Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 991-994
doi:10.4028/www.scientific.net/AEF.6-7.991

HIDS and NIDS Hybrid Intrusion Detection System Model Design

Zhenqi Wang[1, a], Dankai Zhang[1,b]

[1]Information & Network Management Center, North China Electric Power University,Baoding, China

[a]w-zhenqi@ncepubd.edu.cn, [b]zhangdankai@163.com

Keyword: Intrusion Detection System ; Agent ;hybrid intrusion detection system

Abstract. With the popularity of Internet applications, network security has become one of the issues affecting the world economy. Currently, there is a large space to develop for intrusion detection systems as a relatively new field. For the faults of HIDS or NIDS network intrusion detection system, Papers has designed a hybrid HIDS and NIDS intrusion detection system model, and the introduction of Agent systems, finally through analysis the hybrid model of intrusion detection system, we can acquire its advantages.

Introduction

Intrusion detection technology which is to be a proactive security protection technology, provides internal attacks and mishandling of real-time protection, external attack, block and responses before intrusion system compromise the network.

Currently most host-based intrusion detection system or network-based intrusion detection, but they are flawed. Therefore, to overcome both defects and take advantage of both, we design a mixture model of intrusion detection system.

In recent years, attacks have becomed more and more distributions and complicate and the intruder in the implementation of the time of the invasion is often accompanied by variety of means of the invasion in order to improve the success rate of intrusion, and cover up the true purpose of the invasion in the early implementation of the attack and make implement of intrusion and attack the main rendering of hidden. Therefore, IDS also need to research new technologies to meet the increasingly complex attacks. And the distributed system on Agent is a good solution[1].

Design a distributed NIDS model of systerm

Design a distributed NIDS model of system, as shown in Figure 1:

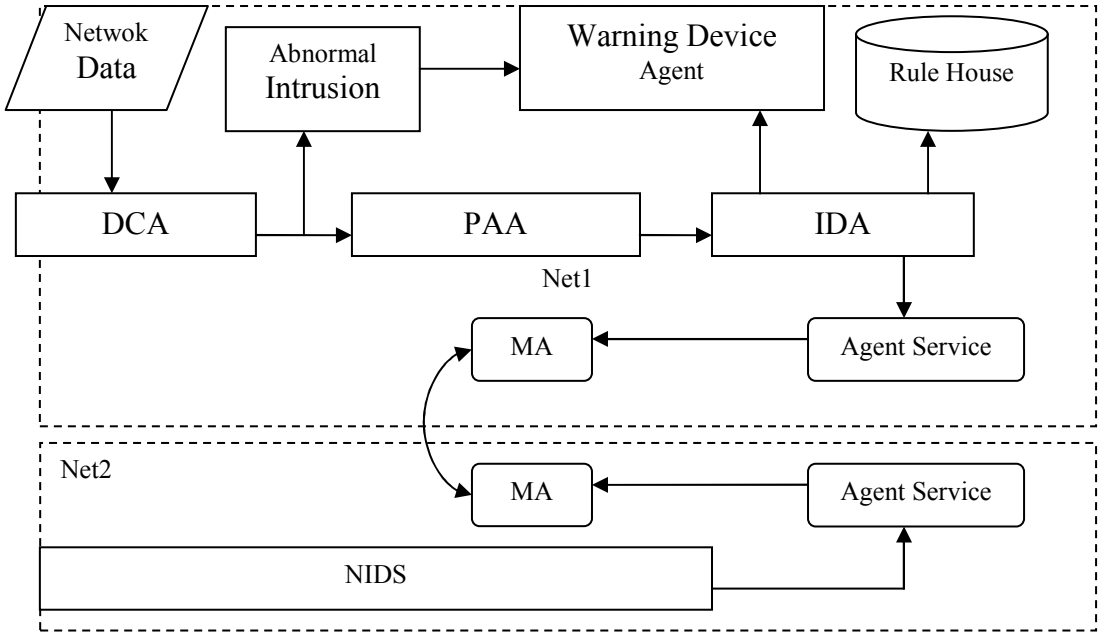

Fig.1 Network-based intrusion detection system

Introducing Agent in the network-based intrusion detection system, it can carry data and protocols directly move, improve network security, and so on.

A. Data Collection Agent（DCA）

Data collection Agent is mainly responsible for simple filtering packets on the network, reducing the data of the follow module you want to analyze, and relieve pressure on the system,then capture packets that are not filtered, and packets. Implement two functions: data capture and data filtering.

B. Protocol Analysis Agent（PAA）

Protocol Analysis Agent is the whole core of the intrusion detection system, in accordance with protocol analysis algorithm for IP network-layer intrusion detection analysis of the attack, and in accordance with the protocol network packets for analysis of the results of the analysis, enabling packets to divert to the analysis of intrusion detection system based on protocol analysis to be dealt with.

C. Intrusion Detection Agent（IDA）

Primarily responsible for systems management, detection of an intrusion, write rules to update the data, and so on. Alarm Agent is detected after the intrusion and do various forms of reactions.

D. Mobile Agent[2]（MA）

Collect data for intrusion detection system, when necessary, coordinate the network operation and collaboration of the intrusion detection system, increase interface of Mobile Agent in intrusion detection subsystem so that it has the ability to interact with mobile code closely.

Design a distributed HIDS model of systerm

Structure a model of Host-based intrusion detection system，as shown in Figure 2：

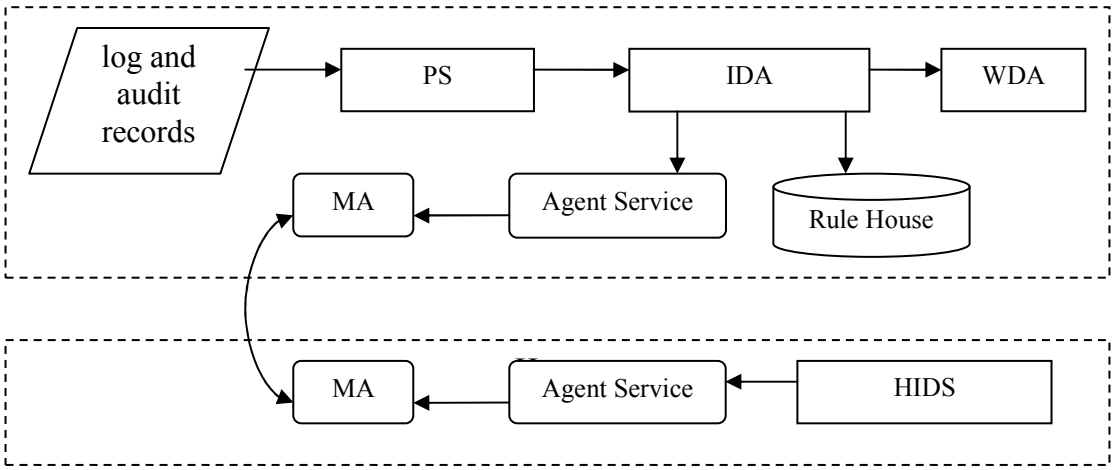

Fig.2 Host-based intrusion detection system

A. Preprocessing Section（PS）

The data of Host-based intrusion detection system mainly from log and audit records of system, preprocessing section is responsible for data normalization processing, extracting useful information, improve testing efficiency.

B. Intrusion Detection Agent（IDA）

Similar to the network-based IDS. Differences: when detecting abnormal behavior, it will produce alarm logs, and put it into the rule base for future query analysis.

C. Mobile Agent[2]（MA）

Role of Mobile Agent: intrusion detection system detects an event, because of their limited, failed to make accurate judgments, then the assistance request to the Agent server on this computer, server send one or more Agent to the server which may accept the agent on other hosts, getting specific information back to the original host, providing appropriate treatment.

D. Warning Device Agent（WDA）

For information of intrusion detection Agent sent to, and then under response policy to make instant response, MAIL alarm, voice alarm, disconnected TCP session, break the process, and so on.

Design A NIDS and HIDS hybrid intrusion detection system model

Many IDS tend to use detection methods of network-based or host-based detection methods to achieve security. However, the inadequate of HIDS and NIDS: in the face of complex network environments, NIDS shortcomings is that monitoring of the amount of data is too large and cannot be combined with the operating system features to accurately judge your network behavior. In addition, NIDS could not be collected in real time all data packets. HIDS is limited by its deployment environment, only support a single host security, lack of cross-platform, poor portability, so limited the scope of application and intrusions to the network protocol can do about it.

For these defects, construct a HIDS and NIDS hybrid intrusion detection system model, as shown in Figure 3:

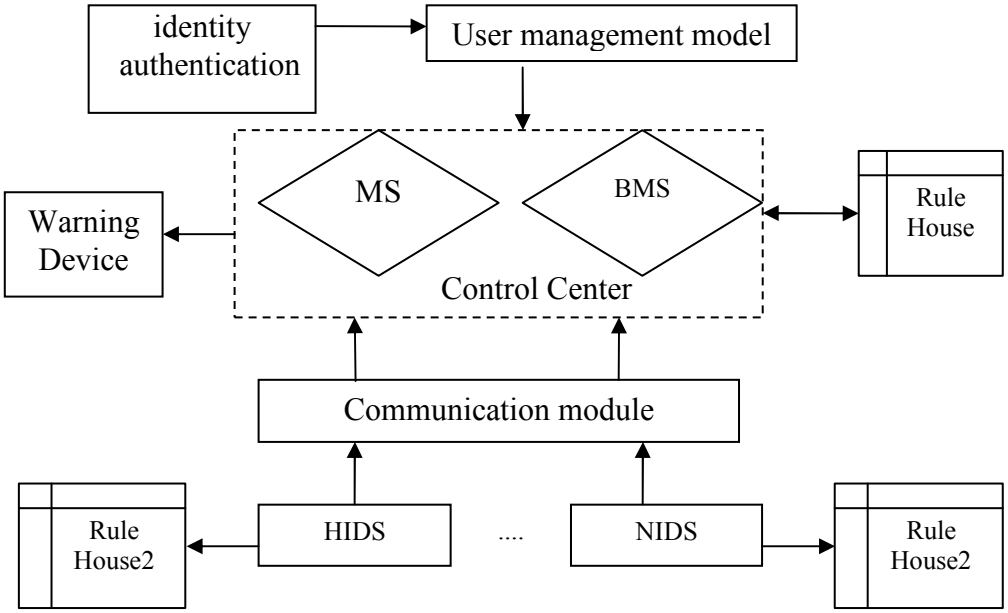

Fig.3 NIDS and HIDS hybrid intrusion detection system

Control Center is mainly used to determine whether a sophisticated intrusion attacks, master system and other network communications to exchange information, update rules, assignment rules information database, make the appropriate alert. It includes a master system （MS）and based-on the master system（BMS）, master is the core of the system, the second control system is a backup of the master system, preventing the master control center attack when not working, replaced the main control system completes the task.

Communication module is done through the SOCKET mechanism to control center and HIDS (NIDS) for information exchange. Communication components should have basic functionality: message delivery, receives message and message.

Rule: (1) if detected on packets with attack signatures, stored it in database, systems analysis, statistical sampling or statistical analysis modules; (2) storage rules of characteristics of intrusion or invasion as intrusion detection data analysis model if there are exceptions based on the package.

User management model is to pass identity authentication, and then manage the entire system, including rule base to upgrade and improve, the system log management, analysis and other functions.

Comprehensive analysis

Taking into account the increase of real-time intrusion detection, avoid overloading the network communication and other issues such as improving the efficiency of the system, introduced Agent technology in the network and host IDS, using static Agent for data collection, intrusion analysis, response, etc. Mobile Agent can be run across the network, cross-platform, it can be implemented using the Mobile Agent intrusion tracing of certain functions, search for the trace of the attackers, and forensics, make up for the traditional IDS systems platform of insurmountable and so on.

Intrusion detection system, based on "static Agent, Mobile Agent supplement" principle, that is, you can use the static Agent, Mobile Agent is not used as much as possible, to reduce the complexity of the system.

Host-based IDS and network-based IDS, however there is still a lot of shortcomings. Such as HIDS apart from take up valuable resources, monitoring only the host itself outside of the host, there is no detection of conditions on the network; NIDS will appear in a switched Ethernet environment detection range limits, are not suitable for handling encrypted sessions, and poor accuracy of detecting intrusion, is difficult to configure in a switched network environment, prevention of intrusion deception is relatively poor.

Intrusion detection system using a hybrid-type system whose master of intrusion detection system in general further judgment, give full play to host based IDS and network-based IDS of both advantages, make up for the lack of both, to do both detection of network attack information, can also be found in log an exception from the system.

Comparison network-based intrusion detection system (NIDS) or host-based intrusion detection system (HIDS) with hybrid intrusion detection system (Mixed Intrusion Detection System, MIDS). Because of the MIDS data sources extensively, with good communication, and the control center can detect more complex attacks, so the MIDS testing more comprehensive. However, from the detection time, detection of MIDS need a longer time.

References

[1] Dayou Liu, Yangkun, Jianzhong Chen. Research status and development trend on Agent. Journal of software, November 2000 pp：315-321

[2] Yongzhong Li, Yunsheng Luo,Sunyan.Research based on Mobile Agent for an intelligent intrusion detection system structure. Computer research and development. June 2006 pp:296-301.