Design and Implementation of intrusion detection punctual response system

Yafang Lou[1,a], Dongna Zhang[3,c], Zhe Lv[2,b]

[1, 2,3]Department of Computer Science and Technology, ZhuHai College of JiLin University, ZhuHai, 519041, China

[a,b,c]luckylou@sohu.com

Keywords: Intrusion Detection, Real-time response, Multithreading

Abstract. With the rapid development of IT technology and Internet, Network security has become an unavoidable issue, the pure firewall strategy can't satisfy the need of safe and highly sensitive departments. The network defense must adopt a deep, various means, intrusion response technology research has become a pressing matter of the moment. The system model using ACE adaptive communication environment, using object-oriented open source (OO) framework, the fusion of multi thread, XML technology developed. it has autonomous, adaptive, real-time features.

Introduction

Characteristics of information highly sensitivity and the network's own causes the network security has become an unavoidable problem. However, the pure firewall strategy can't satisfy the need of safe and highly sensitive departments. The network defense must adopt a deep, various means. Facing the continuous development today, collaborative and distributed automation mode of attack, intrusion response technology research has become a pressing matter of the moment.

The system model using ACE adaptive communication environment, using object-oriented open source (OO) framework , the fusion of multi thread, XML technology developed. The system is composed of the perception module, analysis module, response of three function module. The perception module is mainly used for identification and receiving attack information; analysis module completed the XML text into objects, judge the attack types and Strategies of Library in response to strategies for query matching function; and the response module. The introduction of SSL encryption communication protocol to realize the communication between the modules.

System design

In the past of intrusion detection response of system research and design, usually focus on the design of a system and the development of more effective new detection technology, lack of sufficient research on intrusion response, intrusion response technology far have not kept pace with the pace of development of attack technology. Most of the current intrusion response system strategy is simply to alarm management personnel, this way for a room 24 hours a day are specifically responsible for the situation can be, but is generally managers over a few hours or a few days later to obtain this information, the system may have been destroyed.

Real time response to the intrusion detection system, the framework of the ACE platform, using VC++ as the development tool to realize the. It including three modules: perception module, analysis module and the response module. Communication between the modules using network encryption communication protocol SSL implementation.

Through the above analysis, combined with business needs, this system was related to the implementation of the system, finally, through the module test, integration test, system performance testing, has achieved the anticipated target. The topological structure as shown in fig.1:

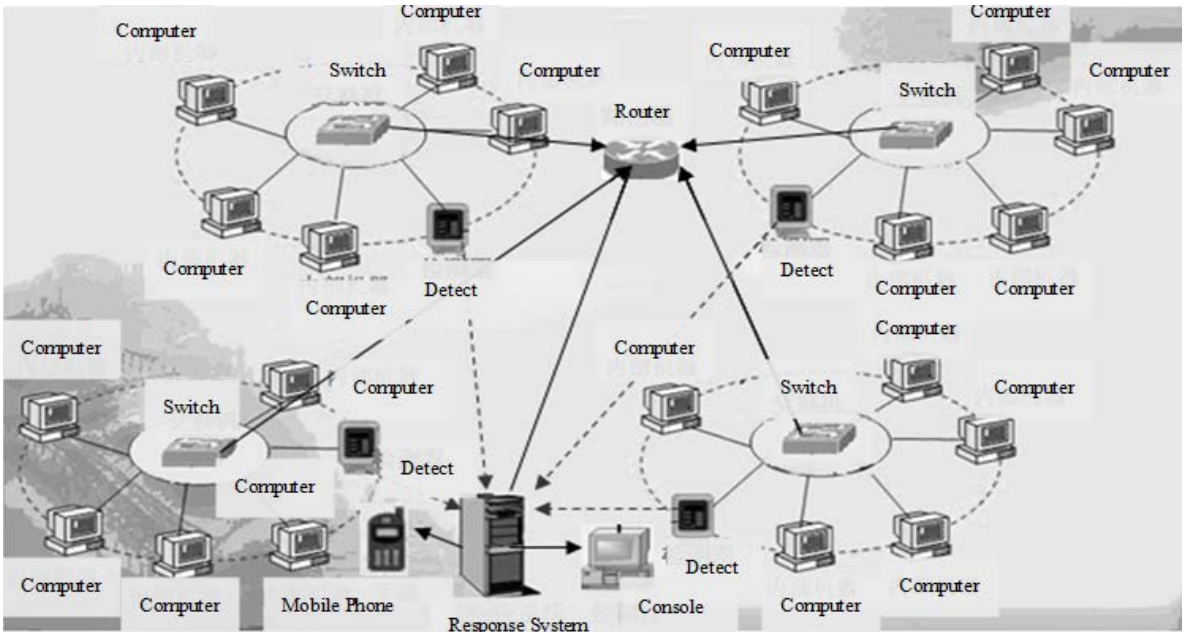

Fig.1. The intrusion detection and real-time response model

Fig.1 is a topological structure of the intrusion detection system real-time response, the topology constructed multiple subnets, multiple inter sub-network connection through the network equipment, a detector is arranged in each sub network, for the realization of the sub network attack detection function, the core of this system is to develop a intrusion detection system real-time response (a response from the server), when the response server receives the attack information report of each sub net, and after a reasonable analysis, active response (automatic response) treatment or to the console and handheld devices for alarm (passive response), through linkage with each local area network equipment, construction a network defense system, inhibit attack.

The system adopts ACE adaptive communication environment (Adaptive Communication Environment), using the object-oriented open source (OO) framework (Framework), using the core patterns for concurrent communication software, system architecture is divided into three levels: attack, attack, attack response analysis of perception. The architecture is shown in fig.2:

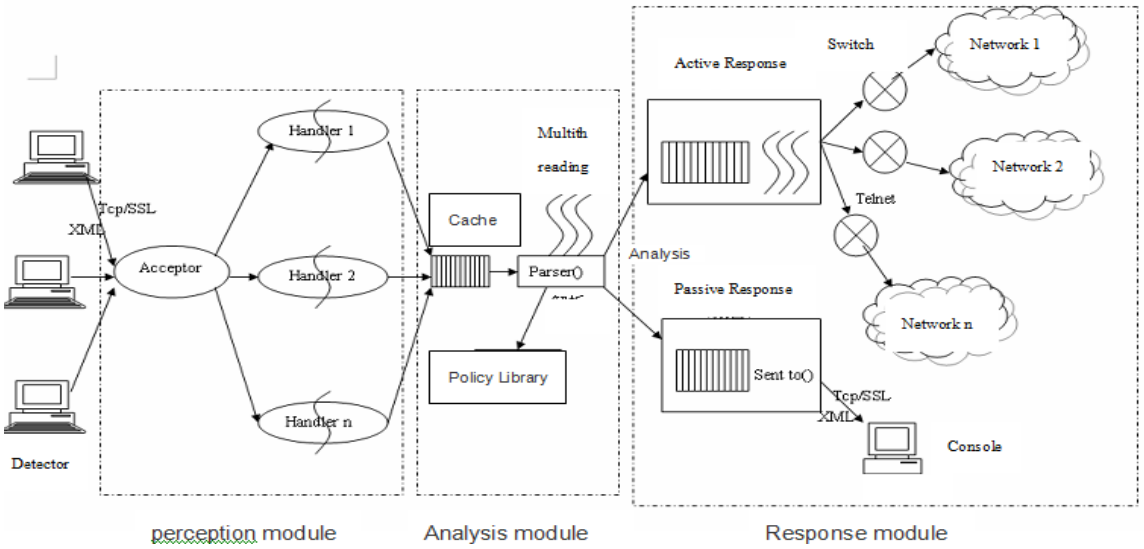

Fig.2. The architecture of intrusion detection and real-time response model

The system implementation

This system mainly realizes the real-time response of network attack, the greatest characteristic of the system is the liberation of the administrator from 24 hours tracking detection condition,

embodies the characteristics of real-time system; set a variety of response mode, make full use of the advantages of wireless communication, realizes the automatic response and alarm passive response. Characteristics of the system is real-time, automatic and so.

The perception module (Sensor Module, referred to as SM): used as perceived by the detection system detects the attack information, and receive complete data recognition. The module mainly uses the receiver in ACE (Acceptor) to listen to attack information, will be detected by the detector and attack into the system to recognize the objects, into memory, waiting for the analysis module analyzes the. Analysis module (Analysis Module, referred to as AM); according to the strategy library already exists, reasoning in a reasonable way, realize the parsing of the perception module recognition attack. The module has the XML file will be converted into object, judge the attack type and response strategy, strategy of query function in the library.

Response module (Response Module, referred to as RM): when matching response strategy analysis module to attack, take the corresponding response measures. The part of the response set two response modes: active response (automatic response) and passive response (alarm).

When the detector detects the attack information, the perception module will both sides of the communication detector and server communications by network security protocol SSL, using the receiver (Acceptor) listening detector connection request, when listening to the connection request, calling the Handler to start a new thread to receive recognition and attack information, namely, the perception module completed attack information recognition function; from the perception module recognition after the attack information, the system is put in the queue for caching, based on queue FIFO principle out attack information into the parser, the analytical solutions for the start of multiple threads to parse out the attack information, and to query matching by database administrators to customize response strategy in; according to the results of analysis, part of the attack information is put into the active response (automatic response) in the queue, by changing the network device (router / switch) access control list ACL, blocking the attacker to be the attacker's network connection, the realization of automatic response.

We select attack data sample to test the system model, select the port is 21, 80, 53, select the second, will test data into 180 time intervals, of which there are 150 time intervals for normal data, 80 interval contains attacks, the experimental results as shown in table 1:

Table 1 the test results

	Normal data	Attack	
		Known attacks	Unknown attacks
Total number of samples	150	40	40
Number Identification	142	36	34
Recognition rate（%）	94.6%	90%	85%

We can see from the experimental results, the system model for a particular host can be effective for intrusion detection and recognition.

Conclusion

Network has affected all aspects of society, pure firewall strategy can't satisfy the need of safe and highly sensitive departments. The network defense must adopt a deep, various means. Facing the continuous development today, collaborative and distributed automation attacks, intrusion response system occupy the important position in all aspects of production, life, electronic commerce, network management, plays a tremendous role, on the intrusion response technology research has become the urgent task at. It has important practical value to the research and development of this system.

References

[1] Ying zhang,hui wang. An interactive intrusion detection system [J]. Computer Engineering and Application, 2003,6(35):90-95.

[2] J.PAnderson. Computer security threat monitoring and Surveillance[R].Technical report,1980,4.

[3] Jun li,weihua li. A security vulnerability classification based on star network model [J]. Computer Engineering and Application,2002,38(7):42-44.

[4] Hanies J, Lippmann R.1999 DARPA Intrusion De-tection Evaluation[J]:Design and Procedures. USA:Ma-ssachusetts Institute of Technology,2001.

[5] Yf lou. Design and implementation of intrusion detection punctual response system[D].da lian:Da lian University of Technology,2007.

[6] D.E Denning.An intrusion detection model[J].IEEE transaction on software engineering, 1987,1(2): 222-232.

[7] Tengguo feng. Computer communication and network security[M].Beijing: tsinghua university Press.2001.