International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.113-122
http://dx.doi.org/10.14257/ijsia.2014.8.1.11

A Study on the Integrated Security System based Real-time Network Packet Deep Inspection

Chang-Su Moon[1]and Sun-Hyung Kim[1]

Dept. of Information & Communication Eng., Graduate Soonchunhyang Univ., Chungnam, Republic of Korea
csm@gns.kr, shkim@sch.ac.kr

Abstract

With the volume of Internet communication continuing to increase, there are more cases of worm and virus intrusion through the network. The security system against external attacks that use various security vulnerabilities consists of firewall and intrusion detection and prevention subsystem, and its functionality is becoming more advanced. As indicated by the recent security issues and intrusion cases, however, APT attacks and worm and hacking must be dealt with continuously. As such, enterprises are investing in various measures for an integrated security system to identify the threats of network security-based security vulnerabilities and cope with theme effectively. This paper proposes a network packet in-depth test-based, integrated security system that analyzes the threat factors through a total study of network packets circulated in realtime and applies various security functions to cope with intelligent security threats in the future.

Keywords: *Real-time Network Packet, DPI (Deep Packet Inspection), APT(Advanced Persistent Threat), IDS, IPS*

1. Introduction

Intrusion by worms or viruses through the network is continuously increasing and evolving. Moreover, incidents such as leak of high volume of personal information and large-scale system faults caused by external hacking often occur. Although firewalls block attempts at unauthorized intrusion, they only inspect the headers of the packets; thus, they are still vulnerable to attacks through the authenticated IP and open ports. Intrusion detection on the network layer involves monitoring various network services and finding abnormal service or behaviors by monitoring the IP packets of the service or sessions as the connections between the terminals. In the former, the system can monitor and analyze a packet to determine which malicious contents it has and which known attack patterns it contains, since communication is established through packet exchanges between an origin and a destination. Such monitoring of packets is widely applied in traditional security systems and network analysis system such as IDS(Intrusion Detection System) and IPS(Intrusion Prevention System). Since it must inspect all packets in the network, however, it generates high overhead in the analysis system and has difficulties in detecting unknown attack patterns. To address such problem, the system applies deep packet inspection (DPI) technology to inspect the packet in depth in terms of contents<?>.

The task that takes the most time in a network-based security system -- such as firewall or IPS -- is pattern matching inspection, which compares the packets with a set of pattern rules.

[1]Corresponding author: Tel.:+82-31-000-; Fax:+82-31-000-0000.

ISSN: 1738-9976 IJSIA

Pattern matching inspection is multi-pattern matching that matches multiple patterns simultaneously. The method of comparing the port, IP address, and type of pattern used only in the existing security system to evaluate harmfulness is not suitable under the large-capacity, intelligent, and advanced persistent threat (APT) environment. In particular, since even organizations with highly advanced security systems have been vulnerable to attacks such as APT, which continuously targets a specific subject, many enterprises and organizations struggle to find countermeasures.

Therefore, this paper seeks to discuss the concept and functions of an integrated security system based on real-time network packet deep inspection to cope with possible hacking and security threats in cyber space.

2. Related Research and Technology Trends

2.1. Intelligent Security

Intelligent security refers to the next-generation security information analysis technology that improves security intelligence by analyzing the correlation between the data and security events generated by the network, system, and application system of the main IT systems to cope with unknown fatal attacks such as APT.

Existing security methods have shown limitations against the subtler, more precise cyber-attacks under the rapidly changing IT environment; hence the importance of detecting subtle attacks by understanding the correlations instead of simply blocking a threat factor.

Intelligent security as defined by the Gartner Group is the concept and methodology enabling the interaction of various security technologies. It pertains to the context-based analysis technology that integrates data from various sources and has interrelationship. From the short-term perspective, it is expressed in the form of context-aware security and is considered the leading security technology for the next 5 ~10 years.

Therefore, it is expected to overcome the limitations of the pattern-based attack control technique utilized by existing security systems and evolve into a technology that detects new unknown attacks by analyzing the correlation of various elements (system process, activity level, network transaction, *etc.*,).

Studies are actively being conducted on the integrated security system -- an intelligent security technology utilizing security event information management technology integrating the network and system security products group to defend against targeted attacks -- and big data processing technology.

2.2. Network Packet Structure and Type of Test

Network packets and IP (Internet Protocol) network, which is the smallest unit, are transferred or routed.

A network packet is mainly divided into header and payload. A header can be further divided into IP header and protocol header (Figure 1).

Figure 1. Structure of Network Packet

Located at the outer edge of a packet, an IP header contains data such as the source IP address, destination IP address, and length of packet in bytes. It is similar to the address in a mail, and it may also contain other data such as transmission priority. Next to the IP header is a transmission layer header called TCP, which has the function of identifying the address of the end terminal and providing the error data when the packet is lost. A TCP header consists of the source and destination port, sequence number, *etc*.

Data are partitioned, encrypted, compressed, and packed before they are transmitted and subsequently unpacked, decrypted, and reassembled following their transmission. Such process is deployed by a reference model generally called OSI (Open System Interconnection) layer. In the OSI layer and packet architecture, headers occupy 1 ~ 4 layers, but the payload occupies layer 5 or higher.

The network equipment generally includes the switch hub, firewall, router, and server. The functions of each network device are performed in OSI layers 1 ~7. As shown in Figure 2, a switch hub processes the MAC header, whereas the firewall decomposes and processes 4 layers including the IP header.

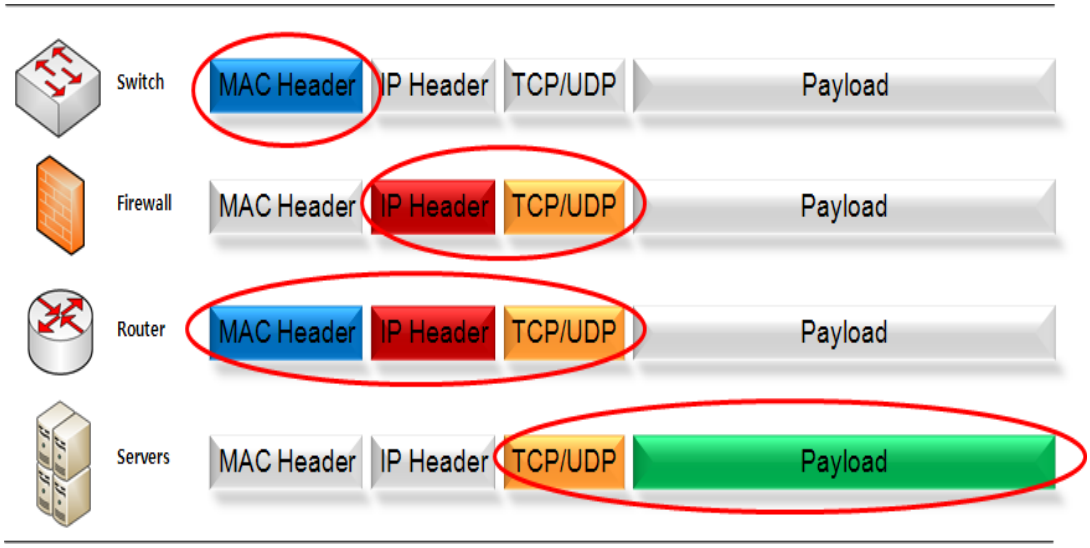

Figure 2. Packet Utilization Range of Network Equipment

The network packet inspection type is generally categorized by how many network layers are inspected. Although there is no definite category, Parsons (2008) categorized them in 3 levels, whereas Cooper(2010) categorized them in 2 levels. This study adopted the categorization by Parsons (2008)[10].

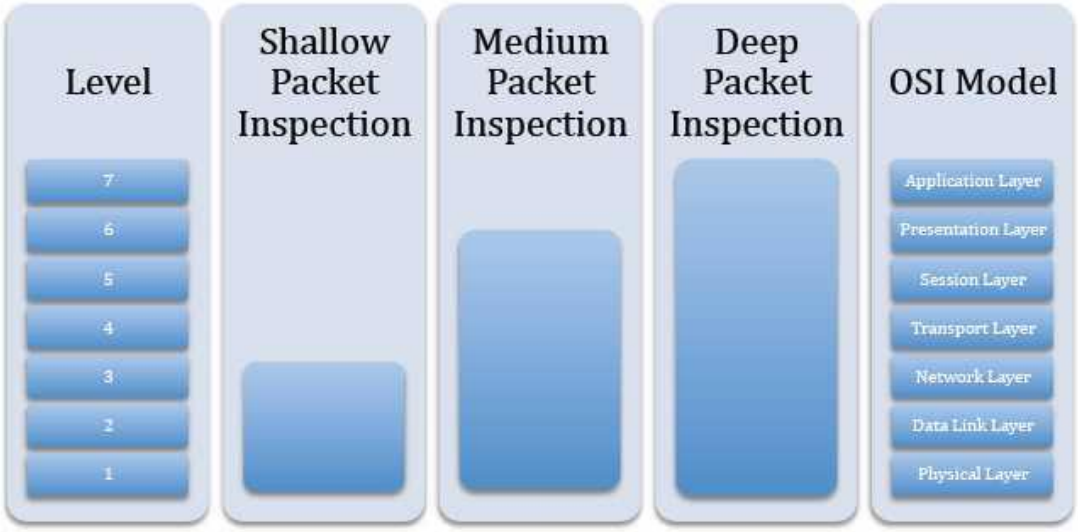

Figure 3. OSI 7 Layers and Packet Inspection Level

3-level packet inspection is divided into shallow packet inspection (orstatefulpacket inspection, SPI), medium packet inspection (MPI), and deep packet inspection (DPI). Figure 3 shows the levels of SPI, MPI, and DPI in the OSI architecture described above. It inspects the header data and drops the packet if the data are included in the blacklist. In other words, SPI cannot read the session, presentation, and application layers; consequently, it cannot inspect the payload part of the packet. Since it evaluates the packet using only the header data, SPI cannot thoroughly analyze (especially inference of the application) the traffic but can process high-volume traffic very fast compared to DPI.

MPI means the application proxies because it does not retrieve the data directly from the PC but passes it through a temporary storage unit called proxy. When a packet is inputted into a proxy system, the proxy system checks the packet header in accordance with the parse list. An application proxy is aligned with the network routing devices so that network administrators can apply the predefined rule across-the-board by having all traffic pass through the proxy system. To decide whether a packet will be transmitted, the blacklist of SPI only considers the IP address, whereas the parse list of MPI decides based on the data format type and Internet address. For example, an administrator can use the MPI system to make sure that a flash file or an image file in a website of SNS will not be opened in a PC. On the other hand, an MPI system lacks scalability and consequently requires a separate application gateway for each application if there are diverse applications, but such can delay the transmission. Therefore, it may not be useful to Internet providers operating a large-scale network supporting various applications.

The concept of DPI first appeared around 2000. Its exact meaning is somewhat vague since it is not a standardized technology. Although generally known as the technology for inspecting not only the packet header but also the payload part with contents, how it is deployed is not usually disclosed since it is considered the proprietary information of each DPI vendor. Unlike SPI or MPI, DPI can be used in a large-scale network environment since

it is designed to process hundreds of thousands of packets and determine which program generates which packets in a second. A DPI system stores hundreds of thousands of packets in the memory until there is sufficient information to match the already identified packet type. When a new packet is matched to the identified packet list, the system recognizes which application created the packet and applies the rule to decide whether the packet will be transmitted [10]. If the DPI system cannot identify the application even after inspecting the packet header and payload parts, it checks the pattern to find out how the packet is exchanged between the computers.

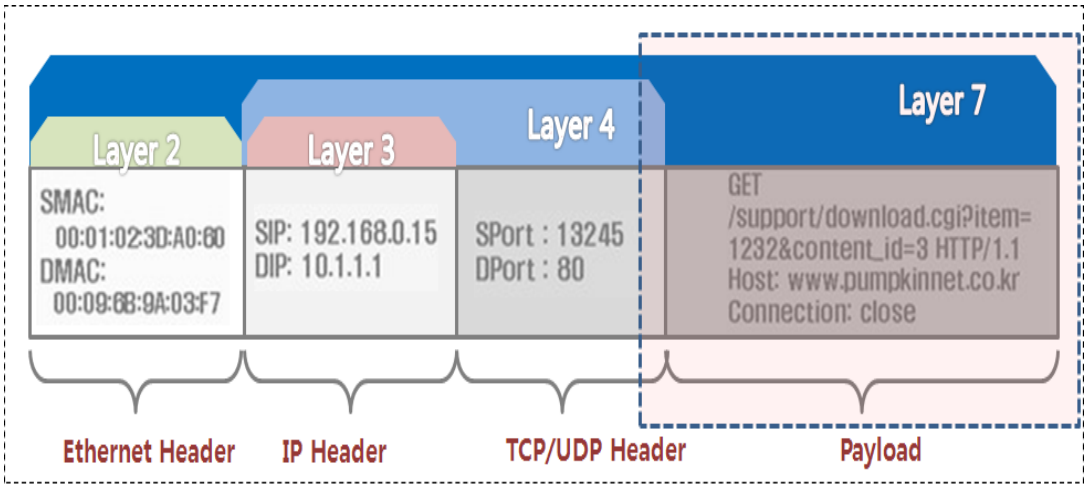

Figure 4. Inspection of Real-time Packet Based Layer 7

Real-time DPI -- wherein security devices such as router and switch read and analyze in realtime not only the packet header but also the payload part containing the data contents of the OSI 7 layer-based packet as shown in Figure 4 -- indicates two attributes. First, the DPI technology has evolved to analyze Internet traffic in realtime and process them differentially. Second, many different functions can be supported by a system. As such, it can be used for various purposes such as security, traffic management, blocking of malicious contents, and customized advertising.

Therefore, real-time total inspection of network packets must use DPI to inspect even the payload part in the 7-layer architecture. DPI-based network traffic analysis enables checking of vulnerabilities, risk factors, and possibility of intrusion such as hacking by collecting network traffic pattern data and performing total inspection and analysis of the packets. Moreover, an appliance integrating HW and operating SW is needed to predict service change according to the analysis result and enable service optimization and service personalization.

2.3. Concept of Integrated Security Systems

An integrated security system is an information system that integrates the functions of individual security systems to enable real-time network packet inspection, analysis, vulnerability prevention, service optimization, network control, and network log recording.

As shown in Figure 5, a commercial security system consists of the network, device, contents, and platform to perform various functions. Network security solutions include IPS, IDSS, firewall, network access control system, integrated risk management system, and VPN. An integrated security system is a security system integrating the security systems performing the above functions.

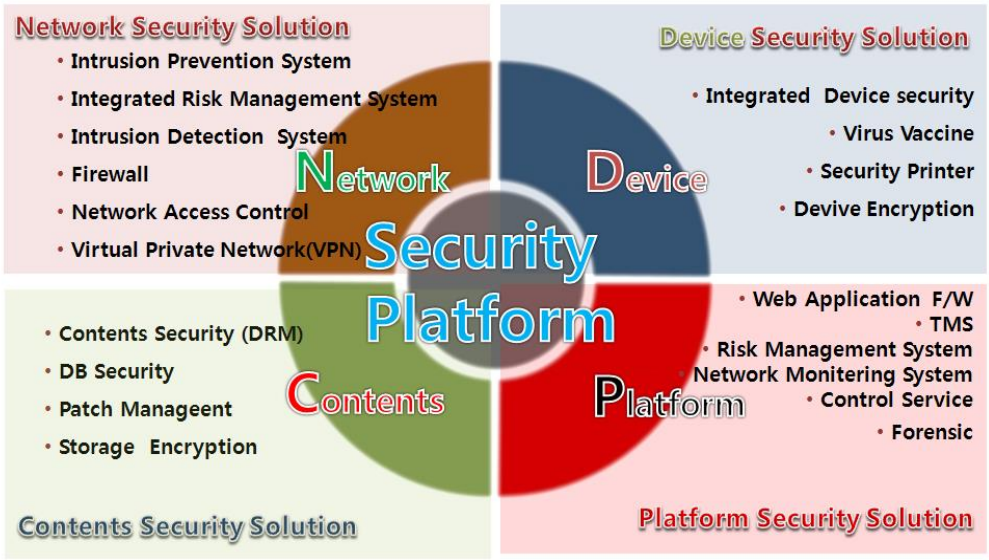

Figure 5. Features of Integrated Security System

3. Integrated Security System Utilization

3.1. Architecture of Integrated Security System

An integrated security system consists of packet signature definition, categorization, control, and authentication steps. It supports the service of each of the assorted application programs as well as the user/group, bandwidth guarantee, and authentication in realtime using the packet inspection policy, visualizes the policy, and monitors it (Figure 6).

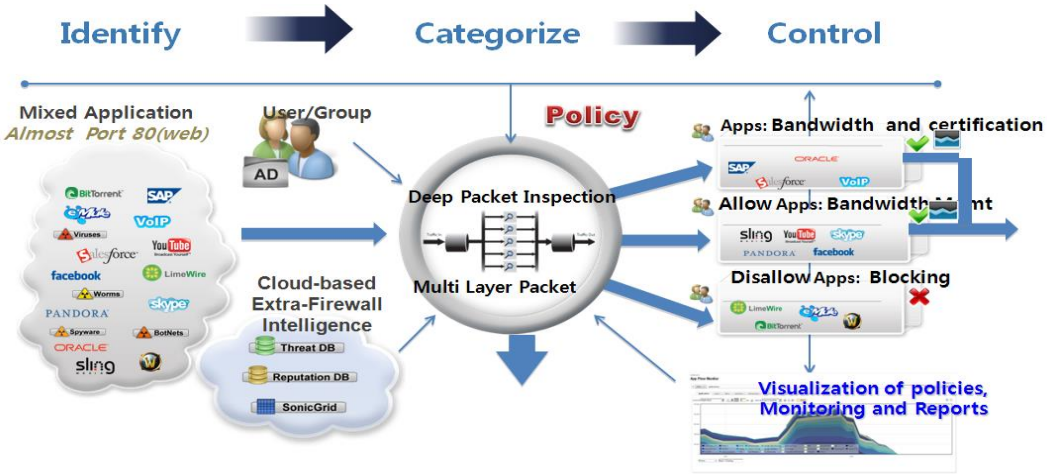

Figure 6. The Operational Architecture of Integrated Security System

Therefore, an integrated security system is not just a conventional UTM (Unified Threat Management) system that simply combines the security systems; it is a system connected to the network and application server to monitor and control security threats in realtime and support PKI-based authentication at the application level (Figure 7).

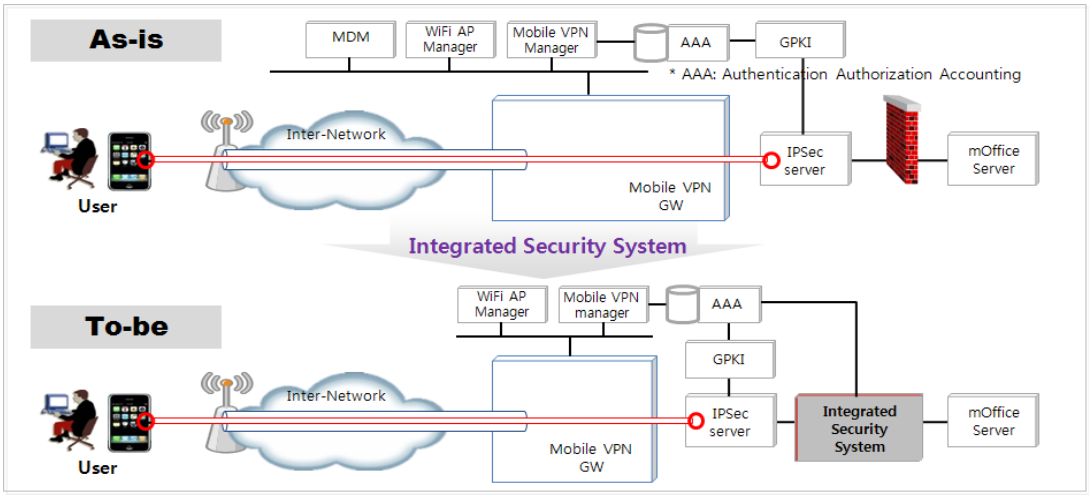

Figure 7. Suggested Integrated Security System

3.2. Key Requirements of Integrated Security System

Conventional security systems are operated mostly to prevent the intrusion of malicious codes and virus using the firewall, IDS, and IPS subsystems. As shown by the "3.20 IT Crisis," which occurred on March 20, 2013, and caused the shutdown of networks of major press and enterprises and infection of many computers by malicious codes in Korea, however, it can neither block the attacks unless they are known malware nor quarantine the network and prevent the proliferation of damage since the network cannot be operated normally once saturated. Tracking the cause is also difficult.

Moreover, since most applications communicate through dynamic ports/IP addresses, the existing security system that performs control using the port and IP address cannot handle hacking and APT attacks.

As such, the real-time, network packet deep inspection-based, integrated security system requires more precise, real-time management of traffic and control of all applications and users beyond simple control using the port and IP address of the network packet.

The real-time, network packet deep inspection-based, integrated security system must inspect all network packets and their payloads without delay and in realtime and analyze and subsequently process the signature-based services quickly. It must also manage the traffic of all application program sessions passing through the system and save the traffic logs. The main functions of an integrated system are listed in Table 1.

Table 1. Main Functions of the Integrated Security System

Requirement	Scope
Storage/Integrated Analysis	APP-ID, UserID, etc.
App Detection	Signature-based detection
Integrated Authentication	Transmitted/Received packets and contents
Access Control	Network and contents control
Log Management	Event and log collection and utilization
Policy Control	User/Access policy
Monitoring	Real-time event

3.3. Applications of Integrated Security System

The real-time, network packet deep inspection-based, integrated security system can be applied in various areas in addition to security system function, personal information protection, and security control. It can manage network traffic, and it can be utilized in system tracking tasks such as packet-based billing solution and network load measurement and management by analyzing the log (Figure 8).

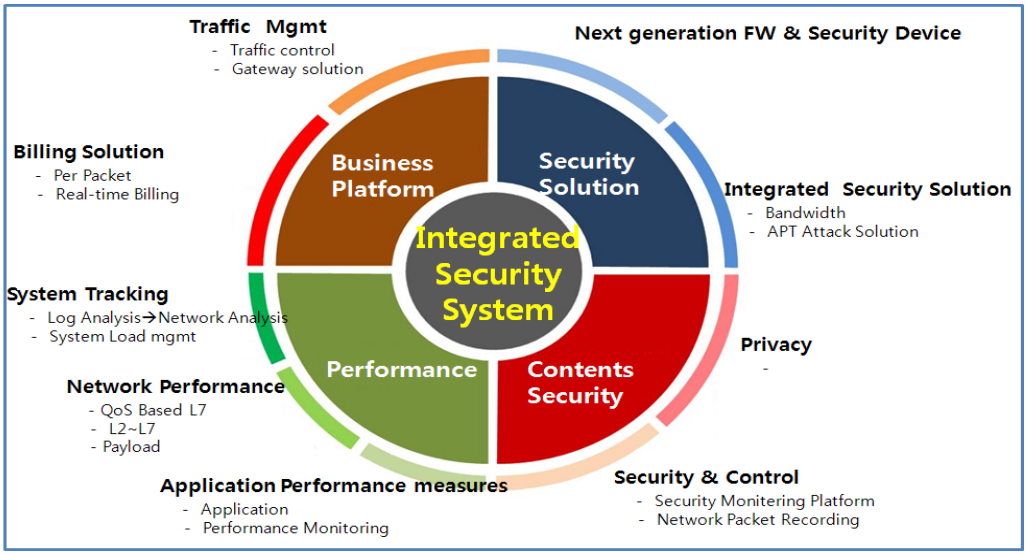

Figure 8. Various Areas Where the Integrated Security System can be Utilized

4. Operational Cases and Performance Evaluation

To evaluate objectively the performance of the integrated security system, the instrument conforming to the network performance test standard RFC2544(Methodology for Network Interconnect Devices) and SmartFlow software were used.

Figure 9. Integrated Security System Operation Screen (example)

For the performance evaluation, the throughput, latency, number of flows simultaneously processed, and new flows per second were measured. A separate tool was used to obtain the detailed status data (actual cache access rate and error generation frequency) of the kernel and processor.

Table 2. Result of Integrated Security System Evaluation

Tested Item	Test Result
RFC 2544Test	128 Byte: 99.7% 256 Byte: 99.4% 512 Byte: 99.3% 1024 Byte: 99.4% 1280 Byte: 99.2% 1518 Byte: 99.1%
Service Recognition Test	Service recognition rate of actual traffic: Around 87%
No. of Flows Processed Simultaneously	30 million flows
New Flows per Second	1.5 million flows/sec.
Latency	FPGA processing: 3 μs Host processing: 160 ~ 180 μs

The performance evaluation indicates that the system can process at least 99% without delay using the existing network equipment. Neither were there performance degradation ordelay, new flows/sec., *etc.*, in the high-volume network environment.

5. Conclusions

This paper uses an example to confirm that the network packet deep inspection-based, integrated security system, which can effectively cope with various security threats by identifying and authenticating 7 layers of Internet traffic, can be applied without overloading the network traffic. As indicated by the recent security issues and intrusion cases, APT attacks and worm and hacking must be dealt with continuously.

The real-time, network packet deep inspection-based, integrated security system proposed in this paper can be used as an effective security measure based on the policy of the enterprise operating the information system and understanding of the administrator. It can also be regarded as the optimum solution to cope with unknown network-based threats in the future.

For future studies, intelligent security analysis using big data -- in addition to network packet storage, management, and restoration -- is recommended.

References

[1] M. Nicolett and K. M. Kavanagh, "Magic Quadrant for Security Information and Event Management," Gartner Group, **(2012)** May.
[2] Allot Communications (2007). "Digging Deeper Into Deep Packet Inspection(DPI)." H. Asghari, M. van Eeten and M. Mueller, "Unraveling the Economic and Political Drivers of Deep Packet Inspection", GigaNet 7th Annual Symposium, **(2012)** Novmber 5.
[3] BEREC, "BEREC response to EC questionnaire on specific aspects of transparency, traffic management and switching in an Open Internet", **(2012)**.
[4] BoR(12)145 rev.1. 2012. 12. 19. Broadband Traffic Management (2013. 2. 14). "[Transparency Market Research]: DPI Market to Reach $3.8B by 2018".
[5] R. Bendrath, "Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection", International Studies Annual Convention, New York City, **(2009)** February 15-18.
[6] C. R. Clark and D. E. Schimmel, "Scalable pattern matching for high speed networks", Field-Programmable Custom Computing Machines, 2004. FCCM 2004. 12th Annual IEEE Symposium on, **(2004)**.
[7] A. Cooper and E. Llans, "Adoption of Traffic Sniffing Standard Fans WCIT Flames", Center for Democracy & Technology, **(2012)** November 28.
[8] A. Cooper, "Doing the DPI Dance", **(2011)** April 11.
[9] A. Cooper, "The Singular Challenges of ISP Use of Deep Packet Inspection", Deep Packet Insepction.ca, **(2010)**.
[10] C. Parsons, "DPI in perspective: tracing its lineage and surveillance potential." the new transparency surveillance and social sorting. Working paper, **(2008)**.
[11] Telecompaper, "Opta rejects request for info on DPI investigation." http://www.telecompaper.com/news/opta-rejects-request-for-info-ondpi-investigation--823541, **(2011)** August 29.

Authors

Chang-Su Moon, received B.S. degrees degrees in Electronic Engineering from the Dongkook University, Seoul, Korea, in 1982 and M.S. degree from the Soonchunhyang University in 2013.

March 2013- the present: Department of Information and Communication Engineering, Soonchunhyang University, Ph.D

From 2012 to the Present, he was a chairman of Information and Communication Financial Cooperative

His research interests include Network, CCTVandInformation and Communication Corporation Act.

Sun-Hyung Kim, received his B.S., M.S. and Ph.D. degrees in Electronic Engineering from Sungkyunkwan University, Korea, in 1979, 1981 and 1988, respectively. Since 1989, He has been a professor in Department of Information and Communication Engineering, Soonchunhyang University.

From 2005 to the Present, he was a vice-chairman of Korea University Invention Association. From 2013 to the Present, he was a vice-chairman of Korea Institute of Information Technology.

His research interests include Data Communication, Embedded system, Network, etc.

