(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
H04L 9/32 (2006.01)
H04L 12/28 (2006.01)

(11) 공개번호 10-2007-0015389
(43) 공개일자 2007년02월02일

(21) 출원번호 10-2006-7020093
(22) 출원일자 2006년09월28일
심사청구일자 없음
번역문 제출일자 2006년09월28일
(86) 국제출원번호 PCT/US2005/006927
국제출원일자 2005년03월04일
(87) 국제공개번호 WO 2005/089120
국제공개일자 2005년09월29일

(30) 우선권주장 60/549,959 2004년03월04일 미국(US)

(71) 출원인 스위트스폿 솔루션즈
미국 애리조나 85206 메사 스위트 104 이스트 베이스라인 로드 4856

(72) 발명자 벡 저스틴 엠.
미국 애리조나 85213 메사 이 헤일 스트리트 3115
스웬슨 차드 엘.
미국 애리조나 85205 메사 이스트 매클레란 넘버 11 4140

(74) 대리인 송봉식
박종혁
김정욱
정삼영

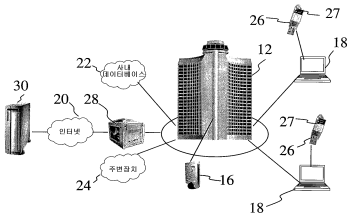
전체 청구항 수 : 총 20 항

(54) 무선랜 애플리케이션 용 보안 인증 및 네트워크 관리시스템

(57) 요약

Wi-Fi랜 용 인증 및 네트워크 관리 시스템은 네트워크 관리 장치와 상기 네트워크 관리 장치에 접속된 복수의 Wi-Fi랜을 포함한다. 각각의 랜은 Wi-Fi무선부를 구비한 적어도 하나의 액세스 포인트 장치를 포함한다. 복수의 엔드 유저 장치는 노드를 형성하는 네트워크에 부착가능하고, 각각의 엔드 유저 장치는 부속품을 접속하기 위하여, USB포트등의 입력 플러그를 구비하고 있다. 인증 장치는 네트워크에 부착된 엔드 유저 장치를 인증하기 위하여 네트워크내에 제공된다. 복수의 인증 키가 제공되는데, 각각의 키는 엔드 유저 장치의 입력 플러그에 부착될 수 있다. 각각의 키는 내부에 유효성 증명서를 포함하고, 인증 장치는 네트워크로의 접속을 승인하기 전에 엔드 유저 장치에 접속된 키상의 현재의 유효성 증명서의 존재를 확인한다.

대표도



특허청구의 범위

청구항 1.

Wi-Fi무선부를 구비한 적어도 하나의 액세스 포인트 장치;

노드를 형성하는 네트워크에 부착가능하고, 부속품을 연결하기 위한 입력 플러그를 구비한 복수의 엔드 유저 장치;

상기 네트워크에 부착된 상기 엔드 유저 장치를 인증하기 위한 인증 장치; 및

각각이 엔드 유저 장치의 입력 플러그에 부착가능하고, 내부에 유효성 증명서를 포함하고 있는 복수의 인증 키를 포함하고, 상기 인증 장치는 상기 네트워크로의 접속을 승인하기 전에 상기 엔드 유저 장치에 접속된 키에 현재 유효성 증명서의 존재를 확인하는 것을 특징으로 하는 Wi-Fi무선랜.

청구항 2.

제 1 항에 있어서, 각각의 키는 인증 프로세스를 위해 키와 인증 장치사이에 가상 사설 네트워크 터널을 구축하는 것을 특징으로 하는 Wi-Fi무선랜.

청구항 3.

제 1 항에 있어서, 각각의 키는 1" 내지 5" 정도의 길이이고 Wi-Fi무선랜 오퍼레이터를 나타내는 표시를 포함하는 것을 특징으로 하는 Wi-Fi무선랜.

청구항 4.

제 1 항에 있어서, 상기 네트워크상의 상기 엔드 유저는 i) 고속 인터넷 서비스, ii) 사내 데이터베이스, 및 iii) 특정 장비 중 어느 하나에 접속이 승인되는 것을 특징으로 하는 Wi-Fi무선랜.

청구항 5.

제 1 항에 있어서, 각각의 키는 상기 엔드 유저 장치의 범용 시리얼 버스에 부착되는 것을 특징으로 하는 Wi-Fi무선랜.

청구항 6.

제 1 항에 있어서, 상기 인증 장치에 접속된 네트워크 관리 장치를 더 포함하고, 상기 관리 장치는 상기 키의 유효성 증명서의 액티브 디렉토리를 유지하고 상기 인증 장치에 이러한 목록을 전송하는 것을 특징으로 하는 Wi-Fi무선랜.

청구항 7.

제 8 항에 있어서, 상기 액세스 포인트 장치는 내부에 신호 증폭기를 더 포함하고 상기 네트워크 관리 장치는 인터넷을 통해 상기 인증 장치에 접속되는 것을 특징으로 하는 Wi-Fi무선랜.

청구항 8.

제 1 항에 있어서, 각각의 키는 (i) 키가 할당되는 특정 유저와 연관된 네트워크상에 특권을 승인하는 개인키사에 개인 프로파일의 결합, 및 (ii) 상기 유저 장치상에 네트워크 보호 소프트웨어의 최소 등급의 존재를 적어도 확인하는 네트워크 보호 소프트웨어 중 적어도 하나를 더 포함하는 것을 특징으로 하는 Wi-Fi무선랜.

청구항 9.

노드를 형성하는 네트워크에 부착가능하고, 부속품을 연결하기 위한 입력 플러그를 구비한 복수의 엔드 유저 장치;

상기 네트워크에 부착된 상기 엔드 유저 장치를 인증하기 위한 인증 장치; 및

각각이 엔드 유저 장치의 입력 플러그에 부착가능하고, 내부에 유효성 증명서를 포함하고 있는 복수의 인증 키로서, 상기 인증 장치는 상기 네트워크로의 접속을 승인하기 전에 상기 엔드 유저 장치에 접속된 키에 현재 유효성 증명서의 존재를 확인하는 상기 복수의 인증 키; 및

상기 인증 장치에 접속된 네트워크 관리 장치로서, 상기 관리 장치는 상기 키의 유효성 증명서의 액티브 디렉토리를 유지하고 상기 인증 장치에 이러한 목록을 전송하는 상기 네트워크 관리 장치를 포함하는 것을 특징으로 하는 보안 무선랜.

청구항 10.

제 9 항에 있어서, 각각의 키는 상기 엔드 유저 장치의 범용 시리얼 버스에 부착되고 인증 프로세스를 위해 키와 인증 장치 사이에 가상 사설 네트워크 터널을 구축하는 것을 특징으로 하는 보안 무선랜.

청구항 11.

제 9 항에 있어서, 상기 네트워크는 Wi-Fi무선부를 구비한 적어도 하나의 액세스 포인트 장치를 포함하는 무선 Wi-Fi네트워크이고, 각각의 키는 1" 내지 5" 정도의 길이이고 상기 엔드 유저 장치의 범용 시리얼 버스 포트에 부착되고, 상기 네트워크상의 상기 엔드 유저는 i) 고속 인터넷 서비스, ii) 사내 데이터베이스, 및 iii) 특정 장비 중 어느 하나에 접속이 승인되는 것을 특징으로 하는 보안 무선랜.

청구항 12.

제 9 항에 있어서, 제 1 항에 있어서, 각각의 키는 (i) 키가 할당되는 특정 유저와 연관된 네트워크상에 특권을 승인하는 개인키상에 개인 프로파일의 결합, 및 (ii) 상기 유저 장치상에 네트워크 보호 소프트웨어의 최소 등급의 존재를 적어도 확인하는 네트워크 보호 소프트웨어 중 적어도 하나를 더 포함하는 것을 특징으로 하는 보안 무선랜.

청구항 13.

A) 네트워크 관리 장치; 및

B) 상기 네트워크 관리 장치에 접속된 복수의 Wi-Fi랜으로서, 각각이

i) Wi-Fi무선부를 구비한 적어도 하나의 액세스 포인트 장치;

ii) 노드를 형성하는 네트워크에 부착가능하고, 부속품을 연결하기 위한 입력 플러그를 구비한 복수의 엔드 유저 장치;

iii) 상기 네트워크에 부착된 상기 엔드 유저 장치를 인증하기 위한 인증 장치; 및

iii) 각각이 엔드 유저 장치의 입력 플러그에 부착가능하고, 내부에 유효성 증명서를 포함하고 있는 복수의 인증 키를 포함하고, 상기 인증 장치는 상기 네트워크로의 접속을 승인하기 전에 상기 엔드 유저 장치에 접속된 키에 현재 유효성 증명서의 존재를 확인하는 상기 복수의 Wi-Fi랜을 포함하는 것을 특징으로 하는 Wi-Fi랜 용 인증 및 네트워크 관리 시스템.

청구항 14.

제 13 항에 있어서, 상기 네트워크 관리 장치는 각각의 랜의 인증 장치에 접속되고, 상기 관리 장치는 상기 네트워크를 위한 상기 키의 유효성 증명서의 액티브 디렉토리를 유지하고 상기 각각의 인증 장치에 이러한 목록을 전송하는 것을 특징으로 하는 Wi-Fi랜 용 인증 및 네트워크 관리 시스템.

청구항 15.

제 13 항에 있어서, 각각의 키는 상기 엔드 유저 장치의 USB포트에 부착되고, 인증 프로세스를 위한 상기 키와 상기 인증 장치사이의 가상 사설 네트워크 터널을 구축하고, 1" 내지 5" 정도의 길이이며 상기 Wi-Fi무선랜 오퍼레이터를 지시하는 표시를 포함하는 것을 특징으로 하는 Wi-Fi랜 용 인증 및 네트워크 관리 시스템.

청구항 16.

제 13 항에 있어서, 각각의 랜상의 상기 엔드 유저는 i) 고속 인터넷 서비스, ii) 사내 데이터베이스, 및 iii) 특정 장비 중 적어도 하나에 접속이 승인되고, 각각의 랜의 액세스 포인트 장치는 내부에 신호 증폭기를 더 포함하는 것을 특징으로 하는 Wi-Fi랜 용 인증 및 네트워크 관리 시스템.

청구항 17.

Wi-Fi무선부를 구비한 적어도 하나의 액세스 포인트 장치, 및 노드를 형성하는 네트워크에 부착가능하고, 부속품을 연결하기 위한 입력 플러그를 구비한 복수의 엔드 유저 장치를 구비한 Wi-Fi랜을 위한 인증 및 네트워크 관리 방법으로서,

상기 네트워크에 부착된 상기 엔드 유저 장치를 인증하기 위한 인증 장치 및 복수의 인증 키를 제공하는 단계로서, 각각의 키는 엔드 유저 장치의 입력 플러그에 부착가능하고, 각각의 키는 유효성 증명서를 내부에 포함하는 상기 인증 장치 및 복수의 인증 키 제공 단계; 및

상기 네트워크로의 접속을 승인하기전에 상기 인증 장치를 갖는 상기 엔드 유저 장치에 접속된 키상에 현재의 유효성 증명서의 존재를 확인하는 단계를 포함하는 것을 특징으로 하는 인증 및 네트워크 관리 방법.

청구항 18.

제 17 항에 있어서, 각각의 키는 상기 인증 프로세스를 위해 상기 키와 인증 장치사이의 가상 사설 네트워크 터널을 구축하고, 각각의 키는 길이가 1" 내지 5" 정도이며 상기 Wi-Fi 무선랜 오퍼레이터를 지시하는 표시를 포함하고, 상기 엔드 유저 장치의 범용 시리얼 버스 포트에 부착되는 것을 특징으로 하는 인증 및 네트워크 관리 방법.

청구항 19.

제 17 항에 있어서, 상기 인증 장치에 접속된 네트워크 관리 장치를 제공하는 단계, 상기 관리 장치상에 상기 키의 유효성 증명서의 액티브 디렉토리를 유지하는 단계, 상기 인증 장치에 이러한 목록을 전송하는 단계를 더 포함하는 것을 특징으로 하는 인증 및 네트워크 관리 방법.

청구항 20.

제 19 항에 있어서, 상기 네트워크 관리 장치는 인터넷을 통해 상기 인증 장치에 접속되는 것을 특징으로 하는 인증 및 네트워크 관리 방법.

명세서

기술분야

본 발명은 무선랜 애플리케이션을 위한 인증 시스템에 관한 것이고, 보다 상세하게는 Wi-Fi랜을 위한 포괄적인 인증 및 네트워크 관리 시스템에 관한 것이다.

배경기술

"근거리 네트워크"를 의미하는 랜은 대체로 사무실이나 가정과 같은 비교적 작은 영역에 이르는 컴퓨터 네트워크이고 고속으로 데이터를 전송할 수 있다. 대부분의 랜은 단일 건물이나 건물의 그룹으로 한정된다. 그러나, 하나의 랜은 전화선과 무선을 통해 원거리의 다른 랜에 연결되어 원거리 네트워크, 즉 WAN을 형성할 수 있다. 대부분의 랜은 네트워크의 노드로 알려진, 워크스테이션과 개인컴퓨터와 같은 엔드 유저 장치를 연결한다. 랜 내의 각각의 노드(예컨대 개별 엔드 유저 장치)는 프로그램을 수행하는 자체 CPU를 가지고 있지만 랜을 통해 어느곳이든 데이터와 장치에 접속할 수도 있다. 이것은 많은 유저들이 데이터는 물론 프린터등의 장치를 공유할 수 있음을 의미한다. 유저들은 이메일을 전송하거나 채팅 세션등에 의해 서로 통신하는데 랜을 사용할 수도 있다.

많은 다른 타입의 랜이 있다. 랜은 링 배열 또는 직선 배열과 같이 네트워크상의 장치의 기하학적 배치인 토폴러지, 데이터를 전송하기 위한 규칙과 인코딩 스펙인 프로토콜, 그리고 트위스트 페어 와이어, 동축 케이블, 광섬유 또는 무선등의 연결 매체에 의해 구분될 수 있다.

무선랜은 WLAN으로도 불리는데 Wi-Fi가 WLAN의 지배적 표준이다. Wi-Fi WLAN은 일반적으로 두 개 이상의 컴퓨터나 기타 장치를 사무실, 가정 또는 (하기할) "핫 스폿"내에서와 같은 100 내지 500피드의 짧은 거리에서 연결한다. 무선 원거리 네트워크, 즉 WWAN은 하나의 시 전체와 같은 광역을 커버하는 무선 네트워크이다. 주된 무선 캐리어에 의해 동작되는 WWAN은 광역에서 음성과 비교적 낮은 대역의 데이터 서비스를 제공하고, 수백개의 통신 탑과 정부로부터 특별 주파수 면허를 받아야하고 구축과 유지관리에 수억 내지 수천억원이 소요된다.

Wi-Fi는 "무선 충실도"의 줄임말이고 무선랜에 대한 글로벌 기술이다. Wi-Fi는 대체로 임의의 타입의 (하기할) 802.11표준 네트워크, 예컨대 802.11b표준, 802.11a표준, 802.11g표준, 듀얼 밴드 표준 등을 언급할 때 사용된다. 일반적으로, 같은 무선 주파수(예컨대, 802.11b 또는 11g표준 용의 2.4GHz, 802.11a표준용의 5GHz)를 사용하는 임의의 Wi-Fi제품은 임의의 다른 타입과 동작할 것이다. 이전에는 Wi-Fi란 용어는 2.4GHz 802.11b표준 대신으로만 사용되었지만, 용어의 일반적 의미가 확대되었다. 범용 Wi-Fi표준을 갖는 이점은 가상의 누구든 저비용의 Wi-Fi네트워크를 구축할 수 있고 가정, 사무실 또는 공공장소를 커버하여 일반적인 다이얼업 모뎀 접속보다 100배 이상 빠른 고속의 무선 인터넷 접속과 같은 네트워크 접속을 제공할 수 있다는 것이다.

"802.11"이란 용어는 WLAN에 대한 전기전자기술자협회, 즉 IEEE가 개발한 스펙군을 의미한다. 802.11표준은 무선 클라이언트와 기지국간 또는 두 개의 무선 클라이언트간 에어 인터페이스를 규정하고 있다. 802.11군에는 다른 많은 스펙이 있다.

802.11표준은 무선랜에 적용되고 주파수 호핑 스프레드 스펙트럼(FHSS)이나 디렉트 시퀀스 스프레드 스펙트럼(DSSS) 중 하나를 사용하는 2.4GHz대역에서 1 또는 2Mbps의 전송율을 제공한다. 802.11a표준은 무선랜에 적용되는 802.11표준의 확장 버전이고 5GHz에서 54Mbps에 달하는 데이터속도를 제공하고 FHSS나 DSSS보다는 직교 주파수 분할 다중화 인코딩 기법을 사용한다. 802.11b표준 또한 무선랜에 적용되는 802.11의 확장 버전이고 2.4GHz대역에서 (5.5, 2 및 1Mbps로의 폴백을 갖는) 11Mbps의 전송속도를 제공하는데 802.11b는 DSSS만을 사용한다. 802.11b표준은 "본래의" Wi-Fi표준이고 판매되는 모든 Wi-Fi장비의 대부분을 차지하고 있다. 802.11g표준은 무선랜에 적용되고 2.4GHz대역에서 20+ Mbps의 속도를 제공한다.

802.11g표준은 802.11b표준의 (하기할) 액세스 포인트, 즉 AP와 구버전 호환가능하다. 즉, 802.11g표준 무선은 802.11g표준과 802.11b표준의 AP 모두에 접속된다. 802.11a표준은 802.11b표준이나 802.11g표준과 호환되지 않기 때문에 802.11a표준 무선은 802.11a표준 AP와만 통신할 수 있다. 그러나, 현재 많은 Wi-Fi PC카드는 802.11b/g표준과 802.11a표준을 지원하고 있다. 현재의 무선 캐리어 네트워크보다 높은 속도를 WWAN에 제공할 802.16이라 명명된 새로운 표준이 나타나고 있다. 802.16표준의 부가적 이점은 면허가 없는 주파수에서 동작은 물론 장비가 훨씬 적게 필요하고, 이것은 인프라 배치 비용을 상당히 줄인다.

액세스 포인트, 즉 AP는 Wi-Fi무선 데이터 트래픽을 송수신하는 무선 통신 허브 또는 "기지국"으로 기능하는 하드웨어이거나 컴퓨터의 소프트웨어이다. AP는 보통 특정 네트워크로, 가장 일반적으로는 라우터를 통해 다시 인터넷으로 접속되는 유선랜에 부착된다. 일반적인 시스템내의 AP는 무선 유저가 접속하는 서비스의 물리적 범위를 확장하고 무선 보안을 제공하기 위해 사용된다.

인프라구조의 모드는 먼저 AP를 통과함으로써 장치가 서로 통신하는 802.11표준 네트워킹 프레임워크이다. 인프라구조 모드에서, 무선 장치는 서로 통신하거나 유선 네트워크와 통신할 수 있다. 인프라구조 모드는 Ad-hoc모드와 반대되는데, Ad-hoc모드에서는 802.11표준 네트워크내의 장치가 AP를 사용하지 않고(예컨대 피어-투-피어 모드) 서로 직접 통신한다.

일반적으로 AP는, 특히 공중에 개방된 AP는 "핫 스폿"이라고도 불리는데, 이러한 AP를 운영하는 사람을 핫 스폿 오퍼레이터 또는 HSO라고 부른다. 상용의 핫 스폿은 일반적으로 카페, 호텔, 공항, 서점, 사무실 건물 로비, 공원 또는 (베뉴(venue)라 불리는) 컨벤션 센터와 같은 공공장소에서 발견되고 일반적으로 고속 무선 접속을 제공하는 네트워크로 접속하기 위해 유료로 유저가 접속할 수 있는 하나 이상의 Wi-Fi액세스 포인트와 액세스 제어 장치를 포함할 것이다. 무료 시설의 핫 스폿은 고객 및/또는 일반 공중에 무료로 무선 인터넷(또는 기타 네트워크) 접속을 제공하는 베뉴이다. 무료 시설 핫 스폿은 영업소에서 설치되고 일반적으로 그 장소의 고객을 위한 것이라는 점에서 무료 커뮤니티 핫 스폿과 다르다. 예컨대, 카페나 호텔은 경쟁 수단으로서 무료로 고객에게 무선 접속을 제공하는 것을 택할 수 있다. 반대로, 무료 커뮤니티 핫 스폿은 대개 가정, 공원, 거리의 코너나 기타 장소에 위치하여 무료로 무선 접속을 제공한다. 무료 커뮤니티 핫 스폿은 영업 시설의 일부로서 보다는 무료 근거리 인터넷 접속을 제공하는 개인이나 작업 그룹에 의해 설치된다.

핫 스폿 집합자, 또는 간단히 집합자는 수개의 핫 스폿을 동작하고 이를 보다 큰 심리스한 네트워크에 결합하는 것이다. 베뉴 소유자는 액세스 포인트, 액세스 제어 장치(하기됨) 및 그 장소로의 고속 인터넷 링크를 배치하는 핫 스폿 집합자와 계약한다. 핫 스폿 집합자는 베뉴 소유자와 수익 및/또는 비용을 공유한다.

Wi-Fi네트워크를 포함하는 임의의 네트워크는 특정 유저가 어떠한 컴퓨터 자원에 접속하는지를 제어할 필요가 있고 일반적으로 네트워크상에서 유저의 활동을 계속 추적할 필요가 있다. 인증은 보통 유저명과 패스워드에 따라, 개인을 식별하는 프로세스이다. 인증은 각 개별 유저가 다른 유저와 구별짓는 고유 정보를 가진다는 사고에 기초한다. 인증은 일단 유저가 유저명과 패스워드를 통하는 등으로, 인증되었다면 네트워크 자원으로 유저의 접속을 승인하거나 거부하는 프로세스이다. 유저가 접속하는 정보량과 서비스량은 유저의 인증 레벨에 좌우된다. 결국, 어카운팅은 네트워크에서 보낸 시간량, 거기 있는 동안 접속된 서비스 및 그 세션동안 전송된 데이터량을 포함하는, 네트워크 자원에 접속하는 동안 유저의 활동을 계속 추적하는 프로세스이다. 어카운팅 데이터는 트렌드 분석, 용량 계획, 과금, 회계 및 비용 할당을 위해 사용된다. 컴퓨터 기술에서, "아이디"는 시스템에 의해 인식되는 사람, 장치, 또는 그 둘의 조합의 고유명이다. 많은 타입의 네트워크 관리 시스템은 네트워크와 그 자원의 보안을 보증하기 위해 고유 아이디에 의존한다.

가상 사설 네트워크, 즉 VPN는 네트워크의 장치를 연결하기 위한 공공 연결(예컨대, 유선 또는 무선 접속)에 의해 구성되는 네트워크이다. VPN은 (하기할)TCP/IP네트워크에서 전송 보안을 위한 시스템을 제공한다. VPN은 모든 트래픽이 암호화되고 보안되는, 네트워크상의 두 포인트간의 보안 "터널"이다. 예컨대, 랩탑 컴퓨터에서 동작하는 VPN소프트웨어는 랩탑에서, 인터넷을 통해 수천 마일 떨어진 회사의 방화벽 뒤의 VPN서버로의 보안 연결을 설정할 수 있다. 이러한 시스템은 승인된 유저만이 네트워크에 접속할 수 있고 데이터가 인터셉터될 수 없도록 하고 보증하기 위한 암호화 및 기타 메커니즘(예컨대, 패스워드)을 사용한다. VPN은, 회사의 Wi-Fi네트워크와 달리, 유저가 쉽게 접속할 수 있도록 된 Wi-Fi의 암호화 기능없이 방송되는 핫 스폿 본연의 비보안성을 극복한다.

액세스 제어 장치는 하나 이상의 AP와 인터넷으로 되접속하는 라우터간의 영업용 핫 스폿 장소에 설치된 네트워크 장비의 일부이다. 액세스 제어 장치는 하나 이상의 인증 시스템으로 결속하고 무선 네트워크를 통해 인터넷으로 누가 접속할 수 있는지를 제어한다. 상용 핫 스폿에서는, 요금 지불 유저만이 시스템에 접속할 수 있게하는 Wi-Fi "현금 등록기"로서, 그리고 명백히 상용 핫 스폿의 중요한 구성요소로서 기능한다.

Wi-Fi무선부는 랩탑, PDA, 휴대폰, 액세스 포인트등의 무선 장치로부터 Wi-Fi전송을 송수신할 수 있는 안테나와 컴퓨터 칩의 세트이다. Wi-Fi PC카드는 랩탑 컴퓨터에 의해 사용될 수 있고 Wi-Fi기능을 제공하는 랩탑 컴퓨터에 부가될 수 있는 Wi-Fi무선부를 포함한다. PC카드 즉, PCMCIA(Personal Computer Memory Card International Association)카드는 가볍고, 휴대용 컴퓨터에 외형을 부착하는 탈착가능한 신용 카드 크기의 모듈이다. PCMCIA Wi-Fi카드는 랩탑과 PDA에 저렴한 Wi-Fi기능을 제공한다. Wi-Fi의 액세스 포인트는 또한 하나 이상의 Wi-Fi무선부를 포함한다. Wi-Fi무선부는 매우 저렴하게 되고 있고 곧 랩탑이나 차량등의 기타 소비자 전자 장치에서 표준이 될 것이다. Wi-Fi무선부의 제조사로는 인터실, 인텔, 아더로스, 브로드컴, 텍사스 인스트루먼트, 아기어 등이 있다.

"서비스 셋 식별자", 즉 SSID는 액세스 포인트를 설정하는 사람에 의해 Wi-Fi네트워크에 주어지는 이름이다. SSID는 방송하도록 설정될 수 있는데, 이 경우 "스니퍼 소프트웨어"에 의해 유저에 탐지되어 디스플레이될 수 있다. 스니퍼 소프트웨어는 Wi-Fi신호(또는 2.5G와 같은 기타 네트워크 신호)를 위한 공중파를 "스니프링"하고, 이를 유저에게 디스플레이하며 유저가 거기에 접속하게 하는 소프트웨어이다. 기본적인 Wi-Fi스니퍼 소프트웨어는 윈도우 XP 및 애플OSX와 같은 기존 운영 시스템에 내장된다. 더욱이, 유저가 상용 핫 스폿에 접속하고 그들의 컴퓨터에 웹브라우저를 열 때, 그 위치내의 액세스 제어 장치가 스플래시 페이지로 알려진, 그들의 컴퓨터상에 "스플래싱"하는 웹페이지를 생성한다. 스플래시 페이지는 로그인 하는 방법이나 등록하는 방법에 관한 그 위치의 핫 스폿 오퍼레이터로부터 정보를 제공한다.

코드 분할 다중 접속, 즉 CDMA는 개별 대화가 유사 랜덤 디지털 시퀀스로 인코딩되는 확산 스펙트럼 기술을 사용하는 디지털 셀룰러 기술이다. 미국에서는 스프린트와 버라이존 양사가 CDMA기술을 이용한다. GSM(Global System for Mobile Communications)은 또 다른 하나의 주도적 디지털 셀룰러 시스템이다. GSM은 협대역 TDMA(Time Division Multiple Access)를 사용하는데, 이는 같은 무선 주파수상에서 8명의 동시 호를 가능하게 한다. CDMA와 GSM과 같은 이러한 기타 무선 기술과 달리, Wi-Fi는 100% 범지구적으로 이용가능하다. 이것은 "TCP/IP"로 알려져 있다. 즉 이것은 모든 개발자, 장비 제조사, 서비스 프로바이드 및 유저를 위한 단일 무선 네트워킹 표준이다. "TCP/IP"라는 용어는 "전송 제어 프로토콜/인터넷 프로토콜"을 의미하고 컴퓨터와 기타 장치가 네트워크상에서 어떻게 통신하는지에 대한 표준의 셋이다. TCP/IP는 1970년대에 출현했고 서로 다른 제조사로부터의 컴퓨터가 인터넷의 기초가 되는 최초로 공통 방식으로 서로 대화할 수 있게 하였다. TCP/IP에 의해 Wi-Fi의 모든 혁신이 Wi-Fi커뮤니티내의 모든 사람에 이익을 제공하고 있다.

수백 개의 원래의 장비 제조사 또는 OEM사가 Wi-Fi무선부과 액세스 포인트를 생산하고 유통하고 있다. 단일 Wi-Fi표준은 이러한 장치 모드가 서로 상호작용하도록 하여, 예컨대 스위트스폿 솔루션즈사가 제조한 액세스 포인트는 링크시스사의 네트워크 카드와 통신이 가능하다. 컴퓨터 산업에서, OEM사는 데스크탑 컴퓨터, 랩탑 및 라우터와 Wi-Fi PCMCIA카드(또는 Wi-Fi PC카드)와 액세스 포인트와 같은 네트워킹 장비를 포함하여, 엔드유저에게 소매업자를 통해 팔리는 장비를 제조하는 일반적인 임의의 회사이다. OEM사는 델, 스위트스폿 솔루션즈, 소니, 애플, 프록심, 링크시스 및 시스코등이 있다.

OEM사는 현재 수백만 개의 Wi-Fi PC카드와 액세스 포인트로 시장에서 범람하고 있다. 단일 Wi-Fi표준은 이러한 장치 모두가 서로 상호작용하도록 하는데, 예컨대 스위트 스폿사가 제조한 액세스 포인트는 넷기어사의 네트워크 카드와 통신 가능하다. 현재 Wi-Fi구성요소는 소비자의 채택 가격 곡선상에 있다. Wi-Fi구성요소의 급속한 상용화로 Wi-Fi장비의 가격의 급격한 하락을 초래했다. AP는 얼마전에 1000달러가 넘었지만 현재 100달러 이하이고, 얼마전에 700달러였던 Wi-Fi카드는 현재 보통 50달러 이하로 팔리고 있다.

가격의 하락으로, 부속품 검사 Wi-Fi장비에 대한 요구가 급격하게 일어났고, 이에 수백만 개의 개인 Wi-Fi장치가 사무실과 가정에 설치되게 되었다. 한가지 제한 요인은 Wi-Fi네트워크의 보안이다. 제안된 IEEE802.11i표준은 IEEE802.11무선랜내의 몇몇 알려진 보안 구멍을 막도록 된 것이지만, Wi-Fi네트워크를 완전하게 보안성을 가지도록 할 수는 없다. Wi-Fi네트워크에서 보안성을 극대화하기 위해서는 데이터가 진정으로 의도된 소스로부터 오게끔 보증하고 보이거나 수정될 수 없는 메커니즘이 있어야한다. 제안된 802.11i표준은 각 세션의 개시에서 프레시 키를 생성하는 시스템을 포함할 것이다. 이는 또한 현재 세션의 일부이고, Walker가 말했듯, 네트워크 유저를 우롱하는 해커에 의해 반복되지 않도록 보증하는 패킷의 체킹 방식을 제공할 것이다. 키를 관리하기 위해서는, 유저와 IEEE802.1x표준을 인증하는 것이 RADIUS(원격 접속 다이얼-인 유저 서비스)를 사용할 것이다. 곧 출현하는 또 다른 보안 업그레이드는 WPA(무선 보호 액세스)표준으로 알려져 있는데, Wi-Fi연합에서 채택한 스펙이다. 이러게 제안된 개선사항이 Wi-Fi네트워크의 모든 보안 문제를 해결해주지는 못한다.

WEP는 Wired Equivalent Privacy의 약자이고 무선랜에 대한 보안 프로토콜이다. WEP은 유선랜과 같은 레벨의 보안을 제공하도록 설계되었다. WEP은 하나의 단말에서 다른 단말로 전송될 때 보호되도록 무선파상에서 데이터를 암호화함으로써 보안을 제공하는 것을 목적으로 하고 있다. 그러나, WEP은 한때 기대한 만큼 보안성이 있지는 않다. WEP에 의해, 수동 네트워크 공격이 RC4의 키 스케줄링 알고리즘내의 몇몇 WEP의 취약성을 이용하여 WLAN가능한 랩탑과 몇몇 용이하게 이용가능한 "난잡한"네트워크 소프트웨어를 가진 거의 모든사람이 네트워크 키를 검색가능하게 함으로써 15분이내에 전체 유저 접속을 가능하게 한다. 사용된 비트수에 따라 선형적으로 변하고 키가 128비트로 증가하면 거의 차이가 생기지 않는다.

기존의 많은 Wi-Fi네트워크는 건물이나 공원 외부에 의해 침입자가 구동하고 무선랜 트래픽을 인터셉트하는 "워 드라이빙"(war driving)에 대항하는 기본적인 보호조차도 이용하고 있지 않다. "워 드라이빙"에 대한 일부 방어로서, 유저는 Wi-Fi장치내에 이미 내장된 WEP암호화를 이용할 수 있다. 부가적 보호를 위해, 유저는 시스템에 침투하기 위한 패키징된 해킹 툴을 사용하는 사람(종종 청소년들)을 참조하는, "스크립트 키디"로부터 자신을 보호하기 위하여 가변 키를 갖는 유저 인증 및 유동 WEP을 구현할 수 있다. 기존 인증 시스템은 EAP-TLS(Extensible Authentication Protocol-Transport Level Security), PEAP(Protected EAP), 또는 시스코사가 WEP상에서 자사 제품의 보안성을 높이기 위한 노력의 일부로서 도입한 시스코의 LEAP(Lightweight EAP)를 포함한다. WPA 및 802.11i에서 사용될 TKIP(Temporal Key Integrity Protocol), 또는, 시스코사가 스톱-갭 방안으로 개발한 802.11i의 권장사항의 재산권으로 보호되는 CKIP(Cisco Key Integrity Protocol)과 같은 강한 암호화 시스템 또한 이용될 수 있다.

미국 특허 제 6,658,500호는 장치용 마이크로칩 카드가 액세스를 허용하는데 사용되는 통신 네트워크(케이블, 휴대폰, 무선 또는 지상선 전화 시스템)를 위한 인증 시스템을 개시하고 있다. 이러한 제안된 보안 시스템은 Wi-Fi네트워크를 위해 식별되거나 실용적이지 않다. 셀룰러 네트워크를 위한 또 다른 보안 시스템이 미국 특허 제 6,611,913호에 개시되어 있는데, 여기서 인증키에 대한 에스크로우드 키 분배 시스템에 대해 설명하고 있다.

Kump등의 미국 공개 특허 출원 제 2004/0022186호에는 액세스 포인트를 모니터하고 이후 승인되지 않은 액세스 포인트를 식별하고 최종적으로 승인되지 않은 액세스 포인트를 통과하는 데이터 흐름을 필터를 적용하는 Wi-Fi네트워크를 제안하고 있다. 본 솔루션은 승인되지 않은 노드를 정확하게 탐지하는 기능을 요하고 이러한 승인되지 않은 노드의 접속이 개시되는 것을 적절히 방지하지는 못한다.

상기 확인된 바와 같이, 산업계에서는 이러한 네트워크의 잠재성을 완전하게 확장시키기 위하여 Wi-Fi네트워크의 인식된 보안 취약성을 해결할 필요성이 있다. 본 발명의 목적은 유저의 보안 문제를 해결하는 Wi-Fi 랜에 대한 포괄적인 인증과 네트워크 관리 시스템을 제공하는 것이다. 본 발명의 또 다른 목적은 핫 스폿내에서 동작하는 핫 스폿 오퍼레이터를 위한 턴키 인증 시스템을 제공하는 Wi-Fi랜을 위한 포괄적인 인증 및 네트워크 관리 시스템을 제공하는 것이다. 본 발명의 또 다른 목적은 다양한 별개의 핫 스폿의 관리를 간단하게 하는 Wi-Fi랜을 위한 포괄적인 인증 및 네트워크 관리 시스템을 제공하는 것이다. 본 발명의 또 다른 목적은 핫 스폿 비지니스의 다양한 응용에 의해 경제적으로 제조되고 용이하게 이용가능한 Wi-Fi랜을 위한 포괄적인 인증 및 네트워크 관리 시스템을 제공하는 것이다.

발명의 상세한 설명

상기 목적은 본 발명에 따른 Wi-Fi랜을 위한 포괄적인 인증 및 네트워크 관리 시스템으로써 수행된다. 본 시스템은 네트워크 관리 장치와 상기 네트워크 관리 장치에 접속된 복수의 Wi-Fi 랜을 포함한다. 각각의 로컬 네트워크는 Wi-Fi무선부를 갖는 적어도 하나의 액세스 포인트를 포함한다. 랩탑, PDA 또는 임의의 엔드 유저 Wi-Fi가능 장치와 같은 복수의 엔드 유

저 장치는 그 노드를 형성하는 네트워크에 부착가능하고, 각각의 엔드 유저 장치는 부속품을 접속하기 위한, USB포트등의 입력 플러그를 구비한다. 네트워크에 부착가능한 엔드 유저 장치를 인증하기 위한 인증 장치가 네트워크내에 제공된다. 각각의 키가 엔드 유저 장치의 입력 플러그에 부착가능한, 복수의 물리적 인증 키가 제공된다. 각각의 키는 유효성 증명서를 포함하고, 인증 장치는 네트워크로의 접속을 승인하기 전에 엔드 유저 장치에 접속된 키에 대한 현재의 유효성 증명서의 존재를 확인한다.

본 발명의 일 실시예에서, 각각의 키는 키와 인증 프로세스를 위한 인증 장치간의 가상 사설 네트워크 터널을 구축한다. 더욱이, 각각의 키는 대체로 기계적 로크(예컨대, 집 키 또는 차 키)를 위한 종래의 키의 크기이고 1" 내지 5"정도이다. 각각의 키는 Wi-Fi무선랜 오퍼레이터를 나타내는 표시를 포함할 수 있다. 각각의 키는 엔드 유저 장치의 범용 시리얼 버스 포트에 부착할 수 있다.

관리 장치는 바람직하게는 키의 유효 증명서의 액티브 디렉토리를 유지하고 인증 장치에 이러한 리스트를 전송할 것이다. 네트워크 관리 장치는 인터넷을 통해 인증 장치에 접속될 수 있다. 본 발명의 또 다른 실시예에서 액세스 포인트 장치는 신호 증폭기를 더 포함한다.

인증키에서 물리적 플러그의 또 다른 기능은 개인키상에 개인 프로파일의 결합이다. 키상에 개인 프로파일을 포함함으로써 프로파일 관리라고 하는, 키가 할당된 특정 유저에 연관된 네트워크상에 키가 특권, 즉 차별적 네트워크 접속을 승인할 수 있도록 한다. 이러한 시스템은 특히 멀티 컴퓨터 환경에서 잘 동작한다. 더욱이, 이러한 시스템은 네트워크의 유저사이에 접속의 레벨을 구분하기 위해 현재 공통적으로 사용되고 있는 PIN/패스워드의 프로파일 관리 툴을 보충한다.

인증키에서 물리적 플러그의 또 다른 기능은 개인키상에 네트워크 보호 소프트웨어, 예컨대 안티바이러스, 안티스팸, 및 안티스파이웨어 소프트웨어의 결합이다. 키는 필요한 소프트웨어와 업데이트가 있는지를 알아보기 위해 유저의 컴퓨터를 단순히 체크할 수 있고 이후 유저가 현재의 것(최근의 보호 소프트웨어를 갖는 최신의)이 아니면, 관리 플랫폼은 유저 장치를 검역하고 필연적으로 유저가 개입할 필요없이 유저의 컴퓨터상에 업데이트를 강제할 수 있다. 업데이트된 소프트웨어는 키로부터 직접올 수 있거나, 키가 필요한 소프트웨어의 존재를 증명하기 위해서만 사용될 수 있고 관리 플랫폼은 실제로 대상 장치에 업데이트를 전송한다. 어느 구현체든 자체 치료 네트워크를 가동한다. 거의 임의의 소프트웨어 애플리케이션이 키상에 결합될 수 있다. 본 발명은 무결성과 소정 네트워크의 건강을 보호하기 위한 유효하고 효율적인 툴을 제공한다.

본 발명의 상기 장점 및 기타 이점은 명세서를 통괄하여 동 부재번호가 동 구성요소를 나타내는 첨부도면을 참조한 바람직한 실시예의 설명으로 명확하게 될 것이다.

실시예

본 발명은 도 1-2에 개략적으로 도시된 Wi-Fi 네트워크(10)를 제공한다. 네트워크(10)는 Wi-Fi배치의 네트워크 관리 태양은 물론 하드웨어, 보안, 및 인증을 해결하기 위한 엔드 투 엔드 솔루션을 제공한다. 네트워크(10)는 개인 무선 네트워크와 무료 시설 및 접속 요금 핫 스폿 비지니스 모델을 포함하는, 모든 WLAN응용에 사용될 수 있다. 본 발명은 Wi-Fi 네트워크(10)와 같은 무선 네트워크에 관하여 설명되고 특히 이러한 네트워크에 잘 들어맞지만, 본 발명의 기능은 유선 네트워크, 및 유/무선 조합 네트워크에 적용될 수 있다. 이러한 이점은 바람직한 실시예의 설명으로 명백해질 것이다.

네트워크(10)는 도 2에 도시된 바와 같이 복수의 핫 스폿(12)을 포함한다. 각각의 핫 스폿(12)은 당업계에서 주지된 바와 같이 단일 건물(14)(예컨대, 호텔, 카페등)내에 있을 수 있고, 또는 건물 집합(예컨대 사무실 공원) 전체에 있을 수 있고, 또는 소정 영역(예컨대 공원 배경)위에 있을 수 있다. 각각의 핫 스폿(12)은 핫 스폿(12)을 위한 적어도 하나의 액세스 포인트 장치(16)을 포함한다. 본 발명에 따른 각각의 액세스 포인트 장치(16)는 바람직하게는 단일 부스터 증폭기와함께 802.11표준(b/g, 또는 심지어 802.16표준 또는 결국에는 802.11i표준)을 단일 장치로 결합한다. 단일 부스터 증폭기와 Wi-Fi무선부를 하나의 장치로 통합함으로써, 액세스 포인트 장치(16)는 종래의 액세스 포인트보다 큰 RF신호 풋프린트를 제공할 수 있다. 핫 스폿(12)이 큰 시설(예컨대 대학 캠퍼스나 비즈니스 건물 집합체)을 커버하는 곳에, 핫 스폿(12)은 전체 시설을 통해(즉, 전체 핫 스폿(12)상에) 무선 신호를 제공하도록 다중 액세스 포인트 장치(16)를 사용할 수 있다.

종래의 Wi-Fi네트워크에 관하여, 네트워크(10)는 랩탑(18)이나 기타 지정된 엔드 유저 Wi-Fi가능 장치(예컨대 PDA 또는 Wi-Fi기능을 갖는 임의의 장치)와 같은 엔드 유저 장치로 네트워크(10)에 접속하는 기능을 갖는 유저를 제공하도록 의도된 것이다. 참조된 목적을 위해, PDA(Personal Digital Assistant)는 컴퓨팅, 전화/팩스, 인터넷 및 네트워킹 장치를 결합하는 공통의 핸드헬드 장치이고, 랩탑은 대개 노트북 컴퓨터로 불리는 소형의 휴대 컴퓨터이다. 네트워크(10)에 관하여, 액세스는 유저에게, 하나의 공통적인 비지니스 모델인 인터넷(20)으로의 고속 접속을 제공할 수 있다. 대안으로, 네트워크

(10)의 핫 스폿(12)은 병원이나 연구 도서관에서와 같은 비밀 사내 데이터베이스(22)로의 접속을 승인하는 것이 주요 용도일 수 있다. 대안으로, 개인의 핫 스폿(12)의 중요 용도는 칼라 프린터와 같은 특별한 장비(24)로의 접속을 승인하는 것일 수 있다. 이러한 용도의 조합 또한 일반적이다. 핫 스폿(12)이나 전체 네트워크(10)의 의도된 용도와 주요 기능은 반드시 제한되는 것은 아니다.

네트워크(10)의 핵심적인 특징은 채용되는 인증 및 네트워크 관리 장치이다. 인증 장치나 키(26)는 네트워크(10)의 노드(랩탑(18)이나 기타 Wi-Fi장치)나 각각의 엔드 유저 장치와 연관된다. 인증 장치나 키(26)는 평균적인 가정 키 정도의 크기인 완전히 휴대가능한 USB플러그인 인증 장치이다. 랩탑(18)등의 엔드 유저 장치는 USB포트등의 표준 입력 플러그를 포함한다. "USB"는 범용 시리얼 버스를 말하고 12Mbps의 데이터 전송 속도를 지원하는 외부 버스 표준이다. 단일 USB포트는 마우스, 모뎀 및 키보드등의 주변 장치와 연결하는데 사용될 수 있다. 각각의 키(26)는 핫 스폿(12)에 연결될 랩탑(18)등의 임의의 엔드 유저 장치의 USB포트에 펄르깅할 것이다. 각각의 키(26)는 네트워크 접속을 승인하는 고유의 전자 유효성 증명성을 전달하고 키(26)는 임의의 장치의 USB포트에 쉽게 플러깅될 것이다. 본 발명의 의미에 포함되는 인증 장치나 키(26)는 연결될 수 있는 하나의 물리적 토큰, 예컨대 랩탑(18)등의 엔드 유저 장치의 USB포트와 같은 표준 입력 장치와 접속하는 플러그이다. 대안으로 키(26)는 디스크 구동을 포함하는 다양한 표준 장치 입력을 사용할 수 있지만, USB포트는 엔드 유저에게 참견하지 않는, 즉 엔드 유저의 장치의 중요한 입력 장치를 구속하지 않는 이점이 있다.

키(26)의 물리적 모양은 키(26)의 인증 기능을 크게 변경하지 않고 변할 수 있음은 명백하다. 키(26)의 크기인, 대략 1"-5"의 길이는 본 발명의 중요한 특징이다. 키(26)의 크기가 더 크다면 유저가 다루기 힘들게 된다. 키(26)의 크기는 유저가 가지고 다니기 용이하고 키의 기능을 유저에게 지시한다(즉, 유저에게 친숙한 기계적 로크의 키와 비슷한 크기이다). 키의 크기는 도 1에 로고(27)로 알 수 있는 바와 같이, 베뉴와 네트워크 관리자에 의해 키의 브랜딩을 가능하게 한다. "브랜딩"(27)은 또한 원한다면, 예컨대, "장치의 USB포트를 플러깅하시오" 또는 "도움을 위해 ....로 연락하시오"와 같은 지시를 유저에게 전달할 수 있도록 한다. 브랜딩(27)은 엔드 유저가 키(26)를 지니고 있고 이러한 용이한 접속 시설임을 쉽게 상기하게 하는 카페나 호텔과 같은 상업적 공중 네트워크에 대하여 특히 유용하다고 생각된다. 하기하는 바와 같이 증명서는 필요하다면 쉽게 "턴오프"될 수 있기 때문에, 시스템의 보안이 키(26)를 지니고 있는 유저에 의해 손상되지 않음을 이해하는 것이 중요하다.

네트워크(10)는 각각의 핫 스폿 위치에서 핫 스폿 인증 장치(28)를 구비함으로써 핫 스폿(12)에 턴키 보안과 인증 솔루션을 제공한다. 인증 장치(28)는 용이한 핫 스폿(12) 관리를 제공하는 (키(26)와 마찬가지로) "플러그 앤드 플레이"장치이다. "플러그 앤드 플레이"란 용어는 소프트웨어를 자동적으로 구성하여 동작하는 컴퓨터 시스템 또는 부가 장치의 기능을 말한다(즉, 오퍼레이터는 DIP스위치, 점퍼 또는 기타 구성요소를 설정할 필요가 없다). 인증 장치(28)에는 유효 키(26)를 갖는 유효성 증명서 부속물의 업데이트 가능 목록이 구비된다. 엔드 유저의 USB포트내의 키(26)에 의해, 인증 장치(28)와 키(26)를 갖는 노드 엔드 유저 장치사이에 보안 VPN터널이 생성된다. 이러한 시스템은 패스워드와 WEP타입 암호화와 같은 HSO에 의해 이용되도록 원하는 기존 시스템을 대체하지는 않지만 이에 정합하여 동작한다.

인증 및 네트워크 관리 솔루션의 마지막 부분은 바람직하게는 인터넷(20)등의 임의의 접속을 통해 각각의 핫 스폿(12)에 접속되는 네트워크 관리 장치(30)을 제공하는 것이다. 관리 장치(30)는 다중 핫 스폿(12)을 위한 키(26)의 증명서를 관리할 것이다. 관리 장치(30)는 유효 증명서의 액티브 디렉토리를 유지하고 특정 핫 스폿(12)의 인증 장치(28)에 이러한 목록을 전송할 것이다. 키(26)는 보통 동작중에 다양한 핫 스폿(12)으로부터 부가되고 제거될 것임은 분명하다. 내부에 새로운 증명서가 내장된 새로운 키(26)가 구 키를 대체하고 확장을 위해 부가될 것이다. 구 키(26)는 상실되어 HSO로 복귀하지 않거나 손상되어 유효 증명서의 목록에서 제거될 것이다. 네트워크 관리 장치(30)는 또한 네트워크 불능 알람 및 기타 네트워크의 관리와 운영에 필요한 정보를 수신한다. 그러나 특정 핫 스폿(12)의 인증과 어카운팅 태양은 (유효 증명서 목록의 업데이트외에) 핫 스폿(12)에서 수행된다.

네트워크(10)는 HIPAA, FIPS 및 회사 보안 표준을 충족하는 무선 데이터 전송을 보안한다. 네트워크(10)의 상당한 장점은 특히 사내 네트워크에서 넓게 분포되어 있는 Wi-Fi배치에 방해를 주는 WEP취약성을 극복하는 기능이다. 네트워크(10)는 엔드 클라이언트의 장치(18)상에 있을 키(26)와 인증 장치(28)간의 "로컬 VPN"으로 핫 스폿(12)내의 무선 데이터를 보안한다. WEP보안 요소가 네트워크(10)의 핫 스폿(12)내에서 손상되어도, 데이터 자체는 VPN터널내에서 암호화된다. 따라서, 무선 전송에서는 데이터에 대한 가시성이 없다. 네트워크 키의 해킹은 네트워크의 인증 표준으로 더 가능하지 않게 한다.

네트워크(10)는 고장에 안전한 인증 시스템을 유지하면서 특정 핫 스폿(12)에서 고객의 경험을 강화하는 저렴한 솔루션을 제공한다. 모든 네트워크 구조(인터넷 접속, 회사 데이터 또는 응용)는 네트워크가 임의의 핫 스폿 비지니스 모델에 적용될

수 있도록 하는 로컬 인증 장치(28)뒤에 위치된다. (랩탑(18))내의 엔드 클라이언트상에 위치된 키(26)내의 적당한 증명서 없이는, 네트워크(10)로의 접속이 거부된다. 따라서 현재 출시된 대안의 무선 인증 시스템에서 매우 일반적인 대역폭 해킹, 로그 액세스 포인트 및 기타 불법 접속으로부터의 위협을 제거할 수 있다.

공중 핫 스폿(12)에 대하여, (HSO가 옵션에서 같은 과금 장치를 이용하도록 되어 있을 수 있지만)네트워크가 접속될 때마다 온라인 과금하거나 신용카드를 집어넣을 필요없으므로 유저의 경험은 상당히 개선된다. 있다면, 엔드 유저의 과금은 회의장을 통해 일어난다. 유저의 관점에서 "플러그 앤드 플레이"의 외부에서의 유일한 단계는 먼저 사용될 시스템 드라이버를 인스톨하는 것이다. 드라이버는 로컬 인증 장치(28)상에 저장된 고정 스플래시 페이지에서 다운로드된다. 솔루션의 중앙집중식 네트워크 관리 기능 또한 인증이 핫 스폿(12)에서 일어나므로 간단하다. 집합자의 위치에서 운영하기 위한 대형 데이터 센터나 과금 애플리케이션을 요하지 않는다. 따라서 네트워크 관리를 위한 비용과 운영의 복잡성을 줄이고 네트워크(10) 많은 다양한 핫 스폿(12)에 서비스할 수 있도록 한다. 즉, 네트워크(10)는 특정 핫 스폿 타입이 핫 스폿(12) 전체에 분배되게끔 응용될 수만 있는 네트워크 관리 비용을 요하지 않는다. 네트워크의 관리는 적당한 동작을 보장하는 장비를 모니터링하고 유효 증명서의 데이터베이스를 유지하는 것으로 한정된다.

네트워크(10)는 개인 및 공중 액세스 무선 네트워크(핫 스폿(12))의 저렴한 구축과 관리를 가능하게 하는 제품 및 서비스를 포함하여, 산업계급의 광대역 무선 인프라 솔루션을 제공한다. 네트워크(10)는 Wi-Fi배치를 방해하는 보안과 인증 문제에 대한 고유의 해결책을 제공함으로써 개인 및 공중 네트워크(핫 스폿(12))의 오퍼레이터에게 Wi-Fi솔루션을 제공한다.

바람직하게는 인증 키(26)는 특히 네트워크(10)로의 액세스에 등급이 있는 곳에, 승인된 유저에 연관된 개인 프로파일을 더 첨부할 수 있다. 키(26)에 개인 프로파일을 포함함으로써 네트워크(10)상에 네트워크 특권이라고도 부르는 다양한 접속 세트를 키(26)가 승인하도록 할 수 있다. 이러한 특권은 특정 유저 또는 키(26)가 할당된 사람에 연관될 것이고 이는 프로파일 관리라고도 한다. 이러한 프로파일 관리 애플리케이션은 서로다른 유저가 서로다른 등급의 접속, 예컨대 관리자 등급 접속, 오퍼레이터 접속등이 승인되는 멀티 컴퓨터 환경에서 특히 잘 작용한다. 더욱이, 본 발명의 이러한 프로파일 관리 태양은 네트워크(10)의 유저간의 접속 등급을 구분하는데 현재 일반적으로 사용되고 있는 PIN/패스워드의 프로파일 관리 툴을 보충한다.

인증 키(26)는 네트워크 보호 소프트웨어, 예컨대 안티 바이러스, 안티 스팸 및 안티 스파이웨어 소프트웨어를 더 포함할 수 있다. 키(26)는 필요한 소프트웨어와 업데이트가 장치상에 있는지를 알아보기 위해 유저의 컴퓨터와 기타 접속된 장치를 단순히 체크할 수 있다. 연계된 장치가 현재 필요한 등급의 보호 소프트웨어, 예컨대 최신 안티 바이러스 업데이트를 가지고 있지 않다면, 관리 플랫폼은 네트워크 액세스로부터 특정 장치를 검역하고 유저의 컴퓨터와 기타 장치에 강제로 업데이트하게 한다. 이것은 필수적으로 유저의 개입없이 로그인상태에서 수행될 수 있다. 업데이트된 소프트웨어는 키(26)로부터 직접 온 것일 수 있거나, 또는 키(26)는 필요한 소프트웨어의 존재를 증명하는데만 사용될 수 있고 관리 플랫폼이 실제로 대상 장치에 업데이트를 전송한다. 어느 구현체이든 자체 치료 네트워크를 일으킨다. 키에는 거의 임의의 소프트웨어 애플리케이션이 결합될 수 있다. 본 발명은 소정의 네트워크의 무결성과 건강을 보호하기 위한 유효하고 효율적인 툴을 제공한다.

네트워크(10)는 몇몇 대표적인 예로써 보다 잘 설명될 수 있다. 먼저, 호텔의 시설로서 핫 스폿(12)의 구현을 고려해보자. 호텔 손님은 그들의 체류에 의해 네트워크 접속을 제공받고(또는 구매할 수 있다) 키(26)를 할당받는다. 유저는 랩탑(18) 등의 장치를 사용할 수 있고 그리고/또는 호텔은 비지니스 센터내의 컴퓨터등과 같이 이용가능한 장치를 구비할 수 있다. 키(26)는 필수적으로 체류기간동안만 유효하게 유지된다. 프로파일 관리에 의해 선택된 손님의 특정 키(26)가 (부가 요금이나 "우수 고객"에게 예약된 것으로 전제되는)비즈니스 센터내의 대형 스크린 모니터나 칼라 프린터로의 접속과 같은, 네트워크로의 부가적인 접속이 승인되도록 할 수 있다. 키 자체의 저렴성과 키 인증은 종료한다는 사실때문에, 키(26)를 반환하지 못한다하여 시스템의 무결성에 손상을 주지는 않는다. 더욱이, 키(26)의 "브랜딩"(27)으로 호텔 오퍼레이터가 유저로하여금 키(26)를 이러한 특정 호텔과 시설의 리마인더로서 유지하게 할 것임을 제시하는데, 특정 키(26)의 특정 증명은 유저가 실제로 연이은 체류와 키(26)의 반환동안 반환하면(물론, 새로운 키 또한 쉽게 발행될 수 있다) "비활성화"될 수 있다. 결국 키(26)는 상기한 바와 같이 유저의 특정 장치상에 네트워크 보호 소프트웨어의 최소 등급이 제공되도록 보증하도록 사용될 수 있다. 이것은 최소 등급의 보안이 원하는 대로 엔드 유저 장치의 등급으로 아래로 밀려나게 하는 것으로 구현될 수 있는 네트워크 보호 소프트웨어에 보다 큰 융통성을 제공한다.

다른 예는 대학 환경일 것인데, 여기서는 네트워크가 매우 다양한 학생, 관리, 시설 및 직원의 요구조건을 수용해야한다. 대부분의 대학 환경에서는 학생 풀(pool)이 매 학기마다 변한다. 개인 키(26)를 구비한 본 시스템을 사용함으로써 네트워크 접속에 관한 바뀌는 학생 인구를 추적하는 매우 쉬운 방법을 가능하게 한다. 또한 본 시스템은 키(26)가 반환되지 않으면 손상받지 않는다. 더욱이, 이러한 환경은 키(26)내의 프로파일 관리 구현체의 사용을 돋보이게한다. 공대내의 교직원이

나 대학원생이 (별개의 고유 접속을 가질수도 있는)인문대내의 재학생보다 특정 학내 도서관 및 네트워크 자원으로 보다 많이 접속할 수 있을 것이다. 특정 강의의 등록은 승인된 프로파일과 접속을 변경할 수 있다. 상기 대학 및 호텔의 예는 엔드 유저가 네트워크 상에 엔드 유저 장치를 제공하고 따라서 제어하는 비지니스(또는 심지어 대학의 관리측)와 반대로, 랩탑등의 자체 장치를 구비할 것 같은 상황을 대표하는 것이다.

기타 예는 시스템이 무선 네트워크의 용이한 보안 수용을 가능하게 하는 내부 비지니스 환경에서일 것이다. 본 발명의 프로파일 관리 아이템 또한 네트워크 접속의 가변 등급이 관리 등급 접속, 부분 접속등의 비지니스 응용에서 일반적인(즉, 엔지니어링은 배송과는 다른 네트워크상의 리소스를 갖는다) 것과 같은 그러한 응용에 특히 유용할 수도 있을 것이다. 또한 본 발명의 기능은 무선 네트워크의 장점이 분명히 상실됨에 불구하고, 유선 네트워크와 결합하거나 배타적으로 사용된다면 유지됨을 이해해야한다.

본 발명의 사상과 범위를 이탈하지 않고 본 발명에 대한 다양한 변형이 가능함을 당업자는 이해할 것이다. 본 발명의 범위는 첨부한 청구항고 그 균등물에 의해 정해진다.

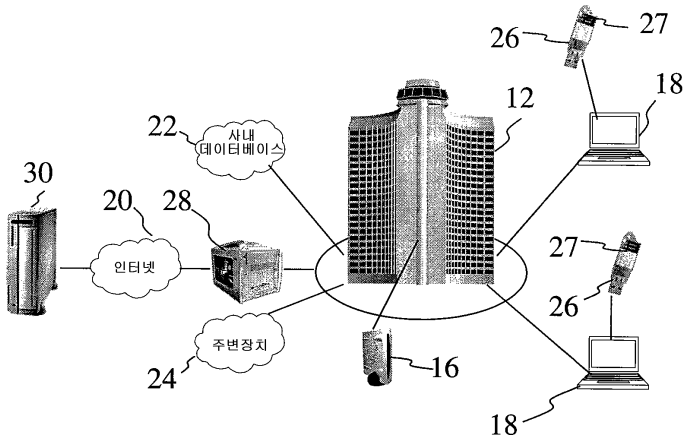
도면의 간단한 설명

도 1은 본 발명에 따른 인증 및 네트워크 관리 시스템을 구비한 Wi-Fi WLAN의 개요도; 및

도 2는 핫 스폿의 집합에 적용된 본 발명에 따른 네트워크 관리 시스템의 개요도.

도면

도면1



도면2