Integrated Security Management Framework for Secure Networking

Su-Hyung Jo*, Jeong-Nyeo Kim*, Sung-Won Sohn**

* Secure Operating System Research Team, Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea
(Tel : +82-42-860-5499; E-mail: shjo@etri.re.kr, jnkim@etri.re.kr)

** Network Security Research Division, Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea
(Tel : +82-42-860-5072; E-mail: swsohn@etri.re.kr)

Abstract: Internet is exposed to network attacks as Internet has a security weakness. Network attacks which are virus, system intrusion, and deny of service, put Internet in the risk of hacking, so the damage of public organization and banking facilities are more increased. So, it is necessary that the security technologies about intrusion detection and controlling attacks minimize the damage of hacking. Router is the network device of managing traffic between Internets or Intranets. The damage of router attack causes the problem of the entire network. The security technology about router is necessary to defend Internet against network attacks. Router has the need of access control and security skills that prevent from illegal attacks. We developed integrated security management framework for secure networking and kernel-level security engine that filters the network packets, detects the network intrusion, and reports the network intrusion. The security engine on the router protects router or gateway from the network attacks and provides secure networking environments. It manages the network with security policy and handles the network attacks dynamically.

Keywords: Secure Networking, Security Management

1. INTRODUCTION

Networking environment is growing rapidly as Internet makes quick progress and popularization. Internet has easy and useful network access and various Internet services, so Internet has the complicated structure. Network attacks which are virus, system intrusion, and deny of service, put Internet in the risk of hacking, so the damage of public organization and banking facilities are more increased. IDS [1, 2] is a next generation security solution that minimizes the damage of hacking, in case a firewall fails in the isolation of intrusions, and responds the intrusion dynamically.

IDS has three types that are Network based IDS (N-IDS), Host based IDS (H-IDS) and Hybrid IDS. N-IDS is installed in network nodes and analyzes the packet from network nodes. N-IDS has some advantages which are OS independence and the low cost of operations and installation, compared with H-IDS. H-IDS is installed in the server which wants to monitor the network. It monitors the system log files stored by an audit and system call in the operation level. But H-IDS is difficult to implement and has the high cost of setup, compared with N-IDS. The limits of IDS are the false positive rates of misuses, the process of encryption packets and the hacking by a roundabout way. New advanced filtering technology and rules, updated by well known patterns, are needed to reduce the rates of misuses.

The core of networking, which is router, controls the flow of data packets and decides the optimal path as packet destination. Router is the network device of managing traffic between Internets or Intranets. The damage of router attack causes the problem of the entire network. So, the security technology about router is necessary to defend Internet against network attacks. Router has the need of access control and security skills that prevent from illegal attacks.

We developed an integrated security management framework for secure networking. It provides kernel-level packet filtering, intrusion detection, audit trail, authentication and access control. An integrated security engine on router or gateway resolves the network attacks. It manages the network with security policy [3] and handles the network attacks dynamically. This paper is organized as follows. Section 2 describes related works that are policy-based network management and COPS [4]. Section 3 designs the architecture of security management framework. Section 4 describes the implementation of security management framework. Finally, section 5 summarizes this paper.

2. RELATED WORKS

2.1 Policy-based Network Management (PBNM)

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. Figure 1 shows client-server model of policy, where 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.

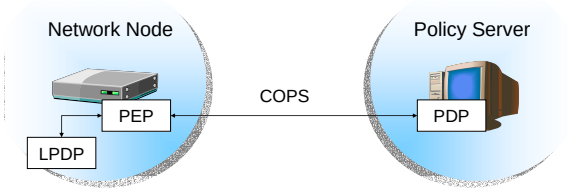

Fig. 1 Client-server model of policy

2.2 Common Open Policy Service (COPS)

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 [5]. 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 [6]. 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 [7] and COPS Client Software Development Kit 3.1 by Intel [8]. 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. SYSTEM DESIGN

3.1 Framework Configuration

Security engine on the router detects network attacks using intrusion detection policy, intercepts attacks, and notifies management system of network attacks. The router of security engine can intercept attacks, make smooth networking. But the normal router, which has not security engine, may be attacked by hacking and then can't perform routing.

Security engine for secure networking provides kernel-level packet filtering, intrusion detection, audit trail, authentication and access control. It optimizes intrusion detection and intercepts the network attacks dynamically in the kernel-level. It provides Internet with secure networking environments using security policy, and convenience using web based management.

Our framework consists of security engine on router, general host, security management system by networks. The security engine on the router provides packet filtering, intrusion detection, intrusion analysis, intrusion response, and policy enforcement. Security management system manages security engine and general host by security policy.

Figure 2 shows the configuration of security management framework. PDP is on security management system and PEP is on router with security engine. PDP communicate with PEP using COPS

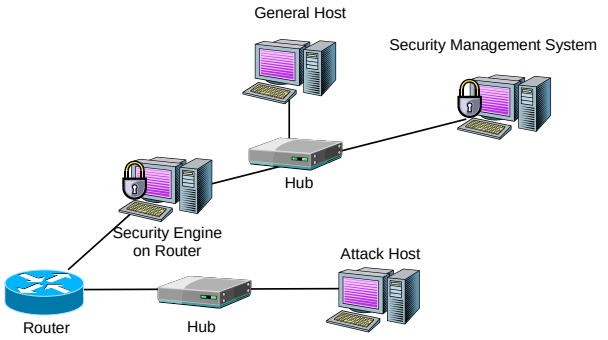

Fig. 2 Configuration of Security Management Framework

3.2 Architecture of Security Management System

Security management system manages the security engine on the router and general host by security policy. Security management system has policy server and web server. Policy server defines policy for intrusion detection and configures target to enforce policy such as access control, filtering rule, and detection rule.

Web server is needed to communicate with the web interface. Web interface is web browser, e.g. Netscape or Internet Explorer, and it provides management tool. We run web browser and put the URL of Security management system. Then web server sends the logon page to web browser and we can access logon page. After putting ID and password on logon, web server checks ID and password. If user is authorized, management applets is downloading form web server. If user is not authorized, web reloads logon page. Figure 3 shows the architecture of Security management system.

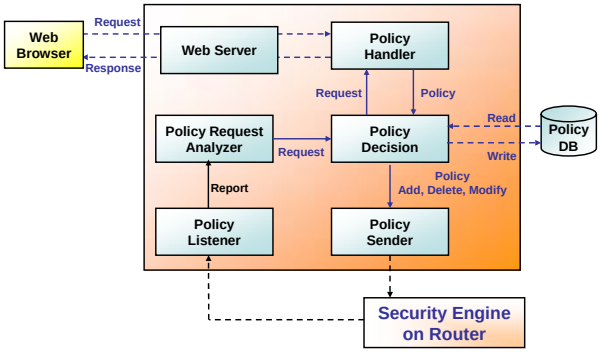

Fig. 3 Architecture of Security Management System

Policy Listener Module (PLM) receives policy request from the security engine on the router and reports the request to Request Analyzer Module (RAM). RAM analyzes the policy request and Policy Decision Module (PDM) decides the proper policy of security engine and sends policy to security engine in Policy Sender Module (PSM). Policy Handler Module (PHM) deals with the request of policy configuration using web browser. Security management system configures and deletes policy, and monitors the network using management tool. Management tool consists of network map, policy configuration, traffic monitoring, and network statistics.

3.3 Architecture of Security Engine

Security engine on router provides packet filtering, intrusion detection, intrusion analysis, intrusion response, audit handle, access control, and policy enforcement. Security engine communicates with security management system through Common Open Policy Service (COPS) and enforces policy for intrusion detection. Security engine captures the packet which passes the router. It analyzes the packet for intrusion detection, and it is operated by policy.

Figure 4 shows the architecture of integrated security engine. It consists of Policy Manager Module (PMM), Policy Agent Module (PAM), Access Control Module (ACM), Packet Sensor Module (PSM), Packet Filter Module (PFM), Intrusion Handler Module (IHM), and Intrusion Analyzer Module (IAM).

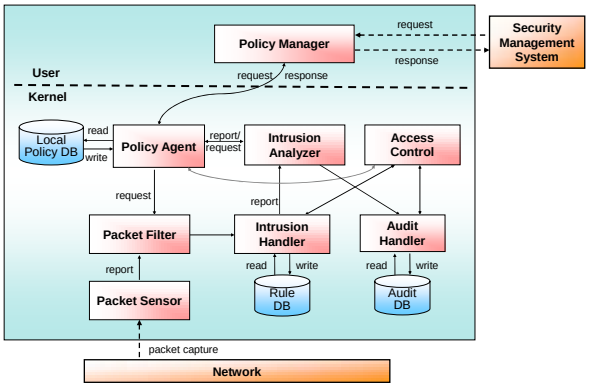

Fig. 4 Architecture of Security Engine

PMM sends the request of policy to management system and receives the proper policy of router. PMM operates with PAM. PAM stores the policy in policy database and provides the functions, search, add, delete and change. PAM is in kernel level and enforces the policy. PAM reads and writes local policy database by ACM. PSM captures the packet which passes the router. PSM makes a copy of the captured packet, and send copied packet to PFM. PFM filters the packet and sends the filtered packet to IHM. IHM classifies the packet by rule. If the classified packet is intrusion packet, then IAM find the type of intrusion and stores intrusion data in audit database. If there is intrusion, PAM informs PMM the intrusion. Rule may be changed, added, deleted, and created by the policy that PAM enforces. As a kind of intrusion detection, PMM can close the session or shut down the detected system.

4. IMPLEMENTATION

We have implemented security management framework in Linux 7.3 (Kernel 2.4.18) using JDK 1.3.1 [9], JSP server (tomcat) 4.0 [10], MySQL 3.23.43 [11], apache 1.3.21 [12], pcap library 0.4 and gcc 2.96. We can access to security management framework using web such as Netscape or Internet Explorer in Windows 2000, Linux or Solaris [13]. Web browser uses HTTP protocol to connect web server in security management system. After management servlet downloads in web browser, we start on management tool for intrusion detection.

Security management system configures and deletes policy, and monitors the network using management tool. Management tool consists of network map, policy configuration, traffic monitoring, and network statistics. Policy is sent to security engine, then security engine enforces policy, collects packet and analyzes intrusion detection of network.

Figure 5 shows the implementation of packet filtering policy. Packet filtering policy is “ACCEPT” or “DROP” as source IP address, destination IP address, input interface, output interface, source port number, destination port number and protocol. Security management framework accepts the permitted packets and denies the disapproval packets using packet filtering policy.

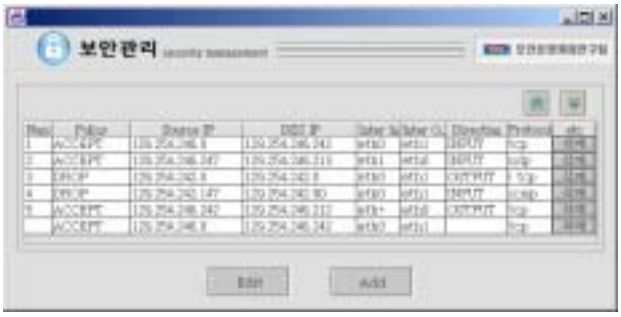

Fig. 5 Implementation of Packet Filtering Policy

Figure 6 shows the implementation of network intrusion detection. It shows the information of attack packet such as source IP address, destination IP address, source port number, destination port number and intrusion type. It changes the icon of host which correspond to the attack.

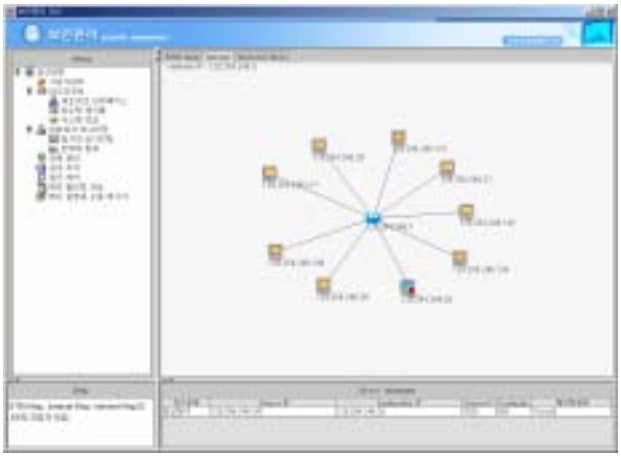

Fig. 6 Implementation of Network Intrusion Detection

5. CONCLUSION

Router is the network device of managing network traffic. The damage of router attack causes the problem of the entire network. So, the security technology about router is necessary to defend Internet against network attacks. Router has the need of access control and security skills that prevent from illegal attacks. We developed an integrated security management framework for secure networking. Integrated security engine is a security technology that provides router or gateway with secure networking. It provides kernel-level packet filtering, intrusion detection, audit trail, authentication, access control, and security management. As integrated security engine offers not in the application-level

but in the kernel-level, so it optimizes intrusion detection and minimizes the overhead of system. Also it intercepts the network attacks in real-time and manages the network with security policy. As the proposed security management framework makes use of Web, it is convenient for managing network.

REFERENCES

[1] Stephen Northcutt and Judy Novak, *Network Intrusion Detection. An Analyst's Handbook*, 2nd ed. New Riders, 2001.

[2] IETF Intrusion Detection Working Group http://www.ietf.org/html.charters/idwg-charter.html

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

[4] 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

[5] S. Herzog, J. Boyle, R. Cohen, D. Durham, R. Rajan, A. Sastry, COPS Usage for RSVP, January 2000.

[6] http://www.ietf.org/rfc/rfc2749.txt

[7] K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavatkar, and A. Smith, COPS Usage for Policy Provisioning (COPS-PR): RFC 3084, March 2001. http://www.ietf.org/rfc/rfc3084.txt

[8] Vovida.org, http://www.vovida.org/

[9] Intel® COPS SDK, http://www.intel.com/labs/manage/cops/

[10] JDK Homepage, http://java.sun.com/

[11] Jakarta Homepage, http://jakarta.apache.org/

[12] MySQL Homepage, http://www.mysql.com/

[13] Apache Homepage, http://www.apache.org/

[14] S. H. Jo, J. N. Kim, & S. W. Sohn, "Design of Policy-based Security Management for Intrusion Detection," *Proc. of The International Conference on Security and Management (SAM'03)*, pp.337-340, 2003.