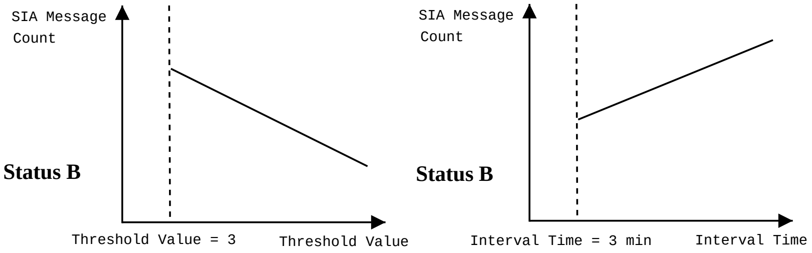

Fig. 4. Status B – evaluation chart

Figure 3 shows the frequency of occurrence of status A according to the threshold value and interval time. We can determine the variation in the status A occurrence rate, when an attack with N:1 status happens. The greater the increase in the threshold value, the smaller the reduction in the frequency of occurrence of status A. In other words, in the case of an attack with N:1 status, as the threshold value rises, the possibility of detecting DDoS type attacks grows smaller. In addition, we find that the frequency of occurrence of status A gradually increases as the interval time increases.

Figure 4 shows the frequency of occurrence of status B as a function of the threshold value and interval time. It shows the rate of occurrence of alert messages,

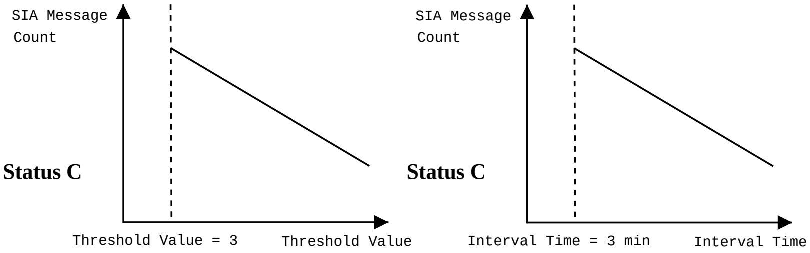

Fig. 5. Status C – evaluation chart

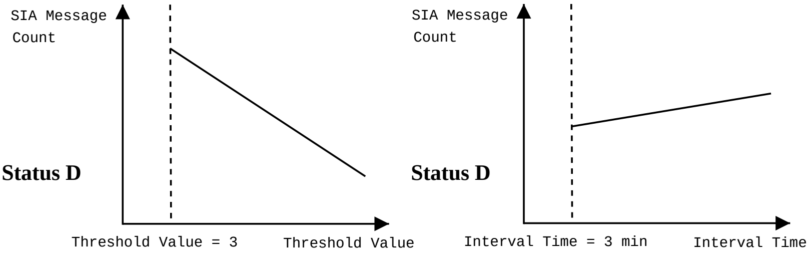

Fig. 6. Status D – evaluation chart

when an 1:N attack happens. Status B is detected, because either a single or several intruders scan and attack many target hosts. We find that as the threshold value increases, the frequency of occurrence of 1:N status is diminished. Also, if the interval time increases, the frequency of occurrence of status B also increases. This means that the number of attacks by a single attacker increases. In the experimental results, we confirm that mainly worm attacks, such as those by Nimda and Codered, are identified as Status B attacks.

Figure 5 shows the frequency of occurrence of status C as a function of the threshold value and interval time. It shows the rate of occurrence of alert messages, when a 1:1 attack happens. In Figure 5, we can observe that as the threshold value increases, the frequency of occurrence of status C is not changed. However, as the interval time increases, the frequency of occurrence of status C decreases linearly. In other words, if the interval time is increased, then the number of 1:1 type attacks detected grows smaller. Therefore, as the monitoring time increases, the number of 1:N, N:1 and N:N type attacks increases.

Figure 6 shows the frequency of occurrence of status D as a function of the threshold value and interval time. It shows the rate of occurrence of alert messages, when an N:N type attack happens. In Figure 6 we can observe that the number of status D attacks decreases continuously as the threshold value increases. This means that the basis 'N' expansion of status D leads to a decrease in the frequency of occurrence of N:N attack status. After having set the threshold value to the minimum value of '3', we attempt to increase the interval time value, and we find that the frequency of occurrence of status D grows incrementally. The threshold count and interval time have an effect on the incidence of the different statuses.

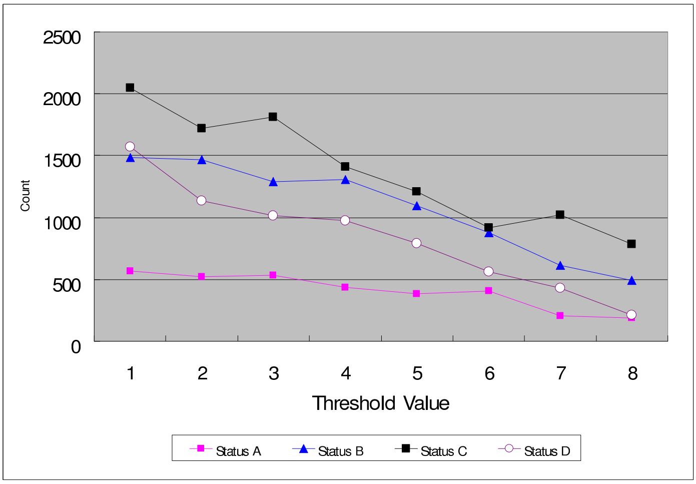

Fig. 7. Status frequency rate according to threshold value

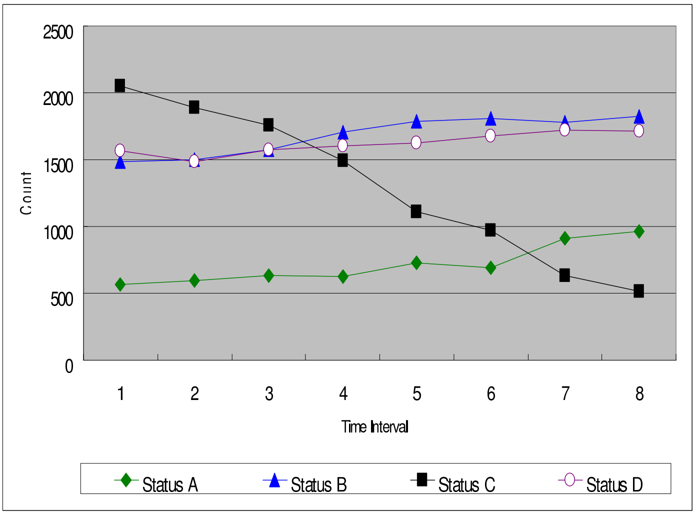

Fig. 8. Status frequency rate according to interval time

Figure 7 shows the frequency of occurrence of all 4 statuses as a function of the threshold value, while Figure 8 shows the frequency of occurrence of all 4 statuses as a function of the interval time.

The threshold count and interval time have an effect on the incidence of the different statuses. In addition, these parameters can be adjusted according to the tool's setup environment The change of status count by the reason of status occurrence can be altered according to methods of attack pattern and worm attack. The threshold count and interval time have an effect on the incidence of the different statuses. In addition, these parameters are adjusted according to the tool's setup environment. The status count can be adjusted by varying the threshold value and interval time, in order to focus searching for a particular attack pattern.

The condition of the key factors:

- threshold value = from 3 to 12
- time interval = from 3 to 8 minute

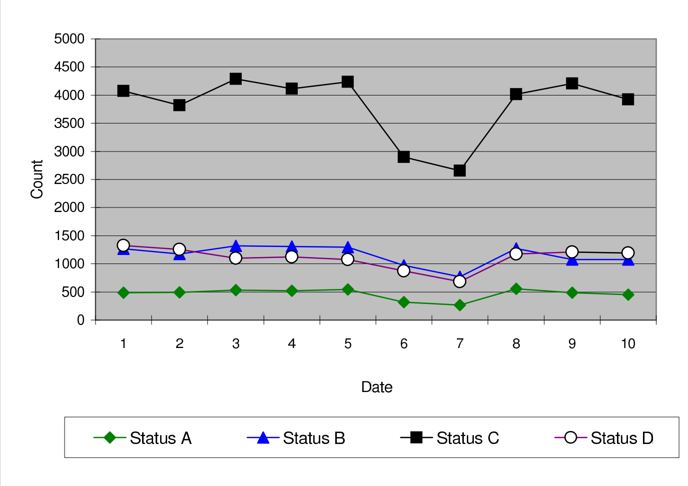

Fig. 9. Status alert count for 10 days

Figure 9 shows the alert counts of the four statuses in the SIA system. In Figure 9, the x axis represents the experimental date (10 days) and the y axis shows alert counts that occurred in the SIA system. The status C means that a 1:1 attack type mainly occurs in our experimental network.

Figure 10 shows the comparison data of the alert counts between the new SIA system and the existing IDS system. In Figure 10, the x axis refers to the experimental date (10 days) and the y axis shows alert counts detected in the SIA and IDS systems. The figure shows that the alert counts are greatly decreased in the SIA system compared with the IDS system. This result shows that the SIA system can reduce the large amount of redundant alert messages generally occurred by mixed attacks, e.g. the Nimda, IRCBot, Phatbot, Niche and Agobot worms, by classifying them into one of four attack statuses. For example, the Agobot worm includes the mixed attack patterns of an exploit attack, SYN flood, UDP flood and ICP flood. Each sensor in IDS system recognizes the individual alert messages even if they are generated by the same worm.

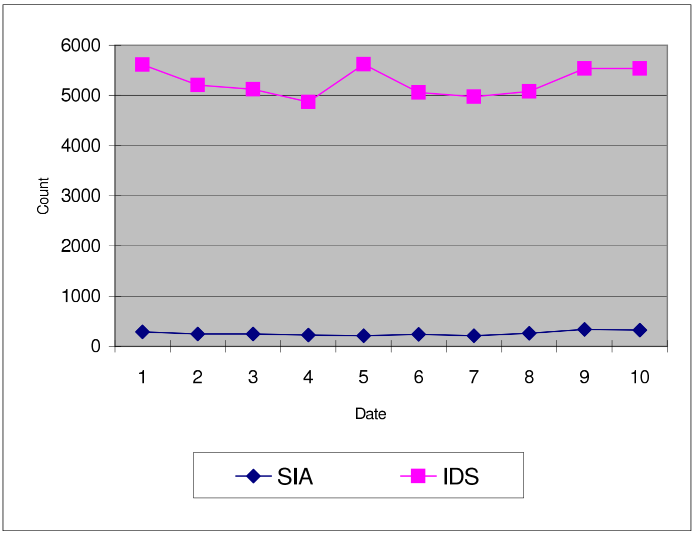

Fig. 10. SIA alert and IDS alert

5 CONCLUSION

The current ESM system is vulnerable to fusion attacks and it is difficult to evaluate the overall security threat to a managed network. Existing IDS systems generate alert messages only for the 1:1 attack status. Also, with these systems, identifying threat factors is very time consuming, even for security experts.

In this paper, we proposed a method of translating the various types of log format into a standard format. Our proposed system then finds and assesses the factors associated with a security threat in a managed network, using parameters associated with the number of intruders and specific target hosts. In addition, we eliminate the large amount of redundant alert messages, in order to reduce the dependency on the human resources required to analyze them. Furthermore, we implement a new Meta-IDS system, by taking into consideration the threat to the entire managed network, rather than individual threat alerts. After testing the SIA system, we confirmed that our system implementation could correctly analyze and evaluate various types of intrusion, and that it was able to distinguish security threats and attack statuses in managed networks.

To improve the performance of the SIA system, further research will be the establishment of a more detailed subdivision of the threat factors associated with a managed network.

REFERENCES

[1] Bass, T.: Intrusion Detection Systems And Multisensor Data Fusion. Communications of the ACM, Vol. 43, 2001, No. 4, pp. 99–105.

[2] Botha, M.—Solms, R. V.—Perry, K.—Loubser, E.—Yamoyany, G.: The Utilization of Artificial Intelligence in a Hybrid Intrusion Detection System. Proceedings of SAICSIT 2002, 2002, pp. 149–155.

[3] Curry, D.: Intrusion Detection Message Exchange Format Extensible Markup Language (XML) Document Type Definition. Available on: `http://www.ietf.org/ids.by.wg/idwg.html`, 2003.

[4] Frincke, D.: Balancing Cooperation and Risk in Intrusion Detection. ACM Transactions on Information and System Security, Vol. 3, 2000, No. 1, pp. 1–29.

[5] IDMEF XML Library (libidmef) Version 0.6.1 API 2002, Silicon Defense. Available on: `http://www.silicondefense.com/idwg/libidmef/API`, 2002.

[6] Lee, W.—Stolfo, S. J.: A Framework for Constructing Features and Models for Intrusion Detection Systems. ACM Transactions on Information and System Security. Vol. 3, 2000, No. 4, pp. 227–261.

[7] Loshin, P.: Information Security Magazine article for Meta-IDS. Available on: `http://www.infosecuritymag.com/articles/june01/columns_standards_watch.shtml`, 2001.

[8] Mell, P.—Marks, D.—McLarnon, M.: A Denial-of-Service Resistant Intrusion Detection Architecture. Computer Networks, Vol. 34, 2000, No. 4, pp. 641–658.

[9] Myerson, J. M.: Identifying Enterprise Network Vulnerabilities. International Journal of Network Management, Vol. 12, 2002, pp. 135–144.

[10] Ning, P.: Abstraction-Based Intrusion Detection in Distributed Environments. ACM Transactions on Information and System Security, Vol. 4, 2001, No. 4, pp. 407–452.

[11] Ning, P.—Cui, Y.—Reeves, D. S.: Construction Attack Scenarios Through Correlation of Intrusion Alerts. ACM1-58113-612-9, 2002, pp. 245–254.

[12] Phillips, C.—Swiler, L. P.: A Graph-Based System for Network-Vulnerability Analysis. Proceedings of the 1998 Workshop on New Security Paradigms, 1998, pp. 71–79.

[13] Richards, K.: Network Based Intrusion Detection: A Review of Technologies. Computer & Security, 1999, Vol. 18, pp. 671–682.

Keun-Hee Han is a Ph. D. candidate in Korea University. He received B. Sc. degree in computer science engineering from Seoul National University of Technology. He received M. Sc. degree in computer science engineering from Hanyang University. He found a Han Secure company and was a CEO. He was a vice-president in Ahn Laboratory, Inc. which is a famous for computer virus vaccine. His research interests include ESM, internet security, mobile security, new generation network.

Sang-Hun Jeon received B. Sc. degree in industrial engineering from Ulsan University. He worked for Infosec company, participated in the development of ESM, and joined the project of simulated hacking and its vulnerability analysis as a security consultant. Also, he worked with SK, Thrunet, financial companies. His research interests include IDS, Firewall, vulnerability analysis, and ISAC.

Il-Gon Kim is a research professor in the Department of Computer Science and Engineering of Korea University. He received M. Sc. and Ph. D. degrees from Korea University. His research interests include formal methods, process algebra, CSP, Casper, FDR, security protocol, and security model.

Kang-Won Lee is currently working as a network software engineer at DACOM. He received B. Sc. and M. Sc. degrees in computer science from Korea University. His research interests include network management systems, mobile security, and communications.

Jin-Young Choi is a professor in the Department of Computer Science and Engineering of Korea University. He received B. Sc. degree in computer engineering from Seoul National University in 1982, M. Sc. degree in computer science from Drexel University in 1986 and Ph. D. degree in computer science from University of Pennsylvania in 1993. His research interests include real-time computing, formal methods (formal specification, formal verification, model checking), process algebras, security and software engineering.