(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년02월23일
(11) 등록번호 10-0884969
(24) 등록일자 2009년02월16일

(51) Int. Cl.
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
H04L 9/32 (2006.01) *H04L 9/00* (2006.01)
(21) 출원번호 10-2007-7004691
(22) 출원일자 2007년02월27일
심사청구일자 2007년02월27일
번역문제출일자 2007년02월27일
(65) 공개번호 10-2007-0034641
(43) 공개일자 2007년03월28일
(86) 국제출원번호 PCT/IB2005/002524
국제출원일자 2005년07월25일
(87) 국제공개번호 WO 2006/021869
국제공개일자 2006년03월02일
(30) 우선권주장
10/923,079 2004년08월23일 미국(US)
(56) 선행기술조사문헌
WO200135569 A1
WO2002011390 A2
전체 청구항 수 : 총 34 항

(73) 특허권자
노키아 코포레이션
핀랜드핀-02150 에스푸 카일알라덴티에 4
(72) 발명자
포졸라이넨 토피
핀랜드 핀-00120 헬싱키 푸나부오렌카투 4 디 22
지스케 에로
핀랜드 핀-01300 반타 레도키티에 7 에이 13
(뒷면에 계속)
(74) 대리인
리앤목특허법인

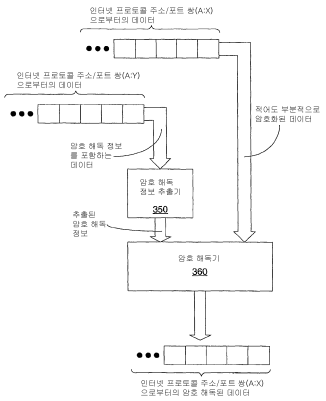
심사관 : 오제욱

(54) 인터넷 프로토콜 레벨의 암호 해독 시스템 및 방법

(57) 요 약

본원에는 암호 해독된 인터넷 프로토콜 패킷들을 전달하는 방법 및 시스템이 개시되어 있다. 상기 전달 방법은 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들의 요구를 애플리케이션으로부터 수신하는 단계; 다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들을 수신하는 단계; 상기 다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들로부터 암호 해독 정보를 추출하는 단계; 상기 추출된 암호 해독 정보를 기반으로 하여 상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 암호화된 인터넷 프로토콜 패킷들을 암호 해독하는 단계; 및 상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 암호 해독된 인터넷 프로토콜 패킷들을 상기 애플리케이션으로 전송하는 단계를 포함한다. 상기 암호 해독 정보는 암호 해독 키(들) 및/또는 속성들 및 매개변수들을 포함할 수 있으며 상기 애플리케이션과 관계없을 수 있다.

대 표 도 - 도3b



(72) 발명자

푸푸티 마티

핀랜드 핀-20500 투르쿠 우덴마안카투 12 비

카라스 티모

핀랜드 핀-02270 에스푸 바르푸티에 2엘

특허청구의 범위

청구항 1

암호 해독된 인터넷 프로토콜 패킷들을 전달하는 방법에 있어서,

상기 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법은,

전송 제어 프로토콜/인터넷 프로토콜 스택이 네트워크를 통해 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들을 수신할 필요성을 나타내는 요구를 애플리케이션으로부터 수신하는 단계;

패킷 수신기가 다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들을 수신하는 단계;

인터넷 프로토콜 보안 키 관리자가 상기 다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들로부터 암호 해독 정보를 추출하는 단계;

인터넷 프로토콜 보안 스택이 상기 추출된 암호 해독 정보를 기반으로 하여 상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들을 암호 해독하는 단계; 및

상기 전송 제어 프로토콜/인터넷 프로토콜 스택이 상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 암호 해독된 인터넷 프로토콜 패킷들을 상기 애플리케이션으로 전송하는 단계를 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 2

제1항에 있어서, 상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들은 상기 애플리케이션과 관계없이 적어도 부분적으로 암호화되는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 3

제1항에 있어서, 상기 제1 인터넷 프로토콜 주소/포트 쌍의 포트는 전송 제어 프로토콜 포트인 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 4

제3항에 있어서, 상기 다른 인터넷 프로토콜 주소/포트 쌍의 포트는 전송 제어 프로토콜 포트인 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 5

제1항에 있어서, 상기 제1 인터넷 프로토콜 주소/포트 쌍의 포트는 사용자 데이터그램 프로토콜 포트인 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 6

제5항에 있어서, 상기 다른 인터넷 프로토콜 주소/포트 쌍의 포트는 사용자 데이터그램 프로토콜 포트인 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 7

제1항에 있어서, 상기 제1 인터넷 프로토콜 주소/포트 쌍 및 상기 다른 인터넷 프로토콜 주소/포트 쌍은 서로 다른 인터넷 프로토콜 주소들을 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 8

제1항에 있어서, 상기 제1 인터넷 프로토콜 주소/포트 쌍 및 상기 다른 인터넷 프로토콜 주소/포트 쌍은 서로 다른 포트들에 주소지정되는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 9

제1항에 있어서, 상기 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법은 적어도 하나의 다른 인터넷 프로토콜 주소/포트 쌍과 상기 제1 인터넷 프로토콜 주소/포트 쌍을 연관시키는 단계를 더 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 10

제1항에 있어서, 상기 암호 해독 정보는 암호 해독 키를 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 11

제10항에 있어서, 상기 암호 해독 키는 인터넷 프로토콜 보안 키인 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 12

제1항에 있어서, 상기 암호 해독 정보는 암호 해독 매개변수를 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 13

제1항에 있어서, 상기 암호 해독 정보는 상기 애플리케이션과 관계없이 상기 다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들로부터 추출되는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 14

제1항에 있어서, 상기 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법은 상기 추출 단계 이전에 상기 다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들로부터 암호 해독 정보를 추출하도록 하는 요구를 전송하는 단계를 더 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 15

제1항에 있어서, 상기 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법은 상기 암호 해독 단계 이전에 상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들을 암호 해독하도록 하는 요구를 전송하는 단계를 더 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 방법.

청구항 16

컴퓨터 실행가능 명령어들을 저장한 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터 실행가능 명령어들은,

전송 제어 프로토콜/인터넷 프로토콜 스택이 네트워크를 통해 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들을 수신할 필요성을 나타내는 요구를 애플리케이션으로부터 수신하는 단계;

패킷 수신기가 다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들을 수신하는 단계;

인터넷 프로토콜 보안 키 관리자가 상기 다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들로부터 암호 해독 정보를 추출하는 단계;

인터넷 프로토콜 보안 스택이 상기 추출된 암호 해독 정보를 기반으로 하여 상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들을 암호 해독하는 단계; 및

상기 전송 제어 프로토콜/인터넷 프로토콜 스택이 상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 암호 해독된 인터넷 프로토콜 패킷들을 상기 애플리케이션으로 전송하는 단계를 수행하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 17

암호 해독된 인터넷 프로토콜 패킷들을 전달하는 시스템에 있어서,

상기 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템은,

인터넷 프로토콜 패킷들의 요구들을 수신하고 인터넷 프로토콜 패킷들을 전송하도록 구성된 전송 제어 프로토콜/인터넷 프로토콜 스택;

상기 전송 제어 프로토콜/인터넷 프로토콜 스택과의 통신을 이루는 패킷 수신기로서, 인터넷 프로토콜 패킷들을 수신하고 인터넷 프로토콜 패킷들을 전송하도록 구성된 패킷 수신기;

상기 전송 제어 프로토콜/인터넷 프로토콜 스택 및 상기 패킷 수신기와의 통신을 이루는 인터넷 프로토콜 보안 키 관리자로서, 암호 해독 정보가 제1 인터넷 프로토콜 주소/포트 쌍으로부터 추출되게 하도록 구성된 인터넷 프로토콜 보안 키 관리자; 및

상기 전송 제어 프로토콜/인터넷 프로토콜 스택 및 상기 인터넷 프로토콜 보안 키 관리자와의 통신을 이루는 인터넷 프로토콜 보안 스택으로서, 상기 암호 해독 정보를 기반으로 하여 제2 인터넷 프로토콜 주소/포트 쌍으로부터 암호화된 인터넷 프로토콜 패킷들을 암호 해독하도록 구성된 인터넷 프로토콜 보안 스택을 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 18

제17항에 있어서, 상기 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템은 상기 인터넷 프로토콜 보안 키 관리자와의 통신을 이루는 디지털 권한 관리 컴포넌트로서, 상기 제1 인터넷 프로토콜 주소/포트 쌍으로부터 상기 암호 해독 정보를 추출하도록 구성된 디지털 권한 관리 컴포넌트를 더 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 19

제18항에 있어서, 상기 인터넷 프로토콜 보안 키 관리자는 디지털 권한 관리 컴포넌트를 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 20

제17항에 있어서, 상기 제1 및 제2 인터넷 프로토콜 주소/포트 쌍은 서로 다른 인터넷 프로토콜 주소들을 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 21

제17항에 있어서, 상기 제1 및 제2 인터넷 프로토콜 주소/포트 쌍들은 서로 다른 포트들에 주소지정되는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 22

제17항에 있어서, 상기 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템은 상기 전송 제어 프로토콜/인터넷 프로토콜 스택과의 통신을 이루는 애플리케이션으로서, 인터넷 프로토콜 패킷들을 요구하고 인터넷 프로토콜 패킷들을 수신하도록 구성된 애플리케이션을 더 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 23

제22항에 있어서, 상기 암호 해독 정보는 상기 애플리케이션과 관계없는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 24

제17항에 있어서, 상기 제1 및 제2 인터넷 프로토콜 주소/포트 쌍들은 서로 연관되는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 25

제17항에 있어서, 상기 암호 해독 정보는 암호 해독 키를 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 26

제25항에 있어서, 상기 암호 해독 키는 인터넷 프로토콜 보호 키인 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 27

제17항에 있어서, 상기 암호 해독 정보는 암호 해독 매개변수를 포함하는 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 28

제17항에 있어서, 상기 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템은 인터넷 프로토콜 데이터캐스트의 디지털 비디오 방송 타입 시스템인 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 29

제17항에 있어서, 상기 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템은 디지털 비디오 방송 핸드헬드 타입 시스템인 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 30

제17항에 있어서, 상기 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템은 지상파 디지털 비디오 방송 타입 시스템인 것을 특징으로 하는 암호 해독된 인터넷 프로토콜 패킷들의 전달 시스템.

청구항 31

인터넷 프로토콜 패킷 스트림을 암호 해독하는 시스템에 있어서,

상기 인터넷 프로토콜 패킷 스트림의 암호 해독 시스템은,

제1 인터넷 프로토콜 주소/포트 쌍;

상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 제2 인터넷 프로토콜 주소/포트 쌍;

상기 제2 인터넷 프로토콜 주소/포트 쌍에서 수신된 데이터로부터 암호 해독 정보를 추출하는 수단으로서, 상기 암호 해독 정보는 애플리케이션과 관계없는 수단; 및

상기 추출된 암호 해독 정보를 기반으로 하여 상기 제1 인터넷 프로토콜 주소/포트 쌍에서 수신된 데이터의 적어도 일부분을 암호 해독하는 수단을 포함하는 것을 특징으로 하는 인터넷 프로토콜 패킷 스트림의 암호 해독 시스템.

청구항 32

제31항에 있어서, 상기 제1 인터넷 프로토콜 주소/포트 쌍에서 수신된 데이터가 적어도 부분적으로 암호화되는 것을 특징으로 하는 인터넷 프로토콜 패킷 스트림의 암호 해독 시스템.

청구항 33

암호 해독 정보의 전달을 관리하는 시스템에 있어서,

상기 암호 해독 정보의 전달을 관리하는 시스템은 인터넷 프로토콜 보안 키 관리자를 포함하며, 상기 인터넷 프로토콜 보안 키 관리자는,

제1 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들의 암호 해독에 대한 필요성을 나타내는 요구를 수신하도록 구성되고,

다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들을 요구하도록 구성되며,

상기 다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들로부터 추출된 암호 해독 정보를 획득하도록 구성되고,

상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들을 암호 해독하는데 사용하기 위해 상

기 추출된 암호 해독 정보를 전송하도록 구성되는 것을 특징으로 하는 암호 해독 정보의 전달을 관리하는 시스템.

청구항 34

암호화된 인터넷 프로토콜 데이터를 수신하는 방법에 있어서,

상기 암호화된 인터넷 프로토콜 데이터의 수신 방법은,

전송 제어 프로토콜/인터넷 프로토콜 스택이 네트워크를 통해 주어진 인터넷 프로토콜 주소/포트 쌍에서의 인터넷 프로토콜 패킷들을 수신할 필요성을 나타내는 요구를 애플리케이션으로부터 수신하는 단계;

패킷 수신기가 상기 주어진 인터넷 프로토콜 주소/포트 쌍에서의 인터넷 프로토콜 패킷들을 암호 해독하기 위한 정보를 다른 인터넷 프로토콜 주소/포트 쌍으로부터 획득하는 단계;

인터넷 프로토콜 보안 스택이 상기 주어진 인터넷 프로토콜 주소/포트 쌍에서 수신된 인터넷 프로토콜 패킷들의 스트림을 암호 해독하는 단계; 및

상기 전송 제어 프로토콜/인터넷 프로토콜 스택이 상기 암호 해독된 인터넷 프로토콜 패킷 스트림을 상기 애플리케이션에 제공하는 단계를 포함하는 것을 특징으로 하는 암호화된 인터넷 프로토콜 데이터를 수신하는 방법.

명 세 서

기 술 분 야

<1> 본 발명은 일반적으로 기술하면 암호화된 인터넷 프로토콜 패킷들을 암호 해독하는 시스템 및 방법에 관한 것이다. 더 구체적으로 기술하면, 본 발명은 암호 해독을 위해 암호화의 세부 정보를 공급하는 애플리케이션 없이 인터넷 프로토콜 레벨의 조건부 액세스 암호 해독 방법 및 시스템에 관한 것이다.

배 경 기 술

<2> 인터넷의 기본 통신 언어 또는 프로토콜은 전송 제어 프로토콜/인터넷 프로토콜(Transmission Control Protocol/Internet Protocol)이며 이는 인터라넷(intranet)이든 익스트라넷(extranet)이든 개인 네트워크에서 통신 프로토콜로서사용될 수 있다. 전송 제어 프로토콜/인터넷 프로토콜은 복수 개의 네트워크에 내재하는 다른 하드웨어 및 소프트웨어 아키텍처들을 지니는 여러 컴퓨터가 서로 통신하는 것을 허용하는 네트워킹 프로토콜이다. 전송 제어 프로토콜/인터넷 프로토콜은 프로토콜 스택의 여러 기능을 계층으로 설명하는 프로토콜 스택 모델로 언급되는 것이 일반적이다. 이하에 언급되어 있는 바와 같이, 도 1에는 그러한 프로토콜 스택 모델 중 대표적인 모델(100)이 도시되어 있다. 상기 모델은 하나의 스택으로서 언급되는데, 그 이유는 소프트웨어 모듈들이 상호작용할 목적으로 서로 상부에 적층되어 있기 때문이다.

<3> 전송 제어 프로토콜/인터넷 프로토콜은 종종 4개의 기능 계층을 사용하여 설명되지만, 실제의 전송 제어 프로토콜 및 인터넷 프로토콜 부분 집합들은 4개의 계층 중 2개의 계층으로 이루어지는 것이 일반적이다. 도 1에 도시된 바와 같이, 애플리케이션 계층(101)과 같은 계층은 다수의 프로토콜 중 어느 한 프로토콜에 의해 수행될 수 있는 데이터 통신 기능을 식별한다. 전송 제어 프로토콜/인터넷 프로토콜 통신은 주로 점 대 점(point-to-point) 또는 피어 투 피어(peer-to-peer)인데, 이것이 의미하는 것은 각각의 점 또는 호스트 컴퓨터가 프로토콜 스택의 동일 계층에서 같은 프로토콜을 구현하고 있는 경우에 각각의 통신이 네트워크 내의 한 점 또는 호스트 컴퓨터로부터 다른 한 점 또는 호스트 컴퓨터로 이루어진다는 것을 의미한다. 전송 제어 프로토콜/인터넷 프로토콜 통신은 적합한 통신을 위해 표준화된다.

<4> 전송 제어 프로토콜(TCP)은 인터넷과 같은 네트워크를 통해 전송되고 결국 수신지 컴퓨터의 전송 제어 프로토콜 계층에 의해 수신되는 더 작은 패킷들로 메시지 또는 데이터를 어셈블링하고, 상기 수신지 컴퓨터는 상기 패킷들을 원래의 메시지 또는 데이터로 다시 어셈블링한다. 인터넷 프로토콜(Internet Protocol; IP)은 상기 패킷들이 정확한 수신지에 이르도록 각각의 패킷을 주소지정한다. 네트워크상의 매개 컴퓨터들은 인터넷 프로토콜 주소를 검사하여 상기 패킷을 어디에 보내야 할지를 결정한다. 원래의 메시지로부터의 각각의 패킷은 상기 수신지 컴퓨터에 다르게 라우팅될 수 있고, 결국 그러한 패킷들이 동일 수신지에서 다시 어셈블링된다.

<5> 도 1에는 대표적인 프로토콜 스택 모델(100)에 대한 블록 선도가 예시되어 있다. 상기 프로토콜 스택 모델(100)은 4개의 기능 계층, 즉 애플리케이션 계층(101), 전송 계층(103), 인터네트워크 계층(105), 및 네트워크 인

터페이스 계층(107)을 포함할 수 있다. 상기 프로토콜 스택 모델(100)의 최상위 계층은 상기 애플리케이션 계층(101)이다. 상기 애플리케이션 계층(101)은 사용자 프로그램에 필요한 기능들을 관리하며 운영 애플리케이션에 매우 의존한다. 모든 사용자 지향 접근 프로토콜들은 상기 애플리케이션 계층(101) 내에 유지된다. 상기 전송 계층(103)과 상호작용하는 기능들은 상기 애플리케이션 계층(101) 내에 유지된다. 또한, 상기 애플리케이션 계층(101)은 데이터 압축 및 압축 해제 외에도 데이터 암호화 및 암호 해독에 관련된 기능들을 포함한다. 가장 널리 알려진 전송 제어 프로토콜/인터넷 프로토콜 애플리케이션 계층 프로토콜들은 하이퍼텍스트 전송 프로토콜(Hypertext Transfer Protocol; HTTP), 파일 전송 프로토콜(File Transfer Protocol; FTP), 텔렛(Telnet), 및 단순 메일 전송 프로토콜(Simple Mail Transfer Protocol: SMTP)을 포함한다. 또한, 상기 애플리케이션 계층(101)은 도메인 네임 서비스(Domain Name Service; DNS), 라우팅 정보 프로토콜(Routing Information Protocol; RIN), 단순 네트워크 관리 프로토콜(Simple Network Management Protocol; SNMP), 및 네트워크 파일 시스템(Network File System; NFS)과 같은 프로토콜들을 포함할 수 있다.

<6> 전송 계층(103)은 전송 제어 프로토콜 부분집합을 포함할 수 있다. 전송 계층(103)은 단 대 단 접속성 및 데이터 무결성에 대한 프로토콜들을 유지한다. 전송 계층(103)은 오류 제어 기능을 제공한다. 전송 계층(103)은 소실, 중복 또는 변조된 데이터 패킷들의 검출 기능 및 소실, 중복 또는 변조된 데이터 패킷들로부터의 복구 기능을 제공한다. 상기 전송 계층(103)에서, 상기 애플리케이션 계층(101)으로부터의 데이터는 각각의 패킷이 한 블록에 내재하는 패킷들의 순서를 나타내는 시퀀스 번호를 지니는 패킷들로 분할된다. 각각의 패킷이 수신지 컴퓨터의 전송 계층(103)에 의해 수신됨에 따라, 상기 수신지 전송 계층(103)은 상기 패킷을 검사하며, 완전한 패킷 시퀀스가 수신될 경우에 다음으로 예상된 시퀀스 번호를 나타내는 확인(acknowledgement; ACK) 신호를 발신지 컴퓨터로 전송한다. 전송 계층(103)은 전송 제어 프로토콜(Transmission Control Protocol; TCP) 및 사용자 데이터그램 프로토콜(User Datagram Protocol; UDP)을 포함한다. 사용자 데이터그램 프로토콜은 전송 제어 프로토콜 대신에 특수 목적에 사용된다. 다른 프로토콜들은 상기 전송 계층(103)에 유지될 수 있다. 또한, 전송 계층(103)은 상기 애플리케이션 계층(101) 및 상기 인터네트워크 계층(105) 간에 데이터를 이동시키는 기능을 수행한다.

<7> 인터네트워크 계층(105)은 인터넷 프로토콜 부분집합을 포함한다. 인터네트워크 계층(105)은 인터네트워크들을 통해 메시지들 또는 데이터를 라우팅하는 프로토콜들을 유지한다. 인터네트워크 계층(105)은 모든 데이터 패킷을 전달하도록 시도하지만 소실 또는 변조된 패킷들을 재전송하지 못한다. 게이트웨이들 또는 라우터들은 네트워크들 간에 메시지들 또는 데이터를 라우팅하는 기능을 수행한다. 상기 인터네트워크 계층(105)은 데이터그램 네트워크 서비스를 제공한다. 데이터그램들은 헤더, 데이터, 및 트레일러(trailer)를 포함하는 정보 패킷들이다. 상기 헤더는 네트워크가 상기 패킷들을 라우팅할 필요가 있는 정보를 포함한다. 헤더 정보의 예들은 패킷에 대한 수신지 주소, 패킷에 대한 발신지 주소, 및 보안 라벨들을 포함한다. 상기 트레일러는 종종 데이터가 이동 중에 있는 동안 어느 부적합하거나 승인되지 않은 방식으로 처리되지 않게 하는 체트섬(checksum)을 포함한다. 상기 인터네트워크 계층(105)에서 유지될 수 있는 다른 프로토콜은 인터넷 제어 메시지 프로토콜(Internet Control Message Protocol; ICMP)을 포함한다. 또한, 인터네트워크 계층(105)은 상기 전송 계층(103) 및 상기 네트워크 인터페이스 계층(107) 간에 데이터를 이동시키는 기능을 수행한다.

<8> 네트워크 인터페이스 계층(107)은 장치 및 상기 장치가 연결된 네트워크 간의 데이터 교환을 관리하고 동일한 네트워크상의 장치들 간에 데이터를 라우팅하는 프로토콜들을 유지한다. 네트워크 인터페이스 계층(107)은 상기 네트워크에 의해 전송되는 프레임들로 인터넷 프로토콜 데이터그램들을 캡슐화하며 또한 상기 네트워크에 의해 사용된 물리적 주소에 상기 인터넷 프로토콜 주소들을 매핑한다. 네트워크 인터페이스 계층(107)은 상기 인터네트워크 계층(105)으로부터 수신된 데이터에 라우팅 정보를 추가한다. 이러한 라우팅 정보는 헤더 필드의 형태로 추가된다.

<9> 상기 프로토콜 스택을 이루는 각각의 계층은 적합한 전달을 보장하도록 제어 정보를 추가한다. 제어 정보는 상기 수신지 주소, 상기 발신지 주소, 라우팅 제어들, 보안 라벨들, 및 체크섬 데이터를 포함할 수 있다. 상기 애플리케이션 계층(101)에서 상기 네트워크 인터페이스 계층(107)에 이르기까지 상기 스택의 각각의 계층에 이르는 경우, 상기 계층은 이전의 계층으로부터 수신된 헤더, 데이터, 및 트레일러 정보를 데이터로서 취급하고 그 자체의 헤더 및 트레일러 정보를 상기 데이터에 추가한다. 프로토콜이 헤더 및 트레일러를 사용하여 다른 프로토콜로부터 데이터를 패키징할 경우에, 그러한 프로세스는 캡슐화(encapsulation)라고 지칭된다.

<10> 도 2에는 여러 프로토콜 스택 모델 계층 내에 데이터를 캡슐화하는 프로세스에 대한 블록 선도가 예시되어 있다. 다른 한 컴퓨터에 전송하는데 필요한 원래의 데이터(201)는 상기 애플리케이션 계층으로부터 취해지고 상기 전송 계층에 전송된다. 상기 전송 계층에서, 애플리케이션 계층으로부터의 제어 정보와 원래의 데이터(201)

는 상기 전송 계층 내의 애플리케이션 계층 데이터(211)를 포함한다. 상기 전송 계층에서, 헤더(215) 및 트레일러(217)는 상기 애플리케이션 계층 데이터(211)에 추가될 수 있다. 헤더(215), 애플리케이션 데이터(211) 및 트레일러(217)는 상기 인터네트워크 계층에 대한 전송 계층 데이터(221)가 된다. 상기 인터네트워크 계층에서, 헤더(225) 및 트레일러(227)는 상기 전송 계층 데이터(221)에 추가될 수 있다. 헤더(225), 전송 계층 데이터(221) 및 트레일러(227)는 네트워크 인터페이스 계층에 대한 인터네트워크 계층 데이터(231)가 된다. 상기 네트워크 인터페이스 계층에서, 헤더(235) 및 트레일러(237)는 상기 인터네트워크 계층 데이터(231)에 추가될 수 있다. 헤더(235), 인터네트워크 계층 데이터(231) 및 트레일러(237)는 상기 네트워크로부터 전송되는 최종 데이터(241)가 된다.

<11> 위에서 언급된 바와 같이, 애플리케이션 계층(101)은 데이터의 암호화 및 암호 해독에 관련된 기능들을 포함할 수 있다. 애플리케이션 계층(101)은 인터넷 프로토콜 보안 스택 내에 포함될 수 있다. 인터넷 프로토콜 보안 스택은 인터넷 프로토콜 측정들의 집합을 포함하는 프로토콜 스택이다. 특히, 인터넷 프로토콜 보안은 패킷 스트림의 모든 패킷의 헤더 필드에서의 발신 주소의 유효성을 검증하도록 헤더 필드를 통한 인증을 지원한다. 캡슐화 보안 페이로드(encapsulating security payload; ESP) 헤더 필드는 암호화 매개변수들/속성들을 기반으로 하여 전체의 데이터그램을 암호화한다. 인터넷 프로토콜 보안을 사용하여 인터넷 프로토콜 패킷들을 보호하려면 수신지 호스트 컴퓨터는 패킷들의 콘텐츠를 사용할 수 있기 전에 수신된 패킷들을 암호 해독할 필요가 있다. 상기 암호 해독은 키 또는 한 세트의 키들을 사용하여 그리고/또는 몇몇 추가의 매개변수들/속성들을 사용하여 구현된다. 상기 키들 및 상기 매개변수들/속성들은 암호화된 인터넷 프로토콜 패킷들의 정확한 암호 해독을 위한 시스템의 전송 제어 프로토콜/인터넷 프로토콜 스택/아키텍처에 공급된다. 암호화 매개변수들/속성들은 애플리케이션에 의해 인터넷 프로토콜 보안 스택에 공급된다.

<12> 애플리케이션들이 암호화 정보를 상기 인터넷 프로토콜 스택에 공급하여야 할 경우에, 상기 애플리케이션들은 더 복잡해진다. 전송 제어 프로토콜/인터넷 프로토콜 서비스들을 사용하는 애플리케이션들이 단순해지고 상기 서비스들의 가능한 암호화를 알지 못하게 할 필요가 있다. 서비스가 암호화되지 않은 것처럼 나타내는 애플리케이션의 관점에서 볼 때 임의의 인터페이스를 통해 주변 시스템이 서비스들을 암호 해독된 형태로 상기 애플리케이션들에 제공할 필요가 있다.

발명의 상세한 설명

<13> 본 발명의 실시태양들에 의하면, 애플리케이션으로부터의 요구는 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들에 대하여 수신된다. 상기 포트는 전송 제어 프로토콜 포트일 수 있으며 본 발명의 한 실시예에서는 상기 포트가 사용자 데이터그램 프로토콜 포트이다. 다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들이 또한 수신된다. 암호 해독 정보는 상기 다른 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들로부터 추출되며 상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 인터넷 프로토콜 패킷들은, 수신 및 암호화될 경우에, 상기 추출된 암호 해독 정보를 기반으로 하여 암호 해독된다. 그리고나서, 상기 제1 인터넷 프로토콜 주소/포트 쌍과 연관된 암호 해독된 인터넷 프로토콜 패킷들은 상기 애플리케이션으로 전송된다.

<14> 본 발명의 다른 한 실시태양은 암호 해독된 인터넷 프로토콜 패킷들을 전달하기 위한 시스템을 제공한다. 전송 제어 프로토콜/인터넷 프로토콜 스택은 인터넷 프로토콜 패킷들에 대한 요구들을 수신하고 인터넷 프로토콜 패킷들을 전송하도록 구성된다. 상기 전송 제어 프로토콜/인터넷 프로토콜 스택과의 통신을 이루는 패킷 수신기는 인터넷 프로토콜 패킷들을 수신하고 인터넷 프로토콜 패킷들을 전송하도록 구성된다. 상기 전송 제어 프로토콜/인터넷 프로토콜 스택 및 상기 패킷 수신기와의 통신을 이루는 인터넷 프로토콜 보안 키 관리자는 제1 인터넷 프로토콜 패킷 스트림으로부터의 암호 해독 정보의 추출 및 상기 암호 해독 정보의 전송을 조정하도록 구성된다. 상기 인터넷 프로토콜 보안 키 관리자와의 통신을 이루는 디지털 권한 관리 컴포넌트는 상기 암호 해독 정보를 추출하도록 구성되고, 상기 전송 제어 프로토콜/인터넷 프로토콜 스택 및 상기 인터넷 프로토콜 보안 키 관리자와의 통신을 이루는 인터넷 프로토콜 보안 스택은 상기 암호 해독 정보를 기반으로 하여 제2의 적어도 부분적으로 암호화된 인터넷 프로토콜 패킷 스트림으로부터 암호화된 인터넷 프로토콜 패킷들을 암호 해독하도록 구성된다. 상기 암호 해독 정보는 애플리케이션과 관계없을 수 있다.

<15> 본 발명 및 본 발명의 이점들은 동일 참조번호들이 동일 특징들을 나타내는 첨부도면들을 고려한 이하의 설명을 참조하면 더 완전하게 이해될 수 있을 것이다.

실 시 예

<21> 이하의 여러 실시예들에 대한 설명에서는, 본원 명세서의 일부를 형성하며 본 발명이 구현될 수 있는 여러 실시예를 예로써 나타낸 첨부도면들이 참조된다. 여기서 이해해야 할 점은 다른 실시예들이 채용될 수 있으며 구조적 및 기능적 변형들이 본 발명의 범위로부터 벗어나지 않고서도 이루어질 수 있다는 것이다.

<22> 본 발명의 여러 실시태양에 의하면, 제1 인터넷 프로토콜 주소/포트 쌍은 다른 인터넷 프로토콜 주소/포트 쌍과 연관되고 그리고/또는 상기 제1 인터넷 프로토콜 주소/포트 쌍에 전송된 제1의 암호화된 인터넷 프로토콜 데이터 스트림의 암호 해독에 필요한 매개변수들/속성들은 상기 다른 인터넷 프로토콜 주소/포트 쌍에 전송된다. 예를 들면, 잘 정의된 전송 제어 프로토콜 포트는 모든 인터넷 프로토콜 주소와 연관될 수 있다. 이때, 이와 같이 잘 정의된 포트는 상기 제1 인터넷 프로토콜 주소의 다른 모든 포트에 전송된 패킷들을 암호 해독하기 위한 인터넷 프로토콜 보안 키들 및/또는 매개변수들/속성들에 대한 수신지 포트로서 사용된다. 그러한 포트들은 전송 제어 프로토콜 또는 사용자 데이터그램 프로토콜 타입의 포트들일 수 있다. 변형 실시예에서, 암호화 매개변수들/속성들 및/또는 키(들)는 암호화된 서비스와 동일한 포트에 전송될 수 있지만, 호스트 및 수신지 장치들의 인터넷 프로토콜 주소는 서로 다르다.

<23> 도 3a에는 본 발명의 적어도 하나의 실시태양에 따른 인터넷 프로토콜 패킷들의 암호 해독에 필요한 정보를 추출하기 위한 전송 제어 프로토콜/인터넷 프로토콜 스택 아키텍처(300)에 대한 블록 선도가 예시되어 있다. 여기서 당업자가 이해하여야 할 점은 도 3a에 예시된 전송 제어 프로토콜/인터넷 프로토콜 스택 아키텍처가 단지 하나의 예이며 다른 요소들 및/또는 통신 경로들이 본 발명의 실시태양들을 실시하는데 사용/구현될 수 있다는 것이다. 예를 들면, 인터넷 프로토콜 보안 키 관리자(308) 및 디지털 권한 관리 요소(310)와 같은 어느 한 컴포넌트에 의해 수행되는 동작들 및/또는 기능들은 단일의 컴포넌트에 의해 수행될 수 있다.

<24> 전송 제어 프로토콜/인터넷 프로토콜 스택 아키텍처(300)는 특정한 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍으로부터 패킷들을 수신할 것을 초기에 요구하는 애플리케이션(302)을 포함한다. 본원에서는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍이 인터넷 프로토콜 주소, 콜론, 전송 제어 프로토콜 포트의 순차적인 구성으로 설명된다. 예를 들면, 대표적인 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍은 168.198.0.1:80일 수 있다. 본원에서 사용되는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍은 인터넷 프로토콜 주소(A) 및 2개의 다른 전송 제어 프로토콜 포트(X,Y)를 지정하도록 A:X 및 A:Y로 언급된다. 애플리케이션(302)은 전송 제어 프로토콜/인터넷 프로토콜 스택(304)에 대한 통신 링크를 지닌다. 전송 제어 프로토콜/인터넷 프로토콜 스택(304)은 지정된 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍으로부터 인터넷 프로토콜 패킷들을 요구 및 수신하기 위해 패킷 수신기(306)와의 통신을 이루는 것으로 도시되어 있다.

<25> 전송 제어 프로토콜/인터넷 프로토콜 스택(304)은 또한 인터넷 프로토콜 보안 스택(312)과의 통신을 이루는 것으로 도시되어 있다. 인터넷 프로토콜 보안 스택(312)은 전송 제어 프로토콜/인터넷 프로토콜 스택(304)으로부터 수신되는 암호화된 인터넷 프로토콜 패킷들에 관하 암호 해독을 수행한다. 인터넷 프로토콜 보안 스택(312)은 또한 인터넷 프로토콜 패킷들의 암호 해독을 완료하면 상기 암호 해독된 인터넷 프로토콜 패킷들을 전송 제어 프로토콜/인터넷 프로토콜 스택(304)으로 복귀시킨다.

<26> 패킷 수신기(306)는 인터넷 프로토콜 보안 키 관리자(308)와의 통신을 이루는 것으로 도시되어 있다. 인터넷 프로토콜 보안 키 관리자(308)는 암호 해독 키(들) 및/또는 속성들/매개변수들을 추출하고 상기 암호 해독 키(들) 및/또는 속성들/매개변수들을 상기 인터넷 프로토콜 스택(312)에 전송하도록 구성된다. 본 발명의 적어도 한 실시태양에 의하면, 인터넷 프로토콜 보안 키 관리자(308)는 인터넷 프로토콜 보안 키 관리자(308) 컴포넌트 내에 포함될 수 있다. 암호 해독 속성들/매개변수들은 암호 해독 패턴, 다시 말하면 패킷의 어느 비트들을 암호 해독해야 할지 그리고 어느 비트들을 암호 해독하지 않아야 할 지와 같은 암호 해독 패턴, 암호 해독 기법, 다시 말하면 암호 해독 목적에 사용되는 알고리즘과 같은 암호 해독 기법, 및/또는 다른 정보를 포함할 수 있다. 인터넷 프로토콜 보안 키 관리자(308)는 또한 디지털 권한 관리(Digital Rights Management; DRM) 요소(310)와의 통신을 이룬다. 디지털 권한 관리 요소(310)는 단지 디지털 콘텐츠에 대한 허용에 적용가능한 권한들뿐만 아니라 모든 권한을 관리한다. 이러한 권한들은 사용, 복제 권한 부여 및/또는 제한, 편집 권한, 및 전송 권한을 포함한다. 디지털 권한 관리 요소(310)는 상기 애플리케이션(302)과 관계없이 다른 전송 제어 프로토콜 포트로부터 추출된 인터넷 프로토콜 보안 키(들) 및 암호 해독 매개변수들/속성들을 제공한다. 본 발명의 적어도 한 실시태양에 의하면, 상기 디지털 권한 관리 요소는 오프 모바일 얼라이언스(Open Mobile Alliance; OMA) 디지털 권한 관리(DRM) 컴포넌트, 예컨대, 오픈 모바일 얼라이언스(OMA) 디지털 권한 관리(DRM) 1.0 또는 오픈 모바일 얼라이언스(OMA) 디지털 권한 관리(DRM) 2.0일 수 있다. 본 발명의 적어도 하나의 실시태양에 의하면, 디지털 권한 관리 요소(310)의 기능들은 인터넷 프로토콜 보안 관리자(308) 컴포넌트 내에 포함될 수 있다.

<27> 본 발명의 여러 실시태양은 기존의 소프트웨어 모듈들 외부에 추가의 소프트웨어 모듈을 필요로 할 수 있는 기존의 전송 제어 프로토콜/인터넷 프로토콜 스택 아키텍처들에 적합하다. 어떠한 비-암호화된 인터넷 프로토콜 서비스에 관한 제한이 전혀 없으며 애플리케이션들(302)이 실제로 인터넷 프로토콜 레벨의 암호화를 전혀 알지 못한다. 본 발명의 여러 실시태양은 예컨대 인터넷 프로토콜 데이터캐스트(Internet Protocol Datacast; IPDC)의 디지털 비디오 방송(Digital Video Broadcasting; DVB), 지상파 디지털 비디오 방송(DVB-Terrestrial; DVB-T)과 같은 디지털 비디오 방송의 변형들 및 디지털 비디오 방송 핸드헬드(DVB-Handheld; DVB-H)를 사용할 경우에 서비스 암호화 시스템의 일부로서 사용될 수 있다. 그 외에도, 본 발명의 여러 실시태양은 미국의 고성능 텔레비전 시스템 위원회(Advanced Television Systems Committee; ATSC) 및 일본의 통합 지상파 디지털 방송 서비스(Integrated Services Digital Broadcasting-Terrestrial; ISDB-T) 및 지상파 디지털 멀티미디어 방송(Digital Multimedia Broadcasting Terrestrial; DMB-T)과 같은 다른 디지털 비디오 및 텔레비전 시스템들에 사용될 수 있다.

<28> 도 3b에는 본 발명의 적어도 하나의 실시태양에 따른 인터넷 프로토콜 패킷들의 암호 해독에 필요한 정보를 추출하는 프로세스에 대한 블록 선도가 예시되어 있다. 인터넷 프로토콜 주소/포트 쌍(A:Y)으로부터의 데이터는 암호 해독 정보 추출기(350)로 전송된다. 암호 해독 정보 추출기(350)는 인터넷 프로토콜 보안 키 관리자(308) 및/또는 디지털 권한 관리 요소(310)를 포함할 수 있다. 상기 인터넷 프로토콜 주소/포트 쌍(A:Y)으로부터의 데이터는 다른 인터넷 프로토콜 주소/포트 쌍(A:X)과 연관된 암호 해독 정보를 포함한다. 상기 암호 해독 정보 추출기(350)는 상기 인터넷 프로토콜 주소/포트 쌍(A:Y)으로부터의 데이터에서 상기 암호 해독 정보를 추출하고 상기 암호 해독 정보를 암호 해독기(360)로 전송한다. 상기 암호 해독 정보는 어느 부분들을 암호 해독해야 할지 및 암호 해독에 사용되는 알고리즘과 같은 암호 해독 키(들) 및/또는 암호 해독 속성들/매개변수들을 포함할 수 있다. 암호 해독기(360)는 인터넷 프로토콜 보안 키 관리자(308) 및/또는 인터넷 프로토콜 보안 스택(312)을 포함할 수 있다.

<29> 상기 암호 해독기(360)는 상기 인터넷 프로토콜 주소/포트 쌍(A:X)으로부터의 데이터를 수신한다. 상기 인터넷 프로토콜 주소/포트 쌍(A:X)으로부터의 데이터는 적어도 부분적으로 암호화된 데이터이다. 암호 해독기(360)는 상기 암호 해독 정보 추출기로부터 수신된 암호 해독 정보를 기반으로 하여 인터넷 프로토콜 주소/포트 쌍(A:X)으로부터의 데이터를 암호 해독하다. 그리고나서, 암호 해독기(360)는 암호 해독 형태로 인터넷 프로토콜 주소/포트 쌍(A:X)으로부터의 데이터를 출력한다. 이와 같이 암호 해독된 인터넷 프로토콜 주소/포트 쌍(A:X)으로부터의 데이터는 원래 상기 데이터를 요구한 애플리케이션으로 전송될 수 있다. 상기 애플리케이션의 관점에서 보면, 상기 인터넷 프로토콜 주소/포트 쌍으로부터 요구된 데이터는 결코 암호화되지 않는다.

<30> 도 4a 및 도 4b에는 본 발명의 적어도 하나의 실시태양에 따른 인터넷 프로토콜 패킷들의 암호 해독에 필요한 정보를 추출하기 위한 대표적인 방법에 대한 플로 차트가 예시되어 있다. 도 4a에 도시된 바와 같이, 그러한 프로세스는 애플리케이션(302)과 같은 애플리케이션이 특정한 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)에 대한 인터넷 프로토콜 패킷들의 요구를 전송 제어 프로토콜/인터넷 프로토콜 스택으로 전송하는 단계(402)에서 개시된다. 상기 전송 제어 프로토콜/인터넷 프로토콜 스택은 전송 제어 프로토콜/인터넷 프로토콜 스택(304)일 수 있다. 단계(404)에서, 상기 전송 제어 프로토콜/인터넷 프로토콜 스택은 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)에 대한 인터넷 프로토콜 패킷들에 대한 수신 요구를 위해 패킷 수신기에 신호를 보낸다. 상기 패킷 수신기는 패킷 수신기(306)일 수 있다. 그리고나서, 상기 프로세스는 상기 패킷 수신기가 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)을 향하도록 예정된 인터넷 프로토콜 패킷들에 대한 인터페이스를 개방하는 단계(406)로 진행한다.

<31> 단계(408)에서, 상기 패킷 수신기는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)에 대한 인터넷 프로토콜 패킷들의 암호 해독 요구를 위해 인터넷 프로토콜 보안 키 관리자에게 신호를 보낸다. 상기 인터넷 프로토콜 보안 키 관리자는 인터넷 프로토콜 보안 키 관리자(308)일 수 있다. 단계(408)에서 상기 패킷 수신기로부터의 요구를 수신할 경우에, 상기 인터넷 프로토콜 보안 키 관리자는 단계(410)에서 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:Y)을 향하도록 예정된 인터넷 프로토콜 패킷들의 요구를 전송 제어 프로토콜/인터넷 프로토콜 스택으로 전송한다. 본 발명의 적어도 하나의 실시태양에 의하면, 키(들) 및/또는 속성들/매개변수들은 잘 정의된 인터넷 프로토콜 스트림 내에 유지된다. 상기 인터넷 프로토콜 보안 관리자는 상기 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)을 향하도록 예정된 인터넷 프로토콜 패킷들을 암호 해독하는데 필요한 암호 해독 정보를 획득하기 위해 특정한 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)을 감시하도록 구성될 수 있다.

<32> 상기 프로세스는 전송 제어 프로토콜/인터넷 프로토콜 스택이 인터넷 프로토콜 주소/전송 제어 프로토콜 포트

쌍(A:Y)을 향하도록 예정된 인터넷 프로토콜 패킷들의 수신 요구를 위해 상기 패킷 수신기에 신호를 보내는 단계(412)로 진행한다. 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:Y)은 잘 알려진 인터넷 프로토콜 주소/포트 쌍일 수 있다. 단계(414)에서, 상기 전송 제어 프로토콜/인터넷 프로토콜 스택은 상기 패킷 수신기로부터 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:Y)을 향하도록 예정된 인터넷 프로토콜 패킷들을 수신한다. 상기 인터넷 프로토콜 보안 키 관리자는 단계(416)에서 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:Y)에 대한 인터넷 프로토콜 패킷들을 수신한다. 그리고나서, 상기 프로세스는 도 4b에 예시된 단계(418)에서 계속된다.

<33> 단계(418)에서, 상기 인터넷 프로토콜 보안 키 관리자는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:Y)을 향하도록 예정된 인터넷 프로토콜 패킷들의 콘텐츠를 디지털 권한 관리 요소에 제공한다. 상기 디지털 권한 관리 요소는 디지털 권한 관리 요소(310)일 수 있다. 단계(420)에서, 상기 디지털 권한 관리 요소는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:Y)을 향하도록 예정된 인터넷 프로토콜 패킷들의 콘텐츠를 수신하고 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)으로 전송된 인터넷 프로토콜 패킷들에 대한 인터넷 프로토콜 보안 키(들) 및/또는 암호 해독 속성들/매개변수들을 추출한다. 단계(422)에서, 상기 인터넷 프로토콜 보안 키 관리자는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)을 향하도록 예정된 인터넷 프로토콜 패킷들의 암호 해독을 위한 인터넷 프로토콜 보안 키(들) 및/또는 암호 해독 속성들/매개변수들을 인터넷 프로토콜 보안 스택으로 전송한다. 상기 인터넷 프로토콜 보안 스택은 인터넷 프로토콜 보안 스택(312)일 수 있다.

<34> 상기 프로세스는 인터넷 프로토콜 보안 스택이 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)을 향하도록 예정된 인터넷 프로토콜 패킷들을 전송 제어 프로토콜/인터넷 프로토콜 스택으로부터 수신하는 단계(424)로 진행한다. 상기 수신된 인터넷 프로토콜 패킷들 중 일부 또는 모두는 암호화될 수 있다. 단계(426)에서, 상기 전송 제어 프로토콜/인터넷 프로토콜 스택으로부터 인터넷 프로토콜 패킷들을 수신할 경우, 단계(422)에서 인터넷 프로토콜 보안 스택은 인터넷 프로토콜 보안 키 관리자로부터 수신된 키(들) 및 암호 해독 속성들/매개변수들을 사용하여 암호화된 인터넷 프로토콜 패킷들을 암호 해독한다. 단계(428)에서, 인터넷 프로토콜 보안 스택은 상기 암호 해독된 인터넷 프로토콜 패킷들을 상기 전송 제어 프로토콜/인터넷 프로토콜 스택으로 전송하고, 단계(430)에서, 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)을 향하도록 예정된 암호 해독된 인터넷 프로토콜 패킷들은 상기 전송 제어 프로토콜/인터넷 프로토콜 스택으로부터 상기 애플리케이션으로 전송된다. 상기 애플리케이션의 관점에서 볼 때, 인터넷 프로토콜 패킷들의 요구는 데이터가 상기 프로세스에서 암호화 및/또는 암호 해독되었다는 어떠한 표시 없이도 요구 및 수신되었다. 더욱이, 상기 애플리케이션은 상기 요구된 인터넷 프로토콜 패킷들을 획득하는데 사용된 암호화 및/또는 암호 해독 정보를 제공할 필요가 없다.

<35> 본 발명의 하나 이상의 실시태양들은 하나 이상의 컴퓨터들, 셋톱 박스들, 이동 단말기들, 또는 다른 장치들에 의해 실행되는 하나 이상의 프로그램 모듈들에서와 같은 컴퓨터 실행가능 명령어들에서 구현될 수 있다. 일반적으로, 프로그램 모듈들은 컴퓨터 또는 다른 장치의 프로세서에 의해 실행될 경우에 특정한 태스크들을 수행하거나 특정한 추상 데이터 타입들을 구현하는 루틴들, 프로그램들, 객체들, 컴포넌트들, 데이터 구조들 등등을 포함한다. 컴퓨터 실행가능 명령어들은 하드 디스크, 광 디스크, 착탈가능한 저장 매체, 고체 메모리, RAM 등등과 같은 컴퓨터 판독가능 매체 상에 저장될 수 있다. 당업자라면 알 수 있겠지만, 프로그램 모듈들의 기능은 여러 실시예에서 필요에 따라 조합 또는 분산될 수 있다. 그 외에도, 상기 기능은 집적 회로들, 필드 프로그램가능 게이트 어레이(FPGA) 등등과 같은 펌웨어 또는 하드웨어 등가물에서 전체적으로 또는 부분적으로 구현될 수 있다.

도면의 간단한 설명

<16> 도 1은 종래의 대표적인 프로토콜 스택 모델을 블록 선도로 보여주는 도면이다.

<17> 도 2는 종래의 여러 프로토콜 스택 모델 계층 내에 데이터를 캡슐화하는 프로세스를 블록 선도로 보여주는 도면이다.

<18> 도 3a는 본 발명의 적어도 하나의 실시태양에 따른 인터넷 프로토콜 패킷들의 암호 해독에 필요한 정보의 추출을 위한 전송 제어 프로토콜/인터넷 프로토콜 스택 아키텍처를 블록 선도로 보여주는 도면이다.

<19> 도 3b는 본 발명의 적어도 하나의 실시태양에 따른 인터넷 프로토콜 패킷들의 암호 해독에 필요한 정보의 추출을 위한 프로세스를 블록 선도로 보여주는 도면이다.

<20> 도 4a 및 도 4b는 본 발명의 적어도 하나의 실시태양에 따른 인터넷 프로토콜 패킷들의 암호 해독에 필요한 정

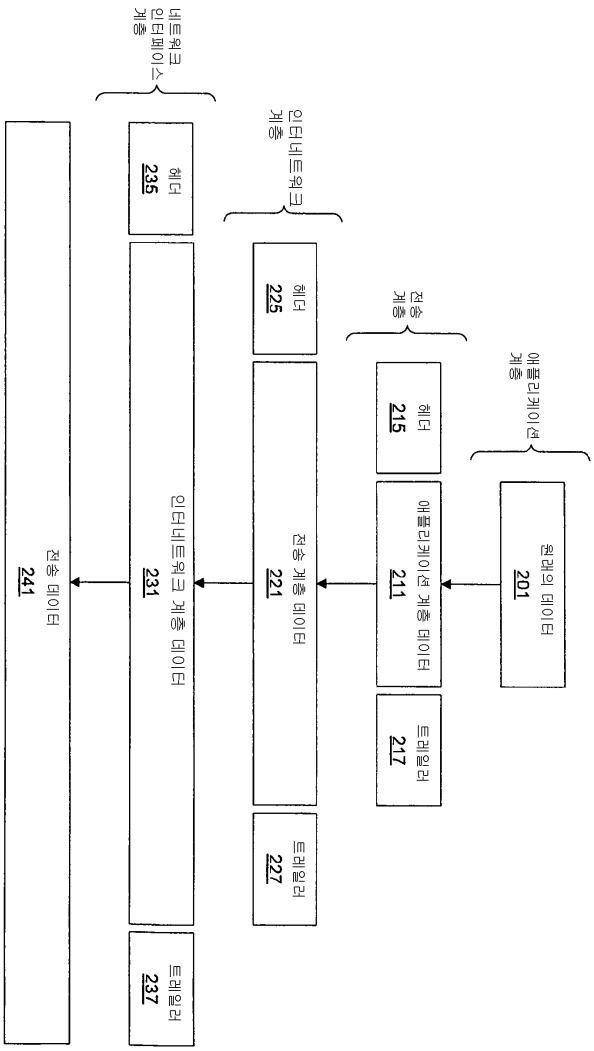
보의 추출을 위한 대표적인 방법을 플로차트로 보여주는 도면이다.

도면

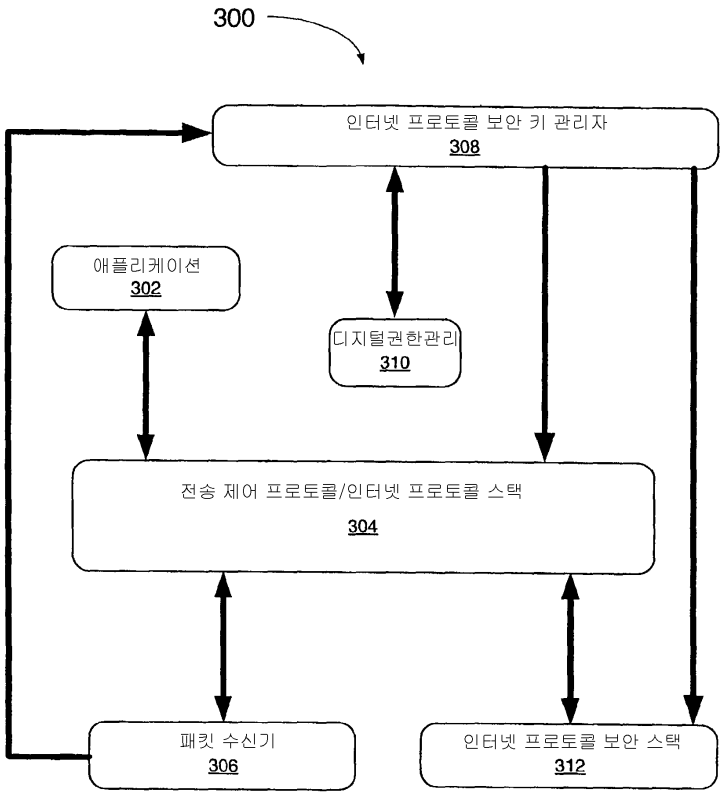
도면1

프로토콜 스택 모델

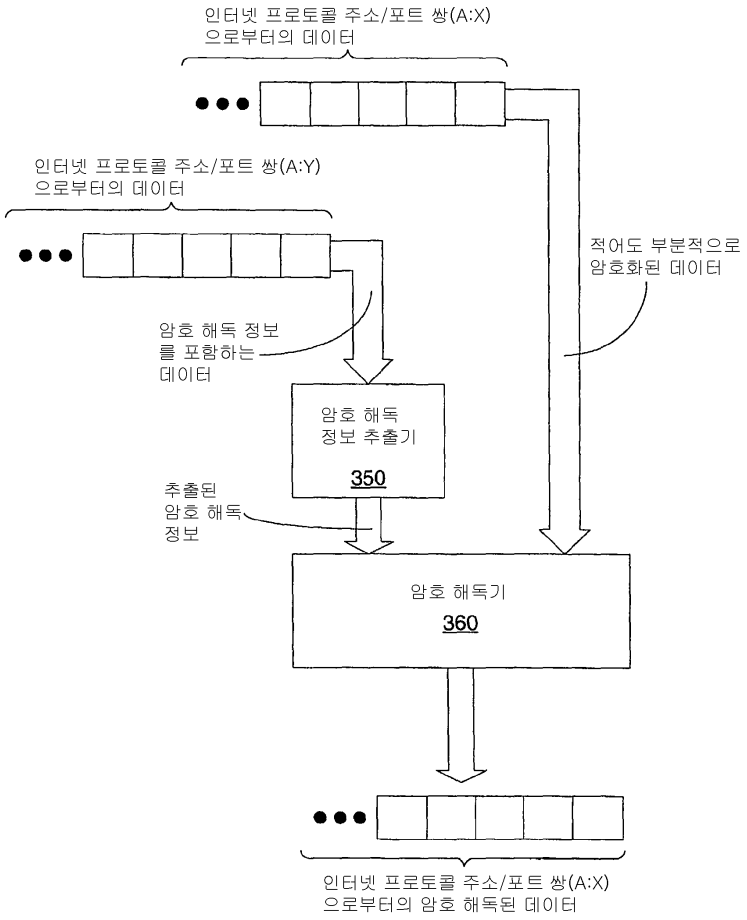
도면2


애플리케이션 계층
원래의 데이터 201
전송 계층
헤더 215
애플리케이션 계층 데이터 211
트레일러 217
인터네트워크 계층
헤더 225
전송 계층 데이터 221
트레일러 227
네트워크 인터페이스 계층
헤더 235
인터네트워크 계층 데이터 231
트레일러 237
전송 데이터 241

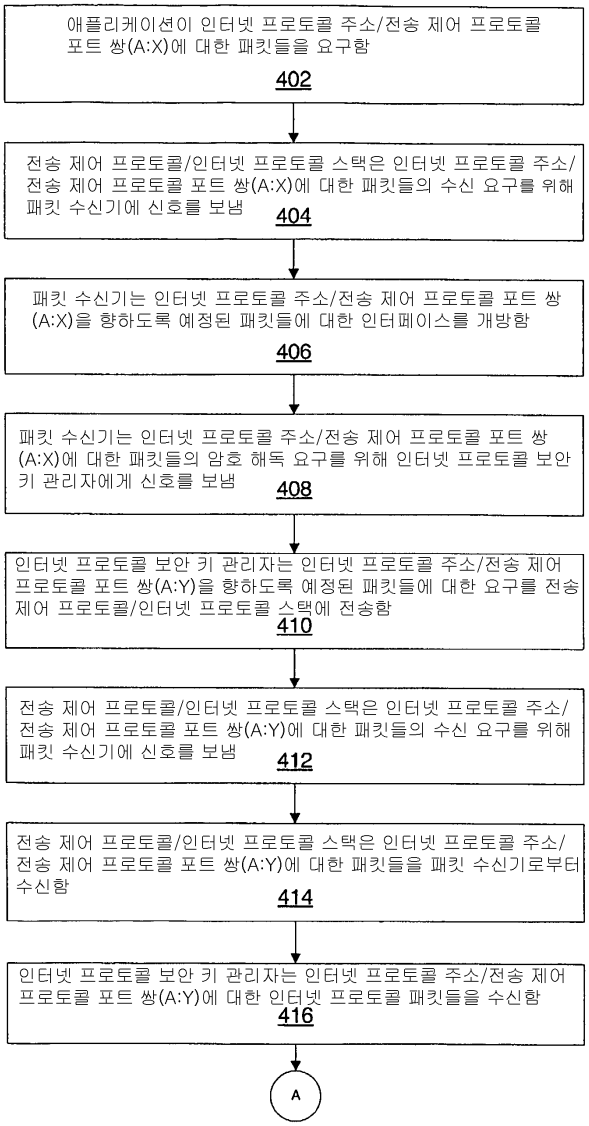
도면3a


300
인터넷 프로토콜 보안 키 관리자
308
애플리케이션
302
디지털권한관리
310
전송 제어 프로토콜/인터넷 프로토콜 스택
304
패킷 수신기
306
인터넷 프로토콜 보안 스택
312

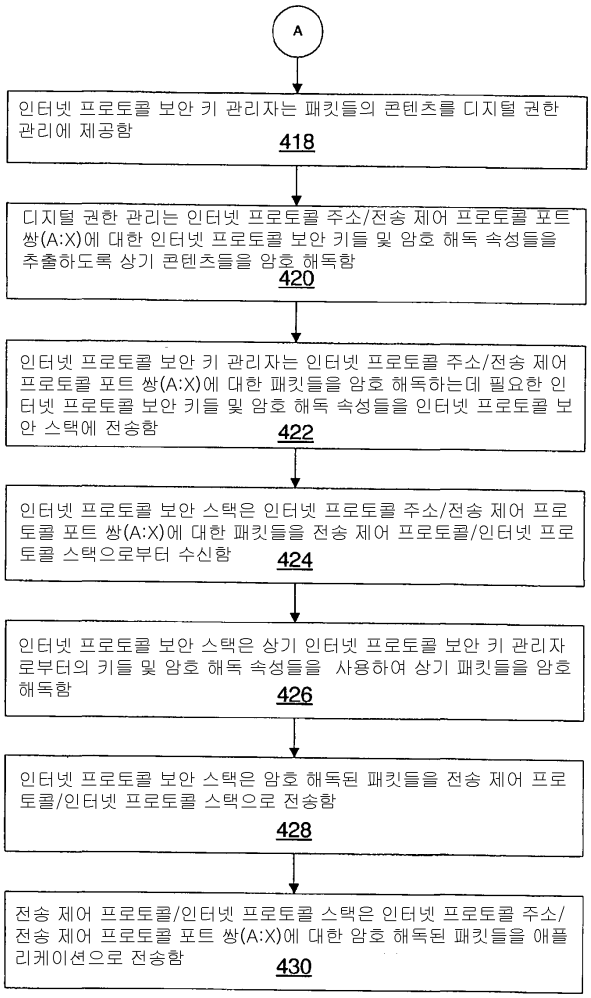
도면3b


인터넷 프로토콜 주소/포트 쌍(A:X)
으로부터의 데이터
인터넷 프로토콜 주소/포트 쌍(A:Y)
으로부터의 데이터
적어도 부분적으로
암호화된 데이터
암호 해독 정보
를 포함하는
데이터
암호 해독
정보 추출기
350
추출된
암호 해독
정보
암호 해독기
360
인터넷 프로토콜 주소/포트 쌍(A:X)
으로부터의 암호 해독된 데이터

도면4a


애플리케이션이 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)에 대한 패킷들을 요구함
402
전송 제어 프로토콜/인터넷 프로토콜 스택은 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)에 대한 패킷들의 수신 요구를 위해 패킷 수신기에 신호를 보냄
404
패킷 수신기는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)을 향하도록 예정된 패킷들에 대한 인터페이스를 개방함
406
패킷 수신기는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)에 대한 패킷들의 암호 해독 요구를 위해 인터넷 프로토콜 보안 키 관리자에게 신호를 보냄
408
인터넷 프로토콜 보안 키 관리자는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:Y)을 향하도록 예정된 패킷들에 대한 요구를 전송 제어 프로토콜/인터넷 프로토콜 스택에 전송함
410
전송 제어 프로토콜/인터넷 프로토콜 스택은 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:Y)에 대한 패킷들의 수신 요구를 위해 패킷 수신기에 신호를 보냄
412
전송 제어 프로토콜/인터넷 프로토콜 스택은 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:Y)에 대한 패킷들을 패킷 수신기로부터 수신함
414
인터넷 프로토콜 보안 키 관리자는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:Y)에 대한 인터넷 프로토콜 패킷들을 수신함
416
A

도면4b


A
인터넷 프로토콜 보안 키 관리자는 패킷들의 콘텐츠를 디지털 권한 관리에 제공함
418
디지털 권한 관리는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)에 대한 인터넷 프로토콜 보안 키들 및 암호 해독 속성들을 추출하도록 상기 콘텐츠들을 암호 해독함
420
인터넷 프로토콜 보안 키 관리자는 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)에 대한 패킷들을 암호 해독하는데 필요한 인터넷 프로토콜 보안 키들 및 암호 해독 속성들을 인터넷 프로토콜 보안 스택에 전송함
422
인터넷 프로토콜 보안 스택은 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)에 대한 패킷들을 전송 제어 프로토콜/인터넷 프로토콜 스택으로부터 수신함
424
인터넷 프로토콜 보안 스택은 상기 인터넷 프로토콜 보안 키 관리자로부터의 키들 및 암호 해독 속성들을 사용하여 상기 패킷들을 암호 해독함
426
인터넷 프로토콜 보안 스택은 암호 해독된 패킷들을 전송 제어 프로토콜/인터넷 프로토콜 스택으로 전송함
428
전송 제어 프로토콜/인터넷 프로토콜 스택은 인터넷 프로토콜 주소/전송 제어 프로토콜 포트 쌍(A:X)에 대한 암호 해독된 패킷들을 애플리케이션으로 전송함
430