Winter 12-10-2002

Design of Web-based Security Management for Intrusion Detection

Su-Hyung Jo

Jeong-Nyeo Kim

Sung-Won Sohn

Design of Web-based Security Management for Intrusion Detection

Su-Hyung Jo, Jeong-Nyeo Kim, Sung-Won Sohn
Information Security Research Division
Electronics and Telecommunications Research Institute (ETRI)
161 Gajeong-Dong, Yuseong-Gu, Daejeon, KOREA
{shjo,jnkim, swsohn}@etri.re.kr

Abstract

Electronic business is rapidly popularized and extended through Internet. Internet has many security weaknesses, so we need the security solution such Intrusion Detection System that minimizes the damage of hacking and responds the intrusion dynamically. It is difficult for legacy management system to process the security environments and electronic business, because legacy system lacks of security policies and integrated security methods. In order to resolve these problems, we need security management system that has standard security policy, consulting, diagnosis, maintenance, and repair function. In this paper, we design and implement Web-based security management for intrusion detection. Our security system consists of network nodes, general hosts and a management node. A management node manages a network node, that is a secure router, and general hosts by security policies. We design the channel between the management node and the network node using IPsec (IP Security). We have applied java and Web to implementing user interface of security system. As the proposed system makes use of Web, security management system is easily accessed through the Web.

1. Introduction

Nowadays the business markets of Electronic Commerce (EC) [1] have rapidly extended through Internet. Internet has many security vulnerabilities such as sniffing, spoofing and computer virus. It is necessary to provide the security of Internet services for electronic business. In order to overcome the weakness of Internet, we make good use of security services such as firewall, Virtual Private Network (VPN), Enterprise Security Management (ESM) and Intrusion Detection System (IDS) [2].

IDS 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.

Today's standard of IDS is in progress by consortium and IETF. Internet Security System (ISS), Tripwire software, IBM, and Network Associates joint Intrusion Detection System Consortium (IDSC). IETF Intrusion Detection Working Group (IDWG) [3] defines a data format that exchanges the information of various IDS products.

It is difficult for legacy management system to process the security environments and electronic business, because legacy security management hasn't any security policy [4, 5] or integrated management method. In order to resolve these problems, we need security management system that has standard security policy, consulting, diagnosis, maintenance, and repair function. It is necessary to develop security management technologies that are integrated and can be reconfigured in real-time whenever the network administrator wants.

In this paper, we design and implement Web-based security management for intrusion detection. Our system consists of network nodes, general hosts and a management node through networks. A network node is a security router that provides packet filtering, intrusion detection, intrusion analysis, intrusion response, and policy enforcement. A management node manages network nodes and general hosts by security policies. We design the channel between the management node and the network node using IP Security (IPsec) [6].

This paper is organized as follows. Section 2 describes related works which are Java Server Page (JSP) and IPsec. Section 3 designs the architecture of our system. Section 4 describes the implementation of Web-based security management. Finally, section 5 summarizes this paper.

2. Related Work

2.1 Java Server Page (JSP)

Java Server Page (JSP) is a technology for controlling the content or appearance of Web pages using servlets. JSP allows Web developers and designers to rapidly develop and easily maintain Web pages that support

existing business systems. JSP enables rapid development of web-based applications that are platform independent. JSP uses XML-like tags and scriptlets written in the Java programming language to encapsulate the logic that generates the content for the page.

Java Server Page is an extension of the Java Servlet technology. Servlet is a small program that runs on a server and platform-independent module. Servlet provides Web developers with a simple, consistent mechanism for extending the functionality of a Web server and for accessing existing business systems. Servlets have made many Web applications possible. JSP is comparable to Microsoft's Active Server Page (ASP) technology. While a Java Server Page calls a Java program that is executed by the Web server, an Active Server Page contains a script that is interpreted by a script interpreter such as VBScript or JScript before the page is sent to the user. An HTML page that contains a link to a Java servlet is sometimes given the file name suffix of .JSP.

2.2 IP Security (IPsec)

The research on the next generation Internet is already in progress worldwide. IPsec (IP security), which is a common security service, is proper for characteristics of the Internet as a mandatory technology in next generation Internet IPv6. IPsec provides various security services at the IP layer. It is mandatory to implement IPsec in IPv6 and IPsec provides scalability and interoperability that are required to the Internet security protocol. It is not required to modify the software to use the security services of the IPsec and users don't care about the existence of the IPsec. IPsec is an extension of IP, it has Authentication Header (AH) [7] and Encapsulating Security Payload (ESP) [8]. IPsec can provide Internet security services that are access control, connectionless integrity, rejection of replayed packets, data origin authentication, confidentiality, and limited traffic flow confidentiality.

AH is security protocol that provides security services using message checksum (ICV). ESP is security protocol that offers security services using data encapsulation. AH is used to protect an entire IP payload and ESP is used to protect upper-layer protocols of an IP payload. ESP gives security services to only encapsulated field, but AH provides security service for IP packet. AH and ESP support two modes, transport mode and tunnel mode. Transport mode is used to protect upper-layer protocols and tunnel mode is used to protect entire IP datagram.

IPsec SA is that how to protect the traffic, what traffic to protect, and with whom the protection is performed between host and gateway or end hosts. It is consisted of Security Parameter Index (SPI), destination address and security protocol, AH or ESP. SA decides IPsec protocol as simplex connection entity and IKE negotiates about SAs. Since SA is simplex connection, there exist SA tables according to outbound or inbound processing. SAs are indexed by SPI that exists in IPsec protocol headers, the IPsec protocol value, and the destination address.

3. System Design

3.1 System Framework

Our system consists of network nodes, general hosts and a management node through networks. The network node is a security router that provides packet filtering, intrusion detection, intrusion analysis, intrusion response, and policy enforcement. The management node manages the network node and general host by security policies. Figure 1 shows the system framework of Web-based security management for intrusion detection. The management node and the network node communicate using IPsec.

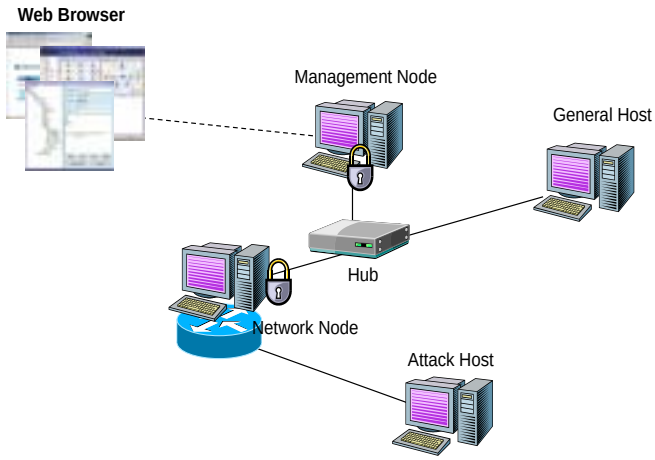

Figure 1. System Framework

3.2 Architecture of Management Node

The management node manages the network node and general host by security policies. Management node has management servlets, network sensor, policy decider, policy parser, audit manager, audit handler and databases. Policy DB stores the policy for intrusion detection such as the access rule, filtering rule, and detection rule. The policy parser writes, configures and deletes policies from policy DB. After the policy parser reads the policy DB, the policy decider selects a suitable policy for the network node.

Tomcat 4.0 provides the servlet engine for management servlets. Management servlets, which are executed by tomcat program, communicate with the Web interface. Web interface is Web browser, e.g. Netscape or Internet Explorer. We run Web browser and put the URL of the management node. Then login servlet sends the logon page to Web browser and we can access logon page. After putting ID and password on logon, login servlet checks ID and password from the user DB. If user is authorized, security management program is downloading form Web server. If user is not authorized, Web reloads the logon page.

Figure 2 shows the architecture of the management node. The network sensor collects network information

such as host data, routing data and packet data from networks, and stores at network DB. The audit handler and audit manager deals with the alarm of illegal access, bad packet and intrusion. The network node is a security router that provides packet filtering, intrusion detection, intrusion analysis, intrusion response, audit handle, access control, and policy enforcement. The network node operates intrusion detection by policy and communicates with the management node using IPsec.

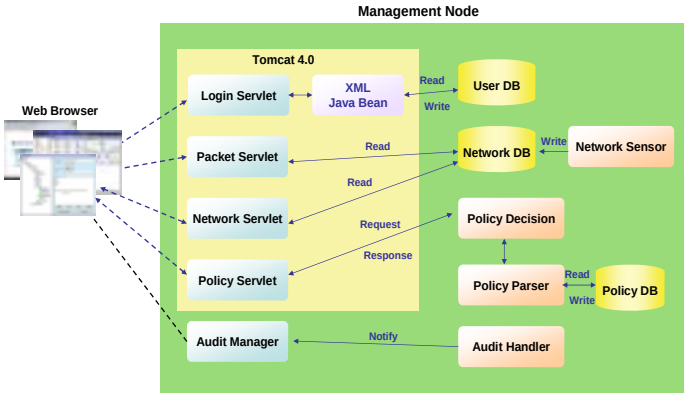

Figure 2. Architecture of Management Node

4. Implementation

We have implemented our system in Linux 7.1 using JDK 1.3.1 [9], JSP server (tomcat) 4.0.3 [10], pcap library 0.4 and gcc 2.96. We can access to security system using Web such as Netscape or Internet Explorer in Windows 2000, Linux or Solaris. A management node configures and deletes policies, and monitors the network. The policy is sent to a network node, then the network node enforces policy, collects packet and analyzes the intrusion detection of networks.

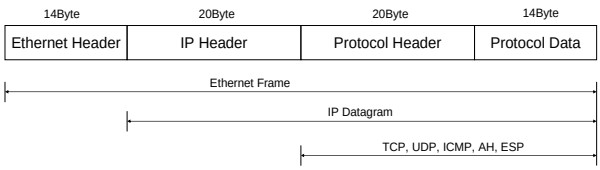

Figure 3. The format of Ethernet Frame

Figure 3 shows the format of Ethernet frame. We define that “default length of snap” is 68bytes of the macro used with the network sensor using pcap library. Length of frame is variable and the minimum length is 68bytes. The minimum length is sum of Ethernet header length, IP header length, TCP header length and protocol data length. Ethernet header is 14bytes, IP header is 20bytes, TCP or UDP header is 20bytes, and the length of protocol data is 14bytes.

```
#define DEFAULT_SNAP_LEN        68
#define DEFAULT_NET_DEV         "eth0"
#define FILTER_RULE_LEN         256
#define ETHER_TRAILER       4
#define LOG_FILE            "packet_info.log"

static void analyze_packet (unsigned char *user, const struct
pcap_pkthdr *pkthdr, const u_char *p) {
        const struct ip *p_ip;
        const struct ether_header *p_ehdr;
        uint16_t ether_type;

            snap_start = p;
        snap_end = p + pkthdr->caplen - 1;
        set_cur_pkt_timestamp (pkthdr->ts);
            frame_time = pkthdr->ts;
        p_ehdr = (const struct ether_header *)p;
        ether_type = ntohs(p_ehdr->ether_type);
        p_ip = (const struct ip *)(p + sizeof(struct ether_header));
            set_cur_pkt_ethertype (ether_type);
            set_cur_pkt_etheraddr (p_ehdr);

        if (ether_type== ETHERTYPE_IP) {
            set_cur_pkt_ipproto(p_ip->ip_p);
                set_cur_pkt_ipaddr(p_ip->ip_src, p_ip->ip_dst);
                    if (is_normal_ip(p_ip)) {
                    analyze_ip_datagram ((const u_char *)p_ip +
                            sizeof(struct iphdr), p_ip->ip_p);
                }
            }
        next_pkt_entry();
}

static void analyze_ip_datagram (const u_char *p, u_char ip_proto)
{
        switch (ip_proto) {
            case IPPROTO_TCP:
                analyze_tcp(p);
                break;
              case IPPROTO_UDP:
                        analyze_udp(p);
                        break;
              case IPPROTO_ICMP:
                        analyze_icmp(p);
                        break;
            }
}
```

The packet is captured from networks, “analyze_packet()” function classifies the header of the packet. “analyze_packet()” function finds out source address, destination address, source port, destination port and protocol. “analyze_ip_datagram()” function classifies protocol using the protocol field of ip header. If the protocol field of ip header is “IPPROTO_TCP”, “analyze_tcp()” function is called. If the protocol field of ip header is “IPPROTO_UDP”, “analyze_udp()” function is called. If the protocol field of ip header is “IPPROTO_ICMP”, “analyze_icmp()” function is called. The analyzed packet is useful about knowing the intrusion detection, packet traffic, and packet statistics.

5. Conclusion

In this paper, we design Web-based Security Management for Intrusion Detection. Our system consists of network nodes, general hosts, management node through networks. The network node is a security router

that provides packet filtering, intrusion detection, intrusion analysis, intrusion response, and policy enforcement. The management node manages the network node and general hosts by security policies. We have applied java and Web to implementing system. Java is used to program the user interface. As the proposed system makes use of Web, security system is easily accessed through the Web in real time.

References

[1] Richard Kee, Roger Walton, Henning Dransfeld, and Nick Harman, *Ovum Forecast the Internet and E-commerce*, Ovum, July 2000.

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

[3] IETF Intrusion Detection Working Group

http://www.ietf.org/html.charters/idwg-charter.html

[4] IETF Policy Working Group

http://www.ietf.org/html.charters/policy-charter.html

[5] 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

[6] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol: RFC 2401, November 1998

http://www.ietf.org/rfc/rfc2401.txt

[7] S. Kent and R. Atkinson, IP Authentication Header: RFC 2402, November 1998.

http://www.ietf.org/rfc/rfc2402.txt

[8] S. Kent and R. Atkinson, IP Encapsulation Security Payload: RFC 2406, November 1998.

http://www.ietf.org/rfc/rfc2406.txt

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

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

[11] S. H. Jo, J. H. Nah, & S. W. Sohn, "Internet Security Management System for IPsec," *Proceeding of NordU2002/USENIX Conference*, Helsinki, Finland, February 2002.