A study about dynamic intelligent network security systems to decrease by malicious traffic

Dea-Woo Park

School of Information Science, Soongsil University, Seoul, Korea

Summary

Firewall and IPS(Intrusion Prevention System) do packet filtering as compare with the filtering rules that set up at security policies. This paper presents dynamic new plans to decrease by harm malice traffic for strengthening network security. It is the ways which designed at these papers. 1) The bypass passage that, first of all, is an enemy of authenticated packet at external routing. 2) Attack detection of an external router. 3) Bandwidth expansion. 4) It is attack information delivery to connected security system. 5) A generation of a filter. 6) Filtering rules setup of IPS and Firewall 7) Dynamic update of blocking filter 8) Dynamic network security system formation. Confirmed that it was to intelligent security system to decrease dynamic malice traffic through application of an idea about this way and the network test results at the paper.

Keywords:

DDoS, Firewall, Hacker Attack, IPS, Network Security

1. Introduction

What is a Hacker? Many journalists and writers have been fooled into using the word hacker to describe crackers. These are people (mainly adolescent males) who get a kick out of breaking into computers [1]. Kevin Mitnick [2] who was a hacker was arrested by 1995 FBI to suspicion to have stolen software and all kinds of data etc. from as penetrated into a computer network.

Security measures about an attack of hackers seem to be paradox of a window and a shield, and it is to develop an early security book to prevent if a form of a new attack of a hacker is grasped. An attack of the hacker who let you damage is attacking DoS(Denial of Service) Attacks using Nameservers in 2000, Code Red II, Nimda in 2001, MS SQL Server slammer in 2002, Blaster in 2003, and W32/Novarg.A, NetSky in 2004 [3] exploit for a vulnerability in phpBB's in 2005 [4]. exploitation of a vulnerability in the way Microsoft Internet Explorer in 2006 [5].

An attack of a hacker caused network traffic, and penetrated illegally into a network computer system, and to be serious over the whole worlds. There are firewall [6] and HIDS, NIDS [7] and Viruswall [8] like Fig.1. in the existing network security system. Firewall does an invasion interception as installed in gateway of an inner network. Be installed in an inner network, and HIDS, NIDS does intrusion detection. Viruswall cures computer Virus of a host and a network.

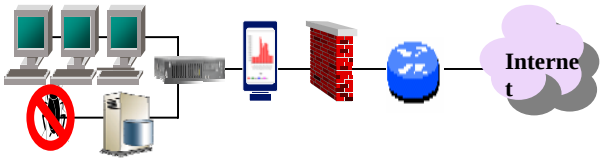

Fig.1. The existing network security system.

The existing Firewall the following disadvantage exists. 1) There is not a defense book about dynamic attacks such as DoS, the Worm which used large packet etc., or response is late. 2) Investigate a header of packet only, and Payload does not investigate it. 3) Proxy Service of Application Level cause bottleneck phenomenon of packets, and communication performance delay at gateway. The existing IDS the following disadvantage exists. 1) Misuse Detection is difficult about an unknown attack pattern. 2) Detection misjudgment ratio is high in case of Anomaly Detection about short length packet [9]. 3) There is a little the protective operation which is aggressive after intrusion detection.

Study of this paper will be studied Intelligent Connection of Network Security System overcoming these disadvantages. And it is composed to a boundary part of external, internal of a network and security systems for invasion prevention to be located in gateway and an internal network like IPS(Intrusion Prevention System) [10].

2. Related Work

I study an attack by generations of the hacker who is the related study that cared for proposed security systems

Manuscript received September 5, 2006.
Manuscript revised September 25 , 2006.

more than. Was infringed from attacks of 5 th generations of hackers at recent 6th generations, and consider it to analysis data through the results and Data Base.

A hacker makes a computer virus through a computer and networks in order to attack the target object. An attack of a hacker and a computer virus try to be divided by generations. 1th generation used Primitive Virus, 2 th generation used Encryption Virus, 3 th generation used Stealth Virus, 4 th generation used Armour Virus.

While 5 th generations circulate it so that use Worm Virus, and viral oneself is duplicated through other network and systems large by intention of an invader did it so as to attack it. This attack is a Code Red v.2 attack like a DoS attack. Propagation of Code-Red Worm used weakness point of Windows index server, and scattered. Buffer overflow of Remote existed in a Microsoft IIS web server version, and was known at that time. Hacker generated Code-Red Worm, and used this weakness point. 2001 years started an attack, and international server more than 359,000 was infected by attacks through 2001. July 19. Code-Red II. Worm through July 12. Code-Red I. Worm. Therefore caused economic assumed loss more than 2,600 million dollars, and avoid same with star statistics national ten high ranks [11].

The A which is a hacker is control to Master through attack commands, adjust Agents, and adjust Reflectors, and attack the target server which becomes to a short time, and the back jockey agents do it according to commands. Cause explosive increase traffic, and attack target server is hard to be equal to traffic, and network service makes discontinuance it like these results.

Let hacker come off an answer to be delivered to hosts to attack as deal with an answer about an accessed connection SYN request from attack object server, and the DDoS attack server of a dependency host attacks a departure of network traffic. And attack it of the N:N which an invader is not exposed to even if I chase it.

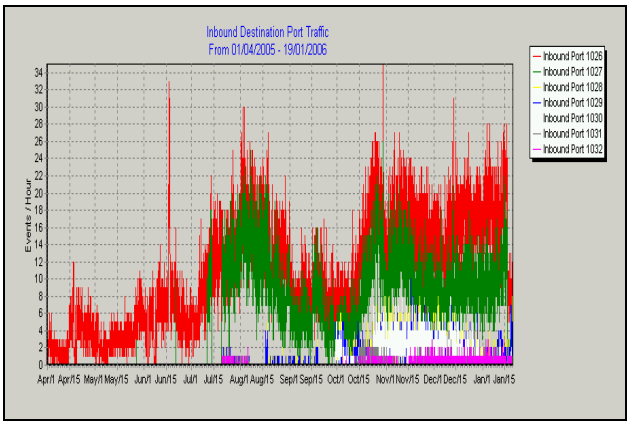

Fig.2. Traffic ratio 01/04/2005~19/01/2006.

Fig.2. showed network traffic by ports from 01/04/2005 to 19/01/2006. The section which was above displayed of a graph is network traffic along an attack. An attack of the current hacker will be made progress to 6 th generations at 5 th generations. Also, use a low-ranking infection system in the state that expose status of an invader, and do not get through a Command union and hacking by hacking Programming, and attack target. A hacking technique is converted in automation ways at manual operation ways, and is mobilizing the way how explosive increases expansion and harmful traffic by a threat about Internet network serviceability.

3. Intelligent Connection of Network Security System

Define target of intelligent connection of network security systems proposing it at this paper.1) Defend dynamically an attack of a DDoS, Worm back causing malicious traffic. 2) Execute actively functional renewal of security algorithm to reduce malicious traffic. 3) Grasp an attack of hackers to intelligent, and dynamic communicate this information to security systems. 4) Reduces traffic bypass authenticated packet. 5) Detect it as use service of Application Level, and analyze intelligent it to through misuse detection and abnormal detection, and be connected to an early IPS, and drop dynamically malicious packet and close the service port.

Propose the intelligent connection of network security systems that structure sets up a situation to gateway and an internal network from external boundaries of a network. The existing firewall system not determinate the victim target which invaders decided on. The packet which is malicious traffic is harmful at a target network or server act. Use an external router and internal router and a switch detect malicious DDoS or traffic by Worm and cut off the attack. Firewall and IPS cut off computer viruses and malicious traffic that attack of a hacker.

A proposed way of intelligent connection of network security system is enforced with 8 phases.

1) The bypass passage that, first of all, is an enemy of authenticated packet at external routing

Packet getting approval introduces priority order, and get the passage through authenticated packet or tunneling at external router as use time, a authentication table for routing to do packet. Bypass works at internal router, and this packet executes service and access control about a port and an invasion interception until application level at gateway firewall.

2) Attack detection of an external router

If authenticated packet traffic exceeds statistical normal capacity, executes packet network time-sharing service at external router. Execute attack detection algorithm about packets connected to exceed normal capacity. The attack detection is carried out at intelligent connection of IPS and modules functional connected invasion detection.

Be delivered to internal router, and use feature extraction and Anomaly Detection, and attack detection information uses again information of OSI 2-4 Layer in order to classify packet. There are an address collation, a HTTP string and a substring collation, general pattern matching, analysis accessed TCP, exceptional packet detection, abnormal traffic detection and TCP/UDP port collation etc. in a detection technique.

Transmit network traffic through Protocol Anomaly Detection engines. Use multi-filters in order to detect malicious packets. A lot of invaders attack target server in case of DDoS attack. Malicious packet has the same destination address about the attack object. If the traffic which had the same destination address is analyzed to a statistical more than normal capacity, use attack detection algorithm of a DDoS back. And operate switching devices, and extend network bandwidth.

Also, the server which a destination address of a computer virus is made voluntarily, or was infected is a network address like layman 192.165.1.0/24. The second server sends out address of infected server. At this time a computer virus has the protocol structure that specified weakness point of the operating system and the similar port number that is used generally. For example, SQL Slammer has UDP 1433port, 1434 fort, and Blaster has TCP 135 port. Therefore, the detection can do packet of an invader by a key word.

3) Bandwidth expansion

Be the only switch type implementation of a device reset, and another thing is buffer type implementation [12]. Use switching unit, and switch type implementation can change setting. The first L4 or L7 switching devices have main setting memory. An attack pattern by a type of an invader renewed to detection module about the existing attack, packet filtering for the existing invasion blocking and new ones and attack packet information are based on information analyzed at data base. A new attack is detected by Anomaly Detection, and malicious traffic in packet analysis operates switching unit, and guarantee does bandwidth.

4) Attack information delivery to connected security system

As is transmitted immediately between internal router and firewall and IPS, attack information is exchanged. Be sent by elaborate identification and reporing engines for real-time reports. Use a network of connection IPS managing, and key management about exchange information uses an extension of BGP (Border Gateway Protocol) and SNMP (Simple Network Management Protocol). Be saved in internal IPS, and the attack form, the attack time that they were analyzed since they were found etc. filtering about a new attack and an blocking module publicize.

5) A generation of a filter

The existing hacker attack finds it at external router, and stop up a fort during packet filtering and filtering against an attack, firewall of gateway and connection of IPS at internal router in Table 1.

Table 1. System design in Intelligent Connection of Network Security System

Connection Limit Optimization									
Syn Flooding Malicious Optimization									
(Input)	Application			Profiling		Engine			(Output)
RECEIVER	**Packet Filtering**	**L4, L7 switch Filters**	**Stateful Inspect Engine**	**Deep Packet Inspection**	**IDS / IPS Checks Protocol Validation**	**IDS / IPS Checks Content Inspection**	**DDoS Filters**	**Rate Limit Filters**	**TRANSMITTER**
	Allow / Block	Allow/ Block	Packet, Session, Handling	Packet, Session, port, Handling	All / Some Checks Monitor, Allow/ Block	All / Some Checks, Monitor, Mitigate, Allow/Block	Allow/ Block	Allow / Block	
Counters Only, Allow / Block, IDS / IPS, Exceed /Transition									
Bypass Mode									
Logging / Reporting									

Generate actively the filter which use the netfilter, iptables which can set up a rule of Packet filtering etc. filtering module, and let you drop packet of an invader and close a service port of an invader. Use these blocking function, TCP expansion, source-port, destination-port, UDP expansion, log, reject, return, queue and load dispersion mind, and to exchange the input that is a chain, output, a chain of user designation to generate a new chain besides forwards, NAT (Network Address Translation) utilization, by the existing strong Round Robin methods change the destination address to 192.165.1.2 this or 192.165.1.3 or 192.165.1.4 etc., and design a function of blocking filter.

Use Stateful Inspection firewall cut off malicious network traffic running layer 2 and layer 3 filtering. Deep Packet Inspection technology carries out an IP Fragment, TCP Segment process protocol, Acceptable Application Use and a verification Stateful pattern matching function through only network processor.

Remove malicious message after abuse detection through IPS Data Base as keep State and Context. Allowable applications use policy, protocol validity check, an attack and a module protective vulnerability Signature, anti-virus, spy ware etc. Like buffer overflow attacks the

traffic that cannot be enough is cut off the protocol refusal that expropriation is possible.

6) Filtering rules setup of IPS and Firewall

As carry interception filter information on its back by priority order works, and is dated, external router executes immediately filtering. Stop up service related to an invader at the connection of internal IPS which firewall of gateway and were become and a fort permitted.

7) Dynamic update of blocking filter

New attack information except the existing attack becomes up-date to connected security systems by IPS. A security rule about a new interception filter is appended to a filter table, and be notified immediately to system administrators.

8) Dynamic network security system formation.

Intelligent connection security systems are operated dynamically automatic filtering and a constabulary book be set up. A new filtering rule is generated to artificial Intelligent at the immediate IPS which attack packet was found, and filtering is reflected dynamically, and a filter becomes a generation to external router, internal router and firewall and IPS.

The current high-speed packet process function is implemented to ASICs. Therefore, filtering policy or use protocols and procedures to exchange board or a chip in order it modifies new information, or carry it on its back, and to date of an invader are necessary. Intelligent connection of IPS proposing it at these papers uses devices reset which can deal with traffic more than 1 Gbps in order to renew dynamically the algorithm that a new filtering rule and discontinuance of service are not whenever a new attack is found.

Be the only switch type implementation of a device reset, and another thing is buffer type implementation. This implementation use switching unit, and switch type implementation can change setting. The first L4 or L7 switching devices have main setting memory. Require 2 times of the hardware device volume of implementation. Buffer type implementation uses dynamic reset memory. First, reset memory is recorded as important configuration, and, second, reset memory is recorded as new setting. Buffer type can save packet during reset, and require switch type than the hardware volume. Be intelligent, and can exchange the attack detection and a dynamic filtering rule for switch type to systems through real-time operations through reset memory with buffer type.

4. Performance Evaluation Experiment

Set up does intelligent connection IPS to gateway firewall of the existing external router and internal router. Set up the attack detection and public information proposed and a device and a system reset intelligent exchange and invasion prevention function of filtering policy for dynamic execution, and established a performance experiment system. Set up an attack system of a hacker through attacks the Slammer computer viruses in indefinite way, SYN flooding attack and DDoS attack.

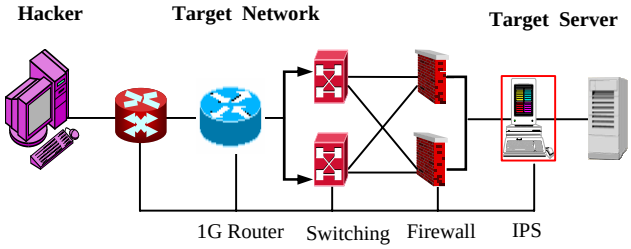

Fig.3. Structure of intelligent connection of network security systems

Fig.3. assumed the network simulation model that network traffic joined an experiment network to have appeared through 1Gbps router the front of internal network and 10 Gbps router which were external router and internal server were connected of 1Gbps router. The external network system that was used so as to verify intelligent connection IPS generates three 2.5 Gbps phosphorus 7.5 Gbps background traffic and 2.5 Gbps traffic getting a SYN flooding attack and DDoS attacks and infection of a Slammer computer virus done to normal MPEG stream.

Evaluated residual bandwidth of an experiment network as analyzed the performance experiment results. Were proposed, and before start of intelligent connection IPS minimized an influence to reach to the experiment results as reset a firewall system for a test.

A host assumes with one state during permission, infection, 3 state of a movement in simulation experiment. Get infection done for the first time, and the start steps other hosts are all converted with permission state as they select voluntarily a host of external. Copy a computer virus on other host whom an address was generated voluntarily, and a infected host transmits it by a speed of a total circuit.

The results of an experiment network show to a chart between time and packet process ratios as analyze relationship.

4.1 Invasion Prevention Experiment about an Attack of a Hacker

A hacker executes it at arbitrary hosts of external for SYN flooding attacks to have been made as use an address to have been forged. SYN flooding attack used The Regents of the University of California [13]. Send the IP address packet which deceive a client, and was forged to a

network. Network Neighborhood executed it for experiment through direct communication lines.
Hacker used Stacheldraht Tool in order to attack DDos. Also, a hacker brings down a command to Master, and induction gets in a moment the server which target becomes to 1 Gbps packet traffic through Agents and Reflectors attacked it.

A Figure 4 is the attack packets which analyzed to the Network Protocol Analyzer Etheral version0.99.0.[14]

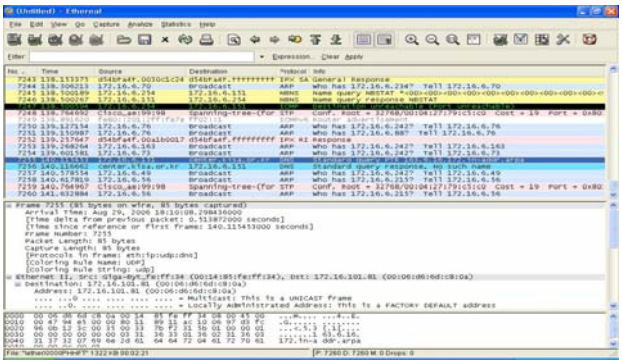

Fig.4. attack packets analyzed to the Etheral version0.99.0

Packet size viral Slammer Worm did it with 376 bytes. Infection delay time did it so as to transmit it after reproductions toward a secondary infection host as played assumption by 0.1 second the beginning [15]. If re-infection by other computer viruses reproduced works, infected host should not exchange an infection action. A traffic generator sends Slammer packet to a traffic analyzer about Slammer computer viruses in order to evaluate efficiency. A generator sends it to the destination address which was selected voluntarily. Assumed increase about radio waves of a Slammer computer virus according to medical charge time of infected hosts in order to analyze the attack detection, analyses and security policy renewal, an influence of invasion prevention.

And were independent, and selected voluntarily the non infected host, and faced the host selected each time of infection process particularly whether or not were by infection tested it.

Fig.5. appeared to what an attack began, and was proposed through SYN flooding within two seconds, and an attack by systems was cut off. Caused a DDoS attack, and in 13 seconds sections of a hacker Fig.4. got you through explosive increasing traffic of 1Gbs about target server of internal.

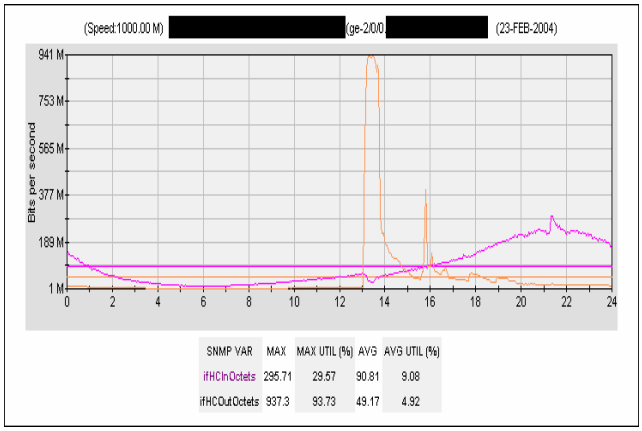

Fig.5. Protective graphs at intelligent connection of network security system

But invasion prevention system to be connected to router, firewall to IPS showed the results that had prevented an attack of DDoS, and 14 seconds sections cut off malicious traffic, and prevented an invasion. Also, the results value graph dynamically normalization got traffic of a network done like the output ratio that used a Slammer computer virus.

Fig.5. were proposed, and a continuous 4th line shows residual bandwidth in internal networks of intelligent connection of IPS. That is, attacked it, and detected it as grasped actively an attack of a hacker, and publicized to intelligent connection system.

The traffic which was a computer virus by invasion blocking and invasion prevention was done away with an interception, and appeared to what can preserve the majority of bandwidth permitted through algorithm of an invasion prevention security rule.

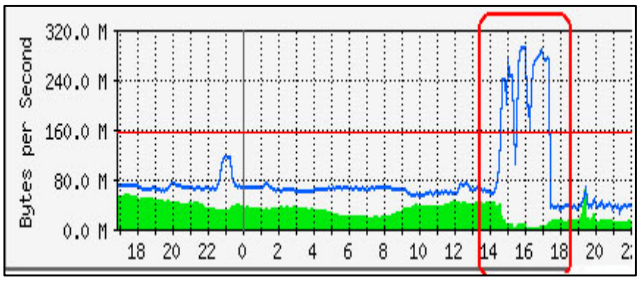

Fig.6. Protective operation about a Slammer virus attack.

MRTG[16] is networks and the system monitoring that used Figure 6. At 15second band, started an attack to a network through port 1433 as used slammer virus. At 17second band, A interception about an attack of slammer virus was performed, and ensured normal network bandwidth.

Obeyed it, and were proposed at the results, the these papers that analyzed the performance evaluation results about an attack of a hacker through attacks and the SQL Slammer computer viruses which used a SYN flooding attack and DDoS, and intelligent connection of IPS was evaluated excellent security.

4.2 Connection Experiment of Invasion Prevention Algorithm

Grasp traffic by attacks of a hacker and ideal of service, and the valuation results of a function up-date of invasion prevention algorithm to devise an aggressive security defense book about this look [12].

A function is changed, and a number of packets to have lost when I use renewal of invasion prevention algorithm. If there is a lot of the packet which have lost, cannot use renewal of invasion prevention algorithm by real time, and invasion prevention algorithm about an attack of a hacker cannot renew it. The progress when packet is not therefore lost shows renewal of normal invasion prevention algorithm. An up-date function of algorithm of middle packet size is renewed at small scale security systems, and be renewed at small scale security systems in case of large packet size. The large size of packet carrying out an independent function to indicate that no packet is lost when a function is renewed [12].

Therefore, be the results to be reliable by a function up-date of invasion prevention algorithm to devise the aggressive security defense book which proposed it at these papers.

5. Conclusions

I studied it with an attack of 5 households and 6 households that was an attack tendency of a recent hacker and investigation about the damage at these papers.

Proposed intelligent connection of IPS at papers watched the existing firewall and a disadvantage of an invasion detection system that was used in order to prevent an attack of a hacker, and to have seen them in order to solve a problem.

It is the ways which designed at these papers. 1) The bypass passage that, first of all, is an enemy of authenticated packet at external routing. 2) Attack detection of an external router. 3) Bandwidth expansion. 4) It is attack information delivery to connected security system. 5) A generation of a filter. 6) Filtering rules setup of IPS and Firewall 7) Dynamic update of blocking filter 8) Dynamic network security system formation. Were designed as proposed, and reset used a possible process, and imposed firewall of external and internal router and switching devices and gateway, and intelligent connection of IPS detected attack packet and service, and installed blocking filter and the IPS which prevented in an internal network.

Executed a SYN flooding attack and a DDoS attack and a Slammer attack to attack traffic of 1 Gbs in speeds wire 10Gbs in performance experiment.

Cut off a SYN flooding attack, and the results that they attacked it, and they executed, the security system that proposed it DDoS attack and Slammer attack did a blocking.

If an attack was detected, these results enlarged bandwidth through reset of L4, L7 switching devices at router. Public information about attack information was performed dynamically, and generated a filter of intelligent filtering algorithm, and dynamic renewal and Up-date were executed.

As a result, packet by attacks of a hacker was drop, and traffic was decreased, and ensured the residual bandwidth which was normal of internal and traffic of an external network besides normal packet.

Improved a traffic delay, and therefore intelligent connection of IPS appeared as improved the existing invasion blocking and a disadvantage of an invasion detection system.

The following study, influence analyses of a protocol about intelligent connection of the section which proposed it and security and algorithm and an invasion prevention researcher up-date filtering about a traffic distribution are necessary.

References

[1] Eric S. Raymond. (Editor): http://www.catb.org /~esr/faqs/hacker-howto.html. 7 Mar 2006

[2] Kevin Mitnick.: http://www.webster.edu/ philosophy /umbaugh/courses/frosh/dairy/mitnick.htm

[3] CERT/CC Incident Notes.: http://www.cert.org/ incident notes

[4] Exploit for a vulnerability in phpBB's.: August 01, 2005-Current Activity. http://www.us-cert.gov/ current /archive/ 2005/ 08/01/ archive.html

[5] Exploitation of a vulnerability in the way Microsoft Internet Explorer.: http://www.us-cert.gov/current/ archive/2006/04/03/archive.html#iememfail

[6] Ray Hunt, Theuns Verwoerdb.: Reactive firewalls a new technique, Computer communication 26. (2003) 1302-1317

[7] Dreger H, Kreibich C, Paxson V, Sommer R.: Enhancing the Accuracy of Network-based Intrusion Detection with Host-based Context.

Lecture Notes in Computer Science, Vol. 3548 (2005) 206-221
[8] TREND MICRO White Papers,: The Trend of Threats Today: 2005 Annual Roundup and 2006 Forecast (2006)
[9] JensTolle, Marko Jahnke, Michael Bussmann, SvenHenkel.: Meta IDS Environments: An Event Message Anomaly Detection Approach. Proceedings of the Third IEEE International Workshop on Information Assurance (2005)
[10] McAfee.: White Paper_Host and Network Intrusion Prevention. http://www.mcafee.com/us/local_ content /white_papers/wp_host_nip.pdf, (2005)
[11] David Moore, Colleen Shannon, Jeffery Brown.: Code-Red: a case study on the spread and victims of an Internet Worm. Internet Measurement Workshop (2002)
[12] Masaru KATAYAMA, Hidenori KAI, Junichi YOSHIDA, Hiroki YAMADA, Kohei SHIOMOTO, and Naoaki YAMANAKA.: A 10Gb/s Firewall System for Network Security in Photonic Era. IEICE TRANS. Vol. E88-B, No. 5, (2005)
[13] Vulnerability Note VU#596827.: http://www.kb.cert.org/ vuls/id/596827 FedCIRC Advisory FA-2000-01 Denial-of-Service Developments.: http://www.us-cert.gov/federal/archive/advisories/FA-2000-01. html
[14] Etheral version0.99.0. http://www.ethereal.com/download. html (2006)
[15] David Moore, Vern Paxson,: Inside the slammer worm. IEEE COMPUTER SOCIETY, (2003)
[16] MRTG -2.14.6. http://oss.oetiker.ch/mrtg/ (2006)

Deawoo Park is an Adjunct Professor of Computer Science Department at the Soongsil University, South Korea. Dr. Park received the B.S. degree in computer science from the Soongsil University in 1995. And he received the M.S. degree in 1998. He received the Ph.D. degree from the computer science department of the Soongsil University in 2004. Dr. Park has worked as the Head of Researcher and Developer Laboratories at Magiccastle co., LTD. Dr. Park is studying it to Senior Researcher of an IT Infrastructure Protection Division of Korea Information Security Agency. His interests include Cyber Reality, Information Security of computer and networks, Mobile Communication, Ubiquitous Information Security.