An Expert System for Preventing and Auditing Intrusion

Zong-pu Jia[1,2] Zhi-lin Yao[1] Shu-fen Liu[1,2]

[1] *College of Computer Science and Technology, Jilin University, Changchun, Jilin, China,130012*
[2] *Department of Computer Science and Technology, Henan Polythechnic University, Jiaozuo, Henan, China, 454000*
jiazp@hpu.edu.cn, yaozl@jlu.edu.cn, liusf@jlu.edu.cn

Abstract

Network security research is an important aspect of CSCW (Computer Supported Cooperative Work). It helps to make work environment essential and reliable. Access control security technology mainly includes firewall technology, intrusion detection technology, and security auditing technology. These technologies still have some problems and shortages though they are matured in some degree. The Expert System for Preventing and Auditing Intrusion is a series of software and hardware systems for reducing the risk of computer network security. It is an effective closed loop control system that integrates with Fire Wall, Intrusion Detection, and Auditing Trail Analysis. It uses the learning ability of expert system to add knowledge and rules. Also it combines the characteristics of real-time and unreal-time to form an access control security system and enhance the security of the network.

Keywords: Network Security, Intrusion Detection, Expert Systems, Learning.

1. Introduction

As the widely adoption of computer network and rapid development of the Internet, security of the network information problem is becoming focus more than ever. A lot of theoretical studies are focus on access control and information confidentiality. But there is a chaos situation of technical application. Generally, to improve the security by means of access control mainly includes firewall technology, intrusion detection technology and security audit technology. Information encrypt technology can be seemed as the complementarities of former technologies, and is not an independent technology to protect the network security.

1.1. Lack of firewall

Firewall is a technology that controls the access to network based on certain rules. It is one of the most important methods to prevent the intrusion to the network. It mainly includes two types of packets filtering and proxy gateway.

Packets filtering firewall only implements large granularity access control. Its rules are mainly based on IP address and service port, and seldom check the content of the packets. Moreover, because of the complex rules configuration and management, it requires the administrator of the network comprehend the network intrusion deeply.

So it is difficult to use it more and more in addition to it's ordinarily effect.

Although the proxy gateway firewall can separate the internal and external users and make internal resource except servers invisible to the external users, it hasn't made up the lack of packets filtering firewall radically. Though we can filter the content of the packets more deeply, but as to the speed requirement of the application, the filtering depth can not go much further. Even then, the speed to support the application is not satisfied.

1.2. Lack of intrusion detection

Intrusion detection is an effective complementary technology of firewall. It can recognize the intrusion behaviors in real-time mode and make alert by the support of the rules base. Intrusion detection system (IDS) includes host-based IDS and network-based IDS. Host-based IDS analyzes the log on local host, it can only detect the intrusion behaviors to the local host. Network-based IDS checks the packets in the network and make alert when find intrusion suspect packets. The detecting speed is important because of the real-time requirement. So the algorithm of it should not be complex. We can not use long-time-window analysis or analyze the history data combined with the real-time data. Thus, we can only analyze the independent data packets or data packets within a short time to make judgment. That brings on high omitting rate and misreporting rate.

Some hackers use distribution technology to send massive garbage packets to IDS to make it overloaded. So the IDS would be invalid because of packets lost. The hackers then would escape from the detection of the IDS.

1.3. Lack of security audit

Security audit is a new technology that records and audits the access behaviors and data to find out the intrusion characters. Common security audit system is an essential part of the entire security framework. It states behind the IDS, function as the complementarities of the IDS and firewall. Figure 1 demonstrates the relationship

of those three systems. In function aspect, the security audit can detect some intrusion that some intrusion detection system could not find out. It can record the intrusions and represent them when ever required to get evidence. And it can be used to find some unknown intrusion model. Compared with traditional intrusion detection system, there is no real-time requirement for security audit system. So it can analyze vast history data. And its analysis methods are more complex and fine. It can find out more kinds of attack, and has lower error rate. The results are shown to the administrator as alert as IDS does. The results can not be transformed into the strategy of the firewall automatically, the administrator need to configure the firewall according to the intrusion type of the alert manually.

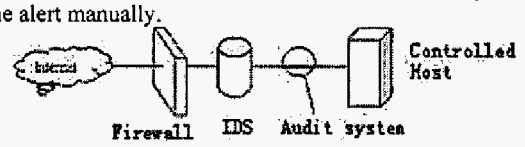

Figure 1. Relationship of Firewall, IDS and Audit system

1.4. Advantage of expert system for preventing and auditing intrusion

Expert system for preventing and auditing intrusion combines former three kinds of technology, and makes audit system, reasoning, detection and controlling integrated to form a closed loop control system[1]. And combined with the ability of learning and the characteristics of real-time and unreal-time, it becomes an effective network security control system. The architecture of it is shown in figure 2. In this expert system, firewall, IDS and security audit system are deployed in deferent hosts. They work at their own time window length respectively. So the system combines the characteristics of real-time and unreal-time together. By the support of the export system, they establish intrinsic relationship. The results of IDS and security audit system can be transformed into the strategies of the firewall by export system, and make the strategies of the firewall optimized.

The design of this export system also includes accumulating ability of knowledge and experience, structure and extensible design of the knowledge base, learning ability and adaptability. The technologies that we adopted have shortage because they are not theoretically matured yet, and we only make common design, but the effect is satisfied.

2. General Design

The expert system for preventing and auditing intrusion is composed by expert system knowledge base, reasoner, database, decision-maker, pre-handler, intrusion detector, auditor, alerter, controller, and learner. The structure of the system is shown in figure 2.

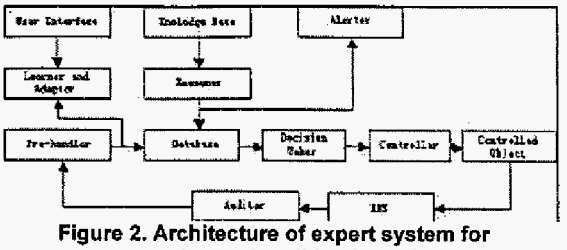

Figure 2. Architecture of expert system for preventing and auditing intrusion

2.1. Design of the knowledge base

We use knowledge base to store the intrusion characters knowledge and rules to distinguish safe event. The content of knowledge base includes intrusion name, confirm condition, reason and handling method, etc. It has typical fixed structure, and suitable to be expressed by framework. Every step of the reasoning procedure can be treated as a knowledge element. A knowledge element is made up by an intrusion framework, several condition frameworks and several handling frameworks. The intrusion framework is the main framework of the knowledge element, the confirm condition slot of it is described by the conditions that attached to it directly. When an intrusion type is confirmed, the confirm condition that it satisfied may partly exceeds the range of the direct condition slot, then the reasoning could search in the indirect condition slot that is at next level. When they satisfy some certain confirm conditions, the procedure may go on.

We use learning function of expert system to create or modify rules in knowledge base. By that means, we make the knowledge base updated and expanded.

2.2. Design of the reasoner

Reasoner is a software system that searches in the knowledge base, complete searching task, and get handle-method according to intrusion characters and reason rules in the knowledge base.

There are two kinds of reasoning method. One is to use heuristic knowledge to reason. It starts from the root node and makes confirm judgment according to the condition framework of the leaf nodes that are passed by, until it finds original source. The other is that if it fails to search according to the reason slot, it would reason step by step according to the direct reason slot, using knowledge of qualitative physical model and finite depth principle. These two methods are both fast and have short reasoning time. So the system has some real-time feature.

2.3. Database design

Database mainly use to store the handling suggestion of the reasoner and past handling suggestion, as well as the information like intrusion name, feature condition,

and time data that are produced by the information handler. The main function of it is to provide handling method and correlative background, so that the decision-maker can produce controlling strategy.

When the decision-maker needs information, it picks up the data from the database to add to the controlling strategy. Takes IP address of the intruder for example, after get it, decision-maker will add it to the blacklist of the controlling strategy. When the decision-maker produces a new strategy, it would pick up the current strategy from the database, and compare it with the new one to decide whether it is necessary to update the strategy of the controller or not.

2.4. Decision-maker design

When the reasoner produces a result, the decision-maker will be activated and begin to make decision. Firstly, it will combine the handling suggestion and background data to produce new controlling item, then it will compare the item with the item of current strategy to decide whether to append it or not. If appending, new controlling strategy would be produced, it would generate strategy file that are accord with the format of the controller according to the requirement of the decision-maker and send it to the controller.

2.5. Pre-handler design

The function of the pre-handler is to pre-handle the information delivered by the auditor. Pick up features of the event that provided by the audit, and make them to be condition and reason, so that the reasoner can reason according to them.

2.6. IDS design

IDS is the host system and software system that is deployed at the entrance of the network. Its function is to read the packets that pass through the network, analyze them in segment time window mode to ensure real-time feature[2]. Because it only reads and not transmits the packets, the network at this point is equal to passed through, and has no bottleneck problem. The check results of it are delivered to the export system to produce firewall strategy. The firewall, namely the controller, is responsible for the access control.

Our IDS system is based on agent system technology. The multi agent system is an ideal tool to implement distribution application in complex network environment because of its advantages of self-determination, distribution, and self-adaptation[3]. The IDS based on agent system can adapt to dynamic complex network environment automatically. It can elevate detection ability by self-learning and self-evolution, and can work corporately by utilizing network resources. We use several kinds of data mining technologies in our IDS[4]. When check the collected data, we also use it as training data to train the IDS detection model. That makes the detection model can adapt to new environment and can get the detection rules that adapt to new environment, and makes the system easier to configure.

2.7. Auditor design

Auditor is the host system and software system that is deployed at the entrance of the network. It reads and analyzes the packets in the network, and send out the auditing result in time. Like the IDS, it only reads the packets and will not produce bottleneck problem[5][6].

In auditor design we use three matured algorithms. They are association analysis algorithm, sequential pattern algorithm, and classification algorithm. We construct normal communication pattern by analyzing normal communication data to detect intrusion. And we use association analysis algorithm to discover the relationship between data items in the database records. The discovered relationship will provide important evidence to determine whole character set of audit system; use sequential pattern algorithm to discovery relationship of database records in time window. It can discovery the events sequence model appeared in database according to some event temporal relationship; use classification algorithm to map data to predefined classes. The output result of it is to produce a classifier that represented by a rule set or decision tree. It can collect the normal and abnormal audit data of related user application first, and then use classification algorithm to produce a rule set. By this mean it can predict the new audit data is belonged to normal behavior or not.

2.8. Alerter design

When the reasoner is unable to reason out completely matched result, the alerter will report this situation to the administrator and will require the administrator to deal with it initiatively. The accuracy of alert is an important index. In order to manage and control remotely, we use web browser as manage interface. The system use email, video, audio to give alert.

2.9. Design of controller

Controller is a device that accepts controlling strategy and makes effective control. The function of it is like that of the firewall. It is an independent device. It can be the firewall or proxy server. Its task is to perform the controlling strategy, isolate the controlled objects. In our system we adopt proxy server as the controller.

2.10. Design of learner

The function of learner is to append the new knowledge provided by the administrator according to

the structure of the knowledge base. Also it should implement the automatic study function by adding the handler results that produced by the pre-handler and feature conditions of the intrusion to the knowledge base.

3. Procedure of work

The flowchart of the system is shown in figure 3. The IDS and the auditor check the packets at their own analysis depth, the intrusion type and the intrusion packets would be sent to the pre-handler to pick up the features, than the packets, together with the intrusion features, would be sent to the reasoner, the reasoner search the knowledge base. If the reasoner finds the completely matched handling method, it would put the information into the database and activate the decision-maker, the decision-make would make decision according to the situation. It would compare the modified strategy with original one. If it is a new strategy, than send it to the controller; if the conditions are not completely matched, it would start the learner and adaptor to combine and optimize the matching conditions and produce new knowledge to append to the knowledge base, than make sure that the information be pass to the decision-maker to update the controlling strategy, meanwhile, alert to the administrator. If the conditions are completely not matched, alert directly, let the administrator the handle the situation.

The procedure of the system is a closed loop control system and it is good in real-time aspect. The knowledge base can be expanded during the continuously learning, that makes the distinguish ability can be elevated during using process.

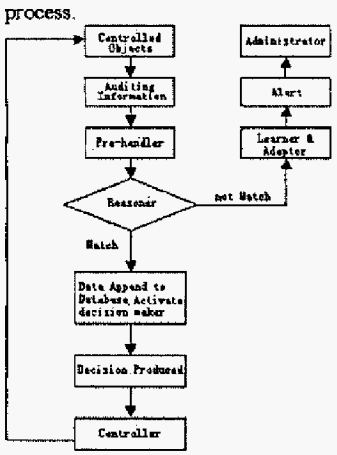

Figure 3. Flow chart of the system

4. Conclusion

The work of this article uses expert system to produce controlling strategy, makes the complex configuration of the firewall finished automatically, remarkably improves the security of the network, and integrates the function of the firewall, IDS and security audit system, makes them work together. Also, applies the closed loop control technology to the network security, makes the response of defense rapid and effective.

Reference

[1] WANG Jun-pu, Intelligent Control, Chinese Science and technology publishing house, 1996.

[2] Wenke lee and Salvatore J. Stolfo,Dat Mini Approaches for Intrusion Detection, Computer Science Departmemt, Columbia University.

[3] HE Xian-feng, HUANG Ming-di, HUANG Yu, LIU Jia fen, Intrusion Detection System Designed Based on Agent, Computer Application, 2003, 9, 42-44.

[4] HAN Jun, ZHANG Huan-guo, LUO Min, A Distributed Intrusion Detection System Based on Data Mining. Computer Engineering and Application, 2004, 8, 126-128.

[5] Giovinna Vigna, Diparti, Inspect: A Light weight Distributed Approach to Automated Audit Trail Analysis.

[6] WANG Wei-zhao, LI Cheng, LI Jia-bin, Implementation of the Network Audit System, Computer Application and Software, 2002, 11, 24-26.