(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년12월20일
(11) 등록번호 10-1213935
(24) 등록일자 2012년12월12일

(51) 국제특허분류(Int. Cl.)
G06Q 50/00D1 (2008.03)
(21) 출원번호 10-2011-0001730(분할)
(22) 출원일자 2011년01월07일
심사청구일자 2011년02월07일
(65) 공개번호 10-2011-0009729
(43) 공개일자 2011년01월28일
(62) 원출원 특허 10-2004-0016409
원출원일자 2004년03월11일
심사청구일자 2009년03월11일
(30) 우선권주장
10/683,624 2003년10월10일 미국(US)
(뒷면에 계속)
(56) 선행기술조사문헌
US06321267 B1
US20020198950 A1
전체 청구항 수 : 총 47 항

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
라이언, 제임스 에이.
미국 워싱턴주 레드몬드
아트킨선, 밥
미국 워싱턴주 레드몬드
(뒷면에 계속)
(74) 대리인
제일특허법인

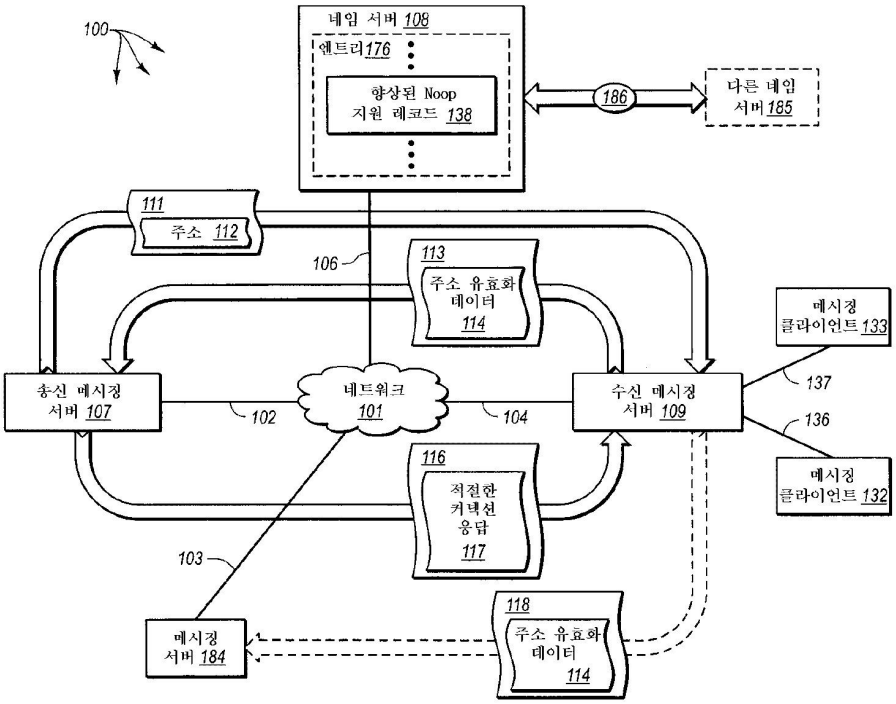
심사관 : 최석규

(54) 발명의 명칭 **불필요하고 요청되지 않은 전자 메시지를 감소시키는 방법**

(57) 요 약

본 발명은 예를 들어 불필요하거나 요청되지 않은 전자 메시지를 보다 신뢰성 있게 분류하는 것을 촉진하기 위하여 메시지 분류 모듈에 제공될 수 있는 입력 생성을 제공한다. 일 실시예에서, 송신 메시징 서버는 주소 검증 데이터에 적절한 응답을 제공하고, 이에 의하여 송신 메시징 서버가 위조된 네트워크 주소를 사용할 가능성을 감소시킨다. 다른 실시예에서, 메시징 서버가 도메인용 전자 메시지를 송신하도록 인가될 지의 여부가 결정된다. 또 다른 실시예에서, 도메인에 의하여 준수되는 전자 메시지 전송 정책이 인식된다. 또 다른 실시예에서, 송신 컴퓨터 시스템은 연산 리소스를 소비하여 연산 퍼즐을 해결하고 전자 메시지에 응답 문서를 포함한다. 수신 컴퓨터 시스템은 전자 메시지를 수신하고, 응답 문서를 검증한다.

대 표 도



(72) 발명자

카츠, 하비

미국 워싱턴주 레드몬드

라운트웨이트, 로버트

미국 워싱턴주 레드몬드

(30) 우선권주장

10/684,020 2003년10월10일 미국(US)

60/454,517 2003년03월12일 미국(US)

특허청구의 범위

청구항 1

하나 이상의 수신 컴퓨터 시스템들에 네트워크 접속 가능하고, 전자 메시지들을 상기 수신 컴퓨터 시스템들에 송신하도록 구성된 송신 컴퓨터 시스템에서,

송신 컴퓨터 시스템에 의해 송신되는 접속 초기화(connection initiation)에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인(originate)하는 것을 확인하기 위한 방법으로서,

지정된 수신 컴퓨터 시스템으로 접속 초기화 데이터를 송신하는 동작 - 상기 접속 초기화 데이터는 상기 송신 컴퓨터 시스템의 송신 주소로 추정된(purported) 송신 주소를 포함함 -;

주소 검증 데이터와, 통상은 접속 설정에 포함되어 있지 않는 비표준 데이터의 적어도 일부를 포함하는 변경된 접속 설정 데이터를 수신하는 동작 - 비표준 데이터의 일부가 상기 접속 설정에 포함됨으로써 비표준 데이터의 일부가 접속 응답에 제공될 것이라는 것을 알지 못하고서는 상기 변경된 접속 설정 데이터에 대응하는 접속 응답을 제공할 가능성을 감소시키며, 상기 비표준 데이터의 적어도 일부는 무작위 문자열(random string of characters)을 포함함 -;

접속 응답이 상기 주소 검증 데이터 및 비표준 데이터의 일부를 포함하였다는 것을 결정하는 것에 기초하여 상기 접속 응답이 상기 지정된 수신 컴퓨터 시스템으로부터 수신되었다는 것을 확인하는 동작;

상기 주소 검증 데이터 및 비표준 데이터의 일부에 기초하여 상기 변경된 접속 설정 데이터에 대응하는 접속 응답을 생성시키는 동작 - 상기 응답은 확인된 수신 컴퓨터 시스템에 의해 인식되는 형태의 비표준 데이터의 일부를 포함함 -; 및

상기 변경된 접속 설정 데이터에 대응하는 상기 접속 응답 데이터를 상기 수신 컴퓨터 시스템으로 송신하는 동작

을 포함하는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 2

제1항에 있어서,

수신 컴퓨터 시스템에 접속 초기화 데이터를 송신하는 동작은 전송 제어 프로토콜(Transmission Control Protocol) 접속 초기화 데이터를 송신하는 동작을 포함하는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 3

제1항에 있어서,

수신 컴퓨터 시스템에 접속 초기화 데이터를 송신하는 동작은 SMTP HELO 명령 또는 SMTP EHLO 명령을 송신하는 동작을 포함하는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 4

제1항에 있어서,

주소 검증 데이터를 포함하는 변경된 접속 설정 데이터를 수신하는 동작은 변경된 접속 설정 데이터를 수신하는 동작을 포함하는데, 상기 변경된 접속 설정 데이터는 접속 초기화 데이터 및 복수의 네트워크 패킷들로 분리된 접속 설정 데이터를 재송신하라는 요구로부터 선택되는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 5

제1항에 있어서,

주소 검증 데이터를 포함하는 변경된 접속 설정 데이터를 수신하는 동작은 문자들의 무작위 시퀀스를 포함하는 HELO 응답 명령 또는 EHLO 응답 명령을 수신하는 동작을 포함하는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 6

제1항에 있어서,

상기 주소 검증 데이터에 기초하여 상기 변경된 접속 설정 데이터에 대응하는 접속 응답을 생성하는 동작은 상기 변경된 접속 설정 데이터에 대응하는 접속 응답을 생성하는 동작을 포함하고, 상기 변경된 접속 설정 데이터에 대응하는 접속 응답은 상기 접속 초기화 데이터를 재송신하는 것과, 상기 변경된 접속 설정 데이터에 대응하는 확인 응답(acknowledgement) 시퀀스 번호를 갖는 네트워크 패킷을 송신하는 것으로부터 선택되는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 7

제1항에 있어서,

상기 주소 검증 데이터에 기초하여 상기 변경된 접속 설정 데이터에 대응하는 접속 응답을 생성하는 동작은 향상된 NOOP 명령 내에 문자들의 무작위 시퀀스를 포함시키는 동작을 포함하고, 문자들의 상기 무작위 시퀀스는 상기 접속 초기화 데이터에 응답하여 상기 수신 컴퓨터 시스템으로부터 수신되는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 8

제1항에 있어서,

상기 수신 컴퓨터 시스템에 상기 변경된 접속 설정 데이터에 대응하는 상기 접속 응답 데이터를 송신하는 동작은 문자들의 무작위 시퀀스를 포함하는 향상된 NOOP 명령을 송신하는 동작을 포함하고, 문자들의 상기 무작위 시퀀스는 상기 접속 초기화 데이터에 응답하여 상기 수신 컴퓨터 시스템으로부터 수신되는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 9

하나 이상의 송신 컴퓨터 시스템들에 네트워크 접속 가능하고, 상기 송신 컴퓨터 시스템들로부터 전자 메시지를 수신하도록 구성된 수신 컴퓨터 시스템에서, 상기 수신 컴퓨터 시스템이 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 방법으로서,

송신 컴퓨터 시스템으로부터 접속 초기화 데이터를 수신하는 동작 - 상기 접속 초기화 데이터는 상기 송신 컴퓨터 시스템의 송신 주소로 추정된 송신 주소를 포함함 -;

주소 검증 데이터와, 통상은 접속 설정에 포함되지 않는 비표준 데이터의 적어도 일부를 포함하도록 표준 접속 설정 데이터를 변경하는 동작 - 비표준 데이터의 일부가 포함됨으로써 비표준 데이터의 일부가 접속 응답에 제공될 것이라는 것을 알지 못하고서는 상기 변경된 접속 설정 데이터에 대응하는 접속 응답을 제공할 가능성을 감소시키며, 상기 비표준 데이터의 적어도 일부는 무작위 문자열(random string of characters)을 포함함 -; 및

변경된 상기 접속 설정 데이터를 상기 추정된 송신 주소로 송신하는 동작 - 상기 추정된 송신 주소를 지닌 송신 컴퓨터 시스템은 상기 접속 응답이 주소 검증 데이터 및 비표준 데이터의 일부를 포함하였다는 것을 결정함에 기초하여 상기 접속 응답이 상기 수신 컴퓨터 시스템으로부터 수신되었다는 것을 확인하도록 구성됨 -

을 포함하는, 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 상기 수신 컴퓨터 시스템에 대한 방법.

청구항 10

제9항에 있어서,

접속 초기화 데이터를 송신 컴퓨터 시스템으로부터 수신하는 동작은 전송 제어 프로토콜 접속 초기화 데이터를 수신하는 동작을 포함하는, 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 상기 수신 컴퓨터 시스템에 대한 방법.

청구항 11

제9항에 있어서,

접속 초기화 데이터를 송신 컴퓨터 시스템으로부터 수신하는 동작은 SMTP HELO 명령을 수신하거나 SMTP EHLO 명령을 수신하는 동작을 포함하는, 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 상기 수신 컴퓨터 시스템에 대한 방법.

청구항 12

제9항에 있어서,

주소 검증 데이터를 포함하도록 표준 접속 설정 데이터를 변경하는 동작은 전송 제어 프로토콜 접속 초기화 데이터의 재전송을 요구하도록 상기 전송 제어 프로토콜 접속 초기화 데이터에 대한 표준 응답을 변경하는 동작을 포함하는, 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 상기 수신 컴퓨터 시스템에 대한 방법.

청구항 13

제9항에 있어서,

주소 검증 데이터를 포함하도록 표준 접속 설정 데이터를 변경하는 동작은 전송 제어 프로토콜 접속 설정 데이터를 복수의 네트워크 패킷들로 분리하는 동작을 포함하는, 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 상기 수신 컴퓨터 시스템에 대한 방법.

청구항 14

제9항에 있어서,

주소 검증 데이터를 포함하도록 표준 접속 설정 데이터를 변경하는 동작은 SMTP HELO 응답 명령 또는 SMTP EHLO 응답 명령 내에 문자들의 무작위 시퀀스를 포함하는 동작을 포함하는, 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 상기 수신 컴퓨터 시스템에 대한 방법.

청구항 15

제9항에 있어서,

상기 변경된 접속 설정 데이터를 상기 추정된 송신 주소로 송신하는 동작은 변경된 전송 제어 프로토콜 접속 설정 데이터를 추정된 인터넷 프로토콜 주소로 송신하는 동작을 포함하는, 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 상기 수신 컴퓨터 시스템에 대한 방법.

청구항 16

제9항에 있어서,

상기 변경된 접속 설정 데이터를 상기 추정된 송신 주소로 송신하는 동작은 문자들의 무작위 시퀀스를 포함하는 SMTP HELO 응답 명령을 송신하거나 SMTP EHLO 응답 명령을 송신하는 동작을 포함하는, 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 상기 수신 컴퓨터 시스템에 대한 방법.

청구항 17

제9항에 있어서,

상기 추정된 송신 주소에 해당하는 컴퓨터 시스템이 상기 주소 검증 데이터에 적절히 응답했는지를 결정하는 동작은 상기 추정된 송신 주소가 변경된 전송 제어 프로토콜 접속 설정 데이터에 적절히 응답했는지를 결정하는

동작을 포함하는, 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 상기 수신 컴퓨터 시스템에 대한 방법.

청구항 18

제9항에 있어서,

상기 추정된 송신 주소에 해당하는 컴퓨터 시스템이 상기 주소 검증 데이터에 적절히 응답했는지를 결정하는 동작은 상기 추정된 송신 주소가 상기 주소 검증 데이터에 포함된 문자들의 무작위 시퀀스를 포함하는 향상된 NOOP 명령어로 응답했는지를 결정하는 동작을 포함하는, 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 상기 수신 컴퓨터 시스템에 대한 방법.

청구항 19

제9항에 있어서,

상기 추정된 송신 주소가 상기 주소 검증 데이터에 적절히 응답하지 않으면, 상기 추정된 송신 주소에 해당하는 DNS 레코드 세트에 대하여 DNS 문의를 발행하는 동작; 및

상기 추정된 송신 주소가 주소 검증 데이터의 사용을 지원하는지 여부를 지시하는 XML 명령어들을 포함하는 하나 이상의 TXT 레코드들을 수신하는 동작

을 더 포함하는, 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하고 있는지를 검출하는 상기 수신 컴퓨터 시스템에 대한 방법.

청구항 20

하나 이상의 송신 도메인들에 네트워크 접속 가능하고, 송신 도메인들로부터 전자 메시지들을 수신하도록 구성된 하나 이상의 수신 메시징 서버들을 포함하는 수신 도메인에서, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법으로서,

상기 송신 도메인으로부터 송신된 것으로 추정되는 전자 메시지를 수신하는 동작 - 상기 전자 메시지는 통상은 접속 설정에 포함되어 있지 않는 비표준 데이터의 적어도 일부를 포함하여, 비표준 데이터의 일부가 상기 접속 설정에 포함됨으로써 비표준 데이터의 일부가 접속 응답에 제공될 것이라는 것을 알지 못하고서는 상기 비표준 데이터의 일부가 포함된 변경된 접속 설정 데이터에 대응하는 접속 응답을 제공할 가능성을 감소시키며, 상기 비표준 데이터의 적어도 일부는 무작위 문자열(random string of characters)을 포함함 -;

비표준 데이터의 일부를 포함하는 상기 전자 메시지의 복수의 파라미터 값들을 검사하여, 상기 접속 응답이 주소 검증 데이터 및 비표준 데이터의 일부를 포함하였다는 결정에 기초하여 상기 접속 응답이 지정된 수신 도메인으로부터 수신되었다는 것을 확인하도록 시도하는 동작;

상기 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가된 네트워크 주소들의 목록에 대하여 네임 서버에 문의하는 동작;

확인된 수신 도메인에 의해 인식되는 형태의 비표준 데이터의 일부의 포함 및 상기 문의에 기초하여, 실제 송신측 네트워크 주소가 상기 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 동작; 및

메시지 분류 모듈이 상기 수신된 전자 메시지를 분류하는 것에 관하여 보다 신뢰성 있는 결정을 할 수 있도록, 상기 결정의 결과들을 상기 메시지 분류 모듈에 제공하는 동작

을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 21

제20항에 있어서,

상기 송신측 도메인으로부터 송신된 것으로 추정되는 전자 메시지를 수신하는 동작은 전자 메일 메시지를 수신하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 22

제20항에 있어서,

상기 송신 도메인으로부터 송신된 것으로 추정되는 전자 메시지를 수신하는 동작은 역경로(Reverse-Path) 파라미터 값을 포함하지 않는 전자 메시지를 수신하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 23

제20항에 있어서,

실제 송신측 네트워크 주소를 식별하는 것을 시도하도록 상기 전자 메시지의 복수의 파라미터 값들을 조사하는 동작은 상기 송신 컴퓨터 시스템에 해당하는 인터넷 프로토콜 주소를 식별하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 24

제20항에 있어서,

실제 송신측 네트워크 주소를 식별하는 것을 시도하도록 상기 전자 메시지의 복수의 파라미터 값들을 조사하는 동작은 복수의 파라미터 값들을 조사하는 동작을 포함하고, 상기 복수의 파라미터 값들 중 적어도 하나는 제1 Resent-Sender 헤더 값, Resent-From 헤더의 제1 메일박스 값, Sender 헤더 값, 또는 From 헤더의 제1 메일박스 값으로부터 선택되는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 25

제20항에 있어서,

상기 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가된 네트워크 주소들의 목록에 대하여 네임 서버에 문의하는 동작은 상기 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가된 네트워크 주소들의 목록에 대하여 도메인 네임 서비스 서버(Domain Name Services server)에 문의하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 26

제25항에 있어서,

상기 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가된 네트워크 주소들의 목록에 대하여 도메인 네임 서비스 서버에 문의하는 동작은 상기 송신 도메인에 대하여 전자 메일 메시지를 송신하도록 인가된 인터넷 프로토콜 주소들의 목록에 대하여 도메인 네임 서비스에 문의하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 27

제20항에 있어서,

상기 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가된 네트워크 주소들의 목록을 수신하는 동작을 더 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 28

제27항에 있어서,

전자 메시지들을 송신하도록 인가된 네트워크 주소들의 목록을 수신하는 동작은 하나 이상의 DNS TXT 레코드들을 수신하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 29

제28항에 있어서,

전자 메시지들을 송신하도록 인가된 네트워크 주소들의 목록을 수신하는 동작은 네트워크 주소들의 상기 목록을 XML 명령어들로 인코딩하는 하나 이상의 DNS TXT 레코드들을 수신하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 30

제29항에 있어서,

네트워크 주소들의 상기 목록을 XML 명령어들로 인코딩하는 하나 이상의 DNS TXT 레코드들을 수신하는 동작은 전자 메시징 구성 정보가 XML 인스턴스에 연접될 수 있도록, 복수의 DNS TXT 레코드들에 걸친 전자 메시지 구성 정보를 수신하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 31

제30항에 있어서,

상기 전자 메시징 구성 정보가 XML 인스턴스에 연접될 수 있도록, 복수의 DNS TXT 레코드들에 걸친 전자 메시지 구성 정보를 수신하는 동작은 상기 DNS TXT 레코드들에 포함된 상기 XML 명령어들이 어떻게 정렬되는지를 지시하는 정렬 데이터를 포함하는 복수의 DNS TXT 레코드들을 수신하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 32

제31항에 있어서,

XML 인스턴스를 생성하기 위하여 상기 정렬 데이터에 따라 상기 XML 명령어들을 연접시키는 동작을 더 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 33

제20항에 있어서,

상기 실제 송신측 네트워크 주소가 상기 송신 도메인에 대하여 전자 메시지들을 전송하도록 인가되는지를 결정하는 동작은 상기 실제 송신측 네트워크 주소가 인가된 네트워크 주소들의 수신된 목록에 포함되어 있는지를 결정하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 34

제20항에 있어서,

상기 실제 송신측 네트워크 주소가 상기 송신 도메인에 대하여 전자 메시지들을 전송하도록 인가되는지를 결정하는 동작은 상기 실제 송신측 네트워크 주소가 인가된 네트워크 주소들의 수신된 목록에 포함되지 않는지를 결정하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 35

제20항에 있어서,

상기 결정의 결과들을 메시지 분류 모듈에 제공하는 동작은 상기 실제 송신측 네트워크 주소가 상기 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가된다는 것을 상기 메시지 분류 모듈에 지시하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 36

제20항에 있어서,

상기 결정의 결과들을 메시지 분류 모듈에 제공하는 동작은 상기 실제 송신측 네트워크 주소가 상기 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되지 않는다는 것을 상기 메시지 분류 모듈에 지시하는 동작을 포함하는, 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법.

청구항 37

하나 이상의 수신 컴퓨터 시스템들에 네트워크 접속 가능한 송신 컴퓨터 시스템에서 사용하기 위한 컴퓨터 판독 가능 기록 매체로서,

상기 송신 컴퓨터 시스템은 상기 수신 컴퓨터 시스템들에 전자 메시지들을 송신하도록 구성되고, 상기 컴퓨터 판독 가능 기록 매체는 상기 송신 컴퓨터 시스템에 의해 송신된 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법을 구현하기 위한 것이며, 프로세서에 의하여 실행될 때, 상기 송신 컴퓨터 시스템으로 하여금, 이하의 동작들을 수행하게 하는 컴퓨터 실행 가능 명령어들을 저장하고,

상기 동작들은

지정된 수신 컴퓨터 시스템으로 접속 초기화 데이터를 송신하는 동작 - 상기 접속 초기화 데이터는 상기 송신 컴퓨터 시스템의 송신 주소로 추정된(purported) 송신 주소를 포함함 -;

주소 검증 데이터와, 통상은 접속 설정에 포함되지 않는 비표준 데이터의 적어도 일부를 포함하는 변경된 접속 설정 데이터를 수신하는 동작 - 비표준 데이터의 일부가 포함됨으로써 비표준 데이터의 일부가 접속 응답에 제공될 것이라는 것을 알지 못하고서는 상기 변경된 접속 설정 데이터에 대응하는 접속 응답을 제공할 가능성을 감소시키며, 상기 비표준 데이터의 적어도 일부는 무작위 문자열(random string of characters)을 포함함 -;

접속 응답이 상기 주소 검증 데이터 및 비표준 데이터의 일부를 포함하였다는 것을 결정하는 것에 기초하여 상기 접속 응답이 상기 지정된 수신 컴퓨터 시스템으로부터 수신되었다는 것을 확인하는 동작;

상기 주소 검증 데이터 및 비표준 데이터의 일부에 기초하여 상기 변경된 접속 설정 데이터에 대응하는 접속 응답을 생성시키는 동작 - 상기 응답은 확인된 수신 컴퓨터 시스템에 의해 인식되는 형태의 비표준 데이터의 일부를 포함함 -; 및

상기 변경된 접속 설정 데이터에 대응하는 상기 접속 응답 데이터를 상기 수신 컴퓨터 시스템으로 송신하는 동작

을 포함하는, 컴퓨터 판독 가능 기록 매체.

청구항 38

제37항에 있어서,

프로세서에 의하여 실행될 때, 상기 송신 컴퓨터 시스템으로 하여금 주소 검증 데이터를 포함하는 변경된 접속 설정 데이터를 수신하도록 하는 컴퓨터 실행 가능 명령어들은, 프로세서에 의하여 실행될 때 상기 송신 컴퓨터 시스템으로 하여금 문자들의 무작위 시퀀스를 포함하는 SMTP HELO 명령 또는 SMTP EHLO 명령을 수신하도록 하는 컴퓨터 실행 가능 명령어들을 포함하는, 컴퓨터 판독 가능 기록 매체.

청구항 39

제37항에 있어서,

프로세서에 의하여 실행될 때, 상기 송신 컴퓨터 시스템으로 하여금 상기 변경된 접속 설정 데이터에 대응하는 상기 접속 응답 데이터를 상기 수신 컴퓨터 시스템에 송신하도록 하는 컴퓨터 실행 가능 명령어들은, 프로세서에 의하여 실행될 때 상기 송신 컴퓨터 시스템으로 하여금 상기 수신된 주소 검증 데이터에 포함된 문자들의 무작위 시퀀스를 포함하는 향상된 SMTP NOOP 명령을 송신하도록 하는 컴퓨터 실행 가능 명령어들을 포함하는, 컴퓨터 판독 가능 기록 매체.

청구항 40

하나 이상의 송신 컴퓨터 시스템들에 네트워크 접속 가능한 수신 컴퓨터 시스템에서 사용하기 위한 컴퓨터 판독 가능 기록 매체로서,

상기 수신 컴퓨터 시스템은 상기 송신 컴퓨터 시스템들로부터 전자 메시지들을 수신하도록 구성되고,

상기 컴퓨터 판독 가능 기록 매체는 상기 수신 컴퓨터 시스템이 송신 컴퓨터 시스템이 접속 설정 응답들을 수신하는지를 검출하는 방법을 구현하며, 프로세서에 의하여 실행될 때, 상기 수신 컴퓨터 시스템으로 하여금, 이하의 동작들을 수행하게 하는 컴퓨터 실행 가능 명령어들을 저장하고,

상기 동작들은

송신 컴퓨터 시스템으로부터 접속 초기화 데이터를 수신하는 동작 - 상기 접속 초기화 데이터는 상기 송신 컴퓨터 시스템의 송신 주소로 추정된 송신 주소를 포함함 -;

주소 검증 데이터와, 통상은 접속 설정에 포함되지 않는 비표준 데이터의 적어도 일부를 포함하도록 표준 접속 설정 데이터를 변경하는 동작 - 비표준 데이터의 일부가 포함됨으로써 비표준 데이터의 일부가 접속 응답에 제공될 것이라는 것을 알지 못하고서는 상기 변경된 접속 설정 데이터에 대응하는 접속 응답을 제공할 가능성을 감소시키며, 상기 비표준 데이터의 적어도 일부는 무작위 문자열(random string of characters)을 포함함 -; 및

변경된 상기 접속 설정 데이터를 상기 추정된 송신 주소로 송신하는 동작 - 상기 추정된 송신 주소를 지닌 송신 컴퓨터 시스템은 상기 접속 응답이 주소 검증 데이터 및 비표준 데이터의 일부를 포함하였다는 것을 결정함에 기초하여 상기 접속 응답이 상기 수신 컴퓨터 시스템으로부터 수신되었다는 것을 확인하도록 구성됨 -

을 포함하는, 컴퓨터 판독 가능 기록 매체.

청구항 41

제40항에 있어서,

프로세서에 의하여 실행될 때, 상기 수신 컴퓨터 시스템으로 하여금 주소 검증 데이터를 포함하도록 표준 접속 설정 데이터를 변경하도록 하는 컴퓨터 실행 가능 명령어들은, 프로세서에 의하여 실행될 때 상기 수신 컴퓨터 시스템으로 하여금 SMTP HELO 응답 명령 또는 SMTP EHLO 응답 명령 내에 문자들의 무작위 시퀀스를 포함하도록 하는 컴퓨터 실행 가능 명령어들을 포함하는, 컴퓨터 판독 가능 기록 매체.

청구항 42

하나 이상의 송신 도메인들에 네트워크 접속 가능한 수신 도메인에서 사용하기 위한 컴퓨터 판독 가능 기록 매체로서,

상기 수신 도메인은 송신 도메인들로부터 전자 메시지들을 수신하도록 구성된 하나 이상의 수신 메시징 서버들을 포함하고,

상기 컴퓨터 판독 가능 기록 매체는 송신 메시징 서버가 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 방법을 구현하며, 프로세서에 의하여 실행될 때, 상기 수신 도메인으로 하여금, 이하의 동작들을 수행하게 하는 컴퓨터 실행 가능 명령어들을 저장하고,

상기 동작들은

상기 송신 도메인으로부터 송신된 것으로 추정되는 전자 메시지를 수신하는 동작 - 상기 전자 메시지는 통상은 접속 설정에 포함되지 않는 비표준 데이터의 적어도 일부를 포함하여, 비표준 데이터의 일부가 포함됨으로써 비표준 데이터의 일부가 접속 응답에 제공될 것이라는 것을 알지 못하고서는 상기 비표준 데이터의 적어도 일부를 포함하는 변경된 접속 설정 데이터에 대응하는 접속 응답을 제공할 가능성을 감소시키며, 상기 비표준 데이터의 적어도 일부는 무작위 문자열(random string of characters)을 포함함 -;

비표준 데이터의 일부를 포함하는 상기 전자 메시지의 복수의 파라미터 값들을 검사하여, 상기 접속 응답이 주소 검증 데이터 및 비표준 데이터의 일부를 포함하였다는 결정에 기초하여 상기 접속 응답이 지정된 수신 도메인으로부터 수신되었다는 것을 확인하도록 시도하는 동작;

상기 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가된 네트워크 주소들의 목록에 대하여 네임 서버에 문의하는 동작;

확인된 수신 도메인에 의해 인식되는 형태의 비표준 데이터의 일부의 포함 및 상기 문의에 기초하여, 실제 송신측 네트워크 주소가 상기 송신 도메인에 대하여 전자 메시지들을 송신하도록 인가되는지를 결정하는 동작; 및

메시지 분류 모듈이 상기 수신된 전자 메시지를 분류하는 것에 관하여 보다 신뢰성 있는 결정을 할 수 있도록, 상기 결정의 결과들을 상기 메시지 분류 모듈에 제공하는 동작

을 포함하는, 컴퓨터 판독 가능 기록 매체.

청구항 43

제42항에 있어서,

프로세서에 의하여 실행될 때, 상기 수신 도메인으로 하여금 실제 송신측 네트워크 주소를 식별하는 시도로 상기 전자 메시지의 복수의 파라미터 값들을 조사하도록 하는 컴퓨터 실행 가능 명령어들은, 프로세서에 의하여 실행될 때 상기 수신 도메인으로 하여금 복수의 파라미터 값들을 조사하도록 하고, 상기 복수의 파라미터 값들 중 적어도 하나는 제1 Resent-Sender 헤더 값, Resent-From 헤더의 제1 메일박스 값, Sender 헤더 값, 또는 From 헤더의 제1 메일박스 값으로부터 선택되는 컴퓨터 실행 가능 명령어들을 포함하는, 컴퓨터 판독 가능 기록 매체.

청구항 44

제1항에 있어서,

상기 송신 컴퓨터 시스템은 DNS 레코드 세트에 비표준 접속 설정 데이터의 교환을 위한 지원을 나타내는 레코드들을 포함하며, 상기 DNS 레코드 세트는 상기 송신 컴퓨터 시스템의 도메인에 대한 전자 메일 정책를 나타내는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 45

제1항에 있어서,

상기 비표준 데이터의 일부는 문자들의 무작위 시퀀스를 포함하는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 46

제1항에 있어서,

상기 비표준 데이터의 일부는 재생성된 접속 초기화 데이터를 포함하는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 47

제1항에 있어서,

상기 비표준 데이터의 일부는 상기 변경된 접속 설정 데이터에 대응하는 승인 시퀀스 번호를 포함하는, 송신 컴퓨터 시스템에 의해 송신되는 접속 초기화에 대한 응답들이 지정된 수신 컴퓨터 시스템으로부터 기인하는 것을 확인하기 위한 방법.

청구항 48

삭제

명 세 서

기 술 분 야

[0001] [관련 출원]

[0002] 본 출원은 2003년 3월 12일에 출원된 미국 가출원 제60/454,517호 "Coordinated Reduction of Unwanted And Unsolicited Electronic Mail Messages"를 우선권으로 주장한다.

[0003] 본 발명은 전자 메일 기술에 관한 것으로, 특히 불필요하고 요구되지 않은 전자 메시지(unwanted and

unsolicited electronic messages)를 감소시키는 것에 관한 것이다.

배 경 기 술

[0004] 컴퓨터 시스템 및 관련 기술은 사회의 많은 면에 영향을 미친다. 실제로, 정보를 처리하는 컴퓨터의 능력으로 인하여, 사람들이 생활하고 일하는 방법이 변하여 왔다. 오늘날에, 컴퓨터 시스템은 자신의 출현 전에는 수동으로 수행되었던 다수의 작업(예를 들면, 워드 프로세싱, 스케줄링 및 데이터베이스 관리)을 흔히 수행한다. 최근에, 컴퓨터 시스템은 서로 연결되어, 데이터를 공유하기 위하여 전자적으로 통신할 수 있는 유선 및 무선 컴퓨터 네트워크를 형성한다. 결과적으로, 컴퓨터 시스템에서 수행되는 다수의 작업(예를 들면, 음성 통신, 전자 메일 액세스, 전자 회의, 웹 브라우징)은 유선 및/또는 무선 컴퓨터 네트워크를 통하여 하나 이상의 다른 컴퓨터 시스템과의 전자 통신을 포함한다.

[0005] 전자 메일이 있는 한, 불필요하고 요구되지 않은 이메일(흔히, "SPAM"이라 함)이 사실상 존재한다. 역사적으로, 스팸으로 인한 성가심과 부하는 (눈에 띄기는 했지만) 충분히 작아서 큰 문제가 아니었다. 하지만, 최근에 SPAM이 사용자의 전자 메일박스에 출현하는 빈도가 크게 증가하였다. 대형의 상업적 전자 메일 박스 제공자가, 그들의 사용자에 의하여 수신된 전자 메일의 절반, 심지어는 3/4 이상이 SPAM이라는 점을 정기적으로 보고하는 것은 보기 드문 일이 아니다. 이 문제는 사용자, 기업 및 경제에 상당한 시간 및 재정 자원의 낭비가 되는 중요한 부분 중 하나가 되었고, 심지어는 유용한 통신 매개체로서의 전자 메일의 이용 가능성을 위협적으로 손상시킨다.

[0006] 종래에, 전자 메일 클라이언트 소프트웨어 및 전자 메일 서버 소프트웨어 디자인은 사용자가 전자 메일을 취급하는 것을 가능하면 효율적이고 유용하며 즐겁도록 하는 것에 중점을 두었다. 이러한 소프트웨어는 사용자가 주어진 전자 메일 메시지에 대해 가질 수 있는 실제적인 관심에 대한 이해 없이 제공되었다. 그러므로, 모든 수신된 전자 메일 메시지는 전자 메일 메시지의 내용에 상관없이 동등하게 다루어지고 사용자에게 제시되는 경향이 있었다. 불행히도, 이러한 전자 메일 메시지 처리로 인하여, SPAM이 정당한 전자 메일 메시지(예를 들면, 아는 송신자로부터의 전자 메시지, 사용자로부터 송신된 전자 메시지에 대한 응답 등)와 실질적으로 구별될 수 없게 되었다.

[0007] 따라서, 전자 메일 메시지를 SPAM으로 분류하여 SPAM과 다른 정당한 전자 메일 메시지를 구별하는 다수의 기술이 개발되어 왔다. 일부 기술은 수신된 전자 메일 메시지를 조사하고, 그 메시지에서 발견된 단어 또는 문구를 기초로 하여 수신된 전자 메일 메시지를 SPAM으로 분류한다. SPAM을 분류하는 다른 기술은, SPAM인 전자 메일 메시지는 일반적으로 매우 많은 수의 사용자에게 송신된다는 사실을 이용한다. 이 다른 기술은 전자 메일 메시지를 SPAM으로 식별하기 위하여 집합적 투표 접근법(collective voting approach)을 사용한다. 흔히 사용되고 유용한 또 다른 기술은 사용자를 대신하여 사용자가 아는 상대방의 목록을 유지하는 것으로, 흔히 "알려진 송신자 목록" 또는 "허용 목록(white list)"라고 하는 접근법이라 한다.

[0008] SPAM으로 분류한 후에, SPAM 전자 메일 메시지는, 예를 들면 자동으로 SPAM 전자 메일 메시지를 사용자의 "SPAM 폴더"로 이동시키거나 심지어는 SPAM 전자 메일이 송신되었다는 것을 사용자가 모른 채 그 메시지를 삭제함으로써, 정당한 전자 메일 메시지와는 다르게 취급될 수 있다.

[0009] 그러나, 다수의 종래 전자 메일 분류 기술은, 전자 메일 메시지가 정당한지 또는 SPAM인지를 결정할 때 전자 메일 메시지의 내용(예를 들면, 전자 메일 메시지의 헤더 및 바디)에만 의존한다. 이러한 기술은 문제점이 있는데, 이는 SPAM을 송신하려는 엔티티(entity)는, SPAM 전자 메일 메시지가 정당한 전자 메일 메시지로서 보이게 그 메시지를 고의로 (흔히 매우 용이하게) 변경할 수 있기 때문이다. 예를 들면, SPAM을 송신하려는 엔티티는, 전자 메일 필터에 의한 검출 가능성이 감소되도록 전자 메일 메시지의 바디를 구성할 수 있다. 더욱이, SPAM을 송신하려는 엔티티는 전자 메일 메시지의 헤더 부분의 특정 주소 지정 정보(addressing information)를 변경할 수 있는데, 이것을 흔히 "도메인 위장(domain spoofing)"이라 한다.

[0010] 도메인 네임을 위장하는 것은 송신자의 전자 메일 주소의 도메인 네임(즉, 전자 메일 주소에서 "@" 후의 텍스트)을 변경시켜서, 사실은 전자 메일 메시지를 송신하지 않은 특정 엔티티로부터 전자 메일 메시지가 송신된 것처럼 보이게 하는 것을 포함한다. 그러므로, 전자 메일 분류 기술은, 사실은 전자 메일 메시지가 SPAM으로 분류되어야 하는 때에도 위장된 도메인 네임에 기초하여 정당하다고 잘못 분류할 수 있다. 따라서, 종래의 메일 분류 기술의 효율은 감소한다.

[0011] 일반적으로, 전자 메일 메시지가 송신 메일 서버로부터 수신 메일 서버로 전달되기 전에, 예를 들면 전송 제어 프로토콜(TCP) 접속과 같은 접속이 송신 메일 서버와 수신 메일 서버 간에 설정된다. 접속 설정은 네트워크 주

소, 포트 번호 및 시퀀스 번호(sequence number)를 포함하는 구성 정보(configuration information)의 교환을 포함할 수 있다. 예를 들면, TCP 접속 설정은 공지의 세 방향 핸드쉐이크 시퀀스(three-way handshake sequence)를 포함한다. 불행히도 TCP 세 방향 핸드쉐이크 시퀀스는 공지이기 때문에, SPAM을 송신하고자 하는 엔티티는 네트워크 주소를 위조하여, 위조된 네트워크 주소로부터 발생한 것으로 추정되는 구성 정보(예를 들면, 시퀀스 번호)를 송신할 수 있다. 수신 메일 서버는, 구성 정보가 위조된 네트워크 주소로부터 발생하였다고 부정확하게 결정할 수 있다.

[0012] 그러므로, 엔티티는 네트워크 주소를 위조하여, 위조된 네트워크 주소로부터 발생한 것처럼 수신 메일 서버에 보이게 접속을 설정할 수 있다. 따라서, 엔티티는 그 후 설정된 접속을 사용하여 위조된 네트워크 주소로부터 발생된 것처럼 보이는 전자 메일 메시지를 송신할 수 있다. 엔티티가 위조된 네트워크 주소의 도메인 네임도 위장하면, 전자 메일 메시지가 실제로 발생한 네트워크 주소를 결정하는 것은 불가능하지는 않을 지라도 어려울 것이다. 위조된 네트워크 주소 및 위장된 도메인 네임에 기초하여, 수신 메일 서버는 전자 메일 메시지를 정당하다고 부정확하게 분류할 수 있다. 따라서, 불필요하고 요구되지 않은 전자 메시지를 함께 감소시키는 메커니즘이 유용하다.

발명의 내용

해결하려는 과제

[0013] 당해 기술의 이전의 수준(prior state of the art)에 있어서의 상술한 문제점들은 본 발명의 원리에 의하여 극복되는데, 본 발명의 원리는 불필요하고 요구되지 않은 전자 메시지를 감소시키는 방법, 시스템, 컴퓨터 프로그램 제품 및 데이터 구조를 목적으로 한다. 요구되는 기능에 따라, 복수의 상이하게 생성된 입력 중 하나 이상은 잠재적으로 전자 메시지에 포함된 메시지 데이터와 함께, 메시지 분류 모듈(message classification module)에 제공될 수 있다. 수신된 입력에 기초하여, 메시지 분류 모듈은 전자 메시지를 정당한 또는 불필요하고/하거나 요청되지 않은 것으로 분류할 수 있다. 복수의 입력(각각의 입력은 전자 메시지의 전송과 연관된 상이한 정보를 표시함)이 이용되면, 메시지 분류 모듈은, 예를 들면 전자 메시지를 불필요하고/하거나 요청되지 않은 것으로 보다 신뢰성 있게 분류하는 것과 같이, 전자 메시지를 보다 신뢰성 있게 분류할 수 있다.

과제의 해결 수단

[0014] 일 실시예에서, 접속 설정 데이터의 표준화된 교환(standardized exchange)은 엔티티가 위조된 네트워크 주소(예를 들면, 위조된 인터넷 프로토콜(Internet Protocol; IP) 주소)로부터 전자 메시지를 송신하는 가능성을 감소시키도록 변경된다. 송신측 컴퓨터 시스템은 추정된 송신 네트워크 주소를 포함하는 접속 초기화 데이터(예를 들면, 포트, 시퀀스 번호 등)를 송신한다. 수신측 컴퓨터 시스템은 추정된 송신 주소를 포함하는 접속 초기화 데이터를 수신한다. 수신측 컴퓨터 시스템은 주소 검증 데이터(address validation data)를 포함하도록 표준 접속 설정 데이터를 변경한다. 수신 컴퓨터는 변경된 접속 설정 데이터를 추정된 송신 네트워크 주소로 송신한다.

[0015] 추정된 송신 네트워크 주소가 송신 컴퓨터 시스템에 해당하면, 송신 컴퓨터 시스템은 주소 검증 데이터를 포함하는 변경된 접속 설정 데이터를 수신할 수 있다. 따라서, 송신측 컴퓨터 시스템은 주소 검증 데이터에 기초하여 적절한 접속 응답 데이터를 생성할 수 있다. 한편, 추정된 송신 네트워크 주소가 송신 컴퓨터 시스템에 해당하지 않으면 (예를 들면, 네트워크 주소가 위조되면), 송신 컴퓨터 시스템은 주소 검증 데이터를 포함하는 변경된 접속 설정 데이터를 수신하지 않는다.

[0016] 송신측 컴퓨터 시스템은 (예를 들면, 추정된 송신 주소에 해당하지 않는 컴퓨터 시스템으로부터의 표준 접속 응답 데이터를 모의하기 위한 시도로서) 표준 접속 응답 데이터를 수신 컴퓨터 시스템에 송신할 수 있다. 하지만, 송신측 컴퓨터 시스템은 주소 검증 데이터를 인식하고 있지 않기 때문에, 송신 컴퓨터 시스템은 주소 검증 데이터에 적절하게 응답할 수 없다. 수신측 컴퓨터 시스템은, 추정된 송신 네트워크 주소에 해당하는 컴퓨터 시스템이 주소 검증 데이터에 적절하게 응답하였는지를 결정한다.

[0017] 다른 실시예에서, 도메인(예를 들면, "test.com")에 대한 네임 서비스(예를 들면, 도메인 네임 서비스) 엔트리는 도메인에 대한 발신 메시지(outgoing message)를 취급하도록 인가된 컴퓨터 시스템의 네트워크 주소를 포함하도록 구성된다. 즉, 네임 서버 엔트리는 도메인에 대하여 전자 메시지를 송신하도록 인가된 컴퓨터 시스템의 네트워크 주소로 구성된다. 수신 메시지 서버는 송신측 도메인으로부터 송신되었다고 추정되는 전자 메시지를 수신한다. 수신 메시징 서버는 전자 메시지를 송신한 송신 메시징 서로에 해당하는 실제 송신측 네트워크 주소

를 (예를 들면, 접속 설정 데이터로부터) 식별한다.

[0018] 수신 메시징 서버는 송신 도메인에 대하여 전자 메시지를 송신하도록 인가된 네트워크 주소의 목록을 네임 서버에 문의한다. 수신 메시징 서버는, 실제 송신측 네트워크 주소가 인가된 네트워크 주소의 목록에 포함되어 있는지를 결정한다. 수신 메시징 서버는 결정의 결과(즉, 송신 컴퓨터 시스템이 도메인에 대하여 전자 메시지를 송신하도록 인가되었는지 또는 인가되지 않았는지 여부)를 메시지 분류 모듈에 제공한다.

[0019] 또 다른 실시예에서, 전자 메시지 전송 정책(Electronic Message Transmission Policies; ETPs)은 도메인에 대한 네임 서비스 엔트리에 포함되거나 수신된 전자 메시지에 포함된다. ETP 인증서(certificate)는 송신 도메인에 의하여 ETP가 준수되었다는 것을 수신 컴퓨터 시스템에 지시하기 위하여 사용될 수 있다. 수신 메시징 서버는 송신 도메인으로부터 전자 메시지를 수신한다. 수신 메시징 서버는 송신 도메인에 해당하는 하나 이상의 ETP(예를 들면, ETP 인증서에 포함됨)를 수신한다. 수신 메시지 서버는, 예를 들면 네임 서버에 문의하거나 수신된 전자 메시지로부터 ETP를 추출함으로써 ETP를 수신할 수 있다.

[0020] 수신 메시징 서버는 관련 ETP를 구문 분석(parse)한다. 관련 ETP는 송신 도메인에 의하여 준수되는 ETP를 지시한다. 수신 메시징 서버는 관련 ETP를 메시지 분류 모듈에 제공한다.

[0021] 또 다른 실시예에서, 송신 컴퓨터 시스템은, 전자 메시지를 송신하기 전에 컴퓨터 리소스(computational resource)이 소비되었는지를 수신 컴퓨터 시스템에 증명한다. 소비된 컴퓨터 리소스는, 송신 컴퓨터 시스템이 연산 퍼즐(computational puzzle)에 적절한 해답(solution)을 제공하면, 수신 컴퓨터 시스템에 의하여 적어도 추정될 수 있다. 연산 퍼즐은, 송신 컴퓨터 시스템이 적절한 해답(예를 들면, 폭력 접근법(brute force approach))을 사용하여 식별된 해답을 생성하기 위하여 증가된 컴퓨터 리소스를 소비하는 것을 요구되도록 구성될 수 있다. 그러나, 상당히 감소된 컴퓨터 리소스가 적절한 해답을 확인하기 위하여 수신 컴퓨터 시스템에서 소비된다. 확인 가능한 해답의 연산(computation)은 전자 메시지를 전자 메시지 수신자에게 송신하는 티켓(ticket)을 (소비된 프로세서 사이클을 통하여) 전자 메시지 송신자가 구입하게 한다. 이러한 연산 퍼즐은 응답 문서(answer document)의 폭력 연산(brute force calculation)을 구현한다.

[0022] 송신 메시징 서버는 전자 메시지에 포함될 전자 메시지 데이터를 수신한다. 송신 메시징 서버는, 예를 들면 전자 메시지 데이터 및/또는 다른 상태 정보(state information)의 상이한 부분으로부터의 초기 문서(initial document)를 생성한다. 퍼즐 입력은 전자 메시지의 하나 이상의 구성 요소로부터 생성된다. 퍼즐 입력은 불필요하고/하거나 요청하지 않은 전자 메시지를 억제하는데 사용하기 위하여 특히 설계된 퍼즐 해시 알고리즘(puzzle hash algorithm)에 제공된다. 예를 들면, 퍼즐 해시 알고리즘은 SHA-1 알고리즘의 서브 함수를 해싱(hashing)하는 것을 이용할 수 있지만, SHA-1 알고리즘과 다른 순서로 서브 함수를 적용한다. 서브 함수를 다른 순서로 적용하면, 퍼즐 해시 알고리즘을 하드웨어로 구현하기에 더 어렵게 되고, 해시 알고리즘의 하드웨어 가속(hardware acceleration)이 정당한 필요로 소망되는 문제 공간(problem space)으로부터 그것의 사용을 구별한다.

[0023] 몇몇 실시예에서, 퍼즐 입력은 초기 문서이다. 다른 실시예에서, 퍼즐 입력은 초기 문서 및 다른 메일 메시지 데이터로부터 연산된다.

[0024] 송신 메시징 서버는, 응답 문서 및 퍼즐 입력(초기 문서 또는 퍼즐 입력 해시 값)의 결합(combination)으로부터 (퍼즐 해시 알고리즘을 사용하여) 연산된 응답 해시 값이 연산 퍼즐에 대한 응답 값이 되도록 응답 문서를 식별한다. 예를 들면, 응답 문서는 특정 수의 선행 0들(a specified number of leading zeros)을 가지는 응답 해시 값을 연산하기 위하여 사용될 수 있다. 서버에서의 송신 메시지는 응답 문서 및 메시지 데이터를 포함하는 전자 메시지를 수신 도메인에 송신한다.

[0025] 수신 도메인에서의 수신 컴퓨터 시스템은 전자 메시지를 수신한다. 수신 컴퓨터 시스템은, 예를 들면 송신 컴퓨터 시스템에서 사용된 메시지 데이터 및/또는 다른 상태 정보의 상이한 부분으로부터 초기 문서를 재생성한다. 수신 컴퓨터 시스템은 (잠재적으로 퍼즐 입력 해시 값을 연산하기 위하여 퍼즐 해시 알고리즘을 사용하여) 초기 문서로부터 퍼즐 입력을 재연산한다. 수신 컴퓨터 시스템은 (퍼즐 해시 알고리즘을 사용하여) 응답 문서 및 퍼즐 입력(초기 문서 또는 퍼즐 입력 해시 값)의 결합으로부터 연산된 확인 해시 값이 연산 퍼즐에 대한 해답을 지시하는 응답인지를 결정한다(예를 들면, 확인 해시 값이 특정 수의 선행 0들을 가지고 있는지를 결정한다). 수신 컴퓨터 시스템은 결정의 결과(예를 들면, 송신 메시징 서버가 확인 가능하거나 확인 가능하지 않은 해답을 제공했는지 또는 전혀 해답을 제공하지 않았는지 여부)를 메시지 분류 모듈에 제공한다.

[0026] 본 발명의 추가적인 특징 및 이점은 후술되는 상세한 설명에서 개시되고, 부분적으로 하기의 설명으로부터 자명

할 것이며, 또한 본 발명의 실시에 의하여 지득될 수 있다. 본 발명의 특징 및 다른 이점은 첨부된 청구항에 특히 개시된 장치 수단 및 결합에 의하여 실현되고 획득될 수 있다. 본 발명의 이들 및 다른 특징은 다음의 설명, 첨부된 청구항으로부터 더 명백해질 것이고, 또는 다음에 개시된 본 발명의 실시에 의하여 지득될 수 있다.

[0027] 본 발명의 원리는 불필요하고 요청되지 않은 전자 메시지를 함께 감소시키는 방법, 시스템, 컴퓨터 프로그램 제품 및 데이터 구조를 목적으로 한다. 접속 설정 데이터의 교환은, 엔티티가 위조된 네트워크 주소를 포함하는 전자 메시지를 송신하는 위험성을 감소시키고, 잠재적으로 억제시키기 위하여 변경된다. 수신 메시징 서버는 도메인에 대하여 전자 메시지를 송신하도록 인가된 서버를 식별하기 위하여 인가된 발신 서버 목록을 조사한다. 수신 메시징 서버는 도메인에 대하여 전자 메시지 전송 정책을 식별한다. 송신 메시징 서버는 연산 퍼즐에 대한 응답을 연산하고, 수신 메시징 서버는 그 응답을 확인한다. 발신 서버 목록 조사의 결과, 식별된 전자 메시지 전송 정책 및 퍼즐 응답 확인은 다른 입력과 함께 전자 메시지 분류 모듈에 제공될 수 있다.

[0028] 본 발명의 범위 내의 실시예는 컴퓨터 실행 가능 명령어 또는 데이터 구조를 수반하거나 가지는 컴퓨터 판독 가능 매체를 포함한다. 이러한 컴퓨터 판독 가능 매체는 범용 또는 특정 목적의 컴퓨터 시스템에 의하여 액세스 가능한 임의의 이용 가능한 매체일 수 있다. 예로서, 이러한 컴퓨터 판독 가능 매체는 RAM, ROM, EPROM, CD-ROM 또는 다른 광 디스크 저장 장치, 자기 디스크 저장 장치 또는 다른 자기 저장 장치, 또는 임의의 다른 매체와 같은 물리적 저장 매체를 포함하지만, 이에 제한되지 않으며, 임의의 다른 매체가 컴퓨터 실행 가능 명령어, 컴퓨터 판독 가능 명령어, 또는 데이터 구조의 형태로 소망하는 프로그램 코드 수단을 수반하거나 저장하기 위하여 사용될 수 있고, 범용 또는 특정 목적의 컴퓨터 시스템에 의하여 액세스될 수 있다.

[0029] 정보가 컴퓨터 시스템에 네트워크 또는 다른 통신 접속(유선(hardwired), 무선, 또는 유선 또는 무선의 조합)상으로 전달되면, 접속은 컴퓨터 판독 가능 매체라고 적절히 간주된다. 그러므로, 임의의 이러한 접속은 적절히 컴퓨터 판독 가능 매체라고 한다. 또한, 상기 매체의 조합은 컴퓨터 판독 가능 매체의 범위 내에 포함되어야 한다. 컴퓨터 실행 가능 또는 컴퓨터 판독 가능 명령어는, 예를 들면 범용 컴퓨터 시스템 또는 특정 목적의 컴퓨터 시스템이 특정 기능 또는 기능의 그룹을 수행하도록 하는 데이터 및 명령어를 포함한다. 컴퓨터 실행 가능 또는 컴퓨터 판독 가능 명령어는, 예를 들면 어셈블리 언어 또는 심지어는 소스 코드와 같은 이진(binaries), 중간 형태의 명령어(intermediate format instructions)일 수 있다.

[0030] 본 명세서 및 첨부된 청구항에서, "컴퓨터 시스템"은 전자 데이터 상에 작업을 수행하기 위하여 함께 동작하는 하나 이상의 소프트웨어 모듈, 하나 이상의 하드웨어 모듈 또는 이들의 조합으로서 정의된다. 예를 들면, 컴퓨터 시스템의 정의에는 퍼스널 컴퓨터의 운영 체제와 같은, 소프트웨어 모듈뿐만 아니라 퍼스널 컴퓨터의 하드웨어 모듈을 포함된다. 컴퓨터 시스템은 네트워크를 통하여 연결된 하나 이상의 컴퓨터를 포함할 수 있다. 유사하게, 컴퓨터 시스템은, (프로세서 및 메모리와 같은) 내부 모듈이 전자 데이터 상에 작업을 수행하기 위하여 함께 동작하는 (이동 전화 또는 개인 휴대 정보 단말기(Personal Digital Assistant; PDA)와 같은) 단일 물리적 장치를 포함할 수 있다.

[0031] 당업자는, 본 발명이 허브, 라우터, 무선 액세스 포인트(access point; AP), 무선국(wireless station), 퍼스널 컴퓨터, 랩탑 컴퓨터, 핸드헬드 장치(hand-held device), 멀티프로세서 시스템, 마이크로프로세서 기반 또는 프로그래머블 가전 제품(programmable consumer electronics), 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터, 이동 전화, PDA, 호출기 등을 포함하는 다수의 유형의 컴퓨터 시스템 구성을 가지는 네트워크 컴퓨팅 환경에서 실시될 수 있다. 또한, 본 발명은 네트워크를 통하여 (유선, 무선, 또는 유선 및 무선 접속의 조합에 의해) 링크된 로컬 및 원격 컴퓨터 시스템이 작업을 수행하는 분산 시스템 환경에서 실시될 수 있다. 분산 시스템 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치에 위치될 수 있다.

[0032] 도 1은 본 발명의 원리에 따라 접속 도용의 감소를 용이하게 하는 네트워크 아키텍처(100)의 예를 도시한다. 네트워크 아키텍처(100)에서, 송신 메시징 서버(107), 수신 메시징 서버(109) 및 메시징 서버(184)는 각각 해당 링크(102, 104 및 103)에 의하여 네트워크(101)에 접속된다. 유사하게, 네임 서버(108)는 링크(106)에 의하여 네트워크(101)에 접속된다. 네트워크(101) 뿐만 아니라 링크(102, 103, 104 및 106)는 시스템 버스의 일부, 근거리 통신망(local area network; LAN)의 일부, 원거리 통신망(Wide Area Network; WAN)의 일부 및/또는 심지어는 인터넷의 일부를 포함할 수 있다. 양방향 화살표(186)에 의하여 도시된 바와 같이, 네임 서버(108)는 재귀적 문의(recursive query)의 목적으로 다른 네임 서버(185)와 통신을 할 수도 있다. 유사하게, 네트워크 아키텍처(100)의 컴퓨터 시스템은 (네트워크 아키텍처(100)의 컴퓨터 시스템을 다른 네임 서버(185)에 접속하는 링크가 명시적으로 도시되어 있지 않지만) 반복적인 문의의 목적으로 다른 네임 서버(185)에 바로 문의할 수 있다.

[0033] 메시징 클라이언트(132 및 133)는 각각 해당 링크(136 및 137)에 의하여 수신 메시징 서버(109)에 접속된다. 메시징 엔티티(예를 들면, 사용자 또는 기업)는 메시징 클라이언트(132 및 133)를 사용하여 수신 메시징 서버(109)에 저장된 전자 메시지를 액세스할 수 있다.

[0034] 송신 메시징 서버(107), 수신 메시징 서버(109) 및 메시징 서버(184)는 다른 컴퓨터 시스템 뿐만 아니라 또 다른 컴퓨터 시스템 간에 접속을 설정하기 위하여 TCP를 이용하는 전자 메시징 서버일 수 있다. 또한, 송신 메시징 서버(107), 수신 메시징 서버(109) 및 메시징 서버(108)는 SMTP(Simple Mail Transfer Protocol)를 이용하여 (예를 들면, 설정된 TCP 접속 상으로) 다른 메시징 서버 및 다른 컴퓨터 시스템과 전자 메일 메시지를 교환할 수 있다. 네임 서버(108)는 도메인 네임(예를 들면, www.test.com)을 IP 주소(예를 들면, 112.45.123.99)로 변환하는 도메인 네임 시스템(Domain Name System; DNS) 서버일 수 있다.

[0035] 네임 서버(108)는, 예를 들면 향상된 NOOP 명령에 대한 지원 또는 다른 SMTP 확장 명령에 대한 지원과 같은 비표준 접속 설정 데이터의 교환을 도메인이 지원한다는 것을 지시하는 하나 이상의 레코드를 저장할 수 있다. 비표준 접속 설정 데이터의 교환에 대한 지원을 지시하는 레코드는, 예를 들면 특수한 NOOP 레코드, TXT 레코드 또는 TXT 레코드의 세트(set)와 같은 DNS 레코드일 수 있다. TXT 레코드 또는 TXT 레코드의 세트는, 예를 들면 XML(eXtensible Markup Language) 명령어와 같이 텍스트 형태로 인코딩된 텍스트 데이터 또는 다른 데이터를 포함할 수 있다. 비표준 접속 설정 데이터의 교환에 대한 지원을 지시하는 레코드는 도메인에 대한 전자 메일 정책을 지시하는 DNS 레코드 세트에 포함될 수 있다.

[0036] 도 2는 본 발명의 원리에 따라 접속 도용을 감소시키는 방법(200)의 예시적인 흐름도를 도시한다. 본 방법(200)은 네트워크 아키텍처(100)에서 도시된 구성 요소에 대하여 개시된다. 본 방법(200)은 추정된 송신 주소를 포함하는 접속 초기화 데이터를 수신 컴퓨터 시스템에 송신하는 동작(동작 "201")을 포함한다. 동작 "201"은 수신 컴퓨터 시스템에 접속 초기화 데이터를 송신하는 송신 컴퓨터 시스템을 포함할 수 있다. 접속 초기화 데이터는, 예를 들면 송신 메시징 서버와 다른 컴퓨터 시스템 간에 TCP 또는 SMTP 접속과 같은 접속의 설정을 초기화하는 데이터일 수 있다. 따라서, 접속 초기화 데이터는 시퀀스 번호, 포트 번호 또는 접속 설정을 초기화하는 다른 적절한 명령을 포함할 수도 있다.

[0037] 예를 들면, 송신 메시징 서버(107)는 주소(112)를 포함하는 접속 초기화 데이터(111)를 수신 메시징 서버(109)에 송신할 수 있다. 송신 메시징 서버(107)는 메시징 서버(184)에 해당하는 네트워크 주소(예를 들면, IP 주소)를 도용하려는 시도를 하고 있을 수 있다. 그러므로, 주소(112)는 메시징 서버(184)에 해당하는 네트워크 주소일 수 있다. 한편, 송신 메시징 서버는 네트워크 주소를 도용하려는 시도를 하지 않고 있을 수 있고, 주소(112)는 송신 메시징 서버(107)에 해당하는 네트워크 주소일 수 있다. 접속 초기화 데이터(111)는, 예를 들면 송신 메시징 서버(107)로부터 송신된 SMTP HELO 명령 또는 SMTP EHLO 명령에 포함될 수 있다.

[0038] 본 방법(200)은 추정된 송신 주소를 포함하는 접속 초기화 데이터를 송신 컴퓨터 시스템으로부터 수신하는 동작(동작 "205")을 포함한다. 동작(205)은 송신 컴퓨터 시스템으로부터 접속 초기화 데이터를 수신하는 수신 컴퓨터 시스템을 포함한다. 수신된 접속 초기화 데이터는, 예를 들면 수신 메시징 서버와 다른 컴퓨터 시스템간에 TCP 또는 SMTP 접속과 같은 접속의 설정을 초기화하는 데이터일 수 있다. 예를 들면, 수신 메시징 서버(109)는 주소(112)를 포함하는 접속 초기화 데이터(111)를 송신 메시징 서버(107)로부터 수신할 수 있다. 접속 초기화 데이터(111)는 수신 메시징 서버(109)에서 수신된 SMTP HELO 명령에 포함될 수 있다.

[0039] 본 방법(200)은 주소 검증 데이터를 포함하도록 표준 접속 설정 데이터를 변경하는 동작(동작 "206")을 포함한다. 동작 "206"은 주소 검증 데이터를 포함하도록 표준 접속 설정 데이터를 변경하는 수신 컴퓨터 시스템을 포함할 수 있다. 예를 들면, 수신 메시징 서버(108)는 접속 초기화 데이터(111)를 수신하는 것에 응답하여 주소(112)로 달리 송신될 표준 접속 설정 데이터를 변경할 수 있다. TCP 접속이 설정될 것이라고 접속 초기화 데이터(111)가 지시하면, 수신 메시징 서버(109)는 표준 접속 응답 데이터를 복수의 네트워크 패킷으로 분리할 수 있다. 선택적으로, TCP 접속이 설정될 것이라고 접속 초기화 데이터(111)가 지시하면, 수신 메시징 서버(109)는 접속 초기화 데이터(111)를 버릴 수 있다. 몇몇 실시예에서, 접속 설정 데이터(111)를 수신하는 것에 응답하여, 수신 메시징 서버(109)는 표준 접속 설정 데이터를 변경하여 무작위 문자열(random string of characters)(또는 비표준 데이터의 다른 일부)을 포함할 수 있다.

[0040] 본 방법(200)은 변경된 접속 설정 데이터를 추정된 송신 주소로 송신하는 동작(동작 "207")을 포함한다. 동작 "207"은 변경된 접속 설정 데이터를 추정된 송신 주소로 송신하는 수신 컴퓨터 시스템을 포함할 수 있다. 예를 들어, 주소(112)가 송신 메시징 서버(107)에 해당하면, 수신 메시징 서버(109)는 주소 검증 데이터(114)를 포함하는 변경된 접속 설정 데이터(113)를 송신 메시징 서버(107)에 송신할 수 있다. 한편, 주소(112)가 메시징 서

버(184)에 해당하면, 수신 메시징 서버(109)는 주소 검증 데이터(114)를 포함하는 변경된 접속 설정 데이터(118)를 메시징 서버(184)에 송신할 수 있다.

[0041] 변경된 접속 설정 데이터(113 및 118)는 접속 설정 데이터, 접속 초기화 데이터를 재전송하기 위한 요구, 또는 무작위 문자열(또는 비표준 데이터의 다른 일부)을 포함하는 SMTP HELO 응답 또는 SMTP EHLO 응답 명령을 포함하는 연속적인 패킷들에서 마지막 네트워크 패킷일 수 있다. 이러한 유형의 접속 설정 데이터는 표준 접속 설정 데이터와 다를 수 있다. 따라서, 네트워크 주소를 도용하려는 시도를 하는 컴퓨터 시스템이 변경된 접속 설정 데이터에 대한 적절한 응답을 정확하게 예측할 가능성이 줄어든다.

[0042] 본 방법(200)은 주소 검증 데이터를 포함하는 변경된 접속 설정 데이터를 수신하는 동작(동작 "202")을 포함한다. 동작 "202"는 주소 검증 데이터를 포함하는 변경된 접속 설정 데이터를 수신하는 송신 컴퓨터 시스템을 포함할 수 있다. 예를 들면, 송신 메시징 서버(107)는 주소 검증 데이터(114)를 포함하는 변경된 접속 설정 데이터(113)를 수신 메시징 서버(109)로부터 수신할 수 있다.

[0043] 몇몇 실시예에서, 접속 초기화 데이터를 송신하지 않은 메시징 서버는 변경된 접속 데이터를 수신한다. 예를 들어, 주소(112)가 메시징 서버(184)에 해당하면, 메시징 서버(184)는 주소 검증 데이터(114)를 포함하는 변경된 접속 설정 데이터(118)를 수신 메시징 서버(109)로부터 수신할 수 있다. 수신된 변경된 접속 설정 데이터(118)가 해당 접속 초기화 데이터에 응답하여 수신되지 않았으면, 메시징 서버(184)는 변경된 접속 설정 데이터(118)를 단순히 버릴 수 있다. 그러므로, 송신 메시징 서버(107)가 메시징 서버(184)로부터 접속을 모의(그러므로 도용)하려고 시도하고 있으면, 수신 메시징 서버(109)는 주소 검증 데이터(114)에 대한 적절한 응답을 수신하지 못할 수 있다. 예를 들면, 수신 메시징 서버(109)는 주소 검증 데이터(114)에 포함된 문자들의 무작위 시퀀스를 반사(echoing back)하는 향상된 NOOP 명령을 수신하지 못할 수 있다.

[0044] 따라서, 수신 메시징 서버(109)는 네임 서버(108)에 문의하여, 메시징 서버(184)(주소(112)에 해당하는 메시징 서버)가 변경된 접속 설정 데이터를 지원하는지를 결정할 수 있다. 엔트리(176)는 메시징 서버(184)를 포함하는 도메인에 대한 DNS 엔트리일 수 있다. 수신 메시징 서버(109)는, 예를 들면 향상된 NOOP 지원 레코드(138)(특별한 NOOP 지원 레코드 또는 TXT 레코드)와 같은 변경된 접속 설정 지원 레코드에 대한 엔트리(176)를 문의할 수 있다. 메시징 서버(184)가 변경된 접속 설정, 예를 들면 향상된 NOOP 명령을 지원한다고 지시되면, 주소 검증 데이터(114)에 대한 적절한 응답 수신 실패는, 접속 초기화 데이터(111)가 메시징 서버(184)로부터 송신되지 않았다는 것을 지시할 수 있다.

[0045] 본 방법(200)은 주소 검증 데이터에 기초하여 적절한 접속 응답 데이터를 생성하는 동작(동작 "203")을 포함한다. 동작 "203"은 주소 검증 데이터에 기초하여 적절한 접속 응답 데이터를 생성하는 송신 컴퓨터 시스템을 포함할 수 있다. 예를 들면, 송신 메시징 서버(107)는 주소 검증 데이터(114)에 기초하여 적절한 접속 응답 데이터(117)를 생성할 수 있다. 접속 설정 데이터(113)가 복수의 네트워크 패킷 중 마지막 네트워크 패킷이면, 송신 메시징 서버(107)는 마지막 네트워크 패킷의 수신을 수신 확인 응답하는 적절한 시퀀스 번호를 생성할 수 있다. 접속 설정 데이터(113)가 접속 초기화 데이터(111)를 재전송하라는 요구이면, 송신 메시징 서버(107)는 접속 초기화 데이터(111)를 재생성할 수 있다. 접속 설정 데이터가 비표준 데이터(예를 들면, 문자열의 무작위 시퀀스)를 포함하는 SMTP EHLO 응답 명령 또는 SMTP HELO 응답 명령이면, 송신 메시징 서버(107)는 비표준 데이터를 포함하는 향상된 NOOP 명령을 생성할 수 있다.

[0046] 본 방법(200)은 적절한 접속 응답 데이터를 수신 컴퓨터 시스템에 송신하는 동작(동작 "204")을 포함한다. 동작 "204"는 적절한 접속 응답 데이터를 수신 컴퓨터 시스템에 송신하는 송신 컴퓨터 시스템을 포함할 수 있다. 예를 들면, 송신 메시징 서버(107)는 적절한 접속 응답(117)을 포함하는 접속 응답 데이터(116)를 수신 메시징 서버(109)에 송신할 수 있다. 적절한 접속 응답(117)은, 예를 들면 적절한 수신 확인 응답 시퀀스 번호, 재생성된 접속 초기화 데이터 또는 비표준 데이터를 포함할 수 있다. 송신 메시징 서버(107)는, 예를 들면 향상된 NOOP 명령에서, 수신된 SMTP HELO 명령 또는 SMTP EHLO 명령으로부터의 문자열의 무작위 시퀀스를 포함한다.

[0047] 수신 메시징 서버(109)는 접속 응답 데이터(116)를 수신할 수 있다. 그러나, 수신 메시징 서버는 적절한 접속 응답 데이터를 포함하지 않는 다른 접속 응답 데이터를 수신하거나 접속 응답 데이터를 전혀 수신하지 않을 수 있다. 예를 들면, 송신 메시징 서버(107)가 메시징 서버(104)에 해당하는 네트워크 주소를 도용하려는 시도를 하고 있으면, 송신 메시징 서버(107)는 주소 유효와 데이터(114)를 수신하지 않을 수 있다(주소 유효와 데이터(114)가 메시지 서버(184)로 송신되었기 때문임). 그러므로, 송신 메시징 서버(107)는 주소 검증 데이터(114)에 기초하지 않은 접속 응답 데이터를 예측하려는 시도를 할 수 있다. 따라서, 송신 메시징 서버(107)가 적절하지 않은 (예를 들면, 표준인) 접속 응답 데이터를 예측할 가능성이 증가한다.

[0048] 본 방법(200)은, 추정된 송신 주소에 해당하는 컴퓨터 시스템이 주소 검증 데이터에 적절하게 응답했는지를 결정하는 동작(동작 "208")을 포함한다. 동작 "208"은, 추정된 송신 주소에 해당하는 컴퓨터 시스템이 주소 검증 데이터에 적절하게 응답했는지를 결정하는 수신 컴퓨터 시스템을 포함할 수 있다. 예를 들면, 수신 메시징 서버(109)는 주소(112)에 해당하는 컴퓨터 시스템이 주소 검증 데이터(114)에 적절히 응답했는지를 결정할 수 있다. 적절한 접속 응답(117)의 수신은, 주소(112)에 해당하는 컴퓨터 시스템이 주소 검증 데이터(114)에 적절히 응답했다는 것을 수신 메시징 서버(109)에 지시할 수 있다. 예를 들면, 접속 설정 데이터(113)를 포함하는 네트워크 패킷에 대한 적절한 수신 확인 응답 시퀀스 번호, 재전송 요구에 응답하여 접속 초기화 데이터(111)의 재전송, 또는 문자열들의 반사된 무작위 시퀀스를 포함하는 향상된 SMTP NOOP 명령은 적절한 접속 응답을 지시할 수 있다. 수신 메시징 서버(109)가 적절한 접속 응답을 수신하면, 추정된 네트워크 주소가 도용될 가능성이 감소된다.

[0049] 부적절한 접속 데이터에 응답하여, 수신 메시징 서버는 추정된 송신 주소에 해당하는 네임 서버 엔트리를 문의할 수 있다. 예를 들면, 수신 메시징 서버(109)는 엔트리(176)(주소(112)에 해당하는 엔트리)에 문의하여, 메시징 서버(184)가 변경된 접속 설정을 지원하는지를 결정할 수 있다. 메시징 서버(184)가 변경된 접속 설정 데이터, 예를 들면 향상된 NOOP 명령을 지원한다고 지시되면, 메시징 서버(184)로부터의 것이라고 추정되는 부적절한 응답 데이터의 수신은 접속 초기화 데이터(111)가 메시징 서버(184)로부터 송신되지 않았음을 지시할 수 있다.

[0050] 도 3을 참조하면, 도 3은 본 발명에 따른, 인가된 발신 메시징 서버의 식별을 용이하게 하는 네트워크 아키텍처(300)의 예를 도시한다. 네트워크 아키텍처(300)에는 도메인(305, 306 및 307)이 도시된다. 도메인(305, 306 및 307)은, 이들 내부에 도시된 해당 컴퓨터 시스템을 논리적으로 포함한다는 것을 설명하기 위하여 점선으로서 도시된다. 그러나, 도메인에 포함된 컴퓨터 시스템의 물리적 위치는 서로 다를 수 있다. 예를 들면, 메시징 클라이언트(341) 및 메시징 클라이언트(343)는 물리적으로 근접(예를 들면, 동일한 방)하거나, 또는 물리적으로 먼 거리(예를 들면, 상이한 대륙)에 위치할 수 있다.

[0051] 또한, 네트워크 아키텍처(300)에는 네임 서버(308)가 도시된다. 일반적으로, 네임 서버(308)는, 예를 들면 상이한 도메인의 컴퓨터 시스템들 간의 통신을 용이하게 하기 위하여 컴퓨터 시스템에 대한 텍스트 문자열 식별자(textual string identifier)를 해당 숫자 네트워크 주소로 상관시키는 것과 같은 네임 정보를 저장한다. 네임 서버(308)는 도메인 네임(예를 들면, www.test.com)을 IP(Internet Protocol) 주소(예를 들면, 102.33.23.112)로 번역하는 도메인 네임 시스템(DNS) 서버일 수 있다.

[0052] 네임 서버(108)는 도메인에 대한 인가된 발신 메시징 서버를 지시하는 하나 이상의 레코드를 저장할 수 있다. 도메인에 대한 인가된 발신 메시징 서버를 지시하는 레코드는, 예를 들면 RMX 레코드, TXT 레코드 또는 TXT 레코드의 세트와 같은 DNS 레코드일 수 있다. TXT 레코드 또는 TXT 레코드의 세트는 텍스트 데이터, 또는 예를 들면 XML 명령어와 같이 텍스트 형태로 인코딩된 다른 데이터를 포함할 수 있다. 인가된 발신 메시징 서버를 지시하는 레코드는 도메인에 대한 전자 메일 정책을 지시하는 DNS 레코드 세트에 포함될 수 있다.

[0053] 또한, 네트워크 아키텍처(300)에는 네트워크(301)가 도시된다. 도메인(305, 306, 307) 및 네임 서버(308)는 각각 해당 링크(391, 392, 393 및 394)에 의하여 네트워크(301)에 접속된다. 링크(391, 392, 393 및 394) 및 네트워크(301)는 시스템 버스의 일부, 근거리 통신망(LAN)의 일부, 원거리 통신망(WAN)의 일부 및/또는 심지어는 인터넷의 일부를 포함할 수 있다. 네트워크 아키텍처(300)에 도시된 도메인 및 컴퓨터 시스템은, 예를 들면 전자 메일 메시지, DNS 문의 및 DNS 응답(리소스 레코드를 포함함)과 같은 전자 메시지를 도시된 링크 상으로 교환할 수 있다. 양방향 화살표(386)에 의하여 도시된 바와 같이, 네임 서버(308)는 또한 재귀적 문의의 목적으로 다른 네임 서버(385)와 통신할 수 있다. 유사하게, 네트워크 아키텍처(300)의 컴퓨터 시스템은 (아키텍처(300)의 다른 컴퓨터 시스템을 다른 네임 서버(385)에 접속하는 링크가 명시적으로 도시되지 않았지만) 반복적인 문의의 목적으로 다른 네임 서버(385)에 바로 문의할 수 있다.

[0054] 도메인(307) 내부에서, 메시징 클라이언트(341 및 343)는 각각 해당 링크(396 및 397)에 의하여 메시징(387)에 접속된다. 각각의 메시징 클라이언트(341 및 343)는, 예를 들면 전자 메일 클라이언트 소프트웨어에 포함된 모듈과 같은 해당 메시징 인터페이스 모듈(도시되지 않음)을 포함할 수 있다. 메시징 인터페이스 모듈은 메시징 클라이언트 중 하나의 클라이언트의 사용자가 메시징 서버(317)로부터 전자 메시지를 액세스하고 시청하는 메커니즘을 제공한다. 사용자(예를 들면, John Doe)는 사용자에 의하여 사용하도록 배당되거나 그리고/또는 인가된 전자 메시징 주소(예를 들면, jdoe@test2.com)에 송신된 전자 메시지를 시청할 수 있다.

[0055] 도 4는 본 발명에 따라, 인가된 발신 메시지 서버를 식별하는 방법(400)의 예시적인 방법의 흐름도를 도시한다.

인가되지 않은 컴퓨터 시스템은 전자 메시지의 하나 이상의 필드를 변경(이하, "도메인 위조"라고 할 수 있음)하여, 사실 전자 메시지(예를 들면, 전자 메일 메시지)가 지정된 도메인으로부터 전달되지 않은 때에 전자메시지가 지정된 도메인으로부터 전달된 것처럼 보이게 할 수 있다. 따라서, 본 방법(400)은 전자 메시지에 포함된 도메인 네임이 위장된 가능성을 지시하는 입력을 제공하는 것으로 보여질 수도 있다. 도메인 네임이 위장되었다는 높은 가능성은 전자 메시지가 불필요하고/하거나 요청되지 않은 전자 메시지라는 것을 (단독으로 또는 다른 입력과 결합하여) 지시할 수 있다.

[0056] 본 방법(400)은 네트워크 아키텍처(300)에 도시된 구성 요소에 대하여 설명된다. 본 방법(400)은 송신측 도메인으로부터 송신된 것으로 추정되는 전자 메시지를 수신하는 동작(동작 "401")을 포함한다. 동작 "401"은 송신측 도메인으로부터 송신된 것으로 추정되는 전자 메시지를 수신하는 수신 도메인의 수신 메시징 서버를 포함할 수 있다. 예를 들면, (도메인(307)의) 메시징 서버(317)는 메시징 서버(316)로부터 전자 메시지(371)를 수신할 수 있다. 전자 메시지(371)는 전자 메시지(371)가 도메인(305)으로부터 송신된 것을 지시하는 위장된 도메인 네임(372)을 포함한다.

[0057] 추정된 송신 도메인은 전자 메시지에 포함된 파라미터 값으로부터 식별될 수 있다. 예를 들면, 메시징 서버(317)는 전자 메시지(371)에 포함된 파라미터 값으로부터 (예를 들면, 위장된 도메인 네임(372)으로부터) 도메인(305)을 식별할 수 있다. 추정된 송신 도메인은 추정된 송신 엔티티의 도메인 부분(예를 들면, "@" 문자 뒤의 문자들)으로부터 식별될 수 있다. 전자 메시지의 다른 파라미터 값은 실제 송신 네트워크 주소를 포함할 수 있다. 예를 들면, 실제 송신 네트워크 주소는 전자 메시지의 역경로(Reverse-Path; "envelope From address"로서 언급될 수 있음)에 포함될 수 있다. 역경로는 송신 컴퓨터 시스템이 SMTP "MAIL FROM" 명령을 발생하는 결과로서 전자 메시지에 포함될 수 있다. 그러므로, 메시징 서버(371)는 전자 메시지(371)에 대한 이 파라미터 값을 조사하여 실제 송신 네트워크 주소(예를 들면, 메시징 서버(316)의 실제 IP 주소)를 식별하는 시도를 할 수 있다.

[0058] 그러나, 실제 송신 네트워크 주소는 전자 메시지의 제1 Resent-Sender 헤더, 전자 메시지의 Resent-From 헤더의 제1 메일박스, 전자 메시지의 Sender 헤더, 또는 전자 메시지의 From 헤더의 제1 메일 박스에 포함될 수도 있다. 따라서, 메시징 서버(371)는, 실제 송신 네트워크 주소(예를 들면, 메시징 서버(316)의 실제 IP 주소)를 식별하는 시도를 하기 위하여 전자 메시지(317)에 대한 이들 파라미터 값 각각을 (개별적으로 또는 Reverse-Path 파라미터 값을 조사하는 것과 함께) 조사할 수 있다. 전자 메시지의 다수의 상이한 부분이 조사되기 때문에, 전자 메시지의 실제 송신 네트워크 주소가 식별된 가능성이 증가된다. 몇몇 전자 메일 구현법은, 전자 메일 메시지가 빈 역경로를 가지고 송신될 것을 요구한다. 본 발명의 실시예는, 전자 메시지가 역경로 파라미터 값을 포함하지 않는 때에 실제 송신 주소를 식별하는데 유용할 수 있다.

[0059] 위장된 도메인 네임(372)에 기초하여, 메시징 서버(317)는 도메인(305)을 전자 메시지(371)에 대한 추정된 송신 도메인으로서 식별할 수 있다. 역경로 또는 적어도 하나의 나열된 헤더를 포함하지 않는 전자 메시지는 불필요하고/하거나 요청되지 않은 것으로 간주될 수 있다. 이러한 전자 메시지를 불필요하고/하거나 요청되지 않은 것으로 간주하면, 엔티티가 메시지 분류 모듈을 방해하기 위하여 역경로 및 모든 헤더를 의도적으로 생략하는 가능성이 감소된다.

[0060] 본 방법(400)은 송신 컴퓨터 시스템에 해당하는 실제 송신측 네트워크 주소를 식별하는 시도를 하기 위하여 전자 메시지의 복수의 파라미터 값을 조사하는 동작(동작 "402")을 포함한다. 동작 "402"는 송신 컴퓨터 시스템에 해당하는 실제 송신측 네트워크 주소를 식별하는 수신측 컴퓨터 시스템을 포함할 수 있다. 수신측 컴퓨터 시스템은, 예를 들면 전자 메시지(371)의 Reverse-Path, 제1 Resent-Sender 헤더, Resent-From 헤더의 제1 메일박스, 전자 메시지의 Sender 헤더, 또는 From 헤더의 제1 메일박스 중 하나 이상으로부터 실제 송신측 네트워크 주소를 식별할 수 있다. 메시징 서버(317)는 실제 송신측 IP 주소가 메시징 서버(316)에 해당하는 것을 식별할 수 있다. 본 방법(200)은 IP 주소가 위장될 가능성을 감소시키기 위하여 이용될 수 있다.

[0061] 본 방법(400)은 송신측 도메인에 대하여 전자 메시지를 송신하도록 인가된 네트워크 주소의 목록을 네임 서버에 문의하는 동작(동작 "203")을 포함한다. 동작 "403"은 송신측 도메인에 대하여 전자 메시지를 송신하도록 인가된 네트워크 주소의 목록을 네임 서버에 문의하는 수신 컴퓨터 시스템을 포함할 수 있다. 예를 들면, 메시징 서버(317)는 인가된 서버 문의(379)를 포함하는 네임 서비스 메시지(375)를 도메인(307)이 네임 서버(308)에 발행하도록 할 수 있다. 네임 서비스 메시지(375)는 도메인(305)을 식별하는 식별자를 포함할 수 있다.

[0062] 네임 서버(308)는 네임 서비스 메시지(375)를 수신하여 인가된 서버 문의(379)를 처리할 수 있다. 네임 서버(308)에서, 엔트리(376)는 도메인(305)에 해당하는 DNS 엔트리일 수 있다. 엔트리(376)는 인가된 서버 레코드

(336)를 포함하여, 도메인(305)에 대한 하나 이상의 레코드(예를 들면, RMX 및/또는 TXT 레코드)를 포함할 수 있다. 수신된 TXT 레코드는 XML 명령어를 포함할 수 있다. 인가된 서버 레코드(336)는 도메인(105)에 대하여 전자 메시지를 송신하도록 인가된 메시징 서버에 해당하는 네트워크 주소(예를 들면, IP 주소)를 포함할 수 있다.

[0063] 메시징 서버(315)는 도메인(305)으로부터 전자 메시지를 송신하도록 인가된 컴퓨터 시스템으로서 지명되지만, 메시징 서버(316)는 도메인(305)으로부터 전자 메시지를 송신하도록 인가된 컴퓨터 시스템으로서 지명되지 않을 수 있다. 그러므로, 인가된 서버 레코드(336)는 메시지 서버(315)에 해당하는 네트워크 주소(그리고 혹은 다른 컴퓨터 시스템에 대한 네트워크 주소)를 포함하도록 구성될 수 있지만, 메시징 서버(316)에 해당하는 네트워크 주소를 포함하지 않도록 구성될 수 있다. 따라서, 네임 서버 메시지(375)를 수신하는 것에 응답하여, 네임 서버(308)는 인가된 서버 목록(378)을 포함하는 네임 서버 응답(377)을 도메인(307)에 송신할 수 있다. 도메인(307)은 네임 서버 응답(337)을 수신할 수 있고 네임 서버 응답(377)을 메시징 서버(317)에 전달할 수 있다.

[0064] 본 방법(400)은, 실제 송신측 네트워크 주소가 송신 도메인에 대하여 발신 전자 메시지를 송신하도록 인가되었는지를 결정하는 동작(동작 "404")을 포함한다. 동작 "404"는, 실제 송신측 네트워크 주소가 송신 도메인에 대하여 발신 전자 메시지를 송신하도록 인가되는지를 결정하는 수신 컴퓨터 시스템을 포함할 수 있다. 예를 들면, 메시징 서버(317)는, 메시징 서버(316)에 해당하는 네트워크 주소가 도메인(305)에 대하여 전자 메시지를 송신하도록 인가되었는지를 결정할 수 있다.

[0065] 수신 컴퓨터 시스템은 실제 송신측 네트워크 주소와 인가된 서버 목록에 포함된 네트워크 주소를 비교하여, 실제 송신측 네트워크 주소가 인가되었는지를 결정한다. 예를 들면, 메시지 서버(317)는 메시징 서버(316)에 해당하는 네트워크 주소를 인가된 서버 목록(378)에 포함된 네트워크 주소와 비교하여, 메시징 서버(316)가 도메인(305)에 대하여 전자 메시지를 송신하도록 인가되었는지를 결정한다. 실제 송신측 네트워크 주소가 도메인에 대하여 인가된 네트워크 주소의 목록에 포함되면, 이것은 송신측 컴퓨터 시스템이 그 도메인으로부터의 것이라고 추정되는 전자 메시지를 송신하도록 인가되지 않았다는 것을 지시한다. 따라서, 송신 메시징 서버(316)가 전자 메시지(371)에 위장된 도메인 네임을 포함함으로써 도메인(305)을 위장했기 때문에, 메시징 서버(316)는 인가되지 않은 컴퓨터 시스템으로서 발견될 수 있다. 인가되지 않은 컴퓨터 시스템에 의한 전자 메시지의 전송은, 전자 메시지가 불필요하고/하거나 요청되지 않은 전자 메시지라는 지시일 수 있다.

[0066] 한편, 실제 송신측 네트워크 주소가 도메인에 대하여 인가된 네트워크 주소의 목록에 포함되면, 이것은 송신측 컴퓨터 시스템이 그 도메인으로부터의 것이라고 추정되는 전자 메시지를 전달하도록 인가되었다는 것을 지시한다. 예를 들면, 메시징 서버(315)는 전자 메시지에 도메인(305)을 정당하게 포함할 수 있고, 인가된 컴퓨터 시스템으로서 발견될 수 있다. 인가된 컴퓨터 시스템(예를 들면, 메시징 서버(315))에 의한 전자 메시지의 전송은, 전자 메시지가 정당한 전자 메시지라는 지시일 수 있다.

[0067] 본 방법(400)은 그 결정의 결과를 메시지 분류 모듈에 제공하는 동작(동작 "405")을 포함한다. 메시지 분류 모듈은 메시지 분류 모듈에 제공된 입력에 기초하여 전자 메시지를 정당한, 불필요한, 그리고/또는 요청되지 않은 메시지로 분류할 수 있다. 예를 들면, 메시징 서버(317)는 메시징 서버 컴퓨터 시스템(316)(인가되지 않음) 또는 메시징 서버(315)(인가됨)에 관한 결정의 결과를 메시지 분류 모듈(328)에 제공할 수 있다. 메시징 서버(316)가 인가되지 않았다는 것을 지시하는 제공된 결과에 기초하여 (단독으로 또는 다른 제공된 입력과 결합하여), 전자 메일 분류 모듈(328)은 전자 메시지(371)를 불필요하고/하거나 요청되지 않은 전자 메시지로 분류할 수 있다.

[0068] 몇몇 실시예에서, 메시지 분류 모듈은 메시징 클라이언트에 상주한다. 예를 들면, 메시징 클라이언트(343)는 메시지 분류 모듈(353)을 포함한다. 그러므로, 적절한 때에, 메시징 서버(317)는 (도메인에 대하여 전자 메시지를 전달하도록 송신 컴퓨터 시스템의 인가에 관한) 결정의 결과를 전자 메일 분류 모듈(353)에 교대로 제공할 수 있다.

[0069] 이제, 도 5를 참조하면, 도 5는 송신 도메인의 전자 메시지 전송 정책을 인식하고, 본 발명에 따라 연산 퍼즐에 대한 해답을 검증하는 것을 용이하게 하는 네트워크 아키텍처(500)의 예를 도시한다. 도메인(506, 507)이 네트워크 아키텍처(500)에서 설명된다. 도메인(506, 507)은 점선으로 표시되어 도메인(506, 507)이 도메인(506, 507) 내부에 설명된, 대응하는 컴퓨터 시스템을 논리적으로 포함한다는 것을 도시한다. 그러나, 네트워크 아키텍처(300)와 유사한, 네트워크 아키텍처(500)의 도메인에 포함된 컴퓨터 시스템의 물리적 위치는 서로 다를 수 있다.

[0070] 또한 네임 서버(508)가 네트워크 아키텍처(500)에 설명되어 있다. 네임 서버(508)는 일반적으로 다른 도메인에서의 컴퓨터 시스템 간의 통신을 용이하게 하기 위하여, 예를 들어 컴퓨터 시스템용 텍스트 스트링 식별자를 대응하는 숫자 네트워크 주소에 연관시키는 것과 같은 네임 정보를 저장한다. 네임 서버(508)는 도메인 네임(예를 들어 www.test1.com)을 IP 주소(예를 들어 119.46.122.87)로 번역하는 도메인 네임 서버(DNS)일 수 있다. 네임 서버(508)는 또한 도메인이 하나 이상의 전자 메시지 전송 정책(Electronic Message Transmission Policies; ETPs)을 준수한다는 것을 지시하는 레코드 및 도메인이 연산 퍼즐에 대한 해답을 해결 및/또는 검증할 수 있다고 지시하는 레코드를 저장한다.

[0071] ETPs는 예를 들어 특별 ETP 레코드, TXT 레코드 또는 TXT 레코드의 집합과 같은 DNS 레코드에 포함될 수 있다. TXT 레코드 또는 TXT 레코드의 집합은 텍스트 데이터나 예를 들어 XML 명령어와 같이 텍스트 폼으로 인코딩된 다른 데이터를 포함할 수 있다. ETP를 인식하는 레코드는 도메인용 전자 메일 정책을 지시하는 DNS 레코드 집합에 포함될 수 있다. ETPs는 전자 메시지 정책과 관련된 증명을 나타내는 현존 인가 프레임워크 및 기술에 포함될 수 있다. 예를 들어, ETPs는 DNS 레코드에 저장되는 X.509 인증서, XrML(eXtensible rights Marksup Language) 라이센스, 또는 케르베로스(Kerberos) PACS에 포함될 수 있다.

[0072] ETP는 도메인에 바인딩된 참조 텍스트를 포함할 수 있고, 상호 신뢰된 소스에 의하여 발행된다. 예를 들어 발행된 X.509 인증서는 도메인과 매칭되는 라우팅 주소(routing adress)를 포함한다. 이것은 DNS로부터 정책을 검색하는 데 있어서 도메인으로 상태 정책의 일정 바인딩을 제공한다.

[0073] 연산 퍼즐은 예를 들어 특별 퍼즐 지원 레코드, TXT 레코드, 또는 TXT 레코드의 집합과 같은 DNS 레코드에 포함될 수 있다. TXT 레코드, 또는 TXT 레코드의 집합은 텍스트 데이터나 예를 들어 XML 명령어와 같이 텍스트 폼으로 인코딩된 다른 데이터를 포함할 수 있다. 연산 퍼즐용 지원을 지시하는 레코드는 도메인용 전자 메일 정책을 지시하는 DNS 레코드 집합에 포함될 수 있다.

[0074] 또한 네트워크(501)는 네트워크 아키텍처(500)에서 설명된다. 도메인(506, 507) 및 네임 서버(508)는 각각 대응하는 링크(592, 593, 594)에 의하여 네트워크(501)에 연결된다. 네트워크(501) 및 링크(592, 593, 594)는 시스템 버스의 일부, LAN의 일부, WAN의 일부 및/또는 인터넷의 일부까지 포함할 수 있다. 네트워크 아키텍처(500)에 설명된 도메인 및 컴퓨터 시스템은 예를 들어 전자 메일 메시지, DNS 문의 및 설명된 링크에 대한 (리소스 레코드를 포함하는) DNS 응답을 교환할 수 있다. 양방향 화살표(586)에 의하여 도시된 것처럼, 네임 서버(508)는 또한 재귀적 문의의 목적으로 다른 네임 서버(585)와 통신할 수 있다. 유사하게, 네트워크 아키텍처(500)에서의 컴퓨터 시스템은, 아키텍처(500)에서의 다른 컴퓨터 시스템 네트워크를 다른 네임 서버(585)에 연결하는 링크는 명시적으로 설명되지 않았지만, 재귀적 문의의 목적으로 다른 네임 서버(585)를 직접적으로 문의할 수 있다.

[0075] 도메인(507) 내에서, 메일 클라이언트(541, 542, 543)는 각각의 대응하는 링크(596, 597, 598)에 의하여 메시징 서버(517)에 연결된다. 각각의 메일 클라이언트(541, 542, 543)는 예를 들어 전자 메일 클라이언트 소프트웨어 내에 포함된 대응 전자 메시징 인터페이스 모듈(도시되지 않음)을 포함할 수 있다. 전자 메시징 인터페이스 모듈은 메일 클라이언트 중 하나의 사용자가 전자 메시지에 액세스하고 이를 볼 수 있는 메카니즘을 제공한다. 사용자(예를 들어 제인 스미스)는 전자 메시지가 사용자의 사용을 위해 인가되거나 사용자에 할당된 전자 메시징 어드레스(예를 들어 jsmith@test12.net)를 송신한 것을 볼 수 있다.

[0076] 도 6은 본 발명에 따라 송신 도메인의 전자 메시지 전송 정책을 결정하기 위한 방법(600)의 예시적 흐름도를 도시한다. 전자 메시지를 송신하는 도메인은 하나 이상의 ETPs을 준수할 수 있다. 특정 ETPs를 도메인이 준수하는 것은 도메인이 불필요하거나 요청되지 않은 전자 메시지를 송신(또는 다른 도메인이 송신하는 것을 허락)할 가능성이 감소하는 것을 나타낼 수 있다. 반면에, 도메인이 특정 ETPs을 준수하지 않는 것은 도메인이 불필요하거나 요청되지 않은 전자 메시지를 송신(또는 다른 도메인이 송신하는 것을 허락)할 가능성이 증가하는 것을 나타낼 수 있다. 어떤 실시예에서, 실제 송신 네트워크 주소가 (예를 들어 방법(200)에 따라) 도용되는 것을 결정하고, (예를 들어 방법(400)에 따라) 송신 도메인이 위장되고 있지 않는다는 것을 결정한 후 도메인의 ETPs를 인식하는 것이 적절할 수 있다.

[0077] 네트워크 아키텍처(500)에 나타난 컴포넌트와 관련하여 방법(600)을 논의할 수 있다. 방법(600)은 송신 도메인으로부터 전자 메시지를 수신하는 동작을 포함한다(동작 601). 동작(601)은 송신 도메인으로부터 전자 메시지(예를 들어 전자 메일 메시지)를 수신하는 수신 컴퓨터 시스템을 포함할 수 있다. 예를 들어, 메시징 서버(517)는 메시징 서버(516)로부터 전자 메시지(575; 예를 들어 전자 메일 메시지)를 수신할 수 있다. 전자 메시

지(575)는 선택적으로 도메인(506)에 의하여 준수되는 ETPs를 나타내는 ETP 인증서(576)를 포함할 수 있다.

[0078] 방법(600)은 (예를 일정한 사전 정의 표준에 포함된 것과 같은) 송신측 도메인에 의하여 준수되는 관련 전자 메시지 전송 정책을 인식하기 위한 기능적 결과 지향 단계를 포함한다(단계 605). 단계(605)는 송신측 도메인에 의하여 준수되는 전자 메시지 전송 정책을 인식하기 위한 임의의 대응 동작을 포함할 수 있다. 그러나, 도 6에 도시된 방법에서, 단계(605)는 송신측 도메인에 대응하는 하나 이상의 전자 메시지 전송 정책을 수신하는 대응 동작을 포함할 수 있다(동작 602).

[0079] 동작(602)은 송신측 도메인에 대응하는 하나 이상의 전자 메시지 전송 정책을 수신하는 수신 컴퓨터 시스템을 포함할 수 있다. 예를 들어, 메시징 서버(517)는 ETP 인증서(576)를 포함하는 전자 메시지(575)를 포함할 수 있다. ETP 인증서(576)는 도메인(506)에 의하여 준수되는 ETP들을 지시하는 하나 이상의 X.509 인증서일 수 있다.

[0080] 어떤 실시예에서, 보안 다목적 인터넷 메일 확장(S/MIME; Secure Multipurpose Internet Mail Extensions) 전자 메시지(앞으로 ETP S/MIME 메시지라고 함)는 합리적 전자 메시징 행위의 정책을 전달하려는 의도로 서명된다. ETP S/MIME 메시지는 S/MIMEv3-컴피언트(compiant) 전자 메시지일 수 있다. ETP S/MIME 메시지는 멀티파트/서명 포맷일 수 있고 두 MIME 파트를 포함할 수 있다. 제1 MIME 파트는 사인될 전자 메시지(예를 들어 메시지의 완전 텍스트 표현)의 일부를 포함할 수 있다. 제2 MIME 부분은 제1 MIME 부분의 분리된 서명을 포함할 수 있다. 분리된 서명은 ETP 인증서의 지원 하에서 생성될 수 있다. ETP S/MIME 메시지는 비 서명 인식 메시징 시스템(non-signature-aware messaging system)에 서명된 메일의 증가된 역방향 호환성을 제공하는 완전 헤더 내장 모드(entirely-in-headers mode)에서 구현될 수 있다.

[0081] 전자 메시지 수신자는 ETP 합의를 위반하는 엔티티를 인식할 수 있다. 따라서, 전자 메시지 수신자는 ETP S/MIME 메시지에서의 인증서가 취소되었는지 여부를 결정하려고 시도할 수 있다. 전자 메시지 수신자가 인증서가 취소되었는지 여부를 결정하려고 시도하는 최소한 네가지 방법이 존재한다. 일 실시예에서, 전자 메시지 수신자는 인증서가 취소되었는지 여부를 질문하기 위하여, 인증서 발행자에 문의한다. 또 다른 실시예에서, 전자 메시지 수신자는 신뢰되는 인증서 발행자에 의하여 주기적으로 업데이트된 취소된 인증서의 리스트를 관리한다. ETP S/MIME 메시지가 수신될 때, 전자 메시지 수신자는 리스트를 검사하여 포함된 인증서가 취소되었는지 여부를 결정한다. 또 다른 실시예에서, 전자 메시지 수신자는 현재 신뢰된 인증서의 리스트를 관리한다. ETP S/MIME 메시지가 수신될 때, 전자 메시지 수신자는 리스트를 검사하여 포함된 인증서가 신뢰되는지 여부를 결정할 수 있다.

[0082] 또 다른 실시예에서, 신규성의 증거는 포함된 인증서에 따른 ETP S/MIME 메시지에 포함된다. 예를 들어, ETP S/MIME 메시지는 일정 (가능한 최근의) 시간 프레임(예를 들어 1분 또는 15분) 동안 인증서가 여전히 유효하다는 것을 지시하는 발행자로부터의 인증서를 포함할 수 있다. 만약 전자 메시지 수신자가 시간 프레임또는 매우 길지 않은 시간 동안 ETP S/MIME 메시지를 수신한다면, 인증서는 신규하다고 판단된다. 반면에, 만약 전자 메시지 수신자가 타임 프레임 후 일정한 현저한 양의 시간 동안 ETP S/MIME 메시지를 수신한다면, 전자 메시지 수신자는 다른 메카니즘 중 하나에 의지하게 되는데, 예를 들어 인증서 발행자에게 문의하여 인증서가 취소되었는지 알게 된다.

[0083] ETP S/MIME 메시지에서 신규성의 증거를 포함함으로써 전자 메시지 수신자에 대하여 큰 효율상의 장점을 얻을 수 있다. 예를 들어, ETP S/MIME에서의 신규성의 증거를 포함하는 것은 전자 메일 수신자가 초기화하는 문의의 수를 현저하게 감소시킬 수 있다. ETP S/MIME 메시지에서의 신규성의 증거를 포함하는 것은 또한 (만약 존재한다면) 전자 메시지 송신자에 대한 임팩트(impact)를 제한한다. 예를 들어, 전자 메시지 송신은 임의의 수의 전자 메시지에 포함될 수 있는 새로운 신규성의 증거를 가끔씩만(예를 들어, 매 15분마다) 요청하도록 설정될 수 있다. 따라서 인증서 발행자에 대한 문의의 수는 큰 비율로 감소한다.

[0084] 메시징 서버(517)는 또한 송신측 도메인에 대응하는 ETPs용 네임 서버의 문의를 유발할 수 있다. 예를 들어, 메시징 서버(517)는 도메인(507)이 ETP 문의(586)을 포함하는 네임 서버 메시지(585)를 발행하도록 할 수 있다. 네임 서버 메시지(585)는 도메인(506)을 인식하는 식별자를 포함할 수 있다.

[0085] 네임 서버(508)는 따라서 네임 서비스 메시지(585)를 수신하고 ETP 문의(586)을 처리할 수 있다. 네임 서버(508)에서, 엔트리(576)는 도메인(506)에 대응하는 DNS 엔트리일 수 있다. 엔트리(576)는 인증서 레코드(556)를 포함하는, 도메인(305)을 위한 하나 이상의 레코드(예를 들어, 특별 ETP 레코드 및/또는 TXT 레코드)를 포함할 수 있다. TXT 레코드 또는 TXT 레코드의 집합은 XML 명령어를 포함할 수 있다. 인증서 레코드(556)는 도메

인(506)에 의해 준수되는 ETPs를 지시하는 하나 이상의 ETP 인증서(예를 들어, X.509 인증서)를 포함할 수 있다.

[0086] 도메인(506)은 ETPs을 준수하지 않도록 설정될 수 있다. 따라서, 엔트리(576)는 도메인(506)이 ETPs을 준수하지 않음을 지시하는 전자 메시징 구성 정보를 포함할 수 있다. 따라서, 인증서 레코드(556)는 어느 인증서도 포함하지 않을 수 있고, 또는 인증서(556)는 엔트리(576)에 조차 포함되지 않을 수 있다. 도메인(506)이 ETPs을 준수하지 않을 때, 네임 서버 응답(514)은 도메인(506)이 ETPs을 준수하지 않음을 지시하도록 설정될 수 있다. 따라서, 네임 서버 메시지(585)를 수신하는데 대응하여, 네임 서버(508)는 도메인(506)이 ETPs를 지원하지 않는다는 지시를 포함하는 네임 서버 응답(513)을 송신할 수 있다.

[0087] 반면에, 도메인(506)은 하나 이상의 ETPs을 준수하도록 설정될 수 있다. 따라서, 인증서 레코드(556)는 하나 이상의 ETPs를 포함하는 인증서로 설정될 수 있다. 따라서, 네임 서버 메시지(585)에 대응하여, 네임 서버(508)는 도메인(507)로의 ETP 인증서(514)를 포함하는 네임 서버 응답(513)을 송신할 수 있다. 도메인(507)은 네임 서버 응답(513)을 수신하고 네임 서버 응답(513)을 메시징 서버(517)로 전송할 수 있다.

[0088] 단계(605)는 하나 이상의 수신된 전자 메시지 전송 정책으로부터의 관련 전송 메시지 전송 정책을 파싱하는 대응 동작을 포함한다(동작 603). 동작(603)은 하나 이상의 수신된 전자 메시지 전송 정책으로부터의 관련 전송 메시지 전송 정책을 파싱하는 수신 컴퓨터 시스템을 포함한다. 예를 들어, 메시징 서버(517)는 ETP 인증서(576) 및/또는 ETP 인증서(514)로부터 도메인(506)용 ETPs를 파싱할 수 있다. 일정 ETPs는 합리적 메시징 전송 행동이 무엇인지 나타내는 다수의 조직에 의하여 합의될 수 있다.

[0089] 정책은 조직의 특정 그룹을 위하여 적절한 행동에 기반하여 개발될 수 있다. 그러나 어떤 정책 집합도 모든 메시징 사용자에 의하여 준수되어야 할 필요는 없다. 하지만, 예를 들어 비교적 낮은 비율로 전자 메시지를 송신하고/하거나 전자 메시지를 다수의 주소로 송신하는 것을 억제하는 것과 같은, 일정 정책을 도메인이 준수하는 것은, 도메인으로부터의 전자 메시지가 불필요하거나 요청되지 않을 가능성을 감소시키도록 지시할 수 있다. 반면에, 상기 정책의 비준수는 도메인으로부터의 전자 메시지가 불필요하거나 요청되지 않을 가능성을 증가시키도록 지시할 수 있다.

[0090] 방법(600)은 관련 전자 메시지 전송 정책을 메시지 분류 모듈로 제공하는 동작을 포함한다(동작 604). 동작(604)은 관련 전자 메시지 전송 정책을 메시지 분류 모듈에 제공하는 수신 컴퓨터 시스템을 포함한다. 예를 들어, 메시징 서버(517)는 도메인(506)용 관련 ETPS를 메시지 분류 모듈(529)에 제공할 수 있다. (혼자 또는 다른 제공된 입력과 조합된) 관련 ETPS에 기초하여, 메시지 분류 모듈(529)은 정당한 전자 메시지 또는 불필요하거나 요청되지 않은 전자 메시지로 전자 메시지(575)를 분류할 수 있다. 선택적으로, 적절한 때에 메시징 서버(517)는 도메인(106)용 관련 ETPS를 메시지 분류 모듈(553)로 제공할 수 있다. (혼자 또는 다른 제공된 입력과 조합된) 관련 ETPS에 기초하여, 메시지 분류 모듈(553)은 전자 메시지(575)를 정당한 전자 메시지 또는 불필요하거나 요청되지 않은 전자 메시지로 분류할 수 있다.

[0091] 도 7은 본 발명에 따라 연산 퍼즐에 대한 검증을 위한 방법(700)의 예시적 흐름도를 도시한다. 연산 퍼즐의 완료는 송신 컴퓨터 시스템이 전자메시지를 송신하기 전에 다수의 프로세서 사이클을 소비한다는 것을 지시할 수 있다. 소비된 프로세서 사이클의 지시 제공은 송신 컴퓨터 시스템이 비교적 높은 비율로 전자 메시지를 송신하지 않고 있다는 증거 및 소비된 재정적인 리소스의 증거이다. 따라서, 송신 컴퓨터 시스템으로부터의 전자 메시지는 잠재적으로 불필요하거나 요청되지 않을 가능성이 감소한다.

[0092] 방법(700)은 컴퓨터 시스템 및 네트워크 아키텍처(500)에서 설명된 모듈에 관하여 설명한다. 방법(700)은 전자 메시지에 포함되는 전자 메시지 데이터를 수신하는 동작을 포함한다(동작 701). 동작(701)은 송신 메시징 서버 또는 전자 메시지(전자 메일 메시지)에 포함된 전자 메시지 데이터를 수신하는 송신 메시징 클라이언트를 포함할 수 있다. 메시지 데이터는 전자 메시지의 헤더 또는 바디 부분에 포함된 임의의 데이터를 포함할 수 있다. 예를 들어, 메시징 서버(516)에 연결된 메시징 클라이언트는 전자 메시지(545)의 헤더 및/또는 바디에 포함된 메시지 데이터(예를 들어, 전자 주소, 서브젝트, 메시지 바디 등)를 수신할 수 있다. 메시징 서버(516)에서, 전자 메시지 데이터는 배달되는 전자 메시지(예를 들어, 전자 메시지(545))에 이미 포함될 수 있다. 따라서, 메시지 서버(516)는 대응 전자 메시지가 배달되기 전에 프로세싱용 전자 메시지 데이터의 일부(예를 들어, 메시지 데이터(546)의 일부)를 추출할 수 있다.

[0093] 연산 퍼즐에 대한 해답을 연산하기 전에, 수신측 도메인은 연산 퍼즐에 대하나 해답을 검증하도록 설정된다고 검증될 수 있다. 예를 들어 수신 메시징 서버와 같은 수신 컴퓨터 시스템은 네임 엔트리에 연산 퍼즐에 대한

해답을 검증하도록 설정된다고 공지할 수 있다. 예를 들어, 엔트리(577)는 도메인(507)용 네임 정보를 저장할 수 있다. 포함된 엔트리(577)는 도메인(507)이 연산 퍼즐에 대한 해답을 검증하도록 설정된다고 지시하는 해답 검증 지원 레코드(537)이다. 해답 검증 지원 레코드(537)는 예를 들어 특별 퍼즐 지원 레코드, TXT 레코드 또는 TXT 레코드의 집합과 같은 DNS 레코드일 수 있다. TXT 레코드 또는 TXT 레코드의 집합은 텍스트 데이터 또는 예를 들어 XML 명령어와 같은 텍스트 형식으로 인코딩된 다른 데이터를 포함한다.

[0094] 따라서, 메시징 서버(516)는 네임 서버 컴퓨터 시스템(508)에 문의하여(예를 들어 적절한 DNS 문의 메시지를 송신함으로써), 도메인(507)이 연산 퍼즐에 대한 해답을 검증할 수 있는지를 결정할 수 있다. 문의에 대응하여, 네임 서버(508)는 도메인(506)에서 수신된 지시 포함 해답 검증 지원 레코드(537)를 리턴할 수 있다(예를 들어 적절한 DNS 응답 메시지를 송신함으로써). 도메인(506)은 적절하게 수신된 지시를 메시징 서버(516)로 전송할 수 있다.

[0095] 방법(700)은 상태 정보의 다른 부분으로부터 초기 문서를 생성하는 동작을 포함한다(동작 702). 동작(702)은 다른 부분의 상태 정보로부터 초기 문서를 생성하는 송신 컴퓨터 시스템을 포함할 수 있다. 예를 들어, 메시징 서버(516)는 메시지 데이터(546)의 다른 부분으로부터 초기 문서를 생성할 수 있다. 일정 실시예에서, 메시지 데이터의 다른 부분으로부터 초기 문서를 생성하는 것은 전자 메시지로부터 메시지 데이터의 다른 부분을 추출하는 것을 포함할 수 있다. 송신 메시징 서버는 수신 메시징 서버로 전송되는 (예를 들어, 메시징 클라이언트로부터의) 전자 메시지를 수신할 수 있다. 예를 들어, 메시징 서버(516)는 메시지 데이터(546)를 포함하고, 메시징 서버(517)로 전송되는 전자 메시지를 수신할 수 있다.

[0096] 메시징 서버(516)는 전자 메시지(545)에 포함되는 메시지 데이터(546)의 일부를 추출할 수 있다. 예를 들어 메시징 서버(516)는 전자 메시지(545)의 From 필드, To 필드, NotBefore 필드, NotAfter 필드, Date 필드, Body 필드, Attachment 필드, Subject 필드 및/또는 Message-ID 필드 등에 포함되는 데이터의 일부를 추출할 수 있다. 데이터의 일부를 추출하는 것은 전자 메시지에 포함될 수 있는 텍스트 데이터, 그래픽 데이터, URI(Uniform Resource Identifier) 데이터, 실행 가능 데이터 등과 같은 임의 형식의 데이터를 실제로 추출하는 것을 포함한다. 그러면 메시징 서버(516)는 초기 문서를 생성하기 위하여 추출된 부분을 연관시킬 수 있다.

[0097] 초기 문서는 또한 예를 들어, 메시지 유일 넌스(message unique nonce; 예를 들어, 무작위로 생성된 숫자 또는 스트링)와 같은 상태 정보로부터 생성될 수 있다. 예를 들어, 메시징 서버(516)는 전자 메시지(545)에 포함되는 128 비트의 유일 무작위 스트링을 생성할 수 있다. 넌스는 초기 문서를 생성하기 위하여 메시지 데이터의 하나 이상의 부분과 연관될 수 있다.

[0098] 방법(700)은 전자 메시지의 하나 이상의 컴포넌트로부터 퍼즐 입력을 생성하는 동작을 포함한다(동작 703). 동작(703)은 전자 메시지의 하나 이상의 컴포넌트로부터 퍼즐 입력을 생성하는 송신 컴퓨터 시스템을 포함할 수 있다. 예를 들어 퍼즐 연산 모듈(528)은 전자 메시지(545)의 하나 이상의 컴포넌트로부터의 퍼즐 입력을 생성할 수 있다. 퍼즐 입력을 생성하는 것은 추출, 해싱, 연관 또는 전자 메시지의 컴포넌트에 다른 연산을 수행하는 것을 포함한다.

[0099] 일정 실시예에서, 퍼즐 입력은 초기 문서이다. 다른 실시예에서, 퍼즐 입력은 초기 문서를 초기 해시 알고리즘에 입력으로 제공함으로써 연산되는 퍼즐 입력 해시 값일 수 있다. 초기 해시 알고리즘은 보다 통일적인 퍼즐 해결 시간이 되는 통일적 길이의 입력을 생성하기 위하여 사용될 수 있다. 초기 해시 알고리즘은 응답 문서를 연산할 때 사용되는 퍼즐 해시 알고리즘일 수 있다.

[0100] 퍼즐 해시 알고리즘은 불필요하거나 요청되지 않은 전자 메시지를 방지하는데 사용하도록 상세하게 설계될 수 있다. 예를 들어 SHA-1 알고리즘과 같은 해시 알고리즘은 해시 값 생성 동안 다른 시간에 다른 대응 입력의 일부에 적용되는 복수의 서브 함수를 포함할 수 있다. 본 발명의 실시예는 서브 함수 및 입력 부분 간에서 표준 통신을 변화시킴으로써 해싱 알고리즘의 표준 연산을 변경시킨다. 동일한 서브 함수가 사용될 수 있지만, 서브 함수는 표준 연산 동안 적용되었을 데이터의 다른 부분에 적용된다. 예를 들어, 퍼즐 해시 알고리즘은 SHA-1 알고리즘의 해싱 서브 함수를 사용할 수 있지만, SHA-1 알고리즘과 다른 순서로 서브 함수를 적용한다. 서브 함수를 다른 순서로 적용하는 것은 퍼즐 해시 알고리즘을 하드웨어에 구현하는 것을 더 어렵게 만든다.

[0101] 예를 들어, SHA-1은 다음 공식에 따라 80개의 서브 함수를 특정한다.

$f_t(B,C,D) = (B \text{ AND } C) \text{ OR } ((\text{NOT } B) \text{ AND } D)$ $(0 <= t <= 19)$

$f_t(B,C,D) = B \text{ XOR } C \text{ XOR } D$ $(20 <= t <= 39)$

$f_t(B,C,D) = (B \text{ AND } C) \text{ OR } (B \text{ AND } D) \text{ OR } (C \text{ AND } D)$ $(40 <= t <= 59)$

[0102] $f_t(B,C,D) = B \text{ XOR } C \text{ XOR } D$ $(60 <= t <= 79)$

[0103] 변경된 SHA-1 알고리즘은 다음 공식에 따라 80개의 서브 함수를 특정한다.

$f_t(B,C,D) = B \text{ XOR } C \text{ XOR } D$ $(0 <= t <= 19)$

$f_t(B,C,D) = (B \text{ AND } C) \text{ OR } ((\text{NOT } B) \text{ AND } D)$ $(20 <= t <= 39)$

$f_t(B,C,D) = B \text{ XOR } C \text{ XOR } D$ $(40 <= t <= 59)$

[0104] $f_t(B,C,D) = (B \text{ AND } C) \text{ OR } (B \text{ AND } D) \text{ OR } (C \text{ AND } D)$ $(60 <= t <= 79)$

[0105] 표 1은 대응하는 변경된 SHA-1 해시 출력에 따른 텍스트 데이터의 예시를 도시한다.

[0106] 표 1

Test Data	Altered SHA-1 Hash Output
the string "abc"	6092C49D 8092E074 4B14298E 12E00ED2 DE4611A0
the string "abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"	7D3E33E1 8BB7F842 9055CB29 40BE227F CF562276
a string consisting of 1,000,000 a's	21F4D548 88AF926B 9DF19A69 EC753DDD 850D7E20
an empty string	D212F400 92F2D374 E86AB4E4 C1BE75D3 7853FDBA

[0107]

[0108]

[0109] 방법(700)은 응답 문서의 조합으로부터 응답 해시 값이 연산되고 퍼즐 입력이 연산 퍼즐용 입력값이 되도록 응답 문서를 인식하는 동작을 포함한다(동작 704). 동작(704)은 응답 문서 및 퍼즐 입력의 조합으로부터 연산된 응답 해시 값이 연산 퍼즐용 응답 값이 되도록 응답 문서를 인식하는 송신 컴퓨터 시스템을 포함한다. 예를 들어, 퍼즐 연산 모듈(528)은 연산 퍼즐용 응답인 응답 해시 값이 되는 응답 문서를 인식할 수 있다.

[0110] 일 실시예에서, 연산 퍼즐은 퍼즐 입력 과 조합된 때의 응답 문서(예를 들어 초기 문서 또는 퍼즐 입력 해시 값)를 인식하고, 그러면 응답 문서 및 퍼즐 입력의 조합이 해싱되고(예를 들어 변경된 SHA-1 알고리즘을 사용하여), 복수의 비트 포지션(예를 들어, 결과 해시 값을 통하여 산재된 비트 포지션)에 특정 값을 갖는 해시 값이 된다. 예를 들어 연산 퍼즐은 제2 비트 포지션에서 1 값을 갖고 제13 및 제54 비트 포지션에서 0값을 갖는 해시 값이 되는 응답 문서를 인식할 수 있다. 그러나, 본 발명의 실시예는 임의의 특정 복수 비트 포지션 또는 특정된 값에 제한되지 않는다.

[0111] 보다 구체적인 구현에서, 연산 퍼즐은 퍼즐 입력에 첨가될 때의 응답 문서를 인식하고, 응답 문서 및 퍼즐 입력

의 연관이 해싱되고, 적어도 (정렬된 각각의 바이트 내에서 MSB를 최초로 취하는) 최초 n비트에 0을 갖는 해시 값이 된다. 예를 들어, 연산 퍼즐은 최초 16비트에서 0 값을 갖는 해시 값이 되는 응답 문서를 인식할 수 있다. 일반적으로, 응답 문서를 인식하는 것은 H(응답 문서° 퍼즐 입력)를 형성하는 것을 포함할 수 있다. 더 구체적으로는, 응답 문서를 인식하는 것은 H(응답 문서° 초기 문서) 또는 H(응답 문서° H(초기 문서))를 형성하는 것을 포함한다. 충분히 크도록 고려한 일정한 n에 대하여, 폭력(brute force) 아닌 다른 수단은 응답 문서를 인식하기에 충분하지 않을 수 있다.

[0112] 연산 퍼즐을 해결하기 위하여 소비된 시간의 분산을 감소시키기 위하여, 최초의 복수의 비트 포지션("집합 A") 및 집합 A에서의 각각의 비트에 대한 특정된 값이 선택된다. 서로 소인 제2 복수의 비트 포지션("집합 B")이 또한 선택된다. 퍼즐 응답은 특정 크기의 복수의 응답 문서("집합 S")이고, 여기에서 각각의 응답 문서가, 퍼즐 입력과 연관되고 해싱될 때, 집합 A에서의 각각의 비트 포지션에서 특정된 값을 갖고, 집합 B의 각각의 비트 포지션에서 각각의 다른 응답 문서용 대응 해시 값과 일치한다.

[0113] 분산 감소의 보다 구체적 구현에서, 집합 A는 결과 해시 값의 프리픽스(prefix)이고, 집합 B는 결과 해시 값의 서픽스(suffix)이다. 따라서, 연산 퍼즐은, 각각의 응답 문서가 퍼즐 입력에 추가되는 때, 각각의 응답 문서 및 퍼즐 입력의 연관이 해싱되고, 적어도 최초 n 비트(집합 A)에서 0을 갖고 동일한 최종 m 비트(집합 B)를 갖는 해시 값이 되도록, 집합 S를 인식한다. 예를 들어, 연산 퍼즐은 최초 24비트에서 0을 갖고 최종 12 비트에서 동일한 값(0 또는 1)을 갖는 해시 값이 되는 16개의 응답 문서를 인식한다. 선택적으로, 최초 24 비트 및/또는 최종 12 비트는 0 및 1값을 산재시키는 특정되 비트 패턴일 수 있다.

[0114] 연산 퍼즐을 해결하는데 소비되는 시간은 집합 A, 집합 B 및/또는 집합 S를 변경함으로써 설정될 수 있다. 집합 A의 크기는 적절한 기대 해결 시간을 획득하기 위하여 변경될 수 있다. 집합 B의 크기 및 집합 S의 크기는 적절한 해답 분산을 획득하기 위하여 변경될 수 있다. 더 긴 해답 시간을 갖도록 연산 문제를 설정하는 것은 해답을 인식하는데 소비되는 컴퓨터 리소스에 그에 대응하는 증가를 초래한다. 반면에, 연산 문제가 더 짧은 해답 시간을 갖도록 설정하는 것은 해답을 인식하는데 소비되는 컴퓨터 리소스에 대응하는 감소를 초래한다. 메시징 서버(예를 들어 메시징 서버(516, 517))는 특정 해답 시간에 일치하거나 특정 해답 시간을 인식하기 위하여 대응 리소스 레코드를 문의할 수 있다. 예를 들어, 메시징 서버(516)는 엔트리(577)에 문의하여 도메인(507)용 특정 해답 시간을 인식할 수 있다.

[0115] 일정 실시예에서, 단방향 퍼즐 해시 함수가 사용된다. 단방향 퍼즐 해시 함수는 불필요하거나 요청되지 않은 전자 메시지를 방지하도록 상세하게 설계될 수 있다. 단방향 퍼즐 해시 함수는 의도적인 또는 하드웨어 가속을 금지하는, 알려진 단방향 해시의 변경일 수 있다. 더 구체적으로, 단방향 퍼즐 해시 함수는, 나눗셈 연산이 하드웨어로 가속하기에 어려우므로, 현저한 수의 나눗셈 연산을 포함할 수 있다.

[0116] 송신 컴퓨터 시스템은 전자 메시지에서의 전자 메시지 데이터에 따른 인식된 응답 문서(또는 응답 문서들)를 포함할 수 있다. 예를 들어, 메시징 서버(516)는 전자 메시지(545; 예를 들어 전자 메일 메시지)에서의 메시지 데이터(546)에 따른 응답 문서(547)를 포함할 수 있다. 방법(700)은 인식된 응답 문서 및 수신측 도메인에 대한 전자 메시지 데이터를 포함하는 전자 메시지를 송신하는 동작을 포함한다(동작 705). 동작(705)은 인식된 응답 문서(또는 응답 문서들) 및 수신측 도메인에 대한 전자 메시지 데이터를 포함하는 전자 메시지를 송신하는 송신 컴퓨터 시스템을 포함한다. 예를 들어, 메시징 서버(516)는 전자 메시지(545)를 송신하고, 이 메시지는 도메인(507)으로의 응답 문서(547) 및 메시지 데이터(546)를 포함한다. 도메인(507)은 전자 메시지(545)를 메시징 서버(517)로 전송할 수 있다. 전자 메시지(545)가 단일 응답 문서(응답 문서(547))를 포함한다고 설명되고 있지만, 전자 메시지(545)는 하나 이상의 추가적 응답 문서를 포함할 수 있다.

[0117] 방법(700)은 전자 메시지 데이터 및 응답 문서를 포함하는 전자 메시지를 수신하는 동작을 포함한다(동작 706). 동작(706)은 전자 메시지 데이터 및 응답 문서(또는 응답 문서들)를 포함하는 전자 메시지를 수신하는 수신 컴퓨터 시스템을 포함할 수 있다. 예를 들어, 메시징 서버(517)는 전자 메시지(545)를 수신할 수 있고, 이 메시지는 응답 문서(547) 및 메시지 데이터(546)를 포함한다. 전자 메시지가 특정 메시지 클라이언트로 배달될 때, 메시징 서버는 전자 메시지를 메시징 클라이언트로 전달한다. 예를 들어, 적당한 때 메시징 서버(517)는 전자 메시지(545)를 메시징 클라이언트(542)로 전송한다. 메시징 클라이언트(542)는 전자 메시지(545)를 수신할 수 있다.

[0118] 방법(700)은 상태 정보의 다른 부분으로부터 초기 문서를 재생성하는 동작을 포함한다(동작 707). 동작(707)은 상태 정보의 다른 부분으로부터 초기 문서를 재생성하는 수신 컴퓨터 시스템을 포함할 수 있다. 예를 들어, 응답 검증 모듈(527) 및/또는 응답 검증 모듈(552)은 메시지 데이터(546)의 일부 또는 전자 메시지(454)에 포함된

다른 상태 정보(예를 들어, 넌스)로부터 초기 문서를 재생성할 수 있다. 초기 문서의 연산과 유사하게, 응답 검증 모듈(527) 및/또는 응답 검증 모듈(552)은 메시지 데이터(546)의 일부 또는 초기 문서를 재생성하는 다른 상태 정보를 추출하고 연관시킬 수 있다.

[0119] 방법(700)은 전자 메시지의 하나 이상의 컴포넌트로부터의 퍼즐 입력을 재연산하는 동작을 포함한다(동작 708). 퍼즐 입력은 초기 문서 또는 송신 컴퓨터 시스템에서 사용되는 동일한 퍼즐 해시 알고리즘(예를 들어, 변경된 SHA-1 알고리즘)을 사용하여 연산된 퍼즐 입력 해시 값으로 재연산될 수 잇다. 예를 들어, 응답 검증 모듈(527) 및/또는 응답 검증 모듈(552)은 재생성된 초기 문서로부터의 퍼즐 입력 해시 값을 재연산하도록 퍼즐 연산 모듈(528)에 의하여 사용된 동일한 퍼즐 해시 알고리즘을 사용할 수 있다. 따라서, 송신 컴퓨터 시스템에서 연산된 퍼즐 입력은 수신 컴퓨터 시스템에서 재연산될 수 있다.

[0120] 방법(700)은 응답 문서 및 퍼즐 입력의 조합으로부터 연산된 검증 해시 값이 연산 퍼즐에 대한 해답을 지시하는 응답 값인지 여부를 결정하는 동작을 포함한다(동작 709). 동작(709)은 응답 문서 및 퍼즐 입력의 조합으로부터 연산된 검증 해시 값이 연산 퍼즐에 대한 해답을 지시하는 응답 값인지 여부를 결정하는 수신 컴퓨터 시스템을 포함할 수 있다. 예를 들어, 응답 검증 모듈(527) 및/또는 응답 검증 모듈(552)은 검증 해시 값이 해답을 지시하는지를 결정하기 위하여 일반 공식 H(응답 문서˚ 퍼즐 입력)를 사용할 수 있다. 검증 해시 값에 걸쳐 산재된 복수의 고정 비트 포지션(예를 들어, 최초 n비트)에서 특정된 값을 가질 때, 검증 해시 값은 해답을 지시할 수 있다.

[0121] 일정 실시예에서, 복수의 검증 해시 값은 복수의 응답 문서 및 퍼즐 입력의 조합으로부터 연산된다. 상기 실시예에서, 검증 해시 값이 최초 복수의 비트 포지션(예를 들어, 해시 값 프리픽스)에 특정된 값을 갖고 제2 복수의 비트 포지션(예를 들어, 해시 값 서픽스)에서의 다른 응답 문서로부터 발생한 다른 검증 해시 값과 동일한 값을 가질 때, 검증 해시 값은 해답을 지시할 수 있다.

[0122] 검증 해시 값이 연산 문제에 대한 해답일 때, 소비된 연산 리소스는 적어도 측정될 수 있다. 말하자면, 연산 퍼즐에 대한 검증 가능한 해답은 연산 퍼즐을 해결하기 위하여 송신 컴퓨터 시스템이 폭력적 접근으로 프로세서 사이클 및 메모리 리소스를 소비하는 수신 컴퓨터 시스템을 지시할 수 있다. 예를 들어, 검증 해시 값이 메시지 데이터(546)에 기초한 연산 퍼즐에 대한 해답일 때, 이것은 응답 검증 모듈(527) 및/또는 메시지 서버(516)가 프로세서 사이클을 소비하는 응답 검증 모듈(552)을 지시한다. 반면에, 검증 해시 값이 연산 문제에 대한 해답이 아닌 때, 이것은 송신 컴퓨터 시스템은 연산 퍼즐을 해결하기 위하여, 잠재적으로 프로세서 사이클을 폭력적 접근법으로 소비하지 않는다는 것을 가리킨다. 예를 들어, 검증 해시 값이 메시지 데이터(546)에 기초한 연산 퍼즐에 대한 해답이 아닌 경우, 이것은 메시지 서버(516)가 잠재적으로 프로세서 사이클을 소비하지 않는 응답 검증 모듈(527) 및/또는 응답 검증 모듈(552)을 가리킨다.

[0123] 방법(700)은 결정 결과를 메시지 분류 모듈에 제공하는 동작을 포함한다(동작 710). 동작(710)은 결정 결과를 메시지 분류 모듈에 제공하는 수신 컴퓨터 시스템을 포함할 수 있다. 예를 들어, 메시징 서버(517)는 (메시징 서버(516)가 프로세서 사이클을 소비했는지 아닌지를 지시하는) 메시징 서버(516)에 관한 결정 결과를 메시지 분류 모듈(529)에 제공할 수 있다. 메시징 서버(516)가 연산 리소스를 (단일하게 또는 다른 제공된 입력과 조합하여) 소비했다고 지시하는 결정을 제공하는데 기초하여, 메시지 분류 모듈(529)은 전자 메시지(545)를 정당한 것으로 분류할 수 있다. 반면에, 메시징 서버(516)가 잠재적으로 컴퓨터 리소스를 (단일하게 또는 다른 제공된 입력과 조합하여) 소비했다고 지시하는 결정을 제공하는데 기초하여, 메시지 분류 모듈(529)은 전자 메시지(545)를 불필요하거나 요청되지 않은 것으로 분류할 수 있다. 선택적으로, 그리고 적절한 때, 메시징 서버(517)는 메시징 서버(516)가 연산 리소스를 소비하였는지 또는 잠재적으로 소비하지 않았는지 지시하는 결과를 메시지 분류 모듈(553)에 제공할 수 있다.

[0124] 본 발명의 일정 실시예에서, 도메인이 특정된 ETPS를 지원하는 지시 또는 송신 컴퓨터 시스템이 연산 퍼즐을 해결했다는 지시는 전자 메시지가 정당하다는 충분한 증거를 제공한다. 예를 들어, 송신 엔티티는 재정적인 리소스 또는 ETP 인증서를 사용하려는 소망이 부족할 수 있다. 그러나 송신 엔티티는 여전히 전자 메시지가 정당하다고 수신컴퓨터 시스템에 지시하기를 원할 수 있다. 따라서, 송신 엔티티는 송신 컴퓨터 시스템을 설정하여, 연산 퍼즐에 대한 해답을 연산할 수 있고, 전자 메시지에서의 응답 문서를 포함할 수 있다.

[0125] 수신 컴퓨터 시스템은 송신 엔티티와 연관된 도메인용 ETP 인증서를 인식하려고 시도하도록 설정될 수 있다. 수신 컴퓨터 시스템은 어떠한 ETP 인증서도 인식되지 않을 때 연산 퍼즐에 대한 해답을 검증하도록 설정될 수 있다. 따라서, 수신 컴퓨터 시스템은 초기에 전자 메시지를 파싱하거나 송신 엔티티에 관련된 도메인에 대응하는 ETP 인증서용 네임 서버에 문의할 수 있다. 만약 ETP 인증서가 인식되고 ETP 인증서가 특정 ETPs용 지원을

지시하면, 특정 ETPs용 지원은 전자 메시지가 정당하다는 충분한 증거가 될 수 있다. 그러나, 만약 어떠한 ETP 인증서도 인식되지 않거나 인식된 ETP 인증서가 특정 ETPs용 지원을 지시하지 않는다면, 그 후에 수신 컴퓨터 시스템은 연산 퍼즐에 대한 포함된 해답을 검증하도록 시도할 수 있다.

[0126] 스키마는 전자 메시징 정보의 의미를 제한하기 위하여 사용될 수 있다. 다음 예시 XML 스키마는 도메인에 관한 전자 메시징 정보의 의미를 제한하기 위하여 사용될 수 있다.

[0127]

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://lessspam.org/1" xmlns="http://lessspam.org/1"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified" blockDefault="#all">
  <xs:element name="emailPolicy">
    <xs:complexType>

      <xs:sequence>
        <xs:element name="inbound" minOccurs="0">
          <xs:annotation>
            <xs:documentation>Policies regarding mail that is received by the entity.
            </xs:documentation>
          </xs:annotation>
          <xs:complexType>
            <xs:choice minOccurs="0" maxOccurs="unbounded">
              <xs:element name="hashedSpam">
                <xs:complexType>
                  <xs:attribute name="minDifficulty" type="xs:nonNegativeInteger">
                    <xs:annotation>
                      <xs:documentation>The minimum acceptable level of difficulty
in
                        the puzzle solution.
                      </xs:documentation>
                    </xs:annotation>
                  </xs:attribute>
                  <xs:attribute name="maxIntervalWidth" type="xs:duration">
                    <xs:annotation>
                      <xs:documentation>The maximum acceptable width of the time
                        interval parameter of the puzzle.
                      </xs:documentation>
                    </xs:annotation>
                  </xs:attribute>
                  <xs:attribute name="dateRequired" type="xs:boolean"
default="false">
                    <xs:annotation>
                      <xs:documentation>Whether a the inclusion of a date parameter
is
                        required (it is always acceptable if present).
                      </xs:documentation>
```

[0128]

```
                </xs:annotation>
              </xs:attribute>
              <xs:attribute name="subjectRequired" type="xs:boolean"
                    default="false">
                <xs:annotation>
                  <xs:documentation>Whether a the inclusion of a subject
parameter
                    is required (it is always acceptable if present).
                  </xs:documentation>
                </xs:annotation>
              </xs:attribute>
              <xs:anyAttribute namespace="##other" processContents="lax"/>
            </xs:complexType>
          </xs:element>
          <xs:any namespace="##other" processContents="lax"/>
        </xs:choice>
      </xs:complexType>
    </xs:element>
    <xs:element name="outbound" minOccurs="0">
      <xs:annotation>
        <xs:documentation>Policies regarding mail that is sent from the entity.
        </xs:documentation>
      </xs:annotation>
      <xs:complexType>
        <xs:choice minOccurs="0" maxOccurs="unbounded">
          <xs:element name="mailServer">
            <xs:annotation>
              <xs:documentation>One group of outbound mail servers. The
                  usesEnhancedSMTPNoop attribute, if present indicates their
known
                  behaviour with respect to that feature.
              </xs:documentation>
```

[0129]

```
        </xs:annotation>
        <xs:complexType>
          <xs:choice minOccurs="0">
            <xs:element name="indirect" type="xs:string">
              <xs:annotation>
                <xs:documentation>An indirection to another domain.
                </xs:documentation>
              </xs:annotation>
            </xs:element>
            <xs:choice maxOccurs="unbounded">
              <xs:element name="address" type="xs:string"/>
              <xs:element name="addressV6" type="xs:string"/>
              <xs:element name="addressRange" type="xs:string"/>
            </xs:choice>
          </xs:choice>
          <xs:attribute name="usesEnhancedSmtpNoop" type="xs:boolean"
                use="optional"/>
          <xs:attribute name="allMailIsETPSigned" type="xs:boolean"
                use="optional"/>
          <xs:anyAttribute namespace="##other" processContents="lax"/>
        </xs:complexType>
      </xs:element>
      <xs:any namespace="##other" processContents="lax"/>
    </xs:choice>
  </xs:complexType>
</xs:element>
<xs:element name="otherInfo" minOccurs="0">
  <xs:annotation>
    <xs:documentation>General other information regarding the entity, such

        certificates that may pertain to it.
      </xs:documentation>
```

[0130]

```
        </xs:annotation>
        <xs:complexType>
          <xs:choice minOccurs="0" maxOccurs="unbounded">
            <xs:element name="x509Certificate" type="xs:base64Binary"/>
            <xs:any namespace="##other" processContents="lax"/>
          </xs:choice>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
    <xs:anyAttribute namespace="##other" processContents="lax"/>
  </xs:complexType>
 </xs:element>
 <xs:element name="ocspResponse" type="xs:base64Binary">
  <xs:annotation>
   <xs:documentation>Base64 encoding of an RFC2560 OCSPResponse.
   </xs:documentation>
  </xs:annotation>
 </xs:element>
</xs:schema>
```

[0131]

[0132] 스키마의 사용은 개발자가 전자 메시징 구성 정보를 처리하는 어플리케이션을 재설계할 필요 없이 전자 메시징 구성 정보가 구조화되는 방법을 유연하게 정의(또는 재정의)하도록 한다. TXT 레코드는 예시 XML 스키마에 의하여 제한되는 XML 명령어를 저장하도록 사용될 수 있다. XML 명령어는 동일한 DNS 레코드 집합에서 복수의 TXT 레코드를 분포시키고, DNS 레코드 집합을 수신하는 컴퓨터 시스템에서 XML 인스턴스로 어셈블링 될 수 있다. 예를 들어, 각각의 TXT 레코드는 복수의 TXT 레코드에 유일한 음아닌 정수의 4자리 10진수 표현(필요한 만큼의 선행하는 0을 가짐)을 포함하는 4개의 문자로 시작한다. 수신할 때, TXT 레코드는 10진수 숫자에 의하여 정렬된다. 최초 4문자(10진수)는 각각의 TXT 레코드로부터 제거되고 결과는 단일 인접 문자 시퀀스(XML 인스턴스)를 형성하기 위하여 함께 연관된다.

[0133] 다음은 도메인용 XML 정책 문서를 도시하는 예시 DNS 설정 파일 단락이다.

```
_emailPolicy TXT ("0002T0H45M0S'/>"
                  "    <hashedSpam minDifficulty='13'
                       maxIntervalWidth='P0Y0M7DT0H0M0S'"
                  "    dateRequired='true' subjectRequired='true'/>"
                  "  </inbound>"
                  "</emailPolicy>" )
          TXT ("0001<emailPolicy xmlns='http://lessspam.org/1'>"
                  "  <inbound>"
                  "    <hashedSpam minDifficulty='13' maxIntervalWidth='P0Y0M0D" )
```

[0134]

[0135] 예시 DNS 설정 파일 단락은 두 TXT 레코드를 포함하는데, 하나는 문자 시퀀스 "0002"를 포함하고, 다른 하나는 문자 시퀀스 "0001"를 포함한다. 문자 시퀀스는 TXT 레코드에 포함된 XML 명령어용으로 적절한 순서를 결정하기 위하여 수신 컴퓨터 시스템에서 사용된다. 그러나, 당업자에게 있어, 상기 설명을 검토한 후, 다른 정렬 메카니즘이 사용될 수 있고, DNS 설정 파일은 추가적 TXT 레코드를 포함할 수 있다는 것은 명백하다. 두 텍스트 레코드는 컴퓨터 시스템에서 (예를 들어 DNS 문의에 응답하여) 수신될 수 있고, TXT 레코드의 일부는 XML 인스턴스로 연관될 수 있다. XML 인스턴스를 복수의 TXT 레코드에 대하여 스패닝하는 것은 전자 메시징 구성 정보의 (2000 문자를 초과하는) 증가된 총량이 전달되도록 허용한다. 또한, XML 인스턴스의 다른 일부가 동일한 DNS 레코드 집합에 포함될 수 있으므로, 다른 일부는 단일 DNS 문의로 검색될 수 있다.

[0136] 예시적 DNS 설정 파일 단락 또는 다른 DNS 설정 파일 단락은 DNS 서브 도메인(예를 들어, 이메일 정책 서브도메인)에 포함될 수 있다. 따라서, 전자 메시징 구성 정보(예를 들어, 예시적 DNS 설정 파일 단락의 TXT 레코드)를 포함하는 하나 이상의 TXT 레코드는 특정 DNS 서브 도메인 내에서의 모든 레코드일 수 있다. 따라서, (다른 서

브도메인에서의) 현존하는 TXT 레코드의 사용과의 충돌 또는 모순이 감소할 수 있다.

[0137] 다음은 예시적 DNS 설정 파일 단락의 일부를 연관시킬 수 있는 예시적 XML 인스턴스이다.

```
<?xml version="1.0" encoding="UTF-8"?>
<emailPolicy xmlns="http://lessspam.org/1">
    <inbound>
        <hashedSpam minDifficulty="13"
maxIntervalWidth="P0Y0M0DT0H45M0S"/>
        <hashedSpam minDifficulty="29"
maxIntervalWidth="P0Y0M7DT0H0M0S"
                dateRequired="true" subjectRequired="true"/>
    </inbound>
</emailPolicy>
```

[0138]

[0139] 예시적 XML 인스턴스는 예시적 XML 스키마에 따라 제한되는 이메일 정책 요소를 포함한다. 예시적 XML 인스턴스는 해시된 스팸(HashedSpam) 연산 퍼즐에 관한 두 인바운드 정책을 표현한다. 제1 인바운드 정책은 적어도 13개의 0 비트를 가지는 퍼즐 해답과 지속적인 45분 이하의 시간 간격 파라미터가 수락 가능하다고 지시한다. 제2 인바운드 정책은 적어도 29개의 0 비트를 갖는 퍼즐 해답과 지속적인 일주일 이하의 시간 간격 파라미터가 또한 수락 가능하다고 지시한다.

[0140] 다른 XML 인스턴스 및 예시적 XML 인스턴스의 일부는 도메인 또는 전자 메시징 서버와 연관된 전자 메시징 구성 정보를 전달하기 위하여 네임 서버에서의 TXT 레코드에 포함될 수 있다. 예를 들어, 이러한 XML 인스턴스는 변경된 접속 설정 데이터, 인가된 아웃고잉 메일 서버, ETP 인증서에 대한 참조를 지원하고 연산 퍼즐을 지원한다. TXT 레코드에서 XML 인스턴스의 일부를 포함하는 것은 또한 클라이언트 및/또는 서버 DNS 소프트웨어가 업데이트되어야 할 필요 없이 새로운 형식의 전자 메시징 정보가 DNS에 추가되도록 허용한다.

[0141] 네임 서버는 전자 메시징 구성 정보를 리턴할 때 시퀀스 숫자를 요구하는 프로토콜을 사용하여 명시적으로 설정될 수 있다. 따라서, 네임 서버를 위장하려는 어떠한 시도도 네임 서버에 의하여 사용된 시퀀스 숫자를 추측해야 하는 추가적인 부담을 갖게 된다. 예를 들어, 네임 서버는 UDP에 대항하여 TCP를 통해 전자 메시징 구성 정보를 리턴하도록 명시적으로 설정될 수 있다. 따라서, 네임 서버를 위장하려는 어떠한 시도도 네임 서버에 의하여 사용되는 적절한 TCP/IP 시퀀스 숫자를 추측하도록 요구될 것이다. 일정 실시예에서, 시퀀스 숫자를 요구하는 프로토콜의 사용은 리턴된 전자 메시징 구성 정보의 길이로부터 발생할 수 있다. 예를 들어, XML 인스턴스가 512 바이트 보다 클 때, TCP의 사용은 자동적으로 발생할 수 있다.

[0142] 전자 메시지 송신자는 불필요하고 요청되지 않은 전자 메시지를 감소시키기 위한 복수의 메카니즘을 사용하여 설정된다. 따라서, 전자 메시지 송신자는 전자 메시지를 송신할 때, 하나, 일부 또는 전부의 설정된 메카니즘을 선택할 수 있다. 마찬가지로, 전자 메시지 수신자는 불필요하고 요청되지 않은 전자 메시지를 감소시키기 위하여 복수의 메카니즘을 사용하도록 설정될 수 있다. 따라서, 전자 메시지 수신자는 전자 메시지를 송신할 때, 하나, 일부 또는 전부의 설정된 메카니즘을 선택할 수 있다. 그러나 전자 메시지 송신자에서 설정된 메카니즘은 전자 메시지 송신자에서 설정된 메카니즘과 다를 수 있다.

[0143] 따라서, 전자 메시지 송신자 및 수신자는 불필요하고 요청되지 않은 전자 메시지용으로 상호 설정된 메카니즘에 일치할 수 있다. 따라서, 다른 설정된 메카니즘에서 발생한 결과의 조합이 메시지 분류 모듈에 제공될 수 있다. 예를 들어, 전자 메시지 수신자는 ETP의 준수 및 전자 메시지 송신자에 의한 노력의 증거 모두를 조사할 수 있고, 메시지 분류 모듈에 두 체크의 결과 모두를 제공할 수 있다. 노력의 증거는 해시 충돌, 암호화 문제에 대한 해답, 메모리 범위 문제에 관한 해답, 역전환 테스트에 대한 해답을 제공하는 것을 포함할 수 있다. 수신 도메인은 제공된 노력의 증거를 검사하고 검사 결과를 메시지 분류 모듈에 제공할 수 있다.

[0144] 상기 설명 및 후술하는 클레임에서, "스키마'는 복수의 컴퓨터 시스템이 표현되고 공유된 어휘에 따라 문서를 처리하도록 허용하는 복수의 컴퓨터 시스템 간의 공유 어휘 표현으로 정의된다. 예를 들어, XML 스키마는 XML 스키마 언어의 스키마 구조를 사용하는 XML 문서 클래스를 정의하고 설명할 수 있다. 이 스키마 구조는 의미, 사용법, 데이터 형간의 관계, 요소 및 그 내용, 속성 및 그 값, 엔티티 및 그 내용, XML 문서에서 사용되는 기호를 제한하고 문서화하기 위하여 사용될 수 있다. 따라서, XML 스키마에 액세스할 수 있는 임의의 컴퓨터 시스템은 XML 스키마에 따라 XML 문서를 처리할 수 있다. 또한, XML 스키마에 접근할 수 있는 임의의 컴퓨터 시

스템은 XML 스키마에 접근할 수 있는 다른 컴퓨터 시스템에 의하여 사용되기 위한 XML 문서를 구성하거나 수정할 수 있다.

[0145] 원하는 기능에 의하여, 잠재적으로 전자 메시지에 포함된 메시지 데이터에 따라, 하나 이상의 복수의 상이한 생성 입력이 메시지 분류 모듈에 제공될 수 있다. 수신된 입력에 기초하여, 메시지 분류 모듈은 전자 메시지를 정당하다고 또는 불필요하거나 요청되지 않았다고 분류할 수 있다. 복수의 입력(전자 메시지의 전송과 연관된 다른 정보를 표시하는 각각의 입력)이 사용될 때, 메시지 분류 모듈은 보다 신뢰성 있게, 예를 들어 전자 메시지를 보다 신뢰성 있게 불필요하거나 요청되지 않은 것으로 분류하는 것처럼, 전자 메시지를 분류할 수 있다.

[0146] 당업자는 본 발명이 PC, 랩탑 컴퓨터, 핸드 헬드 장치, 멀티 프로세서 시스템, 마이크로프로세서-기반 또는 프로그래머블 가전 제품(programmable consumer electronics), 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터, 이동 전화, PDA, 페이저 등을 포함하는 다양한 유형의 컴퓨터 시스템을 갖는 네트워크 컴퓨팅 환경에서 구현도리 수 있다는 것을 이해할 것이다. 또한, 본 발명은, 네트워크를 통하여 (하드웨어적 데이터 링크, 무선 데이터 링크 또는 하드웨어적 및 무선 데이터 링크의 조합에 의하여) 링크된 로컬 및 원격 컴퓨터 시스템이 작업을 수행하는 분산형 컴퓨팅 환경(distributed computing environment)에서도 실시될 수 있다. 분산형 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치에 위치할 수 있다.

[0147] 도 8 및 다음의 설명은 본 발명이 구현될 수 있는 적합한 컴퓨팅 환경에 대한 일반적인 설명을 간략하게 제공한다. 필요한 것은 아니지만, 본 발명은 프로그램 모듈(program module)과 같은 컴퓨터 시스템에 의하여 실행되는 컴퓨터 실행 가능 명령어와 일반적으로 관련하여 설명된다. 일반적으로, 프로그램 모듈은, 특정 작업(task)을 수행하거나 특정 추상 데이터 유형(abstract data type)을 구현하는 루틴(routine), 프로그램, 객체, 콤포넌트(component), 데이터 구조(data structure) 등을 포함한다. 컴퓨터 실행 가능 명령어, 관련된 데이터 구조 및 프로그램 모듈은 여기에 개시된 방법의 동작을 실행하기 위한 프로그램 코드 수단의 예시를 표현한다.

[0148] 도 8을 참조하면, 본 발명을 구현하기 위한 예시적 시스템은 컴퓨터 시스템(820)의 형태인 범용 컴퓨팅 장치를 포함하는데, 이 범용 컴퓨터는 처리 장치(processing unit; 821), 시스템 메모리(822), 및 시스템 메모리를 포함하는 다양한 시스템 콤포넌트를 처리 장치(821)에 연결하는 시스템 버스(823)를 포함한다. 프로세싱 유닛(821)은 본 발명의 특징을 포함하는 컴퓨터 시스템(820)의 특징을 구현하기 위하여 설계된 컴퓨터 실행 가능 명령어를 실행할 수 있다. 시스템 버스(823)는 메모리 버스 또는 메모리 제어기, 주변 장치 버스, 및 다양한 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스를 포함하는 여러 유형의 버스 구조 중 임의의 것일 수 있다. 시스템 메모리는 ROM(read-only memory; 824) 및 RAM(random access memory; 825)을 포함한다. 기동(start-up) 동안과 같이 컴퓨터 시스템(820) 내의 소자들간의 정보 전달을 돕는 기본적인 루틴을 포함하는 기본 입/출력 시스템(BIOS; 826)은 ROM(824)에 저장된다.

[0149] 컴퓨터 시스템(820)은, 자기 하드디스크(839)로부터 판독하고 그것에 기록하기 위한 자기 하드디스크 드라이브(827), 착탈식 자기 디스크(removable magnetic disk; 829)로부터 판독하거나 그것에 기록하기 위한 자기 디스크 드라이브(828), 및 CD-ROM 또는 다른 광 매체와 같은 착탈식 광 디스크(831)로부터 판독하거나 그것에 기록하기 위한 광 디스크 드라이브(830)를 더 포함할 수 있다. 자기 하드디스크 드라이브(827), 자기 디스크 드라이브(828) 및 광 디스크 드라이브(830)는, 각각 하드디스크 드라이브 인터페이스(832), 자기 디스크 드라이브 인터페이스(833) 및 광 드라이브 인터페이스(834)에 의하여 시스템 버스(823)에 접속된다. 드라이브 및 이것과 연관된 컴퓨터 판독 가능 매체는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 및 컴퓨터 시스템(820)를 위한 다른 데이터를 비휘발적으로 저장한다. 예시 환경이 여기에서 자기 하드 디스크(839)를 사용하고 있지만 착탈식 자기 디스크(829) 및 착탈식 광 디스크(831) 및 데이터를 저장하기 위한 컴퓨터 판독 가능한 다른 유형의 매체가 사용될 수 있는데, 이러한 다른 유형의 매체는 자기 카세트, 플래시 메모리 카드, 디지털 비디오 디스크, 베르누이 카트리지(Bernoulli cartridge), RAM, ROM 등을 포함한다.

[0150] 운영 체제(835), 하나 이상의 응용 프로그램(836), 다른 프로그램 모듈(837) 및 프로그램 데이터(838)를 포함하는 하나 이상의 프로그램 모듈을 포함하는 프로그램 코드 수단은 하드디스크(839), 자기 디스크(829), 광 디스크(831), ROM(824) 또는 RAM(825) 상에 저장될 수 있다. 사용자는 키보드(840), 포인팅 장치(pointing device; 842) 또는 마이크로폰, 조이스틱, 게임 패드, 위성 디스크(satellite disk), 스캐너 등과 같은 다른 입력 장치(도시되지 않음)를 통하여 컴퓨터 시스템(820)에 명령어 및 정보를 입력할 수 있다. 이들 및 다른 입력 장치는 흔히 시스템 버스(823)에 연결된 입력/출력 인터페이스(846)를 통하여 처리 장치(821)에 접속될 수 있다. 입력/출력 인터페이스(846)는 논리적으로 시리얼 포트 인터페이스, PS/2 인터페이스, 패러럴 포트 인터페이스, USB 인터페이스, IEEE 1394 인터페이스(예를 들어 FireWire 인터페이스)와 같은 다양한 범위의 다른 인

터페이스를 나타내거나, 다른 인터페이스의 조합을 나타낼 수 있다.

[0151] 모니터(847) 또는 다른 유형의 디스플레이 장치도 비디오 인터페이스(848)를 통하여 시스템 버스(823)에 접속된다. 스피커(869) 및 다른 오디오 출력 장치도 오디오 인터페이스(849)를 통하여 시스템 버스(823)에 연결된다. 예를 들어 프린터와 같은 다른 주변 장치(도시되지 않음)도 컴퓨터 시스템(820)에 연결될 수 있다.

[0152] 컴퓨터 시스템(820)은 예를 들어 사무실 기반 또는 기업 기반 컴퓨터 네트워크, 홈 네트워크, 인트라 넷 및/또는 인터넷과 같은 네트워크에 연결 가능하다. 컴퓨터 시스템(820)은 원격 컴퓨터 시스템, 원격 어플리케이션 및/또는 이러한 네트워크에 걸친 원격 데이터 베이스와 같은 외부 소스와 데이터를 교환할 수 있다. 예를 들어, 컴퓨터 시스템(820)은 컴퓨터 시스템(820)을 구비한 공유 네트워크에 연결된 다른 컴퓨터 시스템과 전자 메시지를 교환할 수 있다.

[0153] 컴퓨터 시스템(820)은, 컴퓨터 시스템(820)이 외부 소스로부터 데이터를 수신하고 외부 소스로 데이터를 전송하는 네트워크 인터페이스(853)를 포함한다. 도 8을 참조하면, 네트워크 인터페이스(853)는 링크(851)를 통하여 원격 컴퓨터 시스템(883)과의 데이터 교환을 용이하게 한다. 네트워크 인터페이스(853)는 예를 들어 네트워크 인터페이스 및 대응하는 네트워크 드라이버 인터페이스 명세 스택(Network Driver Interface Specification stack)과 같은 하나 이상의 소프트웨어 및/또는 하드웨어 모듈을 논리적으로 표현한다. 데이터 링크 (851)는 예를 들어 이더넷 세그먼트와 같은 네트워크의 일부를 표현하고, 원격 컴퓨터 시스템(883)은 네트워크의 노드를 표현한다. 예를 들어, 원격 컴퓨터 시스템(883)은 DNS 문의를 컴퓨터 시스템(820)으로 전송하는 문의 컴퓨터 시스템일 수 있다. 반면에, 원격 컴퓨터 시스템(883)은 수신 DNS 문의에 대응하여 DNS 해답을 컴퓨터 시스템(820)으로 전송하는 DNS 서버일 수 있다.

[0154] 마찬가지로, 컴퓨터 시스템(820)은, 컴퓨터 시스템(820)이 외부 소스로부터 데이터를 수신하고 외부 소스로 데이터를 전송하는 입/출력 인터페이스(846)를 포함한다. 입/출력 인터페이스(846)는 예를 들어, 표준 모뎀, 케이블 모뎀, DSL 모뎀과 같은 모뎀(554)에, 컴퓨터 시스템(820)이 외부 소스로부터 데이터를 수신하고 외부 소스로 데이터를 전송하는 데이터 링크(859)를 통하여 연결된다. 도 8을 참조하면, 입/출력 인터페이스(846) 및 모뎀(854)은 링크(852)를 통하여 원격 컴퓨터 시스템(893)과의 데이터 교환을 용이하게 한다. 링크(852)는 네트워크의 일부를 표현하고, 원격 컴퓨터 시스템(893)은 네트워크의 노드를 표현한다. 예를 들어, 원격 컴퓨터 시스템(893)은 전자 메시지를 컴퓨터 시스템(820)에 송신하는 송신 컴퓨터 시스템일 수 있다. 반면에, 원격 컴퓨터 시스템(893)은 컴퓨터 시스템(820)으로부터 전자 메일 메시지를 수신하는 수신 컴퓨터 시스템일 수 있다.

[0155] 도 8은 본 발명에 대한 적합한 운영 환경을 표현하는데, 본 발명의 원리는 이를 구현할 수 있는 임의의 시스템에서, 필요하다면 적합한 수정을 가하여, 사용될 수 있다. 도 8에 도시된 환경은 단지 예시적이며, 본 발명의 원리가 구현될 수 있는 다양한 환경의 매우 작은 일부에 불과한 것이다.

[0156] 본 발명은 그 원칙이나 주요 특성에서 벗어나지 않는 다른 상세한 형태로 구현될 수 있다. 설명된 실시예는 예시적 측면으로만 고려된 것이며 제한적인 것이 아니다. 따라서 본 발명의 범위는 전술한 설명보다는 첨부된 청구항에 의하여 지시된다. 청구항과 그 의미 및 범위가 등가인 모든 변화는 청구항의 범위에 포함될 것이다.

발명의 효과

[0157] 본 발명은 메시지 분류 모듈에 제공될 수 있는 입력 생성을 제공하여, 불필요하거나 요청되지 않은 전자 메시지를 보다 신뢰성 있게 분류하는 것을 촉진한다.

도면의 간단한 설명

[0158] 도 1은 본 발명의 원리에 따라 접속 도용(connection hijacking)의 감소를 용이하게 하는 네트워크 아키텍처의 예를 도시하는 도면.

도 2는 본 발명의 원리에 따라 접속 도용을 감소시키는 방법의 예시적인 흐름도.

도 3은 본 발명에 따라 인가된 발신 메시징 서버의 식별을 용이하게 하는 네트워크 아키텍처의 예를 도시하는 도면.

도 4는 본 발명에 따라 인가된 발신 메시징 서버를 식별하는 방법의 예시적인 흐름도.

도 5는 본 발명에 따라 송신 도메인의 전자 메시지 전송 정책(sending domain's electronic message transmission policies)을 결정하고 연산 퍼즐(computational puzzle)에 대한 해답을 확인하는 것을 용이하게

하는 네트워크 아키텍처의 예를 도시하는 도면.

도 6은 본 발명에 따라 송신 도메인의 전자 메시지 전송 정책을 결정하는 방법의 예시적인 흐름도.

도 7은 본 발명에 따라 연산 퍼즐에 대한 해답을 확인하는 방법의 예시적인 흐름도.

도 8은 본 발명의 원리에 대하여 적절한 운영 환경을 도시하는 도면.

부호의 설명

< 도면의 주요 부분에 대한 부호 설명 >

107 송신 메시징 서버

108 네임 서버

109 수신 메시징 서버

112 주소

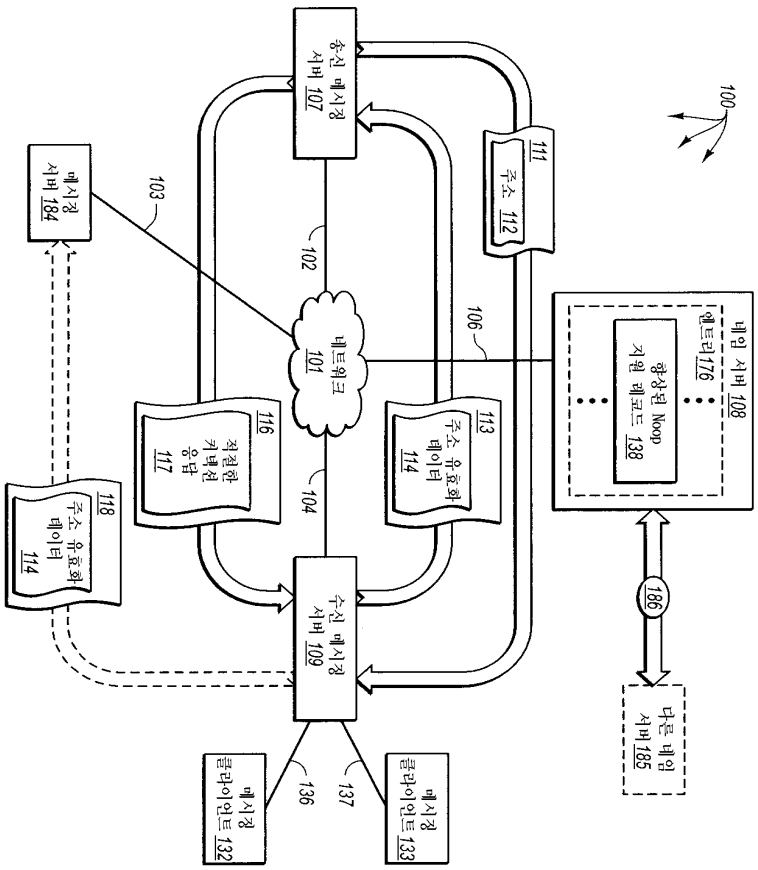
113 주소 검증 데이터

132 메시징 클라이언트

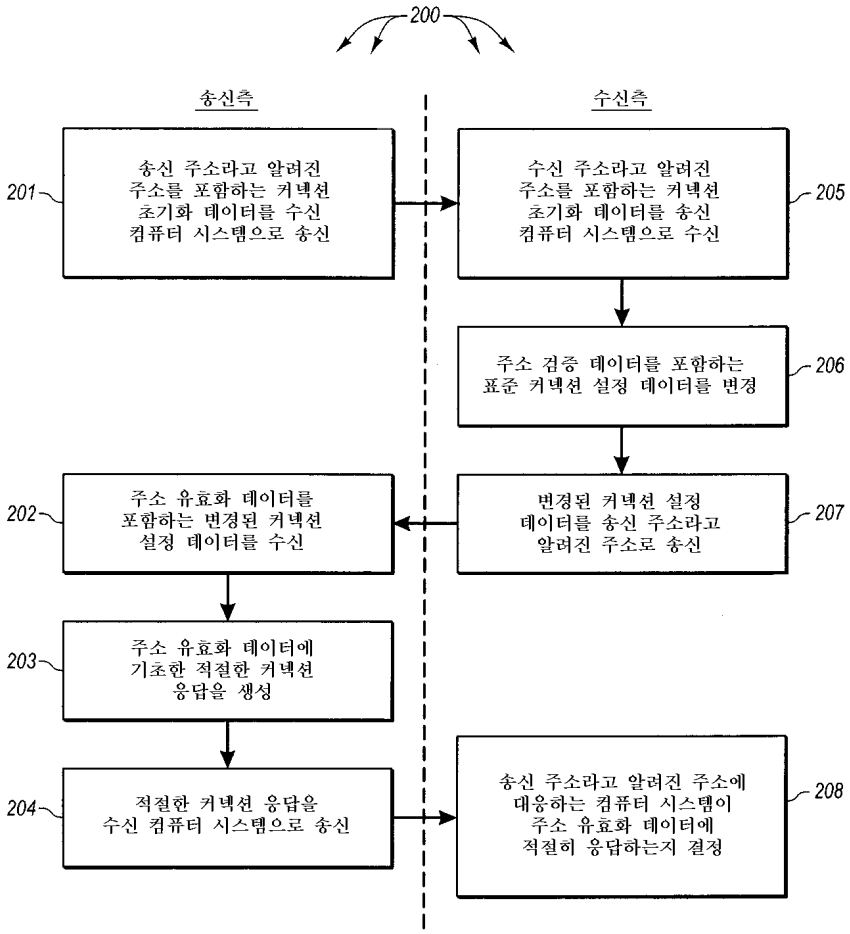
176 엔트리

도면

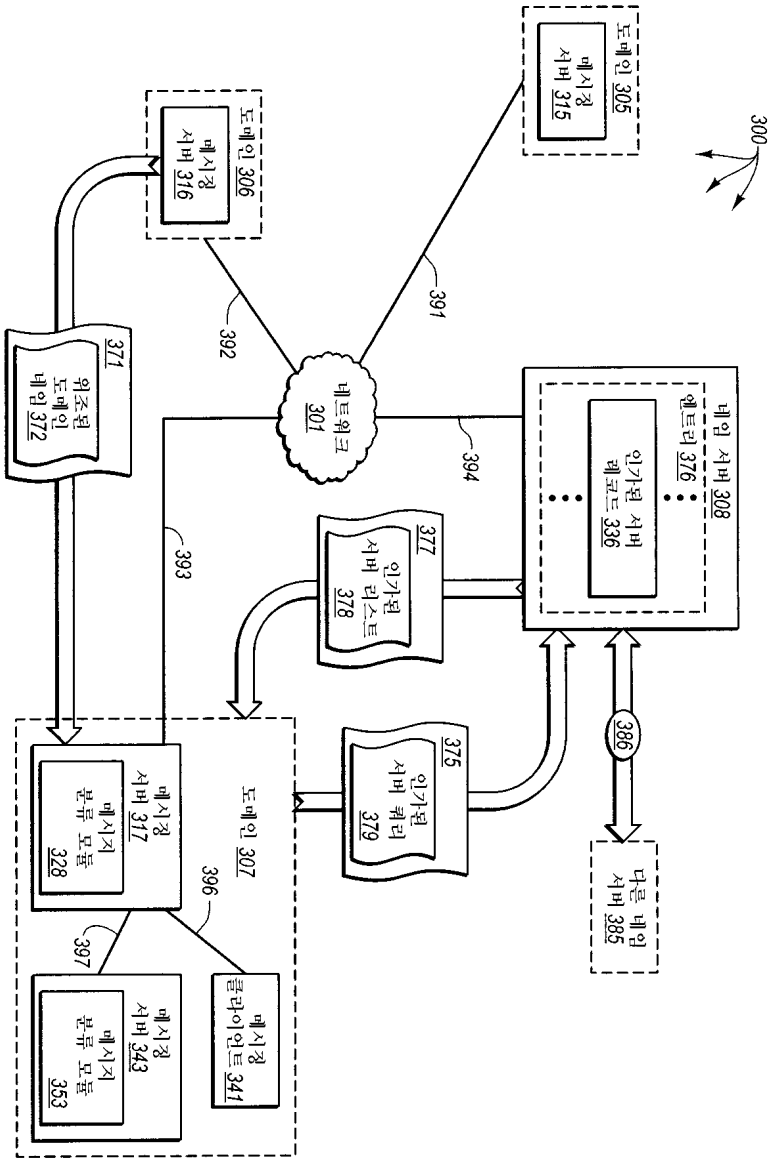
도면1



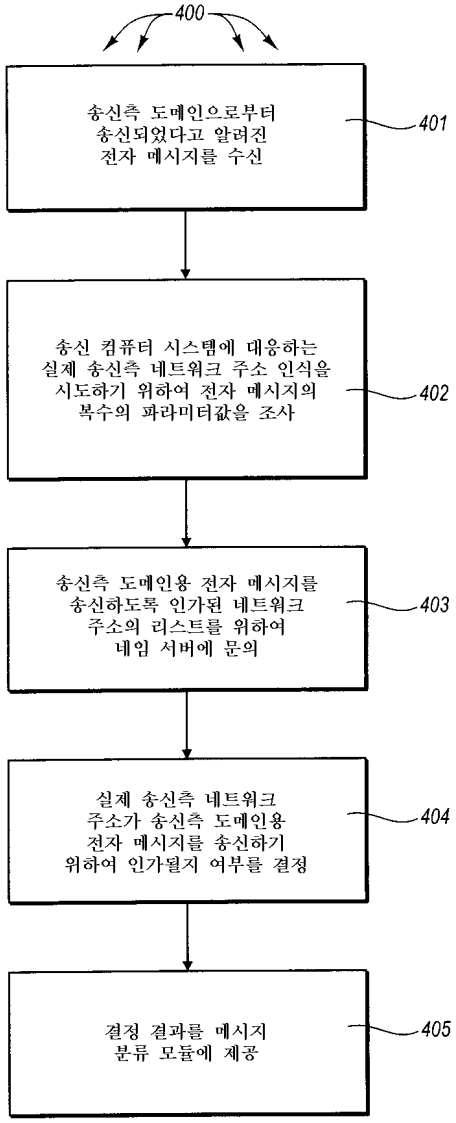
도면2


200
송신측
수신측
송신 주소라고 알려진 주소를 포함하는 커넥션 초기화 데이터를 수신 컴퓨터 시스템으로 송신
201
수신 주소라고 알려진 주소를 포함하는 커넥션 초기화 데이터를 송신 컴퓨터 시스템으로 수신
205
주소 검증 데이터를 포함하는 표준 커넥션 설정 데이터를 변경
206
변경된 커넥션 설정 데이터를 송신 주소라고 알려진 주소로 송신
207
주소 유효화 데이터를 포함하는 변경된 커넥션 설정 데이터를 수신
202
주소 유효화 데이터에 기초한 적절한 커넥션 응답을 생성
203
적절한 커넥션 응답을 수신 컴퓨터 시스템으로 송신
204
송신 주소라고 알려진 주소에 대응하는 컴퓨터 시스템이 주소 유효화 데이터에 적절히 응답하는지 결정
208

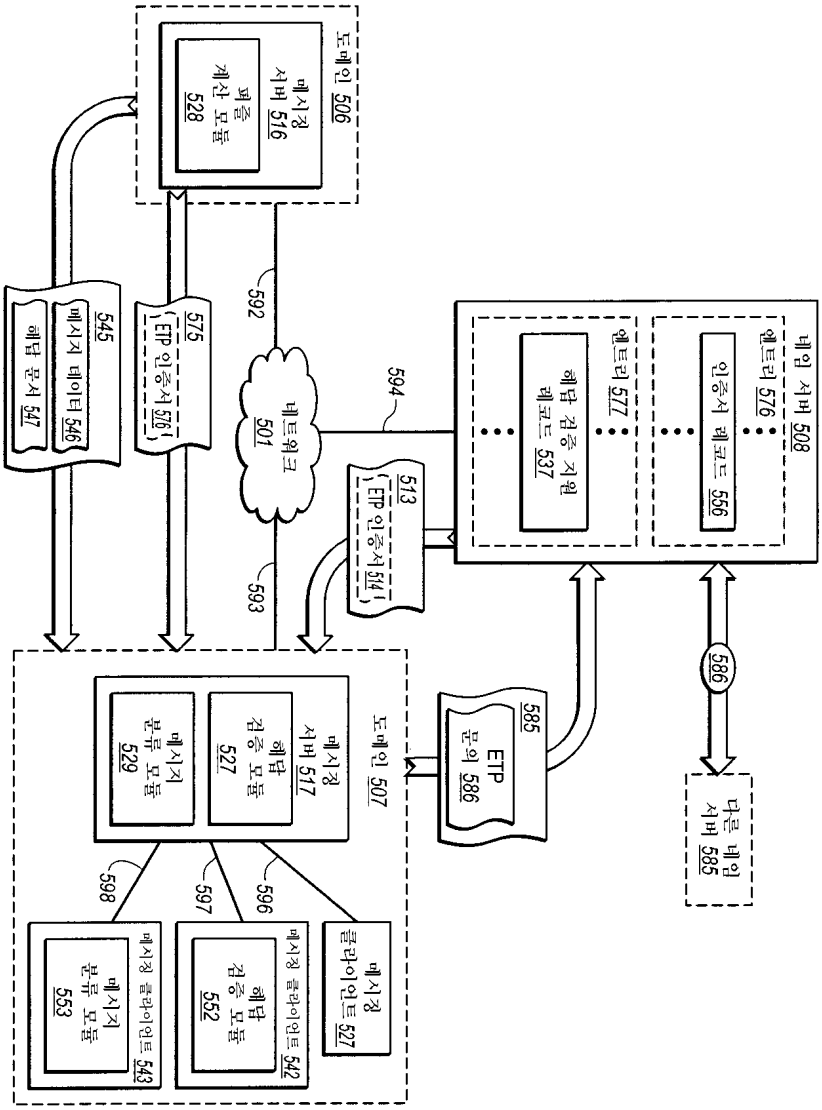
도면3


300
도메인 305
메시징 서버 315
도메인 306
메시징 서버 316
391
392
네트워크 301
네임 서버 308
엔트리 376
인가된 서버 레코드 336
394
371
위조된 도메인 네임 372
393
377
인가된 서버 리스트 378
375
인가된 서버 쿼리 379
386
다른 네임 서버 385
도메인 307
메시징 서버 317
메시지 분류 모듈 328
396
397
메시징 서버 343
메시지 분류 모듈 353
메시징 클라이언트 341

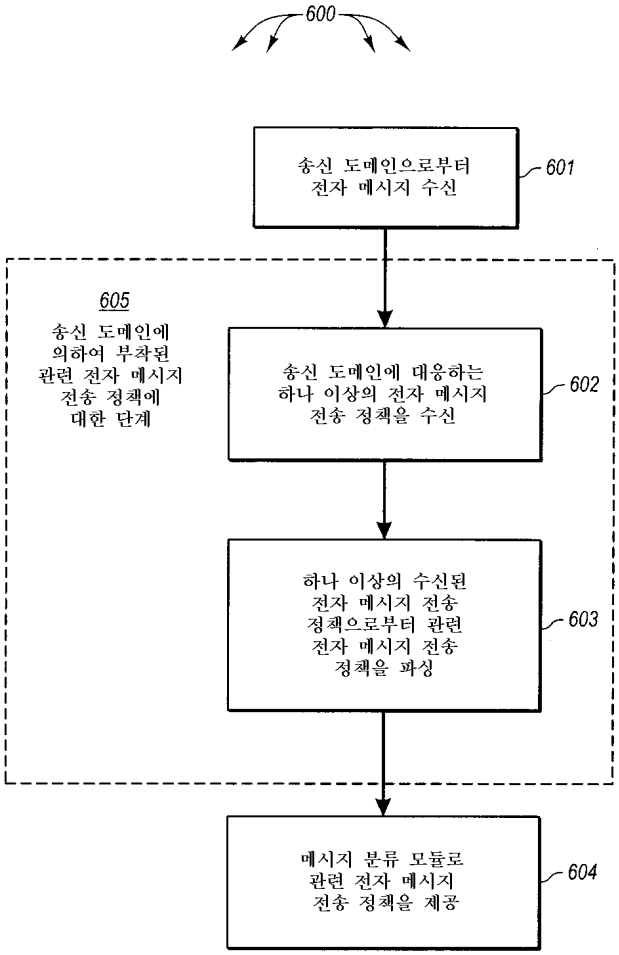
도면4


400
송신측 도메인으로부터 송신되었다고 알려진 전자 메시지를 수신
401
송신 컴퓨터 시스템에 대응하는 실제 송신측 네트워크 주소 인식을 시도하기 위하여 전자 메시지의 복수의 파라미터값을 조사
402
송신측 도메인용 전자 메시지를 송신하도록 인가된 네트워크 주소의 리스트를 위하여 네임 서버에 문의
403
실제 송신측 네트워크 주소가 송신측 도메인용 전자 메시지를 송신하기 위하여 인가될지 여부를 결정
404
결정 결과를 메시지 분류 모듈에 제공
405

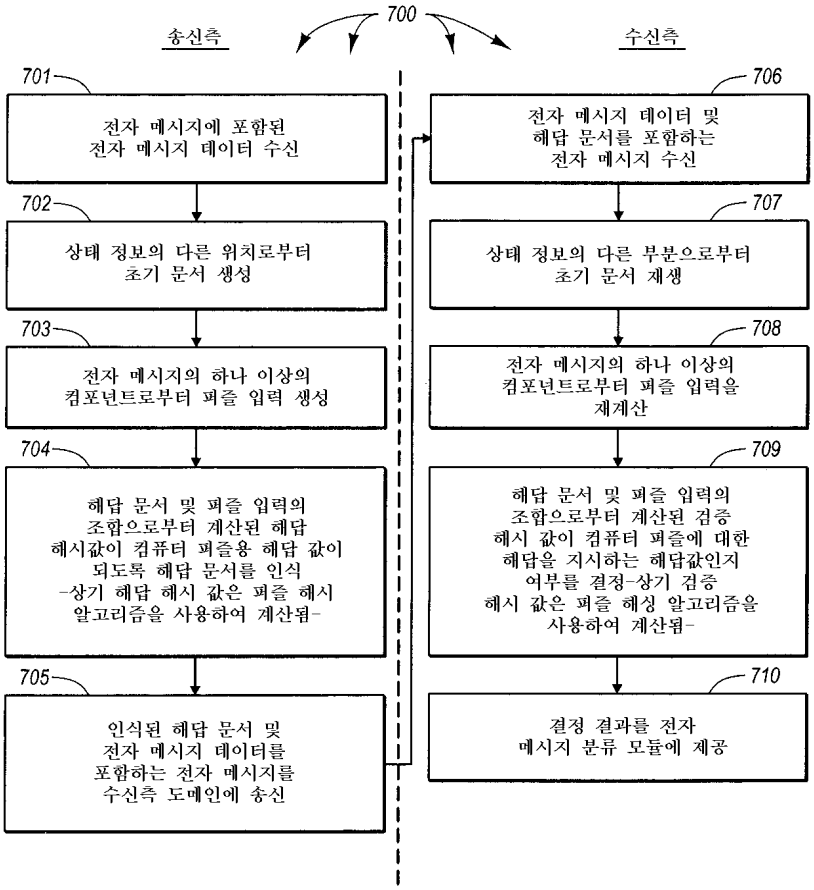
도면5


도메인 506
메시징 서버 516
폐쇄 계산 모듈 528
592
네트워크 501
593
594
575 { ETP 인증서 576 }
545
메시지 데이터 546
헤답 문서 547
513 { ETP 인증서 514 }
네임 서버 508
엔트리 576
인증서 레코드 566
엔트리 577
헤답 검증 지원 레코드 537
586
585
ETP 문의 586
다른 네임 서버 585
도메인 507
메시징 서버 517
헤답 검증 모듈 527
메시지 분류 모듈 529
598
597
596
메시징 클라이언트 527
메시징 클라이언트 542
헤답 검증 모듈 552
메시징 클라이언트 543
메시지 분류 모듈 553

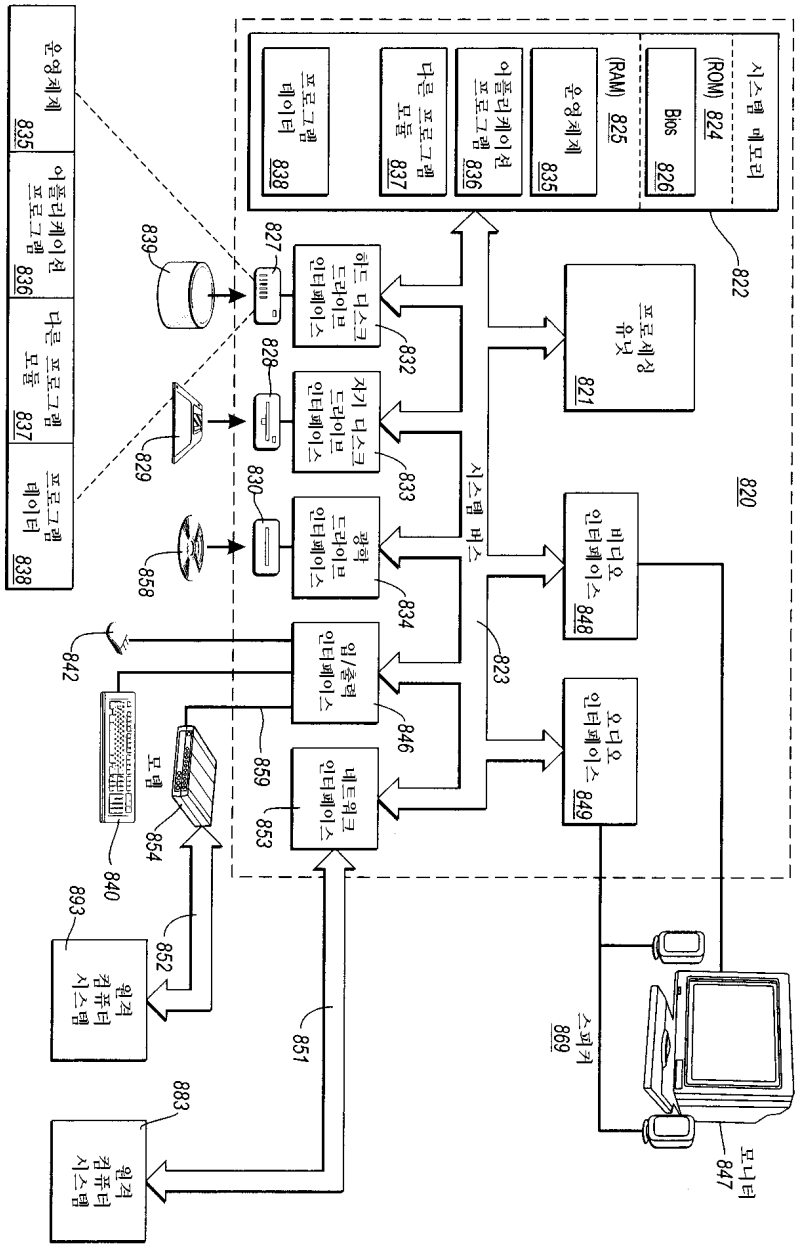
도면6


600
송신 도메인으로부터
전자 메시지 수신
601
605
송신 도메인에
의하여 부착된
관련 전자 메시지
전송 정책에
대한 단계
송신 도메인에 대응하는
하나 이상의 전자 메시지
전송 정책을 수신
602
하나 이상의 수신된
전자 메시지 전송
정책으로부터 관련
전자 메시지 전송
정책을 파싱
603
메시지 분류 모듈로
관련 전자 메시지
전송 정책을 제공
604

도면7


700
송신측
수신측
701
전자 메시지에 포함된
전자 메시지 데이터 수신
702
상태 정보의 다른 위치로부터
초기 문서 생성
703
전자 메시지의 하나 이상의
컴포넌트로부터 퍼즐 입력 생성
704
해답 문서 및 퍼즐 입력의
조합으로부터 계산된 해답
해시값이 컴퓨터 퍼즐용 해답 값이
되도록 해답 문서를 인식
-상기 해답 해시 값은 퍼즐 해시
알고리즘을 사용하여 계산됨-
705
인식된 해답 문서 및
전자 메시지 데이터를
포함하는 전자 메시지를
수신측 도메인에 송신
706
전자 메시지 데이터 및
해답 문서를 포함하는
전자 메시지 수신
707
상태 정보의 다른 부분으로부터
초기 문서 재생
708
전자 메시지의 하나 이상의
컴포넌트로부터 퍼즐 입력을
재계산
709
해답 문서 및 퍼즐 입력의
조합으로부터 계산된 검증
해시 값이 컴퓨터 퍼즐에 대한
해답을 지시하는 해답값인지
여부를 결정-상기 검증
해시 값은 퍼즐 해싱 알고리즘을
사용하여 계산됨-
710
결정 결과를 전자
메시지 분류 모듈에 제공

도면8


운영체제 835
어플리케이션 프로그램 836
다른 프로그램 모듈 837
프로그램 데이터 838
시스템 메모리 (ROM) 824
Bios 826
(RAM) 825
운영체제 835
어플리케이션 프로그램 836
다른 프로그램 모듈 837
프로그램 데이터 838
822
프로세싱 유닛 821
820
시스템 버스
하드 디스크 드라이브 인터페이스 832
자기 디스크 드라이브 인터페이스 833
광학 드라이브 인터페이스 834
입/출력 인터페이스 846
네트워크 인터페이스 853
비디오 인터페이스 848
오디오 인터페이스 849
823
827
828
830
839
829
858
842
859
854
840
852
851
893
883
원격 컴퓨터 시스템
원격 컴퓨터 시스템
모뎀
스피커 869
모니터 847