Design and Implementation of an Initiative and Passive Network Intrusion Detection System

LI Tian
Department of Computer Science and Technology
North China Electric Power University
Baoding, Hebei Province 071003, China
ncepulitian@163.com

ZHAI Xueming
Department of Computer Science and Technology
North China Electric Power University
Baoding, Hebei Province 071003, China
zxm3165@126.com

***Abstract*—In response to the growing number of network security threats, this paper gives a new design based on the combination of initiative and passive network intrusion detection system. The system uses initiative expert system for efficient intrusion detection, and integrates honeypot technology to extract and update the attack knowledge base. It possesses a certain autonomous learning and self-adaptation.**

Keywords—intrusion detection system; honeypot; initiative expert system

I. INTRODUCTION

With the rapid development of computer network technology and Internet, network attack and intrusion are increasing day by day. Had served as the main means of firewall security is based on a static passive strategy, simply using the static defensive measures is very difficult to meet the security needs. In recent years, the initiative and passive intrusion detection technology is receiving increasing attention, it can be an effective strategy to meet the shortfall of a static and passive firewall deficiencies. Intrusion Detection System (IDS) is to collect and analyze information from a number of key points of computer network or computer system [1], and detect the network or system that may exist in all kinds of illegal attacks, vandalism, operator error, such as acts in violation of security policy or signs, and make an effective preventive and defensive behavior [2]. IDS helps network system detect the occurrence of network attacks, expand the security management capabilities of system administrator, and improve the integrity of information security infrastructure. Considered as the second gate behind the firewall, IDS can eavesdrop on the network without affecting the network performance, thereby providing real-time protection to internal attacks, external attacks and misoperation, as in [3].

This paper gives a new design based on the combination of initiative and passive network intrusion detection system. The system uses initiative expert system for efficient intrusion detection, and integrates honeypot technology to extract and update the attack knowledge base. It possesses a certain autonomous learning and self-adaptation.

II. NETWORK INTRUSION DETECTION SYSTEM

The implementation of traditional network security technologies such as firewalls and encryption technology uses "divide and rule" solution. This is a static, passive protection, which can prevent most of external attacks but powerless to internal attacks. As a proactive security tools, Intrusion Detection System provides real-time protection to internal and external attacks as well as misoperation, alarming, intercepting and responding before computer network and system are endangered. Network Intrusion Detection System as shown in Fig. 1.

Information collection module provides information used to analyze for system. This information includes log files of system and network, unexpected changes in directories and files, unexpected behaviors in programs, and physical forms of attacks. Information Collection Module collects target information and saves them, and Information Analytical Module conducts in depth analysis and risk assessment, finding attack and developing event based on the outcome of analysis, delivering events to Processing and Responding Module. Patten matching, statistical analysis and integrity analysis are used for analyzing. Processing and Responding Module classify and alarm to the events and generate the corresponding response.

Network intrusion detection system can be divided into abuse detection and anomaly detection according to different detection methods. Abuse detection is based on attack methods or attack characteristics database, it is useful to the known attack mode but powerless to the unknown; anomaly detection is based on normal behavior mode, it has a detection capacity to unknown attack, but there exists some technical difficulty to realize the protection and the alarm, as in [4].

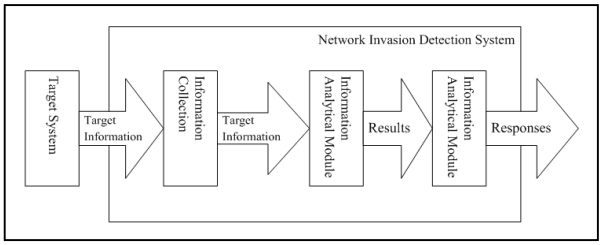

Figure 1. Network Intrusion Detection System

III. DESIGN OF INITIATIVE AND PASSIVE NETWORK INTRUSION DETECTION SYSTEM

Expert system uses field expert knowledge and reasoning mechanism, with a certain degree of intelligent, is one of the most used method of abuse detection. It takes full advantage of the knowledge, matching the network security information with expert knowledge through effective reasoning, in order to determine whether intrusion take places. But this kind of

[1] The work is supported by Youth Research Foundation of North China Electric Power University (200811021)

978-0-7695-3991-1/09 $26.00 © 2009 IEEE
DOI 10.1109/ISISE.2009.29

system lacks of ability to deal with uncertain things [5]. If autonomous learning added to the intrusion detection system, enhancing the system's ability to detect unknown attacks, leakage alarm rate can be reduced a lot. The structure of system as shown in Fig. 2.

Information collection module captures network packet, in the same time overlooks the activities in the host system of the target network, checks the host memory utilization parameters, analyzes data, and sends the information to events engine to analyzing.

Event engine arises event through examining the packet sign, source address, destination address, source port, destination port and other information, passes to the upper expert system module for processing. Event analysis module excavates the intrinsic link between events according to the event generated by engine, and saves them to the blackboard for reasoning analysis module.

Blackboard is a public storage area, used to store middle events and the results of module picking module, information and knowledge used to analyzing. It will directly affect the efficiency of reasoning that whether the blackboard is designed reasonable, the management is doing its work properly.

System brings in active honeypot technology to provide a variety of new information of network attacks for learning module. It designs a deceiving environment under tight control, lures the invaders for their attack or redirects the attack to the tightly controlled environment after detecting attacks in order to protect the actual operation of the system, at the same time, collects the information of intrusion, observes the conduct of the invaders, records their activities, in order to analyze the intruder's level, purpose, used tools, intrusion means and so on [6]. Learning module picks up new knowledge from new attack information and stores them in knowledge base, achieving self-learning function.

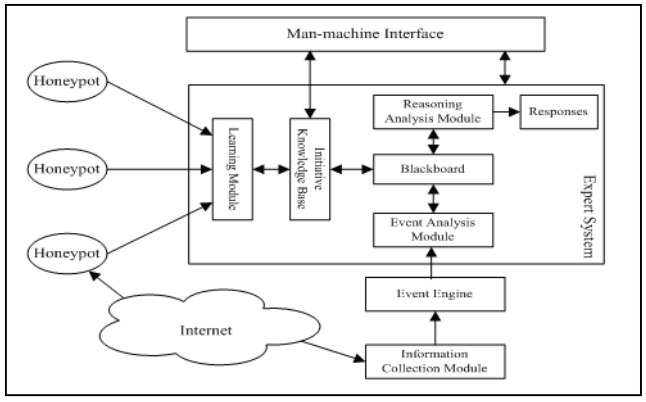

Figure 2. Structure of System

IV. Research of Key Technology in Implementation of System

A. Information Collection

Divided into network packet collection and host information gathering, information collection module provides analysis information of network and host for expert system. Whether getting information effectively is a very key issue.

As part of the main component of the network packet capture, sniffer is a kind of monitoring equipment of network packet capture. It monitors the status of the network, data flows as well as information of transmission in network, collects network packets discretely, analyzes and picks up useful information such as IP address, port number and so on.

Host information-gathering module monitors activities of the various objective systems. When the system changes, it can determine whether being attacked by the changes. Changes are important basis for judgment, including CPU utilization and memory utilization of system performance. According to obtain CPU utilization rate and memory utilization data is an effective way to determining whether there is attack in network.

B. Honeypot Technology and Deployment

Honeypot technology is a proactive network security technology, which records an attacker's actions in a reasonable manner, while minimizing or excluding risks produced by other systems in the internet. It is actually a special intelligence collection system. Honeypot computer attracts attackers. Once the attacker invades, honeypot computer will know how an attacker succeed, keeping abreast of the latest of attacks to servers, meanwhile, understanding the new way of attackers' through analysis their tools. The major technology of honeypot are network deception, port redirection, alarms, data control and data capture and so on.

Honeypot will audit conducts of the invaders, save log files, record events like the beginning of the process, compiling, increasing, deleting and modifying documents, as well as keystrokes. By collecting such data can improve the overall internal network security. Data collected can be used to measure the technical level of hackers, and to track even recognize their identity [6]. Honeypot deployment in the network as shown in Fig. 3.

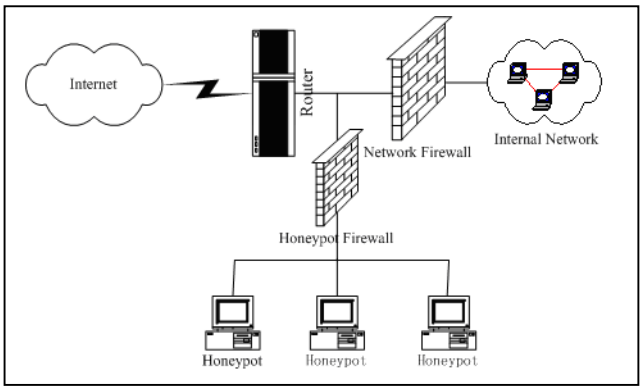

Figure 3. Honeypot in the Internet

There are two firewalls installed in the system. Internal one plays the role of protecting the internal network. Honeypot firewall is one that limits out things but open to in things. The purpose of opening is to let attackers enter the honeypot easily in order to collect the information of attacks in the network. But purpose of limiting is to avoid attacks to internal network generated by honeypot once it is attacked. Honeypot host uses Tiny Honeypot, this is a simple honeypot procedure. It has a

good mechanism of collection of intrusion information and information preservation.

C. Blackboard Management

Using block structure, blackboard stores the data that needed to be detected, analyzed or intermediate results of analysis. The basic structure of blackboard as shown in Fig. 4.

Data buffer stores the events which generated by the results of analysis, and carries out reasoning and analysis. In the process of detection, the contents of data buffer would continue to remove events that have been analyzed, read into new event from the event analysis module.

When data buffer reads new events, initiative knowledge base will search and reason corresponding knowledge in the light of the new events, and save them to knowledge base. When reasoning, if the needed knowledge is not found, the trigger events will search for knowledge in the knowledge base and put them into buffer. The knowledge buffer is compliance with the rules used recently: knowledge in buffer is in associated with a time stamp, when knowledge is called, the blackboard management and control institution makes the time stamp be the current time. Each new knowledge will also be added as part of their time stamp. Once the buffer is full, the oldest knowledge will be replaced by the newest one. This is called "most recently used". This mechanism makes the buffer always be filled with the newest knowledge because new knowledge is often the most about to be used.

Public buffer stores intermediate results and temporary variables generated in the process of reasoning. Every time the end of reasoning, intermediate results and temporary variables are cleared by the management and control institution immediately.

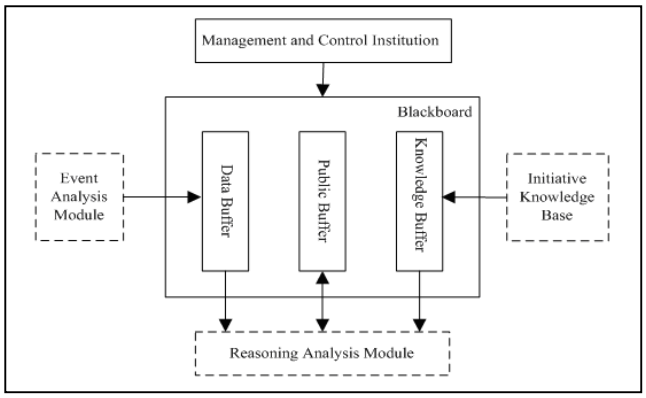

Figure 4. Basic Structure of Blackboard

V. SUMMARY AND OUTLOOK

The development of Artificial Intelligence especially the use of expert system in different fields, injects new impetus to the traditional network intrusion detection system. But intrusion detection system based on expert system is powerless when faced with unknown attacks, especially the current kinds of Trojans and viruses, making the leakage more and more serious. Faced with such problems, this paper advances a new initiative and passive network intrusion detection system with honeypot technology. The system uses initiative expert system for efficient intrusion detection, and integrates honeypot technology to extract and update the attack knowledge base. It possesses a certain autonomous learning and self-adaptation. But with the limit of achievement of Artificial Intelligence, the system needs further improvement, making highly efficient automated data analysis and reasoning tools, analyzing data timely, improving the ability and efficiency of self-learning. As a developing technology, honeypot has its immature aspects, say, how to enhance the safety of their own. It is recommended to use more efficient security honeynet to replace the honeypot.

ACKNOWLEDGMENT

Thanks to North China Electric Power University for providing research foundation. Thanks to my colleagues for giving me good ideas.

REFERENCES

[1] SHI Zhicai, JI Zhenzhou, and HU Mingzeng, "Research on Distributed Network Intrusion Detection Techniques," Computer Engineering, Shanghai, vol.31, pp.112-114, July 2005.

[2] TANG Zhengjun, Network Intrusion Detection System Design and Implementation, Beijing: Publishing House of Electronics Industry, 2002, pp.1-4.

[3] MA Chuanxiang, LI Qinghua, WANG Hui, "A Study Survey of Intrusion Detection," Computer Engineering, Shanghai, vol.31, pp.4-6, February 2005.

[4] HU Changzhen, Network Intrusion Detection Theory and Technology, Beijing: Beijing Institute of Technology Press, 2006, pp.7-18.

[5] DAI Yun, FAN Pingzhi, "An Overview on the Intrusion Detection System," Computer Engineering and Applications, Beijing, pp.17-19, April 2002.

[6] FENG Zhaohui, FAN Ruijun, ZHANG Tong, "Technology Research and Building Example of Honeynet," Computer Engineering, Shanghai, vol.33, pp.132-134, March 2007.