Network Intrusion Protection System Using Rule-based DB and RBAC Policy

Min Wook Kil [1], Si Jung Kim [2], Youngmi Kwon [3], Geuk Lee [4]

[1] Dept. of Computer & Image Information, Mun Kyung College, Mun Kyung, South Korea
mwkil@mkc.ac.kr

[2] Informatiom Technology Center, Chungju National University, Chungju, South Korea
kimsj@chungju.ac.kr

[3] Dept. of InfoCom, Chungnam National University, Daejeon, South Korea
ymkwon@cnu.ac.kr

[4] Security Engineering Research Center, Hannam Univ., DaeJeon, South Korea
leegeuk@hannam.ac.kr

Abstract. Role-Based Access Control (RBAC) is a method to manage and control a host in a distributed manner by applying the rules to the users on a host. This paper proposes a rule based intrusion protection system based on RBAC. It admits or rejects users to access the network resources by applying the rules to the users on a network. Proposed network intrusion protection system has been designed and implemented to have menu-based interface, so it is very convenient to users.

1 Introduction

The purpose of RBAC policy is to protect the computing and transmission resources from being updated, exhibited or destructed caused by the unprivileged access[1]. And the purpose of the intrusion protection system is to protect the network resources from the access of outside users and usually it is located on the local network server[2].

Basically the firewall operates closely related to the router program. It tests the network packets, decides whether it receives the packets or not, and filters some packets. The firewall works interactively with the proxy server whose role is to resolve the requests to the network on behalf of users, or it rather includes the role of proxy server in itself [2]. The firewalls are generally used in the corporation or the public organizations to filter the access from specific user(s) or host(s). But, it is not used in some specific purposed network such as proprietary PC room or Internet cafe.

Because buying a firewall of private security enterprise costs some price and needs some person to operate it. On the other hand, using the freeware based on Linux OS such as ipfwadm, ipchains and iptables [3] is too difficult for non-experts to configure the filtering-policies properly.

Intrusion Protection System (IPS) has mixed characteristics of firewall and Intrusion Detection System. This paper design and implement the IPS based on RBAC method. It provides easy configuration interfaces to the operator. Additionally, it costs down the security tool and makes it easy for the operator to administrate the users on hosts.

In Section 2, we review the related works with RBAC method and network based Intrusion Protection System. And the efficiency of resource management is addressed under the condition that the RBAC is applied to the intrusion protection system. In Section 3, we designed the RBAC based Intrusion Protection System and in Section 4, we show the implementation-related items. Section 5 is the conclusion.

2 Related Works

2.1 RBAC Method

The basic concept of RBAC is to prohibit the information resources of company or organization from an unauthorized user. In RBAC, the access authority is given to the roles and each user is imposed on a proper role. If some user is imposed on some role, that user can access the minimum subset of total resources properly for that role [4]. This approach of authority management has some advantages: it simplifies an administration of a system security, and provides flexibility for a company to implement its specific security policy of its own.

Three DBs are necessary for the operation of RBAC. They are shown in Figure 1. In Operations-DB, the usage and execution authorities of the processes and resources are defined. They are used to decide whether a user or system daemon can use the resources or not. Roles-DB classifies the Operations-DB records according to the roles. And the third DB, Users-DB defines the roles permitted to each users.

The processes of ❶ from Operations-DB in Figure 1 are to add the combined and classified Operations-DB records to the Roles-DB. The processes of ❷ are to assign an authority based on Roles-DB to the system users. This process makes the management of user's authority very simple by distributing the responsibility of administrator management to each user.

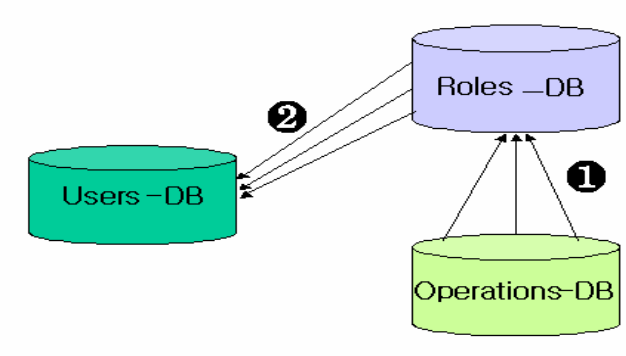

Fig.1. The necessary DBs in RBAC operation

2.2 The Definition of IPS

The IPS is one of the network components to protect the internal networks from the attacks initiated from the outside networks. The IPS uses policies to protect the internal information from incoming or updating by the unauthorized attack. It can be a type of software and/or hardware. It is an active protection process to prohibit from incoming of illegal traffics and permit only the authorized traffics [5]. The purpose of the IPS is an blocking of illegal external attack, preventing the loss, destroy and change of internal information from non-trusted user and hackers through Internet, and helping internal information to be provided to the outside safely.

IPS is located in the rear section of router generally. It permits or denies the forwarded packets to the router by analyzing and comparing with filter-rules.

3 The Design of RBAC-based IPS

3.1 Operational Steps

We made the operational steps of RBAC-based IPS as in Figure 2. The first operational step is to collect all the packets going through its own network by set the Network Interface Card to promiscuous mode.

Figure 2 shows the procedures of RBAC-based Network Intrusion Protection System while the dummy hubs are used in the network. In procedure ❶ , host A transmits a request packet to access to the illegal site or program. Or host A may transmit a packet to reply to backdoor client programs in the remote site. Anyway, transmitted packet from host A is forwarded to the hub and router to go to the external networks. Simultaneously the transmitted packet is broadcasted to the other hosts in a internal network. When host B receives that packet, it discards it silently because it is not

destined to MAC address of itself. But, host X is running a Intrusion Protection System with a promiscuous mode. So host X accepts all the packets going through the local network. In procedure ❷, RBAC-based Network Intrusion Protection System verifies the packets based on the predefined roles and sends an "ICMP Protocol Unreachable" message to the host A when the packets violate the Roles. These roles are stored in RBAC-based DBs in the form of rules. When host A receives an ICMP message, it conceives that there is some trouble or erroneous status at a host which has requested a connection. Therefore, host A notifies that situation the remote host. Procedure ❸ shows that host A ignores the request packets from the erroneous host afterwards.

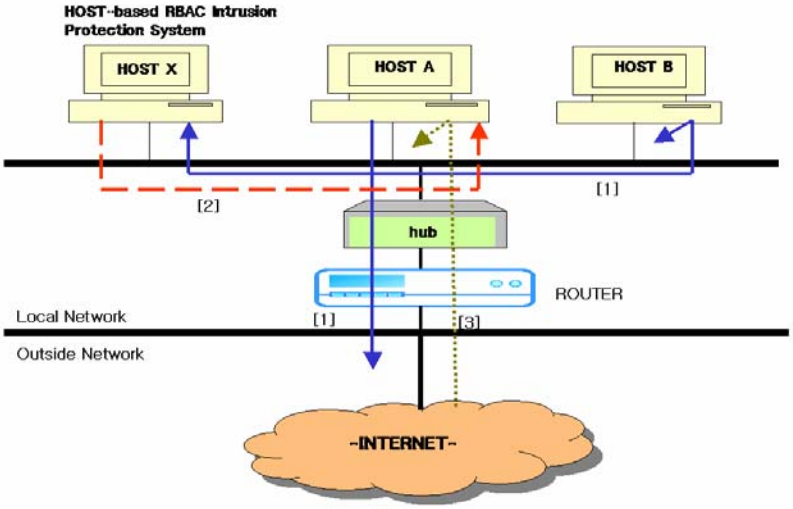

Fig.2. Operational steps in RBAC-based IPS

And for the switch-based network environment, RBAC-based Intrusion Protection System uses an arp-spoofing capability to forward the packets that is going to the router to itself. Forwarded packets are verified based on the Roles, which was established in the IPS. If the verification is failed, IPS sends an "ICMP Protocol Unreachable" message to the host A. Then that host A processes an ICMP message as a normal response. The difference with dummy hub environment is that host A doesn't receive any remote packet from outside network because the reply packet transmitted from host A didn't go out to the outside world actually. Applying these procedures, RBAC-based Network Intrusion Protection Systems can restrict the usage of network resources based on the predefined Roles and assign a specific privilege to the hosts in the inner network.

3.2 Logging and Scheduling

The logs on the logging can be classified into three: site-log, program-log and backdoor-log. Site-log stores the list of illegal sites and domains. Program-log has information of non-permitted network programs. And backdoor-log is used as a backdoor protection log. The Log information filtered by RBAC in filtering module helps an network administrator find out the status of network resources.

4 Implementation of RBAC-based IPS

RBAC-based Intrusion Protection System is implemented on the Linux OS. Figure 3 and 4 shows the implemented command window of RBAC-based IPS. An administrator specifies the IP addresses of Managed Resources and the range of subnets for the managed ports in a file. Then the parsing module of IPS reads and parses the contents of a predefined file and filters all the packets by monitoring and capturing based on the policies of RBAC. Figure 3 is a window showing the definition of check items of packet filtering and Figure 4 is one of the active shots of RBAC-based Intrusion Protection System.

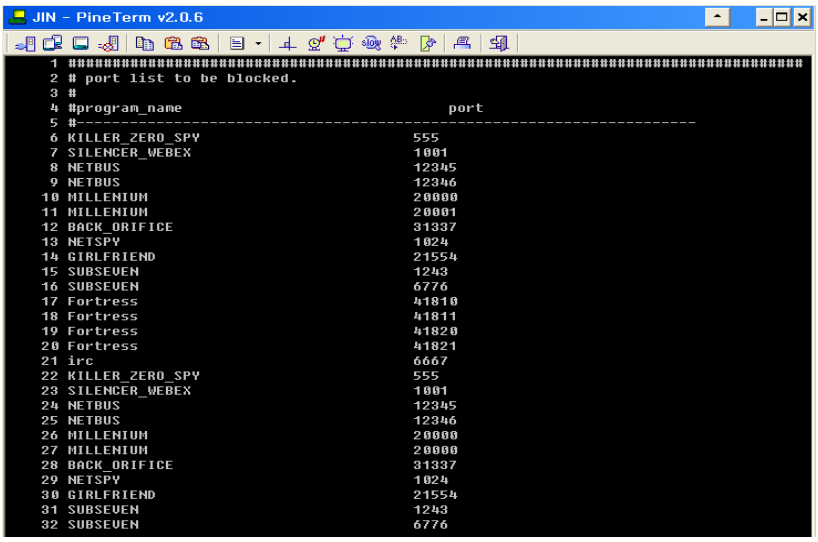

Fig.3. Managed Port Information Table of RBAC-based IPS

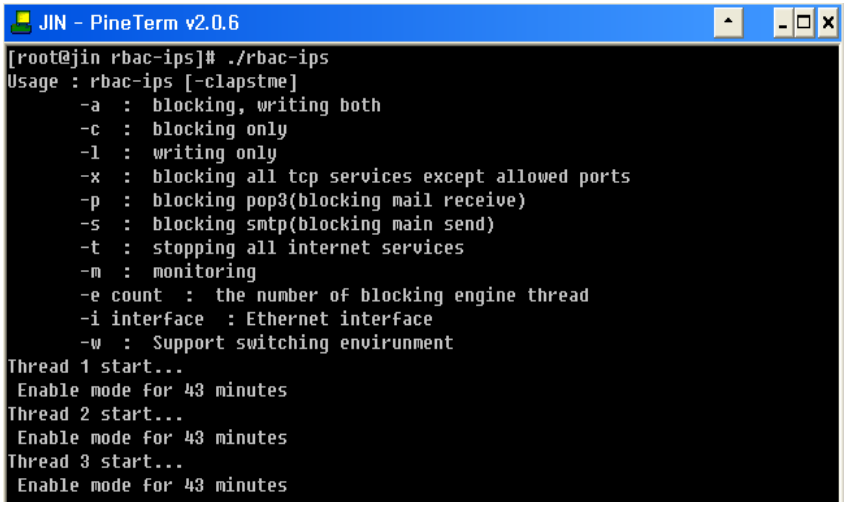

Fig.4. Menus and active shot of RBAC-base IPS

5. Conclusions

This paper designed and implemented an Intrusion Protection System, which manages hosts based on the predefined roles by applying the roles to the hosts in a network, not by applying the roles to the individual users. RBAC-based Intrusion Protection System has an advantage that it can be applied in one of the hosts as well as in the router in a network. Implemented IPS also includes the function of collecting the packets in a switched network using an arp-spoofing method. Additionally, proposed Intrusion Protection System has an effective filtering capability only by applying the predefined roles to the Hosts-DB instead of establishing the complex packet filtering rules by users.

Its application area is the companies, proprietary PC rooms or Internet café that requires security settings for the individual hosts to restrict the network resources.

Though we use an arp-spoofing technique to collect in the switched network environment, it can be a burden to the network. So the further study to lessen the load of arp packets would be required.

Acknowledgement

This work was supported by a grand No.R12-2003-004-02003-0 from Korea Ministry of Science and Technology.

References

1. Ravi S. Sandhu, et al, “Role-based Access Control Model,” IEEE Computer, no.2, vol. 29, 1996.
2. Charlie Kaufman, et al, Network Security: Private Communication in a Public World, Prentice Hall PTR, 2002.
3. Olaf Kirch, et al, Linux Network Administrator’s Guide, O’REILLY Press, 2000.
4. Suk Kyun Oh and Seong Ryeol Kim, “ A Design of RBAC_Linux for the Linux Security System,” The Journal of Korea Society Industrial Information Systems, no. 4, vol. 4, 1999.
5. http://www.terms.co.kr, Dictionary of Computer Terms.
6. Craig Hunt, TCP/IP Network Administration, O’REILLY Press, 2000.
7. David Ferrailo, et al, “Role-based Access Control,” Proceedings of 15th National Computer Security Conference, 1992.
8. Jean Bacon, et al., “A Model of OASIS Role-based Access Control and its Supports for Active Security,” ACM Transaction on ISS, no. 3, vol. 5, 2003.
9. Ravi S. Sandhu, et al, “Decentralized User-Role Assignment for Web-based Intranets,” Proceedings of 3rd ACM Workshop on Role-based Access Control, 1998.