(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 9/14 (2006.01)

(45) 공고일자 2006년05월22일
(11) 등록번호 10-0581590
(24) 등록일자 2006년05월12일

(21) 출원번호 10-2003-0042611
(22) 출원일자 2003년06월27일

(65) 공개번호 10-2005-0000481
(43) 공개일자 2005년01월05일

(73) 특허권자 주식회사 케이티
경기 성남시 분당구 정자동 206

(72) 발명자 박영만
서울특별시노원구상계6동미도아파트102동210호

이성춘
서울특별시강남구대치동미도아파트106동204호

차용주
경기도성남시분당구금곡동청솔마을화인아파트204동303호

(74) 대리인 유미특허법인

(56) 선행기술조사문헌
JP08096043 A
JP09307542 A
JP10155170 A
JP10340255 A
논문
* 심사관에 의하여 인용된 문헌

심사관 : 나용수

(54) 이중 요소 인증된 키 교환 방법 및 이를 이용한 인증방법과 그 방법을 포함하는 프로그램이 저장된 기록매체

요약

본 발명은 이중 요소 인증된 키 교환 방법 및 이를 이용한 인증 방법과, 그 방법을 포함하는 프로그램이 저장된 기록매체에 관한 것이다. 이 이중 요소 인증된 키 교환 방법은 가입자 단말기가 자신의 식별자와 인증 서버의 공개키를 사용하여 생성된 값을 상기 액세스 포인트를 통해 인증 서버로 송신한다. 인증 서버는 가입자 단말기로부터 수신된 값을 사용하여 가입자 관련 패스워드 및 대칭키와 인증 서버의 비밀키를 검출하고, 난수를 생성하여 가입자 단말기로 송신한다. 가입자 단말기는 수신된 난수와 패스워드 및 대칭키를 사용하여 특정 값을 암호화한 값과 생성된 가입자측 인증자를 인증 서버로 송신한다. 인증 서버는 패스워드, 대칭키 및 난수를 사용하여 생성한 제2 특정 값을 복호화 키로 하여 상기 수신된 암호화 값을 복호하고, 복호된 값에 기초하여 가입자측 인증자에 대한 인증을 수행하며, 인증이 성공되는 경우, 패스워드, 대칭키 및 공개키를 사용하여 생성된 인증 서버측 인증자를 가입자 단말기로 송신한다. 가입자 단말기는 대칭키와 패스워드를 사용하

여 인증 서버측 인증자에 대한 인증을 수행한다. 본 발명에 따르면, 이중 요소 인증 방식을 사용하여 다른 어떤 EAP 인증 방식보다 더 강력한 개체 인증을 제공한다. 또한, 공중 무선랜에서 PDAs에 적용할 수 있을 정도로 보안성과 효율성을 가진다.

대표도

도 1

색인어

이중 요소 인증, TAKE, 인증 방법, 키 교환 프로토콜, AKE, 키 설정 방법

명세서

도면의 간단한 설명

도 1은 본 발명의 실시예에 따른 TAKE 프로토콜의 흐름도이다.

도 2는 본 발명의 실시예에 따른 TAKE 프로토콜을 사용한 (공중)무선랜에서의 인증 및 키 교환 흐름도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 인증 및 키 설정(Authentication and Key Establishment:AKE) 프로토콜에 관한 것으로, 보다 구체적으로는 인터넷, 무선랜(wireless LANs), 공중 무선랜(public access wireless LANs) 등의 서비스에서 이중 요소 인증된 키 교환(Two-factor Authenticated Key Exchange:TAKE) 방법과 이를 이용하여 개체(entity) 인증 및 키 설정을 위한 보안을 수행하는 방법 및 그 방법을 포함하는 프로그램이 저장된 기록매체에 관한 것이다.

종래의 인증 및 키 설정 방법에는 대표적으로 인증서를 이용한 TLS(Transport Layer Security) 방식과 패스워드를 이용한 SRP(Secure Remote Password) 방식, EAP-MD5 방식, 그리고 인증서 및 패스워드, 2가지를 모두 이용한 PEAP (Protected EAP), EAP-TTLS(Tunneled TLS) 등이 있으나, 각 방식들은 단점을 가지고 있다. 즉, TLS는 복잡하고 비용이 많이 드는 PKI(Public Key Infrastructure) 및 인증서 관리 시스템이 필요하고, SRP는 사용자 단말측에 많은 연산량(2 exponentiation)을 요구하며, 2-for-1 guess attack에 취약하다. 또한 PEAP와 EAP-TTLS는 MitM(Man-in-the-Middle) 공격에 취약하고, 교환 메시지 횟수가 많다. 그리고 EAP-MD5는 상호 인증과 세션(session) 키를 제공하지 않는 단점이 있다.

특히, (공중)무선랜에서 PDAs(Personal Digital Assistants)를 사용할 경우 적용할 수 있는 안전하고 효율적인 802.1x의 EAP(Extensible Authentication Protocol) 인증방식을 찾기가 쉽지 않다. 왜냐하면 PDAs는 지수화(exponentiation)와 역원(inverse element) 계산과 같은 복잡한 연산량을 수행하는데 시간이 많이 걸리고 전력(power)이 많이 소비되기 때문이다.

한편, 일반적으로 인증 요소에는 (1) 사용자가 기억 하는 것(패스워드)과 (2) 사용자가 가지고 있는 것(토큰(token)이나 무선기기)과 같이 2개의 요소가 있다.

이 중에서 (1)번 항목의 패스워드를 이용한 단일 요소 인증 방식은 다음과 같은 여러 가지 문제점으로 인해 결코 안전하지 않다는 문제점이 있다. 첫 번째로는 사용자가 패스워드를 입력할 때 누군가가 사용자의 어깨너머로 패스워드를 훔쳐 볼 수 있고, 키스트로크 모니터링(keystroke monitoring)으로 패스워드가 노출될 수 있다는 것이다. 두 번째로는 사기, 협박 등과 같은 사회 공작(social engineering)적 방법으로 패스워드를 공격자에게 노출시킬 수 있다는 것이다. 세 번째로는 패스워드는 정보량 측면에서 낮은 엔트로피(entropy)를 가지고 있어 사전 공격(dictionary attack)에 취약하다는 것이다. 네 번째로는 패스워드를 물리적으로 기록하거나 유사 패스워드를 여러 곳에 갱신없이 사용하는 것과 같은 사용자들의 나쁜 습관으로 인해 패스워드가 노출될 수 있다는 것이다. 특히, 핫 스팟(hot spot) 지역에서 네트워크 접속을 시도하는 공중 무

선랜 서비스는 한층 더 공격에 위험하다고 할 수 있다. 비록, 가입자를 패스워드로 인증하는 EAP-SRP, PEAP, EAP-TTLS 방식이 사전 공격(dictionary attack)에 안전한 프로토콜이라 하더라도 공격자는 오프라인상에서 키스트로크 모니터링이나 사회 공작적 방법으로 패스워드를 획득할 수도 있기 때문이다.

또한, (2)번 항목의 토큰이나 무선기기를 이용한 단일 요소 인증 방식은 토큰과 토큰을 읽을 수 있는 입력장치(카드 리더기)가 필요하다는 단점이 있다. 두 번째 요소인 토큰은 스마트 카드, USB(Universal Serial Bus) 키, 그리고 PDAs와 같은 무선 기기 등이 될 수 있다. 따라서, 무선 환경에서는 토큰을 USB 키나 무선 기기로 사용하면 특별히 하드웨어를 추가하지 않아도 되므로 비용이 많이 들지 않는다. 단, 토큰은 대칭 비밀키 또는 개인의 인증 관련 비밀 정보가 저장되어야 하므로, 어느 정도의 불법 변조 방지(temper resistant)특성을 가진 보안 모듈에 저장되어야 한다.

따라서, 인터넷이나 (공중)무선랜 등에서는 상기한 인증 요소들에 의한 인증에 비해 보다 강력한 인증 체계를 요구하며, 특히 다음과 같은 기술적 요구사항을 해결할 수 있는 인증 방법이 요구된다.

① 신원 보호(identity protection) : 도청과 같은 수동적 공격(passive attack)으로부터 가입자(client)의 신원을 보호하는 것은 개인의 통신비밀(privacy)을 위해 필요하다. 특히, DHCP(Dynamic Host Configuration Protocol)로 IP 주소를 할당받는 사용자에게는 유용한 것이다.

② 강력한 상호 인증(mutual authentication) : 공격자(attacker)들은 가입자와 인증서버(Authentication Sever) 사이에 위치하여 MitM 공격을 수행할 수 있기 때문에 가입자와 망(network)에 대한 상호 인증이 필요하다.

③ 세션 키 설정 : 가입자와 망 사이에 교환되는 데이터를 보호하기 위해 세션 키(session key)가 설정되어야 한다.

④ Forward Secrecy(FS) : 프로토콜에 참여하는 개체의 long term secret keying material이 노출되더라도 공격자가 이전에 도청된 세션으로부터 과거 세션 키를 계산할 수 없는 성질인 FS가 제공되어야 한다. 이러한 FS는 half FS와 full FS로 나눌 수 있는데, 전자는 가입자와 인증서버 중 어느 한 개체의 비밀 키가 노출되더라도 공격자는 과거 세션 키를 유도할 수 없음을 의미하고, 후자는 두 개체의 비밀키가 모두 노출된 경우에도 세션 키가 안전함을 의미한다.

⑤ 오프라인 사전(offline dictionary) 공격에 대한 안전성 : 공격자가 오프라인 사전 공격을 수행하여 가입자와 서버간에 공유된 비밀 정보를 얻지 못하도록 프로토콜은 설계되어야 한다.

⑥ MitM(Man-in-the-Middle) 공격에 대한 안전성 : (공중)무선랜 환경에서는 rouge AP(Access Point)나 rouge 무선 NIC을 사용한 MitM공격에 취약하므로 이에 대한 공격에 안전하도록 설계되어야 한다.

⑦ Replay 공격에 대한 안전성 : 공격자가 사용된 메시지를 재전송하여 인증 및 키 설정에 성공할 수 없게 해야 한다.

⑧ 효율성(efficiency)

- 연산 부하의 최소화 : (공중)무선랜 환경에서 PDAs에 적용할 수 있을 정도의 적은 연산량을 요구하여야 한다. 그리고 사전 계산(pre-computation)을 이용하여 온라인(on-line) 계산의 부하를 최소화하여야 한다.

- 메시지 교환 횟수의 최소화 : 망 자원의 효율성과 망 상의 지연(delay) 등을 고려할 때 통신 라운드(round) 수가 적을수록 장점이 있다. 따라서 가입자와 인증서버 사이에 교환하여야 할 메시지의 횟수를 가능한 적게 하여야 한다.

- 통신 대역폭 사용의 최소화 : 프로토콜 메시지의 크기를 가능한 작게하여야 한다.

⑨ 키 확인(key confirmation) : 프로토콜에 참여한 합법적인 사용자가 자신이 의도한 상대방과 실제로 공통의 비밀 세션 키를 공유하였음을 확인하여야 한다.

⑩ 부인 봉쇄(non repudiation) : 서비스 사용 시간과 망 접속 횟수 등과 같은 과금 데이터에 대하여 사용자가 부인할 수 없는 부인 봉쇄 기능이 제공될 수 있어야 한다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명의 목적은 상기한 종래의 문제점을 해결하기 위한 것으로, 2개의 독립적인 인증 요소인 패스워드와 대칭키(symmetric key)가 저장된 토큰을 이용하여 가입자를 인증하는 이중 요소 인증된 키 교환(TAKE) 방법 및 이를 이용한 인증 방법과 그 방법을 포함하는 프로그램이 저장된 기록매체를 제공하는 데 있다.

발명의 구성 및 작용

상기한 목적을 달성하기 위한 본 발명의 특징에 따른 이중 요소 인증된 키 교환 방법은,

유무선 통신을 통해 인증 서버에 접속된 가입자 단말기에서 상호 인증을 위한 키를 교환하는 방법으로서,

a) 상기 가입자 단말기가 자신의 식별자와 상기 인증 서버의 공개키를 사용하여 생성된 키를 상기 인증 서버로 송신하는 단계; b) 상기 가입자 단말기가 상기 인증 서버에서 생성된 난수를 수신하는 단계; c) 상기 수신된 난수와 상기 가입자 단말기에 미리 설정되어 있는 패스워드 및 대칭키를 사용하여 제1 특정 값을 암호화한 값과 생성된 가입자측 인증자를 상기 인증 서버로 송신하는 단계; d) 상기 가입자 단말기가, 상기 송신된 가입자측 인증자에 대한 상기 인증 서버에서의 인증 성공에 따라 상기 인증 서버에서 생성된 인증 서버측 인증자를 수신하는 단계; 및 e) 상기 가입자 단말기가 상기 제 1 특정값과 패스워드를 사용하여 상기 수신된 인증 서버측 인증자에 대한 인증을 수행하고, 상기 인증이 성공되는 경우 상기 인증 서버측 인증자를 받아들이는 단계를 포함한다.

상기 이중 요소 인증된 키 교환 방법은 상기 a) 단계 전에, 상기 가입자 단말기가 등록 과정에서 대칭키 알고리즘에 사용되는 상기 대칭키와 상기 패스워드를 결정하여 상기 인증 서버와 공유하는 단계; 및 상기 가입자 단말기가 상기 인증 서버와 인증을 위한 키 교환을 수행하지 않는 때에 난수를 생성하여 상기 제1 특정 값을 사전 계산하는 단계를 더 포함한다.

여기서, 상기 가입자 단말기는 상기 대칭키, 상기 패스워드 및 상기 인증 서버의 공개키를 토큰에 저장하는 것이 바람직하다.

또한, 상기 a) 단계에서, 상기 생성되는 키는 상기 가입자 단말기의 식별자와 상기 인증 서버의 공개키에 대해 일방향 해쉬 함수를 사용하여 생성되는 것이 바람직하다.

또한, 상기 c) 단계는, 상기 수신된 난수, 상기 패스워드 및 대칭키에 대해 해쉬 함수를 사용하여 제2 특정 값을 생성하는 단계; 상기 생성된 제2 특정 값을 사용하여 상기 제1 특정 값을 암호화하는 단계; 상기 난수와 상기 제1 특정 값을 사용하여 상기 가입자측 세션키를 생성하는 단계; 상기 생성된 세션키, 상기 패스워드, 상기 대칭키 및 상기 가입자 단말기의 식별자에 대해 해쉬 함수를 사용하여 상기 가입자측 인증자를 생성하는 단계; 및 상기 제1 특정 값을 암호화한 값과 상기 가입자측 인증자를 상기 인증 서버로 송신하는 단계를 포함한다.

또한, 상기 e) 단계는, 상기 가입자측 세션키, 상기 패스워드, 상기 대칭키 및 상기 인증 서버의 공개키에 대해 해쉬 함수를 사용하여 제3 특정 값을 생성하는 단계; 상기 생성된 제3 특정 값과 상기 인증 서버로부터 수신된 인증 서버측 인증자가 동일한 지의 여부를 판단하는 단계; 및 상기 생성된 제3 특정 값과 상기 인증 서버로부터 수신된 인증 서버측 인증자가 동일한 경우, 상기 가입자 단말기와 상기 인증 서버간의 인증이 성공된 것으로 판단하여 상기 인증 서버측 인증자를 받아들이는 단계를 포함한다.

본 발명의 다른 특징에 따른 이중 요소 인증된 키 교환 방법은,

유무선 통신을 통해 가입자 단말기에 접속된 인증 서버에서 상호 인증을 위한 키를 교환하는 방법으로서,

a) 상기 인증 서버가 상기 가입자 단말기에서 식별자와 상기 인증 서버의 공개키를 사용하여 생성된 키를 수신하는 단계; b) 상기 인증 서버가 상기 가입자 단말기로부터 수신된 값을 사용하여 상기 가입자 관련 패스워드 및 대칭키와 상기 인증 서버의 공개키를 검출하고, 난수를 생성하여 상기 가입자 단말기로 송신하는 단계; c) 상기 인증 서버가, 상기 송신된 난수에 기초하여 상기 가입자 단말기에서 생성된 암호화 값과 가입자측 인증자를 수신하는 단계; d) 상기 인증 서버가 상기 패스워드, 상기 대칭키 및 상기 난수를 사용하여 생성한 제1 특정 값을 비밀 키로 하여 상기 c) 단계에서 수신된 암호화 값을 복호하여 제2 특정 값을 생성하고, 상기 생성된 제2 특정 값에 기초하여 상기 수신된 가입자측 인증자에 대한 인증을 수행하고, 상기 인증이 성공되는 경우 상기 가입자측 인증자를 받아들이는 단계; 및 e) 상기 인증 서버가 상기 상기 패스워드, 대칭키 및 공개키를 사용하여 생성된 인증 서버측 인증자를 상기 가입자 단말기로 송신하는 단계를 포함한다.

이 이중 요소 인증된 키 교환 방법은 상기 a) 단계 전에, 상기 인증 서버가가 등록 과정에서 대칭키 암호 알고리즘에 사용되는 상기 대칭키와 상기 패스워드를 결정하여 상기 가입자 단말기와 공유하는 단계를 더 포함한다.

여기서, 상기 인증 서버는 상기 대칭키, 상기 패스워드 및 상기 인증 서버의 비밀키를 보안 파일 관련 데이터베이스 내에 저장하는 것이 바람직하다.

또한, 상기 d) 단계는, 상기 패스워드, 상기 대칭키 및 상기 난수에 대해 해쉬 함수를 사용하여 상기 제1 특정 값을 생성하는 단계; 상기 생성된 제1 특정 값을 비밀키로 하여 상기 수신된 암호화 값을 복호하여 상기 제2 특정 값을 생성하는 단계; 상기 생성된 제2 특정 값, 상기 인증 서버의 공개키 및 상기 난수를 사용하여 상기 인증 서버측 세션키를 생성하는 단계; 상기 생성된 세션키, 상기 패스워드, 상기 대칭키 및 상기 가입자 단말기의 식별자에 대해 해쉬 함수를 사용하여 구해진 값과 상기 수신된 가입자측 인증자가 동일한 지의 여부를 판단하는 단계; 및 상기 구해진 값과 상기 수신된 가입자측 인증자가 동일한 경우, 상기 가입자에 대한 인증이 성공된 것으로 판단하여 상기 가입자측 인증자를 받아들이는 단계를 포함한다.

또한, 상기 e) 단계에서 상기 인증 서버측 인증자 생성에 상기 생성된 인증 서버측 세션키가 사용되는 것이 바람직하다.

또한, 상기 a) 단계에서, 상기 가입자 단말기의 식별자가 글로벌 로밍과 과금을 지원하기 위해 NAI(Network Access ID) 형식을 사용하는 경우, 상기 가입자 단말기가 사용자 이름 부분과 상기 인증 서버의 공개키를 해쉬한 값과 영역 이름 부분을 함께 상기 인증 서버로 송신하는 것이 바람직하다.

본 발명의 또 다른 특징에 따른 이중 요소 인증된 키 교환 방법을 이용한 인증 방법은,

액세스 포인트(Access Point)를 통해 가입자 단말기와 인증 서버가 접속된 무선 통신 시스템에서 상기 가입자 단말기와 상기 인증 서버간에 이중 요소 인증된 키 교환을 통하여 상호 인증하는 방법으로서,

a) 상기 가입자 단말기가 상기 액세스 포인트로부터 식별자 요청을 받는 단계; b) 상기 가입자 단말기가 자신의 식별자와 상기 인증 서버의 공개키를 사용하여 생성된 키를 상기 액세스 포인트를 통해 상기 인증 서버로 송신하는 단계; c) 상기 인증 서버가 상기 가입자 단말기로부터 수신된 키를 사용하여 상기 가입자 관련 패스워드 및 비밀키와 상기 인증 서버의 공개키를 검출하고, 난수를 생성하여 상기 액세스 포인트를 통해 상기 가입자 단말기로 송신하는 단계; d) 상기 가입자 단말기가 상기 수신된 난수와 상기 패스워드 및 대칭키를 사용하여 제1 특정 값을 암호화한 값과 생성된 가입자측 인증자를 상기 액세스 포인트를 통해 상기 인증 서버로 송신하는 단계; e) 상기 인증 서버가 상기 패스워드, 상기 대칭키 및 상기 난수를 사용하여 생성한 제2 특정 값을 비밀 키로 하여 상기 d) 단계에서 수신된 암호화 값을 복호하고, 상기 복호된 값에 기초하여 상기 수신된 가입자측 인증자에 대한 인증을 수행하고, 상기 인증이 성공되는 경우, 상기 상기 패스워드, 대칭키 및 공개키를 사용하여 생성된 인증 서버측 인증자를 상기 액세스 포인트를 통해 상기 가입자 단말기로 송신하는 단계; f) 상기 가입자 단말기가 상기 대칭키와 패스워드를 사용하여 상기 수신된 인증 서버측 인증자에 대한 인증을 수행하고, 그 인증 결과를 상기 액세스 포인트를 통해 상기 인증 서버로 송신하는 단계; 및 g) 상기 인증 서버가 상기 가입자 단말기로부터 송신된 인증 결과가 성공으로 나타난 경우 상기 가입자에 대한 접속 허가를 상기 액세스 포인트를 통해 상기 가입자 단말기로 송신하는 단계를 포함한다.

여기서, 상기 가입자 단말기와 상기 액세스 포인트 사이에서는 확장 가능한 인증 프로토콜(Extensible Authentication Protocol:EAP)이 사용되고, 상기 액세스 포인트와 상기 인증 서버 사이에서는 RADIUS 프로토콜이 사용되는 것이 바람직하다.

아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였다. 명세서 전체를 통하여 유사한 부분에 대해서는 동일한 도면 호를 붙였다.

먼저, 본 발명의 실시예에 따른 TAKE 프로토콜을 이용한 인증 방법에 대해 상세하게 설명한다.

도 1은 본 발명의 실시예에 따른 TAKE 프로토콜의 흐름도이다.

도 1을 참조하여 본 발명의 실시예에 따른 TAKE 프로토콜에 대해 설명하기 전에 먼저 본 발명의 실시예에서 기술되는 기호에 대해 다음과 같이 정의한다.

A : 가입자(supplicant 또는 client)

B : 인증 서버(authentication server)

π : 패스워드

t : 대칭키 암호에서 사용되는 대칭키

ID_A : 가입자 A의 식별자(identifier)

$E_K\{\ \}$, $D_K\{\ \}$: 대칭키 K로 대칭키로 암호화 및 복호화

H( ) : 일방향 해쉬함수

sk_A : A가 생성한 세션 키(session key)

p : 큰 소수

q : (p-1)을 나누는 큰 소수인 수

g : 위수(order)가 q인 Z_p^*의 원소인 생성원

b, $g^b \pmod p$: 인증 서버 B의 정적(static) 비밀키, 공개키

다음, 도 1을 참조하면, 본 발명의 실시예에 따른 TAKE 프로토콜의 동작은 등록(enrollment) 단계, 사전계산(precomputation) 단계 및 실행 단계로 나누어질 수 있다.

먼저, 등록 단계에 대해 설명한다.

가입자(Client A), 실질적으로는 가입자의 무선 단말기와 서버(Server B)는 3DES(Data Encryption Standard)나 Rijndael과 같은 대칭키 암호 알고리즘에 사용되는 대칭키(t)와 패스워드(π)를 결정하여 서로 공유한다. 그리고 서버는 특정 가입자에 대한 서버의 비밀키 [1 ~ q-1] 범위의 임의의 수 <b>를 선택하여 안전한 데이터베이스(DB)에 저장하고, 가입자에게 서버의 공개키(g^b)와 도메인 파라메터(p, q, g)를 알려준다. 가입자는 대칭키(t)를 토큰에 저장한다. 서버의 공개키(g^b)와 도메인 파라메터(p, q, g)는 공개될 수 있는 성질의 정보이므로 반드시 안전한 장소에 저장되어야 하는 것은 아니다.

다음, 사전계산(precomputation) 단계에 대해 설명한다.

본 발명의 실시예에 따른 사전계산은 프로토콜 수행 전인 오프라인 상에서 이루어지는 단계로, 프로토콜 수행 중에 소요되는 시간과 계산량을 감소시킨다.

가입자의 무선 단말기는 무선 네트워크를 사용하지 않는 빈 시간(idle time)이나 단말기 파워 온(power on)시에 사전계산을 수행한다. 도 1에 도시된 바와 같이, 가입자 A는 [1 ~ q-1] 범위에 있는 임의의 수 x를 선택한다. 즉, 가입자는 임의의 수 $x \in_R Z_q$를 선택한 후, 선택된 임의의 수 x를 사용하여 g^x, $g^{bx} = c$(이후 mod p)는 생략함)를 사전계산한다.

다음, 실행 단계에 대해 설명한다.

이 실행 단계는 상호 개체 인증과 세션 키 설정을 수행하는 단계로 다음과 같은 절차로 이루어진다.

① 가입자 A는 인터넷이나 (공중)무선랜 서비스 접속을 위해 자신의 식별자 ID_A와 인증 서버 B의 공개키(g^b)를 해쉬한 값인 $H(ID_A, g^b)$를 인증 서버 B에게 보낸다.

만일, 가입자 ID가 글로벌 로밍과 과금을 지원하기 위해 NAI(network access ID) 형식을 사용하는 경우, 예를 들어 가입자 ID가 userid@realm.com인 경우, 사용자 이름 부분과 g^b를 해쉬한 값인 $H(userid, g^b)$와 영역 이름 부분을 함께 보낸다.

② $H(ID_A, g^b)$를 받은 인증 서버 B는 가입자 보안 파일 관련 데이터베이스(DB)에서 <$H(ID_A, g^b)$>, <ID_A>, <π>, <t>, <b>를 검출해 낸다. 인증 서버 B는 [1 ~ q-1] 범위에 있는 임의의 수 $r \in_R Z_q$을 선택하여 가입자 A에게 보낸다.

③ 가입자 A는 인증 서버 B가 보내온 임의의 수 r을 수신하면, π 및 t와 함께 사용하여 해쉬한 값 f=H(r, π, t)를 계산한 후, 이 f를 g^x를 대칭키 암호화하는 대칭키로 사용하여 $e = E_f\{g^x\}$를 계산한다. 그리고, c, g^x 및 r을 해쉬한 값인 세션키 sk_A=H(c, g^x, r)를 계산한 후 π, t 및 ID_A를 해쉬한 값인 인증자 M_A=H(sk_A, π, t, ID_A)를 생성한다.

가입자 A는 상기 생성된 e 와 M_A를 인증 서버 B에게 보낸다.

④ 인증 서버 B는 가입자 A로부터 송신된 e와 M_A를 받아서 r, π 및 t를 사용하여 해쉬하여 f=H(r, π, t)를 계산하고, 수신된 e를 상기 계산된 비밀키 f로 복호화하여 $g^x = D_f\{e\}$를 구한다.

그 후, 인증 서버 B는 상기 구해진 g^x와 b를 사용하여 $c = g^{xb}$를 계산한 후, c와 r을 함께 사용하여 sk_B=H(c, g^x, r)를 계산하고, 이어서 H(sk_B, π, t, ID_A)를 생성하여 상기 수신된 M_A와 동일한 지의 여부를 검사한다. 만일, 두 개의 값이 동일하면 가입자 A에 대한 인증은 성공적이어서 인증 서버 B는 가입자 A로부터 송신된 M_A를 받아들인다. 그리고 인증 서버 B는 M_B=H(sk_B, π, t, g^b)를 계산하여 가입자 A에게 보낸다.

⑤ 가입자 A는 인증 서버 B로부터 수신된 M_B와 자신이 계산한 H(sk_B, π, t, g^b)가 동일한 값인 지의 여부를 검사한다. 만일, 두 개의 값이 동일하면 인증 서버 B에 대한 인증은 성공적이어서, 가입자 A는 M_B를 받아들인다. 이와 같이 가입자 A와 인증 서버 B가 M_A와 M_B를 각각 받아들이면, 가입자 A와 인증 서버 B간의 상호 인증이 성공적으로 이루어진 것이다.

도 2는 본 발명의 실시예에 따른 TAKE 프로토콜을 사용한 (공중)무선랜에서의 인증 및 키 교환 흐름도이다.

도 2를 참조하면, (공중)무선랜 등의 액세스 포인트(Access Point)(200)를 통해 가입자(Supplicant 또는 Client)(100)와 인증 서버(Autnentication Server 또는 RADIUS Server)(300)가 연결되어 가입자(100)에 대한 인증이 인증 서버(300)에 의해 수행된다.

여기서, 가입자(100)와 액세스 포인트(200) 사이에서는 확장 가능한 인증 프로토콜(Extensible Authentication Protocol:EAP)이 사용되고, 액세스 포인트(200)와 인증 서버(300) 사이에서는 RADIUS 프로토콜이 사용된다.

또한, 가입자(100)는 대칭키(t), 패스워드(π), 인증 서버(300)의 공개키(g^b) 및 DH(Diffie-Hellman) 도메인 파라메터(p, q, g)를 저장하고 있으며, 인증 서버(300)는 대칭키(t), 패스워드(π), 인증 서버(300)의 공개키(g^b) 및 DH(Diffie-Hellman) 도메인 파라메터(p, q, g)외에 서버 비밀키(b)를 저장하고 있다.

먼저, 가입자(100)가 (공중)무선랜 등의 서비스 접속을 요청하는 경우, 액세스 포인트(200)는 가입자(100)에게 타입 1 (identity)을 가진 EAP 요청(EAP-Request/Identity)을 보낸다(S100).

가입자(100)는 자신의 식별자 ID_A와 인증 서버(300)의 공개키(g^b)를 해쉬한 값인 $H(ID_A, g^b)$를 identity로 하는 EAP 응답(EAP-Response/Identity $H(ID_A, g^b)$)을 액세스 포인트(200)로 전달한다(S110).

다음, 액세스 포인트(200)는 가입자(100)로부터 전달된 identity를 포함하여 인증 서버(300)에 대한 접속 요청(Radius-Access-Request($H(ID_A, g^b)$))을 보낸다(S120).

인증 서버(300)는 액세스 포인트(200)로부터 송신된 $H(ID_A, g^b)$에 기초하여 관련 데이터베이스에서 <ID_A>, <π>, <t> 및 <b>를 검출해 낸 후, 임의의 값 $r \in_R Z_q$을 선택하여 접속 챌린지 값(Radius-Access-Challenge)으로 액세스 포인트(200)에게 보내면(S130), 액세스 포인트(200)는 이 r값을 TAKE 서브타입1(subtype1)으로 하여 EAP 요청(EAP-Request/TAKE subtype1 (r))을 가입자(100)에게 전달한다(S140).

한편, 가입자(100)는 인증 서버(300)에서 보내온 임의의 값 r을 수신하면, π 및 t와 함께 사용하여 해쉬한 값 f=H(r, π, t)를 계산한 후, 이 f를 g^x를 대칭키 암호화하는 비밀 키로 사용하여 $e = E_f\{g^x\}$를 계산한다. 그리고, c, g^x 및 r을 해쉬한 값인 세션 키 sk_A=H(c, g^x, r)를 계산한 후 π, t 및 ID_A를 해쉬한 값인 인증자 M_A=H(sk_A, π, t, ID_A)를 생성하여, e와 M_A를 TAKE 서브타입1에 대한 EAP 응답(EAP-Response/TAKE Subtype1 (e, M_A))을 액세스 포인트(200)로 보내고(S150), 액세스 포인트(200)는 가입자(100)로부터 전달된 (e, M_A)을 포함하는 접속 요청(Radius-Access-Request (e, M_A))을 인증 서버(300)로 보낸다(S160).

다음, 인증 서버(300)는 가입자(100)로부터 송신된 e와 M_A를 받아서 r, π 및 t를 사용하여 해쉬하여 f=H(r, π, t)를 계산하고, 수신된 e를 상기 계산된 비밀키 f로 복호화하여 $g^x = D_f\{e\}$를 구한다. 그 후, 인증 서버(300)는 상기 구해진 g^x와 b를 사용하여 $c = g^{xb}$를 계산한 후, c와 r을 함께 사용하여 sk_B=H(c, g^x, r)를 계산하고, 이어서 H(sk_B, π, t, ID_A)를 생성하여 상기 수신된 M_A와 동일한 지의 여부를 검사한다. 만일, 두 개의 값이 동일하면 가입자(100)에 대한 인증은 성공적이어서 인증 서버(300)는 가입자(100)로부터 송신된 M_A를 받아들인다. 그리고 인증 서버(300)는 M_B=H(sk_B, π, t, g^b)를 계산하여 접속 챌린지 메시지(Radius-Access-Challenge (M_B))로 액세스 포인트(200)에게 보낸다(S170).

액세스 포인트(200)는 인증 서버(300)로부터 보내온 M_B를 TAKE 서브타입2(subtype2)로 하여 EAP 요청(EAP-Request/TAKE subtype2 (M_B))을 가입자(100)에게 전달한다(S180).

다음, 가입자(100)는 인증 서버(300)에서 보내온 M_B를 수신하여 자신이 계산한 H(sk_B, π, t, g^b)와 동일한 값인 지의 여부를 검사한다. 만일, 두 개의 값이 동일하면 인증 서버(200)에 대한 인증은 성공적이어서, 가입자(100)는 M_B를 받아들인다. 이와 같이 가입자(100)와 인증 서버(300)가 M_A와 M_B를 각각 받아들이면, 가입자(100)와 인증 서버(300)간의 상호 인증이 성공적으로 이루어진 것이다.

다음, 가입자(100)는 확인(acknowledgement)를 의미하는 TAKE 서브타입2에 대한 EAP 응답(EAP-Response/TAKE Subtype2)을 액세스 포인트(200)로 보내고(S190), 액세스 포인트(200)는 가입자(100)로부터 전달된 메시지를 포함하는 접속 요청(Radius-Access-Request)을 인증 서버(300)로 보낸다(S200).

인증 서버(300)는 액세스 포인트(200)를 통해 가입자(100)로부터 보내온 인증 결과가 성공적이면 접속 허용 메시지(Radius-Access-Accept)를 액세스 포인트(200)로 보내면(S210), 액세스 포인트(200)는 이 결과에 따라 EAP 성공 메시지(EAP-Success)를 가입자(100)에게 보낸 후(S220), 인증 서버(300)로부터 접속 허용이 되었다는 것을 알리기 위해 EAPOL-Key 메시지를 가입자(100)에게 보낸다(S230).

여기서, 가입자(100)와 액세스 포인트(200) 사이에 전달되는 메시지 또는 패킷들에는 LAN 프로토콜을 통한 EAP 캡슐화(EAP encapsulation over LAN protocol:EAPOL)가 사용된다.

상기한 바와 같이, 본 발명의 실시예에 따른 TAKE 프로토콜을 이용한 인증 방법이 강력한 인증을 위해 요구되는 기술적 사항을 만족하는 지에 대해 설명한다. 즉 본 발명의 실시예에 따른 TAKE 프로토콜을 이용한 인증 방법에 대한 안전성 분석은 다음과 같다.

① 신원 보호(identity protection) : 가입자는 ID 요청을 받으면 자신의 ID_A 대신에 $H(ID_A, g^b)$를 전송하여 도청자와 같은 수동적 공격자(passive attacker)들이 가입자의 신원을 알 수 없게 한다. 단, 인증 서버는 가입자의 익명과 실제 신원을 매칭시킬 수 있어야 한다.

② 강력한 상호 인증 : 가입자는 패스워드(π)와 비밀키(t), 그리고 인증 서버의 공개키(g^b)를 알아야 인증자 M_A를 유도할 수 있어 가입자 인증을 받을 수 있다. 한편, 인증 서버는 패스워드(π)와 비밀키(t), 가입자 식별자(ID_A) 그리고 서버의 비밀키(b)를 알아야 M_B를 유도할 수 있어 네트워크 인증을 받을 수 있다. 따라서 강력한 상호 인증을 제공하게 된다.

③ 세션 키 설정 : 가입자와 인증 서버 사이에서 데이터 보호를 위해 세션 키(sk_A, sk_B)가 생성된다. 생성된 세션키는 랜덤성과 신규성(freshness)을 제공하는데 이것은 각 개체의 동적인(dynamic) 임의의 수 x와 r의 선택에 기인한다.

④ Forward Secrecy(FS) : 가입자가 소지한 비밀 정보 <ID_A>, <π>, <t>, <g^b>가 공격자에게 모두 노출되었을 경우 공격자는 e 암호문을 복호하여 g^x를 알 수는 있겠지만, $c = g^{xb}$값은 DLP(Discrete Logarithm Problem)에 의해 계산하기 어렵다. 또한, 서버의 비밀 키 <b>가 노출되는 경우에는 $c = g^{xb}$값을 계산하기 위해서 g^x를 알아야 하고, g^x를 알기 위해서는 <π> 및 <t>를 알아야 한다. 즉, 공격자는 <b>, <π>, <t>를 모두 알아야만 세션 키를 계산할 수 있다. 그러나 실제로 (공중)무선랜 환경에서는 서비스를 제공하는 기업들이 큰 기업으로 자체의 강력한 보안 체제를 가지고 있을 것이기 때문에 보안 관련 중요한 비밀 정보가 공격자에게 누설될 가능성은 아주 낮을 것으로 생각된다. 따라서 TAKE 프로토콜은 (공중)무선랜에서는 일반적인 half FS라기보다는 실용적인(practical) half FS라고 말할 수 있다.

⑤ 오프라인 사전(offline dictionary) 공격 : 공격자들은 성공적인 인증에 필요한 비밀정보들을 얻기 위하여 오프라인 사전 공격을 시도할 수 있다. 엔트로피가 적은 패스워드는 이러한 공격에 취약할 수 있으나, TAKE에서는 토큰에 저장된 엔트로피가 높은 비밀키와 패스워드가 임의의 값 g^x를 암호화하는 키로 함께 사용되므로 이러한 공격은 사실상 불가능하다. 즉, 공격자는 패스워드와 비밀키 그리고 임의의 값 g^x까지 추측하여야 한다.

⑥ Man-in-The-Middle(MitM) 공격에 대한 안전성 : 공격자들은 가입자와 서버 사이에 위치하여 MitM 공격을 수행할 수 있다. 그러나 TAKE에서는 강력한 이중 요소 인증을 사용하고 있으므로 이러한 공격은 성공하기가 매우 어렵다.

⑦ Replay 공격에 대한 안전성 : Replay 공격은 공격자가 사용된 메시지를 재 전송하여 이전 세션 키를 다시 설정하려는 공격 방법이다. TAKE에서는 가입자와 서버가 매 세션 마다 임의의 수 x와 r을 각각 생성하여 세션 키를 생성하기 때문에 replay 공격에 안전하다.

⑧ 효율성(efficiency)

- 연산 부하의 최소화 : DH(Diffie-Hellman) 프로토콜은 FS를 제공할 수 있기 때문에 인증 및 키 설정(AKE) 프로토콜에서 많이 사용되고 있지만, 지수화(exponentiation) 계산을 요구하여 연산량이 많게 된다. 해쉬 함수 및 대칭키 암호화/복호화에 걸리는 시간은 아주 작기 때문에 연산에 소요되는 시간의 대부분은 지수화(exponentiation)와 역원 계산, 그리고 곱셈에서 주로 소요된다. 특히, PDAs에서는 연산량이 많아지면 실시간 인증에 걸리는 시간이 많이 소요된다. 따라서 TAKE에서는 온라인상에서 가입자 측이 대칭키 암호 1번과 해쉬 5번을 사용하게 하고, 오프라인에서는 사전계산(pecomputation)으로 2번의 지수화 계산을 하도록 설계되었다. 한편, 서버측에서는 지수화 1번, 대칭 키 복호 1번, 그리고 해쉬 4번의 연산량이 필요하다.

- 메시지 교환 횟수의 최소화 : TAKE에서는 4회의 패스(pass)가 있으므로 가입자와 인증 서버 사이에교환하여야 할 메시지의 횟수가 적다.

- 통신 대역폭 사용의 최소화 : 5개의 메시지 중 3개는 해쉬의 출력 비트 수이고, 한 개는 랜덤 넘버의 비트 수이며, 다른 하나는 g^x 암호문 출력 비트 수이다.

⑨ 키 확인(key confirmation) : TAKE에서는 인증자 M_A와 M_B에 세션 키를 포함시켜 키 확인을 수행함으로써 프로토콜에 참여한 합법적인 가입자가 자신의 의도한 인증 서버와 실제로 공통의 비밀 세션 키를 공유하였음을 확인할 수 있다.

⑩ 부인 봉쇄(non repudiation) : TAKE에서 디지털 서명 방식은 사용하지 않았지만 강력한 이중 요소 인증을 사용하므로 기만적인 사용자들이 서비스를 이용하고 이를 부인하는 것을 방지할 수 있다.

상기한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(씨디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다.

이상에서 본 발명의 바람직한 실시예에 대하여 상세하게 설명하였지만 본 발명은 이에 한정되는 것은 아니며, 그 외의 다양한 변경이나 변형이 가능하다.

발명의 효과

본 발명에 따르면, 이중 요소 인증 방식을 사용하여 다른 어떤 EAP 인증 방식보다 더 강력한 개체 인증을 제공한다.

또한, 공중 무선랜에서 PDAs에 적용할 수 있을 정도로 보안성과 효율성을 가진다.

(57) 청구의 범위

청구항 1.

유무선 통신을 통해 인증 서버에 접속된 가입자 단말기에서 상호 인증을 위한 키를 교환하는 방법에 있어서,

a) 상기 가입자 단말기가 자신의 식별자와 상기 인증 서버의 공개키를 사용하여 생성된 키를 상기 인증 서버로 송신하는 단계;

b) 상기 가입자 단말기가 상기 인증 서버에서 생성된 난수를 수신하는 단계;

c) 상기 수신된 난수와 상기 가입자 단말기에 미리 설정되어 있는 패스워드 및 토큰을 사용하여 제1 특정 값을 암호화한 값과 생성된 가입자측 인증자를 상기 인증 서버로 송신하는 단계;

d) 상기 가입자 단말기가, 상기 송신된 가입자측 인증자에 대한 상기 인증 서버에서의 인증 성공에 따라 상기 인증 서버에서 생성된 인증 서버측 인증자를 수신하는 단계; 및

e) 상기 가입자 단말기가 상기 제 1 특정값과 패스워드를 사용하여 상기 수신된 인증 서버측 인증자에 대한 인증을 수행하고, 상기 인증이 성공되는 경우 상기 인증 서버측 인증자를 받아들이는 단계

를 포함하는 이중 요소 인증된 키 교환 방법.

청구항 2.

제1항에 있어서,

상기 a) 단계 전에,

상기 가입자 단말기가 등록 과정에서 대칭키 알고리즘에 사용되는 상기 대칭키와 상기 패스워드를 결정하여 상기 인증 서버와 공유하는 단계; 및

상기 가입자 단말기가 상기 인증 서버와 인증을 위한 키 교환을 수행하지 않는 때에 난수를 생성하여 상기 제1 특정 값을 사전 계산하는 단계

를 더 포함하는 이중 요소 인증된 키 교환 방법.

청구항 3.

제1항에 있어서,

상기 가입자 단말기는 상기 패스워드 및 상기 인증 서버의 공개키를 토큰에 저장하는 것을 특징으로 하는 이중 요소 인증된 키 교환 방법.

청구항 4.

제1항에 있어서,

상기 a) 단계에서,

상기 생성되는 키는 상기 가입자 단말기의 식별자와 상기 인증 서버의 공개키에 대해 일방향 해쉬 함수를 사용하여 생성되는 것을 특징으로 하는 이중 요소 인증된 키 교환 방법.

청구항 5.

제1항에 있어서,

상기 c) 단계는,

상기 수신된 난수, 상기 패스워드 및 상기 토큰에 저장된 키에 대해 해쉬 함수를 사용하여 제2 특정 값을 생성하는 단계;

상기 생성된 제2 특정 값을 사용하여 상기 제1 특정 값을 암호화하는 단계;

상기 난수와 상기 제1 특정 값을 사용하여 상기 가입자측 세션키를 생성하는 단계;

상기 생성된 세션키, 상기 패스워드, 상기 토큰에 저장된 키 및 상기 가입자 단말기의 식별자에 대해 해쉬 함수를 사용하여 상기 가입자측 인증자를 생성하는 단계; 및

상기 제1 특정 값을 암호화한 값과 상기 가입자측 인증자를 상기 인증 서버로 송신하는 단계

를 포함하는 이중 요소 인증된 키 교환 방법.

청구항 6.

제5항에 있어서,

상기 e) 단계는,

상기 가입자측 세션키, 상기 패스워드, 상기 토큰에 저장된 키 및 상기 인증 서버의 공개키에 대해 해쉬 함수를 사용하여 제3 특정 값을 생성하는 단계;

상기 생성된 제3 특정 값과 상기 인증 서버로부터 수신된 인증 서버측 인증자가 동일한 지의 여부를 판단하는 단계; 및

상기 생성된 제3 특정 값과 상기 인증 서버로부터 수신된 인증 서버측 인증자가 동일한 경우, 상기 가입자 단말기와 상기 인증 서버간의 인증이 성공된 것으로 판단하여 상기 인증 서버측 인증자를 받아들이는 단계

를 포함하는 이중 요소 인증된 키 교환 방법.

청구항 7.

유무선 통신을 통해 가입자 단말기에 접속된 인증 서버에서 상호 인증을 위한 키를 교환하는 방법에 있어서,

a) 상기 인증 서버가 상기 가입자 단말기에서 식별자와 상기 인증 서버의 공개키를 사용하여 생성된 키를 수신하는 단계;

b) 상기 인증 서버가 상기 가입자 단말기로부터 수신된 값을 사용하여 상기 가입자 관련 패스워드 및 토큰에 저장된 키와 상기 인증 서버의 공개키를 검출하고, 난수를 생성하여 상기 가입자 단말기로 송신하는 단계;

c) 상기 인증 서버가, 상기 송신된 난수에 기초하여 상기 가입자 단말기에서 생성된 암호화 값과 가입자측 인증자를 수신하는 단계;

d) 상기 인증 서버가 상기 패스워드, 상기 토큰에 저장된 키 및 상기 난수를 사용하여 생성한 제1 특정 값을 비밀 키로 하여 상기 c) 단계에서 수신된 암호화 값을 복호하여 제2 특정 값을 생성하고, 상기 생성된 제2 특정 값에 기초하여 상기 수신된 가입자측 인증자에 대한 인증을 수행하고, 상기 인증이 성공되는 경우 상기 가입자측 인증자를 받아들이는 단계; 및

e) 상기 인증 서버가 상기 상기 패스워드, 토큰에 저장된 키 및 공개키를 사용하여 생성된 인증 서버측 인증자를 상기 가입자 단말기로 송신하는 단계

를 포함하는 이중 요소 인증된 키 교환 방법.

청구항 8.

제7항에 있어서,

상기 a) 단계 전에,

상기 인증 서버가 등록 과정에서 대칭키 암호 알고리즘에 사용되는 상기 대칭키와 상기 패스워드를 결정하여 상기 가입자 단말기와 공유하는 단계

를 더 포함하는 이중 요소 인증된 키 교환 방법.

청구항 9.

제7항에 있어서,

상기 인증 서버는 상기 토큰에 저장된 키, 상기 패스워드 및 상기 인증 서버의 비밀키를 보안 파일 관련 데이터베이스 내에 저장하는 것을 특징으로 하는 이중 요소 인증된 키 교환 방법.

청구항 10.

제7항에 있어서,

상기 d) 단계는,

상기 패스워드, 상기 토큰에 저장된 키 및 상기 난수에 대해 해쉬 함수를 사용하여 상기 제1 특정 값을 생성하는 단계;

상기 생성된 제1 특정 값을 비밀키로 하여 상기 수신된 암호화 값을 복호하여 상기 제2 특정 값을 생성하는 단계;

상기 생성된 제2 특정 값, 상기 인증 서버의 공개키 및 상기 난수를 사용하여 상기 인증 서버측 세션키를 생성하는 단계;

상기 생성된 세션키, 상기 패스워드, 상기 토큰에 저장된 키 및 상기 가입자 단말기의 식별자에 대해 해쉬 함수를 사용하여 구해진 값과 상기 수신된 가입자측 인증자가 동일한 지의 여부를 판단하는 단계; 및

상기 구해진 값과 상기 수신된 가입자측 인증자가 동일한 경우, 상기 가입자에 대한 인증이 성공된 것으로 판단하여 상기 가입자측 인증자를 받아들이는 단계

를 포함하는 이중 요소 인증된 키 교환 방법.

청구항 11.

제10항에 있어서,

상기 e) 단계에서 상기 인증 서버측 인증자 생성에 상기 생성된 인증 서버측 세션키가 사용되는 것을 특징으로 하는 이중 요소 인증된 키 교환 방법.

청구항 12.

제1항에 있어서,

상기 a) 단계에서, 상기 가입자 단말기의 식별자가 글로벌 로밍과 과금을 지원하기 위해 NAI(Network Access ID) 형식을 사용하는 경우, 상기 가입자 단말기가 사용자 이름 부분과 상기 인증 서버의 공개키를 해쉬한 값과 영역 이름 부분을 함께 상기 인증 서버로 송신하는 것을 특징으로 하는 이중 요소 인증된 키 교환 방법.

청구항 13.

액세스 포인트(Access Point)를 통해 가입자 단말기와 인증 서버가 접속된 무선 통신 시스템에서 상기 가입자 단말기와 상기 인증 서버간에 이중 요소 인증된 키 교환을 통하여 상호 인증하는 방법에 있어서,

a) 상기 가입자 단말기가 상기 액세스 포인트로부터 식별자 요청을 받는 단계;

b) 상기 가입자 단말기가 자신의 식별자와 상기 인증 서버의 공개키를 사용하여 생성된 키를 상기 액세스 포인트를 통해 상기 인증 서버로 송신하는 단계;

c) 상기 인증 서버가 상기 가입자 단말기로부터 수신된 키를 사용하여 상기 가입자 관련 패스워드 및 비밀키와 상기 인증 서버의 공개키를 검출하고, 난수를 생성하여 상기 액세스 포인트를 통해 상기 가입자 단말기로 송신하는 단계;

d) 상기 가입자 단말기가 상기 수신된 난수와 상기 패스워드 및 토큰에 저장된 키를 사용하여 제1 특정 값을 암호화한 값과 생성된 가입자측 인증자를 상기 액세스 포인트를 통해 상기 인증 서버로 송신하는 단계;

e) 상기 인증 서버가 상기 패스워드, 상기 토큰에 저장된 키 및 상기 난수를 사용하여 생성한 제2 특정 값을 비밀 키로 하여 상기 d) 단계에서 수신된 암호화 값을 복호하고, 상기 복호된 값에 기초하여 상기 수신된 가입자측 인증자에 대한 인증을 수행하고, 상기 인증이 성공되는 경우, 상기 상기 패스워드, 토큰에 저장된 키 및 공개키를 사용하여 생성된 인증 서버측 인증자를 상기 액세스 포인트를 통해 상기 가입자 단말기로 송신하는 단계;

f) 상기 가입자 단말기가 상기 토큰에 저장된 키와 패스워드를 사용하여 상기 수신된 인증 서버측 인증자에 대한 인증을 수행하고, 그 인증 결과를 상기 액세스 포인트를 통해 상기 인증 서버로 송신하는 단계; 및

g) 상기 인증 서버가 상기 가입자 단말기로부터 송신된 인증 결과가 성공으로 나타난 경우 상기 가입자에 대한 접속 허가를 상기 액세스 포인트를 통해 상기 가입자 단말기로 송신하는 단계

를 포함하는 이중 요소 인증된 키 교환을 통한 인증 방법.

청구항 14.

제13항에 있어서,

상기 가입자 단말기와 상기 액세스 포인트 사이에서는 확장 가능한 인증 프로토콜(Extensible Authentication Protocol:EAP)이 사용되고,

상기 액세스 포인트와 상기 인증 서버 사이에서는 RADIUS 프로토콜이 사용되는

것을 특징으로 하는 이중 요소 인증된 키 교환을 통한 인증 방법.

청구항 15.

유무선 통신을 통해 인증 서버에 접속된 가입자 단말기에서 상호 인증을 위한 키를 교환하는 프로그램이 저장된 기록 매체에 있어서,

a) 상기 가입자 단말기가 자신의 식별자와 상기 인증 서버의 공개키를 사용하여 생성된 키를 상기 인증 서버로 송신하는 기능;

b) 상기 가입자 단말기가 상기 인증 서버에서 생성된 난수를 수신하는 기능;

c) 상기 수신된 난수와 상기 가입자 단말기에 미리 설정되어 있는 패스워드 및 키를 사용하여 제1 특정 값을 암호화한 값과 생성된 가입자측 인증자를 상기 인증 서버로 송신하는 기능;

d) 상기 가입자 단말기가, 상기 송신된 가입자측 인증자에 대한 상기 인증 서버에서의 인증 성공에 따라 상기 인증 서버에서 생성된 인증 서버측 인증자를 수신하는 기능; 및

e) 상기 가입자 단말기가 상기 토큰에 저장된 키와 패스워드를 사용하여 상기 수신된 인증 서버측 인증자에 대한 인증을 수행하고, 상기 인증이 성공되는 경우 상기 인증 서버측 인증자를 받아들이는 기능

을 구현하는 프로그램을 저장한 기록매체.

청구항 16.

유무선 통신을 통해 가입자 단말기에 접속된 인증 서버에서 상호 인증을 위한 키를 교환하는 프로그램이 기록된 기록 매체에 있어서,

a) 상기 인증 서버가 상기 가입자 단말기에서 식별자와 상기 인증 서버의 공개키를 사용하여 생성된 값을 수신하는 기능;

b) 상기 인증 서버가 상기 가입자 단말기로부터 수신된 값을 사용하여 상기 가입자 관련 패스워드 및 토큰에 저장된 키와 상기 인증 서버의 공개키를 검출하고, 난수를 생성하여 상기 가입자 단말기로 송신하는 기능;

c) 상기 인증 서버가, 상기 송신된 난수에 기초하여 상기 가입자 단말기에서 생성된 암호화 값과 가입자측 인증자를 수신하는 기능;

d) 상기 인증 서버가 상기 패스워드, 상기 토큰에 저장된 키 및 상기 난수를 사용하여 생성한 제1 특정 값을 비밀 키로 하여 상기 c) 단계에서 수신된 암호화 값을 복호하여 제2 특정 값을 생성하고, 상기 생성된 제2 특정 값에 기초하여 상기 수신된 가입자측 인증자에 대한 인증을 수행하고, 상기 인증이 성공되는 경우 상기 가입자측 인증자를 받아들이는 기능; 및

e) 상기 인증 서버가 상기 상기 패스워드, 토큰에 저장된 및 공개키를 사용하여 생성된 인증 서버측 인증자를 상기 가입자 단말기로 송신하는 기능

을 구현하는 프로그램을 저장한 기록매체.

청구항 17.

제 1 항 내지 제 12 항중 어느 하나의 항에 있어서,

상기 토큰에 저장된 키는 대칭 키(symetric key)인것을 특징으로 하는 이중 요소 인증된 키 교환 방법.

청구항 18.

제 13 항 또는 제 14 항에 있어서,

상기 토큰에 저장된 키는 대칭 키(symetric key)인것을 특징으로 하는 이중 요소 인증된 키 교환 방법.

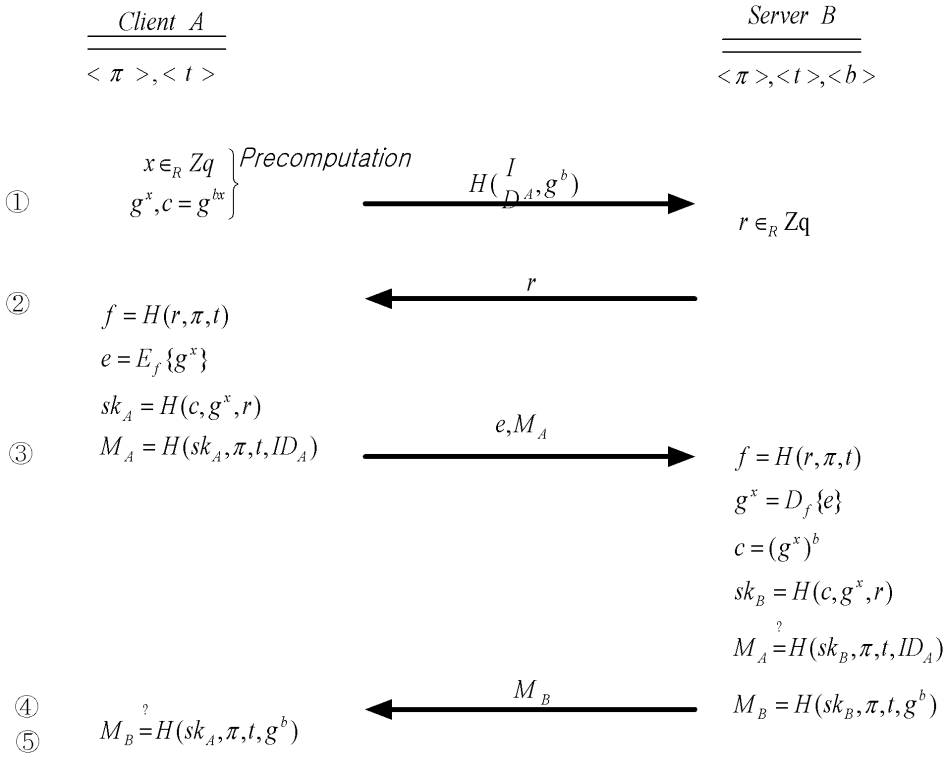
청구항 19.

제 15 항 또는 제 16 항에 있어서,

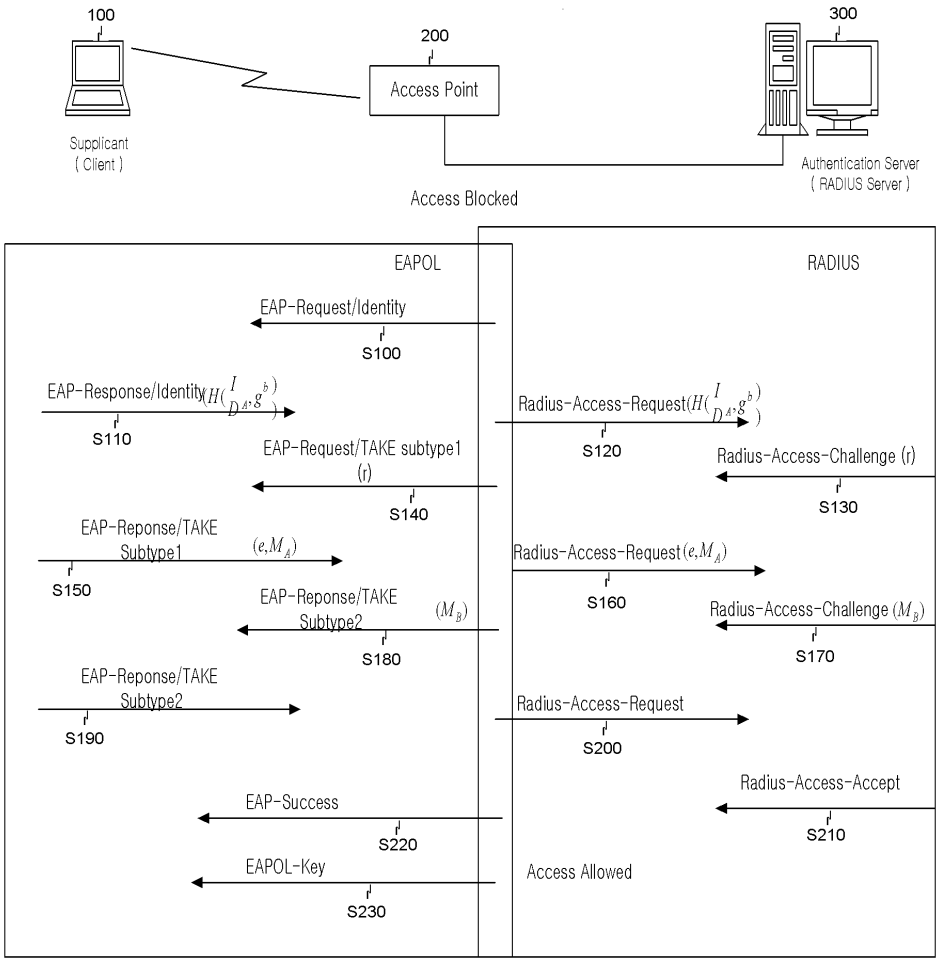
상기 토큰에 저장된 키는 대칭 키(symetric key)인것을 특징으로 하는 이중 요소 인증된 기록 매체.

도면

도면1


Client A
Server B
Precomputation
①
②
③
④
⑤
r
e, M_A
M_B

도면2


100
Supplicant
(Client)
200
Access Point
300
Authentication Server
(RADIUS Server)
Access Blocked
EAPOL
RADIUS
EAP-Request/Identity
S100
EAP-Response/Identity
S110
Radius-Access-Request
S120
Radius-Access-Challenge (r)
S130
EAP-Request/TAKE subtype1
(r)
S140
EAP-Reponse/TAKE
Subtype1
S150
Radius-Access-Request
S160
Radius-Access-Challenge
S170
EAP-Reponse/TAKE
Subtype2
S180
EAP-Reponse/TAKE
Subtype2
S190
Radius-Access-Request
S200
Radius-Access-Accept
S210
EAP-Success
S220
EAPOL-Key
S230
Access Allowed