The design of Secure Node System based on Integrated Security Engine (SNSISE)

JEONG NYEO KIM*, SUNG-WON SOHN*, KANE KIM**
*Electronics & Telecommunications Research Institute, **Univ. of California, Irvine
161 Kajeong-dong, Yuseong-gu, Daejon 305-350
KOREA

Abstract: - Conventional security systems provide the functions like intrusion detection, intrusion prevention and VPN individually, leading to management inconvenience and high cost. To solve these problems, attention has been paid on the integrated security engine integrating and providing intrusion detection, intrusion prevention and VPN. This paper introduces a security framework that allows secure networking by mounting integrated security engine to the network nodes like router or switch. Also, this paper introduces the structure of integrated security engine for router which provides and integrates intrusion detection and intrusion prevention, and describes core functions and algorithms implemented for the functions. Finally, this paper explains the efficiency of integrated security engine by comparing security network structure based on the network node equipped with integrated security engine, and security network structure composed of conventional individual systems.

Key-Words: Integrated Security Engine, Firewall, IDS, VPN, Router

1 Introduction

Conventional internet network used security measures comprising various individual systems like firewall [2][3][4], intrusion detection system, VPN system and server security system. In this environment where individual security systems, including lots of firewalls or intrusion detection systems, are installed on the network, policies may conflict each other in managing the policies on each firewall or intrusion detection system, or a policy set in an individual security system may influence other individual security system. Consequently, the existence of network firewall becomes meaningless, or normal operation of network may be hindered. Also, intrusion detection and intrusion prevention are provided separately, making rapid response impossible. Conventional security systems could not solve network security problems. To solve these problems, firewall, intrusion detection system, VPN system and server security system are implemented into an integrated security engine, allowing easy and cost-effective security management and rapid response.

This paper will introduce an integrated security engine for network node (router and switch), which solves the problems of individual security systems and provides easy security management. Integrated security engine integrates firewall, intrusion detection, VPN and intrusion tolerance, all of which are functions of conventional individual security systems, provides detection and prevention of attacks on system and network, and responds to such attacks. This paper will introduce structure of integrated security engine, and security function elements of integrated security engine.

This paper is structured as following. Chapter 2 introduces integrated security engine products and related studies. Chapter 3 addresses the concept and necessity of integrated security engine, and introduces the structure, functions and implementation level of the integrated security engine developed for network node. Chapter 4 introduces the design and implementation of intrusion detection/prevention and intrusion tolerance, which are core technologies of integrated security engine. And it also introduces network diagram comprising routers equipped with integrated security engine, and prototype of tested security router system. Finally, chapter 6 presents conclusions and future challenges.

2 Related Studies

Security products are evolving from individual system to integrated security appliance, and from system security to network security. Especially, security management function needing management has been highlighted. The products mounting integrated security engine are divided into integrated security appliance and integrated security network node (router or switch).

2.1 Integrated Security Appliance

Integrated security appliances mean "integrated hardware-dedicated products" integrating and providing at least more than two individual security solutions. Since the products provide high cost-effectiveness and easier management than individual security solutions, they have dominated security market. Integrated security appliances providing firewall, intrusion detection, VPN and anti-virus function, include Crossbeam's X40S, Fortinet's Fortigate, Symantec's Gateway Security.

2.2 Integrated Security Network Nodes

These are special-purpose network nodes boasting security functions. Security functions including firewall, intrusion detection and VPN are added to routers and switches. The products providing firewall and VPN include Enterasys Networks XSR-1800 and Nortel Networks Contivity 1700. The products providing additional intrusion detection include CISCO 1710 Security Access Router and CISCO 6500 Series Switch.

3 Integrated Security Engine (ISE)

3.1 The Structure and Function of ISE

Integrated security engine means a security processing engine which can prevent and prescreen the cracking on system and network by integrating conventional individual security solutions into one solution and providing security functions. Integrated security engine installed on the security routers or switches that are network nodes, are shown conceptually as seen in the Fig.1. As such, integrated security engine comprises firewall, intrusion detection, VPN, traffic measurement and control, node's own intrusion tolerance, and security control engine based on the policies to manage the functions described above. If information protection in the conventional network is passive security for protecting the resources in the system or server, new next-generation concept of information protection is active security in terms of network. One of the essential elements for this active network security is integrated security engine, which comprises following functions.

3.1.1 Firewall Engine

Firewall engine receives packets allowed under filtering rules and rejects packets not allowed, in relation to the packets received to network nodes.

3.1.2 Intrusion Detection and Analysis Engine

Intrusion detection and analysis engine detects intrusion by analyzing packets and system log information. If intrusion is detected, the engine logs intrusion or notifies detected intrusion packet information or packet monitoring information, enabling counteractions.

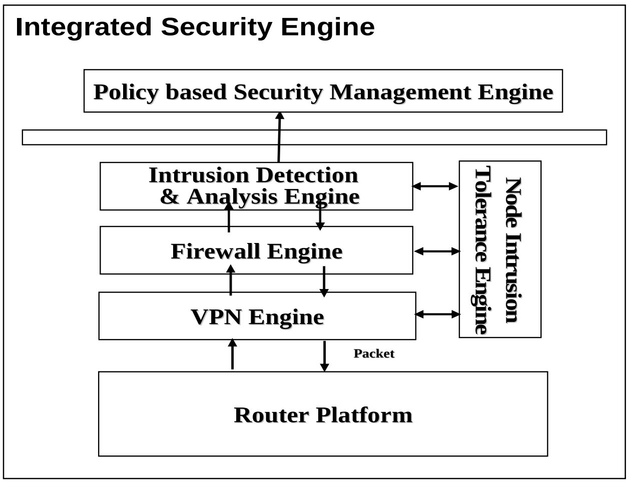
Integrated Security Engine
Policy based Security Management Engine
Intrusion Detection & Analysis Engine
Firewall Engine
VPN Engine
Node Intrusion Tolerance Engine
Packet
Router Platform

Fig.1. Integrated Security Engine Concepts

3.1.3 VPN Engine

VPN engine provides confidentiality and integrity for networking by substituting for private line and forming a virtually secure network. VPN engine uses IPsec to encode network data for transmission, and decode it for processing.

3.1.4 Traffic Measurement and Control Engine

Traffic measurement and control engine detects DDoS attacks including traffic overload by measuring network traffic, and accordingly, controls network traffic. This is a function indispensable for traffic detection system capable of preventing network paralysis due to network overload like 1.25 Internet Attack.

3.1.5 Node Intrusion Tolerance Engine

Even if it is possible to prevent or prescreen cracking on network, failure to prevent cracking on network node leads to null. This engine provides node intrusion tolerance function for controlling access to the inner part of network node. Node intrusion tolerance technologies include authentication of logged-in user based on multi-level security policy, access control based on user role, and audit trail enabling node monitoring.

3.1.6 Policy-based Security Management Engine

Policy-based security management engine provides policy-based security management function in order to manage security of network node providing integrated security function. This engine is controlled by security management server system managing network node. The engine receives policies or sends packet monitoring information or detection packet information to security management server system, providing secure networking.

4 Security network node system

4.1 Security network node system

This chapter introduces SecuRISE (Secure & Reliable Integrated Security Engine: hereafter the "SecuRISE"), which is an integrated security engine designed and implemented in router, which is network node. SecuRISE is an integrated security engine implementing firewall, intrusion detection/analysis, node intrusion tolerance and policy-based security management engine, among the above engine functions. Being installed in router, it provides security and secure networking for the system in the sub-network of relevant router. SecuRISE provides security function without preventing existing router functions. Diagram of router system mounting this engine is as shown in the Fig.2.

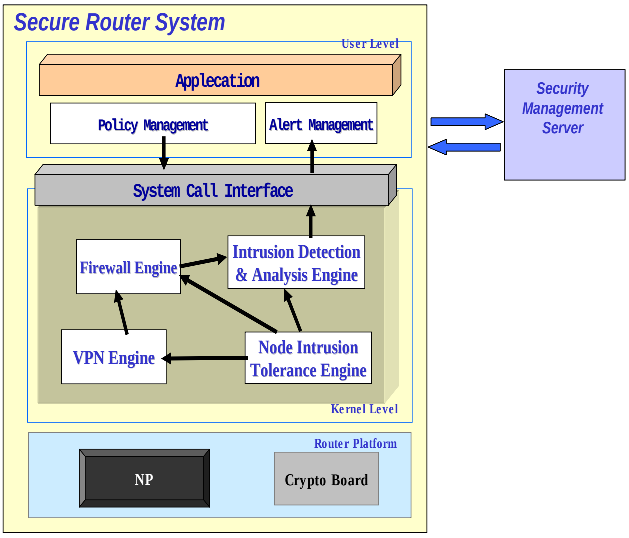

Fig.2. Diagram of Security network node system

4.2 Design and Implementation of SecuRISE

4.2.1 Firewall Engine

Firewall permits or rejects packages, or request packet inspection to intrusion detection and analysis engine, in accordance with the packet filtering rules defined in the process of transmitting, receiving and routing packets. Packet filtering rules comprise Source IP, Destination IP, Protocol, Source Port, and Destination Port, and provide filtering depending on each field. To perform these functions, packet filtering rules comprise the functions like filtering rules management, filtering processing and network interface.

(1) Filtering rules management

This function manages filtering rules DB, and if requested to apply new policies, converts filtering rules to the ones fit to it for saving.

(2) Filtering processing

This function processes filtering on the basis of the rules stored in the rules DB.

(3) Network Interface

Connected with network protocol stack, this module takes over any new packets arrived. This function detects packets to decide whether to filter them.

4.2.2 Intrusion Detection and Analysis Engine

Intrusion detection and analysis engine [11] detects and analyzes detection to protect system and network from intrusion from within or from without. The scope of detecting and inspection intrusion comprises detection of well-known attack techniques, inspection of packet header and payload, and pre-processing inspection and detection. Inspection of well-known attack techniques directs at well-known attacks like virus, backdoor, DoS, Scanning, ICMP attack etc. Inspection of packet header and payload targets TCP flag check, TCP ack check, packet payload pattern matching, etc. Pre-processing inspection and detection directs at Back Orifice, http decode, and Unicode, which are attack techniques detected through pre-processing since they cannot be detected through packet header and payload information.

This engine provides intrusion detection/response and audit trail, all of which are based on the network and host, under security policy. To this end, this engine uses packet and audit data to detect and respond to intrusion, records audit results, and provides the roles of changing policies like change of intrusion detection rules and change of monitoring mode. This engine detects and responds to detection by using access control information transmitted from network packet and node intrusion tolerance engine. This engine transmits packet filtering information, statistical information of intrusion detection, and summarized information of audit record to the policy-applying section for monitoring. Policy-applying section uses proc file system and device driver to transmit the information to the policy-deciding section. Policy change function adds/deletes intrusion detection rules and changes monitoring mode, according to the request to change rules and monitoring modes, which is transmitted from the policy-applying section through system call. Intrusion detection and analysis engine provides engine management and detection handler functions.

(1) Engine management
This function processes initialization related with intrusion detection, and request for to change monitoring mode and intrusion rules. Monitoring information structure and information on the location of rules DB directory are gained through the data structure used by engine management. Intrusion detection rules are subdivided into the rules for inspecting rule type, protocol type, packet header and packet payload, and expressed into LVR(Linked-list of Variable-length Record: hereafter the "LVR"). These LVRs use hierarchically-constituted IDRL (Intrusion Detection Rule List: hereafter the "IDRL") to manage the rules [5]. IDRL is used for intrusion detection. Rules are changed by constituting LVR for changed rules, using pointer changes through LV(Look-up Variable), and reflecting it into IDRL.

(2) Intrusion Handler
Intrusion handler transmits the information on intrusion judgment and monitoring to the policy-applying section by using defined intrusion detection rules and information transmitted to firewall engine. If it judges that intrusion is made, intrusion handler calls response function set in the policy-deciding section and transmits this information to the policy-applying section.
Intrusion is detected in the order of pre-processing inspection, packet header inspection and packet payload inspection. If intrusion is detected in each stage, intrusion handler performs the process of performing response function. Pre-processing inspection inspects http decode attack and Unicode attack, which cannot be found by checking packet header and content information. This inspection is performed before inspecting packet header or payload. Packet header inspection inspects to see whether content defined in the detection rules for each part of packet header exists. Packet payload inspection inspects to see whether specific strings defined in the detection rules exist in the packet payload. After intrusion is detected, response function to cope with it supports two types: Notify and Drop. Notify is divided into Alert and E-mail to target system in order to process intrusion information. Alert sends alert information to security management server system via policy-applying section. E-mail to target system uses e-mail to intrusion results to target system.

4.2.3 VPN Engine

Applying IPsec VPN to routers can guarantee networks to secure by providing encryption channels among network nodes without additional security devices. The integration of various security functions into a single network device is requires to current market for the cost reduction and the effective management of various security devices. Virtual Private Network engine manages secure channel between network nodes. IPsec Protocol has been deployed widely at remote business environment because of its properties, confidentiality and integrity for network traffic. Before Using IPsec protocol, it is needed that negotiations of security associations and keys between two end points of IPsec tunnel. IKE protocol is used when negotiation is done automatically. We developed the light-weight IKE protocol that can be applied to an embedded system such as router. We will prove that this IKE protocol has been implemented based on RFC by working with other commercial IKE protocol.

4.2.4 Node intrusion tolerance Engine

Node intrusion tolerance engine provides security functions for node. The functions comprise user authentication, access control and audit trail.

(1) User authentication
The engine provides security in authenticating user in order to provide secure node functions. User authentication provides user-role-based multilevel authentication necessary for controlling the access through the means other than user ID/Passwd, in line with access control. The basic roles provided by router are security manager and network manager. User can define additional six roles to use.

(2) Role based access control (hereafter the "RBAC")
Users accessing intra-router resources are limited. Since any user acquiring system administrator privileges can change all configurations in the router, access control is necessary. Node intrusion tolerance engine provides RBAC, which is an access control policy combining DAC and MAC in order to control router users' access [6][7][8][9]. RBAC is an access control policy most suitable for commercial environment. This is implemented on the basis of RBAC 96 model proposed by a professor, Mr. Rabi Sandu, in the level of kernel. RBAC mechanism uses the principle of minimum privilege separation, which minimizes the privileges of relevant subjects, gives minimized privileges to user roles, and controls access according to the roles.

(3) Audit trail
Filtering results transmitted from firewall engine, results of intrusion detection created in the intrusion detection and analysis engine, and access control information generated in the node intrusion tolerance engine are recorded in the audit trail DB. Also, firewall, statistical information on intrusion detection, and summarized information on audit trail are sent to policy-applying section to ensure that monitoring is enabled.

4.2.5 Policy-based security management Engine

Policy-based security management engine[12] manages security on the basis of the security policies of network node. It provides three security management functions. First, security management functions. This is a policy-based security management framework implemented in the security management server system managing router. Second, policy-deciding functions. This function allows routers to receive relevant policies from security management server system and decide policies to process. Finally, policy-applying functions. This function applies the policies from security management server system to routers. We used socket for communication between security management server system and security router.

(1) Security management
The function defines security policies for integrated network security management and provides policy-based management. This is implemented in security management server system, providing network management, policy DB management and communication with routers.

(2) Policy decision
This function decides policies to managing router system security. This function comprises communication with security management server system, policy decision and policy DB.

(3) Policy application
This function sends packet monitoring information or intrusion packet information to the policy-deciding section, or applies the policies from the policy-deciding section. This changes firewall rules, sets intrusion detection rules and applies access control policies.

4.3 Design and Implementation of Platform

SecuRISE based security router system was tested on the router based on the Intel Network Processor. We implemented integrated security engine in the source code patched by Linux 2.4.18 kernel [10] in the environment where Red Hat 7.3. was installed, and created Embedded Linux kernel. Test was conducted in the following two ways. First, we made DoS attacks on the server below the router equipped with SecuRISE in the host 1. Security router detected the attacks and sent detection results to the security management server. In turn, the security management server used the information of packet for DoS attacks and prescreened relevant packets. Second, web server as host 2 allowed virus to upload files on the website in order to make them downloaded. When host 4 attempted to download the files, intrusion was detected and detection results were sent to the security management server system. Accordingly, the system coped with attacks. Well-known viruses can be prescreened automatically.

4.3.1 Secure Router Main Board(SRMB)

Main board is main component of Secure Router Hardware Platform, executes routing and intrusion detection functions using network processors. SRMB executes ingress and egress functions using One NPU. Intel IXP2800 NP is installed on SRMB. Also QDR SRAM, RDRAM and TCAL are installed on SRMB for software processing. SRMB has SPI-4.2 and PCI interface for connection between Ethernet Line board and secure router crypto board. We can select network board (SRNB) or crypto board (SRCB) for crypto acceleration and performance.

4.3.2 Secure Router Network Board (SRNB)

Network board is network component of Secure Router Hardware Platform, provides network interface such as MAC and PHY. SRNB has SPI-4.2 and PCI interface for connection of SRMB. SRNB has SFP and RJ-45 for network interface.

4.3.3 Secure Router Crypto Board (SRCB)

Crypto board is component of Secure Router Hardware Platform which is combined network and crypto functions. SRCB has network interface, encryption/decryption algorithm using IPsec protocol, Key Exchange interface, and Database processing function. SRCB provides IPsec protocol using Cavium Chip, the performance is maximum 10 Gbps. SRCB has SPI-4.2 and PCI interface for connection of SRMB. SRCB has SFP and RJ-45 for network interface.

5 Conclusions and Future Work

This paper has described the concept and necessity of integrated security engine, and introduced the design and implementation of integrated security engine based on Linux 2.4.18 kernel. Also, this paper has introduced demo version of security router based on the implemented integrated security engine. Integrated security engine implements firewall, intrusion detection, and node intrusion tolerance in the kernel level, provides excellent performance, and shows easy-to-maintain security management functions based on policies. In addition to these advantages, this engine provides cost-effectiveness by implementing this single integrated security engine. However, it is necessary to study more efficient and improved version in consideration of hardware performance.

Recently, attacks targeting DNS or router as network node in order to paralyze whole system have increased, instead of attacks on one single system like 1.25 internet attacks. To cope with this trend, it is necessary to study the technologies of engine measuring and controlling traffic, which can measure and control network traffic. Also, it is necessary to conduct lots of studies to ensure that node-level audit trail function or system monitoring function can be used to detect and prevent attacks on system and network.

Additionally, it is not easy to evaluate the safety and performance of integrated security engine because the engine is not used wide yet. Also, Korea has not set any standards to evaluate integrated security engine. The standards meeting domestic requirements and satisfying international evaluation requirements should be established to determine the safety and performance of integrated security engine. From this, a strong foundation for developing our own technologies differentiated from foreign products or technologies should be established.

References:

[1] An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12, January 1998.

[2] William R. Cheswick, Steven M. Bellovin Firewalls and Interne Security: Repelling the Willy hacker, Addison Wesley, 1994.

[3] D. Brent Chapman, Elizabeth D. Zwicky, Building Internet Firewalls, O Reilly & Associations, Inc. January 1996.

[4] Chris Hare, Karanjit Siyan, Internet Firewalls and Network Security – 2nd ed., New Readers, 1996.

[5] Peter A. Loscocco, Wtephen D. Dmalley, Patric A. Muckelbauer, Ruth C. Taylor, S.Jeff Truner, John F. Farrel, 'The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments', National Security Agency, 1997.

[6] Bell, David Elliott, & Leonard J. La Padula, “Secure computer system: Unified exposition and multics interpretation,” MITRE Technical Report 2997, MITRE Corp, Bedford, MA, 1975.

[7] David F. Ferraiolo, Ravi Sandu, & Serban Gavrila, “A Proposed Standard for Role-Based Access Control,” ACM transaction on Information and System Security, VOL.4, NO.3, pp.224-274, Aug. 2001

[8] DOD 5200.28-STD. 'Department of Defense Trusted Computer System Evaluation Criteria', December 1985

[9] D.Ferraolo and R, Kuhn, "Role-Based Access Control", Proceeding of the 15th National Computer Security Conference, 1992

[10] Linux 2.4.18 Kernel-RELEASE Source Code

[11] B. H. Jung, J. N. Kim, “Design of Dynamic Intrusion Detection Rule Modification Technique for Kernel Level Intrusion Detection”, *Proc. of Korean Information Processing Society, Vol. 9, No. 2, Nov. 2002.*

[12] S.H. Jo, J. N. Kim, & S. W. Sohn, “Design of Web-based Security Management for Intrusion Detection”, *Proc. of ICEB, ICEB ‘2002*, 2002

[13] J. G. Ko, J. N. Kim, & K. I. Jeong, “Access Control for Secure FreeBSD Operating System,” *Proc. of WISA2001*, 2001.