



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0057134
(43) 공개일자 2014년05월12일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 9/14 (2006.01)
H04L 9/32 (2006.01)
(21) 출원번호 10-2013-0059249
(22) 출원일자 2013년05월24일
심사청구일자 2013년11월15일
(30) 우선권주장
1020120121951 2012년10월31일 대한민국(KR)

(71) 출원인
삼성에스디에스 주식회사
서울특별시 강남구 테헤란로 318 (역삼동)
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
윤효진
서울특별시 강남구 삼성1동 삼성동 빌딩 8층
권태경
서울 송파구 올림픽로 435, 111동 1601호 (신천동, 파크리오)
(74) 대리인
박국진, 노준태

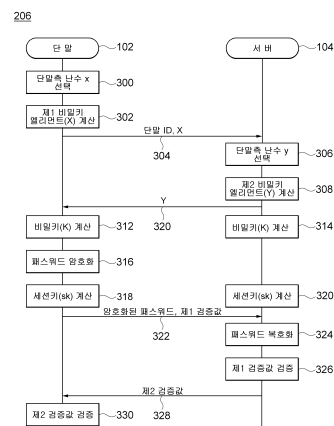
전체 청구항 수 : 총 25 항

(54) 발명의 명칭 **패스워드 기반 인증 방법 및 이를 수행하기 위한 장치**

(57) 요약

패스워드 기반 인증 방법 및 이를 수행하기 위한 장치가 개시된다. 본 발명의 일 실시예에 다른 패스워드 기반 인증 방법은, 단말에서, 상기 단말 사용자의 아이디(ID) 및 서버와 교환한 키 생성 인자를 이용하여 아이디 기반의 비밀키(K)를 생성하는 단계; 상기 단말에서, 생성된 상기 비밀키(K)를 대칭키로 하는 대칭키 암호화 알고리즘을 이용하여 상기 사용자의 패스워드를 암호화하고, 암호화된 상기 패스워드를 상기 서버로 송신함으로써 상기 단말 사용자의 인증을 요청하는 단계; 및 상기 단말에서, 상기 서버로부터 상기 인증 요청에 대한 응답을 수신하는 단계를 포함한다.

대표도 - 도3



특허청구의 범위

청구항 1

단말에서, 상기 단말 사용자의 아이디(ID) 및 서버와 교환한 키 생성 인자를 이용하여 아이디 기반의 비밀키(K)를 생성하는 단계;

상기 단말에서, 생성된 상기 비밀키(K)를 대칭키로 하는 대칭키 암호화 알고리즘을 이용하여 상기 사용자의 패스워드를 암호화하고, 암호화된 상기 패스워드를 상기 서버로 송신함으로써 상기 단말 사용자의 인증을 요청하는 단계; 및

상기 단말에서, 상기 서버로부터 상기 인증 요청에 대한 응답을 수신하는 단계를 포함하는 인증 방법.

청구항 2

청구항 1에 있어서,

상기 비밀키를 생성하는 단계는,

상기 단말에서, 단말측 난수(x)로부터 계산된 제1 비밀키 엘리먼트(X)를 서버로 송신하는 단계; 및

상기 단말에서, 상기 서버로부터 제2 비밀키 엘리먼트(Y)를 수신하는 단계를 포함하며,

상기 단말은, 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)를 이용하여 상기 비밀키(K)를 생성하는, 인증 방법.

청구항 3

청구항 1에 있어서,

상기 단말은, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 이용하여 공통 해시값(e)을 생성하고,

상기 공통 해시값(e), 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 이용하여 상기 비밀키(K)를 생성하는, 인증 방법.

청구항 4

청구항 3에 있어서,

상기 비밀키(K)는 상기 공통 해시값(e), 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 포함하는 제1문자열을 해싱함으로써 생성되는, 인증 방법.

청구항 5

청구항 4에 있어서,

상기 제1 비밀키 엘리먼트(X)는 다음의 수학적식

$$X = g^x$$

$$\tilde{g} \quad g = \tilde{g}^2$$

(이때, g는 유한한 군 $Z_N = \{0, 1, 2, \dots, N-1\}$ 의 최대 순환 부분군의 생성원을 라 할 때, $\tilde{g}$ 으로 생성되는 순환 부분군 G의 생성원, N은 $N=pq$ 를 만족하는 정수, p 및 q는 각각 $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$ 를 만족하

는 소수)

에 의하여 계산되는, 인증 방법.

청구항 6

청구항 5에 있어서,

상기 비밀키(K)는 다음의 수학적식

$$K = h_1(X, (Y, I), (YI^e)^x)$$

(이때, h_1 은 제1 랜덤 해시함수, $I = H(ID)$, H 는 $H: \{0,1\}^* \rightarrow G$ 의 관계를 만족하는 해시함수)

에 의하여 계산되는, 인증 방법.

청구항 7

청구항 6에 있어서,

상기 암호화된 패스워드를 상기 서버로 송신하는 단계의 수행 이후,

상기 단말에서, 상기 공통 해시값(e), 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 포함하는 문자열을 제2 랜덤 해시함수(h_2)로 해싱하여 세션키(sk)를 생성하는 단계;

상기 단말에서, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I), 상기 세션키(sk) 및 상기 패스워드를 포함하는 제2문자열을 제3 랜덤 해시함수(h_3)로 해싱하여 제1검증값을 생성하는 단계; 및

상기 단말에서, 상기 제1검증값을 상기 서버로 송신하는 단계를 더 포함하는, 인증 방법.

청구항 8

청구항 7에 있어서,

상기 세션키(sk)는 다음의 수학적식

$$sk = h_2(X, (Y, I), (YI^e)^x)$$

에 의하여 계산되는, 인증 방법.

청구항 9

청구항 7에 있어서,

상기 단말은, 상기 제1 비밀키 엘리먼트(X)와 함께 상기 아이디를 상기 서버로 송신하거나, 또는 상기 제1검증값과 함께 상기 아이디를 상기 서버로 송신하는, 인증 방법.

청구항 10

청구항 7에 있어서,

상기 제1검증값을 상기 서버로 송신하는 단계의 수행 이후,

상기 단말에서, 상기 서버로부터 제2검증값을 수신하는 단계; 및

상기 단말에서, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I), 상기 세션키(sk), 상기 패스워드 및 제4 랜덤 해시함수(h_4)를 이용하여 상기 제2검증값을 검증하는 단계를 더 포함하는, 인증 방법.

청구항 11

서버에서, 단말 사용자의 아이디(ID) 및 상기 단말과 교환한 키 생성 인자를 이용하여 아이디 기반의 비밀키(K)를 생성하는 단계;

상기 서버에서, 상기 단말로부터 상기 사용자의 암호화된 패스워드를 수신하는 단계; 및

상기 서버에서, 생성된 상기 비밀키(K)를 대칭키로 하는 대칭키 복호화 알고리즘을 이용하여 상기 암호화된 패스워드를 복호화하고, 복호화된 상기 패스워드를 이용하여 상기 단말 사용자를 인증하는 단계를 포함하는 인증 방법.

청구항 12

청구항 11에 있어서,

상기 비밀키를 생성하는 단계는,

상기 서버에서, 키 발급 장치로부터 상기 아이디(ID)에 대응되는 개인키(s_{ID})를 발급받는 단계;

상기 서버에서, 상기 단말로부터 제1 비밀키 엘리먼트(X)를 수신하는 단계; 및

상기 서버에서, 서버측 난수(y)로부터 계산된 제2 비밀키 엘리먼트(Y)를 상기 단말로 송신하는 단계를 더 포함하며,

상기 서버는, 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID) 및 상기 개인키(s_{ID})를 이용하여 상기 비밀키(K)를 생성하는, 인증 방법.

청구항 13

청구항 12에 있어서,

상기 서버는, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 이용하여 공통 해시값(e)을 생성하고,

상기 공통 해시값(e), 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I) 및 상기 개인키(s_{ID})를 이용하여 상기 비밀키(K)를 생성하는, 인증 방법.

청구항 14

청구항 13에 있어서,

상기 비밀키(K)는 상기 공통 해시값(e), 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I) 및 상기 개인키(s_{ID})를 포함하는 제1문자열을 해싱함으로써 생성되는, 인증 방법.

청구항 15

청구항 14에 있어서,

상기 개인키(s_{ID})는 다음의 수학적식

$$s_{ID} = \log_g H(ID) = \sum_{i=1}^{\alpha} s_{IDi}$$

$$\tilde{g} \quad g = \tilde{g}^2$$

(이때, g 는 유한한 군 $Z_N = \{0, 1, 2, \dots, N-1\}$ 의 최대 순환 부분군의 생성원을 $\tilde{g}$ 라 할 때, $\tilde{g}$ 으로 생성되는 순환 부분군 G 의 생성원, N 는 $N = pq$ 의 관계를 만족하는 정수, p 및 q 는 각각 $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$ 를 만족하는 소수, ID_i 는 상기 아이디를 구성하는 i 번째 문자, α 는 상기 아이디의 길이),

$$H(ID) = (h(ID))^2 = \prod_{i=1}^{\alpha} (h(ID_i))^2, \quad s_{IDi} = \log_g H(ID_i)$$

h 는 $h: \{0,1\}^* \rightarrow Z_N$ 의 관계를 만족하는 랜덤해시함수,)

에 의하여 계산되는, 인증 방법.

청구항 16

청구항 15에 있어서,

상기 제2 비밀키 엘리먼트는 다음의 수학적식

$$Y = g^y$$

에 의하여 계산되는, 인증 방법.

청구항 17

청구항 16에 있어서,

상기 비밀키(K)는 다음의 수학적식

$$K = h_1(X, (Y, I), X^{y+sID^*e})$$

(이때, h_1 은 제1 랜덤 해시함수, $I = H(ID)$, H 는 $H: \{0,1\}^* \rightarrow G$ 의 관계를 만족하는 해시함수)

에 의하여 계산되는, 인증 방법.

청구항 18

청구항 17에 있어서,

상기 단말을 인증하는 단계의 수행 이후,

상기 서버에서, 상기 단말로부터 제1검증값을 수신하는 단계;

상기 서버에서, 상기 공통 해시값(e), 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I) 및 상기 개인키(s_{ID})를 포함하는 문자열을 제2 랜덤 해시함수(h_2)로 해싱하여 세션키(sk)를 생성하는 단계; 및

상기 서버에서, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I), 상

기 세션키(sk), 상기 복호화된 패스워드 및 제3 랜덤 해시함수(h_3)를 이용하여 상기 제1검증값을 검증하는 단계를 더 포함하는, 인증 방법.

청구항 19

청구항 18에 있어서,

상기 세션키는, 다음의 수학적식

$$sk = h_2(X, (Y, I), X^{y+sid*e})$$

에 의하여 계산되는, 인증 방법.

청구항 20

청구항 18에 있어서,

상기 서버는, 상기 제1 비밀키 엘리먼트(X)와 함께 상기 아이디를 수신하거나, 또는 상기 제1검증값과 함께 상기 아이디를 수신하는, 인증 방법.

청구항 21

청구항 18에 있어서,

상기 제1검증값을 검증하는 단계의 수행 이후,

상기 서버에서, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I), 상기 세션키(sk) 및 상기 패스워드를 포함하는 제2문자열을 제4 랜덤 해시함수(h_4)로 해싱하여 제2검증값을 생성하는 단계; 및

상기 서버에서, 상기 제2검증값을 상기 단말로 송신하는 단계를 더 포함하는, 인증 방법.

청구항 22

청구항 11에 있어서,

상기 단말을 인증하는 단계는,

상기 서버에서, 하드웨어 보안 모듈을 이용하여 복호화된 상기 패스워드의 MAC 값을 생성하는 단계; 및

생성된 상기 MAC 값을 기 저장된 값과의 일치 여부를 판단하는 단계를 더 포함하는, 인증 방법.

청구항 23

청구항 1 내지 청구항 22 중 어느 한 항에 기재된 방법을 컴퓨터상에서 수행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 24

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하는 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,
상기 프로그램은,

단말 사용자의 아이디(ID) 및 서버와 교환한 키 생성 인자를 이용하여 아이디 기반의 비밀키(K)를 생성하는 단계;

생성된 상기 비밀키(K)를 대칭키로 하는 대칭키 암호화 알고리즘을 이용하여 상기 사용자의 패스워드를 암호화하고, 암호화된 상기 패스워드를 상기 서버로 송신함으로써 상기 단말 사용자의 인증을 요청하는 단계; 및

상기 서버로부터 상기 인증 요청에 대한 응답을 수신하는 단계를 실행하기 위한 명령어들을 포함하는 장치.

청구항 25

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하는 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,
상기 프로그램은,

단말 사용자의 아이디(ID) 및 상기 단말과 교환한 키 생성 인자를 이용하여 아이디 기반의 비밀키(K)를 생성하는 단계;

상기 단말로부터 상기 사용자의 암호화된 패스워드를 수신하는 단계; 및

생성된 상기 비밀키(K)를 대칭키로 하는 대칭키 복호화 알고리즘을 이용하여 상기 암호화된 패스워드를 복호화하고, 복호화된 상기 패스워드를 이용하여 상기 단말 사용자를 인증하는 단계를 실행하기 위한 명령어들을 포함하는 장치.

명세서

기술 분야

[0001] 본 발명은 네트워크 상에서의 보안 기술과 관련된다.

배경 기술

[0002] 패스워드 기반의 키 교환 프로토콜(PAKE; Password Authenticated Key Exchange)이란 통신에 참여하는 둘 이상의 주체가, 이 중 하나 이상의 주체가 알고 있는 패스워드를 기반으로 암호화된 통신을 위한 비밀키를 공유하는 과정을 의미한다. PAKE는 그 구현 방식에 따라 공개키 인증서 기반 PAKE 및 비 공개키 인증서 기반 PAKE로 나눌 수 있다.

[0003] 공개키 인증서 기반 PAKE 경우, 키 교환을 위하여 항상 공개키 인증을 수행하는 절차가 필요하며, 서버의 개인 키가 유출될 경우 해당 계정에 대한 전방향 안전성(forward secrecy)과 후방향 안전성(backward security)이 보장되지 않는 문제가 있다. 한편, 이러한 공개키 인증서 기반의 문제점을 해결하기 위해 제시되었던 비 공개키 인증서 기반 PAKE(관련 표준: IEEE P1363.2 및 ISO/IEC 11770-4)의 경우 패스워드를 직접 지수승하여 저장하는 인증자(verifier) 구성방식으로 인하여 기존 시스템의 마이그레이션(migration) 및 파라미터(parameter) 갱신이 어려운 새로운 문제점이 발생하였다. 또한 이 방식의 경우 패스워드를 그룹 파라미터(group parameter)와 직접 결합해야 하므로 이에 대한 오프라인 분석에 대응하기 위해 상대적으로 많은 실시간 계산량이 필요하고 프로토콜의 메시지 흐름을 유연하게 교체하는 것이 불가능한 문제가 있었다.

발명의 내용

해결하려는 과제

- [0004] 본 발명은 상기와 같은 문제를 해결하기 위한 것으로서, 본 발명의 실시예들은 기존의 패스워드 기반 키 교환 프로토콜에 아이디 기반 암호 기술을 적용함으로써 공개키 인증서 기반의 PAKE 및 비 공개키 인증서 기반의 PAKE의 장점을 모두 갖춘 효율적인 인증 및 키 교환 프로토콜을 제공하는 데 그 목적이 있다.

과제의 해결 수단

- [0005] 본 발명의 일 실시예에 따른 인증 방법은, 단말에서, 상기 단말 사용자의 아이디(ID) 및 서버와 교환한 키 생성 인자를 이용하여 아이디 기반의 비밀키(K)를 생성하는 단계; 상기 단말에서, 생성된 상기 비밀키(K)를 대칭키로 하는 대칭키 암호화 알고리즘을 이용하여 상기 사용자의 패스워드를 암호화하고, 암호화된 상기 패스워드를 상기 서버로 송신함으로써 상기 단말 사용자의 인증을 요청하는 단계; 및 상기 단말에서, 상기 서버로부터 상기 인증 요청에 대한 응답을 수신하는 단계를 포함한다.
- [0006] 상기 비밀키를 생성하는 단계는, 상기 단말에서, 단말측 난수(x)로부터 계산된 제1 비밀키 엘리먼트(X)를 서버로 송신하는 단계; 및 상기 단말에서, 상기 서버로부터 제2 비밀키 엘리먼트(Y)를 수신하는 단계를 포함하며, 상기 단말은, 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)를 이용하여 상기 비밀키(K)를 생성할 수 있다.
- [0007] 상기 단말은, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 이용하여 공통 해시값(e)을 생성하고, 상기 공통 해시값(e), 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 이용하여 상기 비밀키(K)를 생성할 수 있다.
- [0008] 상기 비밀키(K)는 상기 공통 해시값(e), 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 포함하는 제1문자열을 해싱함으로써 생성될 수 있다.
- [0009] 상기 제1 비밀키 엘리먼트(X)는 다음의 수학식에 의하여 계산될 수 있다.
- [0010]
$$X = g^x$$
- [0011] (이때, $\tilde{g}$ $g = \tilde{g}^2$ $\tilde{g}$ 는 유한한 군 $Z_N = \{0, 1, 2, \dots, N-1\}$ 의 최대 순환 부분군의 생성원을 라 할 때, $\tilde{g}$ 으로 생성되는 순환 부분군 G의 생성원, N은 $N=pq$ 를 만족하는 정수, p 및 q는 각각 $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$ 를 만족하는 소수)
- [0012] 상기 비밀키(K)는 다음의 수학식에 의하여 계산될 수 있다.
- [0013]
$$K = h_1(X, (Y, I), (YI^e)^x)$$
- [0014] (이때, h_1 은 제1 랜덤 해시함수, $I = H(ID)$, H 는 $H: \{0, 1\}^* \rightarrow G$ 의 관계를 만족하는 해시함수)
- [0015] 상기 방법은, 상기 암호화된 패스워드를 상기 서버로 송신하는 단계의 수행 이후, 상기 단말에서, 상기 공통 해시값(e), 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 포함하는 문자열을 제2 랜덤 해시함수(h_2)로 해싱하여 세션키(sk)를 생성하는 단계; 상기 단말에서, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I), 상기 세션키(sk) 및 상기 패스워드를 포함하는 제2문자열을 제3 랜덤 해시함수(h_3)로 해싱하여 제1검증값을 생성하는 단계; 및 상기 단말에서, 상기 제1검증값을 상기 서버로 송신하는 단계를 더 포함할 수 있다.
- [0016] 상기 세션키(sk)는 다음의 수학식에 의하여 계산될 수 있다.
- [0017]
$$sk = h_2(X, (Y, I), (YI^e)^x)$$

- [0018] 상기 단말은, 상기 제1 비밀키 엘리먼트(X)와 함께 상기 아이디를 상기 서버로 송신하거나, 또는 상기 제1검증값과 함께 상기 아이디를 상기 서버로 송신할 수 있다.
- [0019] 상기 방법은, 상기 제1검증값을 상기 서버로 송신하는 단계의 수행 이후, 상기 단말에서, 상기 서버로부터 제2 검증값을 수신하는 단계; 및 상기 단말에서, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I), 상기 세션키(sk), 상기 패스워드 및 제4 랜덤 해시함수(h₄)를 이용하여 상기 제2검증값을 검증하는 단계를 더 포함할 수 있다.
- [0020] 한편, 본 발명의 다른 실시예에 따른 인증 방법은, 서버에서, 단말 사용자의 아이디(ID) 및 상기 단말과 교환한 키 생성 인자를 이용하여 아이디 기반의 비밀키(K)를 생성하는 단계; 상기 서버에서, 상기 단말로부터 상기 사용자의 암호화된 패스워드를 수신하는 단계; 및 상기 서버에서, 생성된 상기 비밀키(K)를 대칭키로 하는 대칭키 복호화 알고리즘을 이용하여 상기 암호화된 패스워드를 복호화하고, 복호화된 상기 패스워드를 이용하여 상기 단말 사용자를 인증하는 단계를 포함한다.
- [0021] 상기 비밀키를 생성하는 단계는, 상기 서버에서, 키 발급 장치로부터 상기 아이디(ID)에 대응되는 개인키(s_{ID})를 발급받는 단계; 상기 서버에서, 상기 단말로부터 제1 비밀키 엘리먼트(X)를 수신하는 단계; 및 상기 서버에서, 서버측 난수(y)로부터 계산된 제2 비밀키 엘리먼트(Y)를 상기 단말로 송신하는 단계를 더 포함하며, 상기 서버는, 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID) 및 상기 개인키(s_{ID})를 이용하여 상기 비밀키(K)를 생성할 수 있다.
- [0022] 상기 서버는, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 이용하여 공통 해시값(e)을 생성하고, 상기 공통 해시값(e), 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I) 및 상기 개인키(s_{ID})를 이용하여 상기 비밀키(K)를 생성할 수 있다.
- [0023] 상기 비밀키(K)는 상기 공통 해시값(e), 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I) 및 상기 개인키(s_{ID})를 포함하는 제1문자열을 해싱함으로써 생성될 수 있다.
- [0024] 상기 개인키(s_{ID})는 다음의 수학식에 의하여 계산될 수 있다.

$$s_{ID} = \log_g H(ID) = \sum_{i=1}^{\alpha} s_{IDi}$$

[0025]

$$\tilde{g} \quad g = \tilde{g}^2$$

[0026]

(이때, g는 유한한 군 $Z_N = \{0, 1, 2, \dots, N-1\}$ 의 최대 순환 부분군의 생성원을 라 할 때, $\tilde{g}$ 으로 생성되는 순환 부분군 G의 생성원, N는 $N = pq$ 의 관계를 만족하는 정수, p 및 q는 각각 $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$ 를 만족하는 소수, ID_i는 상기 아이디를 구성하는 i번째 문자, α는 상기 아이디의 길이),

$$H(ID) = (h(ID))^2 = \prod_{i=1}^{\alpha} (h(ID_i))^2, \quad s_{IDi} = \log_g H(ID_i)$$

h는 $h: \{0,1\}^* \rightarrow Z_N$ 의 관계를 만족하는 랜덤해시함수,)

[0027] 상기 제2 비밀키 엘리먼트는 다음의 수학식에 의하여 계산될 수 있다.

[0028]

$$Y = g^y$$

[0029]

상기 비밀키(K)는 다음의 수학식에 의하여 계산될 수 있다.

[0030]

$$K = h_1(X, (Y, I), X^{y+sID*e})$$

[0031]

(이때, h₁은 제1 랜덤 해시함수, I = H(ID), H는 $H: \{0,1\}^* \rightarrow G$ 의 관계를 만족하는 해시함수)

[0032]

상기 방법은, 상기 단말을 인증하는 단계의 수행 이후, 상기 서버에서, 상기 단말로부터 제1검증값을 수신하는 단계; 상기 서버에서, 상기 공통 해시값(e), 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비

밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I) 및 상기 개인키(S_{ID})를 포함하는 문자열을 제2 랜덤 해시함수(h_2)로 해싱하여 세션키(sk)를 생성하는 단계; 및 상기 서버에서, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I), 상기 세션키(sk), 상기 복호화된 패스워드 및 제3 랜덤 해시함수(h_3)를 이용하여 상기 제1검증값을 검증하는 단계를 더 포함할 수 있다.

[0033] 상기 세션키는, 다음의 수식식에 의하여 계산될 수 있다.

[0034] $sk = h_2(X, (Y, I), X^{Y+SID*e})$

[0035] 상기 서버는, 상기 제1 비밀키 엘리먼트(X)와 함께 상기 아이디를 수신하거나, 또는 상기 제1검증값과 함께 상기 아이디를 수신할 수 있다.

[0036] 상기 방법은, 상기 제1검증값을 검증하는 단계의 수행 이후, 상기 서버에서, 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I), 상기 세션키(sk) 및 상기 패스워드를 포함하는 제2 문자열을 제4 랜덤 해시함수(h_4)로 해싱하여 제2검증값을 생성하는 단계; 및 상기 서버에서, 상기 제2검증값을 상기 단말로 송신하는 단계를 더 포함할 수 있다.

[0037] 상기 단말을 인증하는 단계는, 상기 서버에서, 하드웨어 보안 모듈을 이용하여 복호화된 상기 패스워드의 MAC 값을 생성하는 단계; 및 생성된 상기 MAC 값을 기 저장된 값과의 일치 여부를 판단하는 단계를 더 포함할 수 있다.

[0038] 한편, 본 발명의 일 실시예에 따른 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 단말 사용자의 아이디(ID) 및 서버와 교환한 키 생성 인자를 이용하여 아이디 기반의 비밀키(K)를 생성하는 단계; 생성된 상기 비밀키(K)를 대칭키로 하는 대칭키 암호화 알고리즘을 이용하여 상기 사용자의 패스워드를 암호화하고, 암호화된 상기 패스워드를 상기 서버로 송신함으로써 상기 단말 사용자의 인증을 요청하는 단계; 및 상기 서버로부터 상기 인증 요청에 대한 응답을 수신하는 단계를 실행하기 위한 명령어들을 포함한다.

[0039] 한편, 본 발명의 다른 실시예에 따른 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 단말 사용자의 아이디(ID) 및 상기 단말과 교환한 키 생성 인자를 이용하여 아이디 기반의 비밀키(K)를 생성하는 단계; 상기 단말로부터 상기 사용자의 암호화된 패스워드를 수신하는 단계; 및 생성된 상기 비밀키(K)를 대칭키로 하는 대칭키 복호화 알고리즘을 이용하여 상기 암호화된 패스워드를 복호화하고, 복호화된 상기 패스워드를 이용하여 상기 단말 사용자를 인증하는 단계를 실행하기 위한 명령어들을 포함한다.

발명의 효과

[0040] 본 발명의 실시예들에 따른 경우 기존의 패스워드 기반 인증 및 키 교환 프로토콜에 아이디 기반 암호 기술을 적용함으로써 키 교환을 위하여 공개키 인증이 필요하지 않으면서도 전방향 안전성 및 후방향 안전성을 보장할 수 있다.

[0041] 또한, 기존 비 공개키 인증서 기반의 문제점으로 지적되었던 기존 서버의 마이그레이션 및 향후 파라미터 갱신 등이 용이하며, 키 교환을 위하여 클라이언트 및 서버에서 각각 한 번의 지수승 연산만을 실시하면 되므로 기존의 알고리즘에 비해 계산량을 현저히 감소할 수 있는 장점이 있다.

도면의 간단한 설명

[0042] 도 1은 본 발명의 일 실시예에 따른 패스워드 기반 인증 시스템(100)을 설명하기 위한 블록도이다.

도 2는 본 발명의 일 실시예에 따른 패스워드 기반 인증 알고리즘(200)의 전체 단계를 설명하기 위한 도면이다.

도 3은 본 발명의 일 실시예에 따른 패스워드 기반 인증 알고리즘(200)의 키 교환 단계(206)를 상세

히 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0043] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.
- [0044] 본 발명을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [0045] 본 발명의 기술적 사상은 청구범위에 의해 결정되며, 이하의 실시예는 본 발명의 기술적 사상을 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 효율적으로 설명하기 위한 일 수단일 뿐이다.
- [0046] 도 1은 본 발명의 일 실시예에 따른 패스워드 기반 인증 시스템(100)을 설명하기 위한 블록도이다. 도시된 바와 같이, 본 발명의 일 실시예에 따른 패스워드 기반 인증 시스템(100)은 단말(102), 서버(104) 및 키 발급 장치(106)를 포함한다.
- [0047] 단말(102)은 서버(104)와의 안전한 통신을 위하여 서버(104)와의 사이에서 아이디 기반의 비밀키(K)를 생성한다. 즉, 상기 비밀키(K)의 생성 및 검증을 위하여 단말(102) 사용자의 아이디(ID) 및 패스워드가 이용된다. 상기 아이디는 단말(102)의 사용자를 식별하기 위하여 각 사용자별로 고유하게 부여된 식별 정보를 의미한다. 또한, 상기 패스워드는 사용자가 서버(104)에 로그인하기 위하여 상기 아이디와 함께 사용되는 비밀 문자열이다. 본 발명의 실시예에서 사용자의 아이디 및 패스워드는 사용자가 단말(102)을 통해 서버(104)에 로그인하기 위해서 사용되는 동시에, 비밀키(K)를 생성하기 위한 요소로서도 사용될 수 있다.
- [0048] 단말(102)은, 상기 단말 사용자의 아이디(ID) 및 서버와 교환한 키 생성 인자를 이용하여 아이디 기반의 비밀키(K)를 생성한다. 구체적으로, 비밀키(K)의 생성을 위하여 단말(102)은 단말측 난수(x)를 생성하고, 이로부터 제1 비밀키 엘리먼트(X)를 계산한다. 또한 단말(102)은 서버(104)로부터 제2 비밀키 엘리먼트(Y)를 수신하고, 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 사용자의 아이디(ID)를 이용하여 비밀키(K)를 생성한다. 즉, 본 발명의 실시예에서, 단말(102)측에서 비밀키를 생성하기 위한 키 생성 인자는, 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X) 및 상기 제2 비밀키 엘리먼트(Y)를 포함할 수 있다.
- [0049] 상기 비밀키(K)가 생성되면, 단말(102)은 생성된 상기 비밀키(K)를 대칭키로 하는 대칭키 암호화 알고리즘을 이용하여 상기 사용자의 패스워드를 암호화하고, 암호화된 상기 패스워드를 상기 서버로 송신함으로써 상기 단말 사용자의 인증을 요청하게 된다.
- [0050] 서버(104)는 단말(102)와의 안전한 통신을 위하여, 서버에서, 단말 사용자의 아이디(ID) 및 상기 단말과 교환한 키 생성 인자를 이용하여 아이디 기반의 비밀키(K)를 생성한다. 먼저, 서버(104)는 키 발급 장치(106)로 사용자의 아이디(ID)를 송신하고, 이에 대응되는 개인키(s_{ID})를 발급받는다. 또한, 서버(104)는 단말(102)로부터 제1 비밀키 엘리먼트(X)를 수신하고, 이와 별도로 서버측 난수(y)를 생성한 뒤 이로부터 제2 비밀키 엘리먼트(Y)를 계산한다. 이후, 서버(104)는 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID) 및 상기 개인키(S_{ID})를 이용하여 비밀키(K)를 생성한다. 즉, 상기 비밀키의 생성을 위한 서버(104)측 키 생성 인자는 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비밀키 엘리먼트(Y), 및 상기 개인키(S_{ID})를 포함할 수 있다. 이때, 서버(104)에서 생성되는 비밀키(K)는 단말(102)에서 생성되는 비밀키(K)와 동일하다. 즉, 본 발명의 실시예에서 단말(102)과 서버(104)는 서로 비밀키(K)를 직접 주고받지 않고도 서로 동일한 비밀키(K)를 공유할 수 있게 된다. 구체적인 단말(102) 및 서버(104)에서의 비밀키(K) 생성 방법에 대해서는 후술하기로 한다. 한편, 서버(104)는 단말(102)로부터 수신된 패스워드의 인증을 위한 별도의 하드웨어 보안 모듈(HSM; Hardware Security Module)을 포함할 수 있으며, 이에 대해서는 도 3에서 상세히 설명한다.
- [0051] 비밀키가 생성되면, 서버(104)는 단말(102)로부터 상기 사용자의 암호화된 패스워드를 수신한 뒤, 생성된 상기 비밀키(K)를 대칭키로 하는 대칭키 복호화 알고리즘을 이용하여 상기 암호화된 패스워드를 복호화하고, 복호화

된 상기 패스워드를 이용하여 상기 단말 사용자를 인증한 뒤 그 결과를 단말(102)로 회신하게 된다.

[0052] 키 발급 장치(106, Private Key Generator)는 서버(104)로부터 아이디(ID)를 수신하고, 수신된 상기 아이디(ID)에 대응되는 개인키(s_{ID})를 발급한다. 이때 상기 개인키(s_{ID})는 상기 아이디(ID)의 이산로그값으로서, 키 발급 장치(106)는 기 설정된 시스템 파라미터와 자신의 마스터키, 그리고 트랩도어 이산 로그(Trapdoor discrete logarithm) 군에 해당하는 사전계산 데이터를 기반으로 수신된 아이디에 대응되는 개인키를 계산한다. 구체적인 개인키(s_{ID}) 생성 방법에 대해서는 후술한다.

[0053] 이하에서는 상술한 구성을 가지는 패스워드 기반 인증 시스템(100)에서의 구체적인 인증 방법을 설명한다. 도 2에 도시된 바와 같이, 본 발명의 실시예에 다른 패스워드 기반 인증 방법(200)은 셋업(Setup, 202), 개인키 발급(Key extract, 204), 및 키 교환(Key Exchange, 206)의 3단계로 구분된다. 이 중, 셋업 단계(202)에서는 시스템 전체의 구성 요소를 정의하고, 개인키 발급 단계(204)에서는 서버(104)의 요청에 따라 키 발급 장치(106)에서 마스터 키를 기반으로 아이디에 대응되는 개인키를 생성한다. 키 교환 단계(206)에서는 단말(102) 및 서버(104) 간에 공통된 비밀키(K)를 생성하고, 이로부터 세션키(sk)를 생성하게 된다.

[0054] 셋업(202)

[0055] 본 발명의 실시예에서 셋업 단계는 단말(102)과 서버(104) 간의 비밀키 교환을 위한 파라미터 및 마스터키를 정의하는 단계이다.

[0056] 먼저, 각각 $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$ 를 만족하고 B 스무스(B smooth)인 비슷한 크기의 큰 두 소수 p, q로부터 $N = pq$ 를 계산한다. 이 때, p와 q는 주어진 안전성 파라미터에 해당하는 보안 강도 (security level)를 만족하고 암호학적으로 안전한 소수이다. 안전성 파라미터란 암호화 알고리즘에 대한 기본공격의 시간과 비용을 결정짓는 알고리즘의 요소를 의미한다. 이때 기본 공격이란 주어진 데이터(평문과 암호문)를 만족시키는 키를 발견할 때까지 모든 가능한 키 후보를 검색하는 전수조사(Exhaustive Search) 방식의 공격을 의미한다. 전수 조사에 걸리는 시간은 가능한 키의 개수에 의존하고 키의 개수는 키의 길이에 의해 결정되므로, 이 경우 안전성 파라미터는 키의 길이를 의미한다. 또한, B 값은 상기 보안 강도에 따라 적절하게 설정될 수 있다.

[0057] 다음으로, 비밀키 교환에 사용되는 해시 함수 H 및 랜덤 해시 함수 h_i 를 정의한다. 유한한 군 $Z_N = \{0, 1, 2,$

$\tilde{g}$

..., N-1}의 최대 순환 부분군(maximal cyclic subgroup)의 생성원(generator)을 $\tilde{g}$ 라 하자. 이제 생성원 $g = \tilde{g}^2$

으로 생성되는 순환 부분군을 G라고 정의하면 이로부터 해시 함수 H는 다음의 수학적 식 1과 같이 정의된다.

[0058] [수학적 식 1]

[0059] $H: \{0,1\}^* \rightarrow G$

[0060] (이때, $\{0,1\}^*$ 은 0과 1로 이루어진 임의의 유한한 비트열)

[0061] 즉, 상기 해시 함수 H는 아이디를 입력값으로 할 때 그 출력값이 군 G의 원소가 되도록 정의된다. 예를 들어, 다음과 같은 랜덤 해시함수 $h: \{0,1\}^* \rightarrow Z_n$ 가 있을 경우, 해시 함수 H는 다음의 수학적 식 2와 같이 정의될 수 있다.

[0062] [수학적 식 2]

- [0063] $H(ID) = h(ID)^2$
- [0064] 또한, 해시 함수 h_i 는 다음의 수학적 식 3과 같이 정의된다.
- [0065] [수학적 식 3]
- [0066] $H_i: \{0,1\}^* \rightarrow \{0,1\}^{n_i}$
- [0067] (이때, $\{0,1\}^{n_i}$ 은 0 또는 1 중 임의의 비트로 구성된 n_i 비트의 문자열을 의미하며, $i \in \{0, 1, 2, 3, 4, 5, 6\}$)
- [0068] 즉, 본 발명의 실시예에서는 6개의 랜덤 해시 함수가 사용되며, 각각의 랜덤 해시 함수의 출력값의 비트수는 알고리즘의 구체적인 형태에 따라 적절히 정해질 수 있다. 즉, n_0 내지 n_6 의 값은 필요에 따라 적절히 설정될 수 있다. 각각의 랜덤 해시 함수로는 예를 들어, SHA1, SHA-256, SHA-512 등이 사용될 수 있으나 본 발명이 특정한 함수에 한정되는 것은 아니다. 또한 상기 실시예에서는 각 랜덤 해시 함수가 0 내지 6의 값을 가지도록 기술하였으나, 이는 단지 각 랜덤 해시 함수를 구분하기 위한 것일 뿐, 각각의 랜덤 해시 함수들이 특정한 순서를 가지는 것은 아니다.
- [0069] 이와 같은 과정을 거쳐 도출되는 시스템 파라미터(param_R) 및 마스터키(mk)는 다음과 같다.
- [0070] $param = \{N, G, g, H, h_0, h_1, h_2, h_3, h_4, h_5, h_6\}$
- [0071] $mk = (p, q)$
- [0072] 개인키 발급(204)
- [0073] 본 단계는 키 발급 장치(106)에서 서버(104)로부터 수신된 아이디를 기반으로 개인키(private key, s_{ID})를 발급하는 단계이다. 키 발급 장치(106)는 상기 시스템 파라미터(param_R) 및 마스터키(mk), 그리고 트랩도어 이산 로그(TDL) 군에 해당하는 사전계산 데이터를 기반으로 주어진 아이디에 대응되는 개인키를 계산한다. 이산 로그 계산이 암호학적으로 불가능하지만 트랩도어를 알고 있을 경우 이산 로그 값을 쉽게 계산할 수 있는 군이 존재하며, 이를 트랩도어 이산 로그 군이라 한다. 본 발명에서는 이와 같은 트랩도어 이산 로그군의 특성을 이용하여 각 아이디에 대응되는 개인키를 계산한다. 즉, 상기 개인키 생성자는 상기 마스터키와 상기 트랩도어 이산 로그군에 해당하는 각 값들에 대한 사전 계산 데이터를, 예를 들어 테이블 등의 형태로 저장해 두었다가 수신되는 아이디와 상기 테이블에 저장된 사전 계산 데이터를 이용하여 수신된 아이디에 대응되는 개인키를 계산한다.
- [0074] 구체적으로, 개인키 생성자(PKG)는 수신되는 아이디(ID)를 한 문자 또는 숫자씩 분리하여 $ID = ID_1 || ID_2 || \dots || ID_\alpha$ (이때, α 는 상기 아이디의 길이)와 같이 표현한다. 예를 들어 ID가 abc01인 경우 $ID_1 = a, ID_2 = b, ID_3 = c, ID_4 = 0, ID_5 = 1$ 로 나타낼 수 있다. 즉, ID_i 는 상기 아이디를 구성하는 i 번째 문자 ID_i 를 의미한다. 각 ID_i 에 대해 해시함수 H 를 이용하여 이를 TDL 군 G 의 원소로 변환하고, 전술한 사전계산 데이터를 이용하여 $H(ID_i)$ 의 밑 g 에 대한 이산로그 값을 계산하며, 이를 수학적 식으로 나타내면 다음과 같다.

[0075] [수학식 4]

$$s_{IDi} = \log_g H(ID_i)$$

[0076]

[0077] 이때, $H(ID)$ 는 수학식 2에서 설명한 바와 같이, 상기 랜덤 해시함수 h 에 대해 $H(ID) = (h(ID))^2 = \prod_{i=1}^{\alpha} (h(ID_i))^2$ 의 관계를 가진다.

[0078] 상기 ID에 대응되는 개인키(s_{ID})는 다음의 수학식 5와 같이 계산된다.

[0079] [수학식 5]

$$s_{ID} = \log_g H(ID) = \sum_{i=1}^{\alpha} s_{IDi}$$

[0080]

[0081] 이와 같이 계산된 상기 개인키(s_{ID})는 안전한 채널을 통하여 서버(104)로 전달된다.

[0082] 키 교환(206)

[0083] 본 단계는 단말(102)과 서버(104) 간의 안전한 통신을 위한 비밀키(K)를 교환하고 이를 이용하여 세션키(sk)를 생성하는 단계이다. 도 3은 본 발명의 일 실시예에 따른 비밀키 교환 과정(206)을 설명하기 위한 블록도이다.

[0084] 먼저, 단말(102)은 상기 202 단계에서 정의된 시스템 파라미터에 따라 Z_N 에서 임의의 단말측 난수(random number) x 를 선택하고(300), 상기 단말측 난수 x 로부터 제1 비밀키 엘리먼트(X)를 계산한다(302). 이때 상기 제1 비밀키 엘리먼트(X)는 다음의 수학식 6과 같이 계산된다.

[0085] [수학식 6]

$$X = g^x$$

[0087] (이때, g 는 상기 순환 부분군 G 의 생성원, N 은 $N=pq$ 를 만족하는 정수, p 및 q 는 각각 $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$ 를 만족하는 소수)

[0088] 상기과 같이 제1 비밀키 엘리먼트(X)가 계산되면, 단말(102)은 상기 제1 비밀키 엘리먼트(X)를 서버(104)로 송신한다. 또한, 도시된 바와 같이 단말(102)은 상기 제1 비밀키 엘리먼트(X)와 함께 아이디(ID)를 서버(104)로 전송할 수 있으나, 반드시 본 단계에서 상기 아이디(ID)를 전송하여야 하는 것은 아니며, 실시예에 따라 후술할 320 단계에서 제1 검증키와 함께 상기 아이디(ID)를 전송하는 것도 가능하다.

[0089] 한편, 서버(104)는 Z_N 에서 임의의 서버측 난수(random number) y 를 선택하고(306), 상기 단말측 난수 y 로부터 제2 비밀키 엘리먼트(Y)를 계산한다(308). 이때 상기 제1 비밀키 엘리먼트(X)는 다음의 수학식 7과 같이 계산된다.

[0090] [수학식 7]

- [0091] $Y = g^y$
- [0092] 상기와 같이 제2 비밀키 엘리먼트(Y)가 계산되면, 서버(104)는 상기 제2 비밀키 엘리먼트(Y)를 단말(102)로 송신한다.
- [0093] 한편, 도시된 실시예에서는 서버(104)에서 단말(102)로부터 아이디 및 제1 비밀키 엘리먼트를 수신한 이후 서버(104)에서 306, 308 단계를 수행하는 것으로 도시되었으나, 본 발명의 실시예들은 이에 한정되는 것은 아니다. 즉, 본 발명의 실시예에서 306 및 308 단계는 300 및 302 단계와는 별도로 수행된다. 즉, 실시예에 따라 제2 비밀키 엘리먼트(Y)는 제1 비밀키 엘리먼트(X)보다 먼저 생성될 수도 있고, 동시에 생성될 수도 있다. 또한, 본 발명의 실시예에서 제1 비밀키 엘리먼트(X) 및 제2 비밀키 엘리먼트(Y)는 각각 단말(102) 및 서버(104)에서 미리 계산되어 저장되는 값일 수도 있다. 이 경우에는 본 방법을 수행하는 데 있어 300 및 302 단계, 306 및 308 단계를 수행할 필요 없이 저장된 값을 불러오기만 하면 되므로, 제1 비밀키 엘리먼트(X) 및 제2 비밀키 엘리먼트(Y)의 계산에 따른 오버헤드가 없어지게 된다. (단, 이때, 해시함수, 대칭키 암호 알고리즘, 곱셈 연산 등의 연산 시간은 무시할 수 있다고 가정한다.)
- [0094] 이와 같이 단말(102)과 서버(104) 사이에 제1 비밀키 엘리먼트(X) 및 제2 비밀키 엘리먼트(Y)가 교환되면, 단말(102) 및 서버(104)는 각각 비밀키(K)를 계산한다.
- [0095] 먼저, 단말(102)은 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)과 상기 해시함수 h_0 를 이용하여 공통 해시값($e = h_0(X, Y, I)$)를 계산한다.
- [0096] 다음으로, 단말(102)은 상기 계산한 공통 해시값(e), 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 포함하는 제1문자열을 해싱함으로써 비밀키(K)를 생성한다(312). 이를 수식으로 나타내면 수학식 8과 같다.
- [0097] [수학식 8]
- [0098] $K = h_1(X, (Y, I), (YI^e)^x)$
- [0099] (이때, $I = H(ID)$)
- [0100] 한편, 서버(104) 또한 단말(102)과 마찬가지로 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)과 상기 해시함수 h_0 를 이용하여 공통 해시값($e = h_0(X, Y, I)$)를 계산하고, 상기 계산한 공통 해시값(e), 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I) 및 상기 개인키(S_{ID})를 포함하는 제1문자열을 해싱함으로써 비밀키(K)를 생성한다(314). 이를 수식으로 나타내면 수학식 9와 같다.
- [0101] [수학식 9]
- [0102] $K = h_1(X, (Y, I), X^{y+S_{ID}e})$
- [0103] 전술한 바와 같이, 상기 312 단계 및 314 단계에서 생성되는 개인키는 동일하다. 즉, 본 발명의 실시예에 따라 경우 단말(102)과 서버(104) 사이에 별도의 비밀키 교환 과정이 없이도 서로 공통된 비밀키를 생성할 수 있다. 또한 비밀키를 생성하기 위하여 단말(102) 및 서버(104)에서 각각 제1 비밀키 엘리먼트(X) 제2 비밀키 엘리먼트(Y)를 얻기 위한 지수승 한 번의 연산만을 수행하면 되므로 비밀키 생성을 위한 계산량이 종래에 비해 현저히 감소하게 된다.
- [0104] 이와 같이, 단말(102)과 서버(104) 사이에 공통된 비밀키(K)가 생성되면, 다음으로 단말(102)은 비밀키(K)를 대

칭키로 하는 대칭키 암호화 알고리즘(symmetric key algorithm, E_k)을 이용하여 단말(102)의 패스워드를 암호화한다(316). 암호화된 상기 패스워드는 이후 서버(104)로 전달되어 단말(102)을 인증하는 데 사용된다.

[0105] 다음으로, 단말(102)은 상기 공통 해시값(e), 상기 단말측 난수(x), 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y) 및 상기 아이디(ID)의 해시값(I)을 포함하는 문자열을 제2 랜덤 해시함수(h_2)로 해싱하여 세션키(sk)를 생성한다(318). 이를 수식으로 나타내면 다음과 같다.

[0106] [수학식 10]

$$sk = h_2(X, (Y, I), (YI^e)^x)$$

[0108] 서버(104) 또한 상기 공통 해시값(e), 상기 제1 비밀키 엘리먼트(X), 상기 서버측 난수(y), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I) 및 상기 개인키(S_{ID})를 포함하는 문자열을 제2 랜덤 해시함수(h_2)로 해싱하여 세션키(sk)를 생성한다(320). 이를 수식으로 나타내면 다음과 같다.

[0109] [수학식 11]

$$sk = h_2(X, (Y, I), X^{y+S_{ID}e})$$

[0111] 이후, 단말(102)은 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I), 상기 세션키(sk) 및 상기 패스워드를 포함하는 제2 문자열을 제3 랜덤 해시함수(h_3)로 해싱하여 제1검증값을 생성하고, 상기 생성된 비밀키(K)를 이용하여 패스워드를 암호화하며, 상기 제1검증값 및 상기 암호화된 패스워드($E_K(pw)$)를 서버(104)로 송신한다(322). 이때 상기 제1검증값은 다음의 수학식에 의해 계산될 수 있다.

[0112] [수학식 12]

$$\text{제1검증값} = h_3(X, Y, I, sk, PW)$$

[0114] 한편, 전술한 바와 같이 304 단계에서 아이디가 송신되지 않은 경우에는 본 단계에서 아이디를 함께 전송할 수도 있다.

[0115] 상기 제1검증값을 수신한 서버(104)는 단말(102)과 동일한 대칭키 암호화 알고리즘을 이용하여 암호화된 패스워드를 복호화하고, 복호화된 패스워드 및 아이디를 이용하여 사용자를 인증한다(324). 즉, 서버(104)에 의하여 복호화된 상기 패스워드는 수신된 상기 아이디와 함께 단말(102)의 사용자를 인증하는 데 사용된다.

[0116] 상기 사용자 인증을 위하여, 서버(104)는 데이터베이스 등 별도의 저장 공간에 각 사용자의 패스워드를 기록하여 두었다가, 단말(102)로부터 수신되어 복호화된 패스워드와 기 저장된 패스워드와의 일치 여부를 검증하도록 구성될 수 있다. 또한, 실시예에 따라 서버(104)는 상기 패스워드 자체를 저장 및 관리할 수도 있고, 또는 패스워드의 해시값을 저장하거나, 별도의 하드웨어 보안 모듈(HSM)을 이용하여 계산된 MAC 값을 저장할 수도 있다.

[0117] 본 발명의 실시예에서, 하드웨어 보안 모듈(또는 HSM 장비로 지칭)는 강력한 인증을 위해 디지털 키를 이용한 하드웨어적 연산을 수행하는 장비이다. HSM 장비는 일반적으로 플러그인 카드(plug-in card) 형태나 임베디드 칩(embedded chip) 형태로 구현되며 탬퍼링(tampering)이나 버스 프로빙(bus probing) 등으로부터 안전한 하나 이상의 보안 크립토프로세서(secure cryptoprocessor)를 탑재하고 있다. 이러한 HSM 장비를 활용하면 종래의 해싱 기법 등에 비해 더욱 안전한 패스워드 관리가 가능하다.

[0118] 서버(104) 측에서 HSM 장비를 이용하여 패스워드 매칭을 수행하는 방법을 설명하면 다음과 같다. 먼저, 서버

(104)는 데이터베이스에 단순한 패스워드의 해시값이 아니라, 서버(104) 측에 구비된 HSM 장비의 비밀키(k_{HSM})가 반영된 MAC(message authentication code) 값 ($MAC_k(pw)$)을 저장한다.

[0119] 이후, 상기 322 단계에서 단말(102)로부터 암호화된 패스워드가 전송될 경우, 서버(104)는 단말(102)로부터 받은 암호화된 패스워드를 복호화하여(324 단계), HSM 장비에 입력한다. 그러면 상기 HSM 장비는 서버(104)로부터 제공받은 패스워드와 탑재한 비밀키 k_{HSM} 를 이용하여 MAC 값($MAC_k(pw)$)을 계산하고, 계산된 MAC 값을 서버(104)로 반환한다. 이후, 서버(104)는 데이터베이스에 기 저장된 MAC 값과 HSM 장비로부터 계산된 MAC 값을 비교하여 사용자를 인증하게 된다.

[0120] 상기 MAC 연산 시간은 기본적으로 대칭키 암호화 연산 시간과 비슷하므로, 이를 이용할 경우 기존 방법에 비해 효율성은 비슷하면서도 더욱 향상된 안전성을 제공한다. 왜냐하면, 일반적인 hash 함수와 달리 MAC의 경우 key 값이 반영되므로 MAC의 output은 단순히 password 길이에 따른 random성 뿐 아니라 key값에 따라 암호학적 안전성 (예를 들어, key 값이 128bit일 경우 기존 AES-128과 동일한 안전성)을 제공할 수 있게 되어 원천적으로 패스워드 크래킹(password cracking)을 불가능하게 하기 때문이다.

[0121] 그러나 기존의 패스워드 기반 키 교환 방법의 경우 알고리즘 상 패스워드 자체를 전달하는 것이 불가능하며, 단지 패스워드의 매칭 여부를 확인할 수 있는 값을 전달하는 형태이므로, 기존의 알고리즘에서 HSM 장비를 활용하기 위해서는 제한한 방법에 비해 2000배 이상 느린 지수승 또는 공개키 암호 연산이 필요하다. 따라서 종래기술에 따른 경우에는 서버와 클라이언트 사이에 매우 빈번히 발생하는 로그인 작업에 HSM 장비를 사용하기 불가능하였다. 그러나 본 발명의 실시예들에 따른 경우 비밀키를 이용하여 서버 측으로 직접 암호화된 패스워드를 전달할 수 있게 되는 바, 사용자 로그인 등의 과정에서 별도의 서버측 부하를 가중시키지 않으면서도 HSM 장비를 적용하여 키 교환 및 인증 과정에서의 안정성을 배가시킬 수 있는 장점이 있다.

[0122] 상기과 같은 패스워드 복호화 및 인증이 완료되면, 다음으로 서버(104)는 복호화된 패스워드를 이용하여 상기 제1검증값을 검증한다(326). 본 단계에서는, 서버(104)에서 알고 있는 인자들, 즉 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 상기 아이디(ID)의 해시값(I), 상기 세션키(sk), 복호화된 패스워드 및 제3 랜덤 해시함수(h_3)를 이용하여 제1검증값을 별도로 생성하고, 이를 수신된 값과 비교함으로써 상기 제1검증값을 검증할 수 있다. 이때 두 개의 값이 서로 일치하는 경우 상기 검증은 성공한 것이 되며, 일치하지 않는 경우 상기 검증은 실패한 것이 된다.

[0123] 이후, 서버(104)는 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 아이디(ID)의 해시값(I), 상기 세션키(sk) 및 상기 패스워드를 포함하는 제2문자열을 제4 랜덤 해시함수(h_4)로 해싱하여 제2검증값을 생성한 뒤 이를 단말(102)로 송신한다(328). 이때 상기 제2검증값은 다음의 수학식에 의해 계산될 수 있다.

[0124] [수학식 13]

[0125] 제2검증값 = $h_4(X, Y, I, sk, PW)$

[0126] 이후, 단말(102)은 자신이 알고 있는 값, 즉 상기 제1 비밀키 엘리먼트(X), 상기 제2 비밀키 엘리먼트(Y), 아이디(ID)의 해시값(I), 상기 세션키(sk), 상기 패스워드 및 제4 랜덤 해시함수(h_4)를 이용하여 별도의 제2검증값을 생성하고, 이를 수신된 값과 비교함으로써 상기 제2검증값을 검증한다. 이때 두 개의 값이 서로 일치하는 경우 상기 검증은 성공한 것이 되며, 일치하지 않는 경우 상기 검증은 실패한 것이 된다. 본 발명에서는 상기 제1 검증값을 통한 검증 및 제2검증값을 통한 검증이 모두 성공한 경우 세션키 교환에 성공한 것으로 판단할 수 있다.

[0127] 한편, 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야에서 통상의 지식을 가진 자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 플로피 디스크와 같은 자기-광 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는

컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0128] 이상에서 대표적인 실시예를 통하여 본 발명에 대하여 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다.

[0129] 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0130] 100: 패스워드 기반 키 교환 시스템

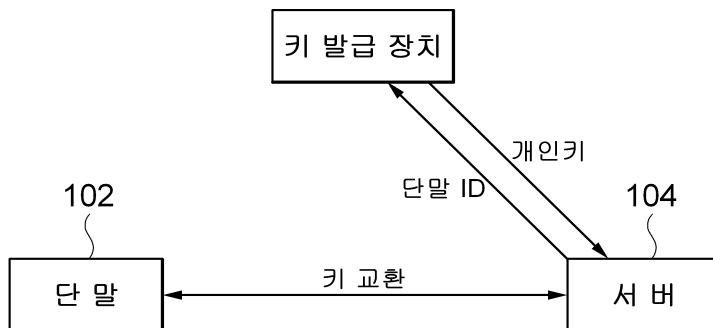
102: 단말

104: 서버

106: 키 발급 장치

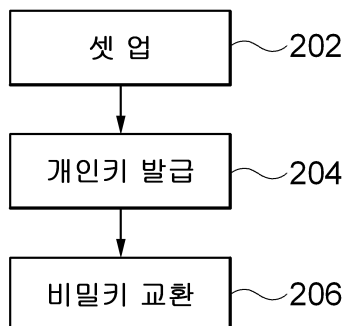
도면

도면1



도면2

200



도면3

206

