DoS Attack Analysis for H-HIPS

Tomoaki SATO,
C&C Systems Center, Hirosaki University
Hirosaki 036-8561 Japan

Kazuhira KIKUCHI, Shuya IMARUOKA, and Masa-aki FUKASE
Graduate School of Science and Technology, Hirosaki University
Hirosaki 036-8561 Japan

ABSTRACT

H-HIPS (Hardware-based and Host-based Intrusion Prevention System) is an IPS that has been achieved by using FPGA (Field Programmable Gate Array). It is different from conventional IPS that has been achieved with software, and it has the advantage of detailed packet analysis processing possible and not consuming CPU resource at a user side. In this paper, we describe DoS (Denial of Service) attack analysis for H-HIPS necessary to improve unauthorized detection rate and achievement of DoS attack prevent function of H-HIPS. Because a method of defending DoS attack has been limited, the development of the unit is indispensable. H-HIPS is able to defend operations of a computer from DoS attack by using futures of H-HIPS.

Keywords: IPS, IDS, Dos attack, FPGA

1. INTRODUCTION

Due to the increase of Wireless LAN-accessible area in all over the world, we enjoy Internet in airports, hotels, and coffee shops, etc. While one of most distinctive features of Wireless LAN environment is Internet access with the anonymity, which has been difficult in conventional wired LAN community, tapping damage is not negligible. It causes information leakage or illegal operation by unauthorized computer access or computer virus. For this reason, we need solution to prevent from damage by information leakage or illegal operation.

Operation of IPS (Intrusion Prevention System) or IDS (Intrusion Detection System) [1] without a problem is indispensable to prevent information leakage or illegal operation. Conventional IPS and IDS are classified into network-based and host-based depend on place where the system is set up and have following problems.

Host-based IPS (HIPS) and Host-based IDS (HIDS)

・They consume CPU power and electric power of buttery by detection processing.

・They are not able to execute a detailed analysis at the packet level that CPU load is demanded.

・They are not able to execute anomaly detection of high accuracy.

Network-based IPS (NIPS) and Network-based IDS (NIDS)

・They are not able to detect unauthorized computer access that occurs between computers in LAN.

・They are hard to process all the packet analyses with the increase of the amount of packet.

・A high performance computer is needed for them and expensive.

In addition, installation of IPS or IDS on an embedded system such as a mobile phone and a PDA is difficult. A CPU of the embedded system operates more low-speed than PC and ultra low-power consumption. And an old or low-speed PC has a similar problem.

To solve these problems, we have developed and H-HIPS (Hardware-based HIPS) and H-HIDS (Hardware-based HIDS) [2]. H-HIPS furnishing the function of both NIPS and HIPS is logic-based HIPS achieved by FPGA (Field programmable gate array). This is reconfigurable hardware. Basic algorithms of conventional HIPS have been made use of to the Netlist of FPGA. In designing H-HIPS, we aim to achieve more advantageous features with less power than conventional HIPS.

In this paper, we describe DoS (Denial of Service) attack analysis for H-HIPS necessary to improve unauthorized detection rate and achievement of DoS attack prevent function of H-HIPS. Because a method of defending DoS attack has been limited, the development of the unit is indispensable. H-HIPS is able to defend operations of a computer from DoS attack by using futures of H-HIPS.

2. H-HIPS

In order to avoid unlawful computer accesses, an IDS [1] has been used in wired LAN. And it that applies the function to defend is an IPS (Intrusion Protection System). The IDS is categorized into network-based IDS (NIDS) and host-based IDS (HIDS). NIDS installed to dedicated network computers at companies and universities makes the real-time analysis of flowing packets and detects unauthorized computer access. The drawback of these processes is that they take long delay to treat large packets. This is hard to solve even if cutting edge high-performance network computers are used for the network-based IDS. Thus, it is not almighty for unlawful computer accesses. Unfortunately, unauthorized computer access once exceeded the network-based IDS invades computers in LAN. The access acts violently among computers within those networks. At present NIDS for WLAN has been announced only by IBM in November 2003. This has a problem similar to conventional IDS [3].

HIDS to be installed in individual host computers for personal uses is really promising for the protection of each of them. However, HIDS so far developed is software that works statically in checking falsified files, information set on operating systems, and process information. Thus, conventional HIDS lacks real-time response and has poor ability to analyze packet. To solve such issues, we have proposed H-HIDS (Hardware-based HIDS).

H-HIDS furnishing the function of both NIDS and HIDS is logic-based HIDS achieved by FPGA (Field programmable gate array) and can easily achieve the IPS function. This is reconfigurable hardware. Basic algorithms of conventional HIDS have been made use of to the Netlist of FPGA. In designing H-HIDS, we aim to achieve more advantageous features with less power than conventional HIDS. Intrusion detection processing on logic requires cipher such as WEP and CRC (Cyclic Redundancy Check) at high-speed with less-power consumption. Power consumption is one of most important properties for a mobile computer and PDA (Personal Digital Assistance) driven by a battery. The analysis of a detailed packet level is crucial for fulfilling these requirements.

2.1Security Problems of Wireless LAN

An IDS is a system for detecting intrusion. Especially, the introduction of the IDS is indispensable for Wireless LAN. It includes monitoring security violation, detection, and management of detected information by computers on computer networks, and is classified into network-based and host-based depending on place where the system is set up.

Basically, network-based IDS works for intrusion detection. The shortage of network-based IDS has been supplemented by host-based IDS. Host-based IDS monitors intrusion statically by falsified files and set information and processes on operating system. Table 1 summarizes principal features of both types IDS.

Judging from Table 1, important research topics of IDS are

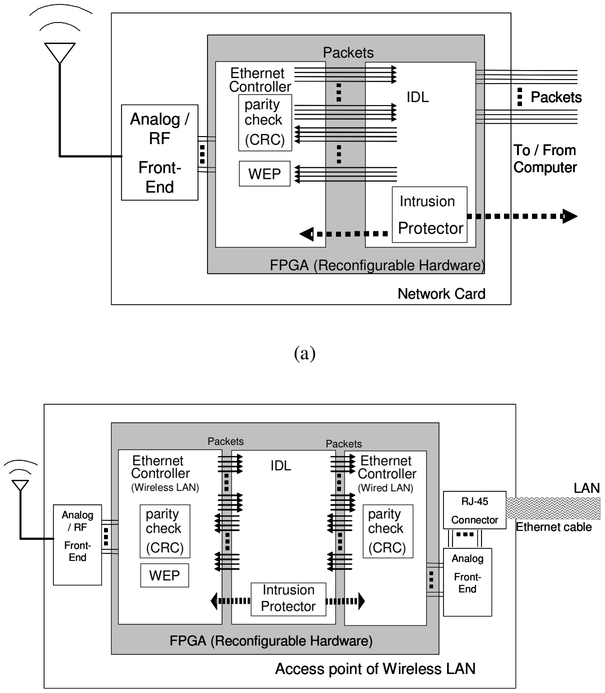
- Improvement of the detection rate of intrusion detection
- Development of effective detection method to prevent mal-function in normal access.

In case of host-based IDS, a multivariate analysis was studied [4]. A tradeoff of detection technique is accuracy and CPU load.

Network-based IDS is practically limited by the performance of processing computer. Thus, it is hard to process all the packet analyses with the increase of the amount of packet. In [5], a detection technique by the traffic pattern was described. However, it is necessary to analyze all packets in detail to do more accurate detection.

Table 1: *Features of conventional host-based and network-based IDS / IPS*

IDS / IPS	**Real-time intrusion Detection**	**Intrusion detection in LAN**	**Detailed analysis processing of packet level**	**All the packet processing in a Gigabit network**	**CPU resource at users side**
Network-based	Possible	Impossible	Possible	Impossible	No consumption
Host-Based	Impossible	Possible	Impossible	Impossible	Consumption



(a)

(b)

Fig. 1: H-HIPS hardware structure.

(a) NIC. (b) AP.

2.2 Intrusion Detection Logic

The H-HIDS that we propose in Fig. 1 is composed of NIC (Network Interface Card) and AP (Access Point) as well as conventional Wireless LAN System. Fig. 1(a) shows the basic organization of our proposed NIC of Wireless LAN. The new host-based IDL of NIC that plays in part the function of network-base IDS should process the packet analysis more than three layers of OSI (Open Systems Interconnection) layer model.

After manufacturing custom design VLSI processor cannot change hardware, it cannot add a limitation to a specific protocol and a new function. Therefore, it cannot be used for IDL. Then, the hardware processing that is only software becomes possible by using FPGA as for IDS. The TCP/IP Flow Monitor circuit [6] was achieved with FPGA for such reasons.

Fig. 1(b) shows the basic organization of our pro-posed AP of Wireless LAN. The IDL of AP has network-base IDS function as well as the IDL of NIC. And it sup-plements IDL functions of NIC.

The host-based IDL is really useful for packet analysis and port monitoring. Port monitoring so far supported by OS watches port access whose number is used for speci-fying network applications such as mail, web, and DNS according to TCP/IP and UDP/IP. Then, the function of port monitoring gives response for network applications that makes the user-specified ports active and the other ports inactive. Since the built-in hardware IDS gives im-mediate response, it is also helpful for host computers to forbid unauthorized access. Besides, the monitoring func-tion is effective for Denial of Service (DoS) attack that sends a burst of packets such as Smurf and SYN FLOOD to computers.

Table 2 summarizes the features of conventional software IDS and IDL proposed by us. The IDL solves the problem of software IDS. In

Table 2: *Software IDS / IPS vs.IDL*

Item	**Software**		**Logic**
	Host-based IDS / IPS	***Network-Based IDS / IPS***	***Host-based IDL***
Installation place	Computer on user side	Network node	Computer on user side
Input data	File and action in computer	Packet in network	Packet which inputs and outputs computer
Costs	Software	Exclusive use and High performance computer, Software	FPGA Chip Netlist
Detection time	Unreal-time	Real-time	Real-time
CPU load on user side	Yes	No	No
Processing capacity	Non-correspondence of high-load processing	Limit by amount of packet	High ability
Detect of internal attack	Possible	Impossible	Possible
Problem of a protection function	CPU resource consumption	Difficult setting	None

addition, it is cost-effective. The cost of FPGA chip is 22 US dollars or less in the scale of 250,000 unit volumes [7]. Thus, the IDL can be introduced in an individual environment such as a Wireless LAN. Moreover, it can cover a large-scale net-work because the packet analysis function of conven-tional network-based IDS is distributed by each host.

3. DOS ATTACK ANALYSIS UNIT

DoS attack send a large amount of packets to a computer, and it gives the computer an over load. As a result, the computer loses functions. The use of anti-virus software is one of the solutions for protecting DoS attack. However, the protection of using software consumes CPU and memory resource.

To solve this problem, we propose to build H-HIPS into Dos Attack Analysis Unit. The unit is composed of FPGA as well as other analyses and protecting units. We develop the unit by using the development environment shown in Table 3.

Table 3: *Development Environment*

Platform	Microsoft Windows 2000
CPU	Intel Pentium III (1GHz)
Main Memory	512 MBytes
CAD	Altera Quartus II
FPGA	Altera Cyclone EP1C20F400C7

To protect Dos attack, the unit needs a sender IP address and the number of packets. Because Dos attack gives a load to a computer by a great deal of packets of short time, Dos attack is judged by the number of packets each unit time. The flow chart of Dos Attack Analysis Unit is shown in Fig, 2 and the hardware structure is shown in Fig. 3.

We simulate circuits of Fig. 3 at the gate level. Results of Stored Unit is shown in Fig.4 and Results of Detecting Unit is shown Fig. 5. According to results, 56.8 MHz operation is confirmed. Because word size of Circuits of Dos Attack Analysis Unit is 48 bits, the unit can correspond to 2.6Gbps.

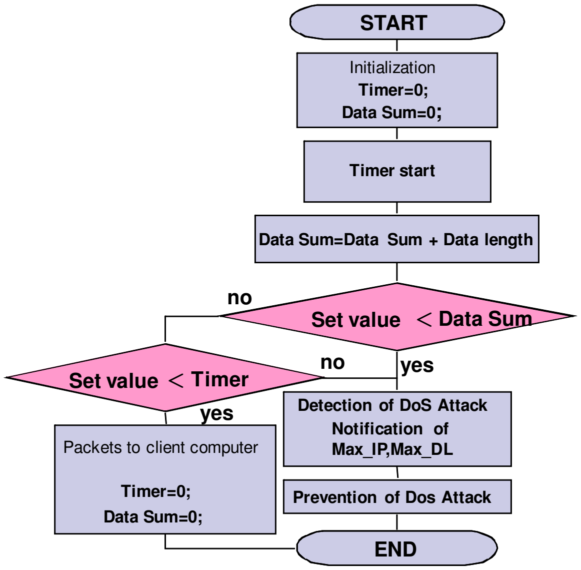


Fig. 2:*Flow chart of Dos Attack Analysis Unite.*

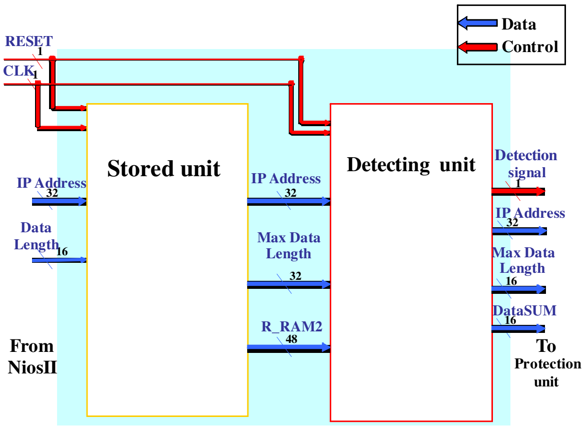


Fig. 3:*Hardware structure of Dos Attack Analysis Unit.*

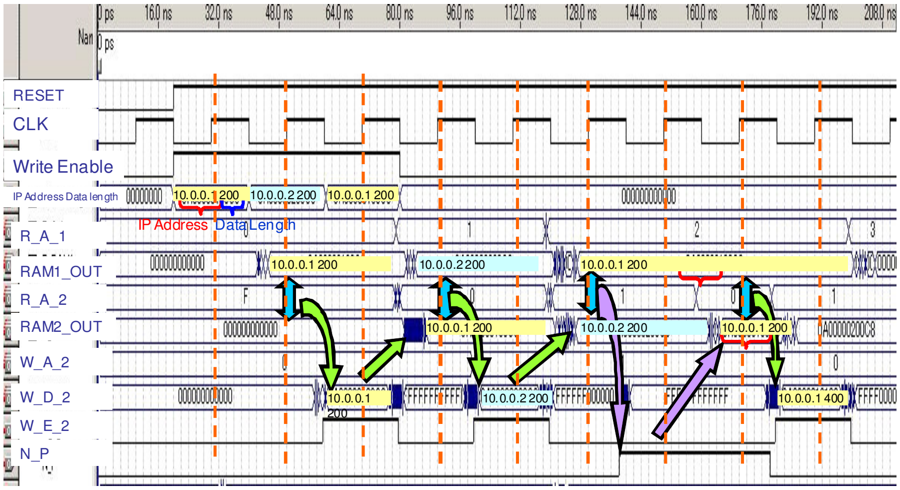


Fig. 4:Simulation results of Stored Unit.

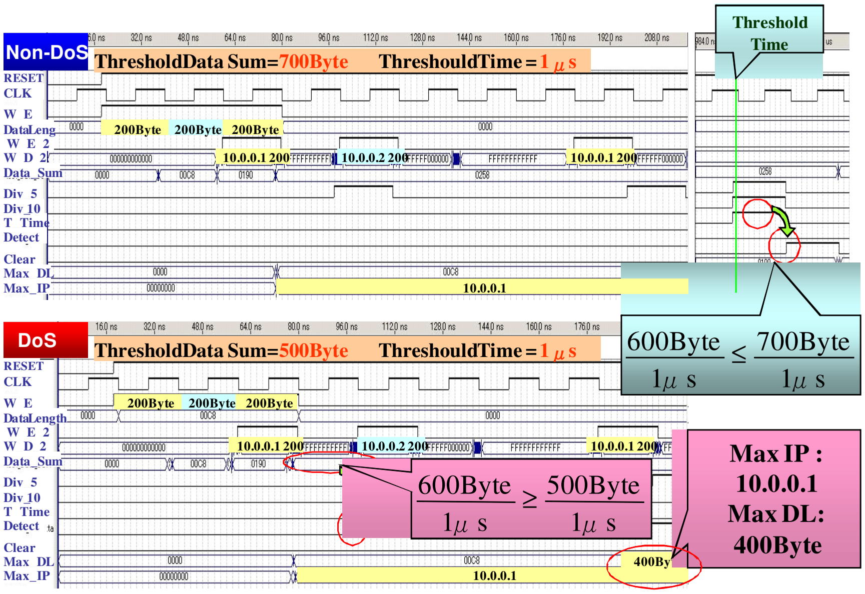


Fig. 5:Simulation results of Detecting Unit.

4 CONCLUDING REMARKS

In this paper, we described that H-HIPS into which Dos attack analysis unit is built is able to protect user side computer without consume its CPU power and memory. The unit is designed by using FPGA which is low-speed operation. However, according to the gate-level simulation, throughput of the unit is 2.6 GHz.

In our future works, build the unit into H-HIPS, and the whole of H-HIPS is evaluated. When H-HIPS is used in a mobile computing, low-power consumption is indispensable. Processing speed that exceeds a gigabit Ethernet is reconstructed to making to low power consumption.

REFERENCES

[1] Keiji TAKEDA and Hiroshi Isozaki, “Network Intrusion Detection,” Soft Bank Pub., 2002.

[2] T. Sato, R. Sakuma, D. Miyamori, and M. Fukase, “Hardware Security-Embedded Wireless LAN Processor,” Proc. of ECTI-CON 2006, Vol. II, pp 839-842, 2006.

[3] Tomoaki Sato and Masa-aki Fukase, “Reconfigurable Hardware Implementation of Host-Based IDS,” Proc. of the 9th Asia-Pacific Conference on Communication, Vol. 2, pp. 849-853, 2003.

[4] Midori ASAKA, Takefumi ONABUTA, Tadashi INOUE, Shunji OKAZAWA, and Shigeki GOTO, “Remote Attack Detection Method in IDA: MLSI-Based Intrusion Detection with Discriminant Analysis,” Trans. of IEICE, Vol. J85-B, No.1, pp. 60-74, 2002.

[5] Yohsuke TAKEI, Kohei OHTA, Nei KATO, and Yoshiaki NEMOTO, “Detecting and Tracing Illegal Access by using Traffic Pattern Matching Technique,” Trans. of IEICE, Vol. J84-B, No. 8, pp.1464-1473, 2001.

[6] David V. Schuehler and John W. Lockwood, “TCP Splitter: A TCP/IP Flow Monitor in Reconfigurable Hardware,” IEEE Micro, Vol. 23, No. 1, pp. 54-59, 2003.

[7] Lower Cost Drives New FPGAs, http://www.eeproductcenter.com/printableArticle.jhtml?printable=true&articleID=22103038, 2005.

[8] “Power consumption of CF type LAN card and appearances for SL-C700,” http://www.areanine.gr.jp/~nyano/lanlst.html, 2007.

[9] Tomoaki Sato, Kazuhira Kikuchi and Masa-aki Fukase, "Verifying Various Generation of Random Number Sequence on Wave-Pipelined PRNG," Proc. of ECTI-CON 2007, Vol. 1, pp. 21-24, 2007.