(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0044524
(43) 공개일자 2016년04월25일

(51) 국제특허분류(Int. Cl.)
G06F 21/55 (2013.01) *G06F 21/51* (2013.01)
H04L 29/02 (2006.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
G06F 21/554 (2013.01)
G06F 21/51 (2013.01)
(21) 출원번호 10-2016-7006706
(22) 출원일자(국제) 2014년03월19일
심사청구일자 없음
(85) 번역문제출일자 2016년03월14일
(86) 국제출원번호 PCT/US2014/031244
(87) 국제공개번호 WO 2015/023316
국제공개일자 2015년02월19일
(30) 우선권주장
13/967,155 2013년08월14일 미국(US)

(71) 출원인
첸, 다니엘
미국, 98108 워싱턴, 시애틀, 에스. 브랜던 코트 2534
(72) 발명자
첸, 다니엘
미국, 98108 워싱턴, 시애틀, 에스. 브랜던 코트 2534
(74) 대리인
강명구

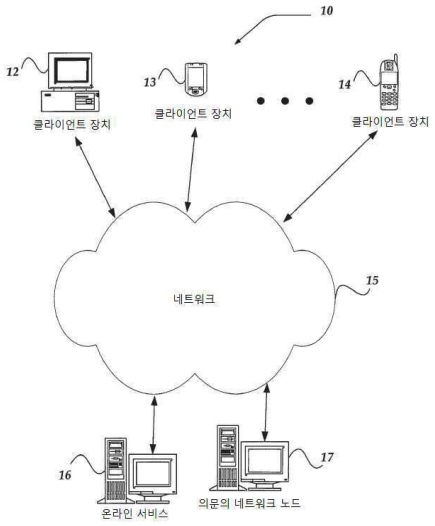
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **의문스런 네트워크 통신 평가**

(57) 요 약

네트워크 통신으로부터 의문스런 네트워크 어드레스를 식별할 수 있다. 일 실시예에서, 네트워크 장치는 들어오는 또는 나가는 연결 요청, 웹 페이지, 이메일, 또는 다른 네트워크 통신을 수신한다. 평가 모듈은 네트워크 통신의 소스 또는 목적지일 수 있는 대응하는 네트워크 어드레스를 위한 네트워크 통신을 평가한다. 네트워크 어드레스는 일반적으로 IP 어드레스를 포함한다. 평가 모듈은 하루 중의 시간, 콘텐트 유형, 방향성, 등과 같이, 네트워크 통신의 하나 이상의 특성을 결정한다. 그 후 평가 모듈은 이 특성들이 IP 어드레스와 연관된 화이트 리스트 내에 명시된 특성에 기초하여 일치하는지 또는 그렇지 않을 경우 허용되는지 여부를 결정한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 29/02 (2013.01)
H04L 63/14 (2013.01)
H04L 63/1416 (2013.01)

명 세 서

청구범위

청구항 1

컴퓨팅 시스템에서, 네트워크 통신을 평가하는 단계를 포함하는 컴퓨팅 시스템의 통신 제어 방법에 있어서,

상기 네트워크 통신 평가는,

인증되지 않은 네트워크 노드를 위한 어드레스를 포함하지 않는, 그리고, 각각의 신뢰 네트워크 어드레스에 대하여, 허용가능 통신 특성 중 하나 이상의 표시사항을 포함하는, 신뢰 네트워크 어드레스의 지정된 화이트 리스트를 수신하는 단계 - 상기 허용가능 통신 특성은, 허용가능 지리적 위치의 표시사항, 허용가능 프로그램의 표시사항, 허용가능 액세스 시간의 표시사항, 허용가능 사용자의 표시사항, 허용가능 데이터 유형의 표시사항, 및 허용가능 액세스 제어의 표시사항 중 복수 개를 포함함 - 와,

상기 네트워크 통신에 대응하는 제 1 인터넷 프로토콜(IP)어드레스를 결정하는 단계와,

상기 네트워크 통신과 연관된 제 1 통신 특성을 결정하는 단계와,

상기 제 1 IP 어드레스에 대응하는 상기 화이트 리스트 내 엔트리에 의해 명시되는 허용가능 통신 특성인 제 2 통신 특성을 결정하는 단계와,

상기 제 1 통신 특성이 상기 제 2 통신 특성에 포함되는지 여부를 결정함으로써, 상기 화이트 리스트와 관련하여 상기 네트워크 통신을 평가하는 단계와,

상기 제 1 통신 특성이 상기 제 2 통신 특성에 포함되지 않는다고 결정함에 응답하여, 상기 네트워크 통신이 불허된다는 표시사항을 설정하는 단계와,

상기 제 1 통신 특성이 상기 제 2 통신 특성에 포함됨을 결정함에 응답하여, 네트워크 통신이 허용된다는 표시사항을 설정하는 단계를 통해 이루어지는,

통신 제어 방법.

청구항 2

제 1 항에 있어서,

상기 화이트 리스트 내 허용가능 통신 특성은, 상기 화이트 리스트 내 각각의 네트워크 어드레스에 대하여, 허용가능 지리 위치의 표시사항을 포함하고,

지리-위치 정보 제공자에 질의함으로써, 상기 제 1 IP 어드레스와 연관된 지리 위치를 결정하는 단계와,

상기 제 1 IP 어드레스와 연관된 지리 위치가 상기 화이트 리스트 내 엔트리에 의해 허용가능하다고 표시되는 상기 지리 위치에 일치하거나 포함되는지 여부를 결정하는 단계를 더 포함하는

통신 제어 방법.

청구항 3

제 1 항에 있어서,

상기 화이트 리스트 내 상기 허용가능 통신 특성은, 상기 화이트 리스트 내 각각의 네트워크 어드레스에 대하여, 상기 네트워크 어드레스를 통해 통신하도록 허용되는 프로그램의 표시사항을 포함하고, 상기 프로그램의 표시사항은 프로그램명 및 프로그램 코드의 해시 중 적어도 하나를 포함하며,

상기 컴퓨팅 시스템 상에서 실행되고 있는, 그리고 상기 네트워크 통신에 참가하고 있는, 통신 프로그램을 결정하는 단계와,

상기 통신 프로그램이 상기 화이트 리스트 내 엔트리에 의해 허용가능하다고 표시되는 프로그램과 일치하는지 여부를 결정하는 단계를 더 포함하는

통신 제어 방법.

청구항 4

제 1 항에 있어서,

상기 화이트 리스트 내 상기 허용가능 통신 특성은, 상기 화이트 리스트 내 각각의 네트워크 어드레스에 대하여, 허용가능 액세스 시간의 표시사항을 포함하고,

상기 네트워크 통신이 이루어지고 있는 시간을 결정하는 단계와,

상기 결정된 시간이 상기 화이트 리스트 내 엔트리에 의해 허용가능하다고 표시되는 액세스 시간에 일치 또는 포함되는지 여부를 결정하는 단계를 더 포함하는

통신 제어 방법.

청구항 5

제 1 항에 있어서,

상기 화이트 리스트 내 상기 허용가능 통신 특성은, 상기 화이트 리스트 내 각각의 네트워크 어드레스에 대하여, 허용가능 사용자의 표시사항을 포함하고,

상기 네트워크 통신과 연관된 사용자를 결정하는 단계와,

결정된 사용자가, 상기 화이트 리스트 내 엔트리에 의해 허용가능하다고 표시되는 사용자에 일치하는지 또는 포함되는지 여부를 결정하는 단계를 더 포함하는

통신 제어 방법.

청구항 6

제 1 항에 있어서,

상기 화이트 리스트 내 상기 허용가능 통신 특성은, 상기 화이트 리스트 내 각각의 네트워크 어드레스에 대하여, 실행가능 코드, 스크립트, 매크로, 오디오, 비디오, 이미지, 및 텍스트 중 하나인 허용가능 데이터 유형의 표시사항을 포함하고,

네트워크 연결을 통해 전달되는 데이터에 대응하는 데이터 유형을 결정하는 단계와,

결정된 데이터 유형이, 상기 화이트 리스트 내 엔트리에 의해 허용가능하다고 표시되는 데이터 유형에 일치하는지 여부를 결정하는 단계를 더 포함하는

통신 제어 방법.

청구항 7

제 1 항에 있어서,

상기 화이트 리스트 내 상기 허용가능 통신 특성은, 상기 화이트 리스트 내 각각의 네트워크 어드레스에 대하여, 비-대화형 프로그램이 상기 네트워크 어드레스를 통해 통신하도록 허용되었는지 여부의 표시사항을 포함하고,

상기 컴퓨팅 시스템 상에서 실행 중인, 그리고 상기 네트워크 통신에 참가 중인, 통신 프로그램을 결정하는 단계와,

상기 통신 프로그램이 대화형 또는 비-대화형 모드로 작동하고 있는지를 결정하는 단계를 더 포함하는

통신 제어 방법.

청구항 8

제 1 항에 있어서,

발신자 시스템에서 삽입되는 소스 이메일 어드레스를 명시하는 발신자 헤더 필드 및 수신자 SMTP 서버에 의해

삽입되는 RECEIVED 헤더 필드를 가진 이메일 메시지의 진위를 평가하는 단계를 더 포함하며, 상기 진위 평가는,

상기 RECEIVED 헤더 필드에 기초하여 상기 제 1 IP 어드레스를 결정하는 단계와,

상기 소스 이메일 어드레스에 기초하여 도메인 네임 탐색을 수행함으로써 제 2 IP 어드레스를 결정하는 단계와,

상기 제 1 및 제 2 어드레스가 일치하는지 여부를 결정하고, 일치하지 않을 경우, 상기 이메일 메시지가 조작된 소스 어드레스를 가진다는 표시사항을 설정하는 단계에 의해 이루어지는

통신 제어 방법.

청구항 9

제 1 항에 있어서,

상기 네트워크 통신은 내부 네트워크 내에서 이루어지고, 상기 제 1 IP 어드레스는 상기 내부 네트워크의 IP 어드레스인

통신 제어 방법.

청구항 10

제 1 항에 있어서,

상기 네트워크 통신은 수신되는 TCP/IP 연결 요청을 통해 개시되는

통신 제어 방법.

청구항 11

제 1 항에 있어서,

상기 네트워크 통신은 발신되는 TCP/IP연결 요청을 통해 개시되는

통신 제어 방법.

청구항 12

제 1 항에 있어서,

상기 화이트 리스트 내 허용가능 통신 성질은, 상기 화이트 리스트 내 각각의 네트워크 어드레스에 대하여, 허용가능 사용자 및 액세스 제어의 표시사항을 포함하고,

상기 네트워크 통신과 연관된 사용자를 결정하는 단계와,

상기 네트워크 통신과 연관된 사용자 액세스 제어를 결정하는 단계와,

사용자 IP 어드레스 및 포트 번호 중 적어도 하나를 결정하는 단계와,

결정된 사용자, 사용자 액세스 제어 권리, 및 사용자 IP 어드레스/포트 번호가 상기 화이트 리스트 내 엔트리에 일치 또는 포함되는지 여부를 결정하는 단계를 더 포함하는

통신 제어 방법.

청구항 13

제 1 항에 있어서,

상기 제 1 IP 어드레스는 고객 컴퓨팅 장치와 연관된 IP 어드레스이고, 네트워크 통신 평가는,

상기 제 1 IP 어드레스가 상기 화이트 리스트에 의해 상기 고객에 대응하는 식별자와 연관되는지 여부를 결정하는 단계와,

상기 제 1 IP 어드레스와 연관된 지리 위치가 상기 화이트 리스트에 의해 상기 제 1 IP 어드레스와 연관된 지리 위치에 포함되는지 여부를 결정하는 단계를 포함하는

통신 제어 방법.

청구항 14

청구항 제 1 항 내지 제 13 항 중 어느 한 항에 따른 방법을 컴퓨팅 장치로 하여금 수행하게 하기 위한 실행가능 명령어를 포함하는, 비-일시적 컴퓨터 판독가능 매체.

청구항 15

네트워크 리소스와 통신하기 위해, TCP/IP 스택을 포함하는 통신 인터페이스와,

명령어를 저장하기 위한 메모리와,

상기 통신 인터페이스 및 메모리와 통신하는 프로세서를 포함하는 통신 제어 시스템에 있어서,

상기 프로세서는 청구항 제 1 항 내지 제 13 항 중 어느 한 항의 방법을 수행함으로써 네트워크 통신을 평가하도록 구성되는,

통신 제어 시스템.

발명의 설명

기 술 분 야

[0001] 여기서 개시되는 발명은 네트워크 보안에 관한 것으로서, 특히, 해커, 불법 침입자, 피싱 소스(phishing source), 바이러스, 이메일 발신자, 및/또는 기타 오류 또는 의문스런 소스로부터 수신될 수 있는, 의심스런 네트워크 통신의 식별 및 금지에 관한 것이다.

배 경 기 술

[0002] 오늘날, 인터넷과 같은 네트워크를 통해, 다른 컴퓨터, 서버, 방화벽, 라우터, PDA, 셀 폰, 게임 콘솔, 및 네트워크에 연결된 그 외 전자 장치를 뚫고 들어오려 시도하는 불법 침입자, 해커, 비인가 사용자, 및 프로그램된 장치들이 존재한다. 예를 들어, 웹사이트 서버, 다른 장치, 및 사용자들은 네트워크 상의 다른 전자 장치에 바이러스, 웜(worm), 애드웨어, 스파이웨어, 또는 그외 다른 파일을 전송할 수 있다. 이러한 파일은 다른 장치로 하여금, 웹 서버와 같은 다른 자비에 대한 네트워크 연결을 개시할 수 있는 일부 멀웨어(malware)를 작동시키거나, 바이러스를 확산시키거나, 다른 바이러스를 획득하게 하거나, 기밀 정보를 다른 곳으로 전송하게 허거나 및/또는 기타 바람직하지 못한 액션을 취하게 할 수 있다. 이러한 액션들을 검출하여 예방하는 것이 바람직하다.

[0003] 파일은 웹-기반 이메일 시스템과 같은, 이메일에 의해 종종 운반된다. 이메일 메시지가 통상적으로 "발신자" 필드 내에 발신자의 식별자를 포함하지만, 발신자 식별자가 유효한지를 보장하는 것은 어려울 수 있다. 예를 들어, 피싱 이메일의 발신자 필드는 적법한 금융 기관의 이메일 서버를 표시하도록 나타나는 발신자의 도메인 네임을 가진 이메일 어드레스를 포함할 수 있다. 사용자는 발신자 식별자가 진짜인지를 결정하기가 어려울 수 있다. 다른 경우에, 네트워크 장치는 웹 페이지, 팝업 광고, 또는 다른 데이터를 운반하기 위해 클라이언트 장치에 액세스를 요청할 수 있다. 요청하는 네트워크 장치의 도메인 네임은 적법한 금융 기관의 서버를 표시할 수 있다. 일부 보안 소프트웨어는 사용자에 대한 어드레스 정보를 가진 메시지를 제공한다. 사용자는 요청의 수락 여부를 선택할 수 있다. 그러나, 많은 사용자들은 발신자의 어드레스 정보가 진짜인지 여부를 결정하기 어려울 수 있다.

[0004] 다른 바람직하지 않은 활동이 피싱(phishing)이라 불린다. 피싱이라는 용어는 통상적으로, 불법적 또는 비인가 용도로 사적 및/또는 기밀 정보를 획득하려는 시도와 관련된다. 통상적으로, 기만자 또는 기만 조직이, 사용자로 하여금 사적 및/또는 기밀 정보를 입력할 수 있게 하는 피싱 웹사이트로의 하이퍼링크를 포함하는 하나 이상의 이메일을 전송한다. 인터넷 피싱 웹사이트는 사람들 자신이 회사 또는 다른 조직의 실제 공식 웹사이트를 입력하고 있다고 믿게 만든다. 이러한 피싱 웹사이트는 통상적으로, 그들의 웹사이트를 공식 웹사이트처럼 보이게 만듦으로써 이를 실현한다. 일반적인 사용자들은 그 후, 피싱 웹사이트에 정보를 제출하였다는 것을 깨닫지 못하면서 사적/기밀 정보를 내놓고, 그 운영자들은 이 정보를 불법 또는 비인가 용도에 사용할 수 있다. 피싱 웹사이트는 통상적으로, 실제 공식 웹사이트와 매우 유사한 도메인 네임을 가진 유니폼 리소스 로케이터(URL)를

이용한다. 도메인 네임은 종종 도메인 네임 어드레스(DNA)로도 불린다. 예를 들어, 피싱 웹사이트는 www.paypal.billing.com과 같은 DNA를 이용하여 사람들로 하여금 이 주소가 Paypal, Inc.의 공식 웹사이트인 것으로 생각하게 한다. 공식 주소인 것처럼 보이는 도메인 네임의 아래에 놓인 인터넷 프로토콜(IP) 어드레스는 일반적으로 사용자를 진짜 회사의 공식 웹사이트가 아닌 피싱 웹 사이트로 안내한다. 또는 피싱 웹사이트가 하이퍼링크용으로 공식 회사 도메인 네임을 이용할 수 있지만, 하이퍼링크에 피싱 웹사이트 IP 어드레스를 이용할 수 있다. 사용자가 이메일 내 하이퍼링크를 또는 웹 페이지를 클릭할 때, 사용자는 공식 웹사이트가 아닌 피싱 웹사이트로 이동하게 된다.

[0005] 인터넷 또는 다른 네트워크 상의 리소스들은 자체 고유 IP 어드레스를 가진다. 회사, 사적 조직, 정부 기관, 등을 포함한 조직들은 자체 고유 IP 어드레스 또는 소정 범위의 IP 어드레스를 할당받는다. 이는 피싱 웹사이트의 경우에도 똑같이 적용된다. 피싱 웹사이트, 또는 다른 네트워크 노드는 인터넷 IP 네트워크 루팅 메커니즘으로 인해 자신의 IP 어드레스를 다른 누군가의 공식 IP 어드레스인 것으로 위조할 수 없다. 사람들이 피싱 웹사이트에 도착하기 위해서는 피싱 웹사이트도 자체 IP 어드레스를 가져야만 한다.

발명의 내용

도면의 간단한 설명

[0006] 도 1은 발명의 실시를 위한 환경의 일 실시예를 나타내는 기능적 블록도를 도시하고,

도 2는 발명을 구현하는 시스템에 포함될 수 있는 클라이언트 및/또는 서버 장치의 일 실시예를 도시하며,

도 3은 본 발명의 일 실시예를 위한 구조 및 통신 시퀀스를 도시하고,

도 4는 본 발명의 일 실시예의 스크린 샷을 도시하며,

도 5는 본 발명의 추가 실시예에 대한 구조 및 통신 시퀀스를 도시하고,

도 6은 네트워크 통신 이벨류에이터 프로세스를 나타내는 흐름도다.

발명을 실시하기 위한 구체적인 내용

[0007] 본 발명은 하드웨어 실시예만의, 소프트웨어 실시예만의, 또는 소프트웨어 및 하드웨어 형태를 조합하는 실시예의 형태를 취할 수 있다. 다음의 상세한 설명은 따라서, 제한적인 면에서 취급되어서는 안된다.

[0008] "또는"이란 표현은 "및/또는"의 의미를 포함한다. "일", "하나"와 같은 단수 표현도 "복수"의 의미를 포함한다.

[0009] 본 명세서에서, "클라이언트"라는 용어는 데이터 또는 서비스의 최종 프로세서로 컴퓨팅 모듈의 일반적 역할을 의미하고, "서버"라는 용어는 하나 이상의 클라이언트에 대한 데이터 또는 서비스 제공자로 컴퓨팅 모듈의 역할을 의미한다. 일반적으로, 컴퓨팅 모듈은 일 거래에서 클라이언트로 작용하여, 데이터 또는 서비스를 요청할 수 있고, 다른 거래에서 서버로 작용하여, 데이터 또는 서비스를 제공할 수 있으며, 따라서, 그 역할을 클라이언트로부터 서버로 또는 그 역으로 변경할 수 있다.

[0010] "웹"이라는 용어는 개인용 컴퓨터, 랩탑 컴퓨터, 워크스테이션, 서버, 미니 컴퓨터, 메인프레임, 셀룰러 폰, 개인용 디지털 보조기기(PDA), 등과 같은, 컴퓨팅 장치와 함께 사용하도록 의도된 하나 이상의 프로토콜, 포맷, 신택스, 및/또는 그외 다른 규약에 따라 네트워크를 통해 액세스가능한 장치, 데이터, 및/또는 다른 리소스의 집합을 나타내는 것이 일반적이다. 웹 프로토콜은 하이퍼텍스트 트랜스퍼 르로토콜(HTTP)을 포함하지만, 이에 제한되지 않는다. 이러한 규약은 하이퍼텍스트 마크업 랭기지(HTML) 및 확장가능 마크업 랭기지(XML)을 포함하지만, 이에 제한되지 않는다. "웹 페이지" 및 "웹 데이터"라는 용어는 일반적으로, 범용 브라우저와 같이, 애플리케이션을 구동하는 컴퓨팅 장치를 이용하여 일반적으로 액세스가능한, 웹 규약을 따르는, 문서, 파일, 애플리케이션, 서비스, 및/또는 기타 데이터를 의미한다. 예시의 범용 브라우저는 Microsoft Corporation의 Internet Explorer.TM., Netscape Communications Corp.의 Netscape.TM., 및 Mozilla Foundation의 Firefox.TM.을 포함한다. 웹 페이지는 일반적으로, 웹 페이지에 액세스할 수 있는 검색 엔지에 의해 인덱싱된다. 예시 검색 엔진은 Google, Inc.의 Google.TM.이다.

[0011] "URL"이라는 용어는 일반적으로 유니폼 리소스 로케이터(uniform resource locator)를 나타내지만, 유니폼 리소스 식별자(uniform resource identifier) 및/또는 기타 다른 어드레스 정보를 또한 포함할 수 있다. URL은 일반적으로, 하이퍼텍스트 트랜스퍼 프로토콜(가령, "http://")과 같은 프로토콜, 호스트명(가령,

"news.google.com") 또는 도메인 네임(가령, "google.com"), 경로(가령, "/intl/en/options"), 및 특정 파일(가령, "pack_installer.html") 또는 질의 스트링(가령, "?hl=en")을 식별한다. 용어 "URI"는 일반적으로, 명칭 또는 웹 리소스의 식별에 사용되는 문자들의 스트링을 나타낸다. URL과 조합되어, 이는 네트워크를 통한 웹 리소스를 나타낸다.

[0012] 요컨대, 발명의 실시예는 통신 비준을 위해 알려진 신뢰 어드레스의 리스트에 대해 소정의 네트워크 어드레스를 평가한다. 복수의 보안 단계들이 제공된다. 일 실시예에서, 상부 단계는 IP 어드레스이고, 제 2 단계는 포트 번호이며, 제 3 단계는 통신 페이로드의 특성이다. 다른 단계들은 통신의 다른 형태와 연관될 수 있다. 하나 이상의 단계들이 선택적으로 구현될 수 있다. 각각의 단계는 통신 승인에 필요한 사용자 관련 레벨과 연관될 수 있다.

[0013] **예시적 작동 환경**

[0014] 도 1은 본 발명이 작동될 수 있는 환경의 일 실시예를 나타낸다. 그러나, 발명의 실시를 위해 이러한 구성요소들 모두가 요구되는 것은 아닐 수 있고, 구성요소들의 배열 및 유형에 대한 변형예가 발명의 사상 또는 범위로부터 벗어나지 않으면서 실현될 수 있다.

[0015] 도면에 도시되는 바와 같이, 시스템(10)은 클라이언트 장치(12-14), 네트워크(15), 온라인 서비스(16), 및 온라인 서비스와 직접 연관없는 의문스런 네트워크 노드(17)를 포함한다. 네트워크(15)는 각각의 클라이언트 장치(12-14), 온라인 서비스(16), 및 의문스런 네트워크 노드(17)와 통신하고 이들 간의 통신을 가능하게 한다. 온라인 서비스(16)는 적법한 웹사이트, 이메일 서비스, 파일 저장 서비스, 도메인 네임 할당 서비스, 네트워크 어드레스 식별 서비스, 등을 위해 하나 이상의 서버를 포함할 수 있다. 의문스런 네트워크 노드(17)는 정직하지 않은 사용자의 클라이언트 장치, 컴퓨터 바이러스 소스, 다른 웹사이트로 가장하는 웹사이트용의 하나 이상의 서버, 해커에 의해 위협받고 있는 유효 네트워크 노드, 또는 부당한 또는 오도하는 용도로 사용되는 다른 네트워크 노드를 포함할 수 있다. 각각의 네트워크 노드는 각각의 네트워크 노드에 고유한 IP 어드레스와 같은, 네트워크 어드레스를 가진다. 네트워크 어드레스는 일반적으로, 특정 통신 세션을 식별하기 위한 포트 번호, 네트워크 노드 내의 특정 리소스, 또는, 노드들 간에 적절한 통신을 위해 네트워크 어드레스에 대한 다른 개선책을 또한 포함한다. 네트워크 노드와의 통신을 위해 진실한 네트워크 어드레스가 필요하다. 어드레스 마스킹, 도메인 네임 변환, 및 다른 기법이 통신 경로를 따라 다양한 지점에서 네트워크 어드레스를 숨길 수 있다. 그러나, 진실한 네트워크 어드레스가 일부 지점에서 도출되거나, 또는 의도된 노드들 간에서 통신이 이루어지지 않을 것이다.

[0016] 클라이언트 장치(12-14)는 온라인 서비스(16)와 같은, 다른 컴퓨팅 장치로부터 네트워크(15)와 같은 네트워크를 통해 메시지를 서로 간에 수신 및 송신할 수 있는 사실상 임의의 컴퓨팅 장치를 포함할 수 있다. 이러한 장치들의 세트는 일반적으로 더 범용의 장치로 간주되는, 그리고, 통상적으로 개인용 컴퓨터, 멀티프로세서 시스템, 마이크로프로세서-기반 또는 프로그래머블 소비자 전자 장치, 네트워크 PC, 등과 같이 유선 통신 매체를 이용하여 연결되는, 장치를 포함할 수 있다. 이러한 장치들의 세트는 일반적으로 더 전용의 장치로 간주되는, 그리고, 통상적으로, 셀 폰, 스마트 폰, 페이저, 워키토키, 무선 주파수(RF) 장치, 적외선(IR) 장치, CB, 위 장치들 중 하나 이상의 조합한 일체형 장치, 또는 사실상 임의의 모바일 장치, 등과 같이, 무선 통신 매체를 이용하여 연결되는, 이동 단말을 또한 포함할 수 있다. 마찬가지로, 클라이언트 장치(12-14)들은 개인용 디지털 보조기기(PDA), POCKET PC, 웨어러블 컴퓨터, 및 유선 및/또는 무선 통신 매체를 통해 통신하도록 장비된 임의의 다른 장치와 같이, 유선 또는 무선 통신 매체를 이용하여 연결할 수 있는 임의의 장치일 수 있다.

[0017] 클라이언트 장치(12-14) 내의 각각의 클라이언트 장치는, 사용자로 하여금 세팅을 조작할 수 있게 하고 작동의 수행을 클라이언트 장치에 지시하는 사용자 인터페이스를 포함한다. 각각의 클라이언트 장치는 웹 페이지, 웹-기반 메시지, 등을 수신 및 송신하도록 구성되는 브라우저 애플리케이션을 또한 포함할 수 있다. 브라우저 애플리케이션은 SGML(Standard Generalized Markup Language), HTML(HyperText Markup Language), XML(Extensible Markup Language), WAP(wireless application protocol), HDML(Handheld Device Markup Language), 가령, WML(Wireless Markup Language), WMLScript, JavaScript, 등을 포함하는, 그러나 이에 제한되지 않는, 사실상 임의의 웹-기반 언어를 이용하여, 그래픽, 텍스트, 멀티미디어, 등을 수신 및 디스플레이하도록 구성될 수 있다. 클라이언트 장치(12-14)는 클라이언트 장치로 하여금 이메일, 인스턴트 메시징(IM), 단문 메시지 서비스(SMS) 메시징, 멀티미디어 메시지 서비스(MMS) 메시징, 인터넷 릴레이 챗(IRC), Mardam-Bey의 인터넷 릴레이챗(mIRC), Jabber, 등을 포함하는, 그러나 이에 제한되지 않는, 동일한 또는 서로 다른 통신 모드를 이용하는 다른 컴퓨팅 장치로부터 메시지를 송신 및 수신할 수 있게 하는 통신 인터페이스를 갖도록 또한 구성될 수 있다.

[0018] 네트워크(15)는 통신을 위해 일 컴퓨팅 장치를 다른 컴퓨팅 장치에 연결하도록 구성된다. 네트워크(15)는 일 전자 장치로부터 다른 전자 장치로 정보를 전송하기 위한 임의의 형태의 매체를 이용하도록 가동된다. 또한, 네트워크(15)는 로컬 에어리어 네트워크(LAN), 와이드 에어리어 네트워크(WAN), 가령, 범용 시리얼 버스(USB) 포트, 다른 형태의 컴퓨터-판독가능 매체를 통한 직접 연결, 또는 이들의 조합에 대한 인터페이스에 추가하여, 셀룰러 네트워크 인터페이스와 같은 무선 인터페이스, 및/또는 인터넷 인터페이스와 같은 유선 인터페이스를 포함할 수 있다. 서로 다른 구조 및 프로토콜에 기초한 것들을 포함한 상호연결된 LAN 세트 상에서, 라우터가 LAN 간에 링크로 작용하여, 메시지를 서로로부터 전송될 수 있게 한다. 또한, LAN 내의 통신 링크는 통상적으로 트위스티드 와이어 페어 또는 동축 케이블을 포함하고, 네트워크 간의 통신 링크는 에어를 통한 셀룰러 전화 신호, 아날로그 전화선, 풀(full) 또는 프랙셔널(fractional) 전용 디지털 신호 라인, 가령, T1, T2, T3, 및 T4, 디지털 신호 레벨 3 (DS3), 광학 캐리어 3 (OC3), OC12, OC48, 비동기 전송 모드 (ATM), 통합 서비스 디지털 네트워크(ISDNs), 디지털 가입자 라인(DSLs), 위성 링크, 또는 당 업자에게 알려진 및/또는 등가인 다른 통신 링크를 포함한 무선 링크를 이용할 수 있다. 더욱이, 원격 컴퓨터 및 기타 관련 전자 장치들은 모뎀 및 임시 전화 링크를 통해 LAN 또는 WAN에 원격으로 연결될 수 있다. 본질적으로, 네트워크(15)는 클라이언트 장치(12-14), 온라인 서비스(16), 및/또는 의문스런 네트워크 노드(17) 간에 정보를 이동시킬 수 있는 임의의 통신 방법을 포함한다. 네트워크(15)는 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP), 사용자 데이터그램 프로토콜(UDP), WAP, 코드 분할 다중 접촉(CDMA), 이동 통신용 전역 시스템(GSM), 등을 포함하는 다양한 통신 프로토콜과 함께 사용하도록 구성된다.

[0019] 앞서 설명된 통신 링크로 정보를 송신하는데 사용되는 매체는 일반적으로, 컴퓨팅 장치에 의해 액세스될 수 있는 임의의 매체를 포함한다. 컴퓨터 판독가능 매체는 컴퓨터 저장 매체, 유선 및 무선 통신 매체, 또는 이들의 조합을 포함할 수 있다. 추가적으로, 컴퓨터 판독가능 매체는 통상적으로, 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 프로세서에게 제공될 수 있는 기타 데이터를 저장 및/또는 운반한다. 컴퓨터 판독가능 매체는 반송파와 같은 변조 데이터 신호, 데이터 신호, 또는 다른 전송 메커니즘을 송신하기 위한 송신 매체를 포함할 수 있고, 임의의 정보 운반 매체를 포함한다. "변조 데이터 신호" 및 "반송파 신호"라는 용어는 시호에 정보, 명령어, 데이터, 등을 인코딩하도록 이러한 방식으로 설정 또는 변화된 특성들 중 하나 이상을 갖는 신호를 포함한다. 예를 들자면, 통신 매체는 무선 매체, 가령, 음향파, RF, 적외선, 및 기타 무선 매체와, 유선 매체, 가령, 트위스티드 페어, 동축 케이블, 광섬유, 도파관, 및 기타 유선 매체를 포함한다.

[0020] 전자 장치의 일 실시예가 도 2를 참조하여 아래에서 더 상세히 설명된다. 논의 용도로, 범용 클라이언트 컴퓨팅 장치가 한 예로 설명된다. 그러나, 서버 장치, 전용 장치(가령, 셀 폰), 및/또는 다른 전자 장치가 발명의 실시예에 사용될 수 있다. 본 예에서, 클라이언트 장치(20)는 사용자가 클라이언트 장치, 포털 서버(16), 및/또는 의문스런 네트워크 노드(17)와 같은, 다른 네트워크 리소스와 통신할 수 있도록 네트워크(15)에 연결할 수 있는 임의의 컴퓨팅 장치를 포함할 수 있다. 클라이언트 장치(20)는 도시되는 바보다 훨씬 더 많은 구성요소를 포함할 수 있다. 그러나, 도시되는 구성요소는 발명의 실시를 위한 예시적 실시예를 개시하기에 충분하다. 클라이언트 장치(20)의 구성요소들 중 다수가 온라인 서비스(16)의 서버, 의문스런 네트워크 노드(17)의 서버, 및/또는 다른 전자 장치에서 또한 복제될 수 있다.

[0021] 도면에 도시되는 바와 같이, 클라이언트 장치(20)는 버스(23)를 통해 대용량 메모리(24)와 통신하는 프로세싱 유닛(22)을 포함한다. 대용량 메모리(24)는 RAM(26), ROM(28), 및 기타 저장 수단을 포함하는 것이 일반적이다. 대용량 메모리(24)는 소정 유형의 컴퓨터 판독가능 매체, 즉, 컴퓨터 저장 매체를 예시한다. 컴퓨터 저장 매체("컴퓨터 판독가능 매체"라고도 함)는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 다른 데이터와 같은, 정보 저장을 위한 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성, 제거가능 및 제거불가능 매체를 포함할 수 있다. 다른 예의 컴퓨터 저장 매체는 EEPROM, 플래시 메모리, 또는 다른 반도체 메모리 기술, CD-ROM, 디지털 다용도 디스크(DVD), 또는 다른 광학적 스토리지, 자기 카세트, 자기 테이프, 자기 디스크 스토리지, 또는 다른 자기 저장 장치, 또는 요망 정보 저장에 사용될 수 있고 컴퓨팅 장치에 의해 액세스될 수 있는 그외 다른 매체를 포함한다.

[0022] 대용량 메모리(24)는 클라이언트 장치(20)의 로우-레벨 작동을 제어하기 위한 기본 입/출력 시스템("BIOS")(30)를 저장한다. 대용량 메모리는 클라이언트 장치(20)의 작동을 제어하기 위한 운영 체제(31)를 또한 저장한다. 이러한 구성요소는 소정 버전의 Windows.TM., UNIX, LINUX.TM., 등과 같은 범용 운영 체제를 포함할 수 있다. 운영 체제는 응용프로그램을 통해 하드웨어 구성요소 및/또는 운영 체제 작동을 통제할 수 있는 가상 기계 모듈을 또한 포함하거나 이와 인터페이싱될 수 있다.

[0023] 대용량 메모리(24)는 다른 것들 중에서도, 프로그램(34) 및/또는 기타 데이터를 저장하기 위해 클라이언트 장치

(20)에 의해 이용될 수 있는 하나 이상의 데이터 저장 유닛(32)을 더 포함한다. 프로그램(34)은 HTTP 통신을 송신, 수신, 및 그외 다른 처리를 위해 HTTP 핸들러 애플리케이션을 구현하도록 클라이언트 장치(20)에 의해 실행될 수 있는 컴퓨터 실행가능 명령어를 포함할 수 있다. 마찬가지로, 프로그램(34)은 안정한 방식으로 외부 애플리케이션과의 통신을 개시하는 것과 같이, 안전한 연결을 취급하기 위한 HTTPS 핸들러 애플리케이션을 포함할 수 있다. 응용프로그램의 다른 예는 스케줄러, 캘린더, 웹 서비스, 트랜스코더, 데이터베이스 프로그램, 워드프로세싱 프로그램, 스프레드시트 프로그램, 등을 포함한다. 따라서, 프로그램(34)은 웹페이지, 오디오, 비디오를 처리할 수 있고, 다른 전자 장치의 다른 사용자와 통신할 수 있다.

[0024] 추가적으로, 대용량 메모리(24)는 메시징 및/또는 기타 애플리케이션을 위한 하나 이상의 프로그램을 저장한다. 메시징 클라이언트 모듈(36)은 이메일, 인스턴트 메시징, SMS, 및/또는 기타 메시징 서비스를 가동하도록 운영체제(31)의 제어 하에 구동될 수 있는 컴퓨터 실행가능 명령어를 포함할 수 있다. 마찬가지로, 클라이언트 장치(20)와 매우 유사하게 구성되는 서버 장치는 루팅, 액세스 제어, 및/또는 기타 서버-측 메시징 서비스를 제공하는 메시징 서버 모듈(37)을 포함할 수 있다. 클라이언트 장치(20)는 일반적으로 유효 발신자, 요청, 및/또는 기타 데이터를 위한 통신을 평가하는 평가 모듈(38)을 더 포함할 수 있다. 일 실시예에서, 평가 모듈(38)은 피싱 웹사이트의 네트워크 어드레스를 클라이언트 장치(20)가 식별할 수 있도록 피싱 웹사이트와 상호작용하는 피싱-방지 모듈을 포함할 수 있고, 네트워크 어드레스가 불법 웹사이트와 연관된 지 여부를 결정할 수 있다. 다른 예의 실시예는 이메일 메시지, 파일 다운로드, 리디렉션, 및/또는 기타 통신을 점검할 수 있는 허가 모듈을 포함한다. 평가 모듈(38)은 (브라우저와 같은) 다른 애플리케이션과 분리하여 구현될 수 있고, (이메일 애플리케이션과 같은) 다른 애플리케이션에 대한 플러그-인으로 구현될 수 있으며, 서버 애플리케이션으로 및/또는 다른 형태로 구현될 수 있다.

[0025] 클라이언트 장치(20)는 키보드, 마우스, 휠, 조이 스틱, 로커 스위치(rocker switches), 키패드, 프린터, 스캐너, 및/또는 도 2에 구체적으로 도시되지 않은 다른 입력 장치와 같은, 입/출력 장치와 통신하기 위한 입/출력 인터페이스(40)를 또한 포함한다. 클라이언트 장치(20)의 사용자는 운영 체제(31) 및/또는 프로그램(34-38)와 분리되거나 통합될 수 있는 사용자 인터페이스와 상호작용하기 위해 입/출력 장치를 이용할 수 있다. 사용자 인터페이스와의 상호작용은 디스플레이, 및 비디오 디스플레이 어댑터(42)를 통한 시각적 상호작용을 포함한다.

[0026] 개인용 컴퓨터와 같은 일부 클라이언트 장치의 경우에, 클라이언트 장치(20)는 컴퓨터 판독가능 저장 매체를 위한 제거가능 매체 드라이브(44) 및/또는 영구 매체 드라이브(46)를 포함할 수 있다. 제거가능 매체 드라이브(44)는 광학 디스크 드라이브, 플로피 디스크 드라이브, 및/또는 테이프 드라이브 중 하나 이상을 포함할 수 있다. 영구 또는 제거가능 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 기타 데이터와 같은, 정보의 저장을 위한 임의의 방법 또는 기술로 구현되는 휘발성, 비휘발성, 제거가능, 및 제거불가능 매체를 포함할 수 있다. 컴퓨터 저장 매체의 예는 CD-ROM(45), 디지털 다용도 디스크(DVD) 또는 다른 광학 스토리지, 자기 카세트, 자기 테이프, 자기 디스크 스토리지 또는 다른 자기 저장 장치, RAM, ROM, EEPROM, 플래시 메모리 또는 다른 메모리 기술, 또는 요망 정보 저장에 사용될 수 있고 컴퓨팅 장치에 의해 액세스될 수 있는 그외 다른 매체를 포함한다.

[0027] 네트워크 통신 인터페이스 유닛(48)을 통해, 클라이언트 장치(20)는 인터넷과 같은 와이어 에어리어 네트워크, 로컬 에어리어 네트워크, 유선 전화망, 셀룰러 전화망, 또는 그외 다른 통신 네트워크, 가령, 도 1의 네트워크(15)와 통신할 수 있다. 네트워크 통신 인터페이스 유닛(48)은 종종 트랜시버, 트랜시빙 장치, 네트워크 인터페이스 카드(NIC), 등으로 알려져 있다.

[0028] **예시적 구현예**

[0029] 사용자가 네트워크 주소를 기억하는 것을 쉽게 하도록, www.cnn.com과 같은 도메인 네임이 수치 IP 어드레스와 연관된다. 도메인 네임은 종종 도메인 네임 어드레스(DNA)로도 불린다. 마크업 문서, 이미지, 또는 다른 데이터와 같은 리소스의 네트워크 위치를 명시하는 수치 유니폼 리소스 로케이터(URL)와 통상적으로 연관되는 유니폼 리소스 식별자(URI)를 명시하기 위해, 경로와 같이, 추가 정보가 도메인 네임에 부가될 수 있다. IP 어드레스와 대응하는 도메인 네임 간의 연관성을 유지하기 위해 중앙 데이터베이스가 통상적으로 사용된다. 일반적으로, 도메인 네임 서버(DNS), 인터넷 서비스 제공자(ISP), 또는 다른 데이터베이스가 이러한 연관성을 유지한다. 인터넷과 관련된 예시 실시예에서, ICANN(Internet Corporation for Assigned Names and Numbers, IANA(Internet Assigned Numbers Authority)과 같은 조직, 또는, 다른 할당 조직이 도메인 네임과 IP 어드레스 간의 연관성을 유지한다. 소유자명, 국가, 및/또는 다른 정보가 각각의 IP 어드레스와 또한 연관된다.

[0030] 의문스런 네트워크 노드를 식별하기 위해 많은 실시예들이 가능하다. 예를 들어, 발명의 실시예는 피싱 웹사이

트를 식별할 수 있다. 다음에 제한되지 않지만, 2개의 예가 아래에서 설명된다.

[0031] 1. 피싱 웹사이트 IP 어드레스 -- 피싱 웹사이트가 클라이언트에게 직접 IP 어드레스를 제공할 경우, IP 어드레스는 로컬 데이터베이스 또는 할당 기관을 이용하여 점검된다. 웹사이트의 IP 어드레스를 로컬 할당 데이터베이스에 또는 ICANN, IANA, 또는 기타 할당 조직에 질의함으로써, 웹사이트 소유자가 식별된다.

[0032] 2. 피싱 웹사이트 도메인 네임 -- 일반적으로, IP 어드레스는 통상적으로 직접 제공되지 않는다. 대신에, www.cnn.com과 같은 도메인 네임이 통상적으로 제공된다. 도메인 네임을 DNS에 질의함으로써, 대응하는 IP 어드레스를 발견할 수 있다. 이 IP 어드레스를 로컬 할당 데이터베이스 또는 ICANN, IANA, 또는 기타 할당 조직의 데이터베이스에 질의하면, 웹사이트 소유자가 식별된다. 당 업자는 이러한 2개의 단계가 단일 서비스에 의해 이루어질 수 있음을 이해할 것이다.

[0033] 서로 다른 애플리케이션에 대해 복수의 실시예가 또한 가능하다. 다음으로 제한되지 않지만, 3개의 예가 아래에서 설명된다.

[0034] A) 임베디드 함수 -- 응용프로그램은 문서 내의 링크를 평가하는 임베디드 함수를 포함한다. 예를 들어, 이메일 프로그램, IM 프로그램, 또는 워드 프로세싱 프로그램은 메시지 또는 문서 내 링크를 평가하기 위해 임베디드 함수를 활성화시키기 위한 메뉴 옵션 또는 버튼을 포함한다. 사용자는 함수를 활성화시킬 수 있고, 또는 함수가 문서 내 링크 검출시 자동적으로 구동될 수 있다. 함수는 IP 어드레스 및 포트 번호를 되찾기 위해 링크와 연관된 어드레스에 액세스한다. 함수는 소유자명 및 국가를 얻기 위해 로컬 또는 원격 할당 데이터베이스에 질의한다. 함수는 가령, 사용자가 링크 위에 또는 지정된 스크린 위치에 마우스 포인터를 위치시킬 때, 소유자명 및 국가를 디스플레이할 수 있다. 함수는 추가적으로, 또는 대안으로서, 도메인 네임과 연관된 알려진 소유자의 데이터베이스에 소유자명 및 어드레스를 비교한다. 지정된 스크린 위치에 또는 마우스 위에 경고가 디스플레이된다.

[0035] B) 브라우저 디스플레이 -- 마찬가지로, 브라우저가 직접 또는 플러그-인을 이용하여 수정되어 하나 이상의 새 필드를 제공할 수 있고, 브라우저에 의해 렌더링되는 웹페이지 또는 현 URL과 연관된 IP 어드레스 소유자명, 및 국가를 보여준다. 추가적으로, 현재의 도메인 네임의 소유자가 해당 도메인에 대해 알려진 소유자명 및 국가와 일치하지 않을 경우, 브라우저가 시각적, 청각적, 또는 다른 경고를 발생시킬 수 있다.

[0036] C) 온라인 서비스 -- 사용자는 온라인 질의 서비스에 웹페이지 필드를 통해 URL 또는 도메인 네임을 제출할 수 있고, 도메인 네임 소유자 실명 및 국가를 수신할 수 있다. 온라인 서비스는 IP 어드레스를 얻기 위해 URL에 액세스하는 위험을 감수한다. 온라인 서비스는 추가적 평가를 위해 제출 사용자의 클라이언트에 IP 어드레스를 리턴시킬 수 있다. 대안으로서, 온라인 서비스는 소유자명 및 국가를 결정할 수 있고, 이 정보를, 제출된 도메인 네임에 대응하는 알고 있는 소유자명 및 국가의 데이터베이스와 비교할 수 있다. 그 후 온라인 서비스는 제출 사용자의 클라이언트에 소유자명 및 국가를 전송한다. 도메인 네임이 도메인 네임 소유자 실명 및 국가와 연관 없을 경우, 온라인 서비스 또는 클라이언트 웹페이지는 사용자에게 경고를 발생시킨다.

[0037] 소유자 및 국가 결정을 위한 추가 세부사항이 이제 제공된다. (가령, IP V4 또는 V6용) IP 어드레스가 일반적으로 위임 방식으로 할당된다. 사용자는 ISP에 의해 IP 어드레스를 할당받을 수 있다. ISP는 일반적으로, 로컬 인터넷 레지스트리(LIR)로부터, 국가 인터넷 레지스트리(NIR)로부터, 또는 하나 이상의 적절한 지역 인터넷 레지스트리(RIR)로부터 IP 어드레스의 할당을 획득한다.

[0038] AfriNIC (African Network Information Centre)--아프리카 지역 (http://www.afrinic.net/)

[0039] APNIC (Asia Pacific Network Information Centre)--아시아/태평양 지역 (http://www.apnic.net/)

[0040] ARIN (American Registry for Internet Numbers)--북미 지역(http://www.arin.net/)

[0041] LACNIC (Regional Latin-American and Caribbean IP Address Registry)--라틴 아메리카 및 일부 카리브제도 (http://lacnic.net/en/index.html)

[0042] RIPE NCC (Reseaux IP Europeens)--유럽, 중동, 및 중앙 아시아 (http://www.ripe.net/)

[0043] 레지스트리 조직은 통상적으로 도메인 네임과 IP 어드레스 간의 연관성을 유지하는 서버를 작동시킨다. 이러한 서버는 종종 "whois"(후이즈) 서버로 불린다. 위 웹사이트 서버들 중 하나 이상에 질의함으로써, IP 어드레스 소유자명 및 국가를 찾을 수 있다. 질의는 적절한 서버에 브라우저가 HTTP 요청을 전송하여 응답을 얻음으로써 수행될 수 있다. 대안으로서, 클라이언트 브라우저 데이터베이스 또는 다른 로컬 또는 캐시 데이터베이스가

"whois" 서버의 하나 또는 모든 데이터베이스를 포함하여 질의를 쉽고 빠르게 만들 수 있다. 소유자 및/또는 국가가 식별되면, 사용자 또는 자동화 프로세스가 웹사이트가 진짜 또는 피싱 웹사이트인지 여부를 결정할 수 있다.

[0044] DNS 데이터베이스와 유사하게, 퍼블릭 whois 데이터베이스가 완전히 신뢰가능하지 않을 수 있다. 피싱 웹사이트 의소유자가 자신을 위한 레지스트리를 이용하기 위해 whois 레지스트에 등록할 수 있다. 이러한 문제 가능성에 대비하기 위해, 소유자명의 분별력을 향상시키기 위해 공공 "whois" 서버로부터 정보를 보완 또는 대체하는데 로컬 데이터베이스가 사용될 수 있다. 예를 들어, 적법한 회사명이 "whois" 서버로부터 명확하게 인지되지 않을 수 있다. 보완 데이터베이스는 IP 어드레스와 함께 이 회사에 관한, 고유 코드와 같은, 더 정밀한 정보를 제공할 수 있다. 다른 예에서, 적법한 금융 기관, 회사, 또는 정부 조직이, 이러한 보완 데이터베이스에 추가되기 전에 개별적으로 검증 및 인증될 수 있다.

[0045] 일부 상황에서, IP 어드레스는 프록시 서버, 네트워크 어드레스 변환(NAT) 서버, 방화벽, 및/또는 다른 네트워크 중간자들을 식별한다. 의심스런 피싱 웹사이트(또는 다른 불법 리소스)의 진실한 IP 어드레스를 찾아내기 위해, 네트워크 중간자 장치, 그 소유자, 또는 다른 인가된 실체가 하나 이상의 중간자 매핑 표, 로그 파일, 및/또는 다른 매핑 데이터를 점검한다. 이러한 중간자 매핑 데이터로부터, 인가된 실체가 시간스탬프 및/또는 TCP 포트 번호를 내부 IP 어드레스 정보에 매핑한다. 내부 IP 어드레스는 명칭, 위치, 및/또는 다른 내부 정보를 결정하기 위해 내부적으로 할당된 명칭과 점검될 수 있다. 이러한 내부 정보 획득은 일반적으로, 인터넷 서비스 제공자로부터, 네트워크 중간자 소유자로부터, 및/또는 다른 소스로부터 협동을 수반한다. 이러한 추가적인 내부 정보는 웹사이트가 유효한지 또는 피싱 웹사이트인지 여부를 결정하기 위해 클라이언트에게 또는 신뢰 평가 서비스에 제공될 수 있다.

[0046] 일 실시예에서, 로그 파일 또는 매핑 데이터는 역탐색(reverse lookup)을 위해 다음 정보를 가질 수 있다:

[0047] 1. 타임스탬프

[0048] 2. 잠재적 피싱 웹사이트, 잠재적 해커 계정, 내부 파일, 및/또는 다른 내부 리소스에 대한 내부 IP 어드레스와 같은 내부/로컬 데이터

[0049] 3. 잠재적 피싱 웹사이트, 잠재적 해커 계정, 및/또는 다른 내부 리소스에 대한 매핑 정보를 식별하는, 인터넷 소스 및/또는 목적 IP 어드레스, 소스 및/또는 TCP/UDP 포트 번호, 및/또는 다른 데이터와 같은 외부 네트워크 데이터. 예를 들어, 중간자 게이트웨이 로그 파일은 피싱 웹사이트에 대한 링크를 가진 이메일을 스패머가 전송했을 때의 소스 IP 어드레스 및 소스 TCP 포트 번호를 포함할 수 있다. 로그 파일은 이메일 메시지를 송신했을 때의 목적 IP 어드레스 및 목적 포트 번호를 또한 포함할 수 있다. 마찬가지로, 로그 파일은 해커가 목적 IP 어드레스 및 목적 포트 번호에 액세스하려 시도할 때의 소스 IP 어드레스 및 소스 TCP 포트 번호를 포함할 수 있는 중간 게이트웨이 로그 파일을 포함할 수 있다. 종종, 포트 번호 80 또는 443이 사용된다. 이러한 포트 번호가 되돌아오지 않을 경우, 링크는 피싱 웹사이트와 연관될 수 있다. 역으로, 유효 웹사이트가 80 또는 443과는 다른 포트 번호를 의도적으로 이용할 경우, 그리고 되돌아온 포트 번호가 80 또는 443일 경우, 대응 링크는 피싱 웹사이트와 연관될 수 있다.

[0050] 도 3은 본 발명의 일 실시예를 위한 구조, 통신 시퀀스, 및 방법을 예시한다. 도시되는 모듈들 전부가 발명의 실시예 요구되는 것은 아니며, 또는, 다른 실시예를 위해 추가적인 모듈이 포함될 수 있다. 다양한 실시예에서, 일부 모듈이 조합될 수 있고, 다른 모듈들이 복수개의 모듈로 나누어질 수 있다.

[0051] 본 예의 실시예에서, 이러한 구조는 피싱 웹사이트에 대응하는 IP 어드레스 웹 서버(17a)에 퍼블릭 인터넷(15a)을 통해 통신하는 클라이언트(20a)를 포함한다. 클라이언트(20a)는 인터넷(15a)과 통신하는 그리고 TCP/IP 스택(33)과 통신하는 운영 체제(31)를 포함한다. TCP/IP 스택(33)은 피상-방지 모듈(38a)과 통신하는 웹 브라우저(34a)와 통신한다. 피싱-방지 모듈은 클라이언트(20a)의 로컬 데이터베이스일 수 있는, 또는, 로컬 네트워크 또는 인터넷(15a)을 통해 가용한 네트워크 어드레스 레지스트리 데이터베이스와 같은, 원격 네트워크 데이터베이스일 수 있는, 네트워크 어드레스 데이터베이스(50)와 통신한다. 네트워크 어드레스 데이터베이스(50)는 일반적으로 IP 어드레스와 도메인 네임 및 그 소유자들 간의 상관성을 저장한다.

[0052] 클라이언트(20a)의 사용자는 링크를 포함하는 이메일을 수신할 수 있고, 브라우저(34a)에 의해 렌더링되는 웹페이지의 링크를 볼 수 있다. 링크가 유효하게 나타날 수 있으나, 사용자가 링크의 유효성을 확신하지 못할 수 있다. 사용자는 링크 위에 마우스 포인터를 위치시키거나 링크를 선택할 수 있다. 일 실시예에서, 사용자는 링크 위에 마우스 포인터를 위치시키고 마우스의 우측 버튼을 눌러 메뉴 옵션을 선택하여 링크 점검을 위한 피싱-방

지 모듈(38a)을 불러올 수 있다. 다른 실시예에서, 사용자는 단순히 링크를 선택할 수 있다. 다음의 논의는 사용자가 웹 브라우저(34a)를 통해 링크를 선택하는 실시예를 설명한다. 그러나, 당 업자는 이메일과 같은 메시징 서비스를 인지할 것이고, 및/또는 다른 애플리케이션이 사용될 수 있다. 마찬가지로, 당 업자는 마우스 우측 버튼을 누를 때 가용한 메뉴 옵션을 통해 링크의 수동적 점검이 수행될 수 있음을 인지할 것이다.

[0053] 본 예의 실시예에서, 브라우저(34a)는 링크의 사용자 선택을 검출하여 통신 단계(101)에서 대응하는 웹 페이지에 대한 요청을 전송한다. 이 요청은 먼저 TCP/IP 스택(33)에 전송되어, 링크 URL을 IP 어드레스로 분석한다. URL 분석은 네트워크 어드레스 레지스트리 데이터베이스, 인터넷 서비스 제공자(ISP), 또는 URL을 대응하는 IP 어드레스와 연관시키는 다른 소스에 대한 액세스를 필요로할 수 있다. 그러나, 이러한 소스로부터의 IP 어드레스가 가려지거나 그렇지 않을 경우 잘못 안내될 수 있다. 또한, URL을 분석함으로써 포트 번호를 꼭 얻는 것도 아니다. 진실한 IP 어드레스 및 포트 번호를 얻는 것을 보장하기 위해, TCP/IP 스택(33)은 통신 단계(102)에서 운영 체제(31a)를 통해 요청을 전송하고, 통신 단계(103)에서 운영 체제는 인터넷을 통해 의문스런 네트워크 노드(17a)에 TCP 연결을 구축한다.

[0054] 의문스런 네트워크 노드(17a)(가령, 대응 서버)는 통신 단계(104)에서 요청받은 웹 페이지를 리턴시킨다. 피싱 웹사이트의 정확한 IP 어드레스 및 포트 번호가 또한 되돌아온다. 클라이언트 운영 체제(31a)는 웹 페이지, 어드레스, 포트 번호를 수신하고, 이 정보를 통신 단계(105)에서 TCP/IP 스택(33)에 건넨다. TCP/IP 스택은 통신 단계(106)에서 웹 페이지를 브라우저(34a)에 건넨다. 통신 단계(107)에서, 브라우저는 TCP/IP 스택으로부터 IP 어드레스 및 포트 번호를 요청한다. 예를 들어, 브라우저는 GetIPAddressByName 객체 또는 GetHostByName 객체를 호출할 수 있다. TCP/IP 스택은 통신 단계(108)에서 브라우저에 IP 어드레스 및 포트 번호를 되보낸다.

[0055] 그 후 브라우저(34a)는 통신 단계(109)에서 IP 어드레스, 포트 번호, 및 URL(또는 도메인 네임 또는 호스트명)을 피싱-방지 모듈(38a)에 건넨다. 피싱-방지 모듈은 통신 단계(110)에서 이 정보를 이용하여 소유자명, 국가, 및/또는 다른 식별 데이터(가용할 경우)를 데이터베이스(50)로부터 요청한다. 데이터베이스(50)는 통신 단계(111)에서, 요청받는 정보를 피싱-방지 모듈(38a)에게로 되보낸다. 피싱-방지 모듈(38a)은 이 정보를 디스플레이를 위해 직접 브라우저(34a)에 건넬 수 있다. 그러나, 일 실시예에서, 피싱-방지 모듈(38a)은 소유자명 및 국가가 URL의 도메인 네임에 대해 알려져 있는 정보와 일치하는지 여부를 결정한다. 일치가 발견될 경우, 그 후 피싱-방지 모듈은 경고를 디스플레이하기 위해 브라우저(34a)를 위해 통신 단계(112)에서 명령어를 전송한다.

[0056] 도 4는 본 발명의 일 실시예를 위한 웹 페이지(200)의 스크린 샷을 도시한다. 본 예에서, 피싱 웹사이트는 Paypal, Inc.와 같은 회사의 공식 웹사이트인 척 한다. 유니폼 리소스 로케이터(URL)(202)가 브라우저 어드레스 필드 내에 도시된다. URL은 청하지 않은 이메일로부터 하이퍼링크를 통해 액세스되었다. URL의 도메인 네임과 연관된 IP 어드레스는 68.142.234.59 다. 연관된 IP 어드레스 소유자명(204) 및 국가(206)가 브라우저 어드레스 필드에 도시되는 도메인 네임 어드레스 근처에 디스플레이된다. 사용자, 피싱-방지 플러그-인, 및/또는 다른 결정 모듈은 소유자명 및 국가를 도메인 네임과 비교하여 진짜 여부를 결정한다. 일부 비교는 비교적 쉽다. 예를 들어, IP 소유자명이 알려지지 않은 조직 또는 개인의 이름이고 도메인 네임이 잘 알려진 회사를 표시할 경우, IP 소유자가 도메인 네임의 진짜 소유자임에 반하는 가중 결정이 존재할 수 있다. 마찬가지로, IP 소유자의 국가가 위조 활동 경력을 가진 국가이거나 알려진 회사의 모국과는 거리가 멀 경우, IP 소유자가 도메인 네임의 진짜 소유자임에 반하는 추가적인 가중화가 존재할 수 있다. IP 어드레스는 알려진 IP 어드레스 또는 알려진 회사의 어드레스 범위와 단순히 비교될 수도 있다. 가중 정보는 IP 어드레스가 진짜 웹사이트가 아닌 피싱 웹사이트라는 결정을 이끌 수 있다.

[0057] 도 4에 도시되는 바와 같이, 웹 페이지(200)는 Paypal, Inc.의 웹페이지처럼 보인다. IP 소유자(202)는 유효한 회사인 Inktomi, Inc.로 디스플레이된다. 그러나, www.paypay.com의 도메인 네임과 연관된 IP 어드레스는 216.113.188.67 이다. 큰 조직은 많은 IP 어드레스를 가질 수 있고, 따라서, IP 어드레스가 유효 조직에 의해 소유되는지 여부가 불명확할 수 있다. URL의 IP 어드레스와 연관된 국가(206)는 미국으로서, 또한 유효해보인다. 따라서, 추가 정보가 사용될 수 있다. 본 예에서, Paypal, Inc. 는 Inktomi, Inc.와 연관없는 회사 Ebay, Inc.에 의해 소유되고 있다고 알려져 있다. 따라서, 도시되는 웹사이트는 피싱 웹 사이트일 가능성이 높다. 선택적인 경고(208)가 다른 브라우저 필드에, 팝업 윈도로, 및/또는 다른 방식으로 디스플레이된다.

[0058] **추가 예시 실시예**

[0059] 인터넷과 같은 IP 네트워크에서, 두 노드 간의 연결 또는 세션은 일반적으로, IP 어드레스 및 TCP/UDP 포트 번호를 이용하여 이루어진다. 어느 노드도 자신의 그리고 다른 한 노드의 IP 어드레스 및 포트 번호를 알고 있다. 포트는 일반적으로 네트워크 노드의 종점이다. 포트 번호는 구체적 통신 세션, 구체적 기능, 구체적 리소스, 또

는 이러한 네트워크 노드 내의 다른 실체를 나타낸다. 포트 번호는 일반적으로 3개의 범위 - 잘 알려진 포트(Well Known Ports), 레지스터드 포트(Registered Ports), 및 동적 및/또는 프라이빗 포트(Dynamic and/or Private Ports) - 로 나누어진다. 잘 알려진 포트는 IANA와 같은 할당 서비스에 의해 일반적으로 할당된다. 레지스터드 포트는 요망 용도로 선택적으로 등록될 수 있다. 동적 또는 프라이빗 포트는 일반적으로, 자주 변경되는 통신을 위해 및/또는 사적 용도로, 네트워크 노드에 의해 사용될 수 있다.

[0060] 다른 노드에 대한 아웃바운드(outbound) 연결 요청을 위하여, 클라이언트는 다른 한 노드의 IP 어드레스 및 포트 번호를 이용한다. 클라이언트에게로와 같이, 아웃바운드 연결을 위해, 요청자는 그 IP 어드레스 및 포트 번호를 식별할 것이다. 인터넷 서비스 제공자 서버와 같이, 중간 노드가 사용될 경우, 중간 노드는 일반적으로, 각 노드의 IP 어드레스 및 포트 번호를 알 것이다. 예를 들어, 서버는 일반적으로 요청하는 노드 및 클라이언트 노드 모두의 IP 어드레스 및 로컬 포트 번호를 알 것이며, 따라서, 중간 서버가 요청 노드와 클라이언트 노드 간의 통신을 중계할 수 있다.

[0061] 마찬가지로, 서버 또는 클라이언트에 의해 개시되는 파일 다운로드를 위해, IP 어드레스 및 포트 번호가 알려져 있다. 예를 들어, 웹사이트 또는 다른 네트워크 서비스로부터의 다운로드일 경우, 파일을 제공하는 네트워크 노드의 IP 어드레스 및 포트 번호가, 앞서 논의한 바와 같이, 공공 또는 로컬 할당 데이터베이스로부터 결정될 수 있다. 일부 상황에서, IP 어드레스 및 포트 번호는 유효한, 신뢰할 수 있는 네트워크 노드의 것일 수 있다. 그러나, 해커가 신뢰할 수 있는 노드에 액세스할 수 있고, 바이러스 또는 다른 바람직하지 않은 파일을 분배하려 시도할 수 있다. 이러한 경우에, 발명의 실시예는 통신의 페이로드(payload)를 평가한다. 일 실시예에서, 평가 모듈은 허용가능 데이터를 표시하는 카테고리 식별자에 대해 페이로드 데이터를 결정 및 점검하기 위해 패킷의 페이로드를 평가한다. 다른 실시예에서, 평가 모듈은 전체 파일 확장자, 파일 작성자, 생성일, 및/또는 전송될 파일의 기타 성질을 평가하여, 파일이 차단되어야할지 및/또는 경고가 발생되어야할지 여부를 결정할 수 있다. 예를 들어, 신뢰 네트워크 노드로부터 새 문서를 다운로드하는 것이 수용가능할 수 있으나, 실행가능 코드를 다운로드하는 것은 아닐 수 있다. 하나 이상의 카테고리 코드가, 각각의 신뢰가능한 노드의 IP 어드레스 및 포트 번호와 연관되어, 이러한 유형의 페이로드 데이터, 다운로드 파일, 또는 허용되는 다른 데이터를 표시할 수 있다.

[0062] IP 어드레스, 포트 번호, 및 카테고리 코드가, 유효한 및/또는 그렇지 않을 경우 신뢰되는 네트워크 노드 및 파일을 식별하는 파일, 데이터베이스, 및/또는 기타 데이터 소스에 저장된다. 이러한 데이터 소스는 여기서 종종 화이트 리스트로 불린다. 화이트 리스트(white list)는 일반적으로, 차단되어야할 또는 그렇지 않을 경우 신뢰되지 않는, 어드레스, 노드, 데이터 소스 또는 기타 정보를 구체적으로 식별하는 블랙 리스트와 구분된다. 예를 들어, 발명의 소정의 실시예에 사용되는 화이트 리스트는 비인가 네트워크 노드 또는 임의의 익명 프록시 서버를 위한 IP 어드레스를 포함하지 않는다.

[0063] 화이트 리스트는 IANA WHOIS 데이터베이스의 서브세트일 수 있다. 이는 적법한 금융 기관, 평판 좋은 웹사이트, 평판 좋은 다운로드 웹사이트, 평판 좋은 안티바이러스 회사 웹사이트, 및/또는 기타 서비스 제공자만의 네트워크 노드를 식별할 수 있다. 이러한 서비스 제공자는 ISP를 포함할 수 있다. 따라서, 화이트 리스트는 하나 이상의 인터넷 서비스 제공자와 연관된 IP 어드레스 및 기타 정보를 포함하도록 설치 중 또는 그외의 경우에 변형될 수 있다. 서비스 제공자는 클라이언트 장비, 또는, 클라이언트 노드가 액세스할 필요가 있는 다른 인터넷 노드, 또는, 특정 기능을 위해 소정의 장치에 액세스하는 것을 승인하는 일부 다른 네트워크 노드에 액세스할 필요가 있다. 추가적으로, 화이트 리스트는 어드레스 소유자의 명칭, 도메인 네임, 카테고리 코드, 및 기타 정보를 포함할 수 있다. 화이트 리스트는 클라이언트에서, 또는, 파일을 제공하는 서버에서, 또는, 통신의 중간 노드에서, 또는, 2개의 단부 노드 간의 통신의 직접적 일부분이 아닌 중립 노드에서, 저장될 수 있다. 복수의 화이트 리스트가 단일 또는 복수 노드에서 사용되어, 가려진 네트워크 어드레스, 프록시 서버, 등을 수용할 수 있다. 예를 들어, 복수의 화이트 리스트가 다양한 라우터 또는 기타 노드에 분산되어, 통신 경로를 따라 메시지, 웹 페이지, 또는 기타 통신이 이동함에 따라 중간 점검을 수행할 수 있다.

[0064] 발명의 실시예는 다단계의 보안성을 제공하도록 구현될 수 있다. 첫번째 단계는 IP 어드레스다. 두번째 단계는 포트 번호다. 세번째 단계는 카테고리다. 다른 단계들은 다른 형태의 통신과 연관될 수 있다. 애플리케이션 요건에 따라, 일 실시예가 다양한 레벨의 평가를 적용할 수 있다. 일 실시예는 단지, 신뢰되는 IP 어드레스에 대한 화이트 리스트를 점검함으로써 제 1 단계 평가를 수행할 수 있다. 더 높은 보안성을 위해, 일 실시예는 평가 모듈 내 평가 레벨을 설정할 수 있다.

[0065] 화이트 리스트 내 다른 정보는 사용자 상호작용이 필요한지 여부를 표시하는데 사용되는 보안 등급(security

rating)을 포함할 수 있다. 예를 들어, 최고 보안 등급의 경우에, 평가 모듈은 자동적으로 평가를 수행하고 모든 결정을 행할 것이다. 다른 보안 등급의 경우에, 통신, 파일 다운로드, 또는 의문스런 네트워크 노드와 관련된 다른 작용을 행하기 위해 사용자 상호작용이 필요할 수 있다. 최저 보안 등급의 경우에, 평가 모듈은 통신, 파일 다운로드, 또는, 다른 액세스를 자동적으로 차단할 수 있다. 추가적으로 또는 대안으로서, 보안 등급은 통신을 점검하면서 확인되거나 개별적으로 결정될 수 있다. 예를 들어, IP 어드레스, 포트 번호, 및 카테고리 코드가 화이트 리스트 내 값과 일치할 경우, 평가 모듈은 높은 보안 등급을 표시할 수 있다. IP 어드레스 및 포트 번호가 일치하지만 카테고리 코드가 일치하지 않을 경우, 평가 모듈은 중간 보안 등급을 결정할 수 있고, 어떻게 진행할지에 대한 사용자 지시를 요청할 수 있다. IP 어드레스 및 포트 번호가 화이트 리스트 내 값과 일치하지 않을 경우, 평가 모듈은 최저 보안 등급을 결정할 수 있다. 평가 모듈 및/또는 다른 애플리케이션이, 보안 등급에 따라 다른 액션을 취할 수 있다.

[0066] 평가 모듈이 하이 리스크 네트워크 노드를 식별함에 있어서 복수의 시나리오가 존재한다. 다음으로 제한되지 않지만 일부 예는 다음을 포함한다:

[0067] 1. 웹사이트, FTP(파일 전송 프로토콜) 사이트 또는 다른 네트워크 노드의 방문과 같이, 아웃바운드 연결 요청의 경우에, 목적 노드의 IP 어드레스 및 포트 번호가 점검된다. 목적 노드의 IP 어드레스 및 포트 번호가 화이트 리스트 내에 없을 경우, 또는 그렇지 않을 경우 하이 리스트로 간주될 경우, 평가 모듈은 연결을 막고, 경고를 나타내며, 사용자 승인을 요구하고, 목적 노드의 추가 인증을 요구하며, 또는 다른 지정된 액션을 수행할 수 있다. 사용자가 연결을 승인해야할 경우, 목적 노드의 IP 어드레스, 포트 번호, 및/또는 기타 정보가 화이트 리스트에 추가될 것이다.

[0068] 2. 아웃바운드 연결 요청의 경우에, 요청 노드의 IP 어드레스 및 로컬 장치 포트 번호가 화이트 리스트에 대해 점검된다. 이는 침입자, 해커, 또는 다른 비인가 사용자가 수신 장치에 대한 액세스를 얻는 것을 중단시킬 수 있다. 수신 장치(또는 중간 노드)는 연결을 거부하거나, 경고를 발생시키거나, 사용자 승인을 요구하거나, 요청 노드의 추가적 인증을 요구하거나, 또는 다른 지정된 액션을 수행할 수 있다. 사용자가 연결을 승인해야할 경우, 요청자 노드의 IP 어드레스, 포트 번호, 및/또는 다른 정보가 화이트 리스트에 추가될 것이다.

[0069] 3. 파일 전송의 경우, 파일 다운로드 이전에 소스 노드가 점검될 수 있다. 역으로, 파일이 의문스런 노드로 전송되기 전에, 목적 노드가 점검될 수 있다. 앞서 논의한 바와 같이, IP 어드레스, 포트 번호, 및 파일 유형이 화이트 리스트에 대해 점검된다. 연결 시나리오와 유사하게, 평가 모듈은 파일 전송을 막고, 사용자 승인을 요구하며, 요청 노드의 추가 인증을 요구하고, 또는, 다른 지정된 액션을 수행할 수 있다. 사용자가 파일 전송을 승인해야할 경우, 의문스런 노드의 IP 어드레스, 포트 번호, 및/또는 다른 정보가 화이트 리스트에 추가될 것이다. 파일 확장자가 대응하는 IP 어드레스, 포트 번호, 및/또는 기타 정보와 함께 카테고리로 또한 저장될 것이다.

[0070] 도 5는 본 발명의 추가 실시예를 위한 구조, 통신 시퀀스, 및 방법을 도시한다. 발명의 실시를 위해 도시되는 모듈 전부가 반드시 요구되는 것은 아닐 수 있고, 또는 다른 실시예를 위해 추가적인 모듈이 포함될 수 있다. 다양한 실시예에서, 일부 모듈은 조합될 수 있고, 다른 모듈은 여러 개의 모듈로 나누어질 수 있다. 예시 실시예들이 다음의 구조와 관련하여 논의된다.

[0071] 본 예의 실시예에서, 구조는 웹사이트, FTP 사이트, 또는 다른 인터넷 서비스에 대응하는 네트워크 노드(317)의 IP 어드레스에 퍼블릭 인터넷(15b)을 통해 통신하는 클라이언트(20b)를 포함한다. 클라이언트(20b)는 인터넷(15b)과 통신하는 그리고 TCP/IP 스택(333)과 통신하는, 운영 체제(31b)를 포함한다. TCP/IP 스택(333)은 인가 모듈(38b)과 통신하는 인터넷 네트워크 애플리케이션(34b)과 통신한다. 인터넷 네트워크 애플리케이션(34b)은 해커, 바이러스, 또는 다른 바람직하지 않은 실체를 수반하는 통신을 막는데 사용될 수 있는 이메일 애플리케이션 또는 기타 애플리케이션일 수 있다. 인가 모듈은 클라이언트(20b)와 통신하는 또는 클라이언트(20b)에 포함될 수 있는 로컬 데이터베이스(350)와 통신한다. 로컬 데이터베이스(350)는 일반적으로, IP 어드레스, TCP/IP 번호, 카테고리, 보안 등급, 도메인 네임, 그 소유자 및/또는 기타 데이터 간의 연관성을 저장하는 화이트 리스트를 포함한다.

[0072] **예시 시나리오 1: 아웃바운드 연결**

[0073] 본 예시 실시예에서, 클라이언트(20b)의 사용자는, 가령, 웹사이트에 대한, 인터넷 연결을 개시할 수 있다. 인터넷 네트워크 애플리케이션(34b)은 통신 단계(301)에서, 연결을 위한 사용자 요청을 검출한다. 이 요청은 먼저 TCP/IP 스택(333)에 전달되어 도메인 네임 또는 URL을 IP 어드레스로 분별한다. 도메인 네임 분별은 DNS 액세스

를 필요로할 수 있다. 그러나, DNS로부터의 IP 어드레스가 가려질 수 있고 또는 그렇지 않을 경우 잘못 안내될 수 있다. TCP/IP 스택(333)은 통신 단계(302)에서 운영 체제(31b)에 요청을 전송하며, 운영 체제는 통신 단계(303)에서 인터넷을 통해 네트워크 노드(317)에 TCP 연결을 행한다.

[0074] 네트워크 노드(317)(가령, 웹사이트의 대응 서버)는 통신 단계(304)에서 요청을 되보낸다. 네트워크 실체의 정확한 IP 어드레스 및 포트 번호가 함께 되돌아온다. 클라이언트 운영 체제(31b)는 IP 어드레스 및 포트 번호를 수신하고, 통신 단계(305)에서 이 정보를 TCP/IP 스택(333)에 건넨다. TCP/IP 스택은 통신 단계(306)에서 제어를 애플리케이션(34a)에 넘긴다. 응용프로그램은 네트워크 노드(317)로부터 수신되는 임의의 파일 또는 다른 데이터의 카테고리 코드를 결정할 수 있다. 통신 단계(307)에서, 애플리케이션은 TCP/IP 스택으로부터 IP 어드레스 및 포트 번호를 요청한다. 예를 들어, 네트워크 애플리케이션은 GetIPAddressByName object 객체 또는 GetHostByName 객체를 호출할 수 있다. TCP/IP 스택은 통신 단계(308)에서 TCP/IP 어드레스 및 포트 번호를 애플리케이션에 되보낸다.

[0075] 그 후 네트워크 애플리케이션(34b)은 통신 단계(309)에서 IP 어드레스, 포트 번호, 카테고리 코드, 및 기타 정보를 인가 모듈(38b)에 건넨다. 인가 모듈은 이 정보를 이용하여 데이터베이스(350)를 점검한다. 인가 모듈은 통신 단계(310)에서 IP 어드레스, 포트 번호, 카테고리 코드, 및 기타 정보를 가진 데이터베이스(350)에 검색 요청을 전송할 수 있다. 데이터베이스(350)는 검색을 수행하여 IP 어드레스 및 기타 정보가 신뢰 정보의 화이트 리스트 내에 포함되어 있는지 여부를 결정할 수 있다. 데이터베이스(350)는 IP 어드레스와 연관된 소유자, 국가, 보안 코드, 및/또는 기타 정보를 또한 결정할 수 있다. 데이터베이스(350)는 통신 단계(311)에서, 요청받은 정보를 인가 모듈(38b)에 되보낸다. IP 어드레스 및 포트 번호가 화이트 리스트 내에 있는지 여부에 기초하여, 인가 모듈은 연결을 닫도록, 수신한 정보를 거부하도록, 경고 메시지를 전송하도록, 사용자 결정을 기다리도록, 및/또는 다른 지정된 액션을 행하도록, 명령어를 전송할 수 있다.

[0076] **예시 시나리오 2: 인바운드 연결(Inbound Connection)**

[0077] 네트워크 노드(317)는 통신 단계(304)에서 클라이언트(20b)에 대한 연결을 요청할 수 있다. 클라이언트 운영 체제(31b)는 네트워크 노드(317)의 IP 어드레스 및 포트 번호를 포함하는 이 요청을 수신한다. 이 요청은 일반적으로, 네트워크 노드가 접촉하고자 하는 리소스로 네트워크 애플리케이션(34b)을 식별하기 위해 네트워크 애플리케이션(34b)의 포트 번호를 또한 포함한다. 이 요청은 네트워크 노드가 요망하는 데이터에 대한 파일명 또는 기타 정보를 더 포함할 수 있다. 운영 체제는 통신 단계(305)에서 이 정보를 TCP/IP 스택(333)에 건넨다. TCP/IP 스택은 통신 단계(306)에서 이 정보를 인터넷 네트워크 애플리케이션(34b)에 넘긴다.

[0078] 그 후 네트워크 애플리케이션(34b)은 통신 단계(309)에서, IP 어드레스, 포트 번호, 및 기타 정보를 인가 모듈(38b)에 건넨다. 인가 모듈은 네트워크 노드(317)에 의해 요청된 정보에 대한 카테고리 코드를 결정할 수 있다. 인가 모듈은 이 정보를 이용하여 데이터베이스(350)를 점검할 수 있다. 인가 모듈은 통신 단계(310)에서, IP 어드레스, 포트 번호, 카테고리 코드, 및 기타 정보를 가진 데이터베이스(350)에 검색 요청을 전송할 수 있다. 데이터베이스(350)는 검색을 수행하여, IP 어드레스 및 기타 정보가 신뢰 정보의 화이트 리스트 내에 포함되는지 여부를 결정할 수 있다. 데이터베이스(350)는 IP 어드레스와 연관된 소유자, 국가, 보안 코드, 및/또는 기타 정보를 또한 결정할 수 있다. 데이터베이스(350)는 통신 단계(311)에서, 요청받은 정보를 인가 모듈(38b)에 되보낸다. 인가 모듈(38b)은 네트워크 애플리케이션(34b)에 직접 이 정보를 건넬 수 있다. IP 어드레스 및 포트 번호가 화이트 리스트 내에 있는지 여부에 기초하여, 인가 모듈은 단계(312)에서, 연결을 닫도록, 수신한 정보를 거절하도록, 경고 메시지를 내보내도록, 사용자 결정을 기다리도록, 및/또는 다른 지정된 액션을 취하도록 명령어를 전송할 수 있다.

[0079] **예시 시나리오 3: 메시징**

[0080] 네트워크 애플리케이션(34b)이 가령, Microsoft Outlook.TM.과 같은 이메일 클라이언트와 같은 메시징 서비스인 경우, 수신되는 이메일 헤더를 점검할 수 있다. 헤더에서, 발신 이메일 장치의 IP 어드레스 및 포트 번호를 가진 "발신" 필드가 존재한다. 헤더는 증정 사본(CC) 수신자와 연관된 장치의 IP 어드레스, 수신 이메일의 임의의 첨부물 표시, 및/또는 기타 데이터와 같은 기타 정보를 포함할 수 있다. 네트워크 애플리케이션(34b)은 임의의 첨부 파일의 카테고리 코드를 결정할 수 있다. 그 후 네트워크 애플리케이션은 IP 어드레스, 포트 번호, 및 기타 정보를 통신 단계(309)에서 인가 모듈(38b)에 건넨다. 인가 모듈은 이 정보를 이용하여 이메일 발신자가 신뢰되는지 여부를 결정할 수 있다. 구체적으로, 인가 모듈은 통신 단계(310)에서 검색 요청 내 IP 어드레스 및 포트 번호(및 가용할 경우 카테고리 코드)를 데이터베이스(350)에 전송한다. 데이터베이스는 화이트 리스트 내 IP 어드레스 및 포트 번호를 점검한다. 데이터베이스는 도메인 네임, 이메일 함수 코드, 보안 등급, 및/또는 기

타 데이터(가용할 경우)를 또한 불러올 수 있다. 데이터베이스(350)는 통신 단계(311)에서 검색 결과를 인가 모듈(38b)에 되보낸다. 인가 모듈(38b)은 이 정보를 이메일 네트워크 애플리케이션(34b)에 직접 건넬 수 있다. IP 어드레스 및 포트 번호가 화이트 리스트 내에 있는지 여부에 기초하여, 인가 모듈은 단계(312)에서, 이메일 삭제, (가령, 휴지통으로) 이메일 리디렉션, 경고 전송, 사용자 지시 대기, 및/또는 기타 액션의 명령어를 전송할 수 있다.

[0081] 세부적으로, 본 발명의 예시 실시예는 간단한 메일 전송 프로토콜(SMTP)을 이용하여 인터넷 이메일 시스템을 포함할 수 있다. 인터넷 이메일의 경우에, SMTP가 메일 전달 또는 불러오기에 사용된다. 이는 중간 메일 서버를 통해 이루어지는 것이 일반적이다. 이메일 수신시, 메일 서버는 발신 메일 클라이언트의 IP 어드레스 및 TCP/UDP 포트 번호를 수신할 것이다. 메일 서버는 이메일 헤더의 "발신" 필드에 발신자의 IP 어드레스를 추가할 것이다. 앞서 설명한 바와 같이, IP 어드레스가 검증될 수 있다.

[0082] 이러한 검증의 다른 실시예는 이메일 발신자의 도메인 네임을 인증하기 위해 메일 서버에 의한 역 DNS 탐색을 또한 포함할 수 있다. 일부 메일 서버는 스팸 이메일 차단을 위해 도메인 정보를 이용한다. 스팸 차단은 메일 서버 도메인 및/또는 클라이언트 발신자 도메인을 점검하기 위해 도메인 정보를 이용할 수 있다. 그러나, 앞서 논의한 바와 같이, 도메인 정보가 가려질 수 있다. DNS 탐색을 이용하여, 또는 DNS 탐색없이, 본 발명의 실시예는 화이트 리스트 데이터베이스에 대해 이메일의 실제 IP 어드레스를 점검함으로써 이메일 발신자를 검증할 수 있다. 그럼에도 불구하고, 소유자 및 국가와 같은 추가적인 정보가 이메일 헤더의 IP 어드레스 정보로부터 얻은 도메인 정보로부터 점검될 수 있다. 수신 IP 어드레스가 수신 이메일 어드레스에 표시된 도메인과 연관됨을 보장하기 위해 도메인 탐색을 이용함으로써 추가적인 신뢰도를 얻을 수 있다. 예를 들어, 인가 모듈은 이메일 헤더로부터의 IP 어드레스를 이용하여, 화이트 리스트를 검색할 수 있고, 도메인 할당 서비스를 이용하여, IP 어드레스와 연관된 도메인 명칭을 결정할 수 있다. 인가 모듈은 그 후, 이메일 메시지의 "발신" 필드에 명시된 도메인 네임에 대하여, 결정된 도메인 네임을 비교할 수 있다. 도메인 네임이 일치하지 않을 경우, 메시지가 불법적일 수 있다. 메시지로부터의 IP 어드레스 및 포트 번호가 화이트 리스트 내 값과 일치함에도 불구하고, 도메인 명칭이 다른 것은 해커가 신뢰 네트워크 노드에 액세스하였음을 표시할 수 있고, 스팸 메시지 또는 다른 바람직하지 않은 활동을 위해 상기 신뢰 네트워크 노드를 이용하고 있음을 표시할 수 있다.

[0083] 이메일이 다른 SMTP 서버에 의해 전달/중계된 경우, 그 수신자 이메일 클라이언트는 전달/중계 메일 서버가 신뢰할만한지를 또한 점검할 것이다. 이메일 헤더가 불완전하거나 전달/중계 메일 서버가 발신자 식별에 사용될 수 없는 경우, 인가 모듈은 이메일을 삭제하거나 앞서 논의된 다른 액션을 취할 수 있다.

[0084] 또한, SMTP 이메일의 경우에, 발신자는 xxxx@msn.com과 같은 이메일 도메인을 이용한다. 이러한 도메인 네임만으로, 이 이메일이 회계 또는 관리부서와 같이, MSN 내 중요 조직의 일원으로부터 온 것인지 또는 일반 MSN 사용자로부터 온 것인지를 식별하는 쉬운 방법은 전혀 없다. 이러한 레벨의 세부사항을 결정할 수 있는 것이, 금융 기관 또는 다른 조직이 갖고자하는 기능이다.

[0085] 이 문제를 해결하기 위해, 발신 이메일 서비스는 소정의 부서에 대해 복수의 IP 어드레스를 구축할 수 있다. 일부 IP 어드레스는 일반 사용자용일 수 있다. 나머지 IP 어드레스는 전용 사용자 및/또는 그외 다른 전용 용도로 사용될 수 있다. 이러한 방식으로, 금융 기관 또는 다른 조직이 금융 정보 이메일을 고객에게 전송할 수 있다. 추가적으로 또는 대안으로서, TCP/IP 포트를 이용하여 이 기능을 지원할 수 있다. 이는 제한된 IP 어드레스가 인터넷 메일 서비스용으로 가용할 때 유용하다. 또 다른 실시예에서, 통신에 서브 조직 코드가 포함될 수 있고, 및/또는 화이트 리스트 데이터베이스에 추가될 수 있어서, 서브 조직 또는 다른 이메일 분류를 식별할 수 있다. 마찬가지로, 통신 용도를 표시하기 위해 통신에 기능 코드가 포함될 수 있고, 및/또는 화이트 리스트 데이터베이스에 기능 코드가 추가될 수 있다. 고객의 클라이언트 장치는 본 발명의 일 실시예를 이용하여 발신자를 인증할 수 있고, 수용가능한 조직용 코드 및/또는 기능 코드를 점검하여, 피싱 이메일로부터 유효 이메일을 구분할 수 있다.

[0086] 피싱 웹사이트용 경고 디스플레이에서처럼, 이메일 클라이언트는 디스플레이 필드를 제공할 수 있다. 이메일 클라이언트는 비준 제어를 위해 메뉴 옵션을 또한 제공할 수 있다. 사용자가 이메일을 수신할 때, 메뉴 옵션 및/또는 디스플레이 필드가 사용자로 하여금 이메일 발신자, 서브조직, 및/또는 다른 기능/데이터를 식별할 수 있게 한다. 일 실시예에서, 수신자 이메일 클라이언트는 발신자의 IP 어드레스, 포트 번호, 및 도메인 네임을 로컬 화이트 리스트 데이터베이스에 자동적으로 비교할 것이다. 발신자의 IP 어드레스(가령, 이메일의 발신자 또는 RECEIVED 필드에 기초하여 결정됨), 포트 번호, 및/또는 도메인 네임이 데이터베이스에 없을 경우, 또는 데이터베이스의 입력사항과 다를 경우, 디스플레이 필드를 이용하여 이메일이 이메일 어드레스에 나타나는 발신자

로부터 온 것인 아닐 수 있음을 표시할 수 있다. 대안으로서, 사용자는 메뉴 옵션을 활성화시켜서 이러한 점검을 수행할 수 있고, 이메일 또는 발신자에 관한 정보를 디스플레이할 수 있으며, 및/또는 다른 작동을 수행할 수 있다.

[0087] 일부 실시예에서, 화이트 리스트는 잘 알려진 조직 IP 어드레스에 추가하여 다음의 특징들 중 하나 이상을 가진다. 설명된 화이트 리스트의 핵심 장점은 (가령, TCP/IP 세션의 일부분으로) 양방향 통신에 사용되는 IP 어드레스가 위조하기 어렵거나 불가능하다는 점이다. 침입자 또는 다른 자가 패킷 내 소스 IP 어드레스를 스푸핑(spoofing)하는 것이 가능하지만, 이러한 스푸핑은 일반적으로, 세션 구축을 위해 양방향 통신이 필요한 TCP/IP 범주에서 사용될 수 없다. 따라서, 네트워크 스택으로부터 획득되는 IP 어드레스를 이용함으로써, 설명되는 기술은 고도의 신뢰도로 의문스런 네트워크 통신을 식별할 수 있다.

[0088] 추가적으로, 의문스런 IP 어드레스가 블랙 리스트에 추가되면, 위 IP 어드레스의 비인가 사용자가 다른 IP 어드레스로 작동하는 다른 컴퓨팅 시스템으로 침입을 옮겨갈 뿐이라는 점에서, 화이트 리스트가 블랙 리스트에 비해 장점을 제공한다. 범죄 조직이 타협 기계들의 전체 네트워크를 작동시키는 세계에서, 이러한 조직들이 그들의 비인가된 활동(가령, 스팸 발송)을 일 기계로부터 다른 기계로 전달하는 것은 사소한 사항이다.

[0089] 설명되는 기술은 주어진 컴퓨팅 시스템 내에 복수의 개별 레벨들로 또한 기능할 수 있다. 예를 들어, 설명되는 기술은 운영 체제 커널, 네트워크 스택, 및 애플리케이션으로부터 수신 또는 획득되는 정보를 이용할 수 있다. 예를 들어, 인가 모듈(38b)(도 5)은 애플리케이션 레벨(가령, 이메일 클라이언트로부터 수신되는 이메일 헤더 필드), 네트워크 레벨(가령, TCP/IP 스택으로부터 수신되는 IP 어드레스), 및 운영 체제(가령, 운영 체제 커널로부터 수신되는 허가 세팅)로부터 수신되는 정보를 이용할 수 있다.

[0090] 또한, 설명되는 기술은 컴퓨팅 시스템의 서로 다른 레벨에서 보안성을 구현하기 위한 인프러스트럭처 또는 프레임웍을 제공한다. 예를 들어, 화이트 리스트 또는 유사 구조는 운영 체제 커널, 네트워크 스택, 및 하나 이상의 애플리케이션 내에서 보안 또는 인가 시설의 구현에 사용되는 정보 또는 성질을 지닐 수 있다.

[0091] 화이트 리스트는 지리 정보와 연관된 IP 어드레스를 지닐 수 있다. 일 유형의 지리 정보는 특정 IP 어드레스를 할당한 지역 인터넷 레지스트리에 기초한다. 앞서 논의한 바와 같이, IP 어드레스는 ARIN, APNIC, LACNIC, AfriNiC, RIPE NCC, 등과 같은, 지역 인터넷 레지스트리에 의해 할당된다. IP 어드레스가 주어졌을 때, 어느 지역 인터넷 레지스트리가 IP 어드레스를 할당하였는지를 결정할 수 있고, 따라서, IP 어드레스와 연관된 영역(가령, 대륙 또는 국가)을 결정할 수 있다. 지역 레지스트리는 해당 국가, 또는, IP 어드레스와 연관된 국가, 주, 또는 도시와 같은, 더 상세한 지리 정보를 제공할 질의를 더 지원할 수 있다. 다른 지리 정보 소스는 국가, 주, 도시, 위도/경도, 우편번호, 지역 코드, 등을 포함한, 미세-단위 지리 정보를 제공하도록 구성된 상용 또는 공공 지리 서비스 및 whois 데이터베이스를 포함한다.

[0092] 지리 정보를 이용하여, 명시된 영역의 사용자에 대한 액세스를 제한할 수 있다. 예를 들어, 정부는 해당 정부의 국가 또는 관할권 내에 위치한 IP 어드레스에 대한 액세스를 제한할 수 있다. 다른 예로서, 특정 영역들에 대한 IP 어드레스가, 이 영역들로부터 작동하는 높은 수준의 컴퓨터 범죄에 기초하여, 위험하다고 플래깅(flag)할 수 있다. 다른 예로서, 전자 상거래 컴퓨팅 시스템(가령, 뱅킹 시스템, 온라인 쇼핑 시스템)은 고객이 거주하는 동일 지리 영역(가령, 도시, 주, 국가)과 연관된 IP 어드레스로부터의 고객 액세스만을 허용할 수 있다. 예를 들어, 특정 고객이 시애틀(Seattle)에 거주할 경우, 특정 전자상거래 시스템은 워싱턴주 또는 미국에 할당된 IP 어드레스로부터의 고객 계정에게만 액세스만을 허용할 수 있다. 또한, 정부 또는 군과 같이 고도 보안 조직의 경우에, 조직은 소정의 지리적 위치만을 액세스시키고 다른 위치(가령, 중국)는 차단할 수 있다.

[0093] 화이트 리스트는 서로 다른 실시예에서 서로 다른 형태를 취한다. 화이트 리스트가 공공 인터넷 및/또는 프라이빗 내부망 상에서 존재할 수 있다. 화이트 리스트는 공공 인터넷을 통해 이용되는 것과 유사한 방식으로 프라이빗 내부망을 위해 생성될 수 있다. 예를 들어, 은행은 고객 인터넷 IP 어드레스를 특정 은행 계좌와 연계시키는 화이트 리스트를 가질 수 있다. 고객측에서, 은행 계좌 소유자는 은행의 컴퓨팅 시스템의 내부 IP 어드레스를 포함하는 화이트 리스트를 가질 수 있다. 또한, 복수의 리스트들이 단일 장치 상에 존재할 수 있다. 예를 들어, 인바운드 트래픽에 대해 하나의 화이트 리스트, 아웃바운드 데이터에 대해 하나다. 추가적으로, 각각의 네트워크 인터페이스 카드(NIC)가 자체 화이트 리스트를 가질 수 있다. 추가적으로, 화이트 리스트는 정적으로(가령, 지정된) 또는 동적으로 발생될 수 있다. 예를 들어, 웹사이트의 경우에, 동적 리스트가, 수신되는 IP 어드레스 정보에 기초하여 발생될 수 있다. 그 후 나중의 액세스들이 리스트에 기초하여 비교될 수 있고, 따라서, 가령, 웹사이트 URL이 리스트에 저장된 것과 다른 IP 어드레스로 분별될 때와 같이, 의문스런 통신이 식별될 수 있다.

[0094] 화이트 리스트가 아래 표 1에 제시되는 다음의 필드 또는 성질 중 하나 이상을 지닐 수 있다. 각각의 필드는 허용된 통신 방향(가령, 업로드, 다운로드, 송신 또는 수신), 허용된 통신 시간 주기(가령, 8AM 내지 11PM 사이), 허용된 프로그램/프로세스(가령, 인터넷 익스플로러), 등과 같이, 하나 이상의 허용가능한 통신 특성을 표시한다. 다른 실시예에서, 표는 통신 불허 시간 주기(가령, 정오에서 오전 4시 사이), 불허 통신 포트(가령, HTTP용으로 흔히 사용되는 포트 80), 등과 같이, 불허 통신 특성의 표시를 또한, 또는 대신에, 포함한다.

표 1

[0095]

필드/성질	설명/기능
IP 어드레스 및 마스크	허용 IP 어드레스 또는 IP 어드레스 범위를 식별. 내부망의 경우, IP 어드레스는 내부(사적) IP 어드레스일 수 있음.
포트 번호	허용 포트 번호 또는 범위를 식별하여, FTP, 텔넷, HTTP, 등과 같은 허용 기능들을 제시
차단 상태	대응 어드레스로부터의 액세스를 허용 또는 불허
카테고리 코드/데이터 유형	실행 코드, 스크립트, 매크로, 오디오, 비디오, 이미지, 텍스트 파일, 등과 같은, 통신으로부터 허용 유형의 데이터 표시
방향	업로드, 다운로드, 수신, 송신과 같은 허용 통신 방향을 규정. 고도 보안 장치는 예를 들어, 인바운드 연결을 불허할 수 있음.
보안 등급	고도-보안, 보안, 일반, 비-보안, 고-위험, 등과 같이, IP 어드레스와 연관된 보안 레벨 명시
서브조직 코드	조직 내 IP 어드레스의 서브세트를 명시. 예를 들어, 조직의 경우, 웹용으로 일 그룹, 텔넷용으로 다른 일 그룹과 같이, IP 어드레스를 서브그룹으로 나눌 수 있음.
URL/URI	IP 어드레스와 연관된 조직 공식 URL. 종종, HTTP 리디렉션은 예를 들어, 바보들에 대한 피싱 웹 사이트를 호스팅하는 매우 유사한 URL로 리디렉션할 수 있다. 다른 예로서, 이메일 내 HTTP 링크가 적법한 URL과 비슷해 보일 수 있다. 통신에 나타나는 URL은 조직 URL과 비교되어, 통신이 의문스런지 여부를 결정할 수 있다. 더욱이, URI 점검이 추가 보호를 제공할 수 있다.
도메인 네임	도메인 네임 일치에 사용가능. 이메일 어드레스는 확인될 수 있는 도메인 네임을 가짐.
지리 위치	국가 코드, 도시, 세부 주소, 우편번호, 등. 이는 소정의 지리 위치에 대한 액세스를 제한하는데 사용될 수 있음.
네트워크 인터페이스 번호	이는 멀티 네트워크 인터페이스(NIC) 장치용임.
프로세스명 또는 시그너처	어느 프로그램이 네트워크에 액세스하거나 주어진 IP 어드레스와 통신하는지를 명시. 이는 바이러스 프로그램이 네트워크 액세스하여 발신, 데이터 수신, 또는 타에게로 확산하는 것을 막음.프로그램은 명칭, 위치, 또는 시그너처/해시에 의해 식별될 수 있음(가령, MD5, SHA1, 등).
대화형/배치 모드	많은 악성 프로그램들이 배치(batch) 또는 비-대화형 모드로 구동될 것이다. 이는 이메일 계정에 액세스하는 바이러스 프로그램이 데이터를 송신 또는 수신하는 것을 방지할 수 있다. 이 모드는 능동 콘솔, UI 윈도, 대화형 입력 장치(가령, 마우스), 등이 있는지 여부를 점검하는 것과 같이, 다양한 방식으로 결정될 수 있다.
액세스 시간	네트워크 액세스가 허용되는 동안의 시간 또는 주기를 명시. 이는 예기치않은 시간(가령, 지난 밤) 동안 구동되는 악성 코드를 방지할 것이다.
연결 수	네트워크에 이루어질 수 있는 연결의 수를 제한. 이는 서비스 거부 공격을 방지하는데 사용가능.
액세스 제어	판독, 기록, 실행, 등을 포함한, 대응하는 IP 어드레스와 관련하여 수행될 수 있는 작동들의 종류를 명시. 이러한 액세스 권리는 운영 체제 특이적이거나 애플리케이션 특이적임. 소정의 애플리케이션이 하위 시스템의 것과는 구분되는 액세스 권리를 제공할 수 있음. 예를 들어, 메시징 애플리케이션에서, 송신 메시지 전송은 수신 메시지 판독과는 구분되는 액세스 권리를 요구할 수 있음.
사용자/그룹 식별자	대응 IP 어드레스를 이용할 허락받은 사용자 또는 사용자 그룹의 식별자(가령, 사용자 명칭, 계좌 번호, 사용자 번호). 인증 용도로, 사용자 식별, 패스워드, 및 IP 어드레스 및/또는 포트 번호를 검증할 수 있다.
인바운드/아웃바운드	인바운드 트래픽은 아웃바운드 트래픽과는 다른 보안 요건을 가질 수 있음. 각각은 화이트 리스트를 분리시켰을 수 있음.

[0096] 위 필드는 다양한 방식으로 조합될 수 있다. 예를 들어, 도 1을 참조하면, 클라이언트(12, 13, 14)가 아웃바운드 연결을 개시할 때, 프로세스명, 액세스 시간 윈도, 배치/대화형 프로세싱, 목적 IP 어드레스, URL/URI 또는 도메인 네임(적절한 경우), 보안 등급, 업로드/다운로드, 카테고리 코드, 또는 페이로드 타입 중 하나 이상을 점검할 수 있다. 일부 실시예에서, 이러한 아이템들 중 어느 하나가 화이트 리스트 내 대응 엔트리/필드와 일치하지 않을 때, 연결이 불허될 수 있다. 다른 실시예에서, 사용자는 의문스런 통신을 설명하는 메시지(가령, 이

메일)의 전송, 팝업 윈도/다이얼로그의 제시, 등에 의해, 사용자가 통지받을 수 있다.

[0097] 다른 예로서, 클라이언트(12, 13, 또는 14)가 인바운드 연결을 수신할 때, 원격 장치의 IP 어드레스 및 포트 번호, 이 연결에 서빙하고 있는(가령, 포트 상에서 듣고 있는) 프로그램(프로세스명), 액세스 시간 윈도, 배치 또는 대화형 프로세스, URL/URI 또는 도메인 네임(적절한 경우), 보안 등급, 업로드/다운로드, 카테고리 코드, 또는 페이로드 유형 중 하나 이상을 점검할 수 있다.

[0098] 이러한 화이트 리스트는 우수한 보안 실례를 가진 잘 알려진 회사와 같은, 일반적으로 안전한 시스템 또는 서비스를 식별하는 엔트리를 또한 포함할 수 있다. (가령, IP 어드레스 또는 도메인 네임에 의해 식별되는) 이러한 시스템의 경우에, 임의의 유형의 데이터의 액세스, 다운로드, 또는 업로드를 허용하는 것이 안전할 수 있다.

[0099] 장치가 바이러스와 같은 악성 코드에 의해 이미 감염되었다면, 설명되는 기술은 프로그램명(가령, 프로세스명), 액세스 시간 윈도, 페이로드 유형, 배치 또는 대화형 모드를 점검함으로써 중요한 정보를 업로드하기 위해 바이러스가 네트워크에 액세스하는 것을 막을 수 있다. 이는 바이러스가 다른 장치로 확산되는 것을 막을 수 있다. 바이러스가 데이터를 내보내기 위해 온라인 이메일 계정에 액세스하고자 허용가능한 프로세스 리스트 상에 이미 존재하는 웹 브라우저와 같은 다른 프로그램을 열려고 시도할 경우, 액세스 시간 윈도 및 배치 모드 점검이, 예를 들어, 모든 배치 모드 웹 브라우저 프로그램을 불허함으로써, 이를 여전히 중지시킬 수 있다.

[0100] 일부 실시예에서 다음의 방식으로 악성 또는 의문스런 이메일이 검출될 수 있다. 첫번째로, 이메일 클라이언트와 연관된 인가 모듈이 이메일 헤더의 발신자 필드로부터 소스 이메일 어드레스(가령, source@hostname.net)를 추출할 수 있다. 악성 이메일에서, 소스 이메일 어드레스는 자주 위조되어, 친구 또는 다른 알려진 자로부터 온 것처럼 보일 수 있다. 그 후, 인가 모듈은 가령, 소스 이메일 어드레스로부터 추출되는 호스트명(가령, hostname.net)을 이용하여 도메인 네임 탐색을 수행함으로써, 소스 이메일 어드레스에 기초하여 제 1 IP 어드레스를 결정한다. 다음에, 인가 모듈은 이메일 헤더 내 RECEIVED 필드로부터 제 2 IP 어드레스를 추출할 것이다. RECEIVED 필드는 통상적으로 수신자의 SMTP 서버에 의해 삽입되고, 발신자의 SMTP 서버의 실제 소스 IP 어드레스를 포함한다. 그 후, 인가 모듈은 제 1 및 제 2 IP 어드레스의 일치를 비교한다. 일치하지 않을 경우, 이메일이 진짜가 아니고 발신자가 소스 이메일 어드레스를 위조하였음이 가능할 수 있고, 사용자에게 통지, 이메일 열기 거절, 이미지, 마크업 랭기지, 또는 코드의 렌더링 불허, 등과 같이, 적절한 액션을 취할 수 있다.

[0101] 도 6은 네트워크 통신 이밸류에이터(evaluator) 프로세스(600)를 예시하는 흐름도다. 이 프로세스는 컴퓨팅 시스템(20)(도 2)에 의해 실행되는 평가 모듈(38)가 같은 모듈에 의해 수행될 수 있다.

[0102] 프로세스는 블록(602)에서 시작하여, 신뢰되는 네트워크 어드레스를 위한 허용가능한 통신 특성을 명시하는 화이트 리스트에 액세스한다. 화이트 리스트 액세스는 화이트 리스트의 수신, 질의, 검색, 또는 그렇지 않을 경우 처리를 포함할 수 있다. 일부 실시예에서, 화이트 리스트는 앞서 표 1에서 설명된 바와 같이, 하나 이상의 허용가능 네트워크 통신 특성의 표시사항과 연관된 신뢰 네트워크 어드레스를 각각 포함하는 로우(rows) 또는 엔트리(entries)를 포함한다.

[0103] 블록(604)에서, 프로세스는 네트워크 통신에 대응하는 IP 어드레스를 결정한다. IP 어드레스 결정은 컴퓨팅 시스템 내 TCP/IP 스택 또는 다른 통신 모듈로부터 IP 어드레스를 요청하는 과정을 포함할 수 있다. IP 어드레스는 소스 또는 수신 IP 어드레스일 수 있다. 통상적으로, 통신이 인바운드 연결인 경우, 소스 IP 어드레스가 점검되고, 통신이 아웃바운드일 경우, 목적 IP 어드레스가 점검된다. 다른 시나리오에서, IP 어드레스는, 다른 방식으로, 가령, 네트워크 통신과 연관된 도메인 네임으로 DNS 서버에 질의함으로써, 결정될 수 있다. 도메인 네임은 예를 들어, URL, 이메일 메시지, 이메일 어드레스, 등을 참조하여 결정될 수 있다.

[0104] 블록(606)에서, 프로세스는 네트워크 통신과 연관된 제 1 통신 특성을 결정한다. 제 1 통신 특성 결정은 표 1에 설명된 성질들 중 하나의 결정을 포함한다. 예를 들어, 프로세스는 하루의 시간, 통신의 방향성, 데이터 페이로드 유형, 등과 같은 성질을 결정할 수 있다. 프로세스는 예를 들어, IP 어드레스로 지리-위치 정보 서비스에 질의하고 IP 어드레스와 연관된 위치(가령, 도시, 주, 국가, 우편번호)의 표시사항에 응답하여 수신함으로써, 네트워크 통신과 연관된 지리 위치를 결정할 수 있다.

[0105] 블록(608)에서, 프로세스는 화이트 리스트에 의해 IP 어드레스와 연관되는 허용가능 통신 특성인 제 2 통신 특성을 결정한다. 제 2 성질 결정은 화이트 리스트 내 IP 어드레스의 탐색과, IP 어드레스와 연관된, 제 1 통신 특성에 대응하는 통신 특성의 불러오기 과정을 포함할 수 있다. 예를 들어, 제 1 통신 특성이 하루의 시간일 경우, 프로세스는 화이트 리스트 내 허용가능 통신 주기를 탐색할 수 있다. 제 1 통신 특성이 지리 위치일 경우, 프로세스는 화이트 리스트 내 허용가능 지리 위치를 탐색할 수 있다.

[0106] 블록(610)에서, 프로세스는 제 1 통신 특성이 제 2 통신 특성에 포함되는지 여부를 결정한다. 제 1 통신 특성이 제 2 통신 특성에 포함되는지 여부의 결정은, 제 2 성질이 제 1 성질을 에워싸거나 지니는지 여부의 결정을 포함할 수 있다. 예를 들어, 제 2 성질이 허용가능 국가((가령, 워싱턴주)일 경우, 제 2 성질은 제 1 성질이 허용가능 국가와 동일하거나 국가 내에 위치할 경우(가령, 워싱턴주, 시애틀, US 우편 번호) 국가에 포함된다. 마찬가지로, 제 2 성질이 허용가능 시간 주기(가령, 오전 6시 내지 오후 11시 사이)일 경우, 제 1 성질은 제 1 성질(가령, 오후 10시)가 상기 시간 주기 내에 있을 경우, 상기 시간 주기에 포함된다.

[0107] 일부 실시예에서, 제 1 성질이 제 2 성질에 포함되는지 여부의 결정은 2개의 성질이 일치하는 지 여부의 결정을 포함한다. 성질 일치는 2개의 스트링, 번호, 또는 다른 데이터 유형간의 균등성(equality)을 위한, 등가성(equivalence) 검사의 수행을 포함할 수 있다. 일부 경우에, 일치는 엄격한 균등성 검사일 수 있고, 반면에 다른 경우에, 경우-무관 스트링 일치에서와 같이, 근사법으로 충분할 수 있다.

[0108] 블록(612)에서, 프로세스는 네트워크 통신의 허용가능성의 표시를 제공한다. 허용가능성 표시 제공은 (가령, 대화 상자 또는 다른 팝업 윈도를 통해) 사용자에게 알림, 메시지 전송(가령, 이메일), 로그에 표시사항 레코딩, 다른 프로세스 또는 코드 블록에 값 리턴, 등을 포함할 수 있다.

[0109] 일부 실시예는 추가적인 또는 대안의 기능을 제공할 수 있다. 일 실시예는 웹 범주에서 나타날 수 있는 것과 같은 사용자 인증을 수행한다. 기존 인증 기법은 사용자명/패스워드 조합을 이용한다. 일부 실시예는 사용자명/패스워드 조합 기법과 연계하여 위-설명된 기술들 중 하나 이상을 또한 이용할 수 있다. 예를 들어, 일부 실시예는 사용자명 및 패스워드에 추가하여 IP 어드레스를 점검할 수 있다. IP 어드레스가 할당되고 네트워크 상에서 고유함에 따라, 타에 의해 쉽게 조작될 수 없다. 따라서, 해커가 사용자의 사용자명 및 패스워드를 훔쳤을 경우, 해커가 정확한 IP 어드레스를 가지지 못할 것이기 때문에 해커가 계정에 잠입할 수 없을 것이다. 포트 번호 및 다른 성질(가령, 하루 중 시간, 지리 영역)이 인증 기법에 또한 포함될 수 있다. 이러한 성질들 중 모두가 아니더라도 많은 부분이 사용자의 참가, 개입, 상호작용없이 결정될 수 있다. 예를 들어, IP 어드레스는 TCP/IP스택을 참조하여 직접 결정될 수 있다.

[0110] 또한, 현재의 인터넷 서비스 제공자는 네트워크 어드레스 변환(NAT) 또는 프록시 서비스를 이용할 수 있어서, 많은 사용자들이 동일 IP 어드레스를 공유할 수 있다. 일부 실시예는, 각각의 내부 IP가 동일한 외부 IP 어드레스를 갖지만 고유의 식별가능 포트 번호를 갖도록, NAT/프록시 모듈에 의해 관리되는 내부 IP 어드레스에 대응하는 정적 TCP 포트 번호를 할당하는 NAT/프록시 서비스(가령, 라우터 또는 게이트웨이에 의해 제공됨)를 이용함으로써 NAT/프록시 범주에서 기능한다.

[0111] 일부 실시예는 다음의 추가적 작동들을 수행하기 위해 도 6의 프로세스를 확장한다: 제 1 IP 어드레스 및 포트 번호를 컴퓨팅 시스템의 TCP/IP 스택으로부터 수신하는 단계와, 네트워크 통신과 연관된 유니폼 리소스 로케이터(URL)/유니폼 리소스 식별자(URI)를 수신하는 단계와, 소유자명을 IP 어드레스와 상관시키는 할당 데이터베이스에 TCP/IP 스택으로부터 수신되는 제 1 IP 어드레스를 질의함으로써, 제 1 IP 어드레스와 연관된 제 1 명칭을 결정하는 단계와, 소유자명을 도메인 네임과 상관시키는 할당 데이터베이스에 네트워크 리소스와 연관된 URL/URI의 도메인 네임을 질의함으로써, URL/URI와 연관된 제 2 명칭을 결정하는 단계와, 제 1 IP 어드레스 및 포트 번호가 신뢰 네트워크 어드레스의 지정된 화이트 리스트 내에 포함되는지 여부와 제 1 명칭이 제 2 명칭과 일치하는지 여부에 기초하여, 통신 작동의 허용 또는 불허의 표시사항을 설정하는 단계.

[0112] 일부 실시예는, 네트워크 리소스와 통신하기 위해, TCP/IP 스택을 포함하는 통신 인터페이스와, 명령어를 저장하기 위한 메모리와, 상기 통신 인터페이스 및 상기 메모리와 통신하는 프로세서를 포함하는 통신 제어 시스템에 있어서, 상기 프로세서는, 인증되지 않은 네트워크 노드를 위한 어드레스를 포함하지 않는, 그리고, 각각의 신뢰 네트워크 어드레스에 대하여, 허용가능한 통신 특성 중 하나 이상의 표시사항을 포함하는, 신뢰 네트워크 어드레스의 지정된 화이트 리스트를 수신하는 단계와, 네트워크 통신에 대응하는 제 1 인터넷 프로토콜(IP)어드레스를 결정하는 단계와, 상기 네트워크 통신과 연관된 제 1 통신 특성을 결정하는 단계와, 상기 제 1 IP 어드레스에 대응하는 화이트 리스트 내 엔트리에 의해 명시되는 허용가능 통신 특성인 제 2 통신 특성을 결정하는 단계와, 상기 제 1 통신 특성이 제 2 통신 특성에 포함되는지 여부를 결정함으로써 화이트 리스트와 관련하여 네트워크 통신을 평가하는 단계와, 제 1 통신 특성이 제 2 통신 특성에 포함되지 않는다고 결정함에 응답하여, 네트워크 통신이 불허된다는 표시사항을 설정하는 단계와, 제 1 통신 특성이 제 2 통신 특성에 포함됨을 결정함에 응답하여, 네트워크 통신이 허용된다는 표시사항을 설정하는 단계에 의해 네트워크 통신을 평가하도록 구성된다.

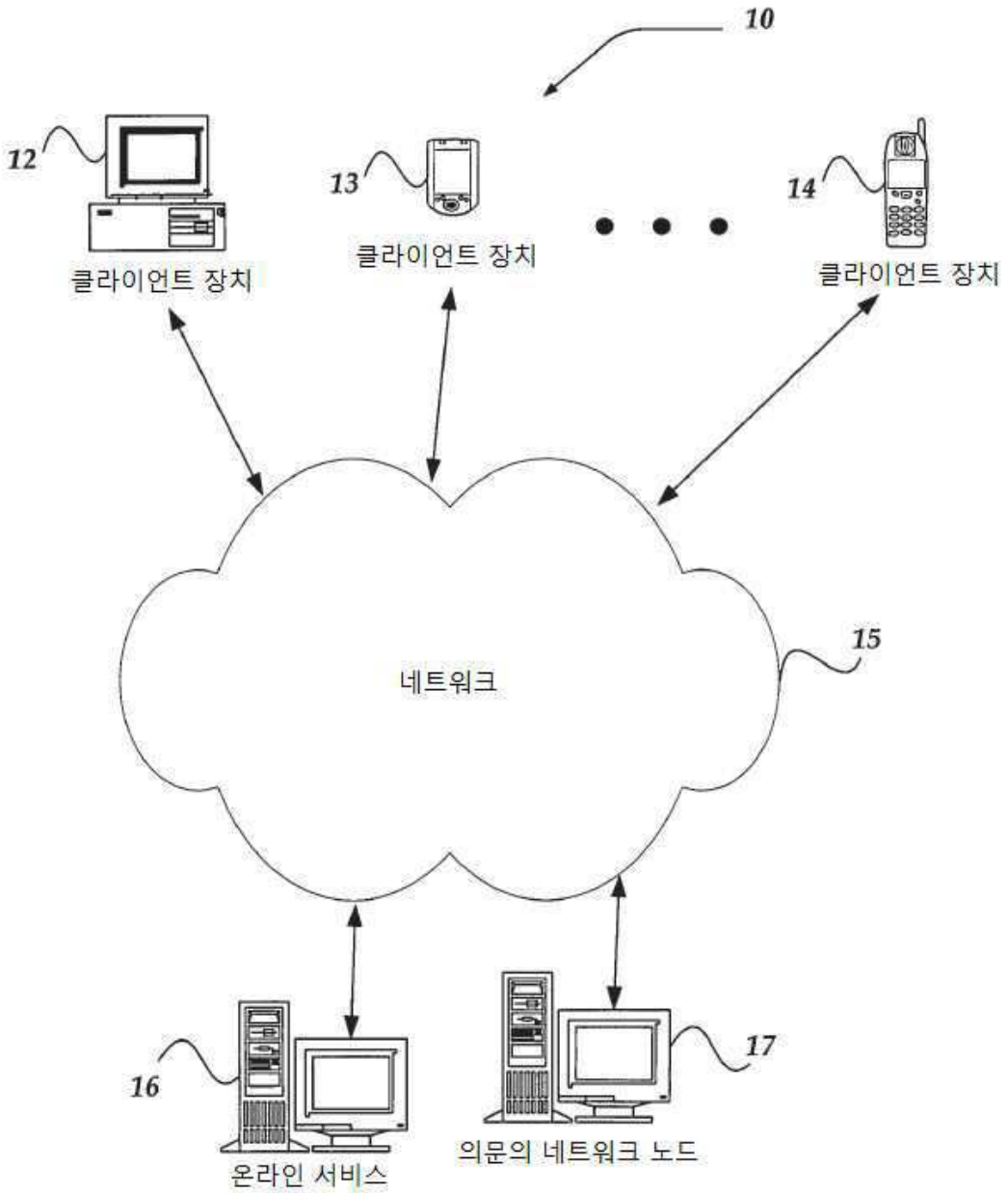
[0113] 2007년 2월 28일 출원된, 발명의 명칭 "Evaluating a Questionable Network Communication"의 미국특허출원 제

11/712,648호(현재 미국특허 제8,621,604호), 2006년 9월 6일 출원된, 발명의 명칭 "Identifying A Network Address Source For Authentication" 미국특허출원 제11/470,581호, 2005년 9월 6일 출원된 발명의 명칭 "Identifying A Network Address Source For Authentication"의 미국특허가출원 제60/714,889호, 및 2006년 3월 17일 출원된 발명의 명칭 "Identifying A Network Address Source For Authentication"의 미국특허가출원 제60/783,446호를 포함하지만, 이에 제한되지 않는, 여기서 언급되는 모든 문헌의 그 내용 전체가 본 발명에 포함된다.

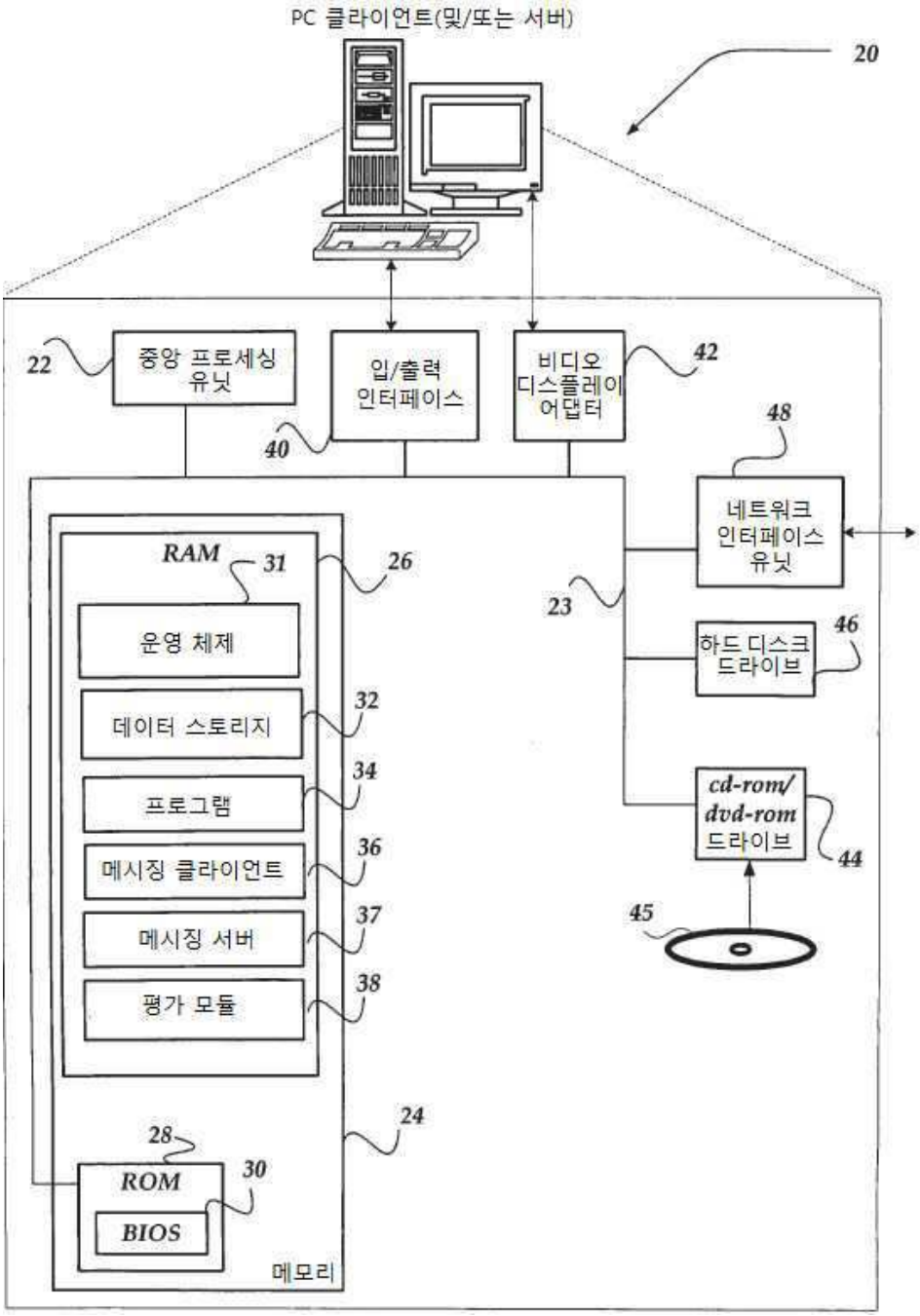
[0114] 위 명세서, 예, 및 데이터는 발명의 구성물의 제조 및 이용의 완전한 설명을 제공한다. 예를 들어, 인증을 위해 디지털 인증서가 사용될 수 있고, 통신을 위해 암호화가 사용될 수 있으며, 다른 특징이 포함될 수 있다. 그러나, 다른 실시예가 당 업자에게 명백할 것이다. 발명의 많은 실시예들이 발명의 사상 및 범위로부터 벗어나지 않으면서 이루어질 수 있기 때문에, 발명은 이후 첨부되는 청구범위에 위치한다.

도면

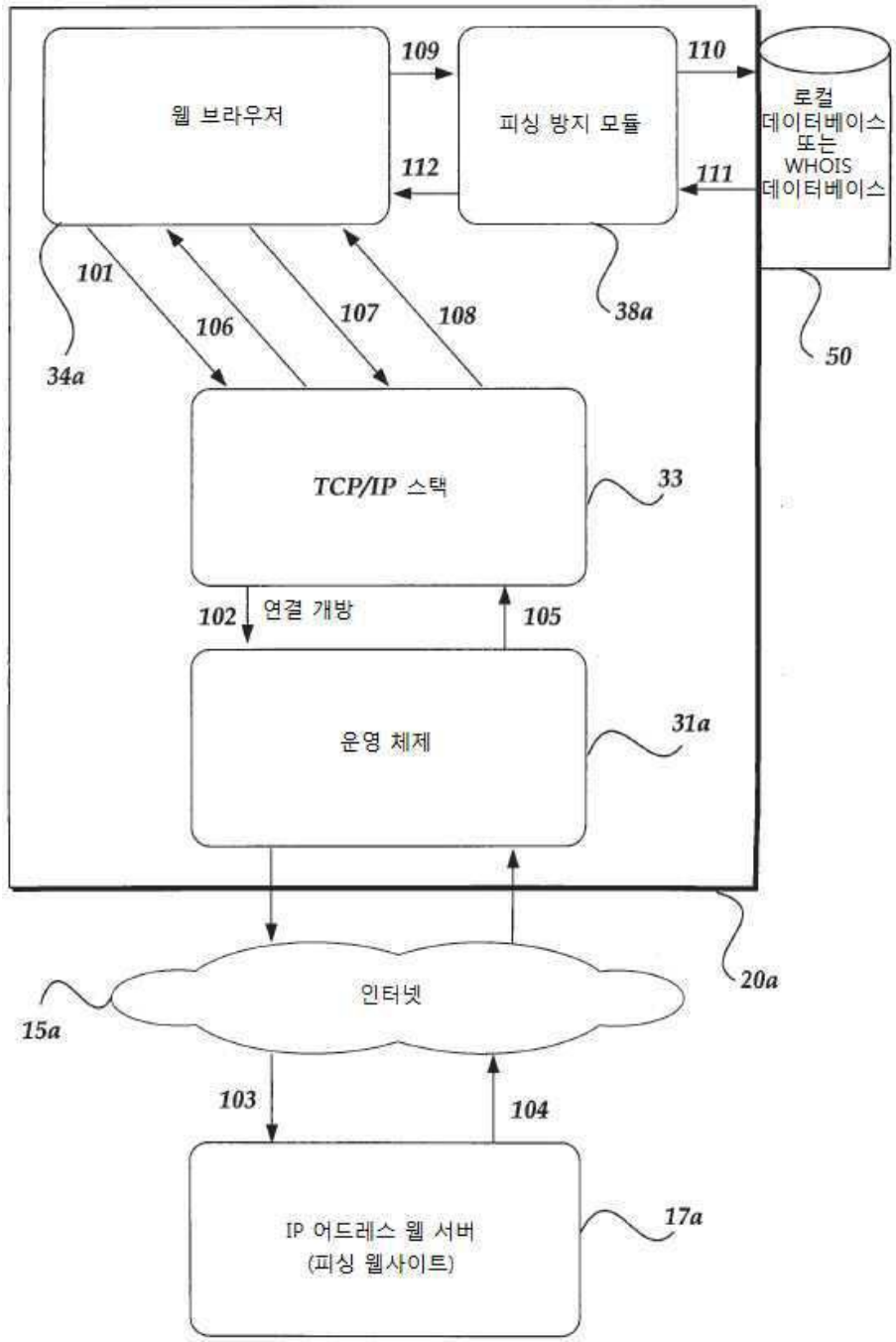
도면1



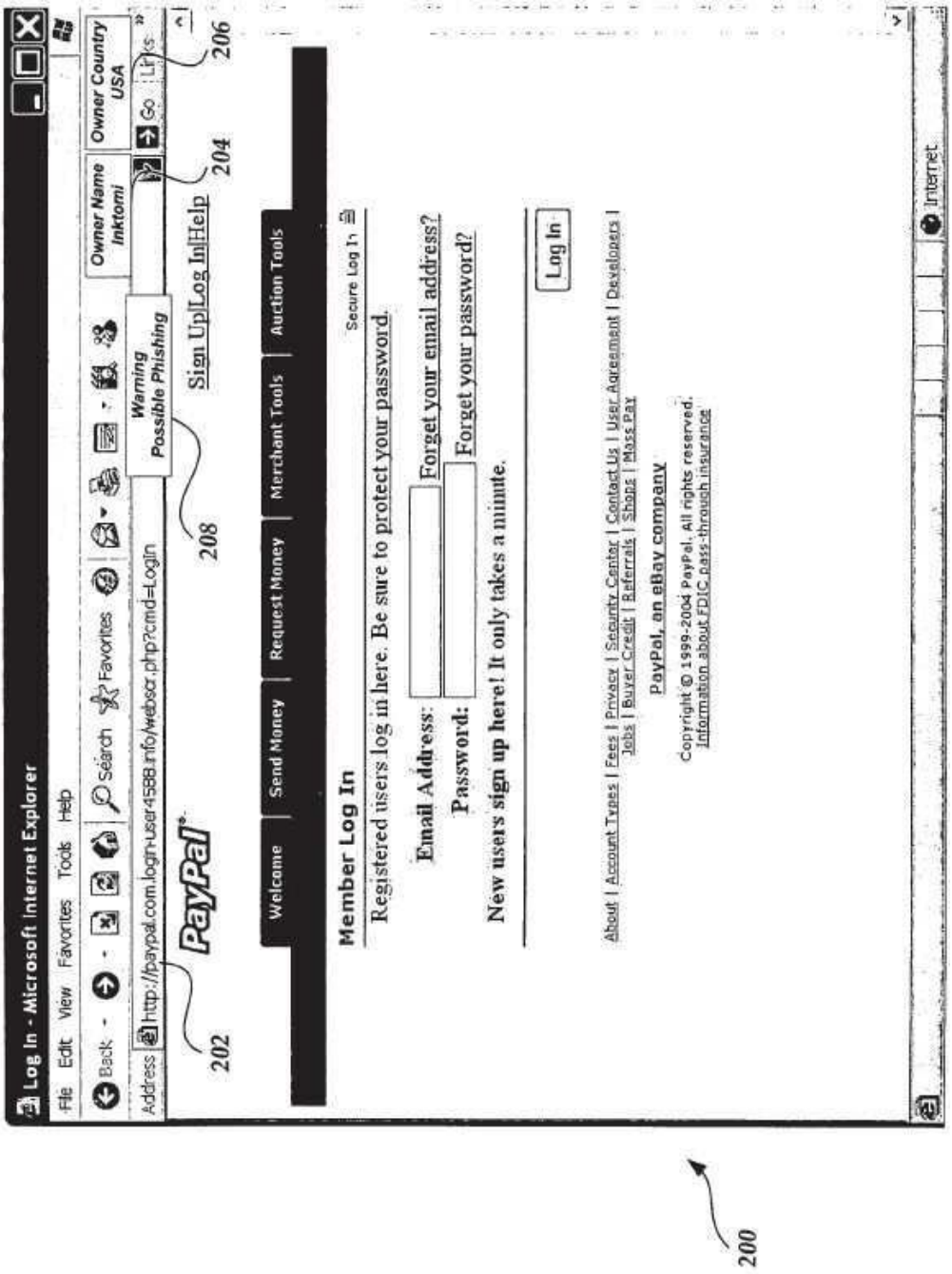
도면2


PC 클라이언트(및/또는 서버)
20
22
중앙 프로세싱 유닛
입/출력 인터페이스
40
비디오 디스플레이 어댑터
42
48
네트워크 인터페이스 유닛
23
RAM
31
26
운영 체제
데이터 스토리지
32
프로그램
34
메시징 클라이언트
36
메시징 서버
37
평가 모듈
38
하드 디스크 드라이브
46
cd-rom/ dvd-rom 드라이브
44
45
24
28
ROM
30
BIOS
메모리

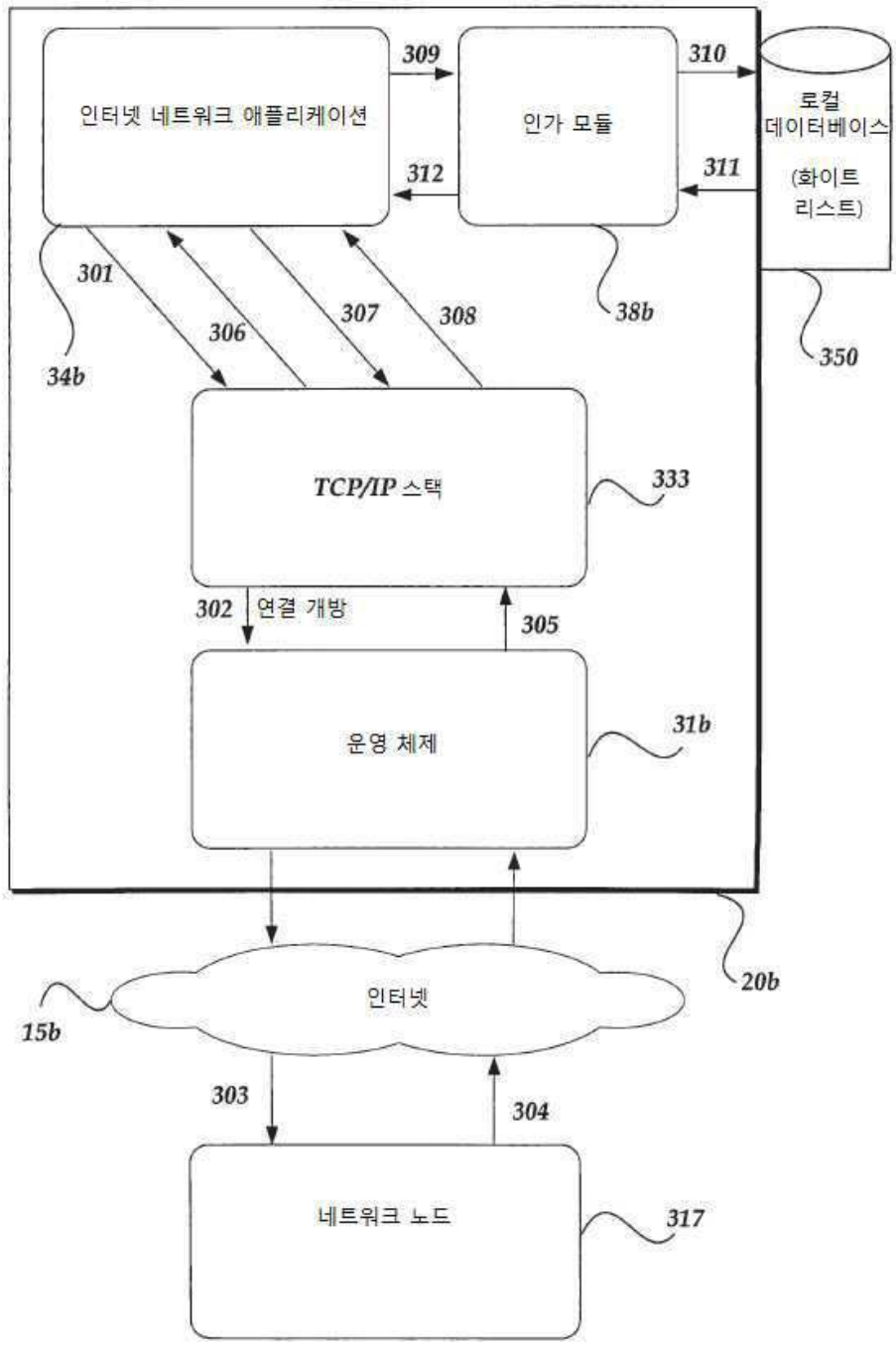
도면3


웹 브라우저
109
피싱 방지 모듈
110
로컬
데이터베이스
또는
WHOIS
데이터베이스
112
111
101
106
107
108
38a
34a
50
TCP/IP 스택
33
102
연결 개방
105
운영 체제
31a
20a
인터넷
15a
103
104
IP 어드레스 웹 서버
(피싱 웹사이트)
17a

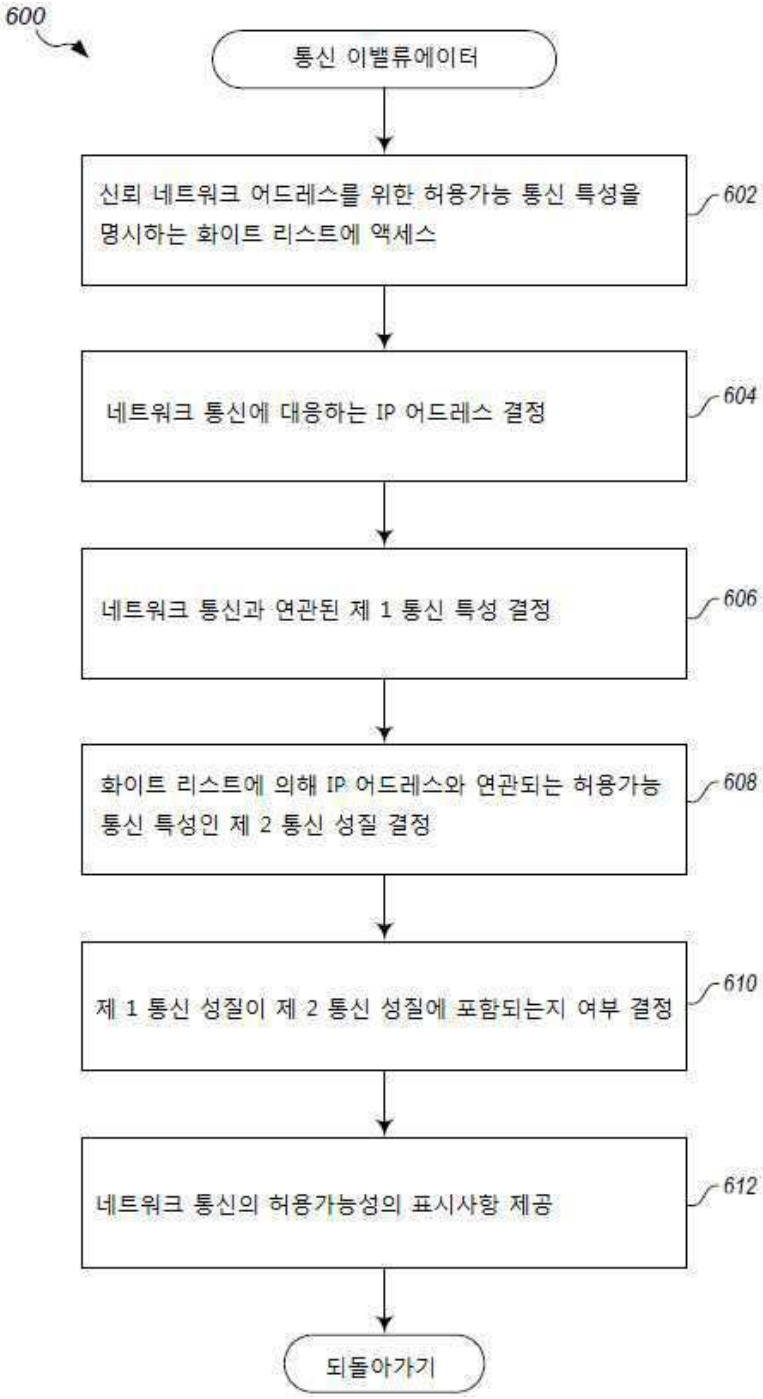
도면4


Log In - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://paypal.com.login-user4588.info/websor.php?cmd=Login
Warning Possible Phishing
Owner Name Inktomi
Owner Country USA
PayPal
Sign Up|Log In|Help
Welcome
Send Money
Request Money
Merchant Tools
Auction Tools
Member Log In
Secure Log In
Registered users log in here. Be sure to protect your password.
Email Address:
Forget your email address?
Password:
Forget your password?
New users sign up here! It only takes a minute.
Log In
About | Account Types | Fees | Privacy | Security Center | Contact Us | User Agreement | Developers | Jobs | Buyer Credit | Referrals | Shops | Mass Pay
PayPal, an eBay company
Copyright © 1999-2004 PayPal. All rights reserved.
Information about FDIC pass-through insurance
Internet
202
208
204
206
200

도면5


인터넷 네트워크 애플리케이션
309
인가 모듈
310
로컬
데이터베이스
(화이트
리스트)
311
312
301
306
307
308
38b
34b
350
TCP/IP 스택
333
302
연결 개방
305
운영 체제
31b
20b
인터넷
15b
303
304
네트워크 노드
317

도면6


600
통신 이밸류에이터
신뢰 네트워크 어드레스를 위한 허용가능 통신 특성을 명시하는 화이트 리스트에 액세스
602
네트워크 통신에 대응하는 IP 어드레스 결정
604
네트워크 통신과 연관된 제 1 통신 특성 결정
606
화이트 리스트에 의해 IP 어드레스와 연관되는 허용가능 통신 특성인 제 2 통신 성질 결정
608
제 1 통신 성질이 제 2 통신 성질에 포함되는지 여부 결정
610
네트워크 통신의 허용가능성의 표시사항 제공
612
되돌아가기