情報保護學會論文誌
第15卷 第6號, 2005. 12

동일 서버를 사용하는 두 사용자간 효율적인 패스워드 기반의 키 교환 프로토콜*

이 성 운,[1†‡] 신 성 철[2]
[1]동명정보대학교, [2]해군사관학교

Efficient Password-based Key Exchange Protocol for Two Users Registered in a Server*

Sung-woon Lee,[1†‡] Seong-chul Shin[2]
[1]Tongmyong University, [2]Republic of Korea Naval Academy

요 약

본 논문에서는 동일한 서버에 등록되어 있는 두 사용자들 사이에 안전한 통신하는데 필요한 패스워드 기반의 키 교환 프로토콜을 제안하였다. 제안된 프로토콜에서 서버는 두 사용자가 적법한지를 인증하는 책임을 가질 뿐 그들 사이에 공유된 세션키를 알 수 없다. 제안된 프로토콜은 검증자 기반의 프로토콜로서 서버 Compromise 공격 뿐 아니라 다양한 공격들에 대하여 안전하고 완전한 전방향 보안성을 제공할 수 있다. 또한 서버의 공개키를 사용하지 않기 때문에 계산적인 면에서 효율적이다.

ABSTRACT

This paper presents a password-based key exchange protocol to guarantee secure communications for two users registered in a server. In this protocol, the server is only responsible for the legality of the users but does not know the session key agreed between them. The protocol can resist the various attacks including server compromise attack and provide the perfect forward secrecy. The proposed protocol is efficient in terms of computation cost because of not employing the server's public key.

Keywords : *Cryptography, Authentication, Password, Key exchange, Key agreement*

Ⅰ. 서 론

인터넷과 같은 공개된 통신망에서 안전하게 통신을 하기 위해서는 서로가 적법한지를 확인할 수 있는 인증과 전송 메시지들에 대한 암호화가 필요하다. 암호화를 위해서는 통신 참여자들 사이에 암호화키를 미리 공유하여야 한다. 사용자 인증을 위해 사람이 가진 소유, 사람이 알고 있는 지식, 사람 자신인 생체정보 중의 한 방법을 사용하거나 이들 중 몇 개를 혼합하여 보안을 강화할 수 있다. 패스워드를 이용한 인증은 사람이 알고 있는 지식을 확인하는 방법으로 여러 장점들로 인해 오래전부터 가장 널리 이용되고 있다. 그러나 이 방법은 사람이 보통 패스워드로 쉽게 기억할 수 있는 정보를 사용하기 때문

접수일 : 2005년 11월 9일 ; 채택일 : 2005년 12월 5일
* 이 논문은 2005학년도 동명정보대학교 학술연구비 지원에 의하여 이루어진 것임
† 주저자, ‡ 교신저자 : staroun@tit.ac.kr

에 사전공격이라고도 불리는 패스워드 추측 공격에 취약하기 쉽다. 몇몇 프로토콜들에서는 이 공격에 안전하도록 프로토콜을 설계하기 위하여 서버의 공개키를 추가적으로 사용하기도 한다. 그러나 이 방법은 클라이언트가 서버의 공개키를 얻고, 검증하고, 안전하게 보관해야 할 뿐 아니라 매우 많은 계산량을 요구하는 비대칭키 암호화 연산을 수행해야 하기 때문에 클라이언트에게 많은 부담을 주게 된다.

일반적으로 인증과 키 교환은 함께 제공되어야 하는데, 이러한 프로토콜을 인증된 키 교환 프로토콜(Authenticated key exchange)이라 한다. 1992년에 Bellovin과 Merrit[1]은 처음으로 패스워드만을 사용하여 패스워드 추측 공격에 안전한 EKE라는 패스워드 기반의 인증된 키 교환 프로토콜을 제안하였다. 그 이후로 다양한 환경에서 많은 프로토콜들이 제안되어 왔다. 패스워드 기반의 키 교환 프로토콜들은 참여자들의 수에 따라 두 참여자 환경, 세 참여자 환경, 그룹 참여자 환경 등으로 나뉠 수 있다. 본 논문에서는 세 참여자들이 프로토콜에 참여하는 환경에만 초점을 맞추고자 한다. 여기서 세 참여자란 한 서버와 이 서버에 등록된 두 클라이언트(사용자)들을 일컫는다. 즉 같은 서버에 자신의 아이디와 패스워드를 등록한 두 사용자가 각각 자신의 패스워드를 사용하여 서버와 상호 인증을 수행하고 세션키를 공유하려는 상황이다. 이때 서버는 두 사용자를 인증하고 그들이 세션키를 공유하도록 도울 뿐 생성된 세션키는 알 수 없기 때문에 두 사용자들 사이에 전송되는 메시지들은 안전하게 보호된다. 지금까지 이 환경에서 몇몇 프로토콜들이 제안되어 왔다.

Steiner[2]은 EKE 프로토콜을 토대로 하여 서버의 공개키를 사용하지 않는 STW-3PEKE라 불리는 세 참여자를 위한 프로토콜을 처음으로 제안하였다. Ding과 Horster[3]는 이 프로토콜이 참여자들이 탐지할 수 없는 온라인 패스워드 추측공격에 안전하지 않음을 보여주었다. 또한 Lin[4]은 STW-3PEKE이 오프라인 패스워드 추측 공격에도 취약하다는 것을 보여주고 서버의 공개키를 사용하여 LSH-3PEKE라 불리는 프로토콜을 제안하였다. 그 후에 Lin[5]은 다시 서버의 공개키를 사용하지 않는 LSSH-3PEKE 프로토콜을 제안하였다. 그러나 LSSH-3PEKE는 LSH-3PEKE 보다 두 번의 추가적인 메시지 교환을 요구한다. 그 후에 Chang[6]은 super-poly-to-one trapdoor라는 추가적인 함수를 사용하여 이 메시지 수를 감소시키는 ECC-3PEKE 프로토콜을 제안하였다. 그런데, 이러한 추가적인 함수의 사용은 프로토콜의 안전성을 떨어뜨릴 수 있을 수 있을 뿐만 아니라 프로토콜의 구조를 복잡하게 하여 구현 시 어렵게 할 수 있다. 한편 Sun[7]은 위의 프로토콜들과는 달리, 서버의 패스워드 파일에 사용자의 패스워드 자체 대신 패스워드로부터 유도된 검증자 값을 저장하는 첫 번째 검증자 기반의 프로토콜인 SCH-3PEKE를 제안하였다. 이러한 검증자 기반의 키 교환 프로토콜은 공격자가 서버의 패스워드 파일을 습득하더라도 바로 합법적인 사용자로 위장할 수 없다는 장점이 있다. 그러나 공격자는 습득한 검증자 값에 대하여 오프라인 패스워드 추측 공격을 수행하면 적은 노력으로 정확한 패스워드를 얻을 수 있다. 또한 이 프로토콜은 패스워드 추측 공격을 막기 위하여 서버의 공개키를 사용하기 때문에 효율적이지 못하다.

본 논문에서는 동일한 서버에 등록되어 있는 두 사용자들에게 안전한 통신 서비스를 제공하기 위한 패스워드 기반의 인증된 키 교환 프로토콜을 제안한다. 제안된 프로토콜은 패스워드 검증자 기반의 키 교환 프로토콜로서 서버 Compromise 공격 뿐 아니라 다양한 공격들에 대하여도 안전하고 완전한 전방향 보안성을 제공할 수 있다. 또한 본 논문에서는 제안된 프로토콜을 간단히 수정함으로써 서버에 저장된 패스워드 파일의 노출에도 패스워드 추측 공격에 안전한 프로토콜을 제시하였다. 이때 사용자들은 안전한 저장장치를 소유해야 한다. 제안된 프로토콜에서 서버는 두 사용자들 사이에 공유된 세션키를 알 수 없기 때문에 사용자들 사이의 통신은 매우 안전하게 유지될 수 있다. 더욱이 서버의 공개키를 사용하지 않고 패스워드 추측공격을 막을 수 있기 때문에 성능 면에서 매우 효율적이다.

II. 관련연구

여기서는 세 참여자들을 위한 프로토콜들 중에서 제안된 프로토콜과 비슷한 환경에서 제안되었던 검증자 기반의 키 교환 프로토콜인 SCH-3PEKE 프로토콜에 대하여 살펴본다. Alice와 Bob은 각각 서버에 검증자 값 $v_A = g^{\pi_A}$와 $v_B = g^{\pi_B}$를 저장하고 있다고 가정하자. 여기서 x_A와 x_B는 Alice와 Bob의 패스워드 π_A와 π_B로부터 계산된 비밀 값들이다. SCH-3PEKE 프로토콜은 다음과 같이 수행된다.

① Alice는 π_A로부터 x_A를 계산한 후 $v_A = g^{x_A}$를 계산한다. 그리고 임의의 정수 a를 선택하

여 g^a를 계산한다. 또한 서버의 공개키 P_K를 사용하여 비대칭키 암호화 연산을 수행함으로써 $X_A = P_K\{A, g^a, v_A\}$를 계산한 후 X_A를 Bob에게 전송한다.

② Bob은 π_B로부터 x_B를 계산한 후 $v_B = g^{x_B}$를 계산한다. 그리고 임의의 정수 b를 선택하여 g^b를 계산한다. 또한 서버의 공개키 P_K를 사용하여 $X_B = P_K\{B, g^b, v_B\}$를 계산한 후 X_A와 X_B를 Bob에게 전송한다.

③ 서버는 Bob으로부터 X_A와 X_B를 받은 후에 자신의 비밀키로 비대칭키 복호화 연산을 수행하여 복호화하고 v_A와 v_B이 정확한지를 검사한다. 이 값들이 정확하다면 서버는 임의의 정수 c, d, e를 선택하여 $X_{SA} = (g^{bc} \cdot v_B)^e$와 $X_{SB} = (g^{ad} \cdot v_A)^e$를 계산하고 X_{SA}, X_{SB}, c, d를 Alice에게 전송한다.

④ Alice는 세션키 $K = (X_{SA})^{ad+x_A} = g^{(bc+x_B)(ad+x_A)e}$를 계산한다. 그리고 K를 키로 대칭키 암호화 연산을 수행하여 $V_{AB} = K\{X_A\}$를 계산한 후 V_{AB}를 Bob에게 전송한다.

⑤ Bob은 세션키 $K = (X_{SB})^{bc+x_B} = g^{(bc+x_B)(ad+x_A)e}$를 계산하고 K를 키로 대칭키 복호화 연산을 수행하여 V_{AB}를 복호화한 후 X_A가 정확한지를 확인한다. 그리고 $V_{BA} = K\{V_{AB}\}$를 계산하여 V_{BA}를 Alice에게 전송한다.

⑥ 마지막으로, Alice는 V_{BA}를 검사하여 Bob이 정확한 세션키 K를 얻었는지를 확인한다.

SCH-3PEKE는 패스워드 추측 공격에 안전하도록 하기 위하여 클라이언트들이 서버의 공개키를 사용하여 비대칭키 암호화 연산을 수행하도록 설계하였기 때문에 클라이언트들에게 많은 부담이 될 수 있다.

Ⅲ. 제안된 프로토콜

1. 시스템 파라미터

먼저 프로토콜에서 사용할 시스템 파라미터들을 정의한다. k와 l은 보안 파라미터들이라 하자. k는 해쉬 함수들과 세션키를 위한 160비트 크기이고 l은 1024비트 또는 2048비트 크기이다. p와 q는 각각 q와 서로소인 임의의 r에 대해 $p = rq + 1$을 만족하는 l과 k 크기의 값들이고, G_q는 곱셈군 Z_p^*의 위수 q를 갖는 부분군, g는 G_q의 생성자라 하자. 프로토콜 기술 중에 'mod p' 표기는 생략하기로 한다. 한편, $\{0, 1\}^*$는 유한한 이진 문자열의 집합이고, $\{0, 1\}^n$는 길이가 n인 이진 문자열의 집합이라 하자. 충돌이 없는 일방향 해쉬 함수 h는 h: $\{0, 1\}^* \rightarrow \{0, 1\}^n$로 표기될 수 있다. 이것은 임의의 길이의 문자열을 필요한 길이의 문자열로 변환할 수 있다. 추가적인 해쉬 함수 h'는 h를 이용하여 쉽게 만들어질 수 있다. 예를 들어 $h'(x) = h('00', x)$.

표 1. 표기

기호	설명
p	큰 소수 (보통 1024 또는 2048비트)
q	$q\|(p-1)$을 만족하는 상대적으로 작은 소수 (보통 160비트)
G_q	위수 q를 갖는 Z_p^*의 부분군
g	G_q의 생성자
A, B, S	각각 Alice, Bob, 서버의 아이디
$h(\cdot)$, $h'(\cdot)$	충돌이 없는 일방향 해쉬 함수
$\oplus$	비트 Exclusive-OR 연산
π_A, π_B	각각 Alice와 Bob의 패스워드
x_A, v_A, x_B, v_B	각각 서버에 저장되는 Alice와 Bob의 검증자 값
a, b, c, d, e	G_q의 원소인 랜덤 정수
K	세션키
$\rightarrow$	메시지 전송
$\approx$	두 값이 같은지를 비교

2. 3PAKE 프로토콜

제안된 프로토콜에서 동일한 서버에 등록되어 있는 두 사용자 Alice와 Bob은 안전한 통신을 하기 위하여 자신들만이 아는 세션키를 공유하고자 한다. Alice와 Bob은 프로토콜이 시작하기 전에 다음과 같은 과정을 통해 서버에 등록한다.

① Alice는 패스워드 π_A를 선택한 후에 $x_A = h'(A, S, \pi_A)$, $v_A = g^{h(A,S,\pi_A)^{-1}}$를 계산하고 x_A와 v_A를 안전한 채널을 통해 서버에 전송한다.

② Bob은 패스워드 π_B를 선택한 후에 $x_B = h'(B, S, \pi_B)$, $v_B = g^{h(B,S,\pi_B)^{-1}}$를 계산하고 x_B와 v_B를 안전한 채널을 통해 서버에 전송한다.

③ 서버는 Alice와 Bob을 위하여 x_A, v_A와 x_B, v_B를 패스워드 파일에 저장한다.

제안된 3PAKE 프로토콜은 동일한 서버에 등록되

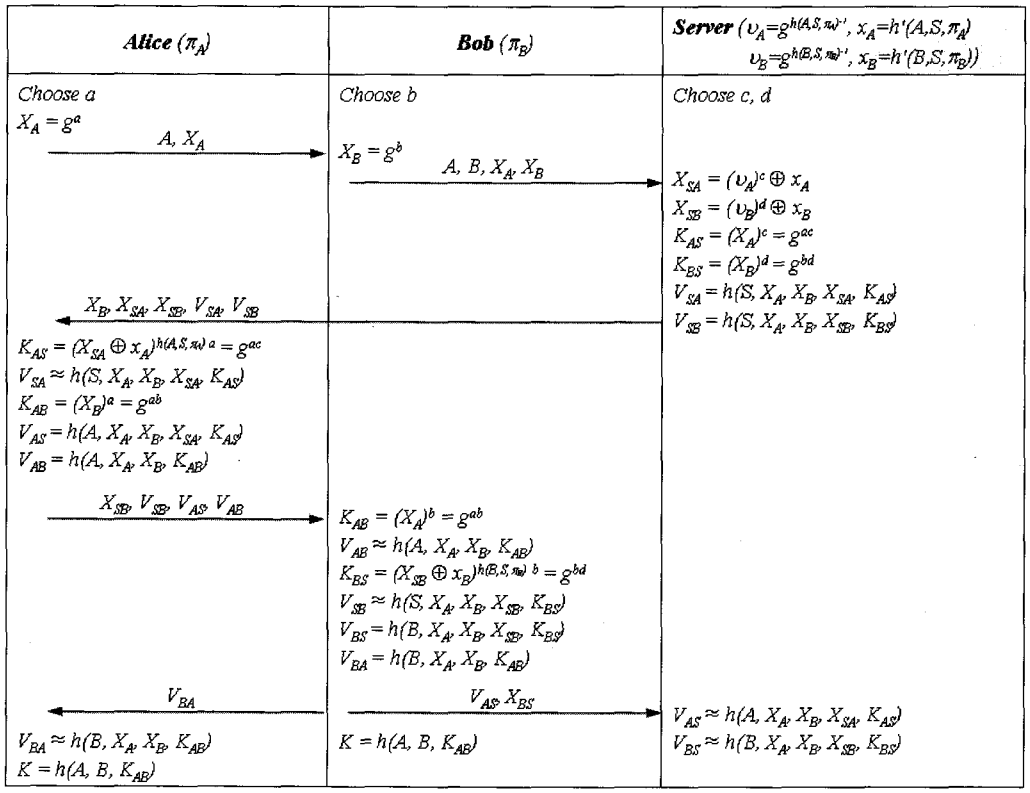


그림 1. 3PAKE 프로토콜

어 있는 Alice와 Bob 사이에 같은 세션키 K를 공유하도록 하기 위하여 다음과 같은 과정을 수행한다.

① Alice는 $a \in_R G_q$를 선택하고 $X_A = g^a$를 계산하여 Bob에게 A, X_A를 전송한다.

② Bob은 $b \in_R G_q$를 선택하고 $X_B = g^b$를 계산하여 A, B, X_A, X_B를 서버에 전송한다.

③ 서버는 패스워드 파일로부터 v_A, x_A, v_B, x_B를 검색하고 c, $d \in_R G_q$를 선택하여 $X_{SA} = (v_A)^c \oplus x_A$, $X_{SB} = (v_B)^d \oplus x_B$, $K_{AS} = (X_A)^c = g^{ac}$, $K_{BS} = (X_B)^d = g^{bd}$, $V_{SA} = h(S, X_A, X_B, X_{SA}, K_{AS})$, $V_{SB} = h(S, X_A, X_B, X_{SB}, K_{BS})$를 순서대로 계산한다. 그리고 X_B, X_{SA}, X_{SB}, V_{SA}, V_{SB}를 Alice에게 전송한다.

④ Alice는 $K_{AS} = (X_{SA} \oplus x_A)^{h(A,S,\pi_A)\cdot a} = g^{ac}$를 계산하고 $V_{SA} \approx h(S, X_A, X_B, X_{SA}, K_{AS})$를 검사함으로 서버를 인증한다. 그리고 $K_{AB} = (X_B)^a = g^{ab}$, $V_{AS} = h(A, X_A, X_B, X_{SA}, K_{AS})$, $V_{AB} = h(A, X_A, X_B, K_{AB})$를 순서대로 계산하고 X_{SB}, V_{SB}, V_{AS}, V_{AB}를 Bob에게 전송한다.

⑤ Bob은 $K_{AB} = (X_A)^b = g^{ab}$를 계산하고 $V_{AB} \approx h(A, X_A, X_B, K_{AB})$를 검사하여 Alice를 인증한다. 또한 $K_{BS} = (X_{SB} \oplus x_B)^{h(B,S,\pi_B)\cdot b} = g^{bd}$계산하고 $V_{SB} \approx h(S, X_A, X_B, X_{SB}, K_{BS})$를 검사하여 서버를 인증한다. 그리고 $V_{BS} = h(B, X_A, X_B, X_{SB}, K_{BS})$와 $V_{BA} = h(B, X_A, X_B, K_{AB})$를 계산하여 V_{AS}, V_{BS}를 서버에 전송하고 V_{BA}를 Alice에게 전송한 후 세션키 $K = h(A, B, K_{AB})$를 계산한다.

⑥ 서버는 $V_{AS} \approx h(A, X_A, X_B, X_{SA}, K_{AS})$와 $V_{BS} \approx h(B, X_A, X_B, X_{SB}, K_{BS})$를 검사하여 Alice와 Bob을 인증한다.

⑦ Alice는 $V_{BA} \approx h(B, X_A, X_B, K_{AB})$를 검사하여 Alice를 인증한 후 세션키 $K = h(A, B, K_{AB})$를 계산한다.

제안된 프로토콜에서 세 참여자들은 상호간에, 즉 Alice와 Server, Bob과 Server, Alice와 Bob 사이에

상호 인증을 수행한다. 서버는 V_{AS}와 V_{BS} 값들을 검사함으로써 Alice와 Bob이 정당한 사용자들인지를 인증할 수 있다. 이것은 Alice와 Bob이 각각 자신의 정확한 패스워드를 사용해야 만이 서버에서 계산한 $K_{AS} = g^{ac}$, $K_{BS} = g^{bd}$와 같은 값들을 계산할 수 있기 때문이다. 비슷하게 Alice와 Bob은 각각 V_{SA}와 V_{SB}를 검사함으로써 서버의 적법성을 인증하고 V_{AB}와 V_{BA}를 검사함으로써 서로를 인증하게 된다. 이러한 인증 과정들이 성공적으로 끝나면 Alice와 Bob은 세션키 $K = h(A, B, K_{AB})$를 계산하고 프로토콜을 종료한다.

추가적으로, 제안된 프로토콜은 사용자가 패스워드 이외에 USB 토큰 같은 추가적인 휴대용 안전한 저장장치를 사용하게 하여 사용자의 안전성을 강화할 수 있다. 이를 위해 Alice와 Bob은 서버에 등록할 때에 각각 임의의 정수 s_A와 s_B를 선택하여 $x_A = h'(A, S, s_A, \pi_A)$, $v_A = g^{h(A,S,s_A,\pi_A)^{-1}}$, $x_B = h'(B, S, s_B, \pi_B)$, $v_B = g^{h(B,S,s_B,\pi_B)^{-1}}$를 계산하고 이들을 안전한 채널을 통해 서버에 저장한다. 또한 자신들의 안전한 저장 장치에도 각각 s_A, x_A와 s_B, x_B를 저장하여 등록을 마친다. 그리고 프로토콜 수행 중에 Alice와 Bob은 각각 $K_{AS} = (X_{SA} \oplus x_A)^{h(A,S,s_A,\pi_A)a}$, $K_{BS} = (X_{SB} \oplus x_B)^{h(B,S,s_B,\pi_B)b}$와 같이 K_{AS}와 K_{BS}를 계산한다. 그러면 공격자가 서버의 패스워드 파일을 습득하여 패스워드 추측 공격을 수행한다할지라도 패스워드에 관한 정보를 전혀 얻을 수 없다.

Ⅳ. 안전성 분석

프로토콜에 참여하는 참여자들 사이의 모든 통신은 공격자의 통제 하에 있다고 가정하자. 즉 공격자는 정당한 사용자들이 전송하는 메시지들을 읽을 수 있고, 메시지를 수정하여 전송하기도 하고, 그들에게 새로운 메시지를 보낼 수도 있으며 메시지를 연착시키거나 이전 메시지들을 재전송하여 공격을 수행할 수도 있다. 제안된 프로토콜의 안전성은 산술시간에 풀기 어렵다고 알려져 있는 이산대수 문제와 Diffie-Hellman 문제의 어려움, 그리고 사용되는 해쉬 함수의 암호학적 강도에 근거한다. 다음에서 제안된 프로토콜이 여러 종류의 공격들에 안전함을 보이고자 한다.

① 수동적이고 적극적인 공격들에 대하여 안전하다.

공격자가 수동적인 공격, 즉 전송되는 메시지들을 도청하였다면 X_A, X_B, X_{SA}, X_{SB}, V_{SA}, V_{SB}, V_{AS}, V_{BS}, V_{AB}, V_{BA} 값들을 얻을 수 있다. 그러나 이 값들로부터 패스워드 π_A, π_B나 세션키 K에 대한 정보를 얻을 확률은 사용된 해쉬 함수의 특성들과 이산대수문제, 그리고 Diffie-Hellman 문제의 어려움 때문에 무시할만하다. 공격자가 적극적인 공격자라면 공격자는 Alice와 Bob이 올바르지 않는 값을 세션키로 받아드리도록 하기 위해 메시지를 수정하거나 그들에게 새로운 메시지를 보낼 수도 있으며 메시지를 연착시키거나 이전 메시지들을 재전송하여 공격을 수행할 수도 있다. 공격자는 이러한 공격을 통하여 많은 정보를 얻을 수 있지만 그러나 이러한 공격이 성공할 확률은 수동적인 공격과 비슷하게 무시할만하다.

② 오프라인 패스워드 추측 공격에 대하여 안전하다.

공격자는 오프라인 패스워드 추측 공격을 수행하기 위하여 메시지들을 도청하거나, Alice나 Bob, 그리고 서버로 위장하여 정보들을 수집한다. 그리고 패스워드 후보자 π'를 추측하고 도청한 값들을 이용하여 π'가 정확한 패스워드인지를 검증해야 한다. 그러나 제안된 프로토콜에서 이 공격이 성공할 확률은 사용된 해쉬 함수의 특성들과 이산대수문제, 그리고 Diffie- Hellman 문제의 어려움 때문에 무시할만하다.

③ Denning-Sacco 공격에 대하여 안전하다.

Denning-Sacco 공격에 안전하기 위해서는 공격자가 이전의 세션키를 안다 할지라도 사용자의 패스워드를 구할 수 없어야 한다. 공격자가 세션키 K를 안다고 가정하자. 공격자는 이 값과 이전 세션에서 도청한 X_A, X_B, X_{SA}, X_{SB}, V_{SA}, V_{SB}, V_{AS}, V_{BS}, V_{AB}, V_{BA} 값들을 이용하여 패스워드 π를 직접 계산하려 하거나 오프라인 패스워드 추측 공격을 수행하려 할 것이다. 그러나 이것이 성공할 확률은 사용된 해쉬 함수의 특성들과 이산대수문제, 그리고 Diffie-Hellman 문제의 어려움 때문에 무시할만하다.

④ 완전한 전방향 보안성을 제공한다.

완전한 전방향 보안성은 공격자가 임의의 시점에 패스워드를 알게 된다할 지라도 이전 세션키들을 계산할 수 없을 때 제공된다. 공격자가 π_A나 π_B를 안다고 가정하자. 공격자는 이 값과 이전 세션에서 도청한 정보 X_A, X_B, X_{SA}, X_{SB}, V_{SA}, V_{SB}, V_{AS}, V_{BS}, V_{AB}, V_{BA} 값들을 이용하여 이전 세션키를 얻으려고 할 것이다. 그러나 이것이 성공할 확률은 해쉬 함수의 특성들과 이산대수문제, 그리고 Diffie-Hellman 문제의 어려움 때문에 무시할만하다.

표 2. SCH-3PEKE 프로토콜과의 성능 비교

프로토콜 \ 비교요소		랜덤 정수	비대칭 키연산	지수 연산	대칭키 연산	해쉬 연산	메시지
SCH-3PEKE	A	2	1	2	2	1	
	B	2	1	2	2	1	5
	S	3	2	4	0	0	
3PAKE	A	1	0	3	0	6	
	B	1	0	3	0	6	6
	S	2	0	4	0	4	

⑤ 서버 Compromise 공격에 대하여 안전하다.

프로토콜이 서버 Compromise 공격에 안전하기 위해서는 공격자가 서버의 패스워드 파일에 저장되어 있는 사용자의 검증자 값을 얻었다할지라도 그 값을 바로 이용하여 그 사용자로 위장할 수 없어야 한다. 공격자가 Alice의 검증자 $x_A = h'(A, S, \pi_A)$, $v_A = g^{h(A,S,\pi_A)^{-1}}$를 안다고 가정하자. 공격자가 Alice로 위장하기 위해서는 정확한 K_{AS}와 V_{AS}를 계산해서 서버의 검증을 통과할 수 있어야 한다. 그러나 공격자는 $h(A, S, \pi_A)$를 알지 못하기 때문에 정확한 K_{AS}를 계산할 수 없고 결국 서버의 인증을 통과할 수 없다.

⑥ 서버는 세션키 K를 알 수 없다.

제안된 프로토콜에서 서버는 c, d, X_A, X_B, X_{SA}, X_{SB}, V_{SA}, V_{SB}, V_{AS}, V_{BS} 값들을 알 수 있다. 그러나 이들로부터 $K_{AB} = g^{ab}$를 계산할 확률은 해쉬 함수의 특성과 이산대수문제, 그리고 Diffie-Hellman 문제의 어려움 때문에 무시할만하다. 그러므로 서버는 세션키 K를 알기 어렵다.

V. 효율성 분석

여기서는 제안된 프로토콜의 성능을 검증자 기반의 프로토콜인 SCH-3PEKE 프로토콜과 비교하고자 한다. 일반적으로 비대칭키 연산과 지수연산은 다른 연산들에 비해 상대적으로 수행시간이 매우 길기 때문에 프로토콜의 성능에 가장 큰 영향을 미친다고 할 수 있다. 또한 지수연산은 160비트 연산을 수행하기 때문에 1024비트 또는 2048 비트 연산을 수행하는 비대칭키 연산에 비해 몇 배 빠르다. 표 2는 제안된 프로토콜인 3PAKE가 대칭키 연산과 비대칭키 연산을 전혀 사용하지 않기 때문에 SCH-3PEKE에 비해 구조적으로 단순하고 성능 면에서 효율적임을 보여준다.

VI. 결 론

본 논문에서는 같은 서버에 등록되어 있는 두 사용자들 사이에 안전하게 키를 공유할 수 있도록 해주는 패스워드 기반의 키 교환 프로토콜을 제안하였다. 또한 제안된 프로토콜에 대한 간단한 수정을 통하여 사용자는 패스워드 이외에 추가적인 안전한 저장장치를 사용함으로써 좀더 강화된 안전성을 제공받을 수 있다. 제안된 프로토콜은 여러 종류의 다양한 공격에 안전할 뿐만 아니라 완전한 전향 보안성을 제공한다. 더욱이 사용자들 사이에 공유된 세션키는 서버라 할지라도 알 수 없어 사용자들 사이에 통신 기밀성은 완전하게 보장된다. 특히 제안된 프로토콜은 서버의 공개키를 사용하지 않기 때문에 비슷한 환경에 있는 기존 프로토콜에 비해 성능 면에서 효율적이며 한 서버에 등록되어 있는 사용자들 사이에 안전한 통신을 필요로 하는 많은 응용들에 사용될 수 있다.

참 고 문 헌

[1] 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.

[2] 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.

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

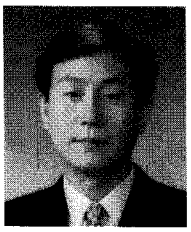
[4] C. Lin, H. Sun, and T. Hwang, "Three-party encrypted key exchange: Attacks and a solution," *ACM Operating Systems Review*, vol. 34, no. 4, pp. 12-20, 2000.

[5] 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.
[6] C. Chang and Y. Chang, "A novel three-party encrypted key exchange protocol," *Computer Standards & Interfaces*, vol. 26, no. 5, pp. 471-476, 2004.
[7] 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, no. 1-2, pp. 63-68, 2005.

〈著者紹介〉

이 성 운 (Sung-woon Lee)
1993년 8월 : 전남대학교 전산통계학과 졸업
1996년 8월 : 전남대학교 전산통계학과 석사
2005년 2월 : 경북대학교 컴퓨터공학과 박사
2005년 3월~현재: 동명정보대학교 정보보호학과 교수
〈관심분야〉 정보보호, 암호학, 암호프로토콜, 네트워크 보안



신 성 철 (Seong-chul Shin)
1983년 2월 : 전남대학교 계산통계학과 졸업
1988년 8월 : 전남대학교 전산통계학과 석사
1995년 2월 : 전남대학교 전산통계학과 박사
1983년 3월~1986년 7월: 육군군수사령부 전산실
1989년 3월~1992년 2월: 송원전문대학 전자계산과 교수
1995년 9월~현재: 해군사관학교 전산과학과 교수
〈관심분야〉 트랜잭션관리, 이동컴퓨팅, 정보보호