To Design an Intrusion Detection System based on Honeypot using Mobile Agent and IP Traceback Technique

Surabhi Thukral[1], Rutba Maqsood[2], Divya Upadhyay[3]

[1]Masters of Technology, Department of CSE, Amity School of Engg. & Technology
Amity University, Noida
thukralsurabhi@gmail.com

[2]Assistant Professor, Department of CSE, Amity School of Engg. & Technology
Amity University, Noida
dupadhyay@amity.edu

Abstract*: Network security technology has become crucial in protecting government and industry computing infrastructure. . In recent years, intrusion detection systems (IDSs) have demonstrated high accuracy, good generalization to novel types of intrusion, and robust behaviour in a changing environment. Still, significant challenges exist in design and implementation of production quality IDSs. There are various problems which the existing intrusion detection system models have, such as more significant network transmission load, lower detection efficiency, and limited data process ability. This paper presents an intrusion detection module based on honeypot technology, which utilizes IP Traceback technique and mobile agents. By using the mobile agents, this module has the capability of distributed detection and response. By the use of honeypot technology the intrusion source can be traced to the farthest.*

Keywords: Mobile Agents, Honeypot technology, Intrusion Detection, IP Traceback.

1. Introduction

Intrusion Detection System (IDS) [6] as an active defense strategy, intrusion detection and prevention of other safety components play an irreplaceable role. The honeypot technology as a strong complement to IDS can greatly reduce the burden of intrusion detection systems, while the greatest degree of access to information the attacker in order to facilitate further tracking the attack source. Traditional intrusion detection system is proposed based on honeypot technology, intrusion detection system can be traced back through the Mobile Agent to achieve interoperability between the various modules, the use of honeypot technology to get the maximum extent possible attack information in order to facilitate further invasion of the source tracking, and signature data to achieve timely and automatic updates.

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

Network intrusion detection system

NIDS is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap. In a NIDS, sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic. An example of a NIDS is Snort.

Host-based intrusion detection system (HIDS)

It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities and state. In a HIDS, sensors usually consist of a software agent. Some application-based IDS are also part of this category. Examples of HIDS are Tripwire and OSSEC.

Stack-based intrusion detection system (SIDS)

This type of system consists of an evolution to the HIDS systems. The packets are examined as they go through the TCP/IP stack and, therefore, it is not necessary for them to work with the network interface in promiscuous mode. This fact makes its implementation to be dependent on the Operating System that is being used. Intrusion detection systems can also be system-specific using custom tools and honeypots.

A. Development Trends

[4] Along with computer network's swift development, the network security problem is becoming more and more important. Using firewalls to protect network security is not enough, because the intruder might try to find open channels behind the firewall. Moreover, as a result of the performance limitations, the firewall cannot normally provide an effective intrusion detection capability. Intrusion detection system is a new network security technology in recent years [1, 2]. It is a combination of hardware and software and it can make up firewall's insufficiency, and provide effective intrusion detection and take necessary protective measures for the protected network [2, 3]. Intrusion detection is a new and rapidly developing area and it has become an important issue in network security [2,3]. Intrusion detection methods and products are constantly being researched and developed. Intrusion detection technology has begun to show its important value of offensive and defensive instance in the network. Host-based or network-based Intrusion Detection System is almost powerless for complex attacks. Distributed intrusion detection system can curb devastating effects of this attack.

B. Problems

Intrusion detection system must comply with the safety and integrity of the principle and parallelism Principle. Intrusion Detection System is very difficult to meet the three principles, so Intrusion Detection System still has many defects and hazards [1]:

• Intrusion detection system can't test the entire packet very well.
• Signature database updates is not timely.
• Detection method is single.• Different Intrusion Detection Systems cannot interoperate.
• Intrusion Detection Systems and other network security products cannot interoperate.

2. IDS Based On Honeypot

Honeypot is a decoy system includes vulnerabilities by simulating one or more vulnerable hosts, the attacker provide an easy target. In other words, it is designed to attract and "decoy" who designed the attacker. [5] Honeypot meaning of existence is to be detected, was offensive. If there are no attacks, honeypots will become meaningless.And firewall technology, virus protection, data encryption and authentication technologies such as passive protection technologies, honeypots is to take a proactive approach. It uses the unique characteristics to attract an attacker to lure attackers to attack its host system, while monitoring the system operation and behavior of all, and the formation of these acts recorded log. Through the log of research, analysis of attackers to the path, use the tools, tactics and purpose, can be more effective intrusion source tracing, but also can conduct real-time network intrusion forensics. Honeypot intruder obtained by information security experts can make a better understanding of the various attacks, security experts to provide a learning platform for all kinds of attacks and better protect the system should be protected. Honeypot intrusion detection system technology is a strong complement. Share a part of its data traffic and simplify the detection process, reducing the burden of intrusion detection systems. When the signature line of events and unknown events after the introduction of the honeypot, the honeypot to monitor visitors to access the action, and then determine whether the incident is unknown attacks. Determine if theaggressive behavior, while recording the attack, on the one hand to provide signatures to the signatures, the intrusion detection system in time to learn new attacks. Honeypot and intrusion detection system not only reduces the combination of traditional intrusion detection system, false negative rate and false alarm rate, but also to overcome the traditional intrusion detection system cannot monitor defect unknown attacks.

3. IP Traceback Technique

IP traceback is a name given to any method for reliably determining the origin of a packet on the Internet. Due to the trusting nature of the IP protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be falsified (IP address spoofing) allowing for Denial Of Service attacks (DoS) or one-way attacks (where the response from the victim host is so well known that return packets need not be received to continue the attack). The problem of finding the source of a packet is called the IP traceback problem. IP Traceback is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DoS attack detection. Such solutions require high numbers of packets to converge on the attack path(s).

3. IDS Based On Mobile Agents

Utilizing the object-oriented design method, the system has been divided into several sub-modules according to the system functions. The system module has concerned with acquiring data agent, pre-treating data agent, analyzing data agent, response agent, agent manager [6].

1. Acquiring data agent: It locates at the destination host, has responsibility for capturing the network packets through host network adaptor, and sending them to pre-treating data agent. It is the pivotal part of packets un-loss.
2. Pre-treating data agent: The raw data is standardized to avoid network communication bottleneck.
3. Analyzing data agent: According to different data sources (i.e. TCP, UDP, ICMP) the different analyzing data agents have been designed to execute different detection tasks. To guarantee that the analyzing data speed keeps pace with capturing data speed, the number of detection intrusion types which analyzing data agent deals with is definitive. That is to say, if a new type analyzing data agent wants to be added, the seldom analyzing data agent type will be

deleted.

4. Response agent: Distinct responses, such as creating text files, showing intrusion alarm information on the screen, cutting TCP connection are triggered aiming at distinct intrusion behaviors.
5. Agent manager: It supplies uses with visualization intrusion detection interface. It is charge of supervising the system, for example, monitoring agent condition, setting initial agent parameters and so on.

The collector is the basic unit of the intrusion detection system. The collector is charge of acquiring the data from network. The raw data format is closely related to the data source format. Therefore, after attaining the network packets, the raw data need to be filtered via event convertor in order to translate them into standard data format handled by the analyzing data agent for detecting the intrusion behaviors. The dispatching agent manager has responsible for managing all agents, such as adding the agents, dispatching the agents, deleting the agents and so on. Manager, as the system interface, has interacted with users. All detecting and analyzing tasks are completed in the mobile agent environment and with platform constraints.

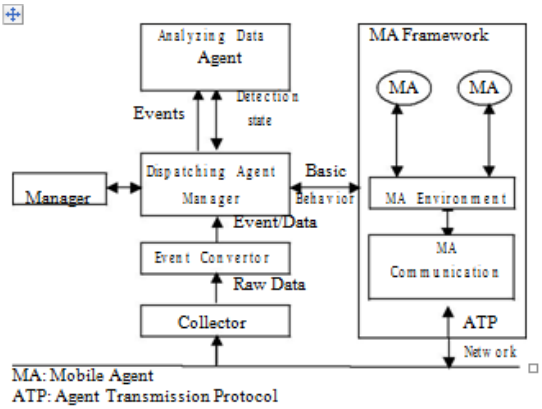

Figure 1: IDS model based on mobile agent

4. Conclusion and Future Scope

The field of computer networks is expanding rapidly, making network intrusion detection and prevention more difficult day by day. The network attacks continue to climb to new record highs every year, new methods are being sought to prevent malicious hackers from accessing private Information. Intrusion Detection System provides real time detecting and defending intrusion behaviours methods for computer security. By the use of honeypot technology combined with mobile agents and ip traceback technique we can build a complementary active defence system.

References

[1] Yixue Wang, A Sort of Multi-Agent Cooperation Distributed Based Intrusion Detection System, Modem computer,2008.
[2] Jianchun Jiang, Hengtai Ma,Dangen Ren,Network Security Intrusion Detection, Journal of Sofiware,2000.
[3] JMarin,D.Ragsdale,and JSurdu, A hybrid approach to the profile creation and intrusion detection, Proc.of DARPA Information Survivability Conference&Exposition 11,2001.
[4] Weijian Huang, YanAn, Wei Du, “A Multi-Agent-Based Distributed Intrusion Detection System, 20IO 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE).
[5] Liu Dongxia Zhang Yongbo, “ An Intrusion Detection System Based on Honeypot Technology,IEEE 2012.
[6] Wang Yu, Cheng Xiaohui, Wang Sheng, “Anomaly Network Detection Model Based on Mobile Agent, 2011 Third International Conference on Measuring Technology and Mechatronics Automation.
[7] Boukhlouf Djemaa1 Kazar Okba2,” Intrusion Detection System: Hybrid Approach based Mobile Agent”, International Conference on Education and e-Learning Innovations,2012
[8] Wattanapongsakorn,Srakaew,” A Practical Network-based Intrusion Detection and
[9] Prevention System”, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications,2012.
[10] Auttapon Pomsathit,” Effective of Unicast And Multicast IP Address Attack Over Intrusion
[11] Detection System with Honeypot,IEEE,2012.
[12] Lirnin Yin,” Research and Development of Intrusion Detection Technology,IEEE 2012.
[13] Chunfu Jia and Deqiang Chen, “Performance Evaluation of a Collaborative Intrusion Detection System”, IEEE, 2009, pp. 409-413.
[14] Jianxiao Liu and Lijuan Li, “A Distributed Intrusion Detection System Based on Agents”, IEEE, 2008, pp. 553-557
[15] Krawetz, N.(2004). Anti-honeypot technology .IEEE Security & Privacy, pp.76- 79.
[16] Liu Jianxia and Li Lijuan, “Research of Distributed Intrusion Detection System Model Based on Mobile Agent”,IEEE, 2009, pp. 53-57.
[17] Wang Hairui and Wang Hua, “Research and Design of Multi-agent Based Intrusion Detection System on Wireless Network”, IEEE, 2008, pp. 444 – 447.
[18] Wira, Z. A. Z., Ahmad, S. R. and Aziz, N. A.(2008).Deploying virtual honeypots on virtual machine monitor.International Symposium on Information Technology,(ITSim),
[19] pp. 1-5.
[20] Yu-Xin Din, Min Xiao and Ai-Wu Liu, “Research and implementation on snort-based hybrid intrusion detection system”, IEEE, 2009, pp.1414-1418.
[21] Zhang Chao. Honeynet and intrusion detection and firewall linkage techniques [J]. Technology market economy, 2007 (3): 42-44.
[22] Tao Wenlin. VMware-based virtual honeynet system research [J].Computer Application and Software, 2006,23 (5) :131-136.
[23] Zheng Junjie, Xiao Jun mold, Liu Zhihua, etc. Based on Honeypot technology, network intrusion detection system. University of Electronic Science and Technology, 2007,36 (2): 257-259 454

Author Profile

Ms. Rutba Maqsood is doing her M.Tech from Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Uttar Pradesh. She would be pursuing PHD in Computer Engineering. Her research area is Cryptography and network Security.

Ms. Surabhi Thukral is doing her M.Tech from Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Uttar Pradesh. She would be pursuing PHD in Computer Engineering. Her research area is Cryptography and network Security.

Divya Upadhyay received her M.Tech in Information Security from GGSIP University, New Delhi. Presently she is working as an Assistant Professor in CSE Department, Amity University, Noida, Uttar Pradesh, India. Her Research area includes Information Security and Security Engineering.