Policy-based Network Security with Multiple Agents (ICCAS 2003)

Hee-Suk Seo*, Won-Young Lee**, and Mi-Ra Yi***

* School of Information & Communication Engineering, Sungkyunkwan University, Seoul, Korea
(Tel : +82-31-290-7221; E-mail: hisstone@hanmail.net)

** School of Information & Communication Engineering, Sungkyunkwan University, Seoul, Korea
(Tel : +82-31-290-7221; E-mail: sonamu@ece.skku.ac.kr)

*** School of Information & Communication Engineering, Sungkyunkwan University, Seoul, Korea
(Tel : +82-31-290-7221; E-mail: miracle@ece.skku.ac.kr)

Abstract: Policies are collections of general principles specifying the desired behavior and state of a system. Network management is mainly carried out by following policies about the behavior of the resources in the network. Policy-based (PB) network management supports to manage distributed system in a flexible and dynamic way. This paper focuses on configuration management based on Internet Engineering Task Force (IETF) standards. Network security approaches include the usage of intrusion detection system to detect the intrusion, building firewall to protect the internal systems and network. This paper presents how the policy-based framework is collaborated among the network security systems (intrusion detection system, firewall) and intrusion detection systems are cooperated to detect the intrusions.

Keywords: policy-based framework, network security, modeling, collaboration.

1. INTRODUCTION

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter [1]. The explosive growth in computer systems and their interconnections via networks has increased the dependence of both organization and individuals on the information stored and communicated using these systems. The intruder can powerless the target network by the simple manipulation though he doesn't understand the special knowledge and technique about the network. Attacker very easily attacks the target system by Distributed Denial of Service tool. But the incident harmed the image of the company and the company losses in a finance.

The Distributed Intrusion Detection System (DIDS) uses a combination of host monitors and local area network monitors to monitor system and network activities with a centralized director aggregating information from the monitors to detect intrusions. It is similar to our agent system for intrusion detection and countermeasures in that it uses multiple monitors and artificial intelligence algorithms to determine the severity of events. The Computer Immunology project explored designs of intrusion detection systems that can effectively detect and defined intrusion in a network computer system in a manner similar to the immune system in animals. One portion of the project researched a method that could provide a component of an immune system for computers. They developed a sense of self for privileged programs by creating a database of normal and abnormal system call traces for instances of execution of the programs.

This paper presents how the policy-based framework [2,3] is collaborated among the network security systems (intrusion detection system [4,5], firewall [6]). Policy-based network management provides a means by which the administration process can be simplified and largely automated. The IETF has defined a policy framework consisting of management interfaces for entering policies, repositories for storing policies, policy decision points (PDPs) for evaluating policies, and policy enforcement points (PEPs) for enforcing policy decisions.

Section 2 shows the backgrounds and section 3 presents the network systems. Section 4 describes the Distributed agent of PB framework and finally conclusion is presented.

2. BACKGROUNDS

2.1 PB framework

The methodology of policy-based network management was developed within the IETF in the context of the Integrated Services model, where it was proposed to use a policy framework for the management of admission control to reservations of network resources. Policy-based framework is constructed into four main components: policy management application, policy repository, policy decision point (PDP), and policy enforcement point (PEP), as shown in Fig. 1.

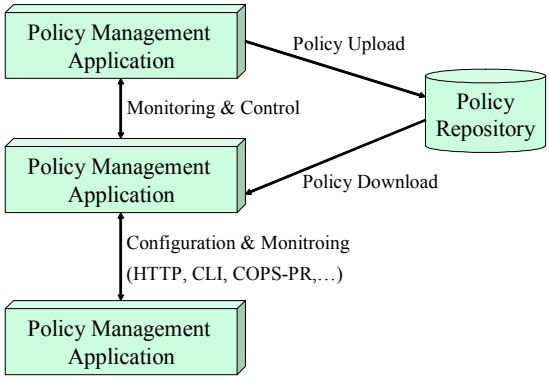

Fig. 1 IETF policy framework

An administrator uses the policy management tool to define the policies to be enforced within the network. A device that can apply and execute the different policies is known as the policy enforcement point. The policy repository is used to store the policies generated by the management tool. In order to ensure interoperability across products from different vendors, information stored in the repository must correspond to an information model specified by the Policy Framework Working Group. A policy enforcement point uses an

intermediary known as the policy decision point to communicate with the repository. The policy decision points responsible for interpreting the policies stored in the repository and communicating them to policy enforcement point. The policy enforcement point or policy decision point may be in a single device or different physical devices. Different protocols are to be used for various parts of the architecture (e.g., Common Open Policy Service (COPS) or Simple Network Management Protocol (SNMP) can be used for PDP-PEP communication). A repository could be a network directory server accessed using Lightweight Directory Access Protocol (LDAP).

2.2 DEVS

The Discrete EVent system Specification (DEVS) formalism [7,8] is a theoretically well grounded means of expressing hierarchical, modular discrete-event models. In DEVS, a system has a time base, inputs, states, outputs, and functions. The system function determines next states and outputs based on the current states and input. In the formalism, a basic model is defined by the structure:

$$M = < X, S, Y, \delta_{int}, \delta_{ext}, \lambda, t_a >$$

where X is an external input set, S is a sequential state set, Y is an external output set, δ_{int} is an internal transition function, δ_{ext} is an external transition function, λ is an output function and t_a is a time advance function. A coupled model is defined by the structure:

$$DN = < D, \{M_i\}, \{I_i\}, \{Z_{i,j}\}, select >$$

where D is a set of component name, M_i is a component basic model, I_i is a set of influences of I, $Z_{i,j}$ is an output translation, select is a tie-breaking function. Such a coupled model can itself be employed in a larger coupled model. Several basic models can be coupled to build a more complex model, called a coupled model

3. NETWROK SYSTEM

3.1 PB framework architecture

Fig. 2 shows the architecture of policy-based framework. Policy-based framework is composed of Network component. Network Component has four modules: security model, intrude model, network devices, and policy-based system.

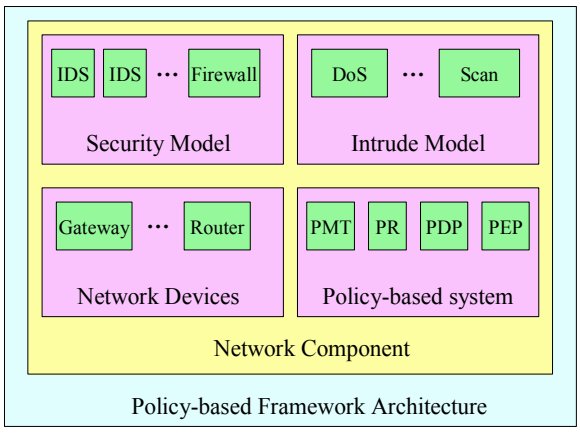

Fig. 2 Policy-based framework architecture

IDS in the security model plays a vital role in network security in that it monitors system activities to identity unauthorized use, misuse or abuse of computer and network system. An intrusion detection system is also an automated auditing mechanism. Like auditing systems, it consists of three parts: agent, director, and notifier. The agent corresponds to the logger. It acquires information from a target (such as a computer system). The director corresponds to the analyzer. It analyzes the data from the agents as required (usually to determine if an attack is in progress or ah occurred). The director then passes this information to the notifier, which determines whether, and how, to notify the requisite entity. The notifier may communicate with the agents to adjust the logging if appropriate.

An agent obtains information from a data source (or set of data sources). The source may be a log file, another process, or a network. The information, once acquired may be sent directly to the director. Usually, however, it is preprocessed into a specific format to save the director form having to do this. Also, the agent may discard information that it deems irrelevant. The director itself reduces the incoming log entries to eliminate unnecessary and redundant records. It then uses an analysis engine to determine if an attack (or the precursor to an attack) is underway. The analysis engine may use any of, or a mixture of, several techniques to perform its analysis. Because the functioning of the director is critical to the effectiveness of the intrusion detection system, it is usually run on a separate system. This allows the system to be dedicated to the director's activity. It has the side effect of keeping the specific rules and profiles unavailable to ordinary users. Then attackers lack the knowledge needed to evade the intrusion detection system by conforming to known profiles or using only techniques that the rules do not include. The notifier accepts information from the director and takes the appropriate action. In some cases, this is simply a notification to the system security officer that an attack is believed to be underway. In other cases, the notifier may take some action to respond to the attack. Many intrusion detection systems use graphical interfaces. A well-designed graphics display allows the intrusion detection system to convey information in an easy-to-grasp image or set of images. It must allow users to determine what attacks are underway (ideally, with some notion of how likely it is that this is not a false alarm). This requires that the GUI be designed with a lack of clutter and unnecessary information.

Firewall in the security model provides a way to restrict access between the Internet and the internal network. It enforces the network security policy, allowing only approved services to pass through and those only within the rules set up for them. It is classified into the proxy and packet filtering. Proxy is a program that deals with external servers n behalf of internal clients. Proxy clients talk to proxy servers, which relay approved client request on to real servers, and relay answers back to clients. Proxy services are specialized application or server programs that take user's request for Internet services (such as FTP and Telnet) and forward them to the actual services. The proxies provide replacement connections and act as gateway to the services. A proxy client is a special version of a normal client program that talks to the proxy server rather than to the real server out on the Internet; in some configuration, normal client programs can be used as proxy clients. The proxy server evaluates requests from the proxy client and decides which to approve and which to deny. If a request is approved, the proxy server contacts the real server on behalf of the client (thus the term proxy) and proceeds to relay requests from the proxy client to the real server, and responses from the real server to the proxy client. A device in the packet filtering takes to selectively control the flow of data to and from a network. Packet filters allow or block packets, usually while routing them from one network to

another (most often from the Internet to an internal network, and vice versa). To accomplish packet filtering, you set up a set of rules that specify what types of packets (e.g., those to or from a particular IP address or port) are to be allowed and what types are to be blocked. Packet filtering may occur in a router, in a bridge, or on an individual host. It is sometimes known as screening. Packet filtering devices that keep track of packets that they see are frequently called stateful packet filters (because they keep information about the state of transactions). They may also be called dynamic packet filters because they change their handling of packets dynamically depending on the traffic they see. Devices that look at the content of packets, rather than at just their headers, are frequently called intelligent packet filters. In practice, almost all stateful packet filters also are capable of looking at the contents of packets, and may are also capable of modifying the contents of packets.

Intrude model generates the intrusion related packets. DoS in the intrude model generates the denial of service (DoS) packets. DoS attack is a form of usurpation, although it is often used with other mechanisms to deceive. The attacker prevents a server from providing a service. Scan techniques provide valuable information for attackers, including employee names and phone numbers, IP address ranges, DNS servers, and mail servers [9].

Present-day IP networks are large complex systems consisting of many different devices. Representative devices are bridge, hub, router, and gateway. Gateway potentially operates in all seven layers of the Open Systems Interconnection (OSI) model. A gateway is a protocol converter. A router by itself transfers, accepts, and relays packets only across networks using similar protocols. A gateway can accept a packet formatted for one protocol and convert it to a packet formatted for another protocol before forwarding it [10].

The management of network infrastructure is difficult and complex with the growth of the Internet. In an era of increasing technical complexity, it is becoming difficult to find trained personnel who can manage the new features introduced into the various servers, routers and security systems. Policies are collection of general principles specifying the desired behavior and state of system. Policy-based network management provides a means by which the administration process can be simplified and largely automated.

3.2 SES of PB system

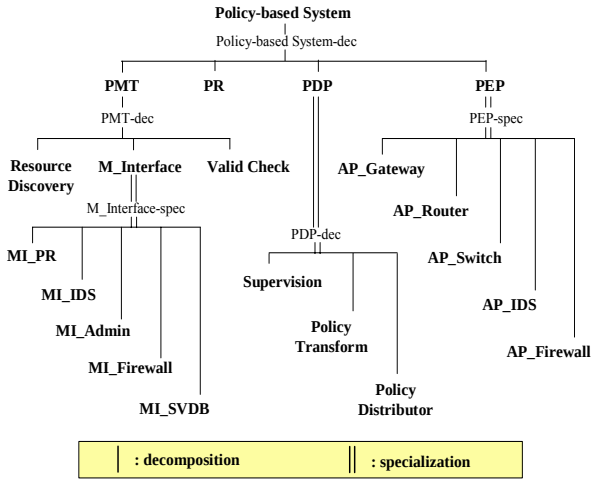

Fig. 3 SES of PBS

The System Entity Structure (SES) [11] is a knowledge representation scheme that combines the decomposition, taxonomic, and coupling relationships. The entities of the SES refer to conceptual components of reality for which models may reside in the model base.

Fig. 3 presents the structure of the Policy-based System. Policy-based System is decomposed into four sub-components: PMT, PR, PDP, and PEP model. PMT model is decomposed again into Resource Discovery, M_Interface, and Valid Check model. M_Interface model is specialized into MI_PR, MI_IDS, MI_Firewall, and MI_Admin model. PDP model is decomposed into Supervision, Policy Transform, and Policy Distributor model. PEP model is specialized into five sub-components: AP_Gateway, AP_Rotuer, AP_Switch, AP_IDS, and AP_Firewall model.

4. DISTRIBUTED AGENT OF PB FRAMEWORK

4.1 Network security system

Each agent cooperates through the BBA [12-14] for detecting intrusions. Blackboard in BBA is hierarchically structured shard working memory through which the agents coordinate by writing and reading the information relevant to detecting the intrusion. The hierarchy in blackboard is set according to Joseph Barrus & Neil C. Rowe [15]. They proposed Danger values to be divided into five different levels. These five blackboard levels are Minimal, Cautionary, Noticeable, Serious and Catastrophic. We classified blackboard levels into five levels for both host attack and network attack based on these divisions. Each agent communicates by two types of messages. One is the control messages, the other is the data messages. The control messages are used to communicate between agents and controller and the data messages are required to send data between agents and blackboard.

To begin with, the blackboard levels for the Host-Attack case are presented. This case is for the detection of attacks to a single host within the network of concern. In this case the attacked host inserts the intrusion related information to the Host-Attack area of the blackboard. Each agent must request the permission by sending a BB_update_request message to the controller in order to manage consistency and contention problems. The controller sends a BB_update_permit message to the agent that is capable of handling the current problem. The agent which receives this message writes (BB_update_action) the intrusion related information to blackboard. After updating is done, the agent sends the BB_update_completion message to the controller. Controller sends a BB_broadcasting_of_action_request message for reporting this event to other IDSs. IDSs, which have received the necessary information from blackboard, send the BB_information_acquisition_completion message to the controller. The blackboard levels transit according to these steps. When the blackboard level is at Serious level, the agent adds the source IP address to the blacklist of the Firewall model, then all packets coming from these sources are blocked.

Next, the blackboard levels for the network attack case are presented. The network attack is defined as some hosts out of the network hosts are attacked. In this case the attacked hosts insert the intrusion related information to the Network-Attack area of the blackboard. As a host is attacked, the blackboard level transits in the Host-Attack area of the blackboard. When the blackboard state is at the Host-Attack and any other host is attacked, the blackboard state is the Network-Attack. The

Minimal, Cautionary, Noticeable, Serious and Catastrophic levels of Network-Attack are for representing the case when multiple hosts are attacked. For example, the Cautionary level of the Network-Attack is defined in a way that at least two hosts are at the Cautionary level of the Host-Attack area. A host is at the Cautionary level of the Host-Attack and other host which starts to be attacked transits a Minimal level to a Cautionary. Then whole network is at the Cautionary level of the Network-Attack area. The message transmission mechanism of the Network-Attack area on the blackboard is basically similar to that of the Host-Attack area. When the blackboard level is at Noticeable level of the Network-Attack area in the composed simulation environment, then attacker's packets coming from attack point are blocked to protect the network. Continuing the attack when the blackboard level is at the Serious level of the Network-Attack area, all packets coming from the network are prevented from the damaging the network. With these responses the network administrator can set the security configuration of the whole network or a specific host and prevent the attacker from damaging the network. The subdivided levels of the blackboard can cope effectively with the attacker and enhance the sensitivity of the intrusion detection.

4.2 Solving the problem with blackboard

This section presents the transition procedure of each blackboard level and response to the transition [16]. As example, the transitions of the blackboard for jolt attack case are shown. The levels of the blackboard are divided by threshold values. Threshold values are selected according to the following contents.

• the policies of the network administrator and system security level : the administrator can enforce the system security configuration to protect the network system. In this case threshold values can be a little low.
• network speed and configuration environment : threshold values can be varied by the network speed and configuration environment. Namely threshold values of network, support the high speed network environment, can be a little higher than relatively low speed. And a case of having many internal processes in a local host is a little higher than many networking processes.
• system performance (CPU : Central Processing Unit, memory, etc.) : threshold values of system, has a fast CPU speed, can be a little higher than relatively low. A memory isn't different from a CPU.
• operating system types : threshold values, the security levels are enforced in OS, can be a little higher than those not.
• attack types : threshold values can be varied according to the attack types

The below contents explains the problem soling process of the jolt attack.

1. Host A is attacked so the blackboard level reaches at Minimal level of Host-Attack area. The blackboard level transits from the initial Passive state to the Minimal level of the Host-Attack area.
2. Continuing the attack of the intruder, threshold value reaches at the value of the Cautionary level. Then the level of the blackboard transits to the Cautionary level Host-Attack area.
3. Also the attack is continued, the level of the blackboard transits from Cautionary level to the Noticeable level of the Host-Attack area.
4. The blackboard level is at the Noticeable level now and the attacker continually sends many intrusion packets to the network. As a result the blackboard level transits to the Serious level of the Host-Attack area. If the blackboard level reaches at the Serious level of the Host-Attack area, the controller transfers attacker's information to Firewall model. Using this mechanism all packets coming from the Internet to the host A are blocked to protect the host A.

4.3 Network security system and PB system

Policies are interpreted by automated manager agents and so the behavior of the agents can be modified dynamically by changing policy rather than recording. We use the term "agent" to refer to an automated component which detects the intrusion and reports to the policy-based framework. The policies thus provide a constrained form of programming of automated agents to change management strategy without shutting down the management system. As management activities can have a drastic impact on the system being managed, it is important to determine and resolve policy conflicts so that the automated management is able to perform correctly. The polices can also apply to humans, for example the roles related to a collaborative software development team.

The intrusion detection system and firewall system, being the major components of network security, collaborate to enhance the security level. If intrusion detection system detects the intrusion through blackboard architecture, its agent modifies the security policy of the firewall with policy-based framework. So that the intrusion packets detected by intrusion detection system can be prevented.

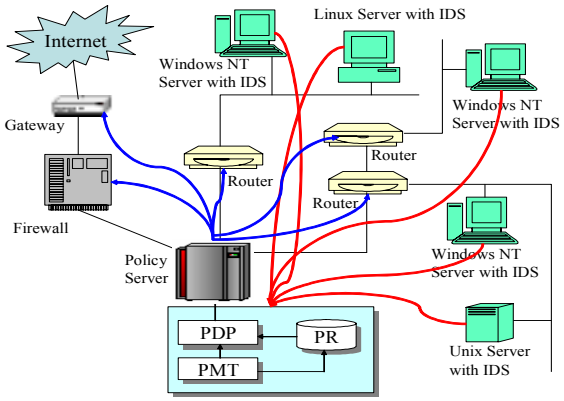

Fig. 4 Network security with PBF

Fig. 4 depicts the collaboration of the network security system with the policy-based framework. PMT of the common policy-based framework is accessed by the network administrator but our system is accessed by the network administrator and intrusion detection. The function is important to the security systems since the automated security management system is very effective to protect the network components. The PEP (policy server) is the component that actually encounters the packets and is responsible for enforcement and execution of policy actions. It is collocated with the packet-forwarding component of an access router or network server. The PDP is the component responsible for determining which actions are applicable to which packets. The PDP interprets policy rules for one or more PEPs based on information contained in data or signing packets, current network condition, as well as dynamic information such as a

account balances, dynamic allocated addresses. As an example, the PDP could decide whether a specific reservation request the originator of the request. A PEP may query the PDP to make decisions on its behalf on the occurrence of specific events, such as the arrival of a new reservation request or a data packet. The policy repository is the location where the policies defined for the domain are stored. The repository may be located in a single physical site within the policy domain, or it may be replicated at several devices. The repository could be a database, a flat file, an administrative server, or a directory server.

5. CONCLUSION

Vulnerabilities and bugs of information systems are often exploited by malicious users to intrude into information systems and compromise security (e.g., availability, integrity, and confidentiality) of information systems. As information systems become increasingly complex, vulnerabilities and bugs of information systems are inevitable for technical and economic reasons. Hence, the possibility of intrusions into information systems always exists. In order to protect information systems, it is highly desirable to detect intrusive activities while they are occurring in information systems. When an intruder attacks a system, the ideal response would be to stop his activity before he can do any damage or access sensitive information. This would require recognition of the attack as it takes place in real time. There are few automated methods to perform this recognition. Some methods are applied manually by human observation by explicitly looking for the attack as a result of previous analysis or due to some triggering event of suspicious behavior, probably recognized by blind luck. The proposed system has an advantage of the management. The administrator can easily apply the policies to the network components (network devices and security system) with the policy-based system. The security system makes a various network situations-the policies should be applied to change the network states. These situations include the response of intrusion detection system and policy change by the firewall, etc. Policy-based framework supports the automatic and flexible environment for changing the network situation.

REFERENCES

[1] S. Malik, *Network Security Principles and Practices*, Cisco Press, 2003.

[2] D.C. Verma, "Simplifying network administration using policy-based management," *Network, IEEE*, Vol. 16, pp. 20-26, 2002.

[3] P. Martinez, M. Brunner, J. Quittek, F. Strauss, J. Schonwalder, S. Mertens, and T. Klie, "Using the script MIB for policy-based configuration management," *Network Operations and Management Symposium*, PP. 187-202, 2002.

[4] R. Bace, *Intrusion Detection*, Macmillan Technical Publishing, 2000.

[5] H.S. Seo, T.H. Cho, "Simulation of Network Security with Collaboration among IDS Models," *Lecture Notes on Artificial Intelligence, Springer Verlag, LNAI* 2256, pp. 438-448, Dec. 2001.

[6] E. D. Zwicky, S. Cooper and D. B. Chapman, *Building Internet Firewalls second edition*, O'reilly & Associates, 2000.

[7] B.P. Zeigler, H. Praehofer, and T.G. Kim, *Theory of modeling and simulation: Integrating discrete event and continuous complex dynamic system*, San Diego: Academic Press, 2000.

[8] H.S. Seo, T.H. Cho, and S.D. Chi, "Modeling and Simulation of Distributed Security Models," *Lecture Notes on Computer Science, Springer Verlag, LNCS* 2660, pp. 809-818, Jun. 2003.

[9] J. Scambray, S. McClure, and G. Kurtz, *Hacking Exposed second edition*, McGraw-Hill, 2001.

[10] B.A. Forouzan, *TCP/IP*, McGraw-Hill, 2000.

[11] H.S. Seo, T.H. Cho, "An application of blackboard architecture for the coordination among the security systems," *Simulation Modelling Practice and Theory, Elsevier Science B.V.*, Vol. 11, Issues 3-4, pp. 269-284, Jul. 2003.

[12] G. Van Zeir, J. P. Kruth and J. Detand, "A Conceptual Framework for Interactive and Blackboard Based CAPP," International *Journal of Production Research*, Vol. 36(6), pp. 1453-1473, 1998.

[13] K. Decker, A. Garvey, M. Humphrey and V. R. Lesser, "Control Heuristics for Scheduling in a Parallel Blackboard System," *International Journal of pattern Recognition and Artificial Intelligence*, Vol. 7, No. 2, pp. 243-264, 1993.

[14] G. M. P. O'Hare and N. R. Jennings, *Foundation of Distributed Artificial Intelligence*, John Wiley & Sons Inc., 1996.

[15] J. Barrus and N. C. Rowe, "A Distributed Autonomous-Agent Network-Intrusion Detection and Response System," *Proceedings of Command and Control Research and Technology Symposium*, Monterey CA, pp. 577-586, Jun. 1998.

[16] H.S. Seo, T.H. Cho, "Modeling and Simulation for Detecting a Distributed Denial of Service Attack," *Lecture Notes on Artificial Intelligence, Springer Verlag, LNAI* 2557, pp. 179-190, Dec. 2002.