Study on Intrusion IPv6 Detection System on LINUX

Zhang Yu
College of Computer and Information Engineering
Harbin University of Commerce
Harbin, China
Zh y@hrbcu.edu.cn

***Abstract*—With the rapid development of information society, intrusion has been increasing gradually, initiating a series of security problems. Traditional firewall only guards against external attacks, and can not prevent internal intrusions. Intrusion detection system can supplement the firewall insufficiency and has become one of the critical techniques in information security assurance. This paper mainly researches LINUX-based IPv6 intrusion detection system. Firstly, it introduces the concept, models and classification of intrusion detection system, models; secondly, it discusses new intrusion detection techniques based on IPv6; finally, it researches the methods of using LINUX to detect various kinds of intrusion under coexisting network environments of IPv4 and IPv6.**

***Index Terms*—intrusion detection,IPv6, feature library**

I. INTRODUCTION

Although firewalls can solve a part of security problems, it only prevents external attacks, and can not guard against internal intrusions. Also, firewall is easy to be bypassed. So the computer system only relying on firewall has been able to deal with rampant intrusion behaviors, so intrusion detection system as the second defense line dealing with intrusions has been playing a more and more important role.

Information system security assurance is a defense system, which includes 4 levels such as protection, detection, reaction and recovery. Intrusion detection system is an important part and plays the role of EWR aircraft 'in digital space.

We know that IPv6 as a new generation of IP is coming into the people's vision. Introduction of new protocol will not only have positive effects on network security, but also bring new problems. In September 2004, Larry J. Blunk had made a report titled as Global Infrastructure Security and IPv6 Implications at Fall 2004 Internet Member Meeting, in which he proposed that application security of IPv6 would be a key to global fundamental network security, and pointed out that the coexistence of IPv6 and IPv4 would last several years, so security problems for such coexistence should be considered [1]. With rapid development of IPv6 application technology, intrusion technology under the IPv6 environment also appears accordingly, and shows a trend of fast growth. The research of intrusion detection under the IPv6 environment has been general concerns of domestic and overseas security experts. How to prevent intrusion and ensure the normal operation of Internet under IPv6 and IPv4 coexistence environment has been an urgent issue [2]. This paper uses IPv6 environment to research intrusion detection technology under the new protocol and intrusion detection system under IPv6 environment (IPv6IDS).

II. CONCEPT, MODELS AND CLASSIFICATION OF INTRUSION DETECTION SYSTEM

Intrusion Detection System is referred to as IDS, which is a system for monitoring computer network. Its main function is to seek the features of intrusion (unauthorized users) or misusing (authorized user beyond the privilege).

A The Concept of Intrusion Detection System

Heady considered intrusion is a behavior set which attempted to destroy the integrity, confidentiality and usability of the resources. From the point of view of classification, Smaha pointed out that intrusion had six types including attempts to break in, disguised attack, security control system penetration, leakage, denial of service, malicious use. Researchers of Carnegie Mellon University defined intrusion as illegally entering information system, including the acts of violating security policy or legal protection regulations of information system [3]. Intrusion detection is to find the behaviors of violating the security strategy or endangering the system security in the system through collecting information of operating system, system programs, applications, network packets. System with intrusion detection function is called as intrusion detection system.

B Models of Intrusion Detection System

The earliest intrusion detection model is given by Denning, which generates several profiles of the system mainly according to audited record data of the host system, monitors the change difference of profiles to discover intrusion behavior of the system. Types of intrusion are increasing continuously, range of intrusion expands constantly, and many attacks are conducted through online collaboration based on long time preparation. In this case, sharing of such attack information is very important among different function components and different IDSs [4]. Therefore, someone proposes another kind of Common Intrusion Detection Framework (CIDF). This model shows that the intrusion detection system consists of event generators, event analyzers, response units and event databases. CIDF calls data that intrusion detection system needs to analyze as event, which may be data packet in the

978-1-4244-4607-0/09/$25.00 ©2009 IEEE

network or messages obtained from other ways such as system log. Event generators obtain events from the whole computing environment and provide them to other parts of the system. Event analyzers analyze the obtained data and generate analysis results. Response units have a response to analysis results, such as emergency responses including disconnecting, changing file properties, simple alarm. Event databases store intermediate and final data. The data storage form can be complex database or simple text files.

C The Classification of the Intrusion Detection System

There are many kinds of classification methods for intrusion detection system. According to difference in information sources and analysis method, intrusion detection system can be divided into three types: Host-based intrusion detection system (HIDS), Network-based intrusion detection system (NIDS) and integrated intrusion detection system[5].

For host-based intrusion detection system (HIDS), its information source is system logs of the host. It analyzes audit log of the host to find the illegal use of host and the intrusion into the host by loading the intrusion detection software on detected host. When audit log changes, intrusion detection software will compare the logs with known attack characteristics stored in the database to see whether they match each other. If they match each other, it will make alarm to system administrator or make responses appropriately. Because it uses system logs as the input data, false alarm rate of HIDS is lower. However, it needs to install software, different host engine needs to be installed for different systems and different versions, installation configuration is relatively complex, and it will affect system operation and stability. In addition, because it only covers a single host, it can not scan and detect abnormal condition of the whole network.

At present, new generation of HIDS appears to have more perfect functions. Besides monitoring log and file system, it also has the host actions including detection service, process, conversation and operation etc., thus improving the security range to a new level within a single host and making it suitable for security protection of advanced and important servers. Main advantages of HIDS include: it is very applicable to encryption and exchanging environment; it is close to real-time detection and response; it needs no additional hardware.

For network-based intrusion detection system (NIDS), its information source is information flow of network. It mainly monitors the network where NIDS host is located, and can detect intrusion in this network segment. By placing NIDS in more important network segment, it constantly monitors and analyzes all kinds of data packets transmitted in the network segment. Once the attack is detected, IDS responses module makes response to the attack by informing, alarming and disconnecting etc. The advantages of NIDS include real-time detection and response, detection of unsuccessful attack attempt, and independence of the operating system.

As mentioned above, HIDS and NIDS are complementary to a certain extent. Many organizations integrate the above two kinds of IDS for simultaneously network security solutions, namely integrated intrusion detection system. The integrated IDS can detect external internet attack by installing NIDS outside the firewall. Because many ports of the user are open to the outside, and can not be completely shielded, and DNS, Mail and Web services within the enterprise intranet may not be insulated from the outside, they often become attack target. Therefore installing HIDS in the host within the firewall is complementary, and system administrators can obtain a complete report by analyzing intrusion detection results of two systems, so they can use it to make further adjustment and improvement of future security strategy.

III. NEW INTRUSION DETECTION TECHNOLOGY UNDER IPV6

The intrusion detection based on IPv6 is proposed against IPv6 used next generation internet and possible intrusion under IPv6 environment. It is first to discuss the differences between IPv6 and IPv4.

A Differences between IPv6 and IPv4

In comparison with IPv4, IPv6 has more new features and makes great improvement based on IPv4. Here we compare them mainly in three aspects: the head format, automatic configuration, security.

IPv4 header is thirteen fields totally, its fixed length is 20 bytes, and plus options, its maximum length can reach 60 bytes. IPv6 header consists of basic header and extension header chain, totalling 8 fields, and with the length being 40 bytes. This design can add options more conveniently to achieve the purposes of improving network performance, security or adding new functions.

(1) Fixed IPv6 basic header

Basic header of IPv6 is fixed to be 40 bytes, and it makes the router accelerate processing speed of data packet, and improve transmission efficiency, thus improving the whole throughput of network and achieving faster information transmission.

(2) Simplified basic header of IPv6

In basic header of IPv6, fields including header length, mark, flag, fragment offset, header calibration, option, padding in IPv4 are deleted. Then segment offset, header, option and padding field are put in extension header of IPv6 for processing. Header checksum is deleted and mid router will not check data packet any more.

The domain related to IP fragmentation is deleted in basic header of IPv6, and then the router needs no fragmentation of data pocket. Fragmentation will be is done by terminal based on maximum transmission unit (MTU) path. Then IPv6 data packets are so far more than 64bytes, applications transmission utilizing MTU is more quickly and reliable

IPv4 length is 32 bits, which can theoretically provide about 43 billion IP addresses. IPv6 header uses 128 bits address length, and this is mainly difference between IPv6 and IPv4. Such massive addresses can meet the needs of a great number of potential customers.

Automatic configuration function is added to IPv6 proposal. After a host is registered in Internet, it can work with little modification when location or configuration changes, which

can greatly reduce configuration and address mapping management by the network administrator, and mobile users can also access the Internet easily anywhere at any time. IPv6 protocol can generate a "Local Host IP address" for any host, and this address maps an Ethernet address. Because MAC address is only one in the world, IP address will not be repeated, IPv6 automatic configuration function is based on this concept of the only address.

There are a series of security hole in IPv4; application can completes the operation only through its private ownership and authentication operation mechanism. With extensions of the data header, IPv6 can provide router level security. Compulsory security of IPv6 includes two aspects:

(1) Receiver of IPv6 data pocket may require the sender to "log on" using IP6 authentication header (data header extensions), and then receive data pocket. This logon is algorithm independent. In this way, it can be effective to prevent attacks from network hacker.

(2) For the group that must be kept confidential, closed safety data header of IPv6 (data header extensions) can be used to encrypt data pocket. The header starts with a 32-bit key number, and is followed by cryptographic load segment. This encryption is also algorithm independent, and the encryption algorithm is consultated by the sender and receiver, which means data can be transferred on the Internet safely, don't worry about the data intercepted by third-party.

B New Intrusion Detection Technology under IPv6

Combining the similarities and differences of IPv6 and IPv4, the key technology of IPv6 intrusion detection mainly centers on the following four aspects: capturing and understanding of IPv6 packet, research and implementation of IM intrusion detection system, IM packet pre-processing, extraction of intrusion features under IM environment, fast detection and matching of intrusion attacks.

IM intrusion detection technology may be defined as a process to identify and respond to malicious use of computer and network resources by the attacker using IM network protocol. Because IM protocol is incompatible with IPv4, intrusion detection under IM may face many new problems, and we also have to study a new field. Firstly, comparing with IPv4, IPv6 has made great changes in data header, so the original intrusion detection products can not be used directly in IM network, and there must be some changes. The Socket interface function for IM has been defined in RFC2133 (Basic function of Socket with Extends for IM); previous applications must be changed with reference to new API. Intrusion detection system matching process is based on IP address, TCP and UDP port numbers. IP head and TCP head are connected closely under IPv4 and its length is fixed, so the intrusion detection system can find the head easily, and use the corresponding strategies. However, positions of TCP and UDP heads under IM have changed fundamentally, they are no longer connected together, and usually have other extension heads between them, such as the router option head, AH and ESP head etc. Firewall must understand the whole packet before filtering, which can influence the intrusion detection processing performance greatly. Secondly, if using transmission mode to conduct end-to-end encryption in IM, IDS can not work because it will receive encrypted packets, which cannot be understood. Of course, one of the solutions is to let IDS decrypt these data pockets, but this will bring new safety problems. Simultaneously, whether IM can be as reliable as that was originally intended will also be tested by the time.

In general, the research target of new generation of IM network intrusion prevention technology is to create a new technology, to make intrusion prevention system adapt to network environment with high bandwidth and high load, to support the latest IM network protocol, and to be able to adapt to existing IPv4 and various transition mechanisms, thus forming a new generation of broadband network intrusion detection technology, a new generation of network security system structure model and a new generation of network security control platform.

IV. DETECTION OF VARIOUS INTRUSIONS UNDER IPV4 AND IPV6 COEXISTING NETWORK ENVIRONMENT BASED ON LINUX SYSTEM

We know that the security of Pv6 application is a focal point of global basis network security, and the coexistence of IPv6 and IPv4 could continue for several years, so the security problems under the coexisting environment should be considered. We will discuss below how to prevent intrusion in IPv4 and IPv6, coexisting environment, how to safeguard the normal operation of network and how to realize the intrusion detection system in the common environment of IPv6 and IPv4.

A System Modules Composition

The operating system development platform used by the intrusion detection system is red hat Linux9.0, which adopts feature based intrusion detection method, and supports IPv4 and IPv6 protocol. It includes eight related modules, such as feature detection, rule management, quick capturing packets, high-speed matching, network blocking, flow analysis, checking the IP and visualization etc. (figure 1).

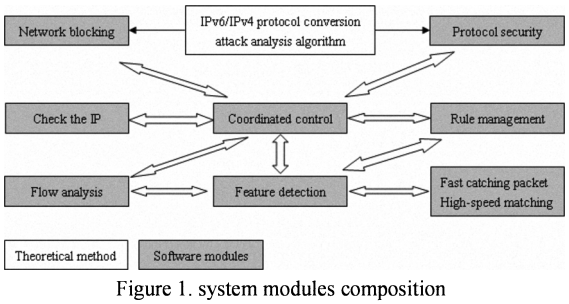

Figure 1. system modules composition

B Specific Research and Realization of Key Technology Modules

Intrusion detection system under IPv6 environment uses flexible rule language to describe data message, so it can make quick translation of network attack, organize a series of related rules to build intrusion feature rule library, conduct protocol analysis, searching content matching of messages intercepted by intrusion detection system based on this feature library, and

detect all kinds of attacks and detection. IPv6IDS has the ability of real-time alarm, and can write alarm data into MySQL database. In addition, this system has good expansion ability, it supports plug-in system, it can add new function conveniently through the interface it defines and it supports visualized management. Feature detection structure is composed of the following four primary parts: (1) the feature rule database for storage and management of intrusion characteristic rules. It is realized with MySQL in this module; (2) Rule set processing engine for analysis of pockets intercepted by the system, searching content matching in characteristics rule library, and detection of all kinds of attacks and detecting behaviors; (3) Visualized management console, which can real-time show alarm messages of intrusion attacks, conduct classification analysis of alarm information, and provide accurate intuitive monitoring message to the administrator; (4) Rule management module, which can design and modify rules, update database, and then can detects new attack behaviors.

Intrusion detection engine is the intrusion detection system based on the rule set. Through the visual processing of rules, it is easy to maintain, update, and modify the intrusion detection engine rules (figure 2). The Web-based visual console controls the whole visualization process; background management function mainly completes maintenance and management of rules, modifies, deletes and adds rule according to the results of the visualized processing, and stores the final results; visualized processing completes maintenance and processing of various rules such as checking a certain type of rules, adding, deleting and modifying a certain type of rules etc. Conduct visualized configuration of intrusion detection engine, set options and path of the used library; conduct visualized operation of rule configuration for intrusion detection engine, classify, edit, generate, delete, query the rules; controlling operation of intrusion detection engine can control the intrusion detection engine to load new rule set and restart; configure output database options.

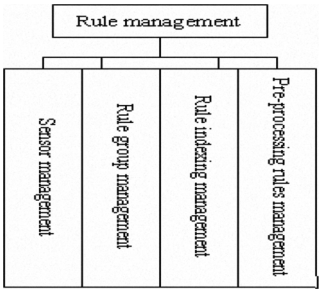

Figure 2. Function structure diagram of rules management

This module is an important part of intrusion detection system, which is used to implement active blocking of IPv6 and IPv4. According to the deployment of IDS in the network, it mainly includes series and bypass blocking modes. Series blocking mode is realized by using the IPtables and IPv6tables of Linux system, and bypass blocking mode is realized by sending a TCP connection reset packet, IPv6 network error packet, and forming neighbors to find such errors packet. When IPv6IDS intrusion detection analysis gets a great number of repeated alarms, it must timely process for these intrusions, and disconnect network connection when necessary. For network intrusion, the above several methods for intrusion are used together to block intrusions. after IPv6IDS detects the intrusion, administrator is required to classify alarm according to his knowledge and experience.

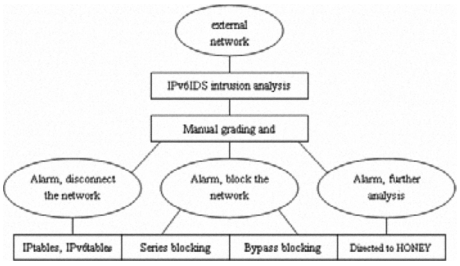

Figure 3. software system modules composition

Now intrusion detection in high-speed network faces the following problems: with the increase of network speed, a single node processing speed is saturated, causing phenomenon of packet loss. The method to solve the problems is to use extensible multi-node processing system and to improve the processing speed of a single detecting node. The primary focus of adopting distributed IDS is how to balance the flow distribution and to ensure network message flow distribution.

This module software runs high_client on the detector, and runs pre_filter on the network bridges. Specific functions are that high_client runs in every detector to notify the network bridge that the detector has run, and notify NIC address and IP address of the detector host; pre_filter network bridges module is used to repack and distribute the data packet of the host according to IP address and MAC address of the currently running detector host.

V. CONCLUSIONS

To sum up, IPv6 is a long-term solution to establish a reliable, manageable, safe and highly effective IP network. After applying new technology of IPv6, internet will become simpler, and can provide users with more efficient service quality. In addition, intrusion detection system in the above functional modules can be achieved by using C language, PHP scripts, Perl scripts, and MySQL database.

REFERENCES

[1] Research and Implementation of Linux-based IPv6 Protocol Stack in High-Performance Routers. Telecommunication Engineering, 2005 (1),pp:57-61

[2] Zhang Yaping, Comparative Research of IPv4 and IPv6 [J], Scientific Economy Market, 2006(3)

[3] Xie Shuizhen, Two Technologies of Transition from IPv4 to IPv6 [J], Scientific Economy Market, 2006(02)

[4] I.Foster,C.Kesselman,and S.Tuecke. The Anatomy of the Grid : Enabling Scabling Virtual Organizations[J]. Int'l J.Supercomputer Applications, 2001,vol.15,no.3.

[5] L.Pearlman and colleagues.A Community Authorization Service for Group Collaboration[J].Proc.IEEE CS Press, 2002, pp:.50－60