December 2004

Design and Implementation of Risk Analysis system for ISP Network

Ho-Kun Moon
KT Technology Laboratory

Jin Choe
KT Technology Laboratory

Dae-Hyun Ryu
Hansei University

Design and Implementation of Risk Analysis system for ISP Network

Ho Kun Moon
KT Technology Laboratory
hkmoon@kt.co.kr

Jin Gi Choe
KT Technology Laboratory
jingiya@kt.co.kr

Dae Hyun Ryu
Hansei University
dhryu@hansei.ac.kr

Abstract

The need for more effective ways to analyze network risks in real time has been recognized by security planners. However, most existing risk analysis tools provide only methodological analysis procedures, and cannot reflect continually changing vulnerability and threat information concerning individual network systems in real time. For this reason, this study suggests a new system design methodology which shows a scheme to collect and analyze data from network intrusion detection systems and vulnerability analysis systems and estimates risk levels. Through field tests, it was proven that the proposed system can provide log analysis functions that help in reasoning out the behavior of an attacker. This paper includes a design concept, the main algorithm and test results.

Keywords: Risk, Quantitative Analysis, Asset value, N-IDS, Vulnerability

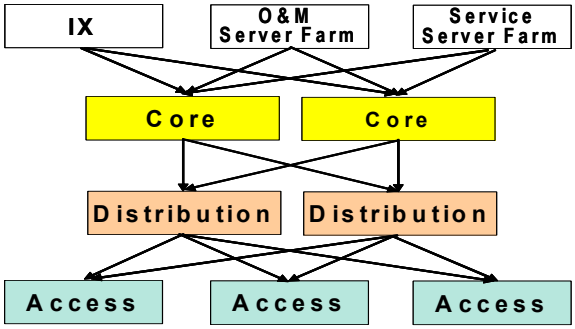
1. Introduction

Today, most Internet Service Providers (ISPs) have and operate various methods to effectively protect their assets, connected through networks, from all types of cyber attacks. At this stage, risk analysis methodology[1-8], which utilizes information about elements of vulnerability and threats to the network assets, is applied as a means to determine the protection method and level.

In order to solve such problems, this study proposes a design plan for a system, which will be able to conduct real-time based risk analysis by correlating the information supplied from network assets value assessment, Network Intrusion Detection Systems (N-IDS) and Venerability Analysis Systems (or VAS). This rest of this paper is organized as follows: In chapter II, methods of estimating the value of the asset are explained. In chapter III, the structure, functions and analysis algorithm of the proposed system are explained. In chapter IV, the results of experiments of a network are described. Finally, conclusion and future research directions are suggested

2. Asset Value Assessment Method

As a part of the network risk management process, risk analysis starts from identifying the value (or importance) of the asset subject to protection by the security policy, and the vulnerabilities and threats faced by the asset. The vulnerabilities and threats become direct causes that generate risk and the asset value has the same meaning as the level of loss induced by the risk. The existing risk analysis methodologies consider the risk as the comprehensive attributes of asset, vulnerability and threat level and determine the risk level by combining these factors.



* IX : Internet eXchange
* O & M : Operation and Maintenance

(Fig. 1) General ISP Network Model

However, categorizing assets, vulnerabilities and threat levels into only a few levels based on attributes, is problematic. The decision for risk level classification tends to mainly rely on subjective judgments. Also, when combining the asset value level, which is expressed in a form of quantitative estimation value, and vulnerability and threat level, which are expressed as step counts in descriptive form, the possible step counts increase and it becomes difficult to incorporate the characteristics of the ISP subjected to the risk analysis. Therefore, there is the problem of decreasing the objectivity of the results. Accordingly, the asset loss modeling technique, recommended by Ho Kun Moon [10] is adopted in this study in order to solve the above problem. Through this method, the asset value is expressed as a sum of service value generated through the asset and the physical fixed asset value.

For example, a specific asset on network a_k has a fixed asset value of $\boldsymbol{V_f(a_k, x)}$ in x year based on its purchasing point and if the generated service value in that year is $\boldsymbol{V_s(a_k, x)}$, the total asset value of a_k, $V_t(a_k, x)$ in x year can be shown in the following formula (1)..

$$V_t(a_k, x) = V_f(a_k, x) + V_s(a_k, x) \qquad (1)$$

If the fixed amortization method is applied according to the accounting rules in depreciation, the value of $V_f(a_k, x)$ decreases linearly each year and after five years, in typical ISP network equipment accounting standards, it converges to 0 or an arbitrary remaining value. After the purchase of the asset, the fixed asset value of a_k in x year can be expressed by the following formula (2).

$$V_f(a_k, x) = -\frac{(V_f(a_k, 0) - V_{fr})}{(x+n)} x + V_f(a_k, 0) \qquad (2)$$

Where, x : No. of passed year after purchase, $x > 0$ integer
n : Remaining years
$x + n$: Typically 5 years for ISP
$V_f(a_k, 0)$: .Asset value at purchasing point
V_{fr} : Remaining asset value

Through the individual assets on network a_k, m unit of services can be offered, and if the service value created by a_k through the distribution of a particular service is $V_{psw}(a_k, x)$., the entire service value created through a_k can be shown as the following formula (3).

$$V_s(a_k, x) = \sum_{k=1}^{m} V_{psw_k}(a_k, x) \qquad (3)$$

If the service value of the particular asset and fixed asset value has a relationship of. $V_s > 10V_t$, $V_t \cong V_s$ is approximated since the service value is a major element in entire asset value. However, calculating the aforementioned $V_{psw}(a_k, x)$ in formula (3) is considerably difficult in an actual network. The reason is that the degree of contribution of an asset to generating individual service changes from time to time and it is nearly impossible to separate the particular service-related traffic amongst other traffic processed by each asset. Therefore, the asset loss modeling technique, suggested by Ho Kun Moon [7], uses a method that deduces each service value $V_s(a_k, x)$ of an asset generated annually. To achieve this, it incorporates the characteristics of the network that is a systematic combination of each asset and uses a reverse calculation approach to estimate the service value from individual asset components involved for the specific service, based on the revenue generated by the assets. Such approach is possible because the network has attributes, and: (1) All service users have to use the assets to access the network; and (2) the value of a high network layer service is larger or equal to than that of a low network layer service due to the layered structure of a network. Moreover, if the redundant design is not done, it can be assumed that the contributions of the network assets on the same network layer to a particular service are almost evenly proportioned to a year. Under this assumption, if the method to estimate the service value $V_s(a_k, x)$ of individual assets in a given year is simply expressed, the value can be obtained as shown in (Table 1).

(Table 1) Calculation for Total Asset value of Individual Asset

Step 1) Identify the number (m) of entire services offered at the network and each service revenue .($Sv[t]$).
Step 2) Check how many assets are contributing to generate each service revenues $Sv[i]$ and identify the asset components $N[Sv(i)]$ for all m number of services.
Step 3) Calculate $V_s(a_k, x) = \sum_{i=1}^{m} \frac{S_v[i]}{N[S_v(i)]}$ for all asset components n in the same network layer. Apply same procedure for each network layer.
Step 4) Add $V_s(a_k, x)$ to the previously calculated $V_f(a_k, x)$ to calculate $V_t(a_k, x)$.
Step 5) Compare the asset value $V_t(a_k, x)$ of each n components and obtain the priorities $prio(a_k)$ per asset, from the biggest asset value downwards.
Step 6) Repeat (Step 1) to (Step 6) for each network layer.

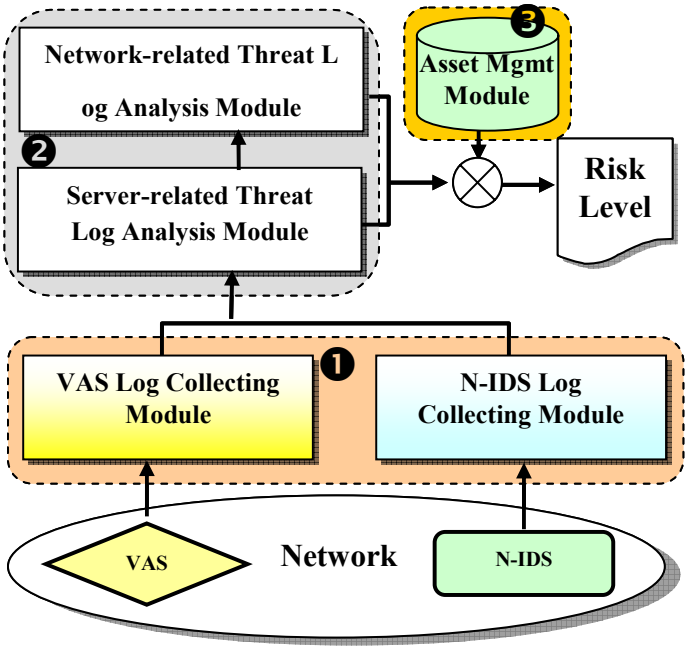
Using this method, when a particular asset is generating a number of service values, the individual service value, generated in a year by a particular asset within the same layer, can be deduced. Such calculation method can be commonly applied to all network layers. By applying such method, when the network security risk is happened, the loss amount of damaged individual assets can be deduced based on the total asset value. Also, in this modeling technique, if the network uses multiple assets that have the same functions at a particular location on the network for the service consistency, the effect from an equivalent asset is additionally considered by the redundant design. For example, for server equipment designed for load balancing and multiple numbers of routers where detour courses are

provisioned for network troubles, the I-FCM (Improved Fuzzy Map) by Jong Pil Lee [9], who improved the FCM (Fuzzy Cognitive Map) by Kosko [10], were used to deduce the asset loss when a particular problem occurs on a specific asset. Different from the existing methodologies, such an approach incorporated the objectivity in asset value estimation. The proposed method [11] can calculate the relative importance of individual assets and the risk dispersion effect due to the redundant design of network assets. The calculated asset value implies the expected loss to the asset when risk occurs, and it can be expressed in a quantitative risk level calculated through risk analysis. In the proposed system, the quantitative risk level of assets is calculated in advance and stored at the asset management DB. It conducts the risk analysis by connecting the asset information with particular system information where risk has occurred or is expected to occur due to vulnerabilities and threats detected and analyzed by the N-IDS and VAS on a real-time basis. The asset information consists of the system name, operation system name, network IP, asset value information and other management information.

3. Risk Analysis System Design

3.1 Design Considerations

In order to analyze the risk level of network assets on a real-time basis, it is essential to know the current distribution status of vulnerabilities and threats on the network. Also, it must be possible to effectively estimate how much risk can be created by specific threats. The proposed system utilizes N-IDS and VAS to collect threat and vulnerability information on the network. Also, it can be independently implemented on the system of a particular solution vendor by using an outside DB. As a result, the asset-related policies in the N-IDS system need not be set separately, so that the system can manage both the volume of typical harmful packets that may cause network interruption and other harmful packets that can directly have adverse effects on the network asset.



(Fig. 2) Risk Analysis System Structure Diagram

Previous studies [12, 13], have mainly focused on the improvement of detecting the patterns of the individual threat originations. In cases where the offensive packets originate from an address that has been spoofed, such an approach is not effective. Focused on the targeted asset subjected to the threats, the objective of this study is to improve the interpretation method of the correlation of attributes and time information from the detected information to analyze what type of risk these threats can create on the relevant assets

3.2 System Structure and Functions

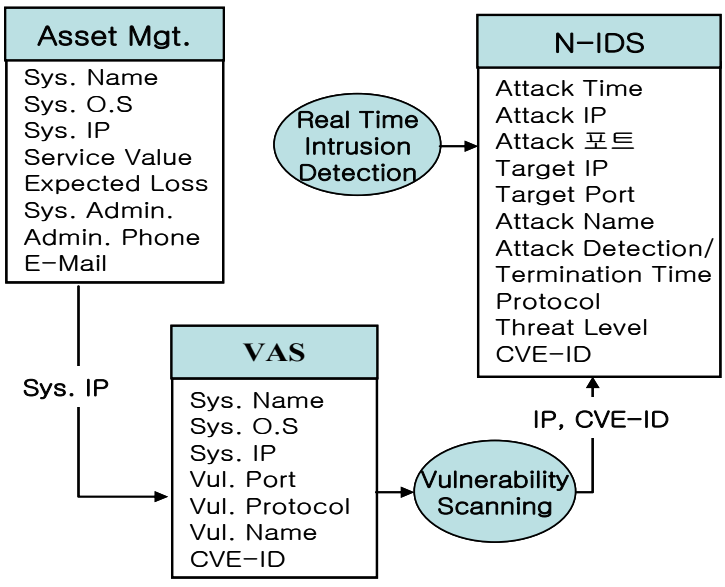
As shown in (Fig. 2), the proposed system is composed of a module (□) that collects detected information from the N-IDS and the VAS, a module (□) that separates the N-IDS log into server-related threats and network-related threats and analyzes each part, and an asset management module (□) DB that stores the expected loss values of individual assets. The functions of each module are as follows:

3.2.1 Asset Management Module

Typically, an asset is defined as anything that has value to the organization. Various classification standards and value assessment methods have been suggested. In this study, using the asset loss modeling technique [11], asset value information is estimated with the consideration of both physical value and intangible service value of systems that have information distribution and transfer functions on the network. Previously estimated individual asset value information is stored in the asset management DB with system management information (Fig .3).

3.2.2 Log-collecting Module

The proposed system uses detected threat and vulnerability information supplied by commercial N-IDS and VAS. In order to store each system log to an outside DB, it brings the data via a SNMP (Simple Network Management Protocol) trap. Although various elements can cause risks on a network, elements which are not detectable by N-IDS and VAS are not considered.



(Fig. 3) System DB Structure

The data needed for risk analysis from the collected log information of N-IDS and VAS is selected, and each composes the previously defined DB as shown in (Fig. 3). At this point,

for data correlation analysis between N-IDS and VAS, IP address and CVE-ID (Common Vulnerability and Exposures-ID) can be used as a correlation key value

3.2.3 Log Analysis Module

Different from the approaches attempted in existing studies for N-IDS detection performance improvement, the log analysis module uses and analyzes the method that separates the server-related threat log and network-related threat log based on the attributes of the N-IDS log. It can optimize the server-related threat log through correlation analysis with the VAS log [14, 15]. The network-related threat log can show the risk development potentialities through analyses in accordance to the frequency of the threat generated during a certain period, based on attack targets and the forms of constantly generated threats.

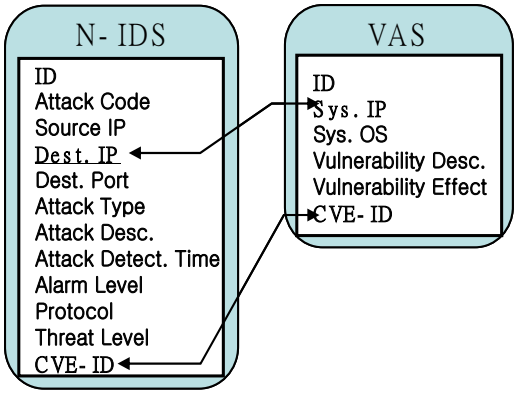
3.3 Analysis Algorithm

This study suggests a method, which separates and analyzes N-IDS log information based on attributes and an efficient information representation method

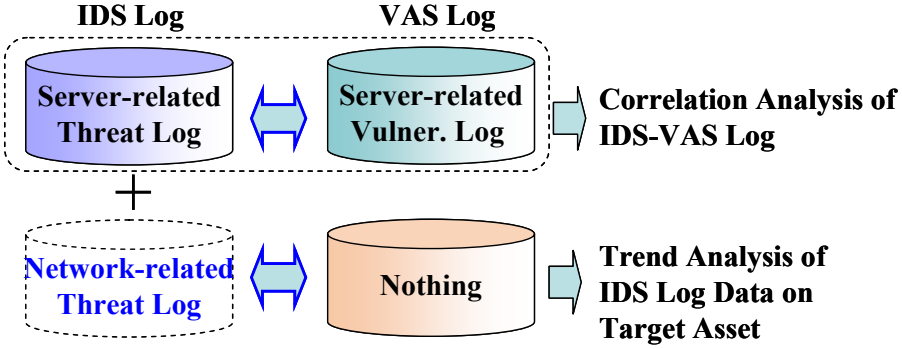
3.3.1 Server-related Threat Log Analysis

If the N-IDS log correlates with the VAS log, the threat information that may create risks can be searched using the vulnerabilities of the server. Also, it could reduce the false positives known as N-IDS problems and decreases the management burden dealing with the false positives of the administrator.

(Fig. 4) shows the forms, which the N-IDS log correlates with particular vulnerabilities detected by the VAS. However, the VAS DB has only the server software vulnerability information as shown in (Fig. 5) so that it could only optimize the threat log in regard to server vulnerabilities amongst the N-IDS log and requires a separate analysis technique for other network-related threats.



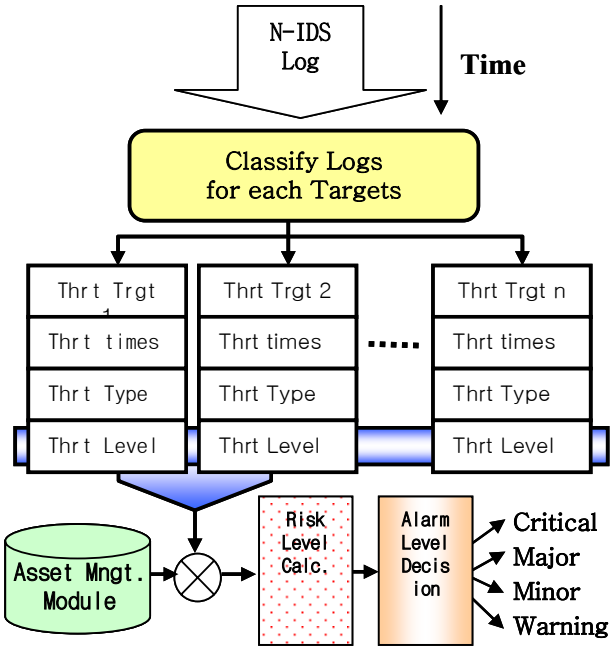
(Fig. 4) Correlation Diagram of VAS Log and N-IDS Log



(Fig. 5) Structure of VAS DB and N-IDS DB

3.3.2 Network-related Threat Log Analysis

First, through the server-related threat log analysis, the remainder, excluded from the N-IDS log correlated with the server vulnerabilities, is left as part of the network-related threat log.



(Fig. 6) Conceptual Diagram of Network Related Threat Log

(Fig. 6) is a conceptual diagram of the network-related threat log analysis module. First, generate a DB record per asset subjected to threat with the log collected in order from the N-IDS and add on the frequency and types of threats developed during a time unit. At this point, threat type information is managed in a form shown in (Fig. 7). Every time a new threat to a particular asset occurs, add on to the same DB record in chronological order.

```
[Attack Time, Source IP, Target Port, Attack Name, Protocol, Risk]
[2004/01/05 11:01:00, 1.1.1.2, 137, Netbios Name query, TCP, Low]
[2004/01/05 11:06:10, 1.1.1.3, 53, DNS Reverse Query, UDP, High]
[2004/01/05 11:08:41, 1.1.1.8, 23, Telnet, TCP, Medium]
... ... ... ...
```

(Fig. 7) Managed information Type of Threat

3.3.3 Threat Level Calculation

The N-IDS has information that contains degrees of risk previously established according to the attributes of detected individual threats [15]. Therefore, this study calculates the threat level for assets, using the risk degree (T) information established in the N-IDS for the frequency of threats to particular assets and individual threats.

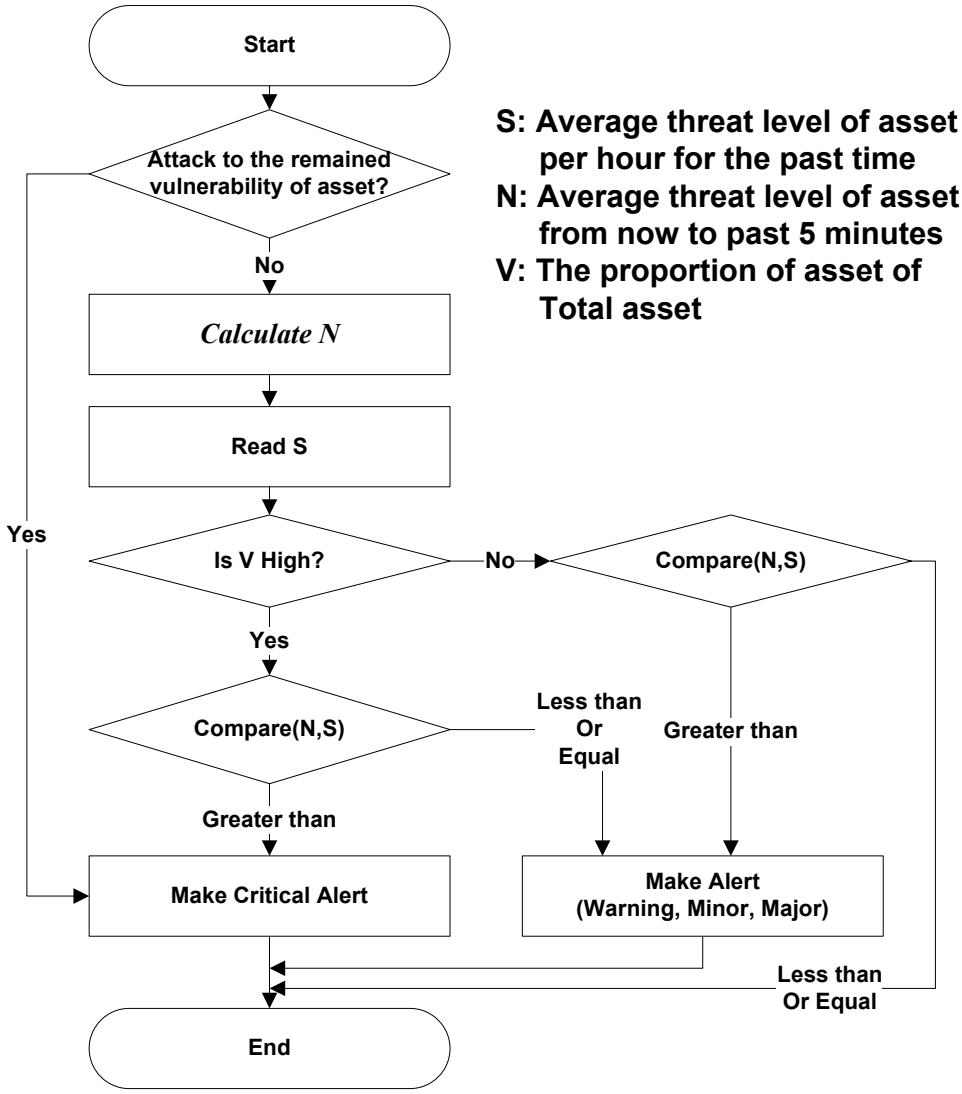
$$\text{Threat Level} = \sum_{i=1}^{n} T_i \qquad (4)$$

(n: Number of threats occurred, T_i : i th threat risk level)

If the accumulated value of the estimated threat level during a unit time (previously determined time window) reaches a certain point in formula (4), it indicates that a problem may arise regarding the availability of the asset subjected to the threat.

3.3.4 Risk Level Estimation and Alert Level Decision

If the threats to particular assets exceed a certain level, the asset management module supplies the sum of the expected loss of the threatened assets as the estimated value of the risk level. However, determination of the alert level signaling according to the risk level from the network operation point of view shall be decided after considering both the threat level and risk level in formula (4). If a threat which may prevent the corresponding asset from functioning normally exists, a prompt reaction is necessary depending on its severity even for an asset with relative low risk level (asset value). Typically, the alert levels are classified into four levels (Critical, Major, Minor and Warning), and a threshold value for dividing each stage shall be established in advance by averaging the value of a threat level during a unit of time.



(Fig. 8) Flowchart for Alert level decision algorithm

4. Test and Evaluation Results

4.1 Test Environment and Method

The proposed system is tested in the network having total 1006 servers with 7 kinds of Operation Systems. For the test, we used commercial VAS and N-IDS system as shown below. With VAS we have scanned system vulnerabilities in the network at every 3 days and stored at DBMS. We also used N-IDS Log detected during 4 days at the same period.
Proposed Log Analysis Algorithm showed that total number of N-IDS Log can be reduced to over 90% through classifying and integrating repeatedly detected N-IDS log according to its attribute. And we showed system processing results in case of intrusion detection that may cause serious impact for specific asset in the network.

- N-IDS : WinsTechnet Co. Sniper 3.0
- VAS : NileSoft Co. SecuGuard NSE 1.2
- DBMS : MS SQL 200

4.2 Test Result and Analysis

Table (1) shows the results from the vulnerability analysis of 1006 systems, using VAS. From total of 32 systems, 15 vulnerabilities are detected.
Table (2) shows the reduction of the N-IDS log according to the proposed method. In this case, all attacks generated for one day are divided per asset subjected to threats. The results showed a more than 90% reduction rate, and this implies that many threats conduct repeated attacks to particular assets.

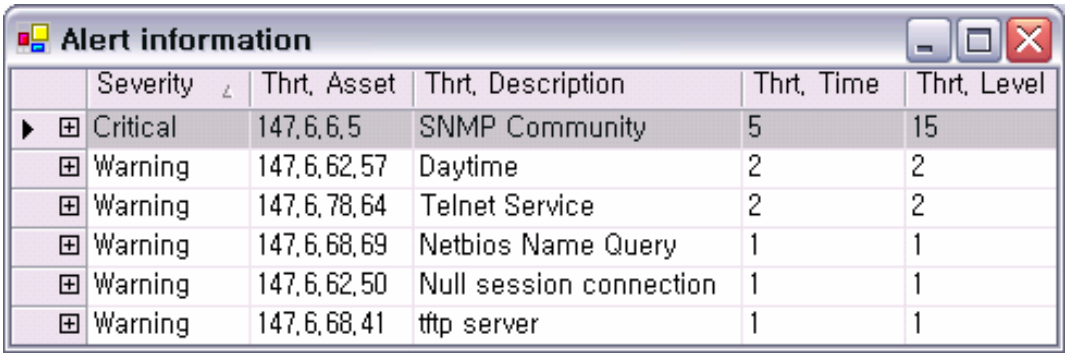
(Table 1) Results from the VAS Inspection

Vulnerability for execution of telnet service	**6**
Vulnerability in telnet service information provision	**5**
Vulnerability in setting http server of Cisco router	**5**
Vulnerability in daytime	**4**
Vulnerability in opening of X server port	**2**
Vulnerability in ICMP timestamp request and others	**10**
Total	**32**

(Table 2) Results from the Reduction of Threat Alarm

Time	N-IDS Thrt. Alrm.	Proposed system	VAS-related Thrt. Alrm	Changes
2004-01-20	**1,037**	**30**	**1**	**97.1**
2004-01-22	**111**	**3**	**0**	**97.3**
2004-01-23	**122**	**4**	**0**	**96.7**
2004-01-24	**238**	**11**	**0**	**95.4**

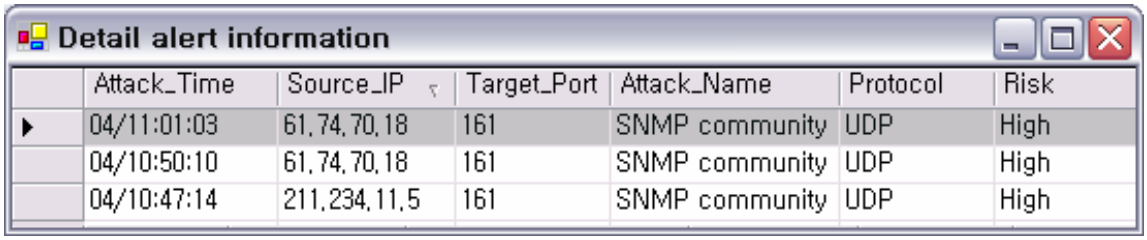
In relation to alert level signaling, the log analysis results were expressed in a form shown in (Fig. 9) in order to deduce the threat development form to the corresponding asset from the perspective of threat subjected asset and the potentiality of risk development.



(Fig. 9) Alert information Print Screen Based on Assets

(Fig. 9) shows the information of an asset which is susceptible to critical severity. (Fig.10) additionally gives detailed and timely arranged threat occurrence information when a specific row showing critical severity is expanded by clicking leftmost plus sign.

If threat level exceeds threshold value, as illustrated in (Fig.10), asset information (expected service loss value) given by asset management DB is automatically provided to the operator's console. The operator can quickly identify where the specific threat happens and can assume whether the threat may cause risk or not.



(Fig. 10) Extended Threat information Print Screen

5. Conclusion and Future Research Directions

Although most systems implemented with risk analysis methodologies offer procedures and methods that broadly consider the vulnerability of individual assets and threat elements from the managerial, physical and technical perspectives, they are not able to offer a function which estimates the risk level faced by the assets according to the changes being undergone by threat elements from the Internet and the software vulnerability of assets on a real-time basis. In order to solve these problems, this study proposes the design idea and experiment results of the system, which effectively detects network- and server-related threats using information supplied by commercial N-IDS and VAS that enables real-time based risk analysis. Through the tests, when the existing N-IDS log information are separated into server-related threats and network-related threats, and when they are correlated by the N-IDS and VAS, the threat log can be reduced by more than 90%, compared to individually operated cases. Moreover, by improving the threat detection capability and threat attribute analysis function, the system was constructed to predict expected risk levels on a real-time basis when certain points are reached. In order to increase accuracy on the risk analysis information, the following studies are further required in the future: application of standard transporting data format IDMEF (Intrusion Detection Message Exchange Format), correlation analysis of individual system logs for optimizing threat warnings and methods for establishing criteria for categorizing threat warning levels.

References

CSE, "A Guide to Security Risk Management for IT Systems", Government of Canada, Communications Security Establishment, 1996.

ISO/IEC TR 13335, Part 3, "Techniques for the management of IT Security", 1998.

ISO/IEC ,"Code of Practice for information Security Management", ISO/IEC 17799, 2000.

British Standards Institution(BSI), BS7799, 1999.

TruSecure Corporation, "A Practical Approach to a comprehensive Security Program", Hurwitz Report, 2001.

CRAMM,"A Practitioner's View of CRAMM", http://www.gammassl.co.uk/.

OCTAVE, "OCATVE Criteria, Version 2.0", Carnegie Mellon Software Engineering Institute, Dec. 2001.

KT, "Information Security Comprehensive Consulting Support System (KT-MECIA) ", Dec. 2002.

Jong Pil Lee, "Design of Fault Diagnosis Expert System Using Improved Fuzzy Cognitive Maps and Rough Set Techniques", 1997.

Bart Kosko, "Fuzzy Thinking", 1993.

Ho Kun Moon, Jong Pil Lee, "ISP Network Security Risk Considered Expected Asset Loss Modeling", CISC-W'03 Proceedings, pp.121-127, December 2003.

Eun Young Lee and 5 others. "Study on Dynamic Importance Computation Method For Reducing False Positives in N-IDS", Information Security Academic Magazine, Volume 13, Chapter 1, pp. 22-31, Feb. 2003.

Soo Jin Lee and 7 others, "Design and Implementation Of Intrusion Detection Information Correlation Analysis System", CISC-W'03 Proceedings, pp. 28-38, December 2003.

Ho Kun Moon, Jin Gi Choe, "N-IDS Log Optimized System Design Using Correlation of Network Asset, Vulnerability and Threat", CISC-W'03 Proceedings, pp. 153-159, December 2003.

http://www.iss.net/ (RealSecure)