The Design of Router Security Management System for Secure Networking

Su-Hyung Jo*, Ki- oung Kim*, and Sang-Ho Lee**

* Secure Operating System Research Team, Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea
(Tel : +82-42-860-5499; E-mail: shjo@etri.re.kr, kykim@etri.re.kr)
**School of Electrical and Computer Engineering, Chungbuk National University
(Tel : +82-43-261-2253; E-mail: shlee@chungbuk.ac.kr)

Abstract: A rapid development and a wide use of the Internet have expanded a network environment. Further, the network environment has become more complex due to a simple and convenient network connection and various services of the Internet. However, the Internet has been constantly exposed to the danger of various network attacks such as a virus, a hacking, a system intrusion, a system manager authority acquisition, an intrusion cover-up and the like. As a result, a network security technology such as a virus vaccine, a firewall, an integrated security management, an intrusion detection system, and the like are required in order to handle the security problems of Internet. Accordingly, a router, which is a key component of the Internet, controls a data packet flow in a network and determines an optimal path thereof so as to reach an appropriate destination. An error of the router or an attack against the router can damage an entire network. This paper relates to a method for RSMS (router security management system) for secure networking based on a security policy. Security router provides functions of a packet filtering, an authentication, an access control, an intrusion analysis and an audit trail in a kernel region. Security policy has the definition of security function against a network intrusion.

Keywords: Router Security, Security Management

1. INTRODUCTION

A rapid development and a wide use of the Internet have expanded a network environment. Further, the network environment has become more complex due to a simple and convenient network connection and various services of the Internet.

However, the Internet has been constantly exposed to the danger of various network attacks such as a virus, a hacking, a system intrusion, a system manager authority acquisition, an intrusion cover-up, DoS attack and the like. Thus, infringement of the Internet is being increased, and the growing damage and influence thereof affect public institutions, social infrastructures and financial institutions.

As a result, a network security technology such as a virus vaccine, a firewall, an integrated security management, an intrusion detection system, and the like are required in order to handle the problems of Internet security.

Accordingly, a router, which is a key component of the Internet, controls a data packet flow in a network and determines an optimal path thereof so as to reach an appropriate destination. An error of the router or an attack against the router can damage an entire network. Moreover, since the router is a device for managing traffic between an internal network and an external network or between different networks, the security thereof is indispensable, thereby requiring a security technology for controlling an access to the router and an illegal network intrusion.

A conventional method of a network security is mainly implemented based on an individual security system having a single function, so that it is difficult to achieve internetworking between security systems and construct an information security infrastructure.

This paper relates to a method for RSMS (router security management system) for secure networking based on a security policy. Security router provides functions of a packet filtering, an authentication, an access control, an intrusion analysis and an audit trail in a kernel region. It is capable of detecting a network intrusion and coping with an illegal network intrusion in real time. Security policy[1] has the definition of security function against a network intrusion.

Section 2 describes related works that are policy-based network management and COPS [2]. Section 3 describes the router security management system. Section 4 describes GUI of the router security management system. Finally, section 5 summarizes this paper.

2. RELATED WORKS

Policy is the rule how to make use of network. Network is automatically operating by network manager s policy. Policy defines bandwidth, latency, priority, access control, authentication, and authorization. It has two contexts which are condition and action. If condition is satisfied, then perform action. Policy Decision Point (PDP) is server, and Policy Enforcement Point (PEP) is client. Local Policy Decision Point (LPDP) can be used by the device to make local policy decisions in the absence of PDP. PDP receives policy and translates it into format applicable to target. PDP makes policy decisions based on policy conditions and configures target to enforce policy such as access list, priority queue related to packet address. PEP sends requests, updates, and deletes to the remote PDP. PDP returns decisions to the PEP.

Common Open Policy Service (COPS) is defined in IETF standard RFC 2748. It is a simple query and response protocol that can be used to exchange policy information between a policy server and clients such as routers, switches, load balancers, and so on. COPS is describing policies and transferring and negotiating them around the network or among devices. If either the server or client is rebooted or restarted, the other would know about it quickly. COPS protocol uses a reliable TCP transport and provides an efficient transport of attributes and an efficient and flexible error reporting.

COPS has two common models, outsourcing model and

configuration model. Outsourcing model is used to provide for the outsourcing of policy decisions for RSVP [3]. It is defined in RFC 2749. PEP requires an instantaneous policy decision and external policy server (PDP) makes decisions. Another usage is for the configuration or provisioning model [4]. It is defined in RFC 3084 and used to be providing or configuring policy. PDP may proactively provision the PEP reacting to external events.

COPS provides message level security for authentication, replay protection, and message integrity. COPS can also reuse existing protocols for security such as IPsec or TLS to authenticate and secure the channel between the PEP and the PDP.

COPS open sources are COPS stack 1.4.0 by Vovida.org [5] and COPS Client Software Development Kit 3.1 by Intel [6]. Vovida.org is a communications community site dedicated to providing a forum for open source software used in telecom environments. COPS stack is developed in C++. The stack is compliant with RFC 2748 and implements all of the functionality outlined in RFC except the support for IPv6 addressing scheme. In addition, the stack also contains implementation of COPS-PR. Intel implements COPS and provide open source of cops. COPS Client SDK is available as open source, but COPS Server SDK is available under a restricted license and not open source.

3. DESIGN OF ROUTER SECURIT MANAGEMENT S STEM

The security router includes a policy server for determining a filtering policy, an intrusion detection policy and an access control policy that are required for detecting and blocking an intrusion into a network. It also includes an access control engine block (AAEB) for preventing an unauthorized user and allowing an authorized user to access to the system in response to an application of the access control policy. Security router has a packet filtering engine block (PFEB) for receiving an allowed packet and denying a disallowed packet in response to the application of the filtering policy. It has an intrusion detection engine block (IDEB) for analyzing and coping with the intrusion into the network in response to the application of the intrusion detection policy.

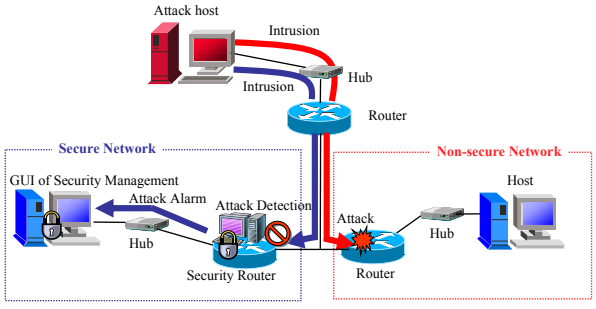

Fig. 1 Schematic diagram of security router

Figure 1 shows a schematic diagram of the security router for blocking an intrusion from an attack system. There is illustrated a secure network including a security router. An attack host attempts to attack the secure network and a non-secure network. Then, the security router in the secure network detects and blocks a network attack by applying a filtering policy and an intrusion detection policy and then informs the security management system of the attack. While the secure network can block the intrusion, the non-secure network cannot block any intrusion, so that a general router cannot perform a routing to a host.

Since only security manager has an authority to modify routing table information of a router, even if an unauthorized user discovers a password of a root by using a sniffing program and acquires a root authority, it is impossible to modify the routing table. As a result, the security of the router can be enhanced.

The condition and the action of the packet filtering policy are as following.

* Condition
  - Priority
  - 5-tuple (Source IP, Source Port, Destination IP, Destination Port, Protocol)
  - Start Time / End Time
  - ICMP Type, ICMP Code
* Action
  - Drop / Accept

5-tuple is source IP address, destination IP address, source begin and end port, destination begin and end port, and protocol. IP has 32bit address and mask address or Any type. Any means IP of packet doesn t care. Protocol is Any type, TCP, UDP, and ICMP. Any means the protocol of packet doesn t care. Time means duration of policy lifetime. The priority classifies the order of adapted policy. So each policy has his own priority, that security router drops the whole packet of A-subnet except one IP.

Router security management system (RSMS) has policy server, policy DB, COPS client, and time controller. Figure 2 is the architecture of RSMS. Policy server stores the policy at DB and enforces the security policy to security router. The security policies are packet filtering policy, intrusion detection policy, trusted channel policy, and access control policy. The security policy is exchanged by COPS protocol. The policy is encoded by BER, because of security. After decoding the policy, it is stored at GDBM (GNU Database Management) database. GDBM makes efficient search of policy and light-weight database.

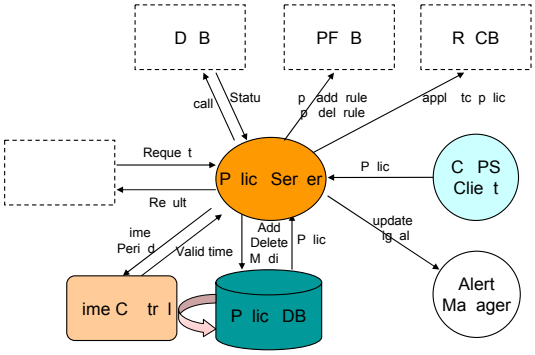

Fig. 2 Architecture of router security management system

If the policy time is NONE , then it means that the policy is installed immediately. If the policy time is 20050708T120000/20050709T120000 , then it means that the policy will be installed at noon 8 July 2005, and will be removed at noon 9 July 2005. Time controller checks the time of policy periodically. It compares the current time with policy time. If current time is between start time and end time of policy, the policy is installed. After end time is over, the policy is removed.

Figure 3 shows a detailed flowchart for describing an operating process of the security router for detecting and coping in real time with an intrusion from the attack system.

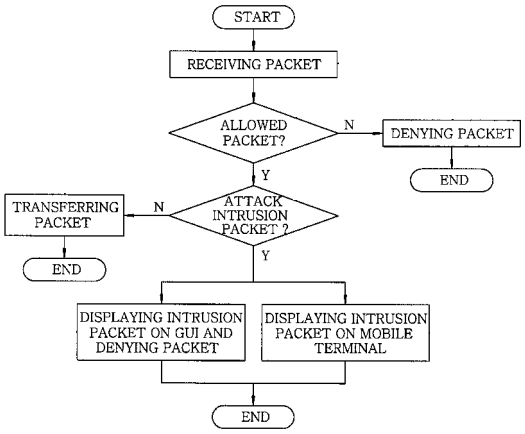

Fig. 3 Flowchart for Operating Process of Security Router

A process for security router is including the steps of (a) receiving a packet from an attack system and examining the packet according to a filtering policy, (b) checking whether the packet is allowed or not, based on the examination result of step (a), (c) passing the packet if the packet is allowed in the step (b) and checking whether or not the allowed packet is an attack intrusion packet according to an intrusion detection policy, and (d) in case the packet is the attack intrusion packet in the step (c), displaying the attack intrusion packet on the GUI of security management system.

Figure 4 presents a detailed flowchart for illustrating a procedure of a security management based on a security policy applied between a router having the security router and the router security management system.

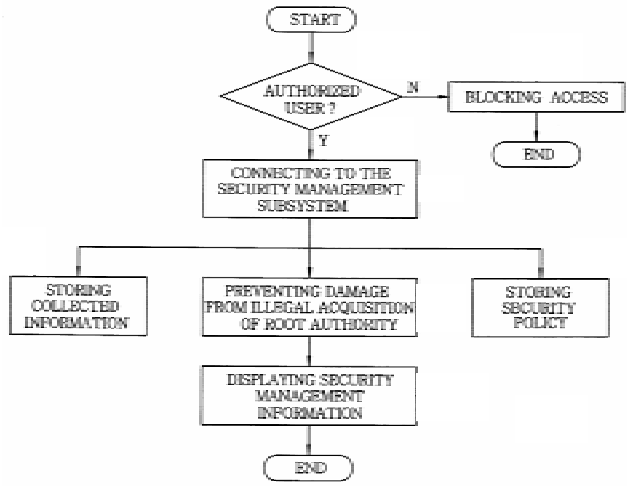

Fig. 4 Flowchart for Operating Procedure of Router Security Management System

Another process for providing an integrative security management by using a security policy applied between a security router and a security management system, the method comprising the steps of (a) checking whether or not a user is authorized through a user registration and authentication process, (b) if the user is authorized in step (a), allowing a user to access to the security management system, collecting information on a network composition of hosts, gateways, and routers and storing the collected information in a network database, and (c) displaying security management information on the GUI of security management system.

4. GUI OF ROUTER SECURIT MANAGEMENT S STEM

Figure 5 shows the packet filtering policy of the router. Source IP is 10.3.1.2 and destination IP is 10.4.1.2. All packet of input tcp packet of eth0 interface are accepted if the destination port is between 1 and 23, and the flags are ACK, PSH, S N flags.

Fig. 5 GUI of Packet Filtering Policy

5. CONCLUSION

A router is managing traffic between an internal network and an external network or between different networks, the security thereof is indispensable, thereby requiring a security technology for controlling an access to the router and an illegal network intrusion.

Security router provides functions of a packet filtering, an authentication, an access control, an intrusion analysis and an audit trail in a kernel region. It is capable of detecting a network intrusion and coping with an illegal network intrusion in real time.

Router security management system is managing security router with security policy, which is the definition of security functions against a network intrusion.

REFERENCES

[1] IETF Policy Working Group http://www.ietf.org/html.charters/policy-charter.html

[2] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry, The Common Open Policy Service

Protocol: RFC 2748, January 2000.
http://www.ietf.org/rfc/rfc2748.txt
[3] S. Herzog, J. Boyle, R. Cohen, D. Durham, R. Rajan, A. Sastry, COPS Usage for RSVP, January 2000.
http://www.ietf.org/rfc/rfc2749.txt
[4] K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. avatkar, and A. Smith, COPS Usage for Policy Provisioning: RFC 3084, March 2001.
http://www.ietf.org/rfc/rfc3084.txt
[5] Vovida.org, http://www.vovida.org/
[6] Intel COPS SDK
http://www.intel.com/labs/manage/cops/
[7] B. Moore, Policy Core Information Model (PCIM) Extensions: RFC 3460, January 2003
http://www.ietf.org/ rfc/rfc3460.txt
[8] R. Sahita, Framework Policy Information Base: RFC 3318, March 2003
http://www.ietf.org/ rfc/rfc3318.txt