(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
H04L 9/32

(11) 공개번호 10-2004-0050625
(43) 공개일자 2004년06월16일

(21) 출원번호 10-2002-0078486
(22) 출원일자 2002년12월10일

(71) 출원인 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 양대헌
대전광역시 서구 만년동 상아아파트 107동 1007호

정병호
대전광역시 서구 월평3동 진달래아파트 110동 105호

(74) 대리인 특허법인씨엔에스

심사청구 : 있음

(54) 대칭형 및 비대칭형 인증 키 교환을 이용한 인증방법

요약

본 발명은 오프라인 사전 공격에 대해 수학적인 안전성 증명을 가지며, 대칭형 인증 및 키교환 프로토콜에서 비대칭형 프로토콜로 체계적인 변환이 가능하며, 계산량 및 통신량의 증가가 크지 않은 사용자 인증방법에 관한 것으로,

사용자 컴퓨터와 인증 서버를 포함하는 통신망에서의 사용자 인증방법에 있어서, 인증에 필요한 각종 시스템 파라미터를 설정하는 제 1 단계; 상기 설정된 파라미터에 의거하여 사용자가 임의로 랜덤 수(r)를 선택하여, 사용자 ID, 상기 랜덤 수 r에 일방향 함수를 적용해서 얻은 시험수(A=Γ(r))로 이루어진 메시지를 상기 인증 서버로 전송하는 제 2 단계; 상기 제 2 단계 수행 후, 상기 사용자 컴퓨터와 상기 인증서버간에 대칭형 인증 및 키 교환을 수행하여 상기 인증 서버를 인증하고 임시 세션키 tsk를 상기 인증 서버와 상기 사용자 컴퓨터가 공유하는 제 3 단계; 상기 제3 단계 수행 후, 상기 인증 서버가 랜덤수 t를 생성해 사용자 컴퓨터로 전송하는 제 4 단계; 상기 사용자 컴퓨터가 상기 랜덤수 t와 상기 임시 세션키 tsk를 이용하여 질문수 c를 생성하고, 상기 질문수 c를 이용해 목격자 수 B를 계산한 다음, 상기 목격자수 B를 상기 인증 서버로 전송하는 제 5 단계; 상기 인증서버가 목격자 수 B를 자신이 가지고 있는 상기 임시 세션키 tsk, 상기 시험수 A, 키 확인자 KV 등을 이용해 검증하는 제 6 단계; 및 상기 제 6 단계에서 검증이 성공하면 상기 인증 서버와 상기 사용자 컴퓨터가 각각 세션키 sk를 계산하는 제 7 단계를 포함한다.

대표도

도 1

색인어

인증, 대화형, 증명, 패스워드, 사용자, 키 교환, 대칭형, 비대칭형

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 대칭형 및 비대칭형 인증 키 교환을 이용한 인증과정을 설명하기 위한 도면.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 통신망에서 사용자 인증방법에 관한 것으로, 더욱 자세하게는 종래의 대칭형 인증 및 키 교환 방식을 이용해 비대칭형 인증 및 키 교환 방식으로 사용자 인증을 수행함으로써, 보다 안정성을 향상시킨 인증방법에 관한 것이다.

대칭형 인증 및 키 교환 프로토콜은 인증 서버에 사용자의 비밀키를 보관하므로써, 상대적으로 효율적인 인증 및 키 교환을 가능하게 하지만, 인증 서버가 해킹당하는 경우 사용자의 비밀키가 그대로 드러나는 문제점을 가진다. 이를 해결하기 위해 인증 서버에는 사용자의 비밀키에 일방향 함수를 적용한 결과만을 보관해 서 인증 및 키 교환을 수행하는 비대칭형 모델 개념이 제시되었다. 하지만, 비대칭형 모델은 설계의 어려움, 수학적 안전성 증명의 부재, 많은 계산량 및 통신량 요구 등의 문제로 널리 사용되고 있지 못하다.

현재 사용되고 있는 인증 및 키교환 프로토콜은 Tom Wu의 SRP, David Jablon의 B-SPEKE, Belloving 등의 EKE 등이 있다. 하지만 이들 프로토콜은 그 안전성이 수학적으로 증명되지 않았다. 최근에는 대칭형 모델인 EKE(encrypted key exchange)의 일부분에 대해 안전성이 증명되었으며, 수학적인 안전성 증명을 갖는 프로토콜들이 제안되었으나 대부분 adhoc 설계에 의존하고 있다.

발명이 이루고자 하는 기술적 과제

따라서, 상기와 같은 종래 기술의 문제점을 해결하기 위해서, 본 발명은 오프라인 사전 공격에 대해 수학적인 안전성 증명을 가지며, 대칭형 인증 및 키교환 프로토콜에서 비대칭형 프로토콜로 체계적인 변환이 가능하며, 계산량 및 통신량의 증가가 크지 않은 사용자 인증방법을 제공하는데 그 목적이 있다.

발명의 구성 및 작용

상기 목적을 달성하기 위한 본 발명은, 사용자 컴퓨터와 인증 서버를 포함하는 통신망에서의 사용자 인증방법에 있어서, 인증에 필요한 각종 시스템 파라미터를 설정하는 제 1 단계; 상기 설정된 파라미터에 의거하여 사용자가 임의로 랜덤 수(r)를 선택하여, 사용자 ID, 상기 랜덤 수 r에 일방향 함수를 적용해서 얻은 시 험수(A=Γ(r))로 이루어진 메시지를 상기 인증 서버로 전송하는 제 2 단계; 상기 제 2 단계 수행 후, 상기 사용자 컴퓨터와 상기 인증서버간에 대칭형 인증 및 키 교환을 수행하여 상기 인증 서버를 인증하고 임시 세션키 tsk를 상기 인증 서버와 상기 사용자 컴퓨터가 공유하는 제 3 단계; 상기 제3 단계 수행 후, 상기 인증 서버가 랜덤수 t를 생성해 사용자 컴퓨터로 전송하는 제 4 단계; 상기 사용자 컴퓨터가 상기 랜덤수 t와 상기 임시 세션키 tsk를 이용하여 질문수 c를 생성하고, 상기 질문수 c를 이용해 목격자 수 B를 계산한 다음, 상기 목격자수 B를 상기 인증 서버로 전송하는 제 5 단계; 상기 인증서버가 목격자 수 B를 자신이 가지고 있는 상기 임시 세션키 tsk, 상기 시험수 A, 키 확인자 KV 등을 이용해 검증하는 제 6 단계; 및 상기 제 6 단계에서 검증이 성공하면 상기 인증 서버와 상기 사용자 컴퓨터가 각각 세션키 sk를 계산하는 제 7 단계를 포함한다.

또한, 본 발명은, 컴퓨터에서, 인증에 필요한 각종 시스템 파라미터를 설정하는 제 1 단계; 상기 설정된 파라미터에 의거하여 사용자가 임의로 랜덤 수(r)를 선택하여, 사용자 ID, 상기 랜덤 수 r에 일방향 함수를 적용해서 얻은 시험수(A=Γ(r))로 이루어진 메시지를 인증 서버로 전송하는 제 2 단계; 상기 제 2 단계 수행 후, 사용자 컴퓨터와 상기 인증서버간에 대칭형 인증 및 키 교환을 수행하여 상기 인증 서버를 인증하고 임시 세션키 tsk를 상기 인증 서버와 상기 사용자 컴퓨터가 공유하는 제 3 단계; 상기 제3 단계 수행 후, 상기 인증 서버가 랜덤수 t를 생성해 상기 사용자 컴퓨터로 전송하는 제 4 단계; 상기 사용자 컴퓨터가 상기 랜덤수 t와 상기 임시 세션키 tsk를 이용하여 질문수 c를 생성하고, 상기 질문수 c 를 이용해 목격자 수 B를 계산한 다음, 상기 목격자수 B를 상기 인증 서버로 전송하는 제 5 단계; 상기 인증서버가 목격자 수 B를 자신이 가지고 있는 상기 임시 세션키 tsk, 상기 시험수 A, 키 확인자 KV 등을 이용해 검증하는 제 6 단계; 및 상기 제 6 단계에서 검증이 성공하면 상기 인증 서버와 상기 사용자 컴퓨터가 각각 세션키 sk를 계산하는 제 7 단계를 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

대칭형 인증 및 키 교환 프로토콜은 서버가 사용자에게 공유 비밀키 x를 이용해서 인증을 받고, 세션키 tsk를 공유하는 프로토콜을 의미한다. 본 발명에서는 대칭형 인증 및 키 교환 프로토콜의 일반적인 사용법과는 다르게 사용자가 서버를 인증하는데 사용한다. 즉, 비밀키 x 대신 키 확인자(KV: Key Verifier)를 사용해 서버가 키 확인자를 가지고 있는지 확인하며, 이를 이용해 세션키 tsk를 생성하는데 사용한다. 키 확인자(KV)는 사용자가 가지고 있는 비밀키 pw에 앞으로 사용될 영지식 증명 프로토콜에 의존적인 일방향 함수를 적용한 값을 의미한다. 따라서, 인증 서버가 해킹 당하더라도 일방향 함수에 의해 비밀키 pw는 보호된다. 본 발명에서 사용되는 영지식 증명은 랜덤수에서 시험수를 만드는 함수 Γ(r), 목격자수가 유효한지 확인하는 함수 Λ(B, KV, c), 목격자 수를 만드는 함수 δ(c, r, pw)로 정의된다. [G, Γ(r), δ(c, r, pw), Λ(B, KV, c)]의 예로서, 영지식증명 프로토콜로서 Schnorr 프로토콜을 사용한다면 [Fp = <g>, $g^r \bmod p$, $r+pw*c \bmod q$, $g^B KV^c \bmod p$], Guillous-Quisquater의 프로토콜을 사용한다면 [Z_n^* , $r^e \bmod n$, $r*pw^c \bmod n$, $B^e KV^c \bmod n$]가 있다. 여기서 p, q, g, Fp 는 Schnorr 프로토콜을, n, Z_n^* 는 Guillous-Quisquater 프로토콜을 참조하면 알 수 있다.

본 발명에 따른 인증방법은, 먼저, 인증에 필요한 각종 시스템 파라미터를 설정한다. 그 후, 그 설정된 파라미터에 의거하여 사용자가 임의로 랜덤 수(r)를 선택하여, 사용자 ID(IDuser), 일방향 함수(Γ)를 적용해서 얻은 시험수(A=Γ(r))로 이루어진 메시지를 서버에게 보낸다. 또한, 사용자는 키 확인자(KV=Γ(pw))를 키로하는 대칭형 인증 및 키 교환 프로토콜을 수행한다. 상기 대칭형 인증 및 키 교환 프로토콜 수행의 결과로 사용자는 인증 서버가 키 확인자(KV)를 알고 있는지를 확인할 수 있으며, 프로토콜이 성공적으로 종료되는 경우 세션키(tsk)를 공유하게 된다. 만약 대칭형 인증 및 키 교환 프로토콜의 수행 결과가 실패한다면 인증세션을 종료한다. 대칭형 인증 및 키 교환 프로토콜가 성공적으로 수행되면 인증 서버는 사용자에게 임의로 선택된 랜덤수(t)를 전송한다. 이 랜덤수는 영지식 증명 프로토콜에서 사용될 질문수를 만드는데 세션키(tsk)와 함께 사용된다. 사용자는 질문수(c=H(t || tsk), H()는 충돌 회피성(collision-freeness)을 갖는 해쉬함수)를 계산하고, 질문수 c를 이용해서 목격자 수를 계산하고, 이를 인증 서버에 전송한다. 인증 서버는 목격자수와 세션키(tsk), 랜덤수(t), 키 확인자(KV), Λ 등을 이용해 사용자를 인증한다. 인증이 성공적이라면 세션키(sk)는 tsk와 주고 받은 메시지의 일부를 이용하여 생성된다.

이하, 도1을 참조하여 본 발명에 따른 인증 방법을 상세히 설명한다.

먼저, 사용자와 인증 서버가 프로토콜을 수행하기 전에 시스템 파라미터를 미리 설정해 둔다. 시스템 파라미터는 사용자와 인증 서버간의 약속으로, 시스템 전체를 통해 사용자들이 공유하게 된다. G는 multiplicative group Z_p^* 나 타원 곡선그룹 등의 유한 순환 그룹이다. Γ()는 일방향 함수(oneway function)로서, 본 발명의 실시 예로서는, RSA(Rivest, Shamir, Adleman) 문제에 기초한 일방향 함수, 이산 대수 문제에 기초한 일방향 함수 또는 소인수 분해 문제에 기초한 일방향 함수 등이 될 수 있다. H()는 sha-1, md5 등의 해쉬함수이고, ||는 연결(concatenation)을 의미한다. 대칭형 인증 및 키 교환 프로토콜에서 사용되는 함수로 ψ()와 χ()가 있으며, 각각 메시지 인증 코드(MAC: Message Authentication Code), 세션키 tsk를 생성하는데 사용된다. 또한 X(KV), Y(KV)는 각각 랜덤하게 선택한 X, Y에 KV를 통한 trapdoor oneway함수를 수행한 것을 의미한다.

도 1에서 사용자의 비밀 정보는 패스워드(pw)뿐이고, 인증 서버의 비밀 정보는 각 사용자에 대한 키 확인자 KV=Γ(pw)가 된다.

도 1에서 사용자 컴퓨터는 사용자 ID(ID_{User}), 랜덤수 r을 임의로 선택해서 계산한 시험수 A=Γ(r)를 포함한 메시지를 서버에게 전송한다. 이에 따라, 대칭형 인증 및 키 교환 프로토콜을 이용한 비대칭형 프로토콜을 시작할 수 있게 된다.

메시지 전송 후 사용자 컴퓨터는 공지의 대칭형 인증 및 키 교환 프로토콜을 수행한다. 공지의 대칭형 인증 및 키 교환 프로토콜은 사용자 컴퓨터에서 랜덤하게 선택한 X에 키 확인자 KV를 통한 trapdoor 일방향 함수를 수행한 X*를 서버로 전송하고, 서버에서는 랜덤하게 선택한 Y에 키 확인자 KV를 통한 trapdoor 일방향 함수를 수행한 Y*를 구한 다음, 인증 값(auth*=ψ(KV, X, Y)과 세션 키(tsk = χ(X, Y)를 계산한다. 그런 다음, 서버는 Y* ‖ auth*를 사용자 컴퓨터로 전송한다. 사용자 컴퓨터는 인증값을 비교하여 일치하면, 서버를 인증하게 되고, 서버와 사용자 컴퓨터는 모두 세션키 tsk를 공유하게 된다. 만약 대칭형 인증 및 키 교환 프로토콜을 구행결과 인증이 실패한다면 사용자 컴퓨터는 서버가 키 확인자 KV에 대한 정보를 가지고 있지 않음을 알게 되고 세션을 종료한다.

대칭형 인증 및 키 교환 프로토콜이 성공적으로 종료했을 경우 서버는, 랜덤 수 t를 생성해 사용자 컴퓨터에게 전송한다. 사용자 컴퓨터는 t와 세션 키 tsk를 이용하여 질문수 c(c←H(tsk ‖ A)를 생성하고, 이에 따라 목격자수 B(=δ(c,r, pw) 그리고 세션키 sk(sk←H(tsk ‖ A ‖ B ‖ 2)를 생성해 낸다. 그리고 사용자 컴퓨터는 인증 서버로 목격자수 B를 전송한다. 인증 서버는 전송받은 목격자수 B와 자신이 가지고 있는 정보인 키 확인자 KV, 그리고 질문수 c를 이용해 목격자수 B를 검증한다(A=Λ(B,KV,c). 검증이 성공하면 인증 서버는 사용자를 인증하게 되고 세션키 sk를 계산한다. 검증이 실패하면 인증 서버는 사용자가 pw에 대한 정보를 모르고 있음을 알 수 있으며 세션을 종료한다.

발명의 효과

이상과 같은 본 발명은 다음과 같은 효과를 갖는다.

먼저, 본 발명은 오프라인 사전 공격(Offline dictionary attack)에 수학적인 안전성 증명을 갖는다. 또한, 대칭형 인증 및 키 교환 프로토콜을 비대칭형 프로토콜로 쉽게 변환할 수 있게 된다. 예를 들어, 널리 알려진 Bellovin 등이 발명한 대칭형 프로토콜의 하나인 EKE(Encrypted Key Exchange)를 쉽게 비대칭형 프로토콜로 변환할 수 있다. 또한, 통신망에서 사용되는 사용자 인증 및 키 교환 프로토콜에 응용될 수 있다. 예를 들어, IEEE 802.11i 그룹에서 논의되고 있는 키 교환 및 인증 프로토콜에 본 발명을 응용할 수도 있다. 또한, UNIX의 사용자 인증 과정을 본 발명으로 대체할 수도 있다. 이렇게 본 발명을 실제로 응용하는 것 이외에도, 본 발명에서 제시한 방법을 이용하여 새로운 인증 및 키 교환 프로토콜을 쉽게 설계할 수 있다. 따라서, 사용자가 암호학에 대한 깊은 지식 없이도, 쉽게 안전한 인증 및 키 교환 프로토콜을 설계할 수 있게 된다.

(57) 청구의 범위

청구항 1.

사용자 컴퓨터와 인증 서버를 포함하는 통신망에서의 사용자 인증방법에 있어서,

인증에 필요한 각종 시스템 파라미터를 설정하는 제 1 단계;

상기 설정된 파라미터에 의거하여 사용자가 임의로 랜덤 수(r)를 선택하여, 사용자 ID, 상기 랜덤 수 r에 일방향 함수를 적용해서 얻은 시험수(A=Γ(r))로 이루어진 메시지를 상기 인증 서버로 전송하는 제 2 단계;

상기 제 2 단계 수행 후, 상기 사용자 컴퓨터와 상기 인증서버간에 대칭형 인증 및 키 교환을 수행하여 상기 인증 서버를 인증하고 임시 세션키 tsk를 상기 인증 서버와 상기 사용자 컴퓨터가 공유하는 제 3 단계;

상기 제3 단계 수행 후, 상기 인증 서버가 랜덤수 t를 생성해 사용자 컴퓨터로 전송하는 제 4 단계;

상기 사용자 컴퓨터가 상기 랜덤수 t와 상기 임시 세션키 tsk를 이용하여 질문수 c를 생성하고, 상기 질문수 c를 이용해 목격자 수 B를 계산한 다음, 상기 목격자수 B를 상기 인증 서버로 전송하는 제 5 단계;

상기 인증서버가 목격자 수 B를 자신이 가지고 있는 상기 임시 세션키 tsk, 상기 시험수 A, 키 확인자 KV 등을 이용해 검증하는 제 6 단계; 및

상기 제 6 단계에서 검증이 성공하면 상기 인증 서버와 상기 사용자 컴퓨터가 각각 세션키 sk를 계산하는 제 7 단계를 포함하는 것을 특징으로 하는 사용자 인증방법.

청구항 2.

제 1 항에 있어서,

상기 제1 단계의 시스템 파라미터로는, 랜덤수에서 시험수를 만드는 함수 Γ(r), 목격자수가 유효한지 확인하는 함수 Λ(B, KV, c), 목격자 수를 만드는 함수 δ(c, r, pw)를 포함하고, [G, Γ(r), δ(c, r, pw), Λ(B, KV, c)]의 예로서, 영지식증명 프로토콜로서 Schnorr 프로토콜을 사용한다면 [Fp = <g>, $g^r \bmod p$, $r+pw*c \bmod q$, $g^{BKV^c} \bmod p$], Guillous-Quisquater의 프로토콜을 사용한다면 [Z_n^* , $r^e \bmod n$, $r*pw^c \bmod n$, $B^e KV^c \bmod n$]인 것을 특징으로 하는 사용자 인증방법.

청구항 3.

컴퓨터에서,

인증에 필요한 각종 시스템 파라미터를 설정하는 제 1 단계;

상기 설정된 파라미터에 의거하여 사용자가 임의로 랜덤 수(r)를 선택하여, 사용자 ID, 상기 랜덤 수 r에 일방향 함수를 적용해서 얻은 시험수(A=Γ(r))로 이루어진 메시지를 인증 서버로 전송하는 제 2 단계;

상기 제 2 단계 수행 후, 사용자 컴퓨터와 상기 인증서버간에 대칭형 인증 및 키 교환을 수행하여 상기 인증 서버를 인증하고 임시 세션키 tsk를 상기 인증 서버와 상기 사용자 컴퓨터가 공유하는 제 3 단계;

상기 제3 단계 수행 후, 상기 인증 서버가 랜덤수 t를 생성해 상기 사용자 컴퓨터로 전송하는 제 4 단계;

상기 사용자 컴퓨터가 상기 랜덤수 t와 상기 임시 세션키 tsk를 이용하여 질문수 c를 생성하고, 상기 질문수 c를 이용해 목격자 수 B를 계산한 다음, 상기 목격자수 B를 상기 인증 서버로 전송하는 제 5 단계;

상기 인증서버가 목격자 수 B를 자신이 가지고 있는 상기 임시 세션키 tsk, 상기 시험수 A, 키 확인자 KV 등을 이용해 검증하는 제 6 단계; 및

상기 제 6 단계에서 검증이 성공하면 상기 인증 서버와 상기 사용자 컴퓨터가 각각 세션키 sk를 계산하는 제 7 단계를 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

도면

도면1