(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
G06F 15/00

(45) 공고일자 2005년07월12일
(11) 등록번호 10-0500589
(24) 등록일자 2005년07월01일

(21) 출원번호 10-2003-0061541
(22) 출원일자 2003년09월03일

(65) 공개번호 10-2005-0024571
(43) 공개일자 2005년03월10일

(73) 특허권자 엘지엔시스(주)
서울특별시 마포구 공덕2동 275번지 LG마포빌딩

(72) 발명자 이상우
인천광역시남동구간석1동금호아파트2-307

류연식
경상북도포항시남구지곡동133포항공대대학원아파트4-1001

표승종
서울특별시성동구금호동1가633번지벽산아파트202동2002호

(74) 대리인 김삼수

심사관 : 여원현

(54) 하드웨어기반의 패턴매칭을 이용한 웜 차단 방법 및 장치

요약

본 발명은 기존의 네트워크 환경의 변화 없이 패턴 매칭을 수행하는 하드웨어 기반의 전용 보드를 탑재한 웜 차단 시스템 및 방법에 관한 것으로, 상기 웜 차단 시스템을 보호하고자 하는 네트워크 앞에 설치하여 통신 선로상의 모든 패킷에 대하여 손실이나 지연 없이 웜 관련 패턴이 존재하는지를 검사하고 해당 보안규칙에 따라 패킷을 통과시키거나 차단시킨 후 결과를 실시간으로 관리자에게 알려주는 것이다. 특히, 기가비트 환경에 적당하도록 한 하드웨어 기반의 웜 관련 패킷의 탐지 및 차단 방법 및 시스템에 관한 것이다.

대표도

도 4b

색인어

웜, 차단, 패턴 매칭,

명세서

도면의 간단한 설명

도 1은 본 발명에 의한 시스템 구성도이다.

도 2는 관리 콘솔의 로그정보 수신 및 보안규칙 전송 기능 흐름도이다.

도 3은 호스트 시스템의 기능 흐름도이다.

도 4a는 PCI 보드의 내부 구성 블록도이다.

도 4b는 PCI 보드의 기능 흐름도이다.

도 5는 보안규칙 메시지 포맷이다.

도 6은 웜 차단 시스템에서 관리 콘솔로 송신되는 로그 메시지 포맷이다.

< 도면의 주요부분에 대한 부호의 설명 >

10 : 클라이언트 20 : 서버

30 : 게이트웨이 40 : 웜 차단 시스템

50 : 관리 콘솔 410 : ILC(In Line-Control)

430 : 헤더 서치엔진 450 : 콘텐트 서치 엔진

470 : 보안규칙 데이터 베이스

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 기존의 네트워크 환경의 변화 없이 패턴 매칭을 수행하는 하드웨어 기반의 전용 보드를 탑재한 웜 차단 시스템 및 방법에 관한 것으로, 상기 웜 차단 시스템을 보호하고자 하는 네트워크 앞에 설치하여 통신 선로상의 모든 패킷에 대하여 손실이나 지연 없이 웜 관련 패턴이 존재하는지를 검사하고 해당 보안규칙에 따라 패킷을 통과시키거나 차단시킨 후 결과를 실시간으로 관리자에게 알려주는 것이다. 특히, 기가비트 환경에 적당하도록 한 하드웨어 기반의 웜 관련 패킷의 탐지 및 차단 방법 및 시스템에 관한 것이다.

웜은 단일 컴퓨팅 시스템 내에서 프로그램 사이를 이동하거나 네트워크를 통해 서로 다른 컴퓨터로 자동 전파되는 프로그램 조각으로서, 바이러스와 달리 특별한 감염 대상을 가지고 있지 않으며, 컴퓨터 시스템을 직접 파괴하거나, 오작동을 유발하는 코드를 포함하고 있지는 않다. 그러나, 웜이 전파되는 과정에서 컴퓨터 시스템 내부와 네트워크에 엄청남 부하를 걸 수 있기 때문에, 웜에 의해 시스템 또는 네트워크가 다운되는 원인을 제공하기도 한다. 특히, 특별한 감염 대상을 가지고 있지 않은 상태에서, 감염자로부터 획득된 임의 정보를 바탕으로 확산되는 웜은, 일단 발송자로부터 외부로 방출된 후에는 기존의 어떤 방법으로도 통제나 제어가 거의 불가능하다는 특징을 가지고 있다.

컴퓨터 바이러스는 컴퓨터 내에 침투하여 자료를 손상시키거나 다른 프로그램들을 파괴하여 작동할 수 없도록 하는 악성 프로그램으로서, 감염 대상을 가지고 있다는 특징이 있으며, 현재 감염 대상을 감염시키고 다른 감염 대상을 찾아 전파되기 위해 자신을 스스로 복제한다는 특징이 있다.

웜 바이러스는 상기 설명한 웜과 컴퓨터 바이러스가 결합된 형태의 바이러스로서, 컴퓨터 바이러스가 웜을 통해 빠른 속도로 전파되는 특징을 가지고 있다. 실제로 외국에서 최초 보고된 웜 바이러스가 불과 몇 시간 안에 국내에 유입되고, 국내에 유입된 지 하루도 되지 않아 수만 명이 감염될 정도로, 웜 바이러스의 전파 속도는 빠르고 파괴적이다. 최근 웜 바이러스에는 기본적인 웜과 컴퓨터 바이러스 이외에, 백도어(Back Door)와 같은 해킹 도구나 트로이안(Trojan)과 같은 스파이웨어 기능이 추가되고 있으며, 그 기능과 파괴력, 그리고 전파 속도는 더욱더 빠르고 강력해지고 있으며, 현금으로 표현되는 웜 바이러스 피해 액수는 상상을 초월할 정도로 커지고 있다.

따라서, 종래부터 상기 웜 또는 웜 바이러스를 차단하기 위하여 여러 가지 방법이 사용되고 있었다.

일반적으로 웜 차단을 위해서는 각 호스트에 백신 프로그램을 설치하거나 게이트웨이 차원에서 사전에 웜이 전산망에 침투하지 못하도록 소프트웨어 기반의 바이러스 차단시스템을 설치한다. 또한 L7 어플리케이션 스위치의 경우 콘텐트 필터링(contents filtering)를 이용하여 웜 공격을 차단할 수 있다.

종래에는 호스트마다 백신 프로그램을 설치한 경우 해당 호스트로 전송되는 데이터 및 파일에 대하여 웜 감염여부를 확인하여 치료하는 기능을 수행하며, 게이트웨이 차원의 바이러스 차단 시스템의 경우 전산망의 시작점이라 할 수 있는 게이트웨이에서 바이러스가 유입/유출되거나 유해한 정보가 드나드는 것을 원천적으로 차단하기 위하여 모든 트래픽에 대하여 바이러스 감염 여부를 검사 및 치료하는 기능을 수행한다. L7 어플리케이션 스위치의 경우 통과하는 패킷의 데이터 부분에 대하여 어플리케이션 레벨에서 웜 공격에 대한 패턴 매칭을 실시하여 공격 패킷으로 판단될 경우 이를 차단함으로써 웜 공격을 방어할 수 있었다. 종래의 호스트 기반에서 백신 프로그램을 설치하여 웜 공격에 대하여 방어할 경우 네트워크의 규모가 커지면서 커질수록 관리자가 관리하기 어려우며, 게이트 웨이 차원에서 웜 차단 시스템을 설치할 경우 소프트웨어 기반으로 구현이 되어 있기 때문에 트래픽이 증가할수록 바이러스 차단 시스템에 걸리는 부하가 늘어나 속도 저하 등의 문제를 초래할 수 있다. 마찬가지로 L7 어플리케이션 스위치를 이용한 경우 콘텐트 필터링(contents filtering) 수행 시 성능 저하 및 장비가 멈추게 될 수 있다는 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

본 발명은 기존 네트워크 환경의 변화 없이 패턴 매칭을 수행하는 하드웨어 기반의 전용 보드를 탑재한 웜 차단 시스템을 웜 공격으로부터 보호하고자 하는 네트워크 앞에 설치하여, 통신 선로상의 모든 패킷에 대하여 손실이나 지연 없이 웜 관련 패턴이 존재하는지를 검사하고 해당 보안규칙에 따라 패킷을 통과시키거나 차단시킨 후 결과를 실시간으로 관리자에게 알려주도록 하는 것으로 특히 기가비트 환경에 적당하도록 한 하드웨어 기반의 웜 관련 패킷의 탐지 및 차단 방법 및 시스템을 제공함을 목적으로 하고 있다.

발명의 구성 및 작용

상기 목적을 달성하기 위한 본 발명의 하드웨어 기반의 웜 관련 패킷의 탐지 및 차단 시스템은 게이트웨이 뒤에 투과(transparent) 모드로 연결되고 웜 공격으로부터 보호받고자 하는 네트워크의 클라이언트나 서버 앞에 설치되어 웜 공격을 차단하기 위한 호스트 시스템과, 상기 호스트 시스템에 설치되며 상기 호스트 시스템으로부터 수신한 보안규칙에 따라 수신되는 패킷에 대한 패턴 매칭을 하여 일치되는 패킷에 대해서 해당 보안규칙에 따라 차단 동작을 하는 PCI 보드를 구비한다.

또한, 본 발명의 웜 관련 패킷의 탐지 및 차단 시스템은 보안규칙을 호스트 시스템으로 전송하고 호스트 시스템으로부터 웜 경고 신호를 받아서 디스플레이하기 위한 관리콘솔을 더 포함할 수 있다.

상기 호스트 시스템은 네트워크 카드를 구비한 일반 컴퓨터 형태이다. PCI 보드는 패킷의 헤더를 체크하는 헤더 서치 엔진, 패턴 매칭을 수행하는 콘텐트 서치 엔진, 패킷 처리를 담당하는 ILC(In Line-Control), 그리고 보안규칙을 저장하고 있는 보안규칙 데이터베이스를 포함한다. ILC는 입력된 데이터 패킷을 헤더 서치 엔진과 콘텐트 서치 엔진으로 보내어 헤더와 콘텐트의 패턴 매칭을 수행하고, 상기 헤더 및 콘텐트 서치 엔진의 패턴 매칭 결과 웜 패턴을 발견한 경우에는 경고 신호를 호스트 시스템으로 전송하고, 상기 발견된 웜 패턴에 대응하는 보안 규칙을 보안규칙 데이터베이스로부터 읽어 들여 그에 따라 패킷을 통과시키거나 차단한다.

또한, 본 발명의 웜 패킷 검색 및 차단 방법은 호스트 시스템에서 PCI 보드를 초기화 하는 단계와, 호스트 시스템에서 웜 패턴을 포함하는 보안 규칙을 PCI 보드로 전송하면 PCI 보드에서 이를 저장하는 단계와, PCI 보드가 입력된 데이터 패킷의 패턴과 저장된 웜 패턴을 비교하여 웜을 탐색하는 단계와, 웜 패턴이 검색되면 PCI 보드가 호스트 시스템에 경고 신호를 전달하는 단계와, PCI 보드가 상기 저장된 보안규칙에서 상기 검색된 웜 패턴에 대응되는 보안 규칙을 찾아서 대응되는 보안 규칙에 따라 상기 웜을 처리하는 단계를 구비한다.

보안규칙은 네트워크를 통해 연결된 관리콘솔로부터 호스트 시스템으로 전송된다. 관리콘솔로부터 호스트 시스템으로 전송되는 보안규칙은 암호화가 되어 있는것이 바람직하며, 이 경우에 호스트 시스템은 수신된 보안규칙을 PCI 보드로 전송하기 전에 복호화한다.

이하, 도면을 참조하여 본 발명의 바람직한 실시예에 대해서 상세히 설명한다.

본 발명에 의한 하드웨어 기반의 패턴 매칭을 이용한 기가비트 환경에서의 웜 차단을 수행하기 위한 구성의 개요도는 도 1에 도시된 바와 같다.

도 1에서 클라이언트(10')와 서버(20')는 인터넷에 연결되어 있고, 웜 공격을 차단하기 위하여 웜 차단 시스템(40)은 기존의 네트워크 환경의 변화 없이 보호하고자 하는 네트워크의 게이트웨이(30) 뒤에 투과(transparent) 모드로 위치하게 된다. 이곳에서 웜 차단 시스템(40)은 보호하고자 하는 네트워크에 있는 호스트 시스템들(10, 20)과 인터넷에 연결된 호스트 시스템들(10', 20')과의 모든 통신 트래픽에 대하여 실시간 웜 탐지 및 차단을 수행하며, 그 결과를 관리콘솔(50)로 전송하게 된다. 그러면, 관리콘솔(50)은 이를 화면에 디스플레이함으로써 관리자가 웜이 발견되었음을 알 수 있도록 한다. 또한 관리콘솔(50)에서는 웜 차단 시스템(40)에 적용할 보안 규칙을 생성할 수 있으며 이를 온라인으로 웜 차단 시스템(40)에 적용할 수 있다.

웜차단 시스템(40)은 호스트 시스템과 호스트 시스템에 설치되는 PCI 형태의 보드로 구성된다. 호스트 시스템은 일반 컴퓨터의 형태를 하고 있으나 실질적으로는 PCI 형태 보드에서 제공하는 로그 정보를 PCI BUS를 이용해서 수신하여 관리콘솔에게 전송하는 기능을 수행한다. 패턴 매칭을 수행하는 PCI 보드 자체에 기가 인터페이스가 있어 네트워크 환경의 변화 없이 인라인(In-Line) 모드로 설치가 가능하며 관리콘솔과의 통신은 호스트 시스템의 네트워크 인터페이스를 사용한다. 호스트 시스템은 TCP/IP 프로토콜을 이용하여 인터넷을 통해 관리 콘솔과 연결되며, 하나의 관리 콘솔에서 원격으로 여러 대의 웜 차단 시스템의 관리를 할 수 있다.

도 2는 관리콘솔(50)에서 수행하는 로그 정보 수신 및 보안규칙 전송에 관련된 기능 흐름도이다. 관리콘솔(50)은 우선 (A1) 단계에서 웜 차단 시스템(40)으로부터 수신된 로그가 있는지 확인한다. 수신된 데이터가 있다면 이를 (A2) 단계에서 SEED 알고리즘으로 복호화 시켜 (A3) 단계에서 화면 출력 및 데이터베이스에 저장하게 된다.

만약 (A1) 단계에서 웜 차단 시스템(40)으로부터 수신된 로그가 없고 (A4) 단계에서 관리자가 웜 관련 패턴 및 정책이 포함된 보안규칙을 전송하려 한다면 관리콘솔(50)은 (A5) 단계에서 전송할 보안규칙을 암호화시킨 후 이를 (A6) 단계에서 해당 웜 차단 시스템(40)으로 전송하게 된다. (A7)단계에서 종료가 아니라면 (A1) 단계에서 (A6) 단계까지의 기능을 반복한다.

도 3은 호스트 시스템의 기능 흐름도이다. 먼저 호스트 시스템은 호스트 시스템에 탑재된 PCI 형태의 패턴 매칭을 담당하는 보드에 대하여 초기화를 수행하고(B1), 관리콘솔(50)로부터 수신한 보안규칙을 파일에서 읽어들여 웜 공격을 탐지할 수 있도록 보드에 적용한다(B2). 또한, 관리 콘솔(50)로부터 보안규칙이 수신되는지를 검사하여(B3), 수신한 보안규칙이 있다면 이를 SEED 알고리즘을 이용하여 복호화 시킨 후 파일로 저장하고(B4), 이를 PCI 보드에 로드한다(B5).

만일, 관리콘솔(50)로부터 보안규칙의 수신이 없다면, 상기 하드웨어 기반의 패턴 매칭을 담당하는 PCI 보드로부터 웜 공격 패킷이 검색되었다는 정보가 전송되는지를 확인한다(B6). PCI 보드로부터 웜 공격 패킷에 대한 정보가 수신되면, 호스트 시스템은 이 정보를 관리 콘솔(50)에서 사용할 로그 형태로 변경하고(B7), 이를 SEED 알고리즘을 이용하여 암호화 시켜서(B8), 이를 관리콘솔(50)로 전송한다(B9). 이러한 과정은 호스트 시스템의 동작이 종료될 때까지 반복된다(B10).

도 4a는 PCI 형태의 패턴 매칭 전용보드의 내부 구성에 대한 블록도이다. PCI 보드는 패킷의 헤더를 체크하는 헤더 서치 엔진(Header Search Engine)(430), 패턴 매칭을 수행하는 콘텐트 서치 엔진(Content Search Engine)(450), 패킷 처리를 담당하는 ILC(In Line-Control)(410), 그리고 보안규칙 데이터베이스(470)로 구성된다.

도 4b는 PCI 보드의 기능 흐름도이다. 도 3의 (B1) 단계에서의 호스트 시스템의 명령에 따라 PCI 보드가 초기화 되면(C1), PCI 보드의 ILC(410)는 입력된 데이터 패킷을 헤더 서치 엔진(430)과 콘텐트 서치 엔진(450)으로 보내어 헤더와 콘텐트의 패턴 매칭을 수행한다(C2). 상기 헤더 및 콘텐트 서치 엔진의 패턴 매칭 결과 웜 패턴을 발견한 경우에(C3), ILC(410)는 로그 메시지를 호스트 시스템으로 전송하고(C4), 상기 발견된 웜 패턴에 대응하는 보안 규칙을 보안규칙 데이터베이스(470)로부터 읽어 들여 그에 따라 패킷을 통과시키거나 차단시킨다(C5). 이러한 과정은 PCI 보드의 동작이 종료될 때까지 반복된다(C6).

한편, 도 4b에는 도시되지 않았으나, 호스트 시스템으로부터 보안규칙의 로드 명령이 수신되면, ILC(410)는 수신된 보안규칙을 보안규칙 데이터베이스(470)에 업데이트한다.

도 5는 관리 콘솔(50)로부터 웜 차단 시스템(40)에 전송되는 보안규칙의 메시지 형태로서 Num은 순번을 의미하며 이 순번이 낮을수록 탐지 우선순위가 상대적으로 높아진다. 로그 형태(log type)은 웜 공격 패킷에 대한 경계 정보를 PCI 버스를 통하여 보드로부터 보드가 설치된 호스트로 전송되는 로그 형태를 정의하는 필드로 로그 형태에 따라 공격명과 패킷 헤더정보만을 전송하는 메시지 형태와 공격명과 패킷 데이터까지 전송하는 전문 형태가 가능하다. 처리는 해당 웜 공격 패킷을 탐지하였을 경우 보드가 취하는 행동을 정의하는 필드로서 패킷허용과 패킷차단으로 설정 가능하며, 웜 패턴은 해당 웜 공격이 갖는 특정 패턴이다.

도 6는 웜 차단 시스템(40)에서 관리 콘솔(50)로 송신되는 로그 메시지 형태로서 src ip, src port, dst ip, dst port는 각각 웜 공격 패킷의 소스 IP 어드레스, 소스포트, 목적지 IP 어드레스, 목적지 포트를 나타내며, time 은 웜 공격이 탐지된 시간을 나타낸다. Protocol은 웜 공격 패킷이 속하는 IP 상위 프로토콜(TCP, UDP, ICMP)을 나타내며 웜 네임은 웜 공격명, 패킷 데이터는 보안규칙의 로그 형태가 전문인 경우에 패킷의 전체 데이터이다.

발명의 효과

상술한 바와 같이 본 발명은 패킷의 손실이나 지연 없이 실시간으로 웜 공격이 들어있는 패킷을 하드웨어 기반의 PCI 카드를 이용하여 탐지 및 차단함으로써 효과적으로 웜 공격에 대하여 방어할 수 있다. 또한 기존의 네트워크 변경 없이 설치 가능하므로 관리상 편리하며, 관리콘솔과 웜 차단 시스템이 SEED 알고리즘을 이용하여 암복호화를 수행하므로 서로 안전하게 통신할 수 있다.

(57) 청구의 범위

청구항 1.

호스트 시스템과 상기 호스트 시스템에 탑재되는 PCI 보드로 이루어지는 웜 차단 시스템을 이용한 웜 차단 방법에 있어서,

호스트 시스템에서 PCI 보드를 초기화 하는 단계;

호스트 시스템에서 웜 패턴을 포함하는 보안 규칙을 PCI 보드로 전송하면 PCI 보드에서 이를 저장하는 단계;

PCI 보드가 입력된 데이터 패킷의 패턴과 저장된 웜 패턴을 비교하여 웜을 탐색하는 단계;

웜 패턴이 검색되면 PCI 보드가 호스트 시스템에 경고 신호를 전달하는 단계;

PCI 보드가 상기 저장된 보안규칙에서 상기 검색된 웜 패턴에 대응되는 보안 규칙을 찾아서 대응되는 보안 규칙에 따라 상기 웜을 처리하는 단계

를 포함하는 것을 특징으로 하는 웜 패킷 검색 및 차단 방법.

청구항 2.

제1항에 있어서,

네트워크를 통해 연결된 관리콘솔로부터 호스트 시스템으로 보안규칙이 전송되면, 호스트 시스템에서 이를 PCI 보드로 전송하고, PCI 보드에서 이를 저장하는 단계를 더 포함하는 것을 특징으로 하는 웜 패킷 검색 및 차단 방법.

청구항 3.

제2항에 있어서,

관리콘솔로부터 호스트 시스템으로 전송되는 보안규칙은 암호화가 되어 있으며,

호스트 시스템은 수신된 보안규칙을 PCI 보드로 전송하기 전에 복호화하는 것을 특징으로 하는 웜 패킷 검색 및 차단 방법.

청구항 4.

제1항에 있어서,

호스트 시스템에서 PCI 보드로부터 경고 신호를 수신하면, 호스트 시스템은 이를 관리콘솔로 전송하는 것을 특징으로 하는 웜 패킷 검색 및 차단 방법.

청구항 5.

제4항에 있어서,

상기 보안규칙에는 웜이 검색되었을 때 PCI 보드에서 전송할 경고 신호의 형태가 포함되는 것을 특징으로 하는 웜 패킷 검색 및 차단 방법.

청구항 6.

제5항에 있어서,

상기 경고 신호의 형태에는 공격명과 패킷 헤더를 전송하는 형태 또는 공격명과 패킷 데이터 전체를 전송하는 형태가 포함되는 것을 특징으로 하는 웜 패킷 검색 및 차단 방법.

청구항 7.

제4항에 있어서,

상기 호스트 시스템은 관리콘솔로 경고 신호를 전송하기 전에 이를 암호화하는 것을 특징으로 하는 웜 패킷 검색 및 차단 방법.

청구항 8.

제1항에 있어서,

상기 보안규칙의 메시지 형태는 Num, 로그 타입, 처리형태, 웜 패턴으로 구성되며,

상기 경고 신호는 소스 IP 주소, 소스 포트, 도달 IP 주소, 도달 포트, 시간, IP 상위 프로토콜, 웜 공격 이름, 패킷 데이터로 구성되는 것을 특징으로 하는 웜 패킷 검색 및 차단 방법.

청구항 9.

하드웨어기반의 패턴 매칭을 이용한 웜 차단 시스템에 있어서,

게이트웨이 뒤에 투과(transparent) 모드로 연결되고 웜 공격으로부터 보호받고자 하는 네트워크의 클라이언트나 서버 앞에 설치되어 웜 공격을 차단하기 위한 호스트 시스템,

상기 호스트 시스템에 탑재되며 상기 호스트 시스템으로부터 수신한 보안규칙에 따라 수신되는 패킷에 대한 패턴 매칭을 하여 일치되는 패킷에 대해서 해당 보안규칙에 따라 차단 동작을 하는 PCI 보드

를 구비하는 웜 패킷 검색 및 차단 시스템.

청구항 10.

제9항에 있어서,

상기 호스트 시스템은 네트워크 카드를 구비한 일반 컴퓨터 형태인 것을 특징으로 하는 웜 패킷 검색 및 차단 시스템.

청구항 11.

제9항에 있어서, 상기 웜 패킷 검색 및 차단 시스템은,

보안규칙을 호스트 시스템으로 전송하고 호스트 시스템으로부터 웜 경고 신호를 받아서 디스플레이하기 위한 관리콘솔을 더 포함하는 것을 특징으로 하는 웜 패킷 검색 및 차단 시스템.

청구항 12.

제9항에 있어서, 상기 PCI 보드는

패킷의 헤더를 체크하는 헤더 서치 엔진,

패턴 매칭을 수행하는 콘텐트 서치 엔진,

패킷 처리를 담당하는 ILC(In Line-Control), 그리고

보안규칙을 저장하고 있는 보안규칙 데이터베이스

를 포함하는 것을 특징으로 하는 웜 패킷 검색 및 차단 시스템.

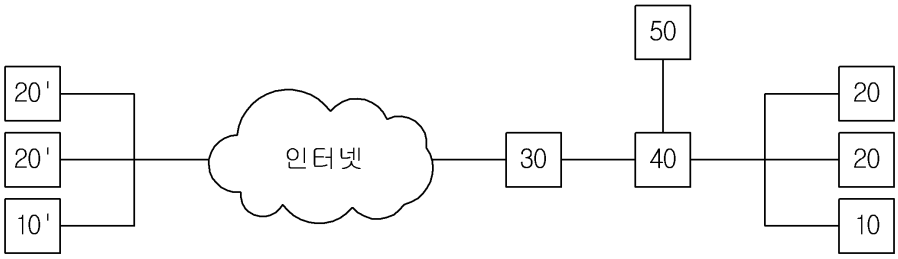
청구항 13.

제12항에 있어서, 상기 ILC는

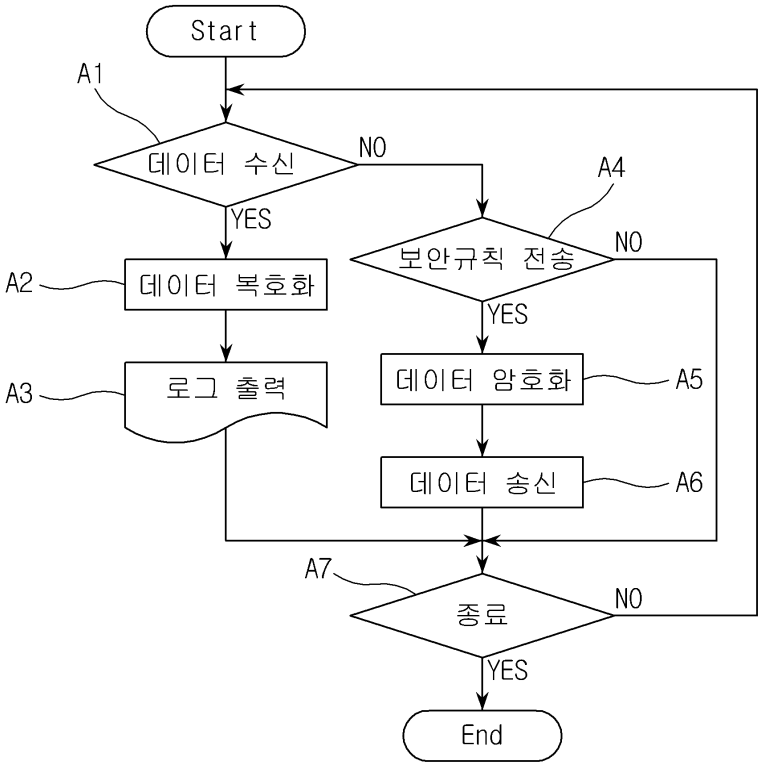
입력된 데이터 패킷을 헤더 서치 엔진과 콘텐트 서치 엔진으로 보내어 헤더와 콘텐트의 패턴 매칭을 수행하고, 상기 헤더 및 콘텐트 서치 엔진의 패턴 매칭 결과 웜 패턴을 발견한 경우에는 경고 신호를 호스트 시스템으로 전송하고, 상기 발견된 웜 패턴에 대응하는 보안 규칙을 보안규칙 데이터베이스로부터 읽어 들여 그에 따라 패킷을 통과시키거나 차단시키는 것을 특징으로 하는 웜 패킷 검색 및 차단 시스템.

도면

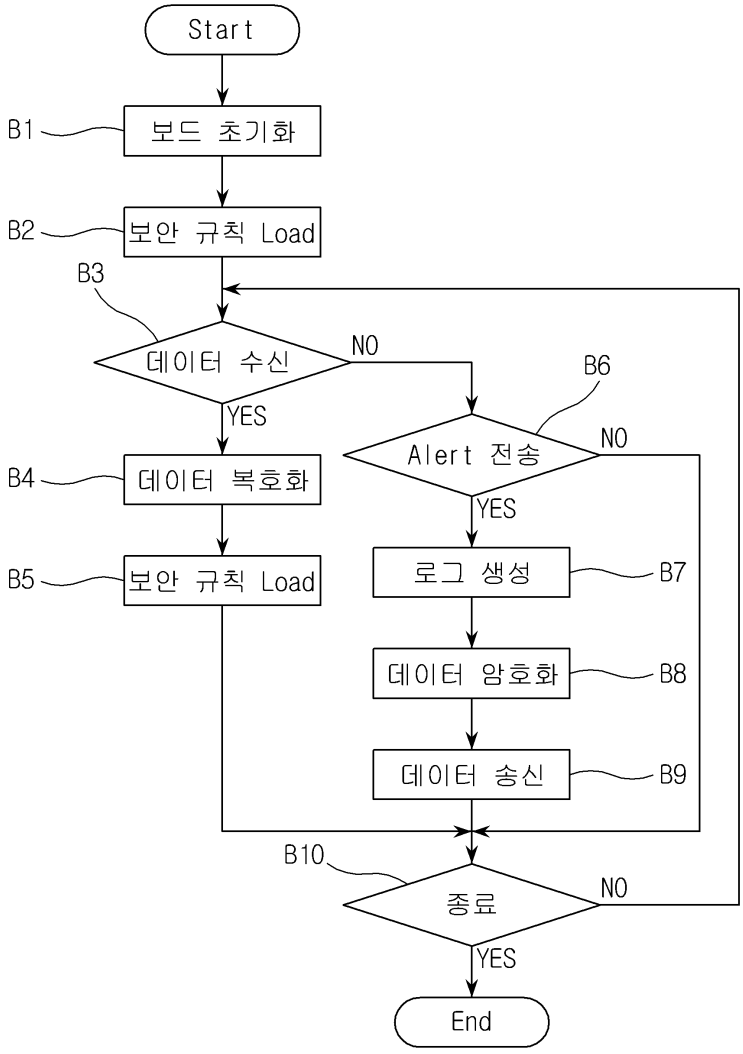
도면1


50
20'
20'
10'
인터넷
30
40
20
20
10

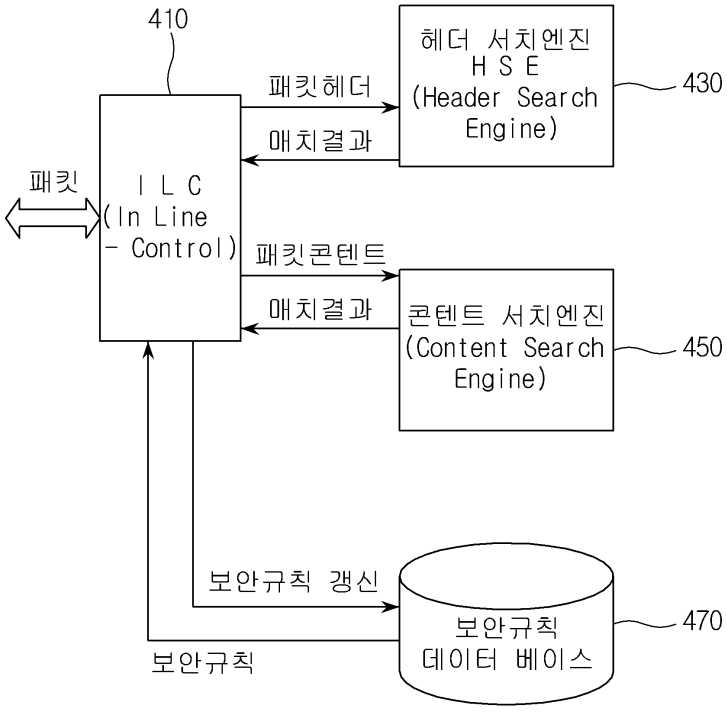
도면2


Start
A1
데이터 수신
NO
YES
A4
보안규칙 전송
NO
YES
A2
데이터 복호화
A3
로그 출력
데이터 암호화
A5
데이터 송신
A6
A7
종료
NO
YES
End

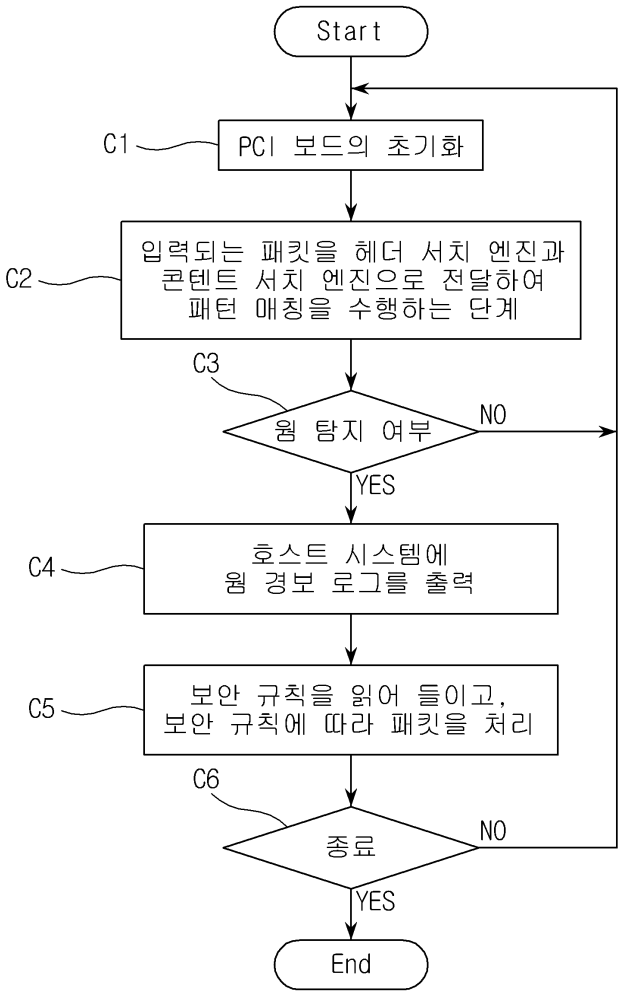
도면3


Start
B1
보드 초기화
B2
보안 규칙 Load
B3
데이터 수신
NO
YES
B4
데이터 복호화
B5
보안 규칙 Load
B6
Alert 전송
NO
YES
로그 생성
B7
데이터 암호화
B8
데이터 송신
B9
B10
종료
NO
YES
End

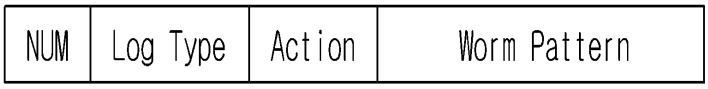
도면4a


410
헤더 서치엔진
H S E
(Header Search
Engine)
430
패킷헤더
매치결과
패킷
I L C
(In Line
- Control)
패킷콘텐트
매치결과
콘텐트 서치엔진
(Content Search
Engine)
450
보안규칙 갱신
보안규칙
보안규칙
데이터 베이스
470

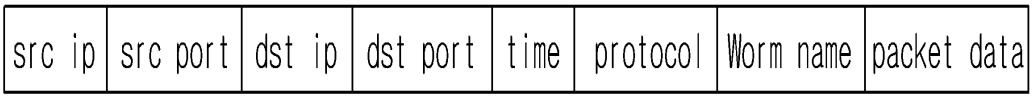
도면4b


Start
C1
PCI 보드의 초기화
C2
입력되는 패킷을 헤더 서치 엔진과
콘텐트 서치 엔진으로 전달하여
패턴 매칭을 수행하는 단계
C3
웜 탐지 여부
NO
YES
C4
호스트 시스템에
웜 경보 로그를 출력
C5
보안 규칙을 읽어 들이고,
보안 규칙에 따라 패킷을 처리
C6
종료
NO
YES
End

도면5


NUM
Log Type
Action
Worm Pattern

도면6


src ip
src port
dst ip
dst port
time
protocol
Worm name
packet data