(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년01월12일
(11) 등록번호 10-0877664
(24) 등록일자 2008년12월30일

(51) Int. Cl.
G06F 11/00 (2006.01)
(21) 출원번호 10-2005-7018428
(22) 출원일자 2005년09월29일
심사청구일자 2006년01월24일
번역문제출일자 2005년09월29일
(65) 공개번호 10-2006-0023952
(43) 공개일자 2006년03월15일
(86) 국제출원번호 PCT/IB2003/005328
국제출원일자 2003년11월20일
(87) 국제공개번호 WO 2004/107706
국제공개일자 2004년12월09일
(30) 우선권주장
03405393.4 2003년05월30일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
KR 1020060013491 A
전체 청구항 수 : 총 10 항

(73) 특허권자
인터내셔널 비지네스 머신즈 코포레이션
미국 10504 뉴욕주 아몬크 뉴오차드 로드
(72) 발명자
리오르단 제임스 에프
스위스 체하-8803 뤼실리콘 알테 란드스트라세 50
(74) 대리인
윤여원, 허정훈

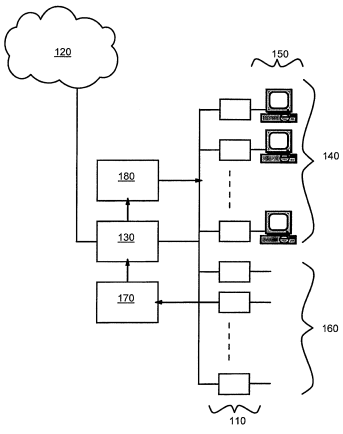
심사관 : 안철용

(54) 어택 검출 방법, 어택 검출 장치, 데이터 통신 네트워크, 컴퓨터 판독 가능 기록 매체 및 침입 검출 애플리케이션의 전개 방법

(57) 요 약

본 발명은 네트워크 내의 데이터 처리 시스템에 할당하기 위한 복수의 어드레스를 구비하는 데이터 통신 네트워크에 대한 어택 검출 방법에 관해 개시한다. 이러한 기법은 임의의 할당된 어드레스(assigned address)에서 발생하여, 임의의 비할당 어드레스(unassigned address)로 어드레싱된 데이터 트래픽(data traffic)을 네트워크 상에서 식별하는 단계를 포함한다. 식별된 임의의 데이터 트래픽은 어택(attack)을 표시하는 데이터가 있는지 검사된다. 상기 어택을 표시하는 상기 데이터가 검출되면 경보 신호(alert signal)가 생성된다.

대 표 도



특허청구의 범위

청구항 1

데이터 통신 네트워크 내의 데이터 처리 시스템에 할당하기 위한 복수의 어드레스를 구비하는 상기 데이터 통신 네트워크에 대한 어택 검출 방법으로서,

임의의 할당된 어드레스(assigned address)에서 발생하여 임의의 비할당 어드레스(unassigned address)로 어드레싱된 데이터 트래픽(data traffic) - 상기 비할당 어드레스는 자유롭고 사용자 데이터 처리 시스템에 할당되지 않은 어드레스임 - 을 네트워크 상에서 식별하는 단계와,

상기 식별된 임의의 데이터 트래픽 중에서 어택(attack)을 표시하는 데이터에 대해 검사하는 단계와,

상기 어택을 표시하는 데이터가 검출되면 경보 신호(alert signal)를 생성하는 단계

를 포함하는 어택 검출 방법.

청구항 2

제 1 항에 있어서,

상기 검사 단계는 식별된 상기 데이터 트래픽 내에 포함된 요청에 대한 응답을 스푸핑(spoofing)하는 단계를 포함하는 어택 검출 방법.

청구항 3

제 1 항에 있어서,

상기 경보 신호가 생성되면, 상기 어택을 표시하는 상기 데이터를 발생시키는 상기 데이터 처리 시스템에 할당된 상기 어드레스에서 발생하는 임의의 데이터 트래픽을 상기 네트워크 상의 감염 제거 어드레스(disinfection address)로 재라우팅(rerouting)하는 재라우팅 단계를 더 포함하는 어택 검출 방법.

청구항 4

제 1 항에 있어서,

상기 경보 신호가 생성되면, 경보 메시지를 상기 감염 제거 어드레스로 전달하는 단계를 포함하는 어택 검출 방법.

청구항 5

제 4 항에 있어서,

상기 경보 메시지는 검출된 상기 어택을 표시하는 데이터를 포함하는 어택 검출 방법.

청구항 6

제 5 항에 있어서,

상기 경보 메시지를 수신하면, 상기 어택을 표시하는 상기 데이터를 발생시키는 상기 데이터 처리 시스템에 할당된 상기 어드레스에 대해 상기 감염 제거 어드레스로부터의 경고 메시지(warning message)를 전송하는 단계를 포함하는 어택 검출 방법.

청구항 7

삭제

청구항 8

데이터 통신 네트워크 내의 데이터 처리 시스템에 할당하기 위한 복수의 어드레스를 구비하는 상기 데이터 통신 네트워크에 대한 어택 검출 장치로서,

제 1 항 내지 제 6 항 중 어느 한 항에 따른 방법의 각각의 단계를 수행하는 각각의 수단을 포함하는

어택 검출 장치.

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

데이터 통신 네트워크로서,

상기 네트워크 내의 데이터 처리 시스템에 할당하기 위한 복수의 어드레스와,

제 8 항에 기재된 상기 네트워크에 대한 어택을 검출하는 장치

를 포함하는 데이터 통신 네트워크.

청구항 16

데이터 처리 시스템의 프로세서 내에 로딩되어, 제 1 항 내지 제 6 항 중 어느 한 항에 따른 데이터 통신 네트워크 상의 어택 검출 방법을 수행하도록 상기 프로세서를 구성하는 컴퓨터 프로그램을 구비한 컴퓨터 판독 가능 기록 매체.

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

객체에 대해 침입 검출 애플리케이션을 전개하는 방법으로서,

임의의 할당된 어드레스에서 발생하여 임의의 비할당 어드레스로 어드레싱된 데이터 트래픽 - 상기 비할당 어드

레스는 자유롭고 사용자 데이터 처리 시스템에 할당되지 않은 어드레스임 - 을 네트워크 상에서 식별하고, 상기 식별된 임의의 데이터 트래픽 중에서 어택을 표시하는 데이터에 대해 검사하며, 상기 어택을 표시하는 데이터가 검출되면 경보 신호를 생성하기 위해 상기 객체에 의해 이용되는 침입 검출 센서를 네트워크에 접속하는 단계와,

상기 경보 신호의 생성에 응답하여, 상기 어택을 표시하는 데이터를 발생시키는 데이터 처리 시스템에 할당된 어드레스에서 발생하는 임의의 데이터 트래픽을 상기 네트워크 상의 감염 제거 어드레스에 대해 재라우팅(rerouting)하는 라우터를 상기 네트워크에 접속하는 단계

를 포함하는 침입 검출 애플리케이션의 전개 방법.

청구항 22

삭제

명 세 서

기 술 분 야

<1> 본 발명은 일반적으로 네트워크 어택(network attacks)의 검출에 관한 것이고, 보다 구체적으로는 데이터 통신 네트워크 상에서의 어택을 검출하는 방법, 장치 및 컴퓨터 프로그램 소자에 관한 것이다.

배 경 기 술

<2> 인터넷은 다수의 상호접속된 데이터 네트워크로 형성된 광대역 데이터 네트워크이다. 동작 시에, 인터넷은 원격으로 위치된 데이터 처리 시스템들의 범위 사이에서 데이터 통신을 구현한다. 이러한 데이터 처리 시스템은 각각 통상적으로 CPU(central processing unit), 메모리 서브시스템, 입/출력 서브시스템 및 CPU에 의해서 실행되며 메모리 서브시스템 내에 저장된 컴퓨터 프로그램 코드를 포함한다. 통상적으로, 인터넷에 접속된 최종 사용자 데이터 처리 시스템은 클라이언트 데이터 처리 시스템 또는 간단하게 클라이언트로서 지칭된다. 이와 마찬가지로, 인터넷을 통해서 클라이언트가 액세스하는 웹 사이트 또는 서비스를 호스팅(host)하는 데이터 처리 시스템은 서버 데이터 처리 시스템 또는 간단하게 서버로서 지칭된다. 최종 사용자 데이터 처리 시스템과 호스팅 데이터 처리 시스템 사이의 인터넷을 통해서 확립된 서버-클라이언트 관계가 존재한다.

<3> 인터넷은 소비자, 소매 상인 및 서비스 제공자 사이에서 전자적으로 실행되는 상업 거래를 용이하게 하는 중요한 통신 네트워크가 되었다. 인터넷으로의 액세스는 통상적으로 ISP(internet service provider)를 통해서 이러한 객체들에게 제공된다. 각각의 ISP는 통상적으로 클라이언트가 가입한 개방형 네트워크(open network)를 동작시킨다. 각 클라이언트에게는 네트워크 상의 IP(Internet Protocol) 어드레스가 제공된다. 마찬가지로, 네트워크 상의 각 서버에도 어드레스가 제공된다. ISP에 의해서 운영되는 네트워크는 라우터(router)로 지칭되는 전용 데이터 처리 시스템을 통해서 인터넷으로 접속된다. 동작 시에, 라우터는 인바운드 통신 트래픽(inbound communication traffic)이 인터넷으로부터 네트워크 상의 지정된 IP 어드레스를 향하게 한다. 마찬가지로, 라우터는 아웃바운드 통신 트래픽(outbound communication traffic)이 네트워크로부터 인터넷 상의 특정 어드레스 방향으로 향하게 한다.

<4> 여러 ISP가 직면하는 문제점은 그들이 작동시키는 네트워크에 대한 전자적 어택의 빈도수가 증가한다는 것이다. 이러한 어택은 컴퓨터 바이러스 어택, 소위 "웜(worm)" 어택을 포함한다. 이러한 특성의 웜 어택은 ISP에 의해 작동되는 네트워크의 상당한 성능 저하를 유발한다. 이 네트워크에 접속된 감염된 시스템은 통상적으로 그 네트워크 내부에서 그 감염을 확산시키려 한다. 수많은 사용자가 이러한 시스템들이 감염되었음을 인식하지 못한다. 이러한 시스템에 대해서, 네트워크의 성능 증가를 위해 감염 제거(disinfection)를 트리거(triggering)하는 기술을 제공하는 것이 바람직할 것이다.

발명의 상세한 설명

<5> 본 발명에 따르면, 네트워크 내의 데이터 처리 시스템에 할당하기 위한 복수의 어드레스를 구비하는 데이터 통신 네트워크에 대한 어택 검출 방법이 제공되는데, 이 방법은 임의의 할당된 어드레스(assigned address)에서 발생되고, 임의의 비할당 어드레스(unassigned address)에 대해 어드레싱된 데이터 트래픽(data traffic)을 네트워크 상에서 식별하는 단계와, 식별된 임의의 데이터 트래픽 중에서 어택(attack)을 표시하는 데이터에 대해 검사하는 단계와, 상기 어택을 표시하는 상기 데이터가 검출되면 경보 신호(alert signal)를 생성하는 단계를

포함한다.

<6> 본 명세서에서 "비할당(unassigned)"이라는 용어는 침입을 검출하거나 어택 서명(attack signature)을 생성하는 장치 이외의 다른 물리적 디바이스로 할당되지 않는 어드레스를 포함하는 것을 의미한다. 즉, 비할당이라는 용어는 자유로운, 즉 사용자 시스템에 할당되지 않은 어드레스를 포함하는 것을 의미한다. 본 발명에 따른 방법을 실행하도록 설계된 장치는 본 발명을 사용하기 위해서 상기 "비할당" 어드레스로 실제로 할당되는 디바이스일 것이다. 이들 어드레스는 서명 생성 또는 침입 검출 기능 이외의 다른 기능을 갖는 임의의 디바이스로 할당되지 않기 때문에 지금까지는 비할당 상태에 있다. 이로써, 이러한 할당되지 않는 어드레스로 어드레싱된 데이터 트래픽은 상기 장치에 의해 수신되며 청구된 방법에 의해 처리된다.

<7> 상기 검사 단계는 식별된 상기 데이터 트래픽 내에 포함된 요청에 대한 응답을 스푸핑(spoofing)하는 단계를 포함하는 것이 바람직하다. 본 발명의 바람직한 실시예는 상기 경보 신호가 생성되면, 상기 어택을 표시하는 상기 데이터를 발생시키는 상기 데이터 처리 시스템에 할당된 상기 어드레스에서 발생하는 임의의 데이터 트래픽을 상기 네트워크 상의 감염 제거 어드레스(disinfection address)에 대해 재라우팅(rerouting)하는 재라우팅 단계를 더 포함한다. 상기 경보 신호가 생성되면, 경보 메시지는 상기 감염 제거 어드레스로 전달될 수 있다. 상기 경보 메시지는 검출된 상기 어택을 표시하는 데이터를 포함할 수 있다. 상기 경보 메시지를 수신하면, 상기 어택을 표시하는 상기 데이터를 발생시키는 상기 데이터 처리 시스템에 할당된 상기 어드레스에 대해 상기 감염 제거 어드레스로부터의 경고 메시지(warning message)를 전송하는 단계를 포함한다. 경고 메시지는 어택을 표시하는 데이터를 발생시키는 데이터 처리 시스템에 의해 실행될 때 어택을 제거하는 프로그램 코드를 포함할 수 있다.

<8> 본 발명의 다른 측면을 고려하면, 네트워크 내의 데이터 처리 시스템에 할당하기 위한 복수의 어드레스를 구비하는 데이터 통신 네트워크에 대한 어택 검출 장치가 제공되는데, 이 장치는 임의의 할당된 어드레스에서 발생되고 임의의 비할당 어드레스에 대해 어드레싱된 데이터 트래픽을 네트워크 상에서 식별하고, 식별된 임의의 데이터 트래픽 중에서 어택을 표시하는 데이터에 대해 검사하며, 상기 어택을 표시하는 데이터가 검출되면 경보 신호를 생성하는 침입 검출 센서(intrusion detection sensor : IDS)를 포함한다.

<9> IDS는 사용 중에 식별된 상기 데이터 트래픽 내에 포함된 요청에 대한 응답을 스푸핑함으로써 식별되는 상기 데이터 트래픽을 검사하는 것이 바람직하다. 또한 이러한 장치는 상기 침입 검출 센서에 접속되어, 상기 경보 신호의 생성에 응답하여 상기 어택을 표시하는 상기 데이터를 발생시키는 상기 데이터 처리 시스템에 할당된 상기 어드레스에서 발생하는 임의의 데이터 트래픽을 상기 네트워크 상의 감염 제거 어드레스에 대해 재라우팅(rerouting)하는 라우터를 더 포함할 수 있다. 바람직하게는, IDS는 상기 경보 신호가 생성되면 상기 감염 제거 어드레스에 경보 메시지를 전달한다. 경보 메시지는 검출된 상기 어택을 표시하는 데이터를 포함하는 것이 바람직하다. 본 발명의 바람직한 실시예는 상기 감염 제거 어드레스로 할당되어, 상기 경보 메시지를 수신하면, 상기 어택을 표시하는 상기 데이터를 발생시키는 상기 데이터 처리 시스템에 할당된 상기 어드레스에 대해 경고 메시지(warning message)를 전달하는 감염 제거 서버를 더 포함한다.

<10> 본 발명은 또한 데이터 통신 네트워크로 확장될 수 있는데, 이러한 데이터 통신 네트워크는 상기 네트워크 내의 데이터 처리 시스템에 할당하기 위한 복수의 어드레스와, 상술된 바와 같은 상기 네트워크에 대한 어택을 검출하는 장치를 포함한다.

<11> 본 발명은 컴퓨터 프로그램 소자를 더 포함하는데, 이러한 컴퓨터 프로그램 소자는 데이터 처리 시스템의 프로세서에 로딩될 때, 상기 프로세서가 상술된 바와 같은 데이터 통신 네트워크 상의 어택 검출 방법을 수행하게 하는 컴퓨터 프로그램 코드 수단을 포함한다.

<12> 본 발명의 바람직한 실시예에서는 데이터 통신 네트워크가 제공되는데, 이러한 데이터 통신 네트워크는 복수의 데이터 처리 시스템을 인터넷에 접속시키는 라우터와, 라우터에 접속된 IDS와, 라우터에 또한 접속된 감염 제거 서버를 포함한다. IDS가 데이터 처리 시스템 중의 하나가 어택에 의해 감염되었다는 것을 검출하는 것에 응답하여, IDS는 라우터에게 명령하여 해당 어택으로부터의 모든 네트워크 트래픽이 감염 제거 서버로 편향되게 한다. IDS는 그와 동시에 감염 제거 데이터를 감염 제거 서버에 공급한다. 감염 제거 데이터는 감염의 특성, 감염된 시스템을 감염 제거하는 방법 및 정규 네트워크 접속성을 회복하는 방법을 나타낸다.

<13> 일반적으로, 주어진 네트워크 상에는 다수의 자유 IP 어드레스가 존재한다. 본 발명의 특히 바람직한 실시예에서, IDS는 네트워크 상에서 자유 IP 어드레스를 향하는 트래픽을 감시한다. 이러한 트래픽은 존재해서는 안 된다. 자유 IP 어드레스 중의 하나에 대해 전달된 요청이 검출되면, IDS는 요청에 대한 응답을 스푸핑한다. 자

유 IP 어드레스는 사용 중이 아니다. 따라서, 예를 들면, 해당 어드레스에서의 서버에 대한 모든 접촉 시도는 선험적 의심 대상(a priori suspicious)이 된다. 다음에 IDS는 스푸핑된 응답에 대한 응답을 감시한다. IDS가 응답 내에서 진단 가능한 어택(diagnosable attack)을 검출하면, IDS는 라우터에게 시그널링하여 감염된 시스템으로부터의 모든 트래픽이 감염 제거 서버로 편향되게 한다. 왜냐하면, IDS는 감염된 시스템에 대한 응답을 대화식으로 스푸핑하기 때문에, 각각의 어택에 대한 정확한 관점을 갖고 있다. 따라서, 잘못된 긍정 응답(false positives)이 최소화된다.

<14> 본 발명의 바람직한 실시예는 첨부된 도면을 참조하여 오로지 예로서 이하에 설명될 것이다.

실 시 예

<19> 먼저 도 1을 참조하면, 데이터 처리 시스템은 CPU(1), I/O 서브시스템(20) 및 메모리 서브시스템(40)을 포함하며, 이들 구성 요소들은 모두 버스 서브시스템(30)에 의해서 상호접속된다. 메모리 서브시스템(40)은 RAM(random access memory), ROM(read only memory) 및 하드 디스크 드라이브, 광 디스크 드라이브 등과 같은 하나 이상의 데이터 저장 디바이스를 포함할 수 있다. I/O 서브시스템(20)은 디스플레이, 프린터, 키보드 및 마우스, 트랙 볼 등과 같은 포인팅 디바이스 및 데이터 네트워크를 통해서 데이터 처리 시스템과 하나 이상의 유사한 시스템 및/또는 주변 디바이스 간의 통신을 가능하게 하는 하나 이상의 네트워크 접속부를 포함할 수 있다. 이러한 네트워크에 의해 상호접속된 이러한 시스템 및 디바이스의 결합은 그 자체로 분산형 데이터 처리 시스템을 형성할 수 있다. 이러한 분산형 시스템은 그 자체로 추가적인 데이터 네트워크와 상호접속될 수 있다.

<20> 메모리 서브시스템(40) 내에는 CPU(10)에 의해 실행되는 컴퓨터 프로그램 코드(50) 및 데이터(60)가 저장된다. 프로그램 코드(50)는 운영 체제 소프트웨어(90) 및 애플리케이션 소프트웨어(80)를 포함한다. CPU(10)에 의해서 실행될 때에 운영 체제 소프트웨어(90)는 애플리케이션 소프트웨어(80)가 실행될 수 있는 플랫폼을 제공한다.

<21> 도 2를 참조하면, 본 발명의 바람직한 실시예에서, 네트워크 내의 데이터 처리 시스템으로 할당하기 위한 다수의 어드레스(100)를 갖는 데이터 통신 네트워크(100)가 제공된다. 본 발명의 특히 바람직한 실시예에서, 네트워크(100)는 복수의 할당 가능 인터넷 프로토콜(IP) 어드레스(110)를 구비하는 인터넷 서비스 시설(internet service installation)의 형태를 갖는다. 네트워크(100)는 라우터(130)를 통해서 인터넷(120)으로 접속된다. 라우터(130)는 데이터 패킷 내에서 특정된 IP 어드레스 데이터를 기반으로 하여 인터넷(120)과 네트워크(100) 사이에서 데이터 패킷의 형태로 통신 트래픽을 라우팅하는 작업을 적절하게 프로그래밍함으로써 앞서 설명된 도 1을 참조하여 상술된 바와 같은 데이터 처리 시스템의 형태로 구현될 수 있다. 네트워크(100) 상의 IP 어드레스(110)의 제 1 그룹(140)은 인터넷 서비스의 사용자에 속하는 시스템(150)으로 할당된다. 각 시스템(150)은 도 1을 참조하여 상술된 데이터 처리 시스템일 수 있다. 네트워크(100) 상의 IP 어드레스(110)의 제 2 그룹(160)은 자유 상태이다. 보다 구체적으로, IP 어드레스(110)의 제 2 그룹(160)은 사용자 시스템(150)에 할당되지 않는다. 침입 검출 센서(IDS)(170)는 또한 네트워크(100)로 접속된다. IDS(170)는 또한 라우터(130)에 접속된다. IDS(170)의 세부 사항은 이하에서 제공될 것이다. 라우터(130)는 감염 제거 서버(180)에 접속된다. 감염 제거 서버(180)는 도 1을 참조하여 상술된 바와 같은 데이터 처리 시스템에 의해서 구현될 수 있다.

<22> 도 3을 참조하면, 본 발명의 특히 바람직한 실시예에서, IDS(170)은 도 1을 참조하여 상술된 데이터 처리 시스템을 포함한다. IDS(170)의 애플리케이션 소프트웨어(80)는 침입 검출 코드(200)를 포함한다. IDS(170)의 메모리 서브시스템(170) 내에 저장된 데이터(60)는 어택 식별 데이터(210) 및 감염 제거 데이터(220)를 포함한다. 또한, 데이터(60)는 네트워크(100) 상의 IP 어드레스가 비어있고, 제 2 그룹(160)에 속하며 네트워크(100) 상의 IP 어드레스가 데이터 처리 시스템(150)으로 할당되고 제 1 그룹(140)에 속하는 레코드를 포함한다. 이 레코드는 다른 어드레스가 할당되거나 기존의 어드레스 할당이 제거될 때마다 갱신된다. 어택 식별 데이터(210)는 알려진 어택을 식별하는 서명을 표시하는 데이터를 포함한다. 감염 제거 데이터(220)는 각 어택의 성질, 각 어택으로 감염된 시스템의 감염을 제거하는 방법, 정상적인 네트워크 접속을 재개하는 방법을 표시하는 데이터를 포함한다. 어택 식별 데이터(210) 및 감염 제거 데이터(220)는 상호 참조된다. CPU(10)에 의해서 실행될 때에 침입 검출 코드(200)는 도 4에 도시된 흐름도에 따라서 작동하도록 IDS(170)를 구성한다.

<23> 도 4를 참조하면, 동작 시에, IDS(170)는 임의의 비할당 어드레스(160)로 어드레싱되며 임의의 할당된 어드레스(140)에서 발생하는 데이터 트래픽을 네트워크(100) 상에서 식별한다. IDS(170)는 어택을 표시하는 데이터에 대해서 식별된 임의의 데이터 트래픽을 검사한다. 어택을 표시하는 데이터의 검출 후에, IDS(170)는 경보 신호를 생성한다. 본 발명의 바람직한 실시예에서, 경보 신호의 생성 후에, 어택을 표시하는 데이터를 발생하는 데

이터 처리 시스템(150)으로 할당된 어드레스(140)에서 발생하는 임의의 데이터 트래픽은 네트워크(100) 상의 감염 제거 어드레스로 재라우팅된다. 특히 바람직한 실시예에서, IDS(170)는 네트워크(100) 상에서 자유 IP 어드레스(160)로 향하는 트래픽을 감시한다. 구체적으로, 블록(300)에서, IDS(170)는 네트워크(100) 상의 어드레스(140)로부터 전송된 요청을 검사하여 블록(310)에서 그 요청이 자유 IP 어드레스(160) 중 하나를 수신지 어드레스로 지정하는지 여부를 결정한다. 그 요청이 자유 IP 어드레스(160) 중 하나를 지정하지 않으면, 블록(320)에서 IDS(170)는 다음 요청을 검사할 것을 대기한다.

<24> 식별은 IDS(170)에 대해 비할당 어드레스를 할당함으로써 실현될 수 있으며 이로써 비할당 어드레스로 향하는 임의의 트래픽이 IDS(170)로 자동적으로 도달할 수 있게 된다.

<25> 그러나, 그 요청이 자유 IP 어드레스(160) 중 적어도 하나를 지정하면, 블록(330)에서 IDS(170)는 요청에 대한 응답을 스푸핑한다. 응답은 네트워크(100) 상의 IP 어드레스로 전송된다. 자유 IP 어드레스(160)는 사용되지 않고 있다. 따라서, 가령 이러한 어드레스에서 시스템을 접촉하려는 시도는 선험적 의심 대상이 된다. 블록(340)에서, IDS(170)은 스푸핑된 응답에 대한 응답을 감시한다. IDS(170)는 어떠한 응답도 사전결정된 기간 내에 수신되지 않으면 타이밍 아웃할 수 있으며, 이 경우에 블록(320)에서 IDS(170)는 다음 요청을 검사할 것을 대기한다. 그러나, 응답이 수신되면, 블록(350)에서 IDS(170)는 의심이 가는 요청 및 응답을 메모리 서브시스템(40) 내에 저장된 어택 식별 데이터(210)와 비교한다. 만일 블록(350)에서 비교 결과가 어택을 식별하는 것을 실패하면, 블록(320)에서 IDS(170)는 다음 요청을 검사할 것을 대기한다. 그러나, 블록(350)에서 비교 결과가 응답 내에서 진단가능한 어택을 검출하면, IDS(170)는 소스 시스템(150)이 감염되었다고 결정한다. 따라서, 블록(360)에서 IDS(170)는 경보 신호를 생성한다. 경보 신호는 라우터(130)로 전송된다. 경보 신호는 라우터(130)로 하여금 감염된 시스템(150)으로부터의 모든 데이터 트래픽을 감염 제거 어드레스로 편향되게 한다. 다시 도 1을 참조하면, 본 발명의 특히 바람직한 실시예에서 감염 제거 서버(180)는 감염 제거 어드레스에 위치된다.

<26> 본 발명의 바람직한 실시예에서, 경보 신호가 생성되면 IDS(170)는 감염 제어 어드레스에 대해 경보 메시지를 전달한다. 바람직하게는 경보 메시지는 검출된 어택을 나타내는 데이터를 포함한다. 따라서, 본 발명의 특히 바람직한 실시예에서, IDS(170)는 메모리 서브시스템(40)에서 검출된 어택에 대응하는 감염 제거 데이터(220)를 검색한다. 블록(370)에서, IDS(170)는 검색된 감염 제거 데이터를 포함하는 경보 신호를 감염 제거 서버(180)가 위치한 감염 제거 어드레스로 전송한다. 이어서, 블록(320)에서, IDS(170)는 다음 요청을 검사하기를 대기한다. 각 요청, 응답 및 이 응답에 대한 응답은 네트워크(100) 상에서 하나 이상의 데이터 트래픽 패킷으로 구현될 수 있다. 따라서, 각 어택의 서명을 하나 이상의 패킷을 걸쳐 있을 수 있다.

<27> 본 발명의 바람직한 실시예에서, 감염 제거 서버(180)로 전송된 감염 제거 데이터(220)는 검출된 어택의 성질, 어택에 감염된 시스템(150)의 감염을 제거하는 방법, 정상적인 네트워크 접속을 재개하는 방법을 표시하는 데이터를 포함한다. 감염 제거 데이터(220)를 IDS(170)로부터 수신한 후에, 감염 제거 서버(180)는 감염된 시스템(150)을 치료하며 네트워크(100)를 복구하도록 설정된다. 본 발명의 다른 바람직한 실시예에서, 감염 제거 데이터(220)는 어택의 성질을 나타내는 데이터를 포함한다. 이어서, 감염 제거 서버는 어택의 성질을 기반으로 하여 감염된 시스템(150)의 감염을 제거하고/또는 네트워크(100)를 복구하기 위한 다수의 사전저장된 기술 중 하나를 선택하여 이 선택된 기술을 실행한다. 이 어택은 수 많은 상이한 형태를 포함할 수 있다. 따라서, 감염 제거 및 네트워크 복구를 위한 대응하는 기술은 어택마다 광범위하게 변할 수 있다.

<28> 본 발명의 바람직한 실시예에서, 감염 제거 데이터를 수신한 후에, 감염 제거 서버(180)는 경고 메시지를 감염된 시스템(150)으로 전송한다. 경고 메시지는 감염된 시스템(150)의 사용자에게 그가 소유하는 시스템이 감염되었음을 알린다. 이 메시지는 사용자로 하여금 감염된 시스템(150) 내에 사전저장된 바이러스 제거 소프트웨어를 동작하여서 감염을 제거하거나 아니면 감염을 격리하도록 지시한다. 이와 달리, 이 메시지는 감염된 시스템(150) 상에서 감염 제거 코드를 실행할 시에 사용자를 보조하는 지침서와 함께, 감염된 시스템(150)으로부터 어택을 제거하기 위한 감염 제거 프로그램 코드를 포함할 수 있다. 다른 실시예에서, 이 메시지는 사용자를 적절한 감염 제거 프로그램 코드가 제공되는 다른 웹 사이트로 향하게 한다. 본 발명의 다른 바람직한 실시예에서, 이 메시지는 감염된 시스템 상에 로딩되어 자동 실행되어 사용자에게 투명한 방식으로 감염을 제거 또는 격리하는 감염 제거 프로그램 코드를 포함한다. 다른 감염 제거 방식도 가능하다.

<29> 상술한 본 발명의 실시예에서, 감염 제거 서버(180)는 도 1에서 참조하여 상술된 바와 같은 단일 데이터 처리 시스템으로 구현된다. 그러나, 본 발명의 다른 실시예에서, 감염 제거 서버(180)는 다수의 상호접속된 데이터 처리 시스템으로 구현된다. 이러한 데이터 처리 시스템들은 분산형 또는 "팜(farm)" 형태로 배치된다. 감염

제거 서버 내의 각 데이터 처리 시스템은 상이한 어택을 처리하는 데에만 전적으로 이용된다. IDS(170)는 또한 다수의 통합된 데이터 처리 시스템으로 구현될 수 있다. 이와 달리, IDS(170) 및 감염 제거 서버(18)는 단일 데이터 처리 시스템으로 통합될 수 있다.

<30> 감염된 시스템(150)으로부터 전송되고 라우터(130)에 의해서 감염 제거 서버(180)로 편향된 네트워크(100) 상의 트래픽은 감염 제거 서버(180)에 의해서 기록(logged) 및/또는 폐기될 수 있다. 상술된 본 발명의 바람직한 실시예에서, IDS(170)는 감염 제거 데이터를 감염 제거 서버(180)로 전송한다. 그러나, 본 발명의 다른 실시예에서, 일단 감염이 검출되면, IDS(170)는 간단하게 라우터(130)로 하여금 IDS(170)가 추가적으로 감염 제거 데이터(220)를 감염 제거 서버(180)로 제공할 필요 없이, 트래픽을 감염된 시스템(150)으로부터 감염 제거 서버(180)로 편향되게 할 수 있다. 이어서, 감염 제거 서버(180)는 간단하게 감염된 시스템(150)에서 발생하는 트래픽에 대한 저장소로서 기능하며 감염된 시스템(150)으로부터 수신한 트래픽을 기록 및/또는 폐기한다. 기록 및 폐기는 감염 제거 서버(180)에 의해서 네트워크(100)의 운영자에게 보고된다. 이러한 보고는 주기적으로 또는 실시간으로 전달될 수 있다. 이러한 보고는 가령 운영자 콘솔(administration console)을 통해서 수행될 수 있다. 그러나, 가령 출력 인쇄와 같은 다른 보고 기술도 가능하다. 이러한 보고를 수신한 후에, 운영자는 네트워크(100)의 감염을 제거하거나 이와 달리 억제시키는 등 적절한 행동을 취할 수 있다.

<31> 본 발명의 상술된 바람직한 실시예에서, IDS(170), 라우터(130) 및 감염 제거 서버(180)는 적절한 프로그램 코드로 프로그래밍된 데이터 처리 시스템에 의해서 구현된다. 그러나, 본 발명의 다른 실시예에서 소프트웨어로 구현되는 바와 같은 상술된 하나 이상의 기능은 고정 배선형 논리 회로(hardwired logic circuitry)에서 적어도 부분적으로 구현될 수 있다.

<32> 또한, 본 명세서에서 상술된 어택 검출 방법은 네트워크(100)를 책임지는 서비스 제공자에 의해 구현되거나 제3 자에 의해서 이 서비스 제공자에 대한 서비스의 형태로 적어도 부분적으로 구현될 수 있다. 이러한 서비스는 서비스 제공자에 의해 제공된 서비스를 그의 경쟁자에 의해 제공된 서비스와 차별화한다. 이러한 구별된 서비스들은 추가적 프리미엄을 위해 거래에서 제공되는 네트워크 서비스의 최종 사용자에 선택적으로 제공될 수 있다.

<33> 서비스 제공자 이외의 다른 객체에 의해 사용된 네트워크에 대해 어택 서명을 검출하는 서비스는 바람직한 실시예에서 제공된 서비스에 대해 청구(billing)하는 단계를 포함한다. 청구될 요금은 통상적으로 서비스 제공자에 의해 체험된 작업량 또는 복잡도를 표시하는 하나 이상의 다수의 요소에 따라서 결정될 수 있다. 제공된 서비스의 양 및 시간 소비량을 표시하는 이러한 요소들은 네트워크의 크기, 모니터링된 비할당 어드레스의 개수, 모니터링된 할당된 어드레스의 개수, 검사된 데이터 트래픽의 용량, 식별된 어택의 개수, 생성된 경보의 개수, 재라우팅된 데이터 트래픽의 용량을 포함한다. 증가된 복잡성 레벨을 식별하는 요소는 식별된 어택의 서명, 성취된 네트워크 보안 정도일 수 있다. 또한, 서비스된 객체에 제공된 서비스의 값을 식별하는 요소들은 객체의 거래액, 객체의 사업 분야 등과 같은 것이다.

<34> 물론, 이전에 언급된 요소들의 임의의 조합이 가능한데, 특히 이는 최종 청구액을 결정하는데 있어서 상이한 가중치를 부여받는다. 청구 단계는 청구액이 어택 검출 프로세스에서 전송된 메시지 중의 하나와 함께 전송된다는 점에서 자동화될 수 있다. 이는 어택 처리를 위해서 메시징을 사용하는 것과 청구 목적을 위해서 그를 사용하는 것을 결합한다는 점에서 유리하다. 이러한 메시지를 이중 사용하면 어택 검출 및 청구 프로세스를 통해 생성된 트래픽 흐름을 감소시키는 기술적 이점을 제공한다. 이와 동시에, 이 방법은 서비스된 객체가 오직 정확하게 제공된 서비스에 대해서만 청구되도록 보증하는데 사용될 수 있다.

<35> 청구를 위한 다른 바람직한 방법은 어택 검출 서비스에 대한 가입을 객체에게 제안하는 것으로서, 이 서비스에 가입하게 되면 객체는 사전결정된 시간, 트래픽의 양, 시스템의 개수 등에 대해서 이득을 얻게 된다. 서비스 제공자는 서비스된 객체에 의해 사용된 네트워크와 결합되어 사용될 호스팅 유닛으로서 그 자신의 감염 제거 서버를 제공할 수 있지만, 감염 제거 서버는 서비스된 객체에 의해서 유지, 관리 및 호스팅 또는 임대될 수 있다.

<36> 바람직한 실시예에서, 서비스 제공자는 어택 검출 서비스를 몇몇 객체에 제공하고 라우터(130), 침입 검출 센서(170) 또는 감염 제거 서버(180)와 같은 자원을 몇 개의 서비스 사이에서 공유함으로써 시너지 효과를 이용할 수 있다. 이로써, 사용된 자원이 효율적으로 사용될 뿐만 아니라 상이한 네트워크 간의 어택 관련 정보가 공유되고 서비스된 네트워크 상의 검출 품질을 개선시키는 데 이용될 수 있다. 가령, 한 네트워크 상의 어택의 검출은 다른 네트워크 상의 검출을 신속하게 하는데, 그 이유는 어택 서명을 결정하는 프로세스가 단축되거나 심지어 제거될 수 있기 때문이다. 또한, 감염 제거 메커니즘이 서비스된 객체들 간에서 공유되며 이로써 감염 제거 메커니즘을 갱신 및 유지하는데 있어서 관련된 노력 및 비용을 줄일 수 있다. 다른 서비스된 객체의 어택을

처리를 개선하기 위해서 한 객체의 네트워크에 대한 어택을 처리하는 것으로부터 유도되는 기술적 데이터를 공유하는 기술적 이점은 침입 검출을 위해 동일한 서비스 제공자에 의해 서비스되는 풀(pool)을 여러 객체에게 제공함으로써 객체에 대한 인센티브를 제공한다는 점이다. 청구 모델은 바람직한 실시예에서 검출 자원을 공유하며 동일한 서비스 제공자를 사용하는 객체 그룹 내에 객체들의 가입을 유도하도록 구성될 수 있다.

<37> 본 명세서에서 "접속하다(connect)"라는 단어는 물리적 접속으로 한정되지 않는다. 예를 들면, 이것은 정보의 송신 및 수신을 가능하게 하는 일반적인 링크를 포함하도록 의도되었다. 여기에서 이러한 접속은 간접적일 수 있다.

도면의 간단한 설명

<15> 도 1은 데이터 처리 시스템을 도시하는 블록도.

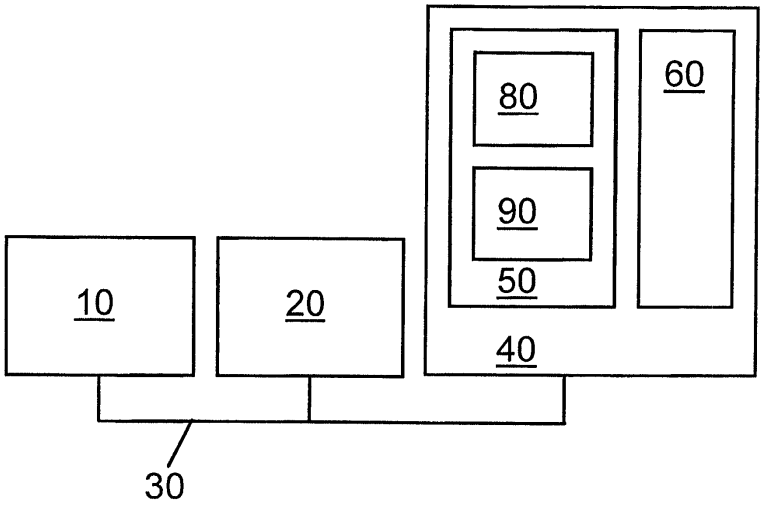
<16> 도 2는 본 발명에서 구현된 데이터 처리 네트워크를 도시하는 블록도.

<17> 도 3은 본 발명에서 구현된 침입 검출 센서를 도시하는 블록도.

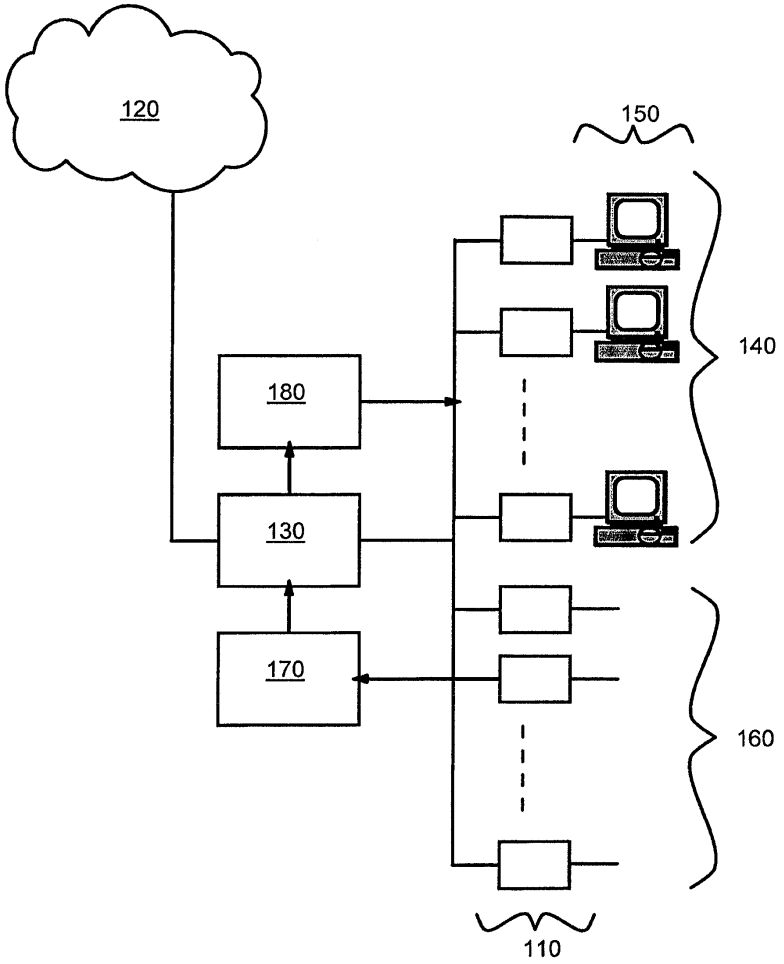
<18> 도 4는 침입 검출 센서와 연관된 흐름도.

도면

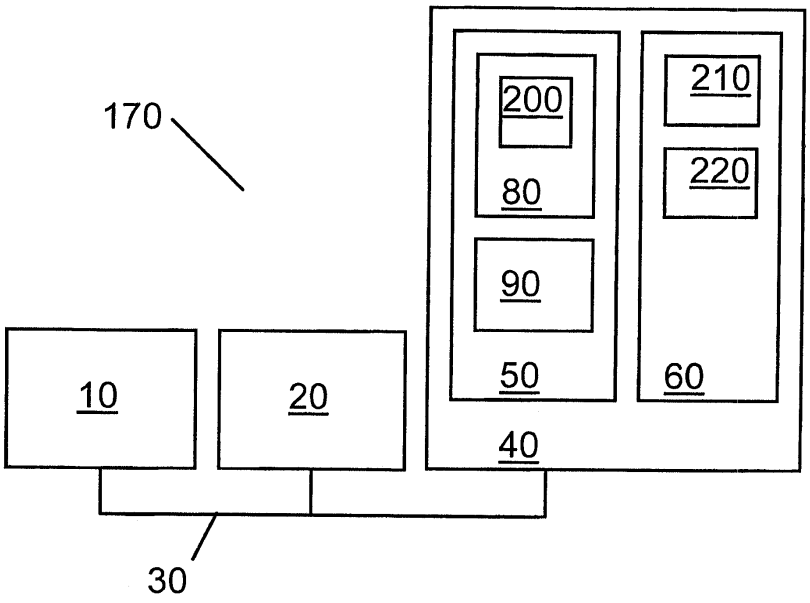
도면1



도면2


120
150
140
180
130
170
160
110

도면3


170
200
80
90
50
210
220
60
40
10
20
30

도면4