

## Threat Evaluation Method for Distributed Network Environment

KEUN-HEE HAN, IL-GON KIM, KANG-WON LEE, JIN-YOUNG CHOI<sup>†</sup>  
AND SANG-HUN JEON\*

*Department of Computer Science and Engineering  
Korea University  
Seoul, 136-701 Korea*

*\*NHN Corporation, IT Security Team  
Kyunggi-do, 463-844 Korea*

The approach proposed in this paper involves the creation of a new algorithm for analyzing correlation alerts and providing the correct information regarding the detection of various types of security attacks, such as DDoS. It also enables the evaluation of the attack status, the degree of danger from the viewpoint of a managed network environment and the assets protected by the security devices. This paper proposes an advanced ESM system (referred to as the "SIA System"), which is capable of grouping a large amount of alert messages, analyzing mixed attacks using correlation alert messages from each sensor and responding to security threats quickly, after classifying them into one of four different statuses. It was confirmed that this system implementation could identify and analyze all types of intrusion by attackers in a managed network. Therefore, it provides a very effective means for security experts to cope with security threats in real time.

**Keywords:** ESM (enterprise security management), Meta-IDS, SIM (security information management), SIA (security information alert), status evaluation logic

### 1. INTRODUCTION

With the ever increasing use of the Internet by all types of companies, security threats such as attacks on enterprise infrastructure by hackers, the leakage of personal data and the infection of confidential business information caused by e-mail based viruses, have become major issues in the security literature over the last few decades. Security systems such as IDS (Intrusion Detection Systems) 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 as well as the increasing use of variant methods, attacks are becoming more common using diverse and mixed techniques, rather than being limited to a single attack technique, or making use of multiple exploits [4]. For example, the Nimda virus, which first appeared in 2001, is a mass-mailing worm that uses many methods to propagate itself. This worm sends itself out by email, searches for open network shares, attempts to copy itself to unpatched or already vulnerable Microsoft IIS web servers, and is a virus that infects both local files and files on remote network shares. Unfortunately, there are currently no information protection systems that can recognize these mixed attacks, such as those involving the

---

Received May 4, 2004; revised November 15, 2004 & April 26, 2005; accepted November 2, 2005.

Communicated by Shih-Pyng Shieh.

<sup>†</sup> Corresponding author.

Nimda and Agobot worm, and sound an alert. Current information protection systems only detect and warn against individual intrusions, and are unable to provide a collective and synthesized alert message. Therefore, it is difficult to detect and react effectively against variant exploits. It not only requires a great deal of time to analyze and determine the practical vulnerabilities from the huge amounts of collected data in order to detect the potential intrusions and protect the system, but it also requires a great deal of manpower, who are skilled in such security issues.

Various methods have been used to solve these problems. References [2] and [8] proposed the translation of security information from an IDS log to a Hybrid format. Reports [8] and [7] were concerned with reducing the number of false alerts by correlating the intrusion alerts and limiting the scope of the redundant alert data. Studies [7] and [1] proposed a methodology for identifying complex attacks using the data warehousing and data mining methods.

This paper we proposes a method for correlating the alerts provided by the IDS systems and Firewalls, and demonstrates the value of this method to the detection of DDoS (Distributed Denial of Service) attacks. This approach facilitates the creation of information necessary to evaluate the degree of danger, together with the attack status of the managed network environment. We implement a new algorithm and a security model, which can be used to tackle security problems quickly through the support of background data. Furthermore, we divide the intrusion model into several different statuses, and define a standard format which can be used to regroup the different log data originating from different vendors' products, in order that security experts can recognize the correct intrusion target and its intention and cope with the situation effectively. In this way, we can classify the various types of attack status into 1:1, 1: $N$ ,  $N$ :1 and  $N$ : $N$ .

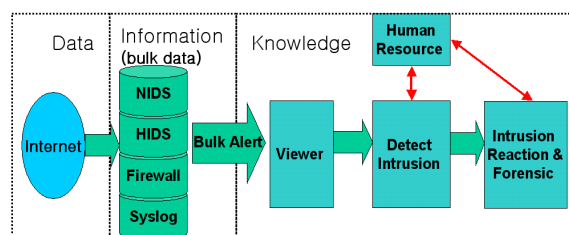


Fig. 1. Current intrusion detection paradigm.

Fig. 1 shows the various steps involved in the detection of intrusions, with the bulk data first being gathered from various sensors and the intrusions subsequently being identified, with the assistance of human intervention. Fig. 2 presents the algorithm proposed in this paper, which groups and classifies the bulk data collected by multiple sensors (i.e Firewall, IDS, IPS, Packet Sniffer, Syslog, etc) in order to limit the dependency on human resources, and enable a more accurate evaluation of the situation.

In particular, the new approach enables various types of attacks to be identified, including those involving either a single host or multiple hosts. This is accomplished by scanning for vulnerabilities using the detection data of the available security systems, including the Firewall and IDS, whose log files are first verified and regrouped to provide SIA (Security Information Alert) logic processing.

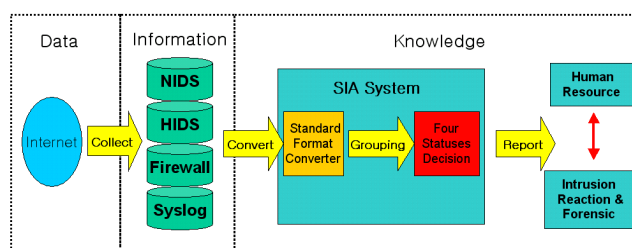


Fig. 2. New intrusion detection paradigm using SIA logic.

The remainder of this paper is organized as follows. Section 2 explains the background of the SIA model, and includes a discussion of the related works, and the current security system status levels. Section 3 explains the Simple Evaluation Logic method proposed in this paper, its evaluation criterions, reasonableness, and the definition of the standard format required for regrouping the information from the different vendors' log formats. Section 4 shows the implementation of the proposed model, along with the experimental results using our implementation tool in a real world environment. Finally, section 5 provides a conclusion this paper and discusses future work.

## 2. RELATED WORKS FOR ESM

There are several approaches that have been made to extract useful information from alerts or events gathered from multiple sensors. These methods originate from the requirement to integrate and analyze the data from the various established security solutions, and have evolved in an attempt to interface with systems that offer a higher degree of security, as the information systems themselves have grown. However, the format in which these alerts and events are stored varies from one vendor's product to another. This inconsistency in the event format poses a problem when it comes to analyzing log data synthetically and might confuse the information security expert. In order to solve this problem, several different approaches have been used in an attempt to obtain a uniform result from the sensors' alerts and events.

ESM [6] (Meta-IDS or SIM) is a management system that can track alert data flowing from a Host-IDS to a Network-IDS. ESM systems can display the alert data obtained from both a Host-IDS and a Network-IDS on one console. The purpose of an ESM is to construct a system from raw data, security alerts and other data, originating from all types of different security systems, and to put this information into a standard format so that it can be more easily managed. However, ESM systems evaluate the threat to an enterprise's network by analyzing the bulk traffic, which involves gigabytes rather than megabytes of information. For example, MIV (Motorola Intrusion Vision) is configured to monitor all supported IDS sensor transmissions, bringing them all together into one place and allowing the consolidated reporting of intrusion alerts. However, it sets a limit on the amount of IDS alert data that can be analyzed.

To solve this problem, for which there are no uniform guidelines, the Intrusion Detection Exchange Format working group (IDWG) of the IETF 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 on 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, in addition to their reluctance to abandon their own event representation, the current ESM (Meta-IDS or SIM) system provides just a simple event format translation. Because an IDMEF, IDXP and IAP are still in the process of standardization and have a complex representation regarding their event format, they are inappropriate for expressing security threats from sources such as the Slammer, CodeRed and Nimda worms. In addition, they are not pertinent when it comes to evaluating the practical threat factors in a managed network. The integration of the alert messages contained in these different security products must be carried out in advance in order to sort and evaluate the practical threat factors.

Therefore, for the unification of the different event formats, the event data of Firewalls and IDS systems first needs to be standardized. The standardization process suggests that the event format of an IDMEF be simplified, in order for it to correspond to a fast network bandwidth and a fusion cyber attack. We constructed a standard format after examining each alert format and defined a standard table. Our implementation of the SIA system proposes a simple standard format for both IDS and Firewall systems, which can unify multi sensors information. Moreover, it can classify the security threats in a managed network and cope with them rapidly, by sorting the data based on the core fields in the alert format. The SIA System can show information on the intrusion using a standard format for the alert and event data, and translate the information stored in the IDS and Firewall knowledge databases, based on an evaluation of the internal system.

In this way, the security expert can analyze and understand the threat factors synthetically, using a knowledge database that contains each threat factor for both the system and the network environment. After recognizing the threat status, the SIA system can evaluate all aspects of the intrusion, analyzing the information level and the data level of the IDS and Firewall in detail.

### 3. STATE OF THE SIA SYSTEM

In the ESM systems, there are two approaches to unifying 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 regroup a large amount of alert messages 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. In summary, the advantages of the SIA System are as follows:

- Integrated monitoring of multiple sensor alerts.
- Real time recognition of security threats in a managed network.
- Classification of unified alert messages according to four status decision logic and optimization of the human resources required to evaluate the security threats.
- Easy understanding and detection of the related information from sensors such as IDS and Firewalls. Evaluation of the influence of security threats on a managed network, in forensic.

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.

### 3.1 Definition of Light-Weight Intrusion Alert Message Format for IDS and Firewall

The SIA System converts Multisensor alarm data into a standard format in order to unify it based on the essential information such as Protocol, IP Address and Port Number. During the process of converting the data into the standard format, redundant information is excluded in an attempt to improve the probability of detecting security threats. Firewall standard format data is configured based on the raw format that is extracted from PIX, Netscreen and FW-1. The data can also be obtained in one of these standard formats from other Firewall products and can be represented in the process of alerts and events (see Table 1). For the definition of the standard format, we analyzed the various products on the market, focusing on the best-known security products such as ICECAP manager and SNORT of ISS, and examining their event formats. Table 2 shows the standard format proposed in this paper. We configured the SIA System in order to extract the information referred to in this standard format from the alerts and events of each IDS and Firewall product. In other words, for each information security system to support this standard format, all that is needed is to make a converter that is capable of translating the raw alert messages into a standard format before applying them to the SIA System. The standard format was configured as shown in Tables 1 and 2.

**Table 1. Firewall standard format.**

Receive Time	yyyymmdd-HHMMSS : message receive time
Action	Firewall Action string
Protocol	TCP/UDP
Interface	Sensor Interface
Sensor Address	Sensor IP address
Source Address	Source IP Address
Destination Address	Destination IP Address
Source Port	Source Port
Destination Port	Destination Port
Detail	Firewall raw message

**Table 2. IDS Standard format.**

Receive Time	yyyymmdd-HHMMSS : message receive time
Sensor Address	Sensor address
Source IP Address	Source IP address
Destination IP Address	Destination IP address
Signature	Detected signature
Priority	Signature priority
Detail	IDS raw message

### 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 a large amount of alerts 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 cannot easily detect these types of attacks. In other words, when complicated and varying attack techniques are used, the intruder detection systems do not concentrate their efforts in order to identify the particular attack.

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. Fig. 3 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 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 vulnerabilities, the 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

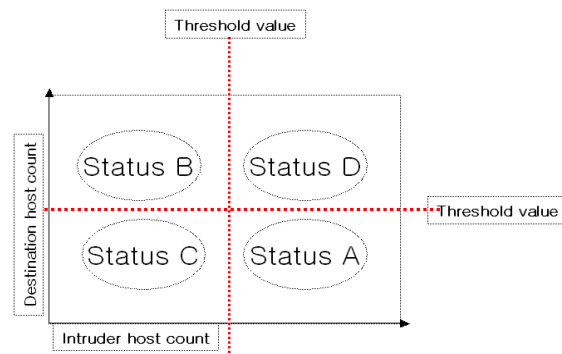


Fig. 3. New analysis.

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):  
DDoS attack or a Multiple connection problem
- Status B:  $1:N$  attack type (a single host attacks many hosts):  
Backdoor attack, targeting some ports such as Net Bus, Back Orifice 2k, or scanning some range of the IP addresses
- Status C:  $1:1$  attack type (a single host attacks a single host):  
Single host scanning, collecting related vulnerability information, and brute force attack such as the Niche, Bagle, Mydoom, phatbot and ircbot worm
- Status D:  $N:N$  attack type (many hosts attack many hosts):  
Full scanning or worm attack on an information system such as the Blaster, Slammer, CodeRed and Nimda

The advantages of using 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.

The classification of each attack status can be simplified as follows:

Intruder IP  $\rightarrow I(i)$ , Destination IP  $\rightarrow D(i)$   
 $M \rightarrow$  small count limit  $\sim$  large count,  $S \rightarrow 1 \sim$  small count  
 A)  $I(i) = M \ \& \ D(i) = S$  : DoS attack warning

- B)  $I(i) = S \ \& \ D(i) = M$  : Information area vulnerability scan warning  
 C)  $I(i) = S \ \& \ D(i) = S$  : Specific target attack or scan warning  
 D)  $I(i) = M \ \& \ D(i) = M$  : Information area scan warning or worm attack

## 4. ARCHITECTURE AND IMPLEMENTATION

### 4.1 Architecture

The implementation of the SIA System treats the Firewall related-messages, IDS alerts, SIA logic and the data separately. The overall architecture of the SIA system consists of two components, a low level and a high level process. The role of the former is to obtain the standard format IDS and Firewall alert data, and to save it in a database, while that of the latter is to process the data saved in the database and display it. The low level process is further divided into two sub processes used for dialoging with the Firewall and the IDS, respectively, as shown in Fig. 4.

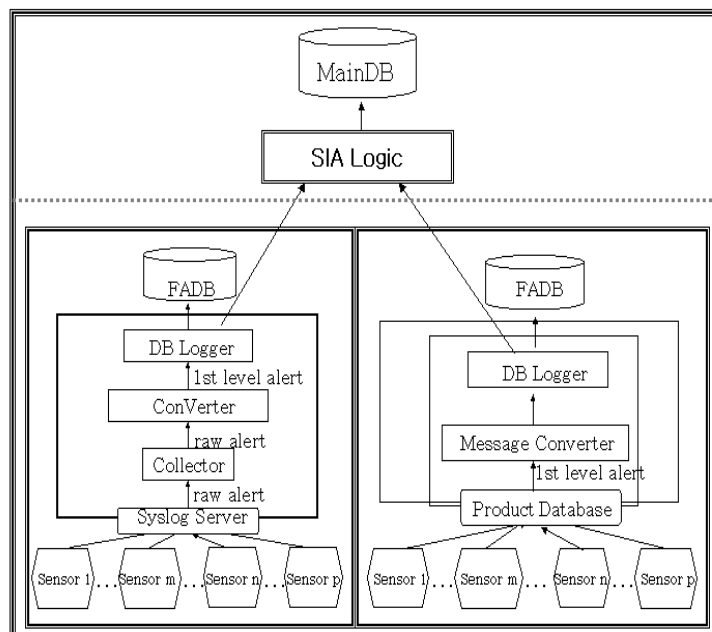


Fig. 4. SIA system diagram.

### 4.2 Implementation

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 800Mhz processors and 256

MB of RAM as the Converter servers, and a second server with Zeon dual processors and 512MB RAM as the Manager server. For the implementation of the DB server, we used an MS SQL 2000, the C programming language, Visual C++ 6 and Visual Basic 6. Its internal architecture was configured to receive the input data from multiple sensors and process it, as shown in Fig. 5. In the Firewall converter design, our support was limited to the Syslog in the current implementation. The Firewall converter can change the Syslog raw messages saved in the DB into a 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.

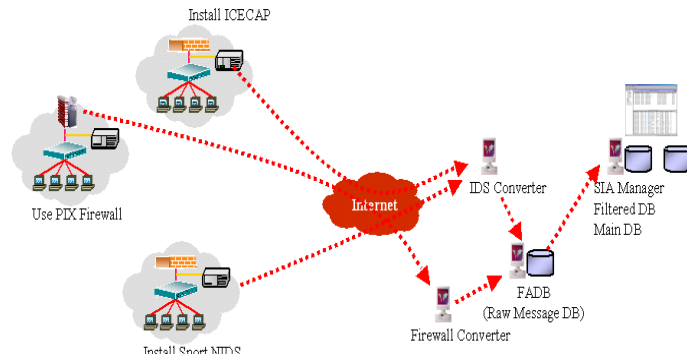


Fig. 5. Network roadmap.

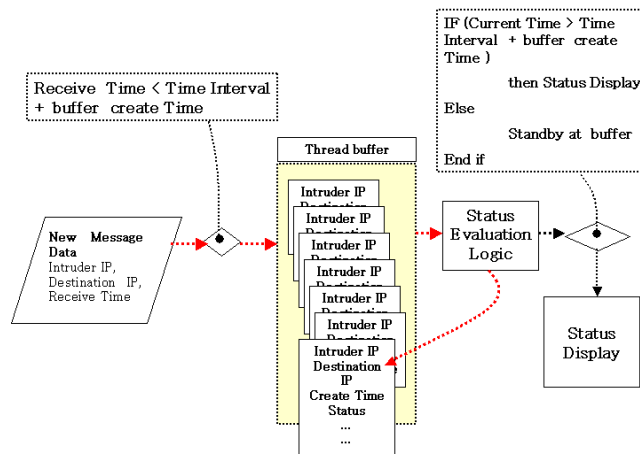


Fig. 6. SIA processing.

### 4.3 Design

The Status Evaluation Logic designed to assess the status of the threat was configured to save several factors that are useful for evaluating the security threat, using thread buffers, after which it decided the security threat status (see Fig. 6). There are several

possible methods that can be used to implement the buffer according to the Status Evaluation Logic and the Interval Time Value. In this study, we implemented the SIA System using a buffer based on threads. Fig. 6 shows the SIA processing procedure and Fig. 7 represents the Status Evaluation Logic proposed in the SIA System.

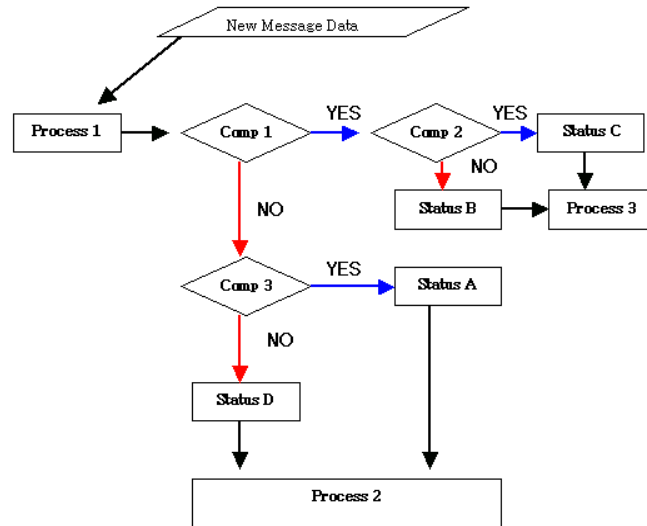


Fig. 7. Status evaluation logic diagram.

#### Comparison Routine

##### Comp1:

```

IF Intruder IP = Buffer saved Intruder IP
  then
    Goto Comp 2
  Else
    Goto Comp 3
  END IF

```

##### Comp2:

```

IF Destination IP = Buffer saved Intruder IP
  then
    IF Destination IP = Buffer saved
      Destination IP
    then
      Goto Status C
    Else
      Goto Status B
    END IF
  END IF

```

##### Comp3:

```

IF Intruder IP = Buffer saved Intruder IP

```

```

then
  IF Destination IP = Buffer saved
    Destination IP
  then
    Goto Status D
  Else
    Goto Status A
  END IF
END IF

```

The pseudo code above shows the procedure used to evaluate one of the four statuses in the SIA system. For example, if the intruder IP is the same as the buffer saved IP in Comp1 step, then Comp2 step proceeds. Next, if the destination IP is the same as buffer saved IP in Comp2, then the SIA system evaluates the attack as Status C.

The role of process 1 is to receive new message data and pass it to Comp1, as shown in Fig. 8.

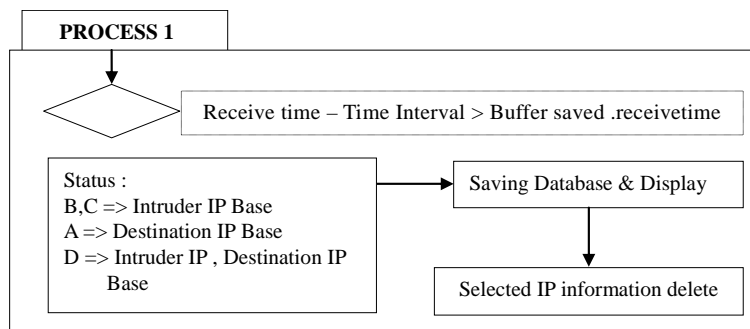


Fig. 8. Process 1 job.

The role of Process 2 is to update buffer value.

- Update Buffer Value :  
Receive Time, Intruder IP, Destination IP (IP can be replaced by host ID)

Process 3 takes control of the following tasks. If the intruder is already present, which means that it is the same as the one stored in the DB and the destination is stored in the DB, then the Status value is changed from D or A to C, otherwise if the destination is not present, which means that it does not coincide with the one in the DB, then the Status Value is changed from D or A to B. The buffer is updated as a function of the new Status Value.

```

IF Intruder IP = Buffer saved Intruder IP and
  IF Destination IP = Buffer saved
    Destination IP
  then Status value change → Status C

```

```

Else
Status value change → Status B
END IF
END IF

```

The logic/pseudo code based on the evaluation condition can be summarized as follows.

```

IF Receive Time > Buffer → ReceiveTime + Time Interval
  If status B, C then
    Buffer.IntruderIP = IntruderIP
  Else If A then
    Buffer.DestinationIP = DestinationIP
  Else
    Buffer .DestinationIP = DestinationIP & Buffer.IntruderIP = Intruder IP
  END IF
Else
  Buffer Clear
END IF

```

#### 4.4 SIA Alert System

The test data of the SIA system collected in an ISP infra-network, over a period of one month. In this experiment, we researched the relationship between the Interval Time and Threshold value. This experiment focused mainly on comparing the new SIA system with existing IDS systems. Before explaining the experimental results, the following two terminologies need to be defined:

- Interval Time: the time from the first raw alert occurrence to the last raw alert occurrence. It is used to evaluate 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 the test cases, it was set to 3 minutes, because it takes at least 3 minutes to integrate and generalize alert messages concerning the Nidma, CodeRed and Welchia viruses. 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 impossible to distinguish the  $1:1$ ,  $1:N$ ,  $N:1$  and  $N:N$  attack statuses. In our test results, in order to be able to classify the attack status correctly, it was confirmed that a minimum setting of 3 was required for the ‘Threshold Value.’ The relationships between the ‘Interval Time’ and ‘Threshold Value’ for the attack statuses are shown in Figs. 9, 10, 11, and 12.

Fig. 9 shows the frequency of the occurrence of status A according to the ‘Threshold Value’ and ‘Interval Time.’ We can determine the variation in the occurrence rate of Status A, when an attack with a  $N:1$  status takes place. The greater the increase in the threshold value, the smaller the reduction in the frequency of the occurrence of Status A. In other words, in the case of an attack with the  $N:1$  status, as the threshold value rises, the possibility of detecting a DDoS type attacks grows smaller. In addition, the frequency of the occurrence of Status A gradually increases as the ‘Interval Time’ increases.

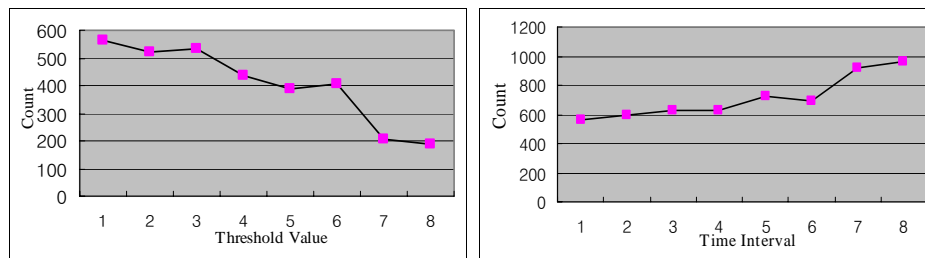


Fig. 9. Status A evaluation chart.

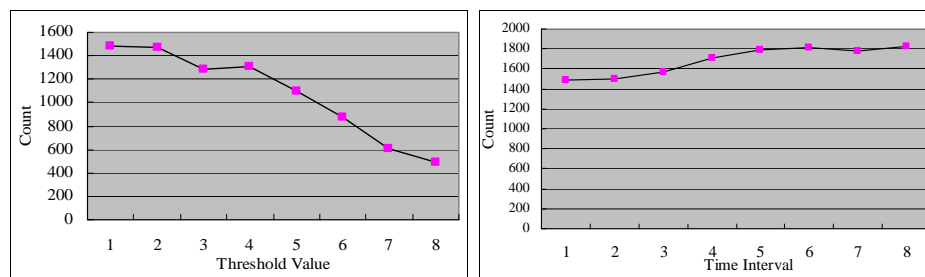


Fig. 10. Status B evaluation chart.

Fig. 10 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, when a  $1:N$  attack take place. Status B is detected, because either a single or several intruders scans and attacks many target hosts. It was found that as the ‘Threshold Value’ increased, the frequency of the occurrence of the  $1:N$  status decreased. 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 confirmed that mainly worm attacks, such as those by the Nimda and CodeRed, were identified as Status B attacks.

Fig. 11 shows the frequency of the 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 occurs. In Fig. 11 we shows that the frequency of occurrence of Status C is not changed as the ‘Threshold Value’ increases. However, as the ‘Interval Time’ increases, the frequency of occurrence of Status C decreases linearly. This means that the number of  $1:1$  type attacks detected grows smaller if the ‘Interval Time’ is increased.

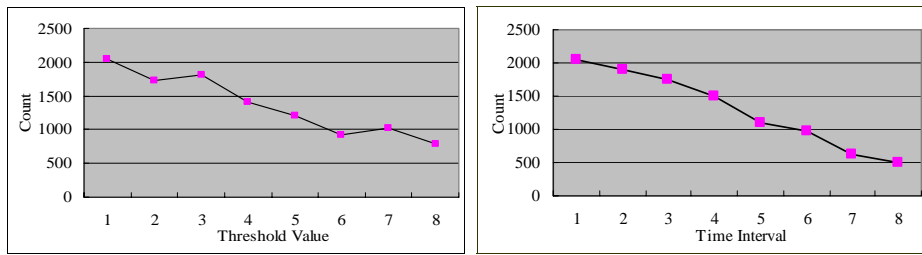


Fig. 11. Status C evaluation chart.

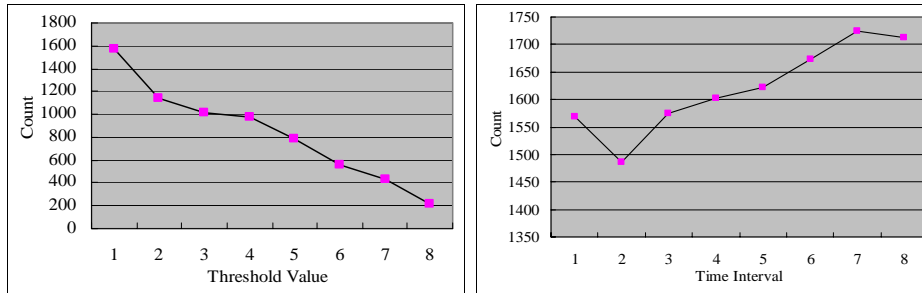


Fig. 12. Status D evaluation chart.

Therefore, as the monitoring time increases, the number of 1:N, N:1 and N:N type attacks increases.

Fig. 12 shows the frequency of the 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 take place. Fig. 12 shows 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 setting the ‘Threshold Value’ to the minimum of ‘3’, we attempted to increase the ‘Interval Time’ value, and found that the frequency of the occurrence of Status D grows incrementally.

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 in the status count by the reason of the status occurrence can be altered according to the methods of the attack pattern and worm attack. The status count can be adjusted by varying the ‘Threshold Value’ and ‘Time Interval’, in order to focus the search for a particular attack pattern.

The conditions of the key factors are as follows:

- Threshold Value = from 3 to 12.
- Time Interval = from 3 to 8 minute.

Fig. 13 shows the comparison data of the alert counts between the new SIA system and the existing IDS system. In Fig. 13, the x axis refers to the experimental date (24 days) and the y axis shows alert counts detected in the SIA and IDS systems. Alert counts

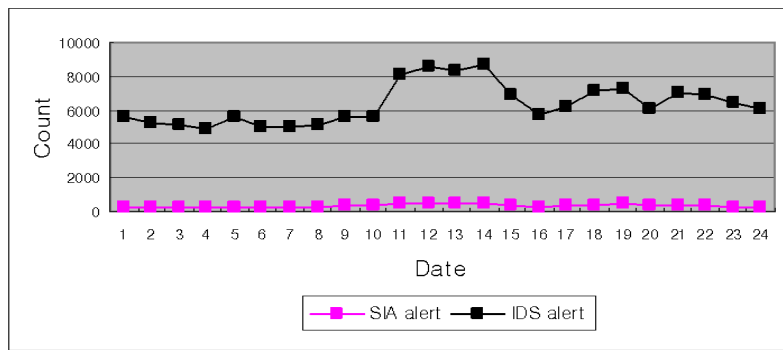


Fig. 13. SIA alert and IDS alert.

in the SIA mean total counts after being classified into four status attacks. On the other hands, alert counts in IDS represent total counts of individual attack signatures gathered from each Sensor.

The figure shows that the SIA system can unify the different log alerts originating from Multisensor and provides supported log alerts, together with IDS log alarms, which are regrouped into four status types (1:1, 1:N, N:1 and N:N). The result means that the log alert counts grouped by the SIA system are smaller when compared with IDS.

Table 3. The alert count comparison between SIA and IDS regarding the Agobot worm.

Systems Hosts	SIA				IDS
	Status A (N:1)	Status B (1:N)	Status C (1:1)	Status D (N:N)	
Host I	0	5	16	0	11,158
Host J	0	4	18	0	20,980
Host K	0	11	7	0	2,286
Other Hosts	41	110	129	97	394,072

[Time Interval = 3 min, Threshold Value = 3, Log Data = 1 hour]

Table 3 shows a comparison of the alert count between the SIA system and the existing IDS. The managed networks for experimental environments are a C class subnet (below 256 hosts). We installed SNORT and ISS Real Secure as Multisensor to construct general IDS. Then we configured the SIA system by locating SNORT and ISS Real Secure in front of SIA logic process, as shown in Fig. 2. Figs. 1 and 2 in the paper show the difference of intrusion detection paradigm between existing IDS and the SIA system.

First, we set the threshold value in SIA system as 3, to group specific hosts over 3 in each status count. Second, we ran the SIA system in order to evaluate the threat status in a C class subnet, and we found that total counts in Status A were 41 and there were no host over threshold value '3.' From this result, we could come to a conclusion that total counts (41 alarms) in Status A didn't represent a danger situation when we considered the number of hosts in a subnet C class. Third, we found that total counts in Status B was 110 and there were three hosts (I, J, K) over threshold value '3.' From this step, we

started to doubt that attack type was 1: $N$  and hosts  $I$ ,  $J$  and  $K$  were attacked hosts. Fourth, we examined the alert counts in Status C. Then we discovered that total counts in Status C were 129 and hosts  $I$ ,  $J$ ,  $K$  were over threshold value '3.' Therefore, we could guess from this result that mixed attacks were occurred in hosts  $I$ ,  $J$ ,  $K$ , and attack types were 1: $N$  and 1:1. Sixth, Security Experts analyzed log files (of IDS and SIA) to Status B and Status C, in order to know more correct intrusion detection information such as worm/virus type, attack source, and vulnerability. From above evaluation steps, finally we could reached a conclusion that the hosts  $I$ ,  $J$ ,  $K$  were attacked by the Agobot worm and they might infect other hosts by running as attacker hosts.

Initially, the SIA system evaluates the security threats by the Agobot worm to be in Status C (1:1). However, as the attack of the target hosts increases, the SIA system recognizes this attack as belonging to in Status B (1: $N$ ). Therefore, the SIA system analyzes mixed attacks such as the Agobot worm and is more capable for filtering redundant alert messages than the existing IDS systems, as shown in Table 3.

Fig. 14 shows the alert counts of the four statuses respectively in the SIA system. In Fig. 14, the  $x$  axis represents the experimental date (24 days) and the  $y$  axis is alert counts that occurred in the SIA system. The highest rate of Status C means that a 1:1 attack type mainly occurs in our experimental network. In addition, the strong increase in Status B during the 18-24 days points out the detection of a 1: $N$  attack type such as the Niche, Bagle, Mydoom, and Agobot. Table 3 shows the log data for only one hour. However, the total log data in 24 days was too large. Consequently, it required a great deal of time for the security expert to analyze the security threats. The size of log data in the SIA system is 20 times smaller than that the IDS system. Therefore, the SIA system responds more quickly to security threats than the existing IDS systems, because it reduces the redundant alert messages, as shown in Figs. 13 and 14.

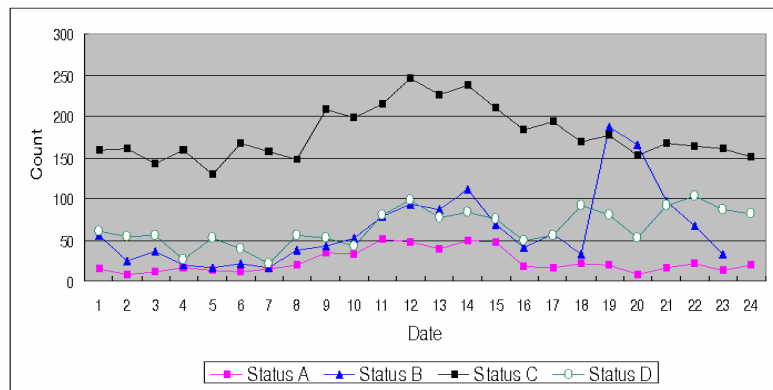


Fig. 14. Status alert count in SIA system.

## 5. CONCLUSION

The vast majority of security intrusions and threats take the form of a DDoS attack, accompanied by a randomized worm attack against a standalone server, rather than by a

single attack or a fusion attack, Due to the complex nature of such attacks, even a security expert might take a long time to assess and deal with security threats in a managed network. However, the current IDS system is vulnerable to fusion attacks and it is difficult to evaluate the overall security threat to a managed network. In addition, with this system, identifying threat factors is quite time consuming, even for Security Experts.

The SIA system can evaluate the factors associated with the security threats to important assets in managed network originating from attackers. This paper proposed a method for translating the various types of log format into a standard format. The proposed system identifies and assesses the factors associated with a security threat in a managed network, using the parameters associated with the number of intruders and the specific target hosts. In addition, the large amount of alert messages was grouped, in order to reduce the dependency on the human resources required to analyze them. We implemented a new ESM system, by considering the threat to the entire managed network, rather than individual threat alerts. After testing the SIA System, we confirmed that the new system implementation could correctly analyze and evaluate various types of intrusion, and could distinguish security threats and attack statuses in managed networks.

However, the SIA system has following disadvantage. If Multisensor recognize an attacker as normal hosts then the SIA system also can't detect an intrusion because false negative alarms will always exist on any good Multisensor. Likewise existing IDS, the SIA system can't evaluate which virus and worms are spread out in the managed networks, without analyzing the log file generated by Multisensor. In other words, the analysis of alert logs by Security Experts must be needed, in order to evaluate the security threat in more correct. In the experiment of Table 3, we set the threshold value as '3' in the SIA system. As changing threshold value, the result of threat evaluation would be different. Therefore the choice of optimized threshold value in the SIA system would be decided by the experience of a security expert.

## REFERENCES

1. T. Bass, "Intrusion detection systems and multisensor data fusion," *Communications of the ACM*, Vol. 43, 2001, pp. 99-105.
2. M. Botha, R. V. Solms, K. Perry, E. Loubser, and G. Yamoyany, "The utilization of artificial intelligence in a hybrid intrusion detection system," in *Proceedings of Annual Conference of the South African Institute of Computer Scientists and Information Technologists*, 2003, pp. 149-155.
3. D. Curry, *Intrusion Detection Message Exchange Format Extensible Markup Language (XML) Document Type Definition*, <http://www.ietf.org/ids.by.wg/idwg.html>, 2003.
4. D. Frincke, "Balancing cooperation and risk in intrusion detection," *ACM Transactions on Information and System Security*, Vol. 3, 2000, pp. 1-29.
5. IDMEF XML Library (libidmef) Version 0.6.1 API, SILICON DEFENSE, <http://www.silicondefense.com/idwg/libidmef/API>, 2002.
6. P. Loshin, "Information security magazine article for Meta-IDS," [http://www.infosecuritymag.com/articles/june01/columns\\_standards\\_watch.shtml](http://www.infosecuritymag.com/articles/june01/columns_standards_watch.shtml), 2001.
7. P. Ning, "Abstraction-based intrusion detection in distributed environments," *ACM*

*Transactions on Information and System Security*, Vol. 4, 2001, pp. 407-452.

8. P. Ning, Y. Cui, and D. S. Reeves, "Construction attack scenarios through correlation of intrusion alerts," in *Proceedings of 9th ACM Conference on Computer and Communications Security*, 2002, pp. 245-254.
9. NetForensics Article, <http://www.netforensics.com>, 2002.



**Keun-Hee Han (韓根熙)** acquired Ph.D. degree in Computer Science, Korea University. He received B.S. degree in Computer Science Engineering from Seoul National University of Technology. He received M.S. 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 lab. Inc which is a famous for computer virus vaccine. His research interests are ESM, internet security, mobile security, and new generation network.



**Il-Gon Kim (金日坤)** is a research professor in the Department of Computer Science and Engineering in Korea University. He received M.S. and Ph.D. degrees in the Department of Computer Science and Engineering from Korea University. His research interests are formal methods, process algebra, CSP, casper, FDR, security protocol, and security model.



**Kang-Won Lee (李康遠)** is currently working as a network software engineer at DACOM Corporation. He received B.S. and M.S. in Computer Science from Korea University. His research interests are network management systems, mobile security, and communications.



**Jin-Young Choi (催振榮)** is a Professor in the Department of Computer Science and Engineering in Korea University. He received B.S. degree in Computer Engineering, Seoul National University in 1982. He received M.S. degree in Computer Science, Drexel University in 1986 and acquired Ph.D. degree in Computer Science, University of Pennsylvania in 1993. His research interests are real-time computing, formal methods (formal specification, formal verification, model checking), process algebras, security and software engineering.



**Sang-Hun Jeon (全尙勳)** received B.S. degree in Industrial Engineering from Ulsan University. He worked for NHN Corporation Company, leading the IT Security Team. Currently from job previously the company is the security specialty company it was active with the security specialist. As the security specialist participated in the development of ESM, and led in the project of simulated hacking and its vulnerability analysis. Also he keeps the actual security reinforcement experience from the many Korean undergarment big businesses and the banking companies. His research interests are zeroday-worm, vulnerability analysis, web hacking, penetration test and SDLC (secure development life cycle).