A Novel Approach of intrusion detection system design for computer network security

Julan YI[1, a]

[1]XINYU UNIVERSITY, Xin Yu 338004, China

[a]julanyi@126.com

Keywords: Intrusion Detection; Network Security; Security Analysis

Abstract. With the development of computer networks, protecting the network information from a variety of attacks are becoming increasingly important as the fundamental purpose of network security. However, due to the diversity of computer networks linking having uneven distribution terminal and network openness, connectivity and other system characteristics, resulting in computer networks vulnerable to hackers, malicious software attacks and other misconduct, network security is increasingly becoming constrained network a key factor in development. Therefore, it is necessary to conduct in-depth comprehensive intrusion detection angles of research.

Introduction

With the continuous development of computer networks, global information technology has become a major trend in human development. However, due to the diversity of computer networks have links, terminals and uneven distribution of open networks, connectivity and other features, resulting in computer networks vulnerable to attacks by hackers, malware, and other misconduct, online security and confidentiality of information, becomes a critical issue. For the transmission of sensitive data, computer network system, its online security and confidentiality of information is particularly important [1]. Therefore, the computer network must have a strong enough safety measures, otherwise the network will be a useless and even endanger the national security of the network. Whether in the LAN or across the WAN, there is a vulnerability and potential threats of natural and man-made, and many other factors. Network security measures should be able in all directions for a variety of threats and vulnerabilities, so as to ensure the confidentiality, integrity and availability of network information [2]. Network security is increasingly becoming a key factor in restricting network development.

Intrusion detection system (Intrusion Detection System, referred IDS) is the information security architecture is an important part, is a necessary complement to the firewall, it is a proactive security protection technology, through the computer network or computer system in a number of key point to gather information and analyze, monitor the host system or user activity on the network, and found the network or system whether there is a violation of security policy behavior and possible intrusions. Intrusion detection system according to the data source is divided into two kinds of host-based and network-based intrusion detection analysis technology is mainly divided into anomaly detection and misuse intrusion detection.

Computer Network Security Analysis

Computer network security is one related to computer science, network technology, communication technology, cryptography, information security technology, applied mathematics, number theory, information theory and other disciplines comprehensive discipline. Network information security means that the data network systems hardware, software and systems are protected from accidental or malicious destruction of reasons, change, disclosure, continuous and reliable system to normal operation, the network service is not interrupted. Broadly speaking, all related to the network confidentiality, integrity, availability, authenticity and control related technical and theoretical information is network information security research. Current threats to

© 2015. The authors - Published by Atlantis Press

computer network security mainly, hacker attacks, lack of defect management, network, software vulnerabilities, misuse, abuse and malicious acts resources and illegal use of the service [3-5].

Intrusion detection as a proactive security technology, provides internal attacks and external attacks and misuse in real-time protection network system compromised prior to intercept and respond to intrusions. From the three-dimensional depth network security, multi-layered defense perspective, intrusion detection by the people's attention, but the status quo is not mature enough intrusion detection, in the development stage, the current domestic intrusion detection products is substantially increased control on the basis of SNORT interface for analysis and detection technology is no substantive progress. Current intrusion detection products is mostly single packet pattern matching detection method. Single package pattern matching detection method has shown a lot of problems, many international companies have invested efforts on the next generation of intrusion detection technology.

Existing intrusion detection methods can only achieve good results for certain or known intrusion, sometimes false alarm rate, affecting the performance of the system. And increase the effective detection or prevention of the occurrence of known and unknown intrusions, reduce false positives, improve the safety and stability of the system, it has been an important subject of active defense technology research. To improve the performance of intrusion detection systems, will be integrated, cooperation, so as to optimize selectivity introduced to the idea of intrusion detection systems, trying to solve a single flaw detection method in effect on the defense. The purpose of this research is in the current domestic popular intrusion detection techniques and methods to analyze the intrusion detection technology, and to improve it, to design an efficient, secure, cross-platform, intrusion detection systems, network security system so as to establish and develop new intrusion detection products has an important role and inspired a certain practical significance.

Intrusion Detection Systems and Technology

Intrusion detection system can autonomously computer networks, real-time attack detection and response. Reincarnation network security monitoring, so that users can customize to interrupt before the system is broken and respond to security breaches and misuse. Real-time monitoring and analysis of suspicious data without affecting the data transmission on the network. It automatically respond to security threats for businesses provides maximum security. After detecting network intrusion, in addition to promptly cut off the attack, but also can dynamically adjust the firewall protection policies, so that the firewall has become a dynamic and intelligent protection system [6]. Intrusion detection system that monitors and analyzes user behavior auditing system configurations and vulnerabilities, assess the integrity of sensitive systems and data, to identify aggressive behavior, abnormal behavior statistics, automatically collect and system-related patch, audit tracking and recognition violation conduct safety regulations, the use of decoy server record hacking and other functions, the system administrator can more effectively monitor, audit and evaluate their own systems. Figure 1 is a generic intrusion detection system model.

Intrusion Detection System as a proactive information security measures, is a necessary complement to the firewall, it is by gathering information on a number of key points in a computer network or computer system and its analysis, and found the network or system, whether there is a violation behavior and signs of being attacked security policy. In recent years, with the rapid development of Internet, information security issues become increasingly prominent, intrusion detection information security architecture is an important part. And other security products different is that intrusion detection system needs more intelligence, it must be able to obtain data for analysis, and draw useful results. Existing intrusion detection methods can only achieve good results for certain or known intrusion, the face of increasingly updated network facilities and the endless stream of attacks, the existing intrusion detection models are still many lacking. Adaptive capacity is not strong; can not detect some new or unknown form of invasion; the cost of high modeling; system updates slow; poor scalability, excessive dependence on the experience of experts. How to effectively detect or prevent the occurrence of intrusion, reduce the false alarm rate has become a serious problem.

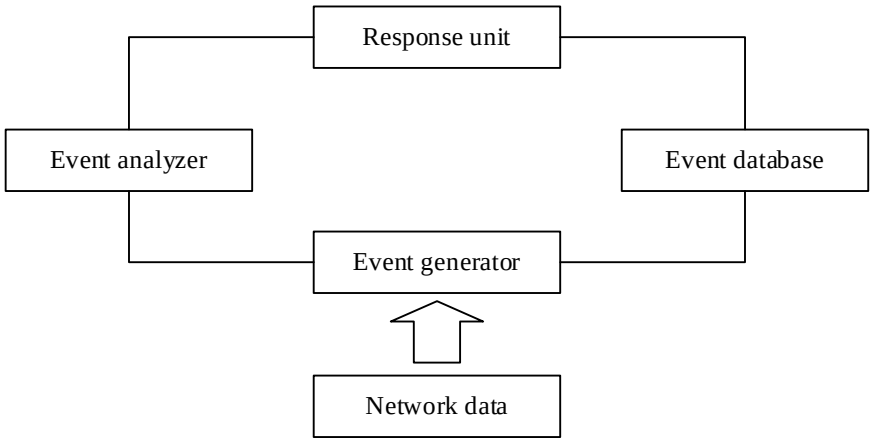

Figure 1. The model of intrusion detection system

Intrusion Detection System Requirements Analysis

Network detection agent is a whole system of grassroots module, responsible for getting packets from the network in real time, and then parse the data packet pattern matching for packet contains abnormal situation alarm. When they said the system designed to detect agents are low-level intrusion detection system, it can still run independently when they are not distributed intrusion detection system components, so we designed the management for its features and user interface and database, as well as It is designed as a simple response strategy. As a result, it can be achieved from a data acquisition, data analysis to entire workflow alarm, the response shown in Figure 2.

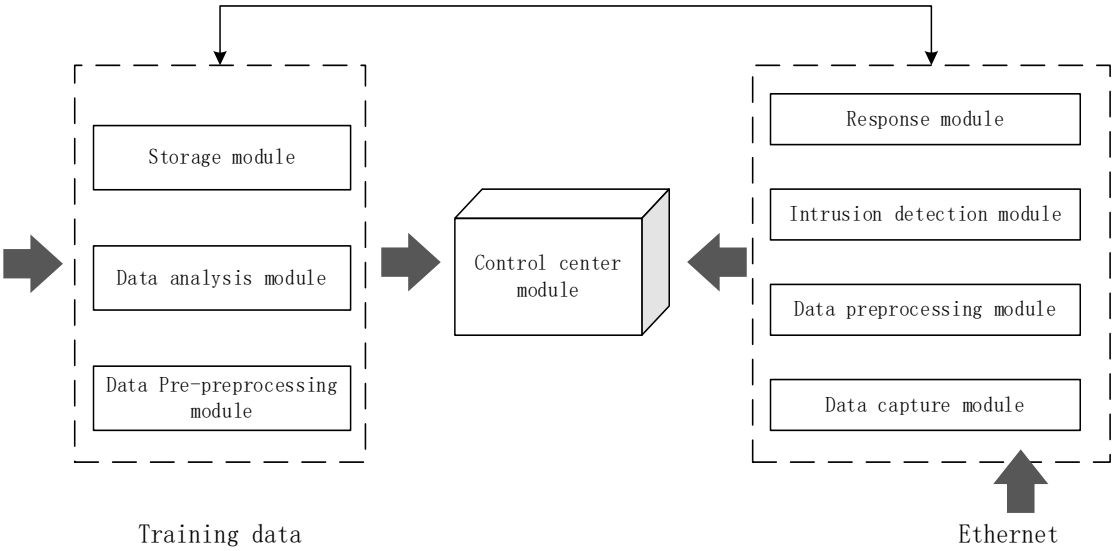

Figure 2. The structure of network intrusion detection system

Packet capture and analysis module. This module complete capture of network traffic packets and the like according to the protocol of the packet header information for resolution.

Preprocessing module the module. Using a flexible "plug-in" architecture, users can load the appropriate preprocessor according to demand, and further enhance the processing capability of the system. The current pre-processing module mainly uses the detectors, decoders, detectors and other top handler.

Detection engine module. This module is the core of the detection system, the detection engine directly affect the efficiency of the performance of the pros and cons of the whole system. The engine is designed to detect a very popular reference design network intrusion detection system on the current international, also adopted the "plug-in" architecture model, that a variety of detection is through a variety of plug-in modules to complete. The use of such a flexible structure model is conducive to constantly update the system, expanded and improved to enhance the system

functionality or system customized user specific needs. Each plug-in will be carried out with the corresponding rule keyword is bound to ensure that in the implementation of the right to be called the detection engine.

Log and alarm module. To complete the module outputs a detection result, when the invasion occurred, to promptly report the intrusion to pity administrator. The module also uses the "plug-in" architecture. System set up three log mode is off, in a readable format recording packet, real-time monitoring to detect information. Alarm mechanism system of the main system log file, sent to the front of the alarm information in the form of messages. In addition, the system also provides an interface for the database support, support to the mode query packet information, and packet traffic within the stage to conduct statistics.

Rule base module. Mainly used for storing attack signatures.

Design of Computer Network Intrusion Detection System

This article is designed network intrusion detection system from the overall sense is a network-based distributed intrusion detection system, wherein the detection agent module uses rule sets and rule parsing engine to process the packet using a protocol analysis and pattern signal analysis method combines match, belonging intrusion detection system based on misuse. Monitoring Agent module in addition to the completion of the information submitted by the discovery agent to manage, it also co-analysis and other monitoring agents, the use of data fusion algorithm to match detection to detect the detection agent can not detect, such as distributed denial of service attacks, etc. attacks against a wide range of networks. Entire experimental system design ideas using the "plug-in" architecture model, in order to improve the flexibility and scalability of the system.

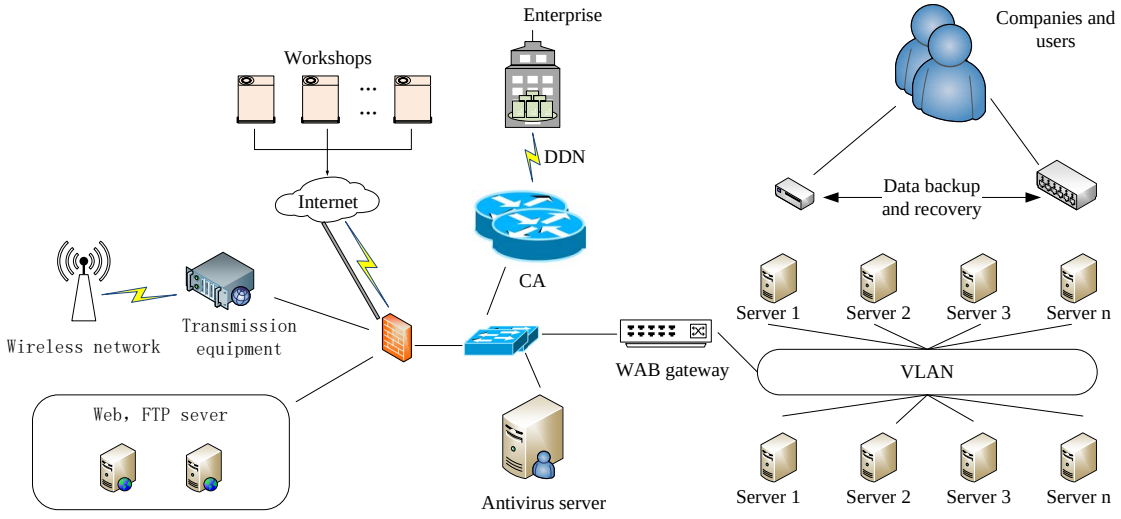

Figure 3. The Topology of network security system for enterprise application

Because Distributed Intrusion Detection has decentralized data sources, analyze the distribution of components, system behavior collaborative features, so in the current network structure of complex and large-scale trends, people began to focus on research and development of distributed intrusion detection above the. This article is designed distributed network intrusion detection system also belongs to one of them. If you use multiple data sources for distributed processing mode, it is called a distributed multi-analysis system. Distributed multi-analysis system truly reflects the significance of Distributed Intrusion Detection System. According to the central processor or operating mode called Analysis node, distributed, multi-analyte system can be further divided into two types of hierarchical analysis systems and collaborative analysis system. HCHM model hierarchical within each monitoring agent detection area of jurisdiction of the pity model, in the area within easy pity sounding proxies pity science, but also conducive to the monitoring agent to multiple distributed data discovery agent has reported high-level abstraction, in order to better identify intrusion or abnormal behavior. Between each detection region, the monitoring agent to

work in a collaborative model of equality, there is no network-wide single central processing node, the effective implementation of the distribution of the inspection tasks, avoid processing bottlenecks key nodes, to improve the system fault tolerance. Also, because the interaction between the monitoring agent data already is refined abstract data instead of the original security audit data, as compared with pure collaborative model can be reduced to a large extent between components across the network transmission the amount of data.

Conclusion

With the improvement of technology and the development of network security, network security perspective, depth, multi-layered defense perspective, intrusion detection systems and techniques to get attention, but because of intrusion detection technology is not mature enough, in the development stage. This paper analyzes and studies the development trend of information security status and intrusion detection systems and technologies have been studied and applied for a variety of intrusion detection technology, the intrusion detection system based on an integrated approach and mechanisms, and cooperative, so as to optimize the idea of introducing the intrusion detection system, we propose a variety of detection methods and techniques based intrusion detection systems, intrusion detection systems make possible to maintain robust, fault tolerance, adaptability, scalability so 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.