(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0050233
(43) 공개일자 2018년05월14일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3236 (2013.01)
H04L 9/0822 (2013.01)
(21) 출원번호 10-2017-0144691
(22) 출원일자 2017년11월01일
심사청구일자 없음
(30) 우선권주장
16306445.4 2016년11월04일
유럽특허청(EPO)(EP)
17305661.5 2017년06월06일
유럽특허청(EPO)(EP)

(71) 출원인
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 잔 다르크 뤼 1-5
(72) 발명자
르 스꾸아르넥, 니꼴라
프랑스 35576 쎄쏭 쎄비네 쎄에스 176 16 자크 데샹 블랑 아브뉘 데 샹 블랑 975 떼끄니꼴로르 에르 에 데 프랑스
노이만, 크리스토프
프랑스 35576 쎄쏭 쎄비네 쎄에스 176 16 자크 데샹 블랑 아브뉘 데 샹 블랑 975 떼끄니꼴로르 에르 에 데 프랑스
(뒷면에 계속)
(74) 대리인
양영준, 전경석, 백만기

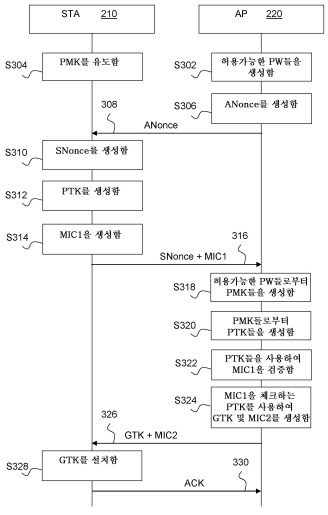
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **클라이언트 디바이스 인증을 위한 디바이스들 및 방법들**

(57) 요 약

액세스 포인트(220)는, 제1 넌스(SNonce) 및 제1 넌스에 대한 제1 암호화 해시(MIC1)를 클라이언트(210)로부터 수신하고 - 제1 암호화 해시는 제2 키(PMK)로부터 유도된 제1 키(PTK)를 사용하여 계산되고, 제2 키(PMK)는 클라이언트(210) 상에 입력되거나 또는 클라이언트(210) 상에 입력된 패스프레이즈로부터 유도됨 -, 저장된 1차 입력 및 유도에서 유효한 적어도 하나의 저장된 2차 입력 각각으로부터 제1 키들(PTK들)을 유도하고(S318, S320) - 저장된 1차 입력 및 적어도 하나의 저장된 2차 입력 각각은 제2 키(PMK) 및 패스프레이즈 중 하나임 -, 제1 암호화 해시(MIC1)를 체크하는 유도된 제1 키를 발견하기 위해 각각의 유도된 제1 키(PTK)를 사용하여 암호화 해시(MIC1)를 검증하고(S322), 제1 암호화 해시(MIC1)를 체크하는 유도된 제1 키를 사용하여 제3 키(GTK) 및 제2 암호화 해시(MIC2)를 생성하고(S324), 제3 키(GTK) 및 제2 암호화 해시(MIC2)를 클라이언트(210)에 전송한다.

대 표 도 - 도3



(52) CPC특허분류
H04L 9/0861 (2013.01)
H04L 9/3268 (2013.01)
(72) 발명자
힌, 올리비에
프랑스 35576 쎄쏭 쎄비네 쎄에스 176 16 자크 데샹 블랑 아브뉘 데 샹 블랑 975 떼끄니꼴로르 에르에 데 프랑스
비구루, 쟝-로낭
프랑스 35576 쎄쏭 쎄비네 쎄에스 176 16 자크 데샹 블랑 아브뉘 데 샹 블랑 975 떼끄니꼴로르 에르에 데 프랑스

명 세 서

청구범위

청구항 1

액세스 포인트(220)에서의 클라이언트 인증을 위한 방법으로서,

상기 액세스 포인트(220)의 적어도 하나의 하드웨어 프로세서(221)에서,

제1 넌스(SNonce) 및 상기 제1 넌스에 대한 제1 암호화 해시(MIC1)를 클라이언트(210)로부터 수신하는 단계 - 상기 제1 암호화 해시는 제2 키(PMK)로부터 유도된 제1 키(PTK)를 사용하여 계산되고, 상기 제2 키(PMK)는 상기 클라이언트(210) 상에 입력되거나 또는 상기 클라이언트(210) 상에 입력된 패스프레이즈(passphrase)로부터 유도됨 -;

저장된 1차 입력 및 상기 유도에서 유효한 적어도 하나의 저장된 2차 입력 각각으로부터 제1 키들(PTK들)을 유도하는 단계(S318, S320) - 상기 저장된 1차 입력 및 상기 적어도 하나의 저장된 2차 입력 각각은 제2 키(PMK) 및 패스프레이즈 중 하나임 -;

상기 제1 암호화 해시(MIC1)를 체크하는 유도된 제1 키를 발견하기 위해 각각의 유도된 제1 키(PTK)를 사용하여 상기 암호화 해시(MIC1)를 검증하는 단계(S322);

상기 제1 암호화 해시(MIC1)를 체크하는 상기 유도된 제1 키를 사용하여 제3 키(GTK) 및 제2 암호화 해시(MIC2)를 생성하는 단계(S324); 및

상기 제3 키(GTK) 및 상기 제2 암호화 해시(MIC2)를 상기 클라이언트(210)에 전송하는 단계

를 포함하는 방법.

청구항 2

제1항에 있어서,

각각의 저장된 2차 입력은 정의되고 제한된 유효 기간을 갖거나, 또는 각각의 저장된 2차 입력은 적어도 하나의 타이핑 에러를 갖는 상기 1차 입력에 대응하는 방법.

청구항 3

제1항에 있어서,

상기 액세스 포인트(210)는 Wi-Fi 액세스 포인트이고, 상기 방법은 제2 넌스(ANonce)를 상기 클라이언트(210)에 전송하는 단계(S308)를 더 포함하고, 상기 제1 키들(PTK들)은 상기 제1 넌스(SNonce) 및 상기 제2 넌스(ANonce)로부터 추가로 유도되는 방법.

청구항 4

제1항에 있어서,

상기 제3 키(GTK)는, 상기 제1 암호화 해시(MIC1)를 체크하는 상기 유도된 제1 키로부터 생성되는 암호 키를 사용하여 암호화되어 전송되는 방법.

청구항 5

제2항에 있어서,

저장된 2차 입력이 무효가 될 때 상기 제3 키를 갱신(renewing)하는 단계를 더 포함하는 방법.

청구항 6

액세스 포인트(220)로서,

통신 인터페이스(223) - 상기 통신 인터페이스는,

제1 넌스(SNonce) 및 상기 제1 넌스에 대한 제1 암호화 해시(MIC1)를 클라이언트(210)로부터 수신하고 - 상기 제1 암호화 해시는 제2 키(PMK)로부터 유도된 제1 키(PTK)를 사용하여 계산되고, 상기 제2 키(PMK)는 상기 클라이언트(210) 상에 입력되거나 또는 상기 클라이언트(210) 상에 입력된 패스프레이즈로부터 유도됨 -,

제3 키(GTK) 및 제2 암호화 해시(MIC2)를 상기 클라이언트(210)에 전송하도록

구성됨 -;

1차 입력 및 적어도 하나의 2차 입력을 저장하도록 구성된 메모리(222) - 상기 1차 입력 및 상기 적어도 하나의 2차 입력 각각은 제2 키(PMK) 및 패스프레이즈 중 하나임 -; 및

적어도 하나의 하드웨어 프로세서(221)

를 포함하고,

상기 적어도 하나의 하드웨어 프로세서는,

상기 저장된 1차 입력 및 상기 유도에서 유효한 적어도 하나의 2차 입력 각각으로부터 제1 키들(PTK들)을 유도하고,

상기 제1 암호화 해시(MIC1)를 체크하는 유도된 제1 키를 발견하기 위해 각각의 유도된 제1 키(PTK)를 사용하여 상기 암호화 해시(MIC1)를 검증하고,

상기 제1 암호화 해시(MIC1)를 체크하는 상기 유도된 제1 키를 사용하여 상기 제3 키(GTK) 및 상기 제2 암호화 해시(MIC2)를 생성하도록

구성되는 액세스 포인트.

청구항 7

제6항에 있어서,

각각의 저장된 2차 입력은 정의되고 제한된 유효 기간을 갖거나, 또는 각각의 저장된 2차 입력은 적어도 하나의 타이핑 에러를 갖는 상기 1차 입력에 대응하는 액세스 포인트.

청구항 8

제6항에 있어서,

상기 액세스 포인트(210)는 Wi-Fi 액세스 포인트이고, 상기 통신 인터페이스(223)는 제2 넌스(ANonce)를 상기 클라이언트(210)에 전송하도록 추가로 구성되고, 상기 적어도 하나의 하드웨어 프로세서(221)는 상기 제1 넌스(SNonce) 및 상기 제2 넌스(ANonce)로부터 추가로 상기 제1 키들(PTK들)을 유도하도록 구성되는 액세스 포인트.

청구항 9

제6항에 있어서,

상기 적어도 하나의 하드웨어 프로세서(221)는, 상기 클라이언트(210)로의 송신 이전에 상기 제1 암호화 해시(MIC1)를 체크하는 상기 유도된 제1 키로부터 생성되는 암호 키를 사용하여 상기 제3 키(GTK)를 암호화하도록 추가로 구성되는 액세스 포인트.

청구항 10

제8항에 있어서,

상기 적어도 하나의 하드웨어 프로세서(221)는, 저장된 2차 입력에 대한 유효 기간 동안에만 상기 저장된 2차 입력으로부터 제1 키들(PTK들)을 유도하도록 추가로 구성되는 액세스 포인트.

청구항 11

제7항에 있어서,

상기 적어도 하나의 하드웨어 프로세서는, 저장된 2차 입력이 무효가 될 때 상기 제3 키를 갱신하도록 추가로 구성되는 액세스 포인트.

청구항 12

Wi-Fi 보호 액세스(Wi-Fi Protected Access)(WPA) 2 엔터프라이즈 인증기 디바이스(230)에서 클라이언트 디바이스(210)를 인증하기 위한 방법으로서,

세션 식별자(SId) 및 제1 챌린지(challenge)(Ach)를 상기 클라이언트 디바이스(210)에 전송하는 단계(S404);

상기 클라이언트 디바이스(210)로부터, 사용자 이름, 제2 챌린지(SCh), 및 제1 챌린지(Ach), 제2 챌린지(SCh), 세션 식별자(SId) 및 패스프레이즈(PW)에 대한 암호화 해시(H)를 수신하는 단계(S408);

유효한 저장된 1차 패스프레이즈 또는 적어도 하나의 유효한 저장된 2차 패스프레이즈가 상기 암호화 해시(H)를 체크하는 경우, 제한되고 정의된 유효 기간 동안 유효한 각각의 저장된 2차 패스프레이즈 또는 적어도 하나의 타이핑 에러를 갖는 상기 1차 입력에 대응하는 각각의 저장된 2차 입력을 검증하는 단계(S410);

패스프레이즈가 상기 암호화 해시(H)를 체크하는 경우:

성공적인 인증을 표시하는 메시지를 상기 클라이언트 디바이스(210)에 전송하는 단계(S412); 및

키를 채택하기 위해 상기 클라이언트 디바이스(210)와 핸드셰이크를 수행하는 단계(S414)

를 포함하는 방법.

청구항 13

Wi-Fi 보호 액세스(WPA) 2 엔터프라이즈 인증기 디바이스(230)로서,

통신 인터페이스 - 상기 통신 인터페이스는,

세션 식별자(SId) 및 제1 챌린지(Ach)를 클라이언트 디바이스(210)에 전송하고,

상기 클라이언트 디바이스(210)로부터, 사용자 이름, 제2 챌린지(SCh), 및 제1 챌린지(Ach), 제2 챌린지(SCh), 세션 식별자(SId) 및 패스프레이즈(PW)에 대한 암호화 해시(H)를 수신하도록

구성됨 -; 및

적어도 하나의 하드웨어 프로세서

를 포함하고,

상기 적어도 하나의 하드웨어 프로세서는,

유효한 저장된 1차 패스프레이즈 또는 적어도 하나의 유효한 저장된 2차 패스프레이즈가 상기 암호화 해시(H)를 체크하는 경우, 제한되고 정의된 유효 기간 동안 유효한 각각의 저장된 2차 패스프레이즈 또는 적어도 하나의 타이핑 에러를 갖는 상기 1차 입력에 대응하는 각각의 저장된 2차 입력을 검증하고,

패스프레이즈가 상기 암호화 해시(H)를 체크하는 경우:

상기 통신 인터페이스를 통해, 성공적인 인증을 표시하는 메시지를 상기 클라이언트 디바이스(210)에 전송하고,

키를 채택하기 위해 상기 클라이언트 디바이스(210)와 핸드셰이크를 수행하도록

구성되는 WPA 2 엔터프라이즈 인증기 디바이스.

청구항 14

비일시적인 컴퓨터 판독가능 매체 상에 저장되고, 제1항 내지 제5항 중 적어도 한 항에 따른 방법의 단계들을 구현하기 위해 프로세서에 의해 실행가능한 프로그램 코드 명령어들을 포함하는 컴퓨터 프로그램 제품.

발명의 설명

기 술 분 야

[0001] 본 개시내용은 일반적으로 네트워크 보안에 관한 것이고, 특히 네트워크들에서 클라이언트 디바이스 인증에 관한 것이다.

배 경 기 술

[0002] 본 섹션은, 아래에서 설명되고 그리고/또는 청구되는 본 개시내용의 다양한 양태들과 관련될 수 있는 본 기술분야의 다양한 양태들을 독자에게 소개하도록 의도된다. 이러한 논의는 본 개시내용의 다양한 양태들의 더 양호한 이해를 돕기 위한 배경 정보를 독자에게 제공하는데 도움이 될 것으로 여겨진다. 따라서, 이러한 설명들은 선행 기술의 인정이 아니라 이러한 관점에서 읽혀져야 함을 이해해야 한다.

[0003] 무선 통신들에서, 소위 액세스 포인트로의 액세스를, 인가된 클라이언트 디바이스들로만 제한하는 것이 바람직하다. 가장 널리 확산된 무선 네트워킹 기술인 Wi-Fi가 본 명세서에서 비제한적인 예시로 사용될 것이다.

[0004] 클라이언트 디바이스들을 인증하기 위한 제1 솔루션은 인증서들을 사용하는 것이지만, 이들은 복잡한 설치 및 관리를 요구하기 때문에 이 솔루션은 많은 경우에 적절하지 않다.

[0005] 제2 솔루션은 사용자가 클라이언트 디바이스 상에 입력하는 공유된 암호를 사용하고, 그 다음, 클라이언트 디바이스는 공유된 비밀의 지식을 액세스 포인트에 입증한다.

[0006] 제2 솔루션은, 표준 IEEE 802.11i에 설명되고 도 1에 예시되는, WPA2 Personal로 지칭되는 제2 버전을 갖는, Wi-Fi 보호 액세스(Wi-Fi Protected Access)(WPA) Personal(또한 WPA-PSK(Pre-Shared Key)로도 공지됨)에서 널리 사용된다.

[0007] 단계들(S102 및 S104)에서, 클라이언트 디바이스(STA)와 액세스 포인트(AP)는, 패스워드-기반 키 유도 기능 2(Password-Based Key Derivation Function 2)(PBKDF2)로 지칭되는 키 유도 기능을 사용하여 공유된 패스프레이즈(passphrase), 서비스 세트 식별자(SSID)로 지칭되는 네트워크 식별자 및 SSID의 길이를 입력으로 취함으로써, 쌍단위 마스터 키(Pairwise Master Key)(PMK)를 서로 독립적으로 유도한다. 대안적으로, PMK는 64개의 16진수 문자들의 스트링으로서 입력될 수 있다.

[0008] 단계(S106)에서, AP는 메시지(108)에서 STA에 전송하는 난수(즉, 넌스) ANonce를 생성한다.

[0009] STA는 단계(S110)에서 난수(즉, 넌스) SNonce를 생성하고, 단계(S112)에서 넌스들로부터의 쌍단위 임시 키(PTK), PMK, 및 클라이언트 디바이스(STA) 및 액세스 포인트(AP)의 매체 액세스 제어(MAC) 어드레스들을 생성한다. 그 다음, STA는 단계(S114)에서, SNonce에 대한 메시지 무결성 코드(MIC)를 생성하고; MIC는 SNonce의 키잉된 암호화 해시(HMAC-SHA1 또는 AES-CMAC)이다. MIC는 128-비트 PTK를 키로서 사용한다. 그 다음, STA는 메시지(116)에서 SNonce 및 MIC를 AP에 전송한다.

[0010] SNonce 및 MIC를 수신하면, 단계(S118)에서 AP는 단계(S112)에서 STA가 수행한 것과 동일한 방식으로 PTK를 유도한다. 단계(S120)에서, AP는 MIC가 정확한 것을 검증한다. 이 때, STA 및 AP는 인증되고 동일한 PTK를 상호 유도한다.

[0011] AP는 그룹 임시 키(GTK) 및 제2 MIC(PTK의 비트들 128-256을 사용하여 암호화됨)를 사용하여 보호되는 시퀀스 번호를 포함하는 메시지(122)를 STA에 전송한다. 메시지(122)를 수신하면, STA는 단계(S124)에서 GTK를 설치하고, 이는 AP에 의해 관리되는 무선 네트워크에 패킷들을 전송하기 위해 사용될 수 있다. 마지막으로, STA는 확인응답(126)을 AP에 전송한다.

[0012] 다른 가능성은 확장가능한 인증 프로토콜(EAP)을 제공하기 위해 상이한 방식으로 작동하는 WPA-Enterprise이다. 많은 EAP 프로토콜들 중에서 보호된 확장가능한 인증 프로토콜(PEAP), 전송 계층 보안(TLS) 및 터널링된 전송 계층 보안(TTLS)이 가장 통상적이다. 이러한 것들 중, TLS는 클라이언트와 서버 둘 모두에서 인증서들을 요구하는 한편, TTLS 및 PEAP는, 이들 둘 모두가 서버 상의 인증서 및 클라이언트에 의해 입력되는 패스워드를 갖는다는 점에서 매우 유사하다.

[0013] 일례로, PEAP는 Microsoft의 챌린지 핸드셰이크 인증 프로토콜 버전 2(MS-CHAP v2)를 사용하여 다음과 같이 패스워드를 교환한다. 클라이언트 및 인증기(RADIUS 서버)는 AP를 통해 터널을 설정한다. 인증기는 세션 ID와 제1 챌린지를 클라이언트에 전송하고, 클라이언트는 사용자 이름, 제2 챌린지, 및 챌린지들의 해시, 세션 ID 및 사용자의 패스워드의 MD4 해시로 응답한다. RADIUS 서버는 해시를 체크하고 적절하게 성공 또는 실패로 응답하고, 클라이언트를 수락하도록 AP에 통지하여, AP로 하여금 공유된 키를 채택하도록 클라이언트와 4-웨이 핸드셰이크를 개시하게 한다.

[0014] 공유된 비밀들 및 패스워드들의 문제는, 이들을 입력하는 것이, 허용가능한 레벨의 보안을 제공하기 위해 종종 Wi-Fi의 경우와 같이, 입력할 데이터가 길거나 복잡한 경우 특히 에러에 취약한 작업이라는 점이다. 이러한 문제를 완화하기 위한 시도로, Wi-Fi 보호된 셋업(WPS)을 사용하는 것이 제안되었다. 그러나, iOS 디바이스들과 같은 많은 디바이스들은 WPS를 지원하지 않고, 보안 문제들로 인해 WPS의 일부 구현들이 곤란하여, 이들의 사용을 제한한다.

[0015] "pASSWORD tYPOS and How to Correct Them Securely"에서, Chatterjee 등은 패스워드들에서의 오타들을 허용하는 인증 방법들을 제안한다. 이 문서는 일부 공식적인 평가를 제공하지만, 이미 존재하는 인증 프로토콜에서 이러한 접근법을 통합하는 방법 또는 임의의 구현들을 제공함이 없이 오직 이론적인 솔루션들만을 제안한다.

[0016] 예를 들어, 클라이언트 디바이스의 수정을 필요로 하는 EP 2947591, EP 2876569, EP 3067811, US 2015/0363588 및 US 2015/0363593, 및 서버가 잘못된 패스워드들에 후속하는 정확한 패스워드를 입력하도록 허용하는 것을 학습하는 US 9280657에서 다른 오류-허용 솔루션들이 설명되었다. 따라서, 이러한 종래의 솔루션들은 단점들을 갖는다.

[0017] Wi-Fi와 같은 기술들에 기초하는 네트워크들에서 공유된 비밀들 및 패스워드들의 또 다른 문제점은 단일 공유된 암호 또는 패스워드를 사용한다는 점이다. 예를 들어, 네트워크에 게스트 액세스를 부여하기 위해, 이는, 게스트에게 네트워크 패스워드를 부여함으로써 수행된다. 이는, 네트워크 패스워드가 변경될 때까지 게스트가 네트워크에 계속 액세스할 수 있음을 의미하고, 이는, 네트워크 패스워드를 변경하는 것이 네트워크에 액세스를 가져야 하는 모든 디바이스에 대해 패스워드를 변경하는 것을 요구하기 때문에 불편하다.

[0018] 한편, 게이트웨이는 예를 들어 인터넷 액세스를 게스트에 제공하기 위해 제2 SSID를 사용할 수 있지만, 제2 SSID는 제1 SSID와 상이하기 때문에 이는 제1 SSID의 네트워크에 대한 액세스를 가능하게 하지 않는다.

[0019] 상이한 솔루션은 일회용 패스워드들의 사용이지만, 이들은 통상적으로 사용자들에 의해 사용되는 것과 동일한 네트워크에 대한 액세스를 게스트에게 제공하지 않는다.

[0020] 무선 통신 네트워크들에서 공유된 비밀들의 입력과 관련된 종래의 문제점들 중 적어도 일부를 극복하는 솔루션을 갖는 것이 바람직함을 이해할 것이다.

발명의 내용

[0021] 제1 양태에서, 본 원리는 액세스 포인트에서의 클라이언트 인증을 위한 방법에 관한 것이다. 액세스 포인트의 적어도 하나의 하드웨어 프로세서는, 제1 넌스 및 제1 넌스에 대한 제1 암호화 해시를 클라이언트로부터 수신하고 - 제1 암호화 해시는 제2 키로부터 유도된 제1 키를 사용하여 계산되고, 제2 키는 클라이언트 상에 입력되거나 또는 클라이언트 상에 입력된 패스프레이즈로부터 유도됨 -, 저장된 1차 입력 및 유도에서 유효한 적어도 하나의 저장된 2차 입력 각각으로부터 제1 키들을 유도하고 - 저장된 1차 입력 및 적어도 하나의 저장된 2차 입력 각각은 제2 키 및 패스프레이즈 중 하나임 -, 제1 암호화 해시를 체크하는 유도된 제1 키를 발견하기 위해 각각의 유도된 제1 키를 사용하여 암호화 해시를 검증하고, 제1 암호화 해시를 체크하는 유도된 제1 키를 사용하여 제3 키 및 제2 암호화 해시를 생성하고, 제3 키 및 제2 암호화 해시를 클라이언트에 전송한다.

[0022] 제1 양태의 다양한 실시예들은 다음을 포함한다:

[0023] 각각의 저장된 2차 입력은 정의되고 제한된 유효 기간을 갖거나, 적어도 하나의 타이핑 에러를 갖는 1차 입력에 대응한다. 저장된 2차 입력이 무효가 되는 경우, 제3 키가 갱신될 수 있다.

[0024] 액세스 포인트는, 제2 넌스를 클라이언트에 또한 전송하는 Wi-Fi 액세스 포인트이고, 제1 키들은 제1 넌스 및 제2 넌스로부터 추가로 유도된다.

[0025] 제1 암호화 해시를 체크하는 유도된 제1 키로부터 생성되는 암호 키를 사용하여 암호화된 제3 키가 전송된다.

[0026] 제2 양태에서, 본 원리들은, 제1 넌스 및 제1 넌스에 대한 제1 암호화 해시를 클라이언트로부터 수신하고 - 제1 암호화 해시는 제2 키로부터 유도된 제1 키를 사용하여 계산되고, 제2 키는 클라이언트 상에 입력되거나 또는 클라이언트 상에 입력된 패스프레이즈로부터 유도됨 -, 제3 키 및 제2 암호화 해시를 클라이언트에 전송하도록 구성되는 통신 인터페이스, 1차 입력 및 적어도 하나의 2차 입력을 저장하도록 구성되는 메모리 - 1차 입력 및 적어도 하나의 2차 입력 각각은 제2 키 및 패스프레이즈 중 하나임 -, 저장된 1차 입력 및 유도에서 유효한 적어도 하나의 2차 입력 각각으로부터 제1 키들을 유도하고, 제1 암호화 해시를 체크하는 유도된 제1 키를 발견하기 위해 각각의 유도된 제1 키를 사용하여 암호화 해시를 검증하고, 제1 암호화 해시를 체크하는 유도된 제1 키

를 사용하여 제3 키 및 제2 암호화 해시를 생성하도록 구성되는 적어도 하나의 하드웨어 프로세서를 포함하는 액세스 포인트에 관한 것이다.

[0027] 제2 양태의 다양한 실시예들은 다음을 포함한다:

[0028] 각각의 저장된 2차 입력은 정의되고 제한된 유효 기간을 갖거나, 적어도 하나의 타이핑 에러를 갖는 1차 입력에 대응한다. 저장된 2차 입력이 무효가 되는 경우, 제3 키가 갱신될 수 있다.

[0029] 액세스 포인트는 Wi-Fi 액세스 포인트이고, 통신 인터페이스는 제2 넌스를 클라이언트에 전송하도록 추가로 구성되고, 적어도 하나의 하드웨어 프로세서는 제1 넌스 및 제2 넌스로부터 제1 키들을 추가로 유도하도록 구성된다. 적어도 하나의 하드웨어 프로세서는 저장된 2차 입력에 대한 유효 기간 동안에만 저장된 2차 입력으로부터 제1 키들을 유도하도록 추가로 구성된다.

[0030] 적어도 하나의 하드웨어 프로세서는, 클라이언트로의 송신 전에 제1 암호화 해시를 체크하는 유도된 제1 키로부터 생성되는 암호 키를 사용하여 제3 키를 암호화하도록 추가로 구성된다.

[0031] 제3 양태에서, 본 원리들은, 세션 식별자 및 제1 챌린지를 클라이언트 디바이스에 전송하고, 사용자 이름, 제2 챌린지, 및 제1 챌린지, 제2 챌린지, 세션 식별자 및 패스프레이즈에 대한 암호화 해시를 클라이언트 디바이스로부터 수신하고, 유효한 저장된 1차 패스프레이즈 또는 적어도 하나의 유효한 저장된 2차 패스프레이즈가 암호화 해시를 체크하면, 제한되고 정의된 유효 기간 동안 유효한 각각의 저장된 2차 패스프레이즈 또는 적어도 하나의 타이핑 에러를 갖는 1차 입력에 대응하는 각각의 저장된 2차 입력을 검증하고, 패스프레이즈가 암호화 해시를 체크하는 경우, 성공적인 인증을 표시하는 메시지를 클라이언트 디바이스에 전송하고, 키를 채택하기 위해 클라이언트 디바이스와 핸드셰이크를 수행함으로써, Wi-Fi 보호 액세스 2 엔터프라이즈 인증기 디바이스에서 클라이언트 디바이스를 인증하기 위한 방법에 관한 것이다.

[0032] 제4 양태에서, 본 원리들은, 세션 식별자 및 제1 챌린지를 클라이언트 디바이스에 전송하고, 사용자 이름, 제2 챌린지, 및 제1 챌린지, 제2 챌린지, 세션 식별자 및 패스프레이즈에 대한 암호화 해시를 클라이언트 디바이스로부터 수신하도록 구성되는 통신 인터페이스, 및 유효한 저장된 1차 패스프레이즈 또는 적어도 하나의 유효한 저장된 2차 패스프레이즈가 암호화 해시를 체크하면, 제한되고 정의된 유효 기간 동안 유효한 각각의 저장된 2차 패스프레이즈 또는 적어도 하나의 타이핑 에러를 갖는 1차 입력에 대응하는 각각의 저장된 2차 입력을 검증하고, 패스프레이즈가 암호화 해시를 체크하는 경우, 통신 인터페이스를 통해, 성공적인 인증을 표시하는 메시지를 클라이언트 디바이스에 전송하고, 키를 채택하기 위해 클라이언트 디바이스와 핸드셰이크를 수행하도록 구성되는 적어도 하나의 하드웨어 프로세서를 포함하는 Wi-Fi 보호 액세스 2 엔터프라이즈 인증기 디바이스에 관한 것이다.

[0033] 제5 양태에서, 본 원리들은 제1 양태의 임의의 실시예에 따른 방법의 단계들을 구현하기 위해 프로세서에 의해 실행가능한 프로그램 코드 명령어들을 포함하는 컴퓨터 프로그램에 관한 것이다.

[0034] 제6 양태에서, 본 원리들은 제1 양태의 임의의 실시예에 따른 방법의 단계들을 구현하기 위해 프로세서에 의해 실행가능한 프로그램 코드 명령어들을 포함하고 비일시적인 컴퓨터 판독가능 매체 상에 저장되는 컴퓨터 프로그램에 관한 것이다.

도면의 간단한 설명

[0035] 본 원리들의 바람직한 특징들은 이제, 첨부된 도면들을 참조하여 비제한적인 예로써 설명될 것이다.

도 1은 종래의 Wi-Fi 보호 액세스(WPA) 개인 프로토콜을 예시한다.

도 2는 본 원리들의 제1 실시예에 따른 예시적인 시스템을 예시한다.

도 3은 본 원리들의 실시예에 따른 디바이스 삽입을 위한 예시적인 방법을 예시한다.

도 4는 본 원리들의 추가적인 실시예에 따른 디바이스 삽입을 위한 예시적인 방법을 예시한다.

발명을 실시하기 위한 구체적인 내용

[0036] 도 2는 본 원리들의 제1 실시예에 따른 예시적인 시스템(200)을 예시한다. 시스템(200)은 클라이언트 디바이스(STA)(210) 및 게이트웨이와 같은 액세스 포인트(AP)(220)를 포함한다. 액세스 포인트(220)는 로컬 네트워크(240) 및 외부 네트워크(250), 예를 들어 인터넷과 인터페이싱하도록 구성되고, 이를 통해 다른 네트워크(도시

되지 않음) 내의 디바이스들에 대한 접속들이 수행될 수 있다. 예시적인 시스템에서, 로컬 네트워크(240)는 Wi-Fi 네트워크이다.

[0037] 클라이언트 디바이스(210) 및 액세스 포인트(220) 각각은 예를 들어 Wi-Fi 인터페이스에서 다른 디바이스들과 통신하도록 구성되는 적어도 하나의 하드웨어 프로세싱 유닛("프로세서")(211, 221), 메모리(212, 222) 및 적어도 하나의 통신 인터페이스(213, 223)를 포함한다. 당업자는, 예시된 디바이스들이 명료성의 이유로 매우 단순화되고 실제 디바이스는 내부 접속들 및 파워 서플라이와 같은 특징들을 추가로 포함할 것임을 인식할 것이다. 비일시적인 저장 매체(260)는 프로세서에 의해 실행되는 경우, 이하 추가로 설명되는 바와 같이 액세스 포인트(220)의 기능들을 수행하는 명령들을 저장한다.

[0038] 가능하게는 로컬 네트워크(240)에 접속되는 클라이언트 디바이스(210)는 사용자 인터페이스(214)를 더 포함한다. 클라이언트 디바이스는 예를 들어 랩탑, 스마트폰 또는 태블릿일 수 있다.

[0039] 액세스 포인트(220)는 로컬 네트워크(240)와 외부 네트워크(250)를 인터페이싱하는 것과 같은 종래의 액세스 포인트 기능들을 수행하도록 구성된다. 액세스 포인트(220)가 예를 들어 분리된 서브넷들의 형태로 복수의 로컬 네트워크들을 제공할 수 있기 때문에, 복수의 클라이언트 디바이스들은 로컬 네트워크(240)에 또는 이를 통해 하나의 로컬 네트워크에 접속될 수 있다. 통상적으로, 네트워크 키와 같은 공유된 네트워크 비밀에 대한 지식을 입증하는 임의의 디바이스는 로컬 네트워크(240)에 대한 액세스가 주어진다.

[0040] 외부 네트워크(250)는 가능하게는 다른 액세스 포인트들(도시되지 않음)을 통해 서버들 및 다른 디바이스들에 접속하기 위해 사용될 수 있다.

[0041] 도 3은 본 원리들의 실시예에 따른 디바이스 삽입을 위한 예시적인 방법을 예시한다.

[0042] 단계(S302)에서, 액세스 포인트("AP")(220)의 프로세서(221)는 액세스 포인트(220)의 구성에서 설정된 메인 패스프레이즈로부터 오류가 있지만 허용가능한 패스프레이즈들의 제한된 세트를 생성하고, 이 세트는 메인 패스프레이즈를 포함한다. 즉, 프로세서(221)는 원래의, 정확한 패스프레이즈 및 적어도 하나의 에러를 포함하는 다수의 변형된 패스프레이즈들을 포함하는 패스프레이즈들의 세트를 생성하고 저장한다. 도입된 에러들은 예를 들어 아래와 같은 통상적인 에러들에 대응하는 것이 선호된다 (괄호 안의 32개 문자 패스프레이즈에 대한 원래의 패스프레이즈를 포함하는 변형들의 수와 함께):

[0043] 임의의 랜덤 위치에서 문자를 생략하는 것(33);

[0044] 대문자를 전환하는 것(2);

[0045] 4개 문자마다 스페이스를 추가하는 것(9);

[0046] I(대문자 i)를 l(소문자 L)로 대체하는 것(2);

[0047] 0(제로)을 O로 대체하는 것(2);

[0048] 하나의 문자(임의의 하나)를 4개의 가장 가까운 것 중 하나로 대체하는 것(4*32+1=129);

[0049] 하나 또는 2개의 문자(임의의 둘)를 4개의 가장 가까운 것 중 하나로 대체하는 것 ($\binom{32}{2} * 4 + 32 * 4 + 1 = 2113$).

[0050] 이들의 임의의 조합(변형들의 수의 곱, 5020488). 이러한 에러들의 조합을 허용하는 경우에도 최대 23 비트의 엔트로피가 제거된다. 문자가 출고시 설정된 패스프레이즈들에서 통상적인 16진수(0-9A-F)인 경우, 원래의 엔트로피는 32 * 4 = 128 비트이다. 이러한 모든 에러들을 허용하는 것은 (적어도) 105 비트의 엔트로피를 남기고, 이는 많은 경우들에서 여전히 충분하다.

[0051] 변형에서, 액세스 포인트("AP")(220)의 프로세서(221)는 메인, 디폴트 패스프레이즈 및 적어도 하나의 유효한 2차 패스프레이즈를 포함하는 허용가능한 패스프레이즈들의 세트를 생성한다. 메인 패스프레이즈는 통상적으로 네트워크의 정규의 사용자들에 의해 사용되고, 예를 들어 네트워크의 사용자 또는 관리자에 의해 변경될 때까지 유효하게 유지되는 패스프레이즈이다. 제2 패스프레이즈는 예를 들어 네트워크의 게스트에 의해 사용되고; 이의 유효성은 통상적으로 시간에서 제한되지만 이는 또한 취소될 때까지 유효할 수 있다.

[0052] 이러한 변형에서, 프로세서(221)는 각각 하루 동안 유효한 2차 패스프레이즈들을 생성하도록 구성될 수 있다. 그 다음, 허용가능한 패스프레이즈들의 세트는 당일 동안 유효한 메인 패스프레이즈 및 2차 패스프레이즈를 포

함한다. 예를 들어, 프로세서는 매일 예를 들어 반복적인 단방향 해싱을 사용하여, 당일 및 후속 N일 동안의 2차 패스프레이즈들을 생성할 수 있다. 이러한 2차 패스프레이즈들은 AP(도시되지 않음)의 사용자 인터페이스에서 디스플레이되거나 또는 자신의 UI(214) 상에의 디스플레이를 위해 메인 패스프레이즈를 사용하여 접속된 사용자의 디바이스 또는 전용 애플리케이션을 실행하는 디바이스에 전송될 수 있다. 프로세서(221)가 복수의 2차 패스프레이즈들을 생성하게 함으로써, 게스트는 복수의 일 동안 즉시 액세스를 부여받을 수 있다.

[0053] 변형의 실시예에서, 액세스 포인트는 "게스트 WPS 버튼"을 포함한다. 이 버튼은, (디폴트 패스프레이즈 대신에) 당일의 패스프레이즈가 클라이언트에 푸시되는 것을 제외하고는 WPS와 동일한 메커니즘을 구현한다.

[0054] 변형의 실시예에서, 사용자는 게스트 디바이스 상의 Wi-Fi 보호 셋업 버튼을 활성화하고, AP(220) 상의 Wi-Fi 보호 셋업 버튼을 활성화한다. 그 다음, AP 및 게스트 디바이스는 Diffie-Hellman 키 교환을 수행하고, 그 후 AP가 당일의 패스프레이즈를 게스트 디바이스에 전송하고, 게스트 디바이스는 네트워크에 대한 접속 동안 패스프레이즈를 사용하고, 그 후 AP는 위에서 설명된 바와 같이 인증을 수행한다.

[0055] 도 1에서 설명된 종래의 프로토콜과의 현저한 차이로서, 액세스 포인트(220)는 반드시 시작 시에 PMK를 유도할 필요는 없고 클라이언트 디바이스("STA")(210)로부터 SNonce + MIC를 수신할 때까지 대기할 수 있다. 프로토콜은 클라이언트 디바이스(210)에 대해 불변으로 유지되는 점을 주목한다.

[0056] 단계(S304)에서, 클라이언트 디바이스(210)는, 입력 패스프레이즈, 서비스 세트 식별자(SSID)로 지칭되는 네트워크 식별자 및 SSID의 길이를 입력으로 취하는 키 유도 기능(이 예에서는 PBKDF2)을 사용하여 쌍단위 마스터 키(PMK)를 유도한다. 대안적으로, PMK는 64개의 16진수 문자들의 스트링으로서 입력될 수 있다.

[0057] 단계(S306)에서, 액세스 포인트(220)는 메시지(308)에서 클라이언트 디바이스(210)에 전송할 난수 ANonce를 생성한다.

[0058] 클라이언트 디바이스(210)는 단계(S310)에서 다른 난수 SNonce를 생성하고, 단계(S312)에서 넌스들로부터의 쌍단위 임시 키(PTK), PMK, 및 클라이언트 디바이스(210) 및 액세스 포인트(220)의 매체 액세스 제어(MAC) 어드레스들을 생성한다. 그 다음, 클라이언트 디바이스(210)는 단계(S314)에서, SNonce에 대한 메시지 무결성 코드(MIC) - 도 3에서는 MIC1 - 를 생성하고; MIC1은 SNonce의 키잉된 암호화 해시(HMAC-SHA1 또는 AES-CMAC)이다. MIC는 128비트 PTK를 키로서 사용한다. 그 다음, 클라이언트 디바이스(210)는 SNonce 및 MIC1을 메시지(316)에서 액세스 포인트(220)에 전송한다.

[0059] SNonce 및 MIC1의 수신 시에, 액세스 포인트(220)는 단계(S318)에서, 허용가능한 패스프레이즈들의 세트의 각각의 패스프레이즈로부터 PMK를 유도한다. 생성된 PMK들은 허용가능한 패스프레이즈들의 세트 대신에 또는 그에 추가로 저장될 수 있다. 대안적으로, PMK가 64개의 16진수 문자들의 스트링으로서 입력되는 경우, 액세스 포인트들(220)은 정확한 PMK로부터 허용가능한 PMK들을 유도하고 저장한다. 이러한 단계는 사전에, 예를 들어 단계(S302) 직후에 수행될 수 있음을 주목한다.

[0060] 단계(S320)에서, 액세스 포인트(220)는 단계(S312)에서 클라이언트 디바이스(210)가 수행한 것과 동일한 생성 방법을 사용하여 단계(S318)에서 생성된 각각의 PMK에 대한 PTK를 생성한다.

[0061] 단계(S322)에서, 액세스 포인트(220)는 단계(S320)에서 생성된 임의의 PTK에 대해 MIC1이 정확한 것을 검증한다. PTK가 MIC1의 검증을 가능하게 하면, 이러한 PTK는 현재 PTK로 설정된다. 이 때, 액세스 포인트(220) 및 클라이언트 디바이스(210)는 인증되고 (메인 또는 2차 패스프레이즈로부터) 동일한 PTK를 상호 유도한다. 어떠한 PTK도 MIC의 검증을 가능하게 하지 않으면, 도 1에 예시된 종래의 방법에서 부정확한 패스프레이즈가 입력된 것처럼, 클라이언트 디바이스(210)는 인증되지 않는다는 점을 주목한다.

[0062] 액세스 포인트(220)는 단계(S324)에서 그룹 임시 키(GTK) 및 (PTK의 비트들 128-256을 사용하여 암호화된) 제2 MIC - 도 3의 MIC2 - 를 사용하여 보호되는 시퀀스 번호를 생성하고, 이들은 메시지(326)에서 클라이언트 디바이스(210)에 전송된다. 메시지(326)를 수신하면, 클라이언트 디바이스(210)는 단계(S328)에서 GTK를 설치하고, 이는 액세스 포인트(220)에 의해 관리되는 무선 네트워크에 패킷들을 전송하기 위해 사용될 수 있다. 마지막으로, 클라이언트 디바이스(210)는 확인응답(330)을 액세스 포인트(220)에 전송한다.

[0063] 확인할 수 있는 바와 같이, 액세스 포인트(220)는 허용가능한 패스프레이즈들의 세트에서, 수신된 MIC, 즉, MIC1이 유효한 패스프레이즈를 발견하려 시도한다. 이러한 패스프레이즈가 발견되면, 클라이언트는 인증될 수 있고, 패스프레이즈는 교환의 나머지(즉, PTK를 유도하고 GTK를 암호화하고 메시지들에 서명하는 것)에 기초하여 사용된다.

[0064] 액세스 포인트는 바람직하게는, 주어진 클라이언트 디바이스(그 MAC 어드레스에 의해 식별됨)에 의해 사용되는 PMK를 저장한다. 즉, 액세스 포인트는 MIC의 검증을 가능하게 하는 PTK를 생성한 PMK를 저장한다. 이러한 방식으로, 다음에 클라이언트 디바이스가 접속할 때 액세스 포인트는 저장된 PMK를 검색할 수 있고, 이는 재접속 시에 추측되는 패스프레이즈들의 수를 감소시킬 수 있다.

[0065] 시간 제한된 패스프레이즈들을 갖는 변형에서, 액세스 포인트(220)는, 유효 일자가 종료된 경우 당일 키를 취소하는 것과 같이 더 이상 유효하지 않은 2차 키들을 취소하는 것이 바람직하다.

[0066] 2차 키 취소에 대한 간단한 접근법은 2차 키가 만료될 때마다 액세스 포인트(220)가 GTK를 갱신하는 것이다. GTK는 IEEE 802.11i에 정의된 소위 그룹 키 핸드셰이크 메커니즘을 사용하여 갱신될 수 있다. 물론, 다른 적절한 메커니즘들이 또한 사용될 수 있다.

[0067] 2차 키 취소에 대한 더욱 정교한 접근법은 게스트 디바이스에 의해 2차 키가 사용되었는지 여부를 액세스 포인트(220)가 추적하는 것이다. 2차 키가 사용되지 않았다면, 2차 키가 만료된 경우 GTK를 갱신할 필요가 없다. 만료된 2차 키가 2차 키의 유효 기간 동안 사용된 경우에만, 예를 들어, 그룹 키 핸드셰이크 메커니즘을 사용하여 GTK가 갱신된다.

[0068] 본 원리들은 패스워드 기반 WPA2 엔터프라이즈(PEAP/EAP-TTLS)의 경우로 확장된다. Wi-Fi의 경우, 인증이 성공인지 여부를 결정하기 위해 허용가능한 패스워드들의 세트가 시도된다.

[0069] 도 4는 본 원리들의 추가적인 실시예에 따른 디바이스 삽입을 위한 예시적인 방법을 예시한다.

[0070] 도 4는 도 2의 클라이언트 디바이스와 동일할 수 있는 클라이언트 디바이스(210)를 예시한다. 도면은 또한 간결성을 이유로 예시되지는 않았지만, 적어도 하나의 하드웨어 프로세싱 유닛("프로세서"), 메모리 및 다른 디바이스들과 통신하도록 구성된 적어도 하나의 통신 인터페이스를 포함하는 인증기(230)를 도시한다.

[0071] 단계(S402)에서, 클라이언트 디바이스(210)는 액세스 포인트(도 2의 220)를 통해 RADIUS 서버와 같은 인증기 디바이스(230)와 전송 레벨 보안(TLS) 터널을 설정한다. 인증기(230)는 메시지(404)에서 클라이언트 디바이스(210)에 세션 ID(SId) 및 챌린지(ACh)를 전송한다. 클라이언트 디바이스(210)는 단계(S406)에서, 사용자 이름, 챌린지(SCh), 및 챌린지들(Ach, SCh), 세션 ID(SId) 및 사용자 패스워드의 MD4 해시를 갖는 메시지(408)를 생성한다. 메시지(408)는 인증기(230)에 전송된다. 지금까지, 이 방법은 종래의 방법에 대응한다.

[0072] 단계(S410)에서, 인증기(230)는, 사용자에 대한 허용가능한 사용자 패스워드들의 세트 내의 임의의 사용자 패스워드가 해시 H를 체크하는지 여부; 즉, 허용가능한 사용자 패스워드들의 세트에서, 챌린지들(Ach, SCh), 세션 ID(SId) 및 사용자 패스워드의 계산된 MD4 해시가 메시지(408)에서 수신된 해시 H와 동일한지 여부를 체크한다.

[0073] 그 다음, 인증기(230)는 메시지(412)를 클라이언트 디바이스(210)에 전송한다. 세트 내의 어떠한 패스워드도 해시 H를 체크하지 않으면, 메시지(412)는 실패를 표시하고, 클라이언트 디바이스(210)는 인증되지 않고 방법은 종료된다. 그러나, 패스워드가 해시 H를 체크하면, 메시지(412)는 성공을 표시하고 클라이언트 디바이스(210)는 인증된다. 그 다음, 클라이언트 디바이스(210) 및 인증기는 키를 채택하기 위해 단계(S414)에서 종래의 4-웨이 핸드셰이크를 개시한다.

[0074] 인식될 바와 같이, 본 원리들은 기존의 클라이언트들과 함께 동작하며, 실시예에 따라 액세스 포인트 또는 RADIUS 서버들에서의 수정만을 요구한다. 추가로, 원래의 패스프레이즈 또는 패스워드는 세트의 일부이고, 방법들은 하위 호환가능하다.

[0075] 도면들에 도시된 엘리먼트들은 다양한 형태들의 하드웨어, 소프트웨어 또는 이들의 조합들로 구현될 수 있음을 이해해야 한다. 바람직하게는, 이러한 엘리먼트들은 프로세서, 메모리 및 입/출력 인터페이스들을 포함할 수 있는 하나 이상의 적절히 프로그래밍된 범용 디바이스들 상에서 하드웨어 및 소프트웨어의 조합으로 구현된다.

[0076] 본 설명은 본 개시내용의 원리들을 예시한다. 따라서, 본 기술분야의 통상의 기술자들은 본원에 명시적으로 설명되거나 도시되지는 않았지만, 본 개시내용의 원리들을 구현하고 그 범위 내에 포함되는 다양한 배열들을 고안할 수 있을 것임을 인식할 것이다.

[0077] 본원에 인용된 모든 예들 및 조건부 언어는, 독자가 본 개시내용의 원리들 및 발명자가 기술을 발전시키는데 기여한 개념들을 이해하는 것을 돕는 교육적 목적을 위한 것이고, 이러한 특별히 인용된 예들 및 조건들을 제한하지 않는 것으로 해석되어야 한다.

[0078] 또한, 본 개시내용의 원리들, 양태들 및 실시예들뿐만 아니라 이의 특정 예들을 기재한 본 명세서의 모든 설명

들은 이의 구조적 및 기능적 등가물들 둘 모두를 포함하도록 의도된다. 추가적으로, 이러한 균등물들은 현재 공지된 균등물들뿐만 아니라 장래에 개발되는 균등물들, 즉 구조와 무관하게, 동일한 기능을 수행하는 임의의 개발된 엘리먼트들 모두를 포함하는 것으로 의도된다.

[0079] 따라서, 예를 들어, 본 명세서에 제시된 블록도들은 본 개시내용의 원리들을 구현하는 예시적인 회로의 개념도들을 표현함을 본 기술분야의 통상의 기술자들은 인식할 것이다. 유사하게, 임의의 플로우차트들, 흐름도들, 상태 전이도들, 의사 코드 등은 컴퓨터 판독가능 매체에서 실질적으로 표현될 수 있고, 따라서 컴퓨터 또는 프로세서가 명시적으로 도시되든 도시되지 않든 이러한 컴퓨터 또는 프로세서에 의해 실행될 수 있는 다양한 프로세스들을 표현함을 인식할 것이다.

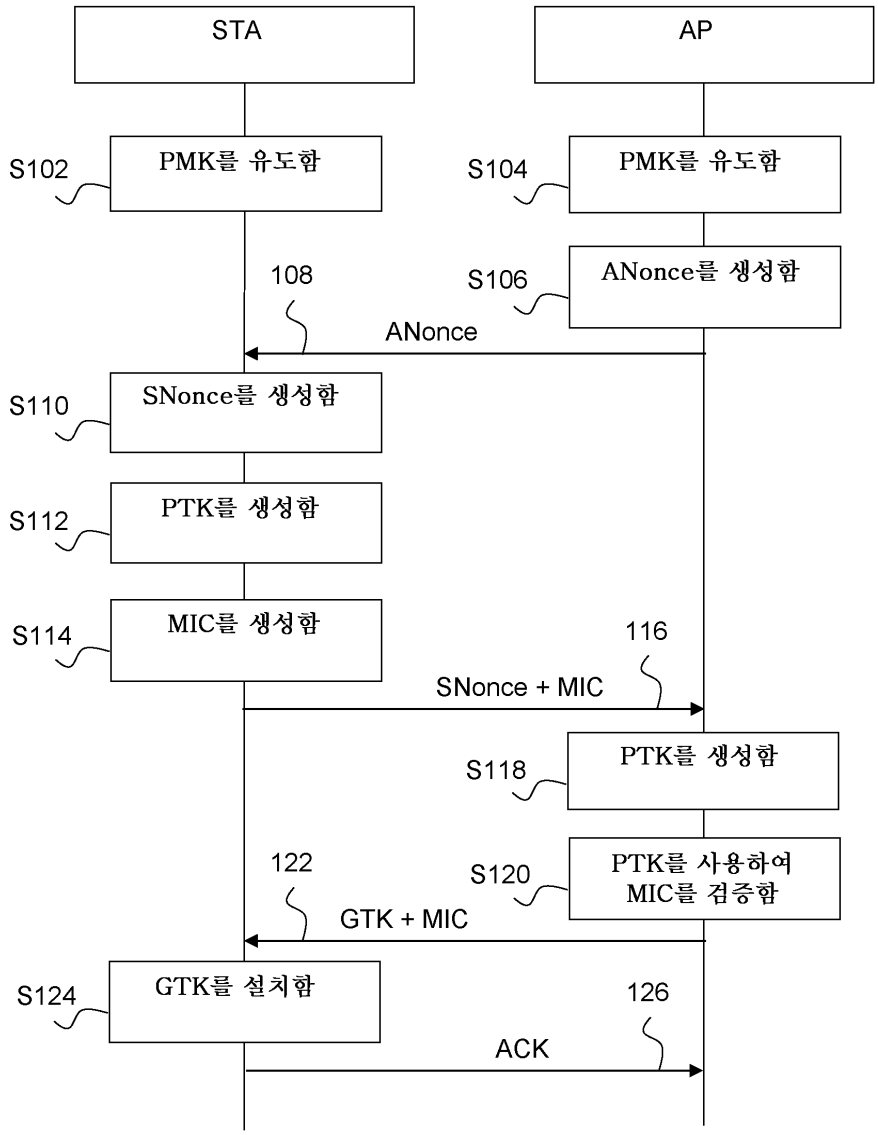
[0080] 도면들에 도시된 다양한 엘리먼트들의 기능들은 적절한 소프트웨어와 관련하여 소프트웨어를 실행할 수 있는 하드웨어뿐만 아니라 전용 하드웨어의 사용을 통해 제공될 수 있다. 프로세서에 의해 제공되는 경우, 기능들은 단일 전용 프로세서, 단일 공유 프로세서, 또는 복수의 개별적인 프로세서들에 의해 제공될 수 있고, 이들 중 일부는 공유될 수 있다. 또한, 용어 "프로세서" 또는 "제어기"의 명시적 사용은 소프트웨어를 실행할 수 있는 하드웨어만을 배타적으로 지칭하는 것으로 해석되어서는 안되며, 제한 없이, 디지털 신호 프로세서(DSP) 하드웨어, 소프트웨어를 저장하기 위한 판독 전용 메모리(ROM) 소프트웨어, 랜덤 액세스 메모리(RAM) 및 비휘발성 스토리지를 묵시적으로 포함할 수 있다.

[0081] 다른 하드웨어(종래 및/또는 주문형)가 또한 포함될 수 있다. 유사하게, 도면들에 도시된 임의의 스위치들은 단지 개념적이다. 이들의 기능은 프로그램 로직의 동작을 통해, 전용 로직을 통해, 프로그램 제어 및 전용 로직의 상호작용을 통해, 또는 심지어는 수동으로 수행될 수 있고, 특정 기술은 문맥으로부터 더 구체적으로 이해되는 바와 같이 구현자에 의해 선택가능하다.

[0082] 본 명세서의 청구항들에서, 특정 기능을 수행하기 위한 수단으로 표현된 임의의 엘리먼트는 예를 들어 a) 그 기능을 수행하는 회로 엘리먼트들의 조합 또는 b) 임의의 형태의 소프트웨어를 포함하는 그 기능을 수행하는 임의의 방법을 포함하도록 의도되고, 따라서, 기능을 수행하기 위해 그 소프트웨어를 실행하기 위한 적절한 회로와 결합된 펌웨어, 마이크로코드 등을 포함한다. 이러한 청구항들에 의해 정의된 바와 같은 개시내용은, 다양한 인용된 수단들에 의해 제공되는 기능들이, 청구항들이 요구하는 방식으로 조합되고 결합된다는 사실에 있다. 따라서, 이러한 기능들을 제공할 수 있는 임의의 수단은 본 명세서에 제시된 것들과 동등하다고 간주된다.

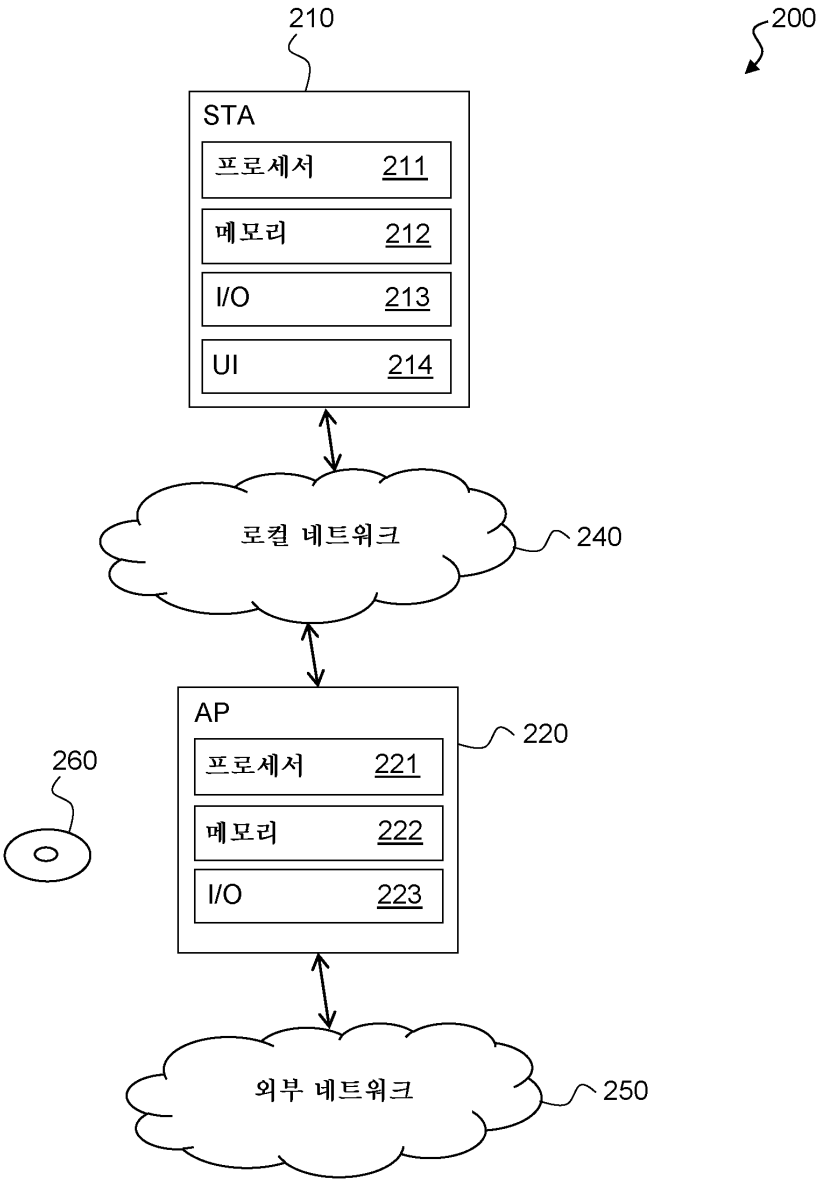
도면

도면1

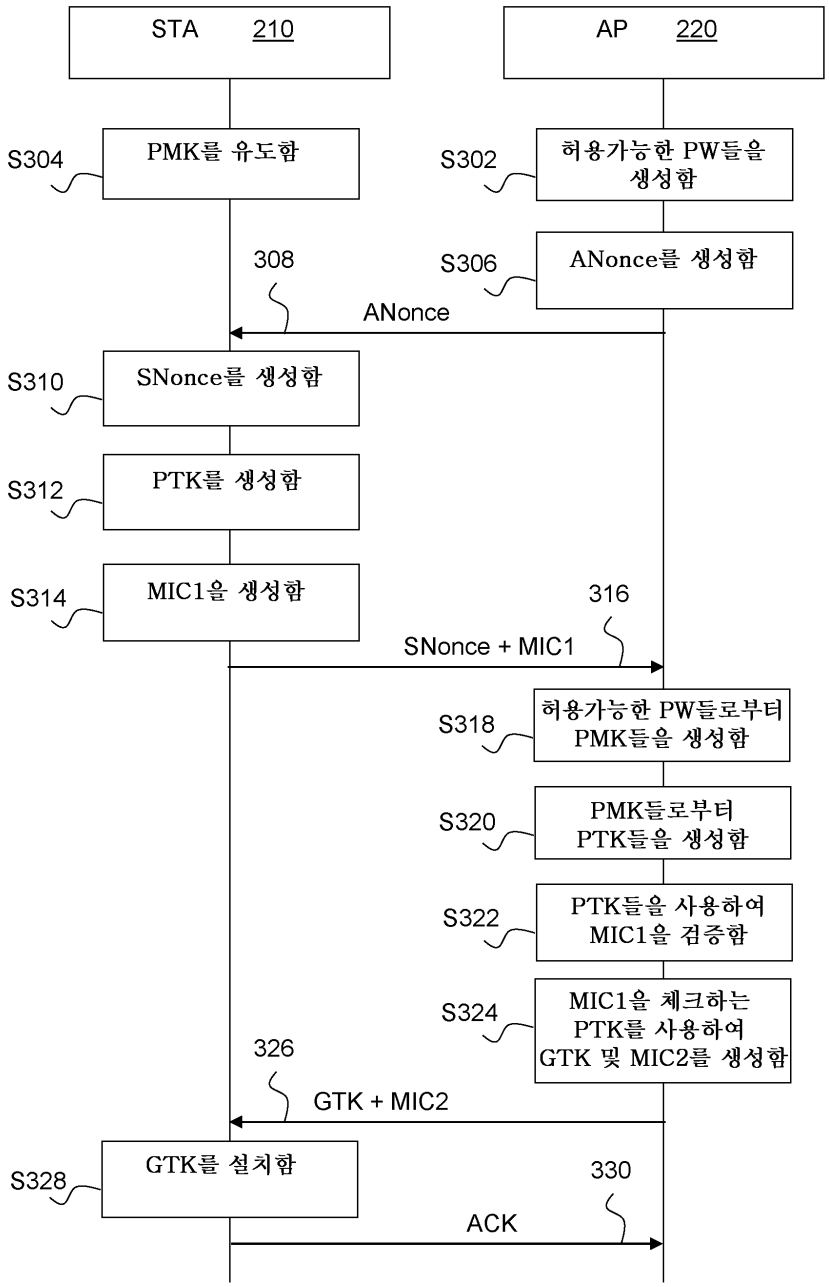

STA
AP
S102
PMK를 유도함
S104
PMK를 유도함
108
S106
ANonce를 생성함
ANonce
S110
SNonce를 생성함
S112
PTK를 생성함
S114
MIC를 생성함
116
SNonce + MIC
S118
PTK를 생성함
122
S120
PTK를 사용하여
MIC를 검증함
GTK + MIC
S124
GTK를 설치함
126
ACK

(종래 기술)

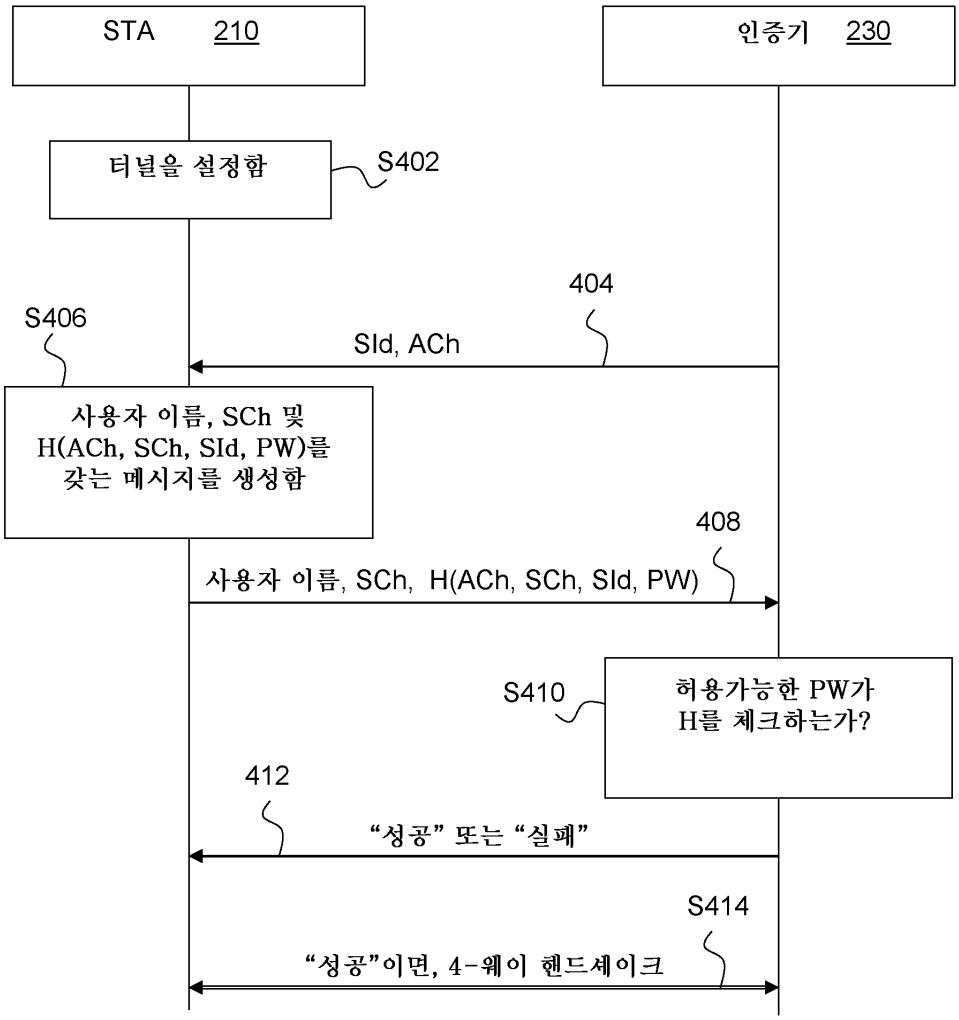
도면2


210
200
STA
프로세서 211
메모리 212
I/O 213
UI 214
로컬 네트워크
240
AP
220
프로세서 221
메모리 222
I/O 223
260
외부 네트워크
250

도면3


STA 210
AP 220
S304
PMK를 유도함
S302
허용가능한 PW들을 생성함
308
S306
ANonce를 생성함
ANonce
S310
SNonce를 생성함
S312
PTK를 생성함
S314
MIC1을 생성함
316
SNonce + MIC1
S318
허용가능한 PW들로부터 PMK들을 생성함
S320
PMK들로부터 PTK들을 생성함
S322
PTK들을 사용하여 MIC1을 검증함
S324
MIC1을 체크하는 PTK를 사용하여 GTK 및 MIC2를 생성함
326
GTK + MIC2
S328
GTK를 설치함
330
ACK

도면4


STA 210
인증기 230
터널을 설정함
S402
404
S406
SId, ACh
사용자 이름, SCh 및
H(ACh, SCh, SId, PW)를
갖는 메시지를 생성함
408
사용자 이름, SCh, H(ACh, SCh, SId, PW)
S410
허용가능한 PW가
H를 체크하는가?
412
"성공" 또는 "실패"
S414
"성공"이면, 4-웨이 핸드셰이크