



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년02월19일
(11) 등록번호 10-1234902
(24) 등록일자 2013년02월13일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) G06F 21/20 (2006.01)
H04L 9/32 (2006.01)
(21) 출원번호 10-2011-0124100
(22) 출원일자 2011년11월25일
심사청구일자 2011년11월25일
(56) 선행기술조사문헌
KR1020060056334 A
KR1020070016696 A
KR100987899 B1
JP2002269047 A

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
이문규
경기도 부천시 원미구 계남로 81, 2222동 702호 (상동, 진달래마을)
송정은
서울특별시 강서구 곰달래로49길 100, 대흥102호 (화곡동)
김진복
인천광역시 남구 경인남길118번길 58, 우당원룸 301호 (용현동)
(74) 대리인
특허법인무한

전체 청구항 수 : 총 7 항

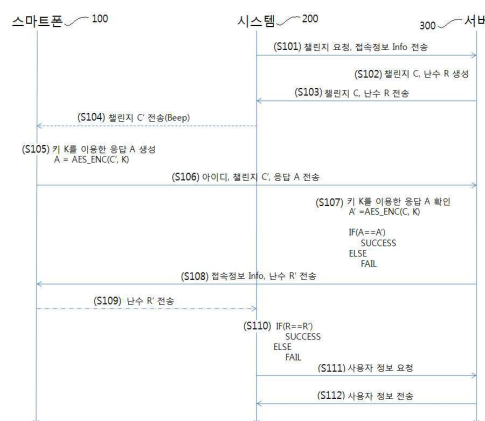
심사관 : 장상배

(54) 발명의 명칭 음향 주파수 분석을 이용한 스마트폰 사용자 인증 방법

(57) 요약

음향 주파수 분석을 이용한 스마트폰 사용자 인증 방법이 개시된다. 단말기의 사용자에게 인증을 수행하는 사용자 인증 방법은 인증 서버에서 사용자가 사용하고자 하는 인증 대상 시스템의 요청에 따라 인증을 위한 챌린지(challenge)를 인증 대상 시스템으로 전송하는 (1) 단계; 인증 대상 시스템에서 음향 채널을 통해 챌린지에 해당하는 비프(beep)를 발생시키는 (2) 단계; 단말기에서 마이크를 통해 챌린지가 수신되면 챌린지에 대한 응답을 생성하여 인증 서버로 전송하는 (3) 단계; 및 인증 서버에서 응답을 통해 사용자를 확인한 후 인증 대상 시스템에 대한 사용자의 접속을 허용하는 (4) 단계를 포함할 수 있다.

대표도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호	KI001824
부처명	지식경제부
연구사업명	산업원천기술개발사업(정보통신)
연구과제명	장애인 및 고령자를 위한 Digital Guardian 기술개발
주관기관	한국과학기술연구원
연구기간	2008.03.01 ~ 2012.02.28

특허청구의 범위

청구항 1

단말기의 사용자에게 대한 인증을 수행하는 사용자 인증 방법에 있어서,

인증 서버에서 상기 사용자가 사용하고자 하는 인증 대상 시스템의 요청에 따라 인증을 위한 챌린지(challenge)를 상기 인증 대상 시스템으로 전송하는 (1) 단계;

상기 인증 대상 시스템에서 음향 채널을 통해 상기 챌린지에 해당되는 비프(beep)를 발생시키는 (2) 단계;

상기 단말기에서 마이크를 통해 상기 챌린지가 수신되면 상기 챌린지에 대한 응답을 생성하여 상기 인증 서버로 전송하는 (3) 단계; 및

상기 인증 서버에서 상기 응답을 통해 상기 사용자를 확인한 후 상기 인증 대상 시스템에 대한 상기 사용자의 접속을 허용하는 (4) 단계

를 포함하는 사용자 인증 방법.

청구항 2

제1항에 있어서,

상기 (2) 단계는,

상기 챌린지에 대하여 일정 크기로 구성된 비프를 적어도 1회 이상 반복하여 발생시키는 것

을 특징으로 하는 사용자 인증 방법.

청구항 3

제1항에 있어서,

상기 (1) 단계는,

상기 인증 대상 시스템에서 상기 인증 서버로 상기 챌린지에 대한 요청과 함께 자신의 접속 정보를 전송하는 단계; 및

상기 인증 서버에서 상기 요청에 따라 상기 챌린지 및 난수를 생성하여 상기 인증 대상 시스템으로 전송하는 단계

를 포함하는 사용자 인증 방법.

청구항 4

제1항에 있어서,

상기 단말기 및 상기 인증 서버에는 상기 사용자의 아이디 및 인증 키가 저장되며,

상기 (3) 단계는,

상기 단말기에서 상기 챌린지 및 상기 인증 키를 이용하여 상기 응답을 생성하는 단계; 및

상기 단말기에서 상기 챌린지와 상기 아이디 및 상기 응답을 상기 인증 서버로 전송하는 단계

를 포함하는 사용자 인증 방법.

청구항 5

제4항에 있어서,

상기 인증 서버는 상기 (1) 단계에서 상기 챌린지와 함께 생성된 난수를 상기 인증 대상 시스템으로 전송하며,

상기 (4) 단계는,

상기 인증 서버에서 상기 단말기로부터 전송된 상기 아이디에 대응되는 상기 인증 키를 이용하여 상기 단말기로부터 전송된 상기 응답을 검증하는 단계;

상기 인증 서버에서 상기 단말기로부터 전송된 상기 챌린지에 연관된 난수와 상기 인증 대상 시스템의 접속 정보를 상기 단말기로 전송하는 단계;

상기 단말기에서 상기 접속 정보를 이용하여 상기 인증 대상 시스템에 접속한 후 상기 인증 서버로부터 전송된 상기 난수를 상기 인증 대상 시스템으로 전송하는 단계; 및

상기 인증 대상 시스템에서 상기 단말기로부터 전송된 난수가 상기 인증 서버로부터 전송된 난수와 일치하면 상기 사용자에게 대한 인증을 완료하는 단계

를 포함하는 사용자 인증 방법.

청구항 6

제1항에 있어서,

상기 단말기와 상기 인증 서버 간의 통신 방식은 SSL(secure sockets layer)/TLS(transport layer security) 기반의 HTTPS(secure hypertext transfer protocol)를 사용하는 것

을 특징으로 하는 사용자 인증 방법.

청구항 7

제1항에 있어서,

상기 단말기에서 타임스탬프(timestamp) 또는 상기 단말기와 상기 인증 서버 간에 공유하는 상태 정보를 상기 응답에 포함시키는 것

을 특징으로 하는 사용자 인증 방법.

명세서

기술 분야

[0001] 본 발명의 실시예들은 마이크와 스피커를 이용하여 스마트폰 사용자에게 대한 인증을 수행하는 인증 방법에 관한 것이다.

배경 기술

[0002] 최근, 스마트폰의 보급이 빠르게 확대됨에 따라 스마트폰 가입자는 천만 명을 넘어섰으며, 이러한 스마트폰 보급의 빠른 확산은 여러 가지 새로운 서비스들을 가능하게 하고 있다. 스마트폰은 인터넷 상에서 인간관계를 형성하는 SNS(Social Networking Service)를 활성화 시키고 있으며, 개인이 인터넷 상에 각종 콘텐츠를 저장하고 언제 어디서나 컴퓨터, 노트북, 스마트폰 등을 이용하여 접속하여 사용할 수 있는 개인형 클라우드 서비스(Cloud service) 기술 발전을 가속화 시키고 있다. SNS나 클라우드 서비스 등과 같이 개인의 데이터를 언제 어디서든 자유롭게 접근할 수 있는 서비스가 증가함에 따라 개인정보보호 문제도 해결해야 할 큰 과제로 남게 되었다. 사용자의 개인 데이터를 안전하게 유지하기 위해서는 데이터에 접근할 수 있는 권한을 제한하는 절차가 필요하며 이를 위해 올바른 접근 권한을 갖는 사용자인지를 확인하는 것이 중요하다.

[0003] 일반적으로, 사용자 인증 방식은 PIN(Personal Identification Number)이나 패스워드를 입력하는 지식 기반 방식, 사용자가 소유하고 있는 장치를 이용하는 토큰 기반 방식과 사용자의 지문이나 행동패턴 등을 이용하는 생체정보 기반 방식으로 분류할 수 있다. 지식 기반으로 인증하는 방법의 경우, PIN이나 패스워드 등을 기억해야 하는 번거로움이 있고, 생체정보 기반으로 인증하는 방법의 경우 생체정보 이용에 대한 사용자 거부감과 생체정보가 유출될 경우 복원할 수 없다는 단점이 있다. 토큰 기반 인증은 이러한 문제점들을 해결할 수 있는 반면, 인터넷 बैं킹을 위한 OTP(One-Time Password)의 예와 같이 인증을 위해 별도의 토큰을 항상 지니고 있어야 한다는 단점이 있다. 별도의 토큰을 지니고 있어야 한다는 단점을 보완하기 위해 휴대 전화나 스마트폰을 토큰으로 활용하는 연구가 활발하게 진행되고 있다. 인터넷 बैं킹을 위한 OTP를 휴대 전화나 PDA 등 모바일 기기에 탑재하거나, 스마트폰을 이용하여 2-D 바코드를 촬영함으로 시스템에 로그인 할 수 있는 인증 방법이 개발되고 있다.

[0004] 국내등록특허 제10-1015633호(등록일 2011년 2월 10일)에는 키보드 해킹 및 엿보기 등으로부터 사용자의 입력 정보를 보호하기 위해, 컴퓨터에서 화면 정보와 음성 정보를 함께 제공하여 사용자로 하여금 이들 두 가지 정보를 조합하여 입력하도록 하는 방식이 개시되어 있다.

[0005] 이와 같은 기존의 안전한 데이터 입력 방식은 기본적으로 음성 챌린지를 사용자에게 전달하고, 이에 사용자가 해당 음향을 직접 확인함으로써 사용자를 인증하는 방식이다. 즉, 기존의 방식들은 신호의 전달하기 위해 인증 대상 시스템이 무선랜, 블루투스(Bluetooth), RF(Radio Frequency) 등의 전파 송수신 장치를 탑재함을 가정하는 경우가 많은데, 일반적으로 노트북 이외의 고정 시스템은 무선 송수신 장치가 기본적으로 장착되어 있지 않으므로 활용도가 떨어진다. 또한, 신호 전달을 위해 초음파 송수신 장치를 이용하는 방식도 토큰 및 인증 대상 시스템에 모두 초음파 송수신 장치를 필요로 하므로 같은 문제점을 가지고 있다. 또한, 스마트폰을 이용하여 2-D 바코드를 촬영하여 인증을 수행하는 방법의 경우 사용자가 2-D 바코드를 촬영하는 동작을 수행해야 되는 번거로움이 있을 수 있다.

[0006] 본 명세서에서는, 사용자가 항상 지니고 있는 스마트폰을 일종의 하드웨어 토큰으로 활용하여 고정시스템 또는 웹사이트 등에 로그인 시 사용자의 불편함을 최소화한 사용자 인증 방식을 제안한다.

발명의 내용

해결하려는 과제

[0007] 사용자가 항상 지니고 있는 스마트폰을 하드웨어 토큰으로 활용함으로써 사용자의 불편함을 최소화 할 수 있는 사용자 인증 방식을 제공한다.

[0008] 고정시스템 또는 웹사이트 등에 로그인 시 사용자의 직접적인 개입이 필요 없는 사용자 인증 방식을 제공한다.

[0009] 정보 입력을 위한 추가적인 장치가 필요하지 않으며 보다 쉽고 간단한 조작만으로 인증을 수행할 수 있는 사용자 인증 방식을 제공한다.

과제의 해결 수단

[0010] 단말기의 사용자에게 대한 인증을 수행하는 사용자 인증 방법은 인증 서버에서 사용자가 사용하고자 하는 인증 대상 시스템의 요청에 따라 인증을 위한 챌린지(challenge)를 인증 대상 시스템으로 전송하는 (1) 단계; 인증 대상 시스템에서 음향 채널을 통해 챌린지에 해당되는 비프(beep)를 발생시키는 (2) 단계; 단말기에서 마이크를 통해 챌린지가 수신되면 챌린지에 대한 응답을 생성하여 인증 서버로 전송하는 (3) 단계; 및 인증 서버에서 응답을 통해 사용자를 확인한 후 인증 대상 시스템에 대한 사용자의 접속을 허용하는 (4) 단계를 포함할 수 있다.

[0011] 일 측면에 따르면, (2) 단계는 챌린지에 대하여 일정 크기로 구성된 비프를 적어도 1회 이상 반복하여 발생시킬 수 있다.

[0012] 다른 측면에 따르면, (1) 단계는 인증 대상 시스템에서 인증 서버로 챌린지에 대한 요청과 함께 자신의 접속 정보를 전송하는 단계; 및 인증 서버에서 요청에 따라 챌린지 및 난수를 생성하여 인증 대상 시스템으로 전송하는 단계를 포함할 수 있다.

[0013] 또 다른 측면에 따르면, 단말기 및 인증 서버에는 사용자의 아이디 및 인증 키가 저장될 수 있으며, (3) 단계는 단말기에서 챌린지 및 인증 키를 이용하여 응답을 생성하는 단계; 및 단말기에서 챌린지와 아이디 및 응답을 인증 서버로 전송하는 단계를 포함할 수 있다.

[0014] 또 다른 측면에 따르면, 인증 서버는 (1) 단계에서 챌린지와 함께 생성된 난수를 인증 대상 시스템으로 전송하며, (4) 단계는 인증 서버에서 단말기로부터 전송된 아이디에 대응되는 인증 키를 이용하여 단말기로부터 전송된 응답을 검증하는 단계; 인증 서버에서 단말기로부터 전송된 챌린지에 연관된 난수와 인증 대상 시스템의 접속 정보를 단말기로 전송하는 단계; 단말기에서 접속 정보를 이용하여 인증 대상 시스템에 접속한 후 인증 서버로부터 전송된 난수를 인증 대상 시스템으로 전송하는 단계; 및 인증 대상 시스템에서 단말기로부터 전송된 난수가 인증 서버로부터 전송된 난수와 일치하면 사용자에게 대한 인증을 완료하는 단계를 포함할 수 있다.

[0015] 또 다른 측면에 따르면, 단말기와 인증 서버 간의 통신 방식은 SSL(secure sockets layer)/TLS(transport layer security) 기반의 HTTPS(secure hypertext transfer protocol)를 사용할 수 있다.

[0016] 또 다른 측면에 따르면, 단말기에서 타임스탬프(timestamp) 또는 단말기와 인증 서버 간에 공유하는 상태 정보

를 응답에 포함시킬 수 있다.

발명의 효과

[0017] 본 발명에서는 스마트폰에 내장되어있는 여러 가지 센서 중에서 기본적인 장치인 마이크를 이용하여 사용자를 인증함으로써 스마트폰을 하드웨어 토큰으로 활용하여 사용자의 불편함을 최소화 할 수 있다. 더욱이, 본 발명은 정보 입력을 위한 추가적인 장치가 필요하지 않고 사용자의 직접적인 개입을 요구하지 않기 때문에 인증 과정의 조작이 보다 쉽고 간단하여 특히 노인이나 시각 장애인 등을 위한 인증 방법으로 활용할 수 있으며 엿보기 공격(Shoulder-surfing attack)에 강하다. 또한, 가청 주파수 중 상대적으로 사람이 듣기 어렵고 소음에 의한 간섭이 적은 15,800Hz~20,000Hz 대역을 이용함으로써 사용자의 불편함을 최소화 하는 동시에 신호 전달 효율을 최대화할 수 있다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 일실시예에 있어서, 음성 챌린지 전달을 위해 사용되는 비프의 할당 주파수 테이블을 도시한 것이다.

도 2는 본 발명의 일실시예에 있어서, 음향 주파수 분석을 이용한 스마트폰 사용자 인증 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0020] 본 실시예들은 음향 신호를 통해 챌린지를 전달하고 별도의 유/무선 채널을 통해 응답을 수신하는 형태로 이루어진 인증 방식에 관한 것이다. 음향을 통해 전달하는 챌린지의 경우, 특정한 주파수 조합의 비프(Beep)를 이용하여 마이크를 통해 해당 비프를 수신하는 기기에서 이를 스펙트럼 방식을 통해 분석하여 인식할 수 있다. 스펙트럼 방식은 마이크를 통해 입력된 음향 신호를 FFT(Fast Fourier Transform) 알고리즘을 통해 해당 음향 신호에 사용된 주파수의 신호강도 형태로 변환하여 분석하는 방식이다. 이때 사용한 신호 강도의 단위는 dBFS(Decibels relative to full scale)이며 디지털 출력의 모든 비트가 1이 되도록 하는 아날로그 입력 레벨을 0dBFS로 나타낸다.

[0021] 본 발명에서 제안하는 인증 방법은 PC나 키오스크(KIOSK)와 같은 고정 시스템을 사용하거나 웹서비스를 이용하기 위해 웹브라우저 상에서 사용자 인증을 수행할 때 사용자가 지닌 스마트폰을 일종의 하드웨어 토큰으로 사용하는 방법이다. 이러한 경우에는 고정 시스템에서 일반적으로 많이 사용하는 스피커를 이용하여 사용자가 지닌 스마트폰으로 음향 챌린지를 전달하므로 추가 하드웨어가 필요하지 않다.

[0022] 본 발명에서 챌린지를 전달하기 위하여 사용하는 비프는 도 1에 도시된 테이블과 같이 구성된다. 일반적으로 음성 통화에 사용되는 스마트폰의 마이크와 스피커는 사람이 들을 수 있는 가청 주파수(20~20,000Hz)에 최적화되어 있으므로 음향의 전달을 위해서는 이영역을 활용하는 것이 바람직하다. 다만, 사람이 쉽게 들을 수 있는 소리를 이용할 경우 사용자의 불편을 초래할 수 있으므로 가청 주파수 영역 중에서도 듣기 어려운 소리에 속하는 15,800~20,000Hz 영역을 사용한다. 이러한 주파수 대역을 챌린지로 사용했을 때 인체에 주는 영향은 크지 않을 것으로 판단되며, 상대적으로 잡음에 의한 간섭도 적다고 볼 수 있다. 다만, 기기마다 인식하는 주파수 영역에 약간의 차이가 있을 수 있으므로, 음향 챌린지 대상 주파수의 선정은 가능한 많은 기기에서 공통적으로 사용하는 영역을 이용하는 것이 바람직하다.

[0023] 동일 시간의 음향 발생으로 많은 데이터를 전달하기 위해서는 해당 주파수 영역을 세분화하여 여러 음향 신호들을 동시에 송신하여야 하나, 음향 신호의 특성상 주파수간 상호 간섭에 의한 잡음인 상호변조잡음(Intermodulation noise)과 원하는 주파수 근방에서 나타나는 불필요한 에너지원에 의한 잡음인 위상잡음(Phase noise) 등으로 인해 동시에 송신될 수 있는 신호의 수에는 한계가 있다. 실험에 의하면, 간섭을 최소화하여 데이터 전달이 가능한 주파수 간격은 약 600Hz이며, 2채널 방식(스테레오 방식)을 이용해 1채널당 하나의 주파수를 발생시킬 경우 해당 대역에서 동시에 4 비트의 신호를 전달할 수 있다. 가령, 두 채널 중 하나의 채널에 15,800Hz, 나머지 한 채널에서 17,000Hz에 해당하는 음향이 감지될 경우 이를 0x0로 인식하게 된다.

[0024] 본 발명에서 제안하는 프로토콜에서 하나의 음향 챌린지는 2바이트의 길이를 가지며, 4비트로 구성된 비프를 4

변 발생시켜 전달한다. 또한, 신호간의 구분을 위하여 1초의 간격을 두고 발생시키며 신호는 1초간 지속되도록 하여 하나의 챌린지 전달에 약 8초가 소요된다.

- [0025] 이하에서는, 특정 시스템에 로그인하기 위해 스마트폰을 토큰으로 활용하는 인증 방법을 구체적으로 설명하기로 한다.
- [0026] 본 발명에 따른 사용자 인증 방법은 인증 대상 시스템이 사용자의 고정 PC인 경우 이외에도 키오스크나 웹브라우저와 같이 고정 시스템을 경유 장치로 활용하는 경우에도 적용할 수 있다. 예를 들어, 온라인상에서 예매한 승차권을 현장에서 키오스크를 통해 발매 받는 경우 스마트폰은 원격 서버에서 키오스크를 경유하여 제공되는 챌린지 정보에 응답하여 키오스크에 로그인하게 되며, 또한 PC에서 웹 브라우저를 통해 웹 서비스에 로그인을 할 경우 스마트폰은 웹 서버에서 제공하는 챌린지에 응답하여 웹사이트에 로그인할 수 있다.
- [0027] 본 실시예에서는 스마트폰을 일 예로 하여 사용자 인증 방법을 설명하고 있으나, 이에 한정되는 것은 아니며 음향 수신이 가능한 모든 단말기에 적용 가능하다.
- [0028] 도 2는 본 발명의 일실시예에 따른 사용자 인증 방법을 도시한 흐름도이다.
- [0029] 도 2에 도시한 바와 같이, 본 발명의 사용자 인증 방법은 스마트폰(100)과 인증 대상 시스템(200) 및 인증 서버(웹 서버)(300)로 이루어진 시스템 구성에 의해 각각의 단계가 수행될 수 있다. 즉, 본 발명의 사용자 인증 방법에 참여하는 주체는 스마트폰(100), 인증 대상 시스템(200), 그리고 인증 서버(300)로 구성될 수 있다. 이때, 스마트폰(100)과 인증 서버(300)는 사전에 신뢰 관계(예컨대, 회원 가입 등)가 성립되어 사용자의 아이디와 16바이트 길이의 인증 키(K)를 공유한다고 가정한다. 이러한 설정은 사용자가 고정 PC에 로그인하는 경우에도 유동 IP 주소 등의 문제로 응답 전송을 위한 목적지 정보를 정할 수 없을 때 유용하게 사용될 수 있으며, 고정 PC가 고정 IP를 보유할 경우에는 인증 서버(300)가 고정 PC와 같은 기기가 되도록 구성하는 것도 가능하다.
- [0030] 본 실시예에서 챌린지 정보는 인증 서버(300)로부터 생성되어 인증 대상 시스템(200)을 경유한 후, 다시 음향 채널을 통해 스마트폰(100)에 전달되며, 응답은 스마트폰(100)의 3G IP 망을 통해 직접 인증 서버(300)로 전달될 수 있다. 응답의 전송 전까지 인증 대상 시스템(200)이나 인증 서버(300)는 사용자의 신원 정보를 알 수 없으며, 신원 정보는 응답과 함께 인증 서버(300)로 전달되도록 한다.
- [0031] 도 2는 본 발명의 일실시예에 따른 사용자 인증 프로토콜을 구체적으로 나타낸 도면이다. 도 2에서 각 구성 간의 통신 흐름을 나타내는 선들 중 실선은 HTTP(Hypertext Transfer Protocol)를 기반으로 한 유/무선통신을, 점선은 음향 채널을, 긴 파선-점선은 소켓 통신을 나타낸다.
- [0032] 상세하게, 인증 절차는 먼저 인증 대상 시스템(200)이 자신의 접속 정보로 소켓통신에 사용할 랜덤한 포트를 설정하여 챌린지 요청과 함께 인증 서버(300)로 전송한다(S101). 이때, 인증 서버(300)는 2바이트의 챌린지 C와 16바이트 길이의 난수 R쌍을 생성하여(S102) 인증 서버(300) 내에 저장한 후, 인증 대상 시스템(200)으로 전송한다(S103).
- [0033] 인증 서버(300)로부터 챌린지를 전달받은 인증 대상 시스템(200)은 구비된 스피커를 통해 챌린지에 해당되는 비프를 발생시킨다(S104). 이에, 인증 대상 시스템(200)으로부터 근거리에서 위치한 스마트폰(100)은 내장된 마이크로 챌린지를 전달 받은 후, 인증 서버(300)와 사전에 교환된 키 K를 이용하여 응답 A를 생성한다(S105). 이때, 응답 A는 사전에 교환된 키 K를 이용하여 음향을 통해 전달받은 챌린지 C'를 암호화하여 생성한 것이다. 다음으로, 스마트폰(100)에서 미리 지정된 사용자의 아이디와 음향을 통해 전달받은 챌린지 C', 그리고 앞서 생성한 응답 A를 인증 서버(300)로 전송한다(S106).
- [0034] 인증 서버(300)에서는 스마트폰(100)에서 전송된 아이디에 해당하는 사용자의 키 K를 이용하여 스마트폰(100)에서 전송 받은 응답 A를 검증한다(S107). 이때, 인증 서버(300)는 인증 대상 시스템(200)으로 전송한 챌린지 C와 사용자의 키 K를 이용하여 검증을 위한 응답 A'를 생성할 수 있다. 그리고, 인증 서버(300)는 스마트폰(100)에서 전송 받은 응답 A와 검증을 위해 생성된 응답 A'가 동일하면, 챌린지 C'에 연관된 난수 R'와 인증 대상 시스템(200)의 접속정보(IP, 포트 등)를 스마트폰(100)으로 전송한다(S108).
- [0035] 인증 서버(300)에 정상적인 응답이 도달하였다는 것은 음성으로 전달되는 챌린지를 스마트폰(100)이 정상적으로 수신하였음을 의미하므로 스마트폰(100)을 지닌 사용자의 위치가 인증 대상 시스템(200)과 근접한 거리에 있음을 보장할 수 있다. 또한, 인증 서버(300)와 사용자만 지닌 키 K를 이용하기 때문에 등록된 사용자인 사실도

확인할 수 있다.

[0036] 다음으로, 스마트폰(100)은 인증 서버(300)로부터 받은 접속정보를 이용하여 인증 대상 시스템(200)에 접근한 후, 소켓통신을 통해 난수 R'를 인증 대상 시스템(200)으로 전송한다(S109). 이때, 난수 R'를 전송 받은 인증 대상 시스템(200)은 인증 서버(300)로부터 받은 난수 R과 사용자의 스마트폰(100)으로부터 받은 난수 R'를 비교하여 세션 정보를 확인한다(S110). 이어, 인증 대상 시스템(200)은 두 난수 R과 R'가 동일하면 인증 서버(300)로 해당 사용자의 신원 정보를 요청하여 인증 서버(300)로부터 제공받아 사용자의 인증을 완료한다(S111)(S112).

[0037] 본 발명의 실시예에 따른 사용자 인증 방법은 일정시간 내에 음향을 이용한 챌린지가 모두 전달되지 않거나, 주어진 챌린지에 대한 응답이 잘못된 경우 인증에 실패하게 된다. 악의적인 공격자 이외에 정상적인 사용자의 경우에도 주변 환경에 따른 챌린지 전달 및 무선 통신 문제 등으로 인증에 실패할 수 있으므로, 사용자는 일정 회수 챌린지를 재요청하여 인증을 다시 수행할 수 있도록 구성한다.

[0038] 본 발명에서의 제안 프로토콜은 스마트폰에서 인증 대상 시스템에 접속하기 위한 인증 과정 중 인증 서버로부터 인증 대상 시스템의 접속정보를 전달받는 과정에서 공격자가 통신로 상에서 데이터를 몰래 획득하는 엿듣기(Sniffing) 공격을 시도할 경우 HTTP 통신만으로는 접속정보가 유출될 수 있다. 그러나, 이 부분은 SSL/TLS 기반의 HTTPS(Secure Hypertext Transfer Protocol)로 간단하게 전환할 수 있으므로 스마트폰과 인증 서버 간 프로토콜의 HTTP 구간은 안전하다고 보아도 무방하다. 또한, 공격자가 과거 인증 세션에서 교환했던 챌린지나 응답을 기록하였다가 이후 세션에 재사용하는 재사용 공격을 고려해 볼 수 있는데, 기본적으로 16비트 챌린지를

이용하고 있으므로 $\frac{1}{2^{16}}$ 확률로 공격에 성공할 수 있다. 이러한 위험 요소는 스마트폰에서의 응답 생성에 있어 타임스탬프(Timestamp)를 포함하거나 스마트폰과 인증 서버 사이에 카운터(Counter) 등 상태 정보를 추가적으로 공유하여 응답 생성 시 포함하도록 함으로써 위협을 감소시킬 수 있다. 보다 근본적으로는, 챌린지의 비트 수를 늘리는 방안을 고려해 볼 수 있으나, 이는 음향 신호 전달을 위해 더 긴 시간이 필요함을 의미하므로 사용자의 불편을 초래할 수 있다.

[0039] 본 실시예에서 사용자 인증 방법의 프로세스는 적어도 하나의 신호 처리 및/또는 애플리케이션에 고유한 집적 회로를 포함하는 하드웨어 및/또는 소프트웨어로 구현될 수 있다.

[0040] 본 발명의 실시예에 따른 방법들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 특히, 본 실시예의 사용자 인증 방법에서 스마트폰에 종속되는 기능들은 모바일 단말 전용 어플리케이션(예를 들어, 스마트폰 어플리케이션, 피쳐폰 VM(virtual machine) 등의 형태)으로 구성될 수 있다. 이는, 스마트폰에서 구동되는 적어도 하나의 프로세서에 의해 실행되도록 구성될 수 있다.

[0041] 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 또한, 상술한 파일 시스템은 컴퓨터 판독이 가능한 기록 매체에 기록될 수 있다.

[0042] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0043] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0044] 100: 스마트폰

200: 인증 대상 시스템

300: 인증 서버

도면

도면1

Bit	주파수(Hz)
0x0	15800, 17000
0x1	16400, 17600
0x2	17000, 18200
0x3	17600, 18800
0x4	18200, 19400
0x5	18800, 20000
0x6	15800, 17600
0x7	16400, 18200
0x8	17000, 18800
0x9	17600, 19400
0xa	18200, 20000
0xb	15800, 18200
0xc	16400, 18800
0xd	17000, 19400
0xe	17600, 20000
0xf	15800, 18800

도면2

