情報保護學會論文誌
第16卷 第6號, 2006. 12

스마트카드를 이용한 3자 참여 인증된 키교환 프로토콜*

전 일 수†
금오공과대학교

Three-Party Authenticated Key Exchange Protocol using Smartcards

Il-Soo Jeon†
Kumoh National Institute of Technology

요 약

최근 Sun등[9]은 서버의 공개키를 사용하고 사용자의 패스워드로부터 유도된 검증자를 이용한 3자 참여 인증된 키교환 프로토콜을 제안하였다. 본 논문에서는 스마트카드를 사용한 패스워드 기반의 3자 참여 인증된 키교환 프로토콜을 제안한다. 제안된 프로토콜은 Sun등의 프로토콜에 비해 공개키 연산 대신 XOR과 해쉬함수 연산을 사용하기 때문에 계산비용이 매우 작으며, 또한 메시지 전송회수도 20% 줄어들기 때문에 효율적으로 인증된 키 교환을 수행할 수 있다. 또한, 제안된 기법에서는 패스워드를 서버에 저장하지 않으므로 패스워드 추측공격에 안전하고, 두 사용자들 간에 공유된 세션키를 서버가 알 수 없기 때문에 서버 Compromise 공격으로부터도 안전하다.

ABSTRACT

Recently, Sun et el.[9] proposed a three-party authenticated key exchange protocol using the public key of the server and the derived verifier from the password of a user. This paper proposes a password-based three-party authenticated key exchange protocol using smartcards. Since the proposed protocol has very low computation cost by using XOR and hash function operation instead of the public key operation, and reduces the count of message transmission to 20% compared with the protocol of Sun et el., it can execute an effective authenticated key exchange. Furthermore, the proposed protocol is safe from password guessing attack by not saving passwords in the server, and it is also safe from server compromise attack because the server cannot know the shared session key between the two users.

Keywords : *Three-party key exchange protocol, Authentication, Hash function*

Ⅰ. 서 론

인터넷과 같은 공개된 통신망을 통하여 안전하게 통신하기 위해서는 전송하려는 정보를 암호화하여야 한다. 암호통신을 하기 위해서는 통신 참여자가 정당한 사용자인지를 확인하는 인증 기법과 메시지의 암호화에 필요한 키를 서로 공유해야 한다. 따라서 통신 참여자들이 서로를 인증하고 키를 공유할 수 있는 키 교환 프로토콜의 개발이 필요하다.

Diffie-Hellman 키 교환 프로토콜[1]은 안전하

접수일: 2006년 8월 18일 ; 채택일: 2006년 10월 11일
* 본 연구는 금오공과대학교 학술연구비에 의하여 연구된 논문
† 주저자, isjeon@kumoh.ac.kr

지 않은 통신상에서 안전하게 세션키를 공유하기 위해 잘 알려진 방법이지만, 이 프로토콜은 참여자들을 인증하는 방법을 제공하지 못하기 때문에 중간 침입자 공격(man in the middle attack)에 대하여 안전하지 못하다. 이러한 문제를 해결하기 위하여 패스워드를 이용한 인증된 키교환 프로토콜이 많이 제안되었다. Bellovin과 Merritt[2]는 패스워드 추측 공격에 대항할 수 있는 패스워드 기반의 EKE (Encrypted Key Exchange) 기법을 제안하였다. 이 기법은 인증을 위해 사용자의 패스워드를 서버에 저장하였는데, 이 경우 서버의 패스워드 파일이 공격당하면 공격자가 쉽게 정당한 사용자로 위장할 수 있다. 이러한 문제점을 해결하기 위해 서버에 패스워드를 그대로 저장하는 대신 패스워드로부터 유도된 검증자(Verifier)를 저장하고 이를 이용하는 기법들[3,4]이 제안되었다.

2자 참여 인증된 키교환 프로토콜 뿐 만 아니라 3자 참여 인증된 키교환 프로토콜들도 제안되었는데, 3자 참여 방식에서 참여자들은 하나의 서버와 그 서버에 등록되어 있는 두 사용자로 구성되며 두 사용자는 서버의 인증을 받아 오직 자신들만이 아는 세션키를 공유한다. Steiner등[5]은 EKE를 기반으로 하는 3자 참여 인증된 키교환 프로토콜(STW-3PEKE)을 제안하였고, Ding과 Horstor[6]는 STW-3PEKE에서 세 참여자들이 감지할 수 없는 온라인 추측공격에 취약함을 보였다. Lin등[7,8]은 STW-3PEKE가 오프라인 추측공격에도 취약함을 보이고, 이를 개선하기 위해 서버의 공개키를 사용한 프로토콜(LSH-3PEKE)[7]을 제안하였고, 그 후에 서버의 공개키를 사용하지 않는 프로토콜(LSSH-3PEKE)[8]를 제안하였다. LSH-3PEKE는 5번의 메시지 전송으로 이루어지지만, LSSH-3PEKE는 서버의 공개키를 사용하지 않는 대신 메시지 전송회수가 2회 더 추가되었다.

최근에 Sun등[9]은 Stenier등[5]이 제안한 STW-3PEKE의 문제점을 해결하기 위해 서버의 공개키를 사용한 패스워드 기반의 개선된 프로토콜(SCH-3PEKE)과, 또한 서버의 공개키를 사용하고 사용자의 패스워드 대신 이로부터 유도된 검증자를 이용한 인증된 키교환 프로토콜을 제안하였다. 서버의 공개키를 이용하는 방식은 온라인 패스워드 추측 공격으로부터는 안전하나 사용자들에게 큰 처리 부담을 요구한다.

본 논문에서는 동일한 서버에 등록되어 있는 두 사용자들에게 안전한 통신 서비스를 제공하기 위해 스마트카드를 사용한 패스워드 기반의 인증된 키교환 프로토콜을 제안한다. 제안된 프로토콜에서는 Cu와 Chen[10]이 제안한 패스워드 기반의 원격 사용자 인증 프로토콜에서처럼 스마트카드를 이용한다. 제안된 프로토콜에서는 처리비용이 큰 지수연산이나 비대칭 암호화 연산 없이 XOR 연산과 해쉬함수만을 사용하고, 또한 SCH-3PEKE보다 적은 수의 메시지 전송으로 효율적인 키교환을 수행한다. 특히, 제안된 기법은 패스워드를 서버에 저장하지 않으므로 패스워드 추측공격에 안전할 뿐만 아니라, 두 사용자들이 공유하는 세션키를 서버가 알 수 없기 때문에 서버 Compromise 공격으로부터 안전한 프로토콜이다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로 SCH-3PEKE[9]에 대해서 살펴본다. 3장에서는 본 논문에서 제안된 프로토콜을 제시하고, 4장에서는 제안된 프로토콜에 대한 암호학적 분석을 제시하며, 5장에는 제안된 프로토콜의 효율성 분석을 한다. 마지막으로 6장에서는 결론을 맺는다.

II. 관련 연구

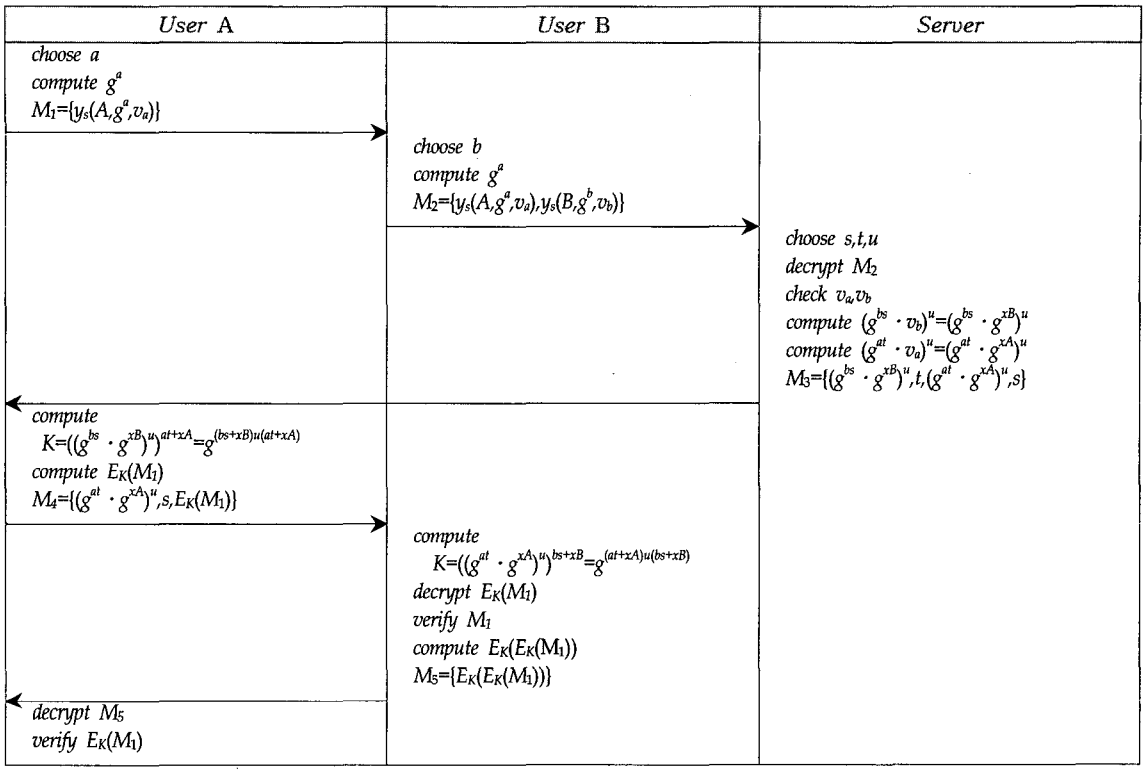
본 장에서는 본 논문에서 제안하는 프로토콜 및 관련된 기존 연구의 프로토콜 기술에 사용되는 용어의 표기법을 정의하고, 관련 연구로 SCH-3PEKE[9]을 간단히 기술한다.

2.1 표기법 정의

본 연구에서 제안된 프로토콜 및 관련연구에서 사용될 용어의 표기법을 〔표 1〕과 같이 정의한다.

〔표 1〕 표기법

기호	설명
G_q	위수 q를 갖는 Z_p^*의 부분군
g	G_q의 생성자
A, B, S	각각 사용자 A, 사용자 B, 서버 S의 아이디
$h()$	일방향 해쉬함수
$y_s()$	서버의 공개키를 이용한 공개키 암호화
$E_K()$	비밀키 K를 이용한 대칭키 암호화
$\oplus$	XOR 연산자
X_A, X_B	각각 A와 B의 패스워드에 의해 생성된 개인키
X_s	서버의 비밀키
V_a, V_b	각각 서버에 저장되는 A와 B의 검증자
K	세션키
$\rightarrow$	메시지 전송



〔그림 1〕 SCH-3PEKE

2.2 SCH-3PEKE

SCH-3PEKE는 두 사용자(A,B)와 하나의 서버(S)가 관련되어 있으며, 두 사용자가 서버의 도움을 받아 세션키를 공유하려는 상황에 적용될 수 있는 프로토콜이다. 두 사용자 A와 B는 인증을 위해 그들의 검증자 v_a와 v_b를 서버에 미리 안전하게 저장해야 한다. 여기서 $v_a = g^{xA}$, $v_b = g^{xB}$ 이고, x_A와 x_B는 A와 B의 패스워드로부터 각각 유도되는 A와 B의 개인키이다. 프로토콜의 세부적인 과정을 다음에 기술하고, 이를 〔그림 1〕에 요약한다.

Step 1. A는 랜덤 값 a를 선택하고 g^a를 계산하여 M_1을 B에게 전송한다.

$M_1 = \{ y_s(A, g^a, v_a) \}$

Step 2. B는 랜덤 값 b를 선택하고 g^b를 계산하여 M_2를 S에게 전송한다.

$M_2 = \{ y_s(A, g^a, v_a),\ y_s(B, g^b, v_b) \}$

Step 3. S는 A의 검증자 v_a와 B의 검증자 v_b를 검증하고, 검증에 통과하면 S는 $(g^{bs}\cdot v_b)^u$와 $(g^{at}\cdot v_a)^u$를 계산하여 M_3를 A에게 전송한다. 여기서 s, t, u는 S에 의해 선택된 랜덤 값이다.

$M_3 = \{ (g^{bs}\cdot v_b)^u,\ t,\ (g^{at}\cdot v_a)^u,\ s \}$

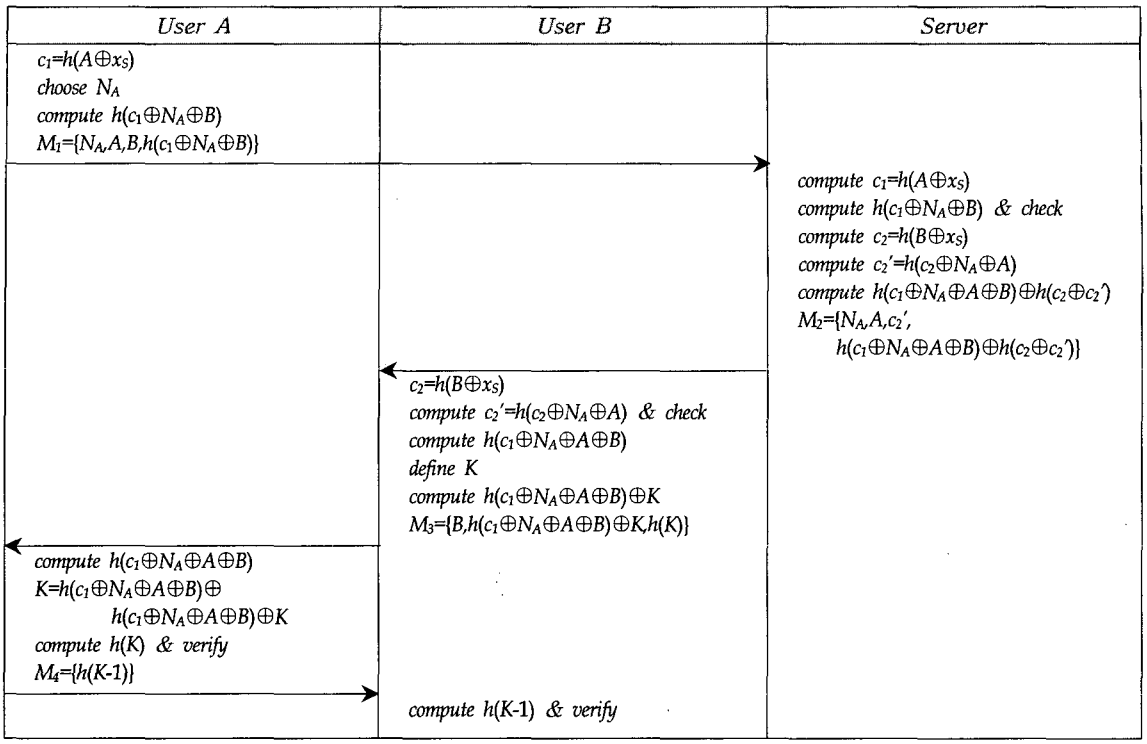
Step 4. A는 세션키, $K=((g^{bs}\cdot v_b)^u)^{at+xA}$를 계산하여 구하고, 또한 $E_K(M_1)$를 계산하여 M_4를 B에게 전송한다.

$M_4 = \{ (g^{at}\cdot v_a)^u,\ s,\ E_K(M_1) \}$

Step 5. B는 세션키, $K=((g^{at}\cdot v_a)^u)^{bs+xB}$ 를 계산하여 구하고, 또한 $E_K(M_1)$를 복호하여 Step1에서 전송받은 M_1과 같은지를 조사한다. 만약 같으면 B는 A가 바른 세션키를 가지고 있음을 확신하고, B는 M_5를 A에게 전송한다.

$M_5 = \{ E_K(E_K(M_1)) \}$

Step 6. A는 M_1을 이용하여 $E_K(E_K(M_1))$를 계산하여 그 결과가 M_5와 같은지를 조사하여 B가 바른 세션키 K를 가지고 있는지 검증한다.



〔그림 2〕 제안된 프로토콜 요약

〔그림 1〕에서 보여주는 바와 같이 SCH-3PEKE는 지수연산과 공개키 암·복호연산, 그리고 대칭키 암·복호연산을 기본으로 한다. 여기서 지수연산과 공개키 암·복호연산은 대칭키 암·복호연산이나 해쉬연산에 비해 연산의 오버헤드가 너무 크다. 그리고 SCH-3PEKE에서는 5번의 전체 메시지 전송을 요구한다. 그러므로 지수연산이나 공개키 암·복호연산보다 복잡도가 낮은 연산을 사용하고 메시지의 전송회수가 적은 새로운 프로토콜에 대한 연구가 필요하다.

Ⅲ. 제안한 키교환 프로토콜

본 장에서는 스마트카드를 이용하고 XOR과 해쉬함수 연산만으로 구성되는 효율적인 3자 참여 인증된 키교환 프로토콜을 제안한다. 제안한 프로토콜을 사용자 등록단계, 로그인단계, 키교환단계로 구별하여 설명한다.

사용자들은 서버에 로그인을 하기 위해 자신의 스마트카드를 서버에 미리 등록해야 하는데 그 과정을 알아보기 위해 사용자 A의 경우를 예를 들어 설명한다.

[등록단계]

Step 1. A는 랜덤 값 r을 선택하고 자신의 패스워드 PW를 이용하여 $h(r\oplus PW)$를 계산하고, 자신의 아이디 A와 함께 메시지 $\{A,h(r\oplus PW)\}$를 서버 S에게 전송한다.

Step 2. S는 자신의 비밀키 x_S를 이용하여 $R=h(A\oplus x_S)\oplus h(r\oplus PW)$를 계산하고, A에게 R과 $h()$가 저장된 스마트카드를 발급한다.

Step 3. A는 스마트카드에 랜덤 값 r을 저장하여 등록을 마친다.

사용자 A의 스마트카드에 R과 $h()$, 그리고 랜덤 값 r이 저장되어 있기 때문에 등록을 마친 사용자 A는 서버에 로그인 하고자 할 때 더 이상 랜덤 값 r을 기억할 필요가 없고 자신이 패스워드만 기억하면 된다.

[로그인단계]

Step 1. A가 자신의 아이디 A와 패스워드 PW를 입력하면 스마트카드는 $R\oplus h(r\oplus PW)$

연산을 하여 그 결과로 $c_1=h(A\oplus x_S)$를 생성한다. c_1과 랜덤 값 N을 이용하여 스마트카드는 S에게 메시지 $\{A, N, h(c_1\oplus N)\}$을 보낸다.

Step 2. S는 받은 메시지에서 아이디 A, 랜덤 값 N, 그리고 자신의 비밀키 x_S를 이용하여 $h(h(A\oplus x_S)\oplus N)$를 계산하여 받은 메시지 상의 $h(c_1\oplus N)$과 같으면 A의 로그인 요청을 수락하고 그렇지 않으면 요청을 거절한다.

서버 S에 등록되어 있는 사용자 A와 사용자 B가 서버에 로그인된 상태에서 안전하게 세션키를 공유할 수 있는 제안된 키교환 프로토콜은 다음과 같고, 이를 [그림 2]에 요약한다.

[키교환단계]

Step 1. A는 스마트카드의 c_1을 이용하여 $h(c_1\oplus N_A\oplus B)$를 계산하고, S에게 메시지 M_1을 보낸다. M_1에서 N_A는 랜덤 값이다.

$M_1 = \{N_A, A, B, h(c_1\oplus N_A\oplus B)\}$

Step 2. S는 M_1에 있는 A와 자신의 비밀키 x_S를 이용하여 $c_1=h(A\oplus x_S)$를 계산하고, 이것과 M_1에 포함된 N_A와 B를 이용하여 $h(c_1\oplus N_A\oplus B)$를 계산하여, 그 값이 M_1에 포함된 그것과 같으면 $c_2=h(B\oplus x_S)$와 $c_2'=h(c_2\oplus N_A\oplus A)$를 계산하고, 이들을 이용하여 $h(c_1\oplus N_A\oplus A\oplus B)\oplus h(c_2\oplus c_2')$를 계산하여 메시지 M_2를 B에게 보낸다.

$M_2 = \{N_A, A, c_2', h(c_1\oplus N_A\oplus A\oplus B)\oplus h(c_2\oplus c_2')\}$

Step 3. B는 스마트카드의 c_2와 M_2에 포함된 N_A와 A를 이용하여 $c_2'=h(c_2\oplus N_A\oplus A)$를 계산하고, 그 값이 M_2에 포함된 그것과 같으면 B는 세션키 K를 결정하고 메시지 M_3를 A에게 보낸다. M_3에서 $h(c_1\oplus N_A\oplus A\oplus B)\oplus K$는 M_2에 포함되어 있는 $h(c_1\oplus N_A\oplus A\oplus B)\oplus h(c_2\oplus c_2')$에 $h(c_2\oplus c_2')$와 세션키 K를 XOR하여 만든다.

$M_3 = \{B, h(c_1\oplus N_A\oplus A\oplus B)\oplus K, h(K)\}$

Step 4. A는 c_1, N_A, A, B를 이용하여 $h(c_1\oplus N_A\oplus A\oplus B)$를 계산하고, 그 결과와 M_3에 포함된 $h(c_1\oplus N_A\oplus A\oplus B)\oplus K$를 XOR하여 세션키 K를 추출한다. 그리고 $h(K)$를 계산하여 그 값이 M_3에 포함된 것과 같으면 A는 세션키 K가 B에 의해 생성되었고, 또한 그 값이 변조되지 않았음을 확신하고 메시지 M_4를 B에게 보낸다.

$M_4 = \{h(K-1)\}$

Step 5. B는 자신이 생성한 세션키 K를 이용하여 $h(K-1)$를 계산하고, 그 결과와 M_4가 같으면 B는 A가 바른 세션키를 가지고 있다고 확신한다.

Ⅳ. 안전성 분석

본 장에서는 본 논문에서 제안한 인증된 키교환 프로토콜의 암호학적 안정성을 분석한다. 제안한 프로토콜을 패스워드 추측공격(Password guessing attack), 서버 compromise 공격(Server compromise attack), 메시지 재전송 공격(Message replay attack), 위장공격(Impersonation attack)의 측면에서 안전성 분석을 한다.

[패스워드 추측공격]

패스워드 추측공격은 온라인과 오프라인 패스워드 추측공격으로 나눌 수 있다. 온라인 패스워드 추측공격은 인증 실패 횟수를 계산함으로써 쉽게 탐지되고 조치될 수 있으므로, 오프라인 패스워드 추측 공격에 대해서만 고려한다. 본 논문에서 제안한 프로토콜에서 패스워드를 획득할 수 있는 유일한 방법은 공격자가 합법적인 사용자에 대하여 도청한 메시지들 즉, M_1, M_2, M_3에 존재하는 c_1, c_2로부터 패스워드에 관한 정보를 유추하는 것이다. 그러나 이들 정보로부터 패스워드를 유추하는 것은 해쉬함수의 일방향성 때문에 불가능하다.

[서버의 비밀키 추측공격]

서버의 비밀키 추측공격 또한 패스워드 추측공격에서와 마찬가지로 공격자가 합법적인 사용자에 대하여 도청한 메시지들로부터 서버의 비밀키에 관한 정보를 유추하는 것이다. 그러나 이들 정보로부터 서버의 비밀키를 유추하는 것도 해쉬함수의 일방향성 때문에 불가능하다.

[메시지 재전송 공격]

만약 공격자가 이전 세션에서 획득한 메시지 M_1

〔표 2〕 제안된 프로토콜과 SCH-3PEKE의 성능 비교

프로토콜 \ 평가요소		계산비용						통신비용
		랜덤정수 생성회수	XOR 연산회수	지수 연산회수	공개키 연산회수	대칭키 연산회수	해쉬 연산회수	메시지 전송회수
SCH-3PEKE	사용자A	2	0	2	1	2	0	5
	서용자B	2	0	2	1	2	0	
	서버S	3	0	4	2	0	0	
제안된 프로토콜	사용자A	1	7	0	0	0	4	4
	서용자B	0	6	0	0	0	3	
	서버S	0	11	0	0	0	6	

를 가지고 A로 가장하고 S에게 그 메시지를 전송하고, B가 A에게 보내는 메시지 M_3를 가로챘다 하더라도 공격자는 세션키 K를 계산할 수 없다. 왜냐하면 K를 계산하기 위해서는 c_1을 계산해야 하고, c_1을 계산하기 위해서는 서버의 비밀키 x_S를 유추해야 하는데 해쉬함수의 일방향성으로 인해 불가능하기 때문이다. 공격자가 B로 가장하고 S에서 B로 보내지는 M_2를 가로챘다 하더라도 같은 원리에 의해 공격자는 세션키 K를 계산할 수 없다. 공격자가 세션키 K를 모르면 제안한 프로토콜에서의 메시지 재전송 공격은 성공하지 못한다. 그러므로 제안된 프로토콜은 메시지 재전송 공격으로부터 안전하다.

[위장공격]

적법한 사용자나 공격자가 타인을 위장하기 위해서는 위장하고자 하는 사용자의 아이디와 패스워드를 알아야 한다. 사용자의 아이디는 공개된 정보이기 때문에 쉽게 알 수 있지만, 사용자의 패스워드는 스마트카드에 $h(A \oplus x_s) \oplus h(r \oplus PW)$의 형태로 저장되어 있어서 해쉬함수의 일방향성으로 인해 추측하기 어렵고, 패스워드를 안다고 하더라도 스마트카드에 저장되어 있는 r과 서버의 비밀키 x_s의 유추는 역시 해쉬함수의 일방향성으로 인해 어려워 c_1을 계산해 낼 수 없으므로 위장공격은 불가능하다.

Ⅴ. 효율성 분석

본 장에서는 관련연구에서 소개한 프로토콜, SCH-3PEKE와 본 논문에서 제안한 프로토콜을 비교 분석하여 제안한 프로토콜의 효율성을 보인다. 프로토콜들의 성능 평가는 계산비용과 통신비용을 측정 비교하여 할 수 있다. 계산비용은 랜덤 값, XOR 연산, 지수연산, 공개키연산, 대칭키연산, 해쉬연산의 개수로 측정하고, 통신비용은 메시지 전송회수로 측정을 한다. 계산비용 중에서도 지수연산과 공개키연산은 다른 연산에 비해 수행시간이 매우 길기 때문에 이들 연산의 회수가 프로토콜의 성능에 매우 큰 영향을 미친다.

〔표 2〕는 제안된 프로토콜과 SCH-3PEKE와의 성능 비교를 보여주고 있다. SCH-3PEKE에서는 관련 연구에서 소개된 프로토콜을 최적화시킨 4라운드로 구성된 프로토콜도 소개하고 있으나, 그 프로토콜은 A와 B의 상호 인증을 제공하지 않으므로 비교 대상을 관련연구에서 소개된 프로토콜로 하였다. 〔표 2〕에서 알 수 있듯이, 제안된 프로토콜은 SCH-3PEKE에서 사용하지 않는 해쉬연산과 XOR 연산을 많이 사용하였지만, SCH-3PEKE에서의 주 연산인 지수연산, 공개키연산, 대칭키연산을 전혀 사용하지 않기 때문에 계산비용이 크게 향상될 뿐만 아니라, 메시지 전송회수도 SCH-3PEKE에 비해 하나 적기 때문에 통신비용도 향상됨을 알 수 있다.

Ⅵ. 결 론

본 논문에서는 동일한 서버에 등록되어 있는 두 사용자들에게 안전한 통신 서비스를 제공하기 위해 스마트카드를 사용한 패스워드 기반의 인증된 키교환 프로토콜을 제안하였다. 제안한 프로토콜은 계산비용이 큰 지수연산 및 공개키연산을 사용하지 않고,

XOR 및 해쉬연산를 주 연산으로 사용하고, 메시지 전송회수가 적기 때문에 기존의 프로토콜에 비해 계산비용이 훨씬 적고 또한 통신비용도 적으므로 매우 효율적으로 인증된 키 교환을 할 수 있음을 보였다. 그리고 제안된 기법은 패스워드를 서버에 저장하지 않으므로 패스워드 추측공격에 안전하고, 사용자들 간에 공유된 세션키를 서버가 알 수 없기 때문에 서버 Compromise 공격으로부터도 안전하다. 본 연구의 결과는 통신 참여자들의 계산 능력이 약한 경우에도 유용하게 사용될 수 있을 것이다.

참 고 문 헌

[1] W. Diffie and M.E. Hellman, "New directions in cryptography," *IEEE Trans.*, Vol. *IT-22*, No. 6, pp. 644-654, 1976.

[2] S. M. Bellovin and M. Merrit, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pp. 72-84, 1992.

[3] S.M. Bellovin and M. Merritt, "Augmented encrypted key exchange : a password-based protocol secure against dictionary attacks and password file compromise," *Technical report, AT&T Bell Laboratories*, 1994.

[4] T. Kwon and J. Song, "Secure agreement scheme for g^{xy} via password authentication," *Electronics Letters* Vol. 35, No. 11, pp.892-893, 1999.

[5] M. Steiner, G. Tsudik, and M. Waidner, "Refinement and extension of Encrypted Key Exchange," *ACM Operating Systems Review*, Vol. 29, No. 3, pp. 22-30, 1995.

[6] Y. Ding and P. Horster, "Undetectable on-line password guessing attacks," *ACM Operating Systems Review*, Vol. 29, No. 4, pp. 77-86, 1995.

[7] C. Lin, H. Sun, and T. Hwang, "Three-party encrypted key exchange: Attacks and a solution," *ACM Operating Systems Review*, Vol. 34, No. 4, pp. 12-20, 2000.

[8] C. Lin, H. Sun, M. Steiner, and T. Hwang, "Three-party Encrypted Key Exchange Without Server Public-Keys," *IEEE Communication Letters*, Vol. 5, No. 12, pp. 497-499, 2001.

[9] H. Sun, B. Chen, and T. Hwang, "Secure key agreement protocols for three-party against guessing attacks," *The Journal of Systems and Software*, Vol. 75, pp.63-68, 2005.

[10] W.C. Ku and S.M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," *IEEE Trans. on Consumer Electron.*, Vol. 50, No. 1, pp. 204-207, 2004.

〈著者紹介〉

전 일 수 (Il-Soo Jeon) 정회원
1984년 경북대학교 전자공학과(공학사)
1988년 경북대학교 대학원 전자공학과(공학석사)
1995년 경북대학교 대학원 전자공학과(공학박사)
1984년~1985년 삼성전자(주)
1989년~2004년 경일대학교 컴퓨터공학과 교수
2004년~현재 금오공과대학교 전자공학부 부교수
관심분야 : 정보보호, 보안 프로토콜
e-mail : isjeon@kumoh.ac.kr