Available online at www.sciencedirect.com
ScienceDirect
Future Generation Computer Systems 25 (2009) 358–363
FGCS
FUTURE GENERATION COMPUTER SYSTEMS
www.elsevier.com/locate/fgcs

Structure design and test of enterprise security management system with advanced internal security

Seoksoo Kim[a,*], Soongohn Kim[b], Geuk Lee[a]

[a] Department of Computer and Multimedia Engineering, Hannam University, Daejeon, South Korea
[b] Department of Computer Multimedia Science, Joongbu University, Choongnam, South Korea

Received 4 November 2005; accepted 21 April 2006
Available online 11 July 2006

Abstract

A security system for a company network is progressing as a ESM (Enterprise Security Management) in an existing security solution foundation. The establishment of the security policy is occupying a very important area in ESM of the security system. We tried to analyze the existing ESM system for this and designed a security solution structure for enhancing the internal security. We applied implementing directly IDS system and tested it. This study examined the structure of security solutions in order to build an enterprise security management system. For this purpose, we analyzed existing enterprise security management systems and, based on the results, proposed a enterprise security management system with reinforced internal security and tested the system. For the test, we used a firewall through log analysis and designed an intra-network using virtual IP system.

Keywords: IDS; EMS; Security; Firewall; Internal; Management

1. Introduction

The Internet based on TCP/IP (Transmission Control Protocol/Internet Protocol) was originally developed as an academic research network connecting schools and research institutes but has been expanded into a commercial network with a larger number of users for diverse uses. Various services including e-commerce and home banking have been introduced through the network and the number of users has increased rapidly. In addition, sharing of electronic records and materials through intranets has spread throughout all areas of society including business and education. At the same time, however, the dysfunctions of informatization such as the distribution of unhealthy information and information crimes are also proliferating together [1].

Common types of information crimes are computer network intrusions, forgery and alteration of electronic records, distribution of various obscene materials, defamation in online communication, production and circulation of viruses, etc. In particular, public organizations and companies are struggling to prevent intrusions from outside [2].

The most typical system security systems are firewall and IDS (intrusion detection system). With the diversification of intrusion patterns, however, it is getting more difficult to detect and defeat intrusions and, as a result, the functions and control of security products are getting more sophisticated. In order to manage various security solutions, security managers should perform the task of enterprise security management and this task needs an enterprise management system [3].

The present study examined the structure of security solutions in order to build an enterprise security management system. For this purpose, we analyzed existing enterprise security management systems and, based on the results, proposed and tested an enterprise security management system with reinforced internal security. For the test, we used a firewall through log analysis and designed an intra-network using virtual IP system.

* Corresponding address: Department of Computer and Multimedia Engineering, Hannam University, 133 Ojung-Dong, Daeduk-Gu, 306-791 Daejeon, Daejeon, South Korea. Tel.: +82 42 629 8336; fax: +82 42 629 8093.
E-mail address: sskim@hannam.ac.kr (S. Kim).

0167-739X/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2006.04.019

2. Internet attack procedure and prevention methods

2.1. Internet attack procedure

Internet attack procedures can be divided into three steps as follows.

A. Information collection step

In the first step, information collection, the attacker collects information about hosts to be attacked and services executed by the hosts and select the final target of attack. In this step, the attacker may collect information through browsing systems and services, OS and topology/firewall filtering rules and gathering data about network servers.

B. System intrusion step

In the second step, system intrusion, the attacker intrudes actual individual systems. Based on information collected in the information collection step, it attacks the most vulnerable part.

C. Attack transition step

In the third step, attack transition, a secondary intrusion follows the primary system intrusion. Based on information obtained from the primary intrusion and additional work, the attacker expands the system intrusion and intrudes other systems as well [4,5].

2.2. Firewall system

A firewall is to protect and isolate a system so that security accidents or threats to the network do not spread. This is an active defense that allows only permitted or authenticated traffic and blocks illegal traffic to protect the internal network of a specific organization. The basic purpose of a firewall is to reduce the risk zone while guaranteeing transparency to network users. There are mainly five types of firewall as follows.

First, in packet filtering, the network-level system is determined by the addresses and the ports of IP packet sender/receiver and ordinary routers provide a network-level intrusion blocking system. However, because of its complex rules, it is difficult to decide the operation of packets and network routes. Moreover, a current network-level firewall is so complicated that it can manage the state of connection, data contents, data types, etc. A distinct point is that the network-level intrusion blocking system can control routers directly, allowing them to use assigned IP blocks legitimately and guarantee fast and transparent services to users [6,7].

Second, an application gateway means a machine that functions as a proxy that blocks, logs and audits traffic between two networks. Because the proxy application is a software part of a firewall, it will be desirable to assign it many log and access control functions. An application-level firewall is not transparent to ordinary users and requires client setting. Recent application-level IDS guarantees transparency, and provides a detailed audit report and a more effective security model than a network-level firewall. It runs on the application layer, has a separate gateway for each interpretation service, and can control packet filtering and packet data.

Third, a circuit gateway exists between the 5th and the 7th layers of OSI network model and, different from an application gateway, it has a general proxy usable to any applications. In order to connect to the internal network through a firewall, the client needs a modified client program that can recognize the circuit proxy. Thus, its disadvantage is that only clients equipped with a modified client program can be integrated into the circuit.

Fourth, stateful inspection, which analyzes state information, is essential for processing new connection requests because it is not sufficient to analyze a single packet in existing routers for complicated services and high security. The analysis of information obtained from previous connections and from the corresponding applications is important in any decision to accept or reject a new connection.

Fifth, there is a hybrid firewall composed of various types of firewall. Functions may be assigned selectively according to the kind of services and for the sake of users' convenience and security. But it is difficult to build and manage this type of firewall because many different security policies have to be applied according to service [8].

2.3. IDS (Intrusion detection system)

Intrusions include all actions that violate the security elements of a computer system through unauthorized access. There are many types of intrusions including port scanning for access and actual intrusions through password hacking. Intrusion detection is monitoring a host or a network to prevent intrusions and intrusion attempts and giving real-time warnings about detected intrusions. The concept of intrusion detection was introduced first by J.P. Anderson in 1980 and the procedure of intrusion detection is generally composed of information collection → information processing and abstraction → intrusion analysis and detection → report and action.

IDS is a intrusion detection system that collects data from the system to be protected, filters out redundant or useless data, detects intrusions using detection techniques, and takes corresponding actions. It guards the entrance of a network, inspects incoming and outgoing packets based on preset security policies, and checks them against rules to decide the passage. A difference of IDS from a firewall is that IDS inspects all packets transmitted inside the network including those going out from and coming into the network.

IDS can be divided into host-based and network-based ones. Network-based IDS receives and analyzes packets for all traffic in the network and processes detected intrusions automatically. It is particularly excellent in detecting accesses unauthorized or exceeding the given authority. It can be used without additional setting of hosts and servers in the network and its failure does not cause serious damage.

On the other hand, it has difficulties in detecting attacks against vulnerable elements with complicated information, requires the exchange of a huge amount of data for analysis and, in the course of data exchange, has to filter data through data abstraction.