ATLANTIS PRESS

*Advances in Engineering Research, volume 141*

5th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering (ICMMCE 2017)

# Design of intrusion detection system oriented to computer network security

Xiao LOU

[1]College of computer science and technology,Zhijiang college of zhejiang university of technology,312030,China

[a]louxiaozj@126.com

**Keywords:** Intrusion Detection; Network Security; Security Analysis

**Abstract.** With the development of computer network, the protection of network information from various attacks is becoming more and more serious, and has become the basic purpose of network security. However, because of diversity and openness of computer network connection with the terminal and the network distribution of the connectivity characteristics of the system, leading to the computer network vulnerable to hackers, malicious software attacks and other misconduct, network security has become a key factor restricting the development of the network. Therefore, it is necessary to carry out the comprehensive research of intrusion detection.

## Introduction

With the continuous development of computer networks, the global information technology has become a major trend of human development. However, because of the diversity of computer networks and open networks, uneven distribution terminals, connectivity and other features, resulting in the computer network vulnerable to hackers, malicious software attacks, and other misconduct, online information security and secrecy, has become a key issue. For the transmission of sensitive data, the online security and privacy information of computer network systems is especially important [1]. Therefore, the computer network must have a strong enough security measure, otherwise the network will be a useless and even endanger the national security network. Both in LAN and WAN, there are many factors, such as vulnerability and potential natural and man-made threats. Network security measures should be able to carry out various threats and loopholes in all directions, so as to ensure the confidentiality, integrity and availability of network information [2]. Network security has increasingly become the key factor restricting the development of the network.

IDS (intrusion detection system, referred to as IDS) is an important part of the information security system, which is a necessary supplement to the firewall, it is a kind of active security technology, through the computer network or computer system in a number of key points to collect information, and analysis, the host system or network user activity monitor find out whether the violation of security policy network or system and a possible intrusion. Intrusion detection system is divided into two kinds of analysis technology based on host and network based on data source, which are divided into anomaly detection and misuse intrusion detection.

## Computer Network Security Analysis

Computer network security is a comprehensive subject which involves computer science, network technology, communication technology, cryptography, information security technology, applied mathematics, number theory, information theory and so on. The network information security means that the data network system hardware, software and systems are protected from accidental or malicious destruction of reason, system changes, disclosure, continuous and reliable to normal operation, the network service is not interrupted. In a broad sense, all the technical and theoretical information related to network confidentiality, integrity, availability, authenticity and control are network information security studies. At present, the main threats to computer network security are

hacker attacks, lack of defects, management, network, software vulnerabilities, misuse, abuse and malicious behavior resources and illegal use of services.

As an active security technology, intrusion detection provides internal attacks and external attacks and misuse, and intercepts and responds to intrusions before the real-time protection network system is destroyed. From the 3D depth network security, multilayer defense point of view, the focus of intrusion detection, but the status quo is not mature in the development stage of intrusion detection, intrusion detection, a substantial increase in domestic products currently control interfaces based on Snort analysis and detection technology is no substantive progress. At present, most of the intrusion detection products are single packet pattern matching detection methods. Single packet pattern matching detection has shown a lot of problems, and many international companies have devoted efforts to the next generation of intrusion detection technology.

Existing intrusion detection methods can only achieve certain effects or known intrusions, and sometimes false positive rate affects the performance of the system. Improving the detection and prevention of known and unknown intrusions, reducing false positives, improving the security and stability of the system has been an important topic of active defense technology research. In order to improve the performance of intrusion detection system, integration, cooperation and optimization are introduced into intrusion detection system, and the effect of single vulnerability detection method on defense is solved. The purpose of this study is to analysis the popular intrusion intrusion detection techniques and methods of the current detection technology, and improvement of the design of a safe, efficient, cross platform, network security system, intrusion detection system, and plays an important role and practical significance for the development of inspired new intrusion detection products.

## Intrusion detection system and technology

Intrusion detection systems can be autonomous, computer networks, real-time attacks, detection and response. Loop network security monitoring allows users to customize interrupts before the system is broken and responds to security vulnerabilities and misuse. Real time monitoring and analysis of suspicious data does not affect data transmission over the network. It automatically provides maximum security against enterprise security threats. In addition to cutting off attacks in time, we can adjust the firewall protection strategy dynamically, and make firewall become a dynamic intelligent protection system. [6]. The intrusion detection system, monitoring and analysis of user behavior audit system configuration and vulnerability assessment system and the integrity of sensitive data, identify the attack behavior, abnormal behavior statistics, automatic collection and system related patches, audit tracking and identification of violations of safety regulations, the use of deception server records hackers and other functions, the system administrator can monitor, audit and assess the system more effective. Figure 1 is a generic model for intrusion detection systems.

The intrusion detection system as a kind of active security, which is a necessary supplement to the firewall, it is through the collection of information on some of the key points in the computer network or computer system and analysis, found that the network or system, if there is illegal behavior, signs of being attacked by the security policy. In recent years, with the rapid development of Internet, the problem of information security has become increasingly prominent. Intrusion detection information security architecture is an important part of it. Unlike other security products, intrusion detection systems need more intelligence, and it must be able to obtain data for analysis and to derive useful results. Only the existing intrusion detection methods have achieved good results, for some intrusion or known, in the face of increasingly updated network facilities and emerge in an endless stream attack, the existing intrusion detection model, there are still many deficiencies. The adaptive ability is not strong, can not detect some new or unknown forms of invasion; cost Gao Jianmo; system update is slow, poor scalability, dependence on expert experience too strong. How to detect or prevent intrusion effectively and reduce the false positive rate has become a serious problem.

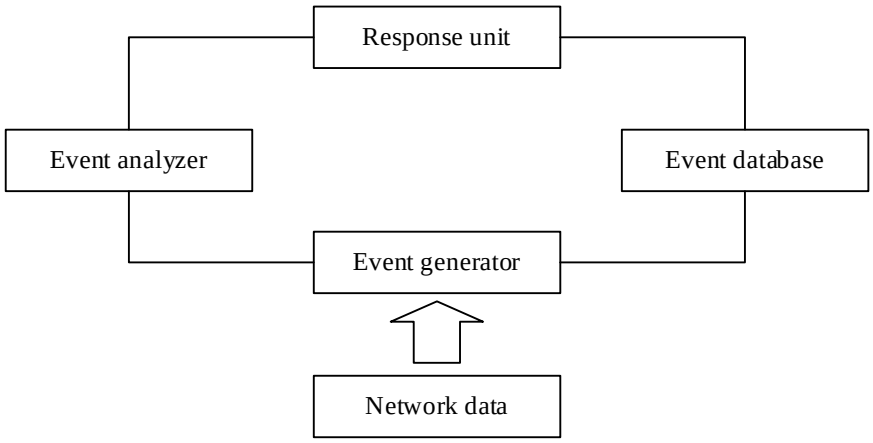


Figure 1. The model of intrusion detection system

**Requirement analysis of intrusion detection system**

The network detection agent is a whole system bottom module, which is responsible for obtaining packets from the network in real time, and then analyzing the packet pattern matching to alarm the packets containing abnormal conditions. When they say the system used to detect intrusion detection agent is a low level system, it can still be run independently, when they are not a part of the distributed intrusion detection system, so we design the management function and the user interface and the database, and it is designed to be a simple coping strategy. As a result, it can be implemented from data acquisition, data analysis to the entire workflow alarm, as shown in figure 2.

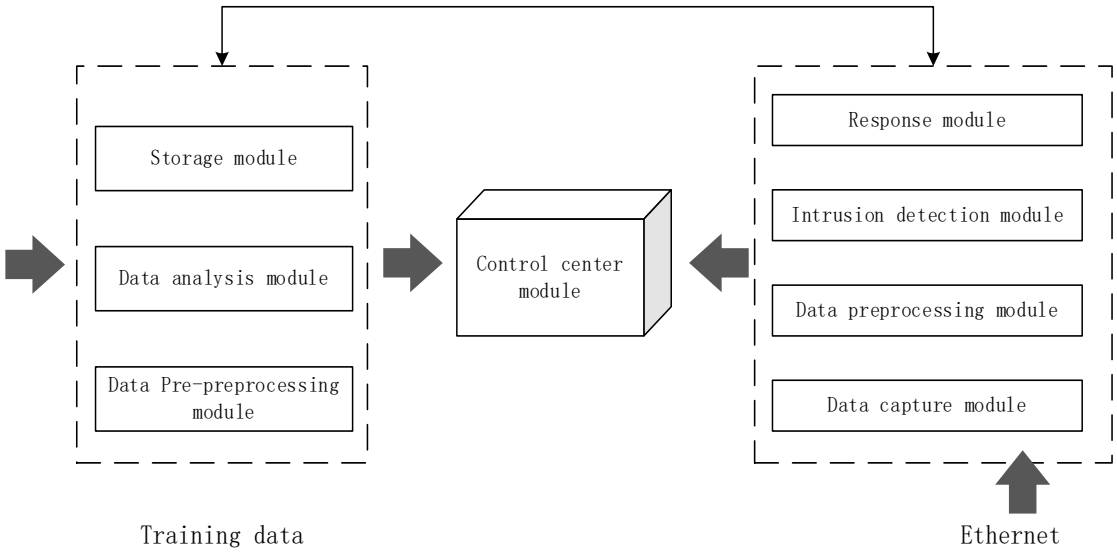


Figure 2. The structure of network intrusion detection system

**Packet capture and analysis module.** According to the protocol of packet header information, the module can capture the network traffic packets and so on.

Module pretreatment module. Using a flexible plug-in architecture, users can load appropriate preprocessor as needed to further improve the system's processing power. The pretreatment module mainly uses advanced processor such as detector, decoder, detector and so on.

**Detection engine module.** The module is the core of the detection system, and the quality of the detection engine directly affects the quality of the whole system. The engine is designed to be a very popular detection network design reference intrusion detection system, the current international also adopted the plug-in architecture model, that all kinds of detection through a variety of plug-in modules to complete. The use of this flexible structure model is conducive to constantly updating the system, expanding and refining, to improve the system function or the specific needs of the system customized users. Each plug-in performs the corresponding rule keyword binding to guarantee the right to be referred to as the detection engine during execution.

**Log and alarm module.** Complete the module output detection results, when the invasion occurs, timely report to the administrator intrusion. The module also uses the plug-in architecture. System settings three log mode closed, in the readable format recording package, real-time monitoring of detection information. The alarm mechanism, the main system log file of the system, sends messages to the form in front of the alarm message. In addition, the system also provides an interface to support the database, supports schema querying, packet information, and statistics traffic within the packet.

**Rule base module.** Mainly used for storing attack signatures.

## Design of Computer Network Intrusion Detection System

The purpose of this article is the intrusion detection system from the whole network is a distributed network intrusion detection system based on signal rules and rules of the parsing engine detection proxy module use protocol analysis and pattern matching analysis method combined with the process of data packet, misuse based intrusion detection system. In addition to being found agency management information submitted complete monitoring agent module, analysis, and CO and other drug monitoring data fusion algorithm, the matching detection agent used in detection, such as distributed denial of service attack a wide range of network. The design of the whole experiment system adopts the plug-in architecture model to improve the flexibility and extensibility of the system.

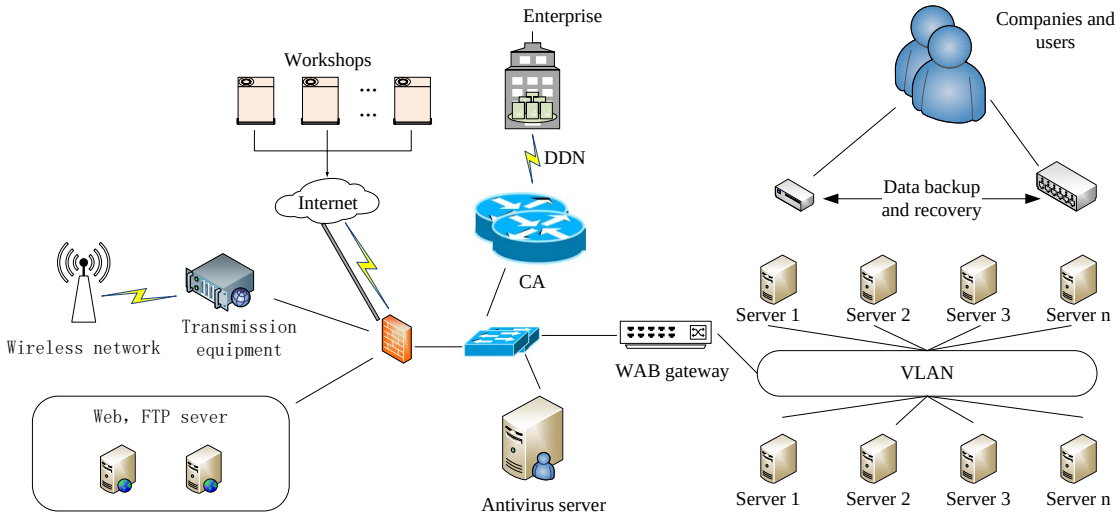


Figure 3. The Topology of network security system for enterprise application

Due to the distributed intrusion detection has distributed data sources, collaborative component distribution, functional analysis of the behavior of the system, so in the trend of complex network structure, at present, people began to study and pay attention to the development of Distributed Intrusion detection. The distributed network intrusion detection system designed in this paper is also one of them. If multiple data sources are used in distributed processing mode, they are called distributed multiple analysis systems. The distributed multi analysis system really embodies the importance of distributed intrusion detection system. According to the central processor or operation mode called the analysis node, the distributed and multi analysis system can be further divided into two kinds of analytic hierarchy system and collaborative analysis system. The jurisdiction of regret hchm model layers of the monitoring agent detection area within easy compassion science phonation agent in the District, but also conducive to the monitoring agent multiple distributed data discovery agents reported a higher level of abstraction, in order to better identify the intrusion or abnormal behavior. Between each detection area, monitoring agent in equal and cooperative work mode, no single central processing node network wide, effective implementation of the inspection task assignment, avoid key node processing bottlenecks, improve the system fault tolerance. In addition, due to the interaction between the monitoring agent data has been refined abstract data instead of the original security audit data, compared with the pure collaborative model, can reduce the inter network data transmission between components to a large extent.

## Conclusion

With the development and progress of science and technology and network security technology, network security angle, depth, multilayer defense perspective, intrusion detection systems and technology to get attention, but because of the intrusion detection technology is not mature, in the stage of development. Study on the current situation of information security and intrusion detection system and the development trend of this technology is studied, and applied to a variety of intrusion detection technology, method and mechanism of an intrusion detection system based on integration, and collaboration, so as to optimize the concept of intrusion detection system, we propose a intrusion detection method and technology of a different the detection system, intrusion detection system can keep robust, fault tolerance, adaptability and expansibility of network security really get better results.

## Reference

[1] Modi C, Patel D, Borisaniya B, et al. A survey of intrusion detection techniques in cloud[J]. Journal of Network and Computer Applications, 2013, 36(1): 42-57.

[2] Manshaei M H, Zhu Q, Alpcan T, et al. Game theory meets network security and privacy[J]. ACM Computing Surveys (CSUR), 2013, 45(3): 25.

[3] Hoque M S, Mukit M, Bikas M, et al. An implementation of intrusion detection system using genetic algorithm[J]. arXiv preprint arXiv:1204.1336, 2012.

[4] Shiravi H, Shiravi A, Ghorbani A. A survey of visualization systems for network security[J]. Visualization and Computer Graphics, IEEE Transactions on, 2012, 18(8): 1313-1329.

[5] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing[J]. Journal of network and computer applications, 2011, 34(1): 1-11.

[6] Chung C J, Khatkar P, Xing T, et al. NICE: Network intrusion detection and countermeasure selection in virtual network systems[J]. Dependable and Secure Computing, IEEE Transactions on, 2013, 10(4): 198-211.