2011 International Conference on Computer and Automation Engineering (ICCAE 2011)
IPCSIT vol. 44 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V44.39

Research on Agent-based System of Security and Defense Cooperation

Guangping Zhou

Zhejiang University of Science and Technology

Abstract. The security of Cyberspace has also become another defense territory for countries in the world following the territory, territorial airspace and territorial sea reached by the national power and the exercise of sovereign. How to establish a powerful and effective information security system in the growing complexity of network environment nowadays has been a global major topic. With the rapid development of network technologies, extensive uses of computers and the Internet, the increasingly large size of the internal networks of units, and the increasingly complex network topological structure, the difficulty to achieve the network security has been growing constantly, posing a severe challenge to the human society. In this paper, it proposes and establishes a preliminary security defense system based on Agent collaborations.

Keywords: security; vulnerability detection; access control; defense system

1. Introduction

With the rapid expansion of global information promoted by the Internet, the computer network has become an important infrastructure which the development of the modern society depends on [1]. The security of Cyberspace has also become another defense territory for countries in the world following the territory, territorial airspace and territorial sea reached by the national power and the exercise of sovereign. How to establish a powerful and effective information security system in the growing complexity of network environment nowadays has been a global major topic. The effectiven[1]ess of security systems of networks and information also depends on their overall strain capacities [2]. With the rapid development of network technologies, extensive uses of computers and the Internet, the increasingly large size of the internal networks of units, and the increasingly complex network topological structure, the difficulty to achieve the network security has been growing constantly, posing a severe challenge to the human society [3]. The study on the Agent-based security system of integrated internal networks is the author's efforts made for facing such challenge. The securities of networks and information are combined into one unit. Roughly speaking, the network is a carrier and distribution channel of information, while information is a reason for the network to survive and service object. The securities of both are complementary. It is the same as the relationship between the power network and its delivered electricity[4]. The security management over networks and information has its own special laws of development in the management over network lines and equipment entities, in the maintenance of information sovereignty in order to guarantee secure storages and transmissions, and in the maximization of efficiencies in the use of information resources and the minimization of costs in operating networks, and has its complexities in spatial distributions, time-variations, and heterogeneous storages, etc. systems[5]. Therefore, the securities of networks and information and the designs and implementations of the defense system belong to the complex system engineering.

2. The Security Model for Agent Authentications Based on Access Controls

ID authentication as the first defensive line for information security, if a user would like to access network service resources, he must first prove his legal identity so that he can obtain the appropriate

+ Corresponding author. Tel.: + 86 571 8507 0318; fax: +86 571 8507 0759.
E-mail address: zhouzhou@zust.edu.cn.

authorization, in which it solves the question that "Who am I" [6]. The basic objective of access controls is to prevent unauthorized accesses to information resources, so that the system can be used within the legitimate scope: determining what users can do, also determining what the programs on behalf of certain users' interests can do [7]. The access control achieved in this paper is the network access control, which dynamically forms and ap`plies filtering rules for host data packets in accordance with users' related roles and related permissions acquired after their logins, and ultimately achieves the mechanism to control users' access to networks through forwarding controls over the logged users' data packets. The ID authentication in this paper is implemented by the use of the software Agent, which integrates functions of users' ID authentications and access controls [8].

2.1. The Basic Concept of Access Control

Object: stipulating the resource that needs to be protected, also known as Target. The object in CINSS is protected network resource, such as the print service, file service, and OA service, etc. Subject: or known as Initiator, is an active entity, stipulating the entity that can get access to the object (usually referred to the procedures implemented by users or on behalf of users). The subject in CINSS is the user, also known as Supplicant [9]. Authenticator: an organization determining whether to allow the user to get access to the object according to his possessed permission [10]. It is actually an organization between the subject and the object. The authenticator in CINSS is to authenticate Agent; it adopts the method of access controls to implement the host user's authorization of network resources, the specific implementation of which is to transfer the authenticator from the network accession equipment to the terminal client computer, thus it is also known as Network Access Control Agent (NAC Agent); this model is called as Agent-based Network Access Control (ABNAC). Authorization: stipulating the action (such as reading, writing, and executing or rejecting accesses) that can be implemented on the resource. In CINSS, the user is authorized to use the appropriate resources based on his level. The basic mode of access controls is shown as in Figure 1.

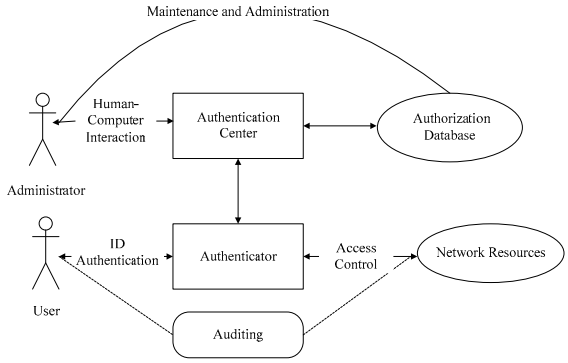

Fig. 1: The basic mode of access controls

The formalization of the access control strategy as an intermediate stage between the definition of strategy and the implementation defines the formal model representing the strategy, and can be used to define and prove security properties. After proving the security of the model and accurately implementing this model, the system can be confirmed to be secure. Access controls mainly include Discretionary Access Control (DAC) and Mandatory Access Control (MAC).

2.2. Access Control List

In the actual system, the number of subjects and objects is relatively large; the use of a matrix to implement large amounts of system resources to be consumed by the access control mechanism and the demand of careful management over the creation and deletion of a subject and an object increase the complexity for implementations. The sparse matrix is a more common situation, that is, a large number of entries in the matrix are empty, or take the same default configuration. The transformation of an access control matrix is to store all sequences represented by objects. In this way, each object is associated with a set of the same sequences and each sequence contains a subject and a set of permissions, and then the specified subject can use these permissions to get access to the associated object.

3. Implementations of Network Access Controls

3.1. Coarse-grained Access Controls

Coarse-grained network access controls need to control the sending and receiving of data packets. ARP packets are filtered prior to TCP/IP packets; if ARP packets are blocked, TCP/IP packets will be surely blocked, and the host will be completely isolated from the network. PARP and PUP packets are defaulted to be blocked. General software firewalls never filter ARP packets, but only target at TCP/IP packets; whereas network access controls have to consider ARP packets, the reasons for which will be elaborated in subsequent section.The actual situation in which is: as long as the ARP packets that have passed authentications, or have overtime authentications or are being authenticated, ARP packets can pass; in other situations they will be blocked. Overtime authentications indicate the host has not found the control center, and the user is using the home network, thus the host is not monitored. The sensor of the Authentication Agent can prevent the situation from occurring through loop detections that the user intentionally unplugs the network cable and then plugs in C1N. The dynamic protective measures of CINSS prevent the user from using other software firewalls to block special packets used for authentications, to ensure the Authentication Agent will not be deceived.

When driver packets implement network access controls, it has to been determined whether they have passed authentications, or have overtime authentications or are being authenticated. After the sensor and the message processor of the Authentication Agent (working + user modes) obtain the statuses of authentications, they transmit the information to the driver. To this end, two pairs of control codes are defined and described as below:

IOCTL XPACKET PASS ALLPACKETS:

All host packets that are being authenticated are released. The released packets also need to be determined whether authenticate host packets.

IOCTL XPACKET BLOCK ALLPACKETS:

All host packets that fail in authentications or are transmitted when the net is blocked, including ARP packets, are blocked.

IOCTL XPACKET AUTHEN PASS:

All host packets that have passed authentications, or have overtime authentications are released.

IOCTL XPACKET AUTHEN DENY:

Under the status of being authenticated, packets that are not specially used for authentications are denied.

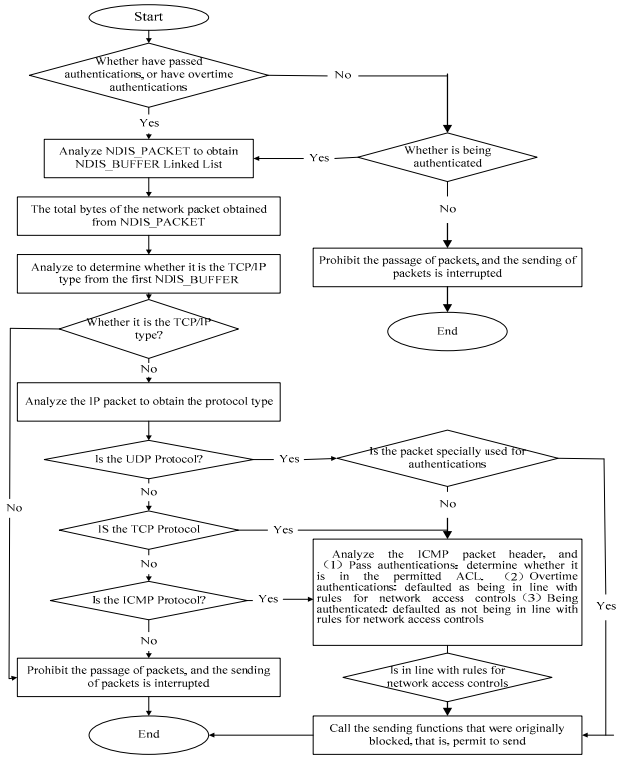

Fig. 2: Procedures of network access control over sending packets

3.2. Fine-grained Access Controls

The fine-grained network access controls analyze the packet headers of HTTP, FTP and other application layer protocols, and determine whether to block the data based on the eigenvalues of reading and writing. Application layer protocols are communicated by sockets, so it uses the SPI technology that can filter all socket communications to achieve this function. SPI is introduced into Winsock 2 to achieve the transparence of service providers; it can send all socket requests to the SPI program through writing this program to complete calling, which is a program under the user mode. SPI supports two service providers: transmission service providers and name-analysis service provider, while the fine-grained mode uses only the former.

When an application program calls the socket (Ws232.d11), Winsock will call the corresponding function of the lower-level transmission service provider. For instance, when an application program calls the Send (WSA Send), Winsock will call the WSP Send of SPI. Hence, as long as several important networking functions are intercepted, it can control the high-level application protocols. The system has provided the SPI that has completed data transmissions, so there is no need to re-implement the function of this part in one's own SPI, as long as one's own SPI program is hooked to the SPI program of the system, which is the above-mentioned Hook technology.

The Agent is impossible to be implemented without the operating system, so the security of Agent is greatly threatened by the security of the operating system and the host user; the host user may intentionally or unintentionally unload or destroy the operation of Agent, the threat of which is very difficult to prevent. Static protections for the Agent essentially can be summarized as protections for files, processes and registration tables. Among them, the process concealing technology can ensure processes not to be "killed" by the task manager. The method of creating remote threads can also ensure processes to be operated. While the Authentication Agent uniformly applies the method of driving programs to protect files, processes and registration tables. It adopts the technology of file filtering drivers to protect files, and adopts the HOOK NTDLL technology to protect processes and registration tables. These technologies are collectively referred to as the kernel reinforcement of the operating system.

Take Windows 2000 file filtering drivers for instance to explain how to protect files of the Authentication Agent. Its main objective is by setting the security access rules independent of security configurations of the system to conduct necessary repairs on the kernel of the file system to avoid or reduce damages from malicious users and codes to Agent files in maximal limitation. The Windows 2000 its own discretionary access control mechanism is unable to achieve the above-mentioned objective, because the damages to the Agent are often conducted by the users that have mastered the system administrator's permissions, whereas the problem can only be solved by transforming the file operations from discretionary access to mandatory access control. It uses the technology of file filtering drivers to implement the location of the mandatory access control module in the file system. Before the request of the user-mode programs arrives at the driver of the file system, it is intercepted by the access control filtering driver. The left arrow indicates the defaulted operation process of the operating system; after the filtering driver is embedded, its process is shown as the right arrow. When application programs communicate with the upper-level system service, the system service sends an order to the file filtering driver, and the latter in accordance with the process permissions of the current dialogs in the system compares with the access control permissions of the files to be operated to determine the dialog user's subsequent actions. In fact, except the uninstall program of Authentication Agent privately owned by the network administrator of CINSS (different from the administrator of the operating system), no other program can delete, modify or rename it. Herein, the object is the Authentication Agent, and the subject is the process. The program is defined to be uninstalled by the subject that has the permission to uninstall. The technology actually implements rules for protecting files or the table of contents: prohibit reading, writing / deleting / renaming and prohibiting getting access.

By reinforcing the security of the operating system kernel, it can effectively achieve static protections for the Authentication Agent. However, for malicious users that want to evade monitoring, it can be implemented by reinstalling the operating system or by means of setting the software firewall to prevent the Authentication Agent from communicating with the control center. The former is because the Authentication Agent is considered as an application program; although its core is various kinds of drivers, it has to rely on

the operating system to achieve its function; the latter is because the communication of the Authentication Agent with the outside world is the message communication based on the TCP/IP protocol, while the software firewall supporting users to define can prevent such communication effectively. The non-controlled node is of such case. Therefore, a method that can dynamically discover the non-controlled node is proposed innovatively to promote users to correct such wrong actions, which is under the premise based on the fact that software firewalls can not filter ARP packets.

Once the Authentication Agent is installed properly, after the operating system is started, it will run forever until the shutdown. Therefore, a simple method to determine whether the Authentication Agent is correctly installed in the host is: by sending an encrypted packet to the appropriate host node, if the node has a corresponding response, the node is considered as a controllable node. There is a problem here that if the host does not respond, it can not prove this is certainly a non-control node, for it may be a dead node. A dead node refers that an IP is not occupied by an active host, or the Authentication Agent of the host occupying the IP fails to be authenticated or the net is closed causing the host cannot be detected. The converse concept is called as an active node. Therefore, it has to first determine whether an IP is an active node, and then send an authentication packet to the IP; if there is any response, the node must be a controlled node; otherwise it must be a non-controlled node. The technology for determining whether an IP is a dead node belongs to the IP Detection (IP Scanning) Technology, which is the basis of network intrusions; most of literatures discuss how to prevent IP detections, only a few of them discuss how to implement detections. The traditional methods of IP detections include ICMP echo, TCP connect, TCP SYN, TCP FIN, and TCP ACK. These methods are of low efficiencies; except the ICMP method, other methods all need to be conducted port tests one by one, all of which cannot penetrate the well set software firewalls. The above-mentioned defects are not existed in the ARP protocol, which is of high efficiency; consequently it is used as the protocol for IP detections.

4. Conclusion

In this paper, it uses the host packet filtering technology of the software firewall to implement the ID authentications and role-based network access controls, and the above functions are encapsulated as the Authentication Agent. Hence, the normal operation of the system depends on that each host in the network must be installed with the Authentication Agent. The Authentication Agent as a software may be damaged by users intentionally or unintentionally, therefore CINSS has to protect it, which is a software self-protection technology. Meanwhile, internal users can still avoid being authenticated to get access to networks without any authorization, by means of carrying a new computer, or reinstalling the operating system, etc. means; consequently, it must monitor the execution environment of the Authentication Agent, and proactively identify and prevent such type of security issues. In addition, hackers or viruses infect the host through vulnerabilities, so it shall integrate the vulnerability detection system and by detecting vulnerabilities in the hosts assess their levels of security risks, as well as isolate the high-risk hosts from networks to achieve defenses in advance for hosts and networks. The security audit or the other security software is encapsulated as a mobile Agent in order to be sent to each node in the network to complete the corresponding security tasks when needed, thereby achieving customizable security strategies. Security tasks are completed through collaborations among various Agents, accordingly the security issue of communications is very important; it can easily make use of hash values of relevant users' login passwords as keys, and then the secure communication mechanism based on the symmetric encryption algorithm is realized.

5. Reference

[1] M.V. Clark, M. Shafi, W.K. Kennedy and L.J. Greenstein. Machine learning for information extraction in information domains. *IEEE Trans. Veh. Technol.*, 1994, 43(1):47-56.

[2] M.V. Clark, M. Shafi, W.K. Kennedy and L.J. Greenstein. Visual Web information extraction with Lixto. *IEEE Trans. Commun.* 1992, 40(6):1128-1135.

[3] M.V. Clark, L.J. Greenstein, W.K. Kennedy and M. Shafi. XWRAP: An XML-enabled wrapper construction system for Web information sources . *PIMRC '92, Conference Proceedings*. IEEE Communications Society, Boston Massachusetts, 2002.

[4] D.L. Noneaker and M.B. Pursley. COMIIX:Towards effective WEB information extraction,integration and query answering. *IEEE Trans. Veh. Technol.,* 43(4): 997–1005.

[5] J.H. Winters. Accordion summarization for end-game browsing on PDAs and cellular phones. *IEEE J. Select. Areas Communic., ,* 2001.

[6] J.H. Winters. Database techniques for the World-Wide Web: A Survery. *ICC '94,* 2008.

[7] J. Salz and P. Balaban. XHTML 1.0:The extensible hypertext markup language. *IEEE Trans. Communic.,*2004, 40(5):885–894.

[8] J. Salz and P. Balaban. The Object Database Standard ODMG-93 1994. *IEEE Trans. Communic.,* 2005, 40(5): 895–907.

[9] R.D. Gitlin, J. Salz and J.H. Winters. Machine Learning. *IEEE Trans. Commun.,* 2003, 42(4):1740–1751,.

[10] J. Salz and J.H.Winters. Professional HTML. *IEEE Trans. Veh. Technol.,* 2002, 43(4):1049–1057.