International Journal of Multimedia and Ubiquitous Engineering
Vol. 1, No. 3, September, 2006

Development of an Attack Packet Generator Using a NP(Network Processor) for Tests of Security System

Seungjae Seong, Wooyoung Soh and Wankyung Kim
Department of Computer Engineering, Hannam University
e-mail: ganda@nate.com,
{wsoh, wankk12}@hannam.ac.kr

Abstract Security systems need be tested on the network, when they are developed, for their security test and performance evaluation. It is desired that the security test being done on the real network environment. However, it is usually tested in a virtual test environment (a closed network environment), due to the possible serious damages occurred during the test, possibly propagated through the network. It is specially the case when the real network environment is too sensitive or important to allow any corruption of network or system during the test, or when building a real-like test environment is too expensive. This paper presents a network attack packet generator, a system that generates high speed network attack packets to closely assimilate the real network for security system tests using a NP(a network processor equipped with an Intel chip).

Keyword: Packet generator, NP

1. Introduction

During the recent years, the information systems through the computer networks have been widely used due to the rapidly increased demand on the Internet applications. Most of the systems have been faced with the security problems related to their vulnerability such as egress of information and illegal access, which results in the development of various security systems (e.g. firewall, IDS, etc.) to counter such security attacks. Security systems are in general operating on a network involving a number of connected information systems. Therefore, such security systems need to be tested on the network, when they are developed, for their security test and performance evaluation. It is desired that the security test is done on the real network environment. However, it is usually tested in a closed network environment, due to the serious damages possibly occurred during the test and possibly propagated through the network. It is specially the case when the real network environment is too sensitive or important to allow any corruption of network or system during the test or when building a real-like test environment is too expensive. When the virtual test network is used, the problem is how to simulate the real network with various factors such as network speed, packet processing cpacity, network load and etc. It is, for instance, very difficult to have enough packet amount and/or packet speed to assimilate the real network environment. Therefore, for the efficient and accurate test of the security system, it is necessary to have a pertinent method of providing the test environment with a high packet speed to assimilate the real attack environment.

This paper presents a network attack packet generator, a system that generates high speed network attack packets to closely assimilate the real network for security system tests using a NP(a network processor equipped with an Intel chip). Attack packets are constructed based on the rule set of Snort[1] which is an open source intrusion detection system.

This paper is organized as follows. Section 2 describes the existing evaluation methods and the test conditions of security systems. After describing the design and implementation of the proposed network attack packet generator for security system tests in section 3, the results of performance evaluation by comparing the proposed packet generator with the existing one(Excalibur[2]) are discussed in section 4. Finally section 5 describes the conclusion and the future works.

2. A mechanism of performance measure for information security system

To develop and select a proper security system, it is necessary to have a proper evaluation method. Among other things, the security test and the performance test are the ones generally used[3][4][5][6]. The security test is a test to observe vulnerabilities of a target system equipped with a security system using a vulnerability analysis tool and a well-known test is the 'penetration test' of CC(Common Criteria)[7][8]. The performance test of information security system is a test which measures general traffic and throughput on the stress factors for information security system.

This chapter discusses the performance test and the test-bed in NSS[9] to derive the factors for the performance test and the configuration of test-bed for the proposed attack packet generator.

2.1 Factors of performance test for security systems

Common factors of performance test for security systems can be summarized as follows from NSS [9]:
Limitation of authorized traffic for reliability Detection rate of defined intrusions Impact on network performance during process of received packets

2.2 Test environment for security systems

The performance test environment for security systems can be divided into two categories: traffic environment or non-traffic environment, although it varies according to the test target. Traffic environment is configured as a real-network environment or a like. In case of testing on a real network environment, it is possible to test including the compatibility with OS. However, there can be a deviation of network traffic in accordance with when and how long the test is done, and further no guarantee that the

necessary attacks happen during the test. Besides, if any security system without verification is installed on a real-network environment, it can be risky. On the other hand, a test on a network environment similarly configured to the real one can exclude the risk, but it bears the size and cost problem of network.

Non-traffic environment is a environment such that the packets including attacks are generated then the test is done with them using switch hub to target system. In this case, there is no risk from installing any non-verified security system and no cost of configuring a real-like network environment. However, it is difficult to test any stress factors as well as non-attack packets, because only the attack packets are used.

The traffic and non-traffic environments have its own merits and demerits. From the above discussion, the requirements of a test environment for security systems can be derived as follows:

- Can construct not only a single attack, but a complex set of attack
- Can construct non-attack packets as well as attack packets
- Can generate real-like traffic environment
- Can generate traffic over the processing ability of a target security system

Should not be affected by the performance of the hardware installed with packet generator

The above 5 requirements can be summarized into 2 categories: capability of constructing complicated attack scenario, and capability of generating packets assimilating real network environment.

This paper intends to develop a network attack packet generator using a NP that can satisfy the above requirements and also provide a real network traffic capability and a real-like test environment for the security system test and development.

3. Design and implementation of the proposed attack packet generator

The proposed packet generator consists of two parts: Host part and NP Part. Host part mainly does the function of constructing the necessary packets, while NP Part mainly does the function of transmitting the constructed packets.

In this paper, the proposed attack packet generator is designed and implemented such that the functions and performances can be accomplished according to the following conditions.

An attack packet generator should be able to minimize the time of constructing and transmitting packets

An attack packet generator should be able to transmit the correct packets of information to the tested system.

The above two conditions are set to meet the requirements derived from the objectives of the real network environment for testing the security systems.

3.1 Host Part

Host Part includes the user interface that serves the ease of constructing necessary attack packets, and also the DB of attack packet information derived by parsing the Snort rule set.

The host part uses RedHat 7.2, Kernel ver. 2.4.17 and PCI Bus for communication between Host Part and NP Part[10].

Host Part is consisted of 4 modules: snort rule parsing module, packet information DB management module, packet information selection module and packet construction module. It provides the ease of managing DB and also the update function of rules with additional information through web GUI.

3.2 NP Part

NP Part is in fact a separate NP based system board and working with Host Part. In other words, NP Part receives the packets from Host Part through the PCI Bus and then transmits them after coping and scheduling. In this paper ENP-2506 by Radisys is used as NP. ENP-2506 uses Intel IXP1200 Network Processor, and supports two multi-optic ethernet port[11]. IXP1200 consists of Storng Arm Core Processor, six Micro Engines, SDRAM, SRAM, PCI BUS and IX BUS[12].

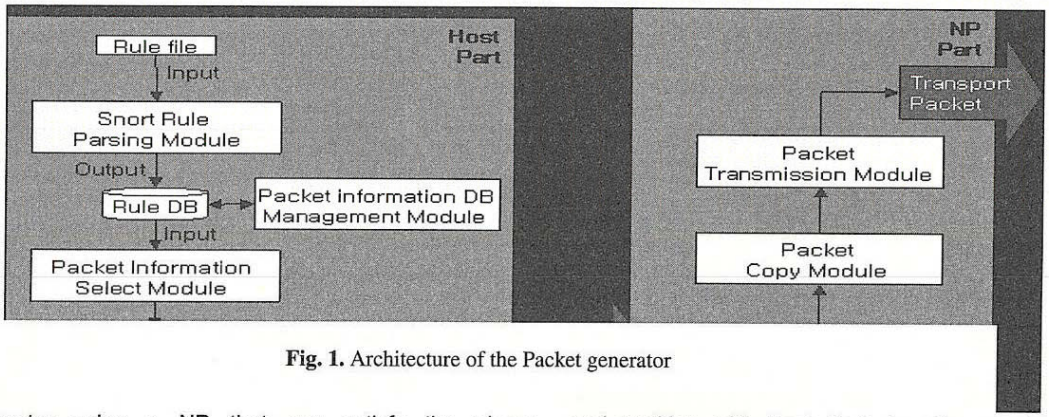


Fig. 1. Architecture of the Packet generator

NP Part can be equipped with a separate OS, and in this paper Embedded Linux Kernel Ver. 2.3.99 is used. NP Part consists of Micro Engine, scheduling module, packet copy module and packet transmit module. It communicates with Host Part through Primary PCI Bus, and IXF1002 chip set communicates through Secondary PCI Bus to provide an external interface between IXP 1200 and a target system.

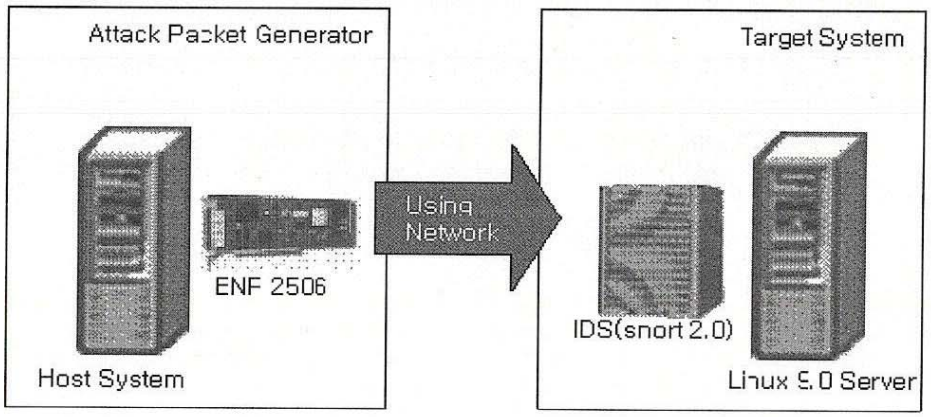


Fig. 2. Test Environment

3.3 Construction and management of packet information DB

The packet information DB is constructed with data gathered by parsing snort rule set. DB consists of a number of tables each of which has the attack information according to the attack type, and a key table which indices the corresponding attack information. The whole packet information is managed through web GUI.

3.4 Packet Construction

Through the key table, users extract the necessary information from DB and construct the desired packet. In other words, users input the transmit and destination IP addresses, and selects a desired attack type and an amount
of packets. Then Packet construction module constructs the necessary packets, then pushes the packets, the amount of packets, and the IP address information into the copy buffer of NP Part.

3.5 Copy and transmission of Packets

Once the packets are pushed into the copy buffer, Micro Engine of NP Part executes Packet Copy Module which copies the packets by putting the IP address information to the packet header and pushes the results into the transmission buffer. Then Packet Transmission Module actually transmits the packets to the target system.

4. Performance of the proposed attack packet generator

To evaluate the performance of the proposed attack pack generator, the two requirements discussed in the previous chapter are evaluated.

Network attacks are generally consisted with more than two complicated attacks and/or sequential attack steps. Furthermore in a real network environment, there exist a great number of background data which may be attack related packets or normal packets to the target system. Therefore, a attack packet generator should be able to generate attack scenario including background data.

The proposed attack packet generator constructs attack packets based on the Snort rule set. Snort has a self-defined rule set of intrusion detection and it contains a various attack packet information as a comparing factor with received packets. Therefore the proposed attack packet generator can generate various patterns of attack including complicated attack scenario.

Table 1. Hardware Specification

Hardware Specification	
CPU	P4-2.6Ghz
RAM	512Mbyte
HDD	120Gbyte
O.S	RedHat Linux 7.1

An open source packet generator, Packet Excalibur [2], has been used for performance evaluation of security systems. It basically reproduces a pre-dumped packets for a predefined time period from a target network area to the tested system. The proposed attack packet generator is compare to evaluate the performance. The hardware specification of the proposed generator and the Packet Excalibur is listed in Table 1.

Packet Excalibur is a script-based network packet generator. It generates packets including background data according to the pre-defined script. For comparison of the two generators were compared by generating 1 GByte of packets including DoS attack packets and background data. The time required generating and transmitting and other factors are listed in Table 2.

The proposed attack packet generator was at least 40% faster than Packet Excalibur in generation and transmission of packets with the different amount of packets. The packets generated by the two were detected by Snort more than 95%, which means they generated packets and transmitted them at the reasonably acceptable rate.

Table 2. Comparison of the proposed generator and Packet Excalibur

	Packet Construction And Transmit time	Scenario(script)		
		Method of Compose	Construction of An Attack Packet	Back - ground Data
Packet Excalibur	4min 40sec	User Inputs OSI 7 Layers	Using Tcpdump data	Using Tcpdump data
Attack Packet generator	2min 50sec	User Selects DB	Using packet Information DB	Using packet Information DB

Chapter 2 derived 5 requirements of a test environment for security systems which can be concluded as follows for the proposed generator with the previous performance evaluation: first, it can generate not only a simple attack packet, but also a complicated attack scenario; second, it can generate background data as well as attack packets; third, it can generate a real-like network traffic; it can generate more than 1GB of traffic; fourth, it can generate a network traffic over the packet processing capability of the current security systems in general; fifth, it is not affected by the performance of the hardware installed with the proposed packet generator due to the use of an NP.

5. Conclusion

The primary purpose of this study is to develop a way of providing a test environment for security systems with several desired characteristics including the ease of assimilating a distributed attack scenario in a single system and the high transmission rate of attack packets in a given short time period with a reasonable packet loss.

The proposed attack packet generator can generate not only attack packets but also background data, thus it can assimilate real network traffic. The proposed generator can minimize the effect of hardware environment, since it uses a NP. It means that with this generator one can configure a real-like network environment in a single Linux system. Thus one can reduce the cost and time of configuring a virtual network environment for testing security systems.

As the result of comparing the performance, processing time of the proposed generator is faster than software based packet generator, Packet Excalibur.

It is expected that the proposed system helps provide a way of developing an efficient test environment closely assimilating a real network environment for the precise test of security systems.

The proposed attack packet generator will be further improved to provide a ease of constructing complicated attack scenario. It is also considered to improve its performance by using the upgraded version of network processor such as IXP2400 and IXP2800 and by optimizing the packet copy and transmit modules in near future. One may also consider developing an evaluation method of security systems with this approach.

References

[1] Martin Roesch, Chris Green, SourceFire,INC., "Snort Users Manual", http://www.snort.org

[2] http://www.securitybugware.org/excalibur/

[3] Nicholas J. Puketza, Kui Zhang, Mandy Chung, BisWansth Mukherjee and Ronald A.Olsson, "A Methodology for Testing Intrusion Detection Systems", IEEE Transactions on Software Engineering, Vol.22, No.10, pp.719 ~ 729, October 1996.

[4] H.Debar, M.Dacier, A.Wespi and S.Lampart, "An Experimentation Workbench for Intrusion Detection Systems", IBM Zurich Lab, Research Report, March 1998.

[5] Richard P. Lippmann, David J. Fried, Isaac Graf, Joshua W. Haines, Kristopher R. Kendall, David McClung, Dan Weber, Seth E. Webster, Dan Wyschogrod, Robert K. Cunningham, and Marc A. Zissman, "Evaluation Intrusion Detection Systems : the 1998 DARPA Off-Line Intrusion Detection Evaluation", Proceedings of the 2000 DARPA Information Survivability Conference and Exposition, 2000.

[6] Robert durst, Terrence champion, Brian written, Eric miller, and Luigi spagnuolo, "Testing and Evaluating Computer Intrusion Detection Systems", Communication of the ACM, Vol.42, No.7, pp.53 ~ 61, July 1999.

[7] CCRA(Arrangement on the Recognition of Common Criteria, **http://www.commoncriteria.org**

[8] CC, "Common Criteria for Information Technology Security Evaluation", Version 2.1, CCIMB-99-031, August 1999.

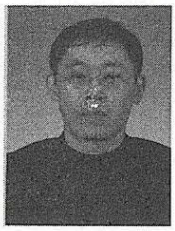
[9] An NSS Group Report V 1.0, "Intrusion Prevention Systems(IPS)", Group Test, NSS, Jan 2004.

[10]RadiSys Corporation, "Linux Setup guide for ENP-XXXX", **http://www.radisys.com**

[11]RadiSys Corporation, "ENP-2506 Hardware Reference Manual", **http://www.radisys.com**

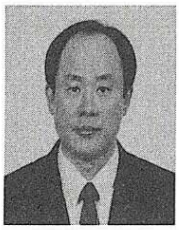
[12]Intel Corporation, "IXP1200 Hardware Reference Manual", http://www.intel.com

Authors



Seungjae Seong

Received a B.S. degree in Computer Engineering from Hannam University 2003, and M.S. degree in Computer Engineering from Hannam University 2005.
Successived CTO at Secuve Corp. in 2001, 3 until 2004, 6 and at Clunix Corp. in 2004, 7 until 2006, 3



Wooyoung Soh

Received a B.S. degree in Computer Science from Jung-Ang University 1979, and M.S. degree in Computer Science from Seoul National University 1981 and Ph D. degree in Computer Science from Maryland University 1991.
In 1991 he joined the faculty of Hannam University where he is currently a professor in Department of Computer & Multimedia Engineering. His research interests include Nueral Networks, Information Security, and Computer Networking. He is a Member of KIPS, KIISC, KMMS, KIAS, and DCS.

Wankyung Kim

Received a B.S. degree in Computer Engineering from Hannam University 2003, and M.S. degree in Computer Engineering from Hannam University 2005.