情報保護學會論文誌
第13券 第5號, 2003. 10

간단하고 효율적인 상호 인증 키 동의 프로토콜*

이 성 운**, 유 기 영**

Simple and Efficient Authenticated Key Agreement Protocol

Sung-Woon Lee**, Kee-Young Yoo**

요 약

본 논문에서는 두 참여자들 사이에 서로를 인증하고 세션키를 공유하기 위하여 패스워드를 이용하는 간단하고 효율적인 두 가지 키 동의 프로토콜(SEKA-H, SEKA-E)을 제안한다. SEKA-H 프로토콜은 프로토콜을 수행하는 중에 공유된 세션키를 검증하기 위해 해쉬 함수를 사용한다. 그리고 SEKA-E 프로토콜은 SEKA-H 프로토콜의 변형으로써 세션키 검증을 위해서 지수 연산을 사용한다. 제안된 프로토콜들은 중간 침입자 공격과 패스워드 추측 공격, 그리고 Denning-Sacco 공격에 안전하고 완전한 전방향 보안성을 제공한다. SEKA-H 프로토콜은 기존에 잘 알려진 프로토콜들과 비교하여 구조가 매우 간단하며 좋은 효율성을 갖는다. SEKA-E 프로토콜은 다른 프로토콜들과 비교하여 비슷한 전체 수행 시간을 필요로 한다.

ABSTRACT

In this paper, we propose two simple and efficient key agreement protocols, called SEKA-H and SEKA-E, which use a pre-shared password between two parties for mutual authentication and agreeing a common session key. The SEKA-H protocol uses a hash function to verify an agreed session key. The SEKA-E protocol, a variant of SEKA-H, uses an exponentiation operation in the verification phase. They are secure against the man-in-the-middle attack, the password guessing attack, and the Denning-Sacco attack, and provide the perfect forward secrecy. The SEKA-H protocol is very simple in structure and provides good efficiency compared with other well-known protocols. The SEKA-E protocol is also comparable with the previous protocols.

keyword : *Password, Authentication, Key exchange, Key agreement*

Ⅰ. 서 론

인터넷과 같은 공개된 통신망을 통하여 안전하게 통신을 하기 위해서는 전송하려는 정보를 암호화하여야 한다. 전송할 자료를 암호화하기 위해서는 통신 참여자들 간에 공통으로 사용하기 위한 세션키를 공유해야 하고, 통신하고 있는 상대가 정확한지를 확인할 수 있어야 한다. 따라서 참여자들이 서로를 인증하면서 그들 사이에 세션키를 공유할 수 있는 키 동의 프로토콜의 개발이 필요하다.

1976년에 제안된 Diffie-Hellman 키 동의 프로토콜(Key agreement protocol)은 안전하지 않은 통신상에서 세션키를 공유하기 위한 가장 잘 알려진 방법이다.[1] 이 프로토콜은 유한 필드 상에서 이산대수 문제와 Diffie-Hellman문제의 어려움을 이용하여 참여자들 간에 세션키를 공유한다. 하지만 참여자들을 인증

* 본 연구는 두뇌한국21 사업의 지원으로 수행하였습니다.
** 경북대학교 컴퓨터공학과(staroun@infosec.knu.ac.kr, yook@knu.ac.kr)

하는 방법을 제공하지 않기 때문에 중간 침입자 공격(Man-in-the-middle attack)에 취약하였다. 참여자 인증을 위한 기술들은 다음과 같은 세가지 범주로 크게 나뉠 수 있다: (1) 패스워드와 같은 사용자가 알고 있는 지식을 통한 인증, (2) 지문이나 홍채와 같은 사용자의 물리적인 특징을 통한 인증, (3) 스마트 카드와 같은 사용자가 소유한 물건을 통한 인증. 이러한 방법 중에서 첫 번째 범주는 간단성, 편의성, 적응성, 이동성, 그리고 하드웨어 사용의 불필요 등의 장점을 가지고 있기 때문에 가장 널리 이용되는 방법이다.

그러나 일반적으로 사람들은 쉽게 기억할 수 있는 패스워드를 선택하는 경향이 있다. 이 때문에 세션키 공유를 위하여 메시지 교환 중에 패스워드를 검증할 수 있는 정보가 공격자에게 노출되면 패스워드 추측 공격(Password guessing attack)을 당할 위험이 있다. 패스워드 추측 공격은 패스워드를 사용하는 프로토콜들에게는 가장 큰 위협이다. 이 문제를 해결하기 위하여 1992년에 Bellovin과 Merritt는 낮은 엔트로피를 가진(사람이 기억할 수 있는) 패스워드를 기반으로 대칭키 및 공개키 암호화 알고리즘들을 사용하여 EKE 프로토콜을 제안하였다.[2] 그 이후 이러한 패스워드 기반의 인증된 키 동의 프로토콜들이 다양하게 제안되었다.[3~10]

본 논문에서는 두 참여자들 사이에 서로를 인증하고 세션키를 공유하기 위하여 패스워드를 이용하는 간단하고 효율적인 두 가지 키 동의 프로토콜(SEKA-H, SEKA-E)을 제안한다. SEKA-H 프로토콜은 프로토콜을 수행하는 중에 공유된 세션키를 검증하기 위해 해쉬 함수를 사용한다. 그리고 SEKA-E 프로토콜은 SEKA-H 프로토콜의 변형으로써 세션키 검증을 위해서 지수 연산을 사용한다. 제안된 프로토콜들은 중간 침입자 공격과 패스워드 추측 공격, 그리고 Denning-Sacco 공격에 안전하고 완전한 전방향 보안성을 제공한다. SEKA-H 프로토콜은 기존에 잘 알려진 프로토콜들과 비교하여 구조가 간단하여 이해하기 쉽고 좋은 효율성을 제공한다. SEKA -E 프로토콜은 다른 프로토콜들과 비교하여 비슷한 전체 수행시간을 필요로 한다.

본 논문의 구성은 다음과 같다. 2장에서는 패스워드 기반의 안전한 키 동의 프로토콜을 설계하기 위하여 만족시켜야 할 보안 요구 사항들을 기술한다. 3장에서는 두 개의 키 동의 프로토콜들을 제안하고 4장에서는 제안된 프로토콜들에 대한 안전성을 분석한다. 5장에서는 제안된 프로토콜들의 효율성을 분석하고, 마지막으로 6장에서는 결론을 맺는다.

II. 보안 요구사항

본 장에서는 패스워드 기반의 키 동의 프로토콜들이 만족시켜야 할 보안 요구 사항들을 기술한다. 안전한 패스워드 기반의 키 동의 프로토콜을 설계하기 위해서는 다음과 같은 보안 요구 사항들이 고려되어야 한다.[10]

• 중간 침입자 공격에 안전해야 한다.

키 동의 프로토콜은 안전하지 않은 통신망에서 메시지 교환을 통하여 세션키를 공유하고 서로를 인증한다. 그래서 공격자는 통신 선로 중간에서 전송 메시지들을 도청(Eavesdropping)하여 세션키의 정보를 알아내려고 한다. 그리고 전송 메시지들을 변경(Modifying), 반송(Reflecting), 또는 이전 세션의 메시지들을 저장해 두었다가 다음 세션들에서 재전송(Replay)하는 방법 등으로 참여자들이 알지 못한 상태에서 잘못된 세션키를 공유하도록 유도할 수도 있다. 또한 공격자는 정당한 참여자로 위장(Masquerading)하여 다른 정당한 참여자와 정상적인 방법으로 세션키를 공유하려고 할 수 있다. 키 동의 프로토콜은 이러한 공격들에도 세션키에 관한 정보를 노출시켜서는 안되며 잘못된 세션키의 공유를 탐지할 수 있어야 한다.

• 패스워드 추측 공격에 안전해야 한다.

패스워드 추측 공격은 온라인 패스워드 추측 공격과 오프라인 패스워드 추측 공격으로 나뉠 수 있다. 온라인 패스워드 추측 공격은 패스워드 인증 실패 횟수를 누적함으로써 쉽게 탐지되고 시도 횟수를 제한함으로써 쉽게 조치될 수 있다. 그러나 공격자는 안전하지 않은 통신상의 메시지를 가로채거나 정당한 사용자로 위장하여 다른 사용자와 세션키를 공유하는 과정 중에 발생하는 정보들을 저장해두고 오프라인으로 패스워드에 관한 정보를 알아내려고 할 수 있다. 이러한 공격을 오프라인 패스워드 추측 공격이라 한다. 오프라인 패스워드 추측 공격은 사용자가 쉽게 기억할 수 있도록 낮은 엔트로피를 가진 패스워드를 사용하는 패스워드 기반의 키 동의 프로토콜들에 있어서 가장 큰 위협이다. 그러므로 패스워드 기반의 키 동의 프로토콜은 패스워드 추측 공격에

안전하도록 설계되어야 한다.

• Denning-Sacco 공격에 안전해야 한다.

Denning-Sacco 공격은 세션키가 노출되었을 때 공격자가 그 동안 통신상에서 도청한 메시지들을 이용하여 패스워드에 관한 정보를 얻고자 하는 공격이다. 패스워드 기반의 키 동의 프로토콜은 이러한 공격에 안전해야 한다.

• 완전한 전방향 보안성을 제공해야 한다.

공격자가 참여자의 패스워드를 알아내었다 할지라도 이전에 사용된 세션키에 관한 정보는 알 수 없어야 한다. 이러한 성질을 완전한 전방향 보안성이라 한다. 패스워드 기반의 키 동의 프로토콜은 이러한 성질을 만족해야 한다.

Ⅲ. SEKA(Simple and Efficient Authenticated Key Agreement Protocol)

본 장에서는 Diffie-Hellman 키 동의 프로토콜을 기반으로 사람이 기억할 수 있는 패스워드를 이용하여 참여자들 사이에 서로를 인증하고 세션키를 공유할 수 있는 두 가지 키 동의 프로토콜들(SEKA-H, SEKA-E)을 제안한다.

3.1 용어정의

제안된 프로토콜들에서 사용할 표기들을 [표 1]과 같이 정의한다.

[표 1] 표기

A, B	각 참여자들
p	큰 소수
g	곱셈군(multiplicative group) Z_p^*상의 생성자(generator)
P	패스워드
P^{-1}	곱셈군 Z_p^*상에서 패스워드 P의 역수
$h()$	강한 일방향 해쉬 함수(strong one-way hash function)
a, b	각 참여자들에 의해 선택된 Z_p^*상의 임의의 원소
K	세션키
$\oplus$	비트 XOR 연산
k	보안 파라미터

3.2 SEKA-H 프로토콜

SEKA-H 프로토콜에서는 랜덤 오라클[11]이라는 해쉬 함수 $h() : \{0,1\}^* \rightarrow \{0,1\}^k$를 사용한다. 보안 파라미터 k는 해쉬 함수의 출력 값의 비트 크기이며 Brute-force 공격을 막을 수 있을 만큼 충분히 큰 크기를 가져야 한다. 또한 $\{0,1\}^*$는 임의의 길이를 갖는 유한한 이진 문자열이고 $\{0,1\}^k$는 k의 길이를 갖는 이진 문자열을 나타낸다. 프로토콜의 참여자인 A와 B는 합법적인 사용자들이다. A와 B는 Z_p^*상의 생성자인 g, 큰 소수인 p, 그리고 사람이 기억할 수 있는 패스워드 P를 안전하게 미리 공유하고 있다고 가정한다. 'mod p' 연산 표기는 생략하기로 한다. 제안된 프로토콜은 다음과 같이 수행한다.

① A는 임의의 정수 a를 선택하고 $X_A = g^a \oplus P$를 계산하여 B에게 전송한다.

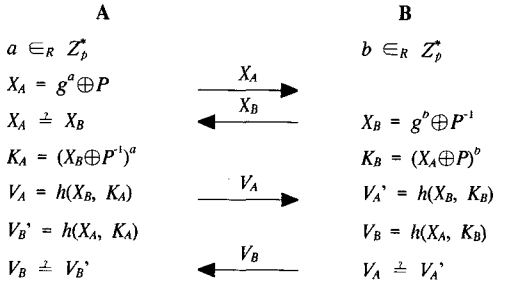
② B는 임의의 정수 b를 선택하고 $X_B = g^b \oplus P^{-1}$를 계산하여 A에게 보낸다. 그리고 A로부터 메시지를 기다리는 동안 $K_B = (X_A \oplus P)^b = g^{ab}$, $V_A' = h(X_B, K_B) = h(g^b \oplus P^{-1}, g^{ab})$, 그리고 $V_B = h(X_A, K_B) = h(g^a \oplus P, g^{ab})$를 계산한다.

③ A는 B로부터 X_B를 받은 후에 $X_B \stackrel{?}{=} X_A$를 검사한다. 두 값이 같다면 A는 프로토콜을 중단한다. 그렇지 않으면 A는 $K_A = (X_B \oplus P^{-1})^a = g^{ab}$와 $V_A = h(X_B, K_A) = h(g^b \oplus P^{-1}, g^{ab})$를 계산하여 V_A를 B에게 전송한다. 그리고 B로부터 메시지를 기다리는 동안 $V_B' = h(X_A, K_A) = h(g^a \oplus P, g^{ab})$를 계산한다.

④ B는 A로부터 V_A를 받은 후에 $V_A \stackrel{?}{=} V_A'$를 검사한다. 두 값이 같다면 B는 A를 검증했다고 확신한다. 그리고 V_B를 A에게 전송한다.

⑤ A는 B로부터 V_B를 받은 후에 $V_B \stackrel{?}{=} V_B'$를 검사한다. 두 값이 같다면 A는 B를 검증했다고 확신한다.

SEKA-H는 [그림 1]과 같이 요약될 수 있다.



[그림 1] SEKA-H 프로토콜

3.3 SEKA-E 프로토콜

본 절에서는 SEKA-H 프로토콜의 한 변형인 SEKA-E 프로토콜을 제안한다. SEKA-E 프로토콜은 SEKA-H 프로토콜과는 달리 프로토콜 수행 과정에서 공유된 세션키를 검증하기 위하여 지수 연산을 사용한다. SEKA-E 프로토콜에 필요한 초기 설정은 해쉬 함수를 제외하고는 SEKA-H 프로토콜과 같다. SEKA-E 프로토콜은 다음과 같이 수행한다.

① A는 임의의 정수 a를 선택하고 $X_A = g^a \oplus P$를 계산하여 B에게 전송한다.

② B는 임의의 정수 b를 선택하고 $X_B = g^b \oplus P^{-1}$를 계산하여 A에게 보낸다. 그리고 A로부터 메시지를 기다리는 동안 $K_B = (X_A \oplus P)^b = g^{ab}$, $V_A' = (X_B)^{K_B} = (g^b \oplus P^{-1})^{g^{ab}}$, 그리고 $V_B = (X_A)^{K_B} = (g^a \oplus P)^{g^{ab}}$를 계산한다.

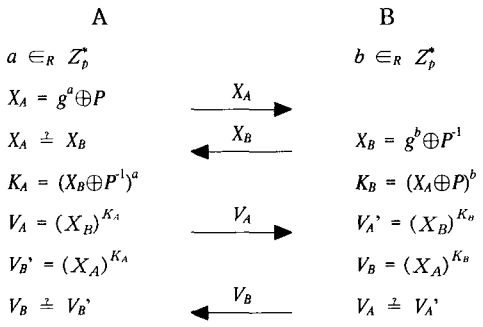
③ A는 B로부터 X_B를 받은 후에 $X_B \stackrel{?}{=} X_A$를 검사한다. 두 값이 같다면 A는 프로토콜을 중단한다. 그렇지 않으면 A는 $K_A = (X_B \oplus P^{-1})^a = g^{ab}$와 $V_A = (X_B)^{K_A} = (g^b \oplus P^{-1})^{g^{ab}}$를 계산하여 V_A를 B에게 전송한다. 그리고 B로부터 메시지를 기다리는 동안 $V_B' = (X_A)^{K_A} = (g^a \oplus P)^{g^{ab}}$를 계산한다.

④ B는 A로부터 V_A를 받은 후에 $V_A \stackrel{?}{=} V_A'$를 검사한다. 두 값이 같다면 B는 A를 검증했다고 확신한다. 그리고 V_B를 A에게 전송한다.

⑤ A는 B로부터 V_B를 받은 후에 $V_B \stackrel{?}{=} V_B'$를 검사한다. 두 값이 같다면 A는 B를 검증했다고 확신한다.

제안된 SEKA-E 프로토콜은 [그림 2]와 같이 요약될 수 있다.

SEKA-E 프로토콜은 프로토콜을 수행하는 과정에서 공유된 세션키를 검증하기 위하여 SEKA-H 프로토콜과는 달리 지수 연산을 사용한다. 그래서 각 참여자는 SEKA-H 프로토콜보다 각각 2번의 추가적인 지수 연산을 수행해야 한다. 지수 연산은 상대적으로 많은 연산 시간을 필요로 하므로 프로토콜에 부담이 될 수 있다. 그러나 SEKA-E 프로토콜에서 각 참여자는 다른 참여자의 응답을 기다리는 대기 시간을 이용하여 이러한 지수 연산들을 수행할 수 있다. 즉, SEKA-E 프로토콜에서 참여자 A는 V_A를 B에게 전송한 후 B의 응답을 기다리는 시간에 V_B'를 계산할 수



[그림 2] SEKA-E 프로토콜

있고, 참여자 B는 A의 메시지를 기다리는 시간을 이용하여 K_B, V_A', 그리고 V_B를 계산할 수 있다.

Ⅳ. 안전성 분석

본 장에서는 먼저 필요한 몇 가지 가정들과 정의들을 기술한다. 그리고 이들에 기반하여 제안된 프로토콜들의 안전성을 분석한다.

제안된 프로토콜의 안전성 분석을 위해 3.2절에 기술된 바와 같이 Brute-force 공격을 막기에 충분한 크기를 갖는 시스템 보안 파라미터 k를 가정한다. 그리고 임의의 사건에 대한 확률 Pr이 2^{-k}보다 작거나 같다면 그 확률은 무시할만하다(Negligible)고 가정한다. 또한 사람이 기억할 수 있는 패스워드 P는 다항식 시간(Polynomial time)에 추측될 수 있는 낮은 엔트로피 $w(k)$ 값을 가진다고 가정한다. 이것은 공격자가 패스워드를 추측할 확률이 $1/2^{w(k)} >> 1/2^k$이다는 것을 의미한다. 논문 [12]에서와 같이 프로토콜에 참여하는 참여자들 사이의 모든 통신은 공격자(Eve)의 제어 하에 있다. 즉 Eve는 통신 중간의 메시지들을 도청(Eavesdropping)하거나 수정(Modifying), 반송(Reflecting), 그리고 재전송(Replaying)할 수 있다. 심지어 정상적인 참여자로 위장(Masquerading)해 프로토콜에 참여할 수도 있다. Eve가 이러한 공격들을 통하여 부정확한 세션키 생성을 유도하거나 패스워드나 세션키를 알아낸다면 공격에 성공했다고 본다.

제안된 프로토콜들의 안전성은 다항식 시간에 풀기 어렵다고 알려져 있는 이산대수 문제와 Diffie-Hellman 문제[13]의 어려움에 근거한다. 두 가지 문제들은 다음과 같이 정의될 수 있다.

[정의 1]

이산 대수 문제(Discrete Logarithm Problem: DLP)는

곱셈군 Z_p^* 상에서 생성자 g와 한 원소 g^a이 주어졌을 때 a를 계산하는 문제이다.

[정의 2]

Diffie-Hellman 문제(Diffie-Hellman Problem: DHP)는 곱셈군 Z_p^* 상에서 두 원소 g^a와 g^b이 주어졌을 때 g^{ab}를 계산하는 문제이다.

DLP와 DHP를 계산할 수 있는 확률은 각각 무시할만하다고 가정한다. 즉, $Pr <= 2^{-k}$이다.

제안된 프로토콜들은 3장에 기술된 바와 같이 공격자의 공격이 없다면 정확하게 동작한다는 것을 알 수 있다. 지금부터 앞에 기술된 가정과 정의들을 이용하여 SEKA-H 프로토콜이 다양한 공격들에 대하여 안전함을 보이고자 한다.

[정리 1]

SEKA-H는 중간 침입자 공격들에 안전하다.

(증명) Eve가 수동적이거나 적극적인 공격들을 통하여 패스워드나 세션키를 발견하거나 또는 프로토콜 참여자들이 알지 못하는 가운데 정확하지 않은 세션키를 공유하도록 유도한다면 공격에 성공한다고 가정하자. 우리는 공격자가 이러한 공격들에 성공할 확률이 무시할만하다는 것을 증명하고자 한다.

(1) Eve가 수동적인 공격자라면 도청을 통하여 다음과 같은 정보를 얻을 수 있다: $X_A = g^a \oplus P$, $X_B = g^b \oplus P^{-1}$, $V_A = h(g^b \oplus P^{-1}, g^{ab})$, $V_B = h(g^a \oplus P, g^{ab})$. 그러나 이 정보들로부터 패스워드 P와 세션키 K (= g^{ab})를 계산할 수 있는 방법은 없다.

(2) Eve가 적극적인 공격자라면 다음의 네 가지 공격이 가능하다.

(2a) 두 참여자들이 프로토콜을 완료(Acceptance)했다면 V_A와 V_B가 성공적으로 검증되었음을 의미한다. 이처럼 두 참여자들이 프로토콜을 완료하고 같은 세션키에 동의했다면 Eve가 전송 메시지들을 수정했을 확률은 무시할만하다는 것을 보이고자 한다. Eve는 통신선로 중간에서 전송 메시지들을 수정하여 수신자에게 전송할 수 있다. 그러나 이러한 공격을 통해 두 참여자들에게 동일한 세션키를 생성하도록 유도하지 못한다면 이 공격은 세션키 검증 시에 탐지될 수밖에 없다. SEKA-H 프로토콜에서 Eve가 X_A와 X_B를 자신이 생성한 값으로 위조해서 각각 B와 A에게 전송했다고 하자. 그러면 A와 B는 이 메시지들을 받은 후에 각각 a와 b를 사용하여 세션키를 계산하게 된다. 그러나 $a, b \in_R Z_p^*$이므로 A와 B에 의해 생성된 K_A와 K_B가 같게 되어 Eve가 공격에 성공할 수 있는 확률은 무시할 만하다.

(2b) Eve는 반송(Reflecting) 공격을 통하여 정확하지 않은 세션키의 생성을 유도할 수 있다. 즉, A가 보낸 X_A와 V_A를 A에게 되돌려 보냄으로써 공격을 수행한다. 그러나 프로토콜의 세 번째 단계에서 A는 $X_B \stackrel{?}{=} X_A$를 검사하기 때문에 이러한 공격은 성공할 수 없다.

(2c) Eve가 A로 위장한다면 그는 자신이 생성한 a와 g^a, 그리고 B로부터 받은 $g^b \oplus P^{-1}$를 알 수 있다. 이 정보들로부터 P를 계산할 수 있는 방법은 없다. 그리고 Eve는 V_A로 응답을 해야 하지만 패스워드를 알지 못하므로, 온라인 패스워드 추측을 통하여 정확한 응답을 할 확률은 $1/2^{w(k)}$이다. 이러한 온라인 패스워드 추측 공격은 패스워드 인증 실패 횟수를 셈으로써 쉽게 탐지되고 시도 횟수를 제한(보통 3회)함으로써 쉽게 조치될 수 있다.

(2d) Eve가 B로 위장한다면 자신이 생성한 b와 g^b, 그리고 A로부터 받은 $g^a \oplus P$와 $h(g^b, (g^b \oplus P^{-1})^a)$를 알 수 있다. 이 정보들로부터 P를 계산할 수 있는 방법은 없다. 그리고 Eve는 V_B로 응답을 해야 하지만 패스워드를 알지 못하므로 정확한 응답을 할 확률은 $1/2^{w(k)}$이다. 이러한 온라인 패스워드 추측 공격은 (2c)에 언급된 바와 같이 쉽게 탐지되고 조치될 수 있다.

그러므로 SEKA-H 프로토콜은 중간 침입자 공격들에 대하여 안전하다.

[정리 2]

SEKA-H는 오프라인 패스워드 추측 공격에 안전하다.

(증명) 공격자가 오프라인 패스워드 추측 공격에 성공하기 위해서는 추측한 패스워드의 정확성을 검증할 수 있어야 한다. 오프라인 패스워드 추측 공격에 대하여 다음과 같은 세가지 측면을 고려한다.

(1) a와 b는 순환군(Cyclic group)에서 정규분포(Uniform distribution)에 의해 선택되고 이 때문에 g^a와

g^b도 순환군에서 정규분포 하에 있게 되며 X_A와 X_B도 마찬가지이다. 그러므로 실패한 패스워드와 남아 있는 패스워드들 사이에는 어떤 연관 관계도 발견할 수 없다. 즉 오프라인 패스워드 추측 공격으로 한 개의 추측된 패스워드가 정확한 패스워드가 아니라면 패스워드 가능 집합은 한 개씩 감소할 뿐이다.

(2) Eve가 수동적인 공격자라면 도청을 통하여 다음과 같은 정보를 얻을 수 있다: $X_A = g^a \oplus P$, $X_B = g^b \oplus P^{-1}$, $V_A = h(g^b \oplus P^{-1}, g^{ab})$, $V_B = h(g^a \oplus P, g^{ab})$. 그리고 Eve는 먼저 패스워드 P'를 추측하고 P'^{-1}를 계산한다. 그리고 나서 Eve는 P', P'^{-1}, X_A, X_B, V_A, 그리고 V_B를 사용하여 추측한 패스워드 P'의 정확성을 검증하려 할 것이다. 그러나 DLP나 DHP를 풀지 않고서는 자신이 추측한 패스워드의 정확성을 검증할 방법이 없다.

(3) 이제 적극적인 공격에 의한 오프라인 패스워드 추측 공격을 두 경우로 나누어 고려해보자.

(3a) Eve가 A로 위장했다면 Eve는 자신이 생성한 a와 g^a, 그리고 B로부터 받은 $g^b \oplus P^{-1}$를 알 수 있다. 그러나 이 정보들을 이용하여 추측한 패스워드의 정확성을 검증할 수 있는 방법은 없다.

(3b) Eve가 B로 위장했다면 자신이 생성한 b와 g^b, 그리고 A로부터 받은 $g^a \oplus P$와 $h(g^b, (g^b \oplus P^{-1})^a)$를 알 수 있다. 그러나 이 정보들을 이용하여 추측한 패스워드의 정확성을 검증할 수 있는 방법은 없다.

그러므로 SEKA-H 프로토콜은 오프라인 패스워드 추측 공격에 안전하다.

[정리 3]
SEKA-H는 완전한 전방향 보안성을 제공한다.

(증명) 완전한 전방향 보안성은 패스워드가 노출된 상황에서도 Eve가 과거의 세션키들을 구할 수 없을 때 보장된다. 이를 분석하기 위해 Eve가 패스워드 P를 알고 있다고 가정하자. Eve는 이 패스워드 관련 정보들과 지난 통신 세션에서 도청한 정보들 즉, P, P^{-1}, $g^a \oplus P$, $g^b \oplus P^{-1}$, $h(g^b \oplus P^{-1}, g^{ab})$, 그리고 $h(g^a \oplus P, g^{ab})$들을 이용해 이전 세션의 세션키 g^{ab}를 계산하려고 시도한다. 그러나 Eve는 DLP나 DHP를 풀지 않고서는 이를 계산할 수 없다. 그러므로 SEKA-H는 완전한 전방향 보안성을 제공한다.

[정리 4]
SEKA-H는 Denning-Sacco 공격에 안전하다.

(증명) Denning-Sacco 공격에 안전하기 위해서 프로토콜은 세션키가 노출되어도 Eve가 패스워드를 구할 수 없어야 한다. Eve가 세션키 g^{ab}를 알고 있다고 가정하자. Eve는 이 정보와 이전 세션에서 도청한 정보들 즉, g^{ab}, $g^a \oplus P$, $g^b \oplus P^{-1}$, $h(g^b \oplus P^{-1}, g^{ab})$, 그리고 $h(g^a \oplus P, g^{ab})$들을 이용해 패스워드를 계산하려고 하거나 추측한 패스워드의 정확성을 검증하려고 한다. 그러나 Eve는 DLP나 DHP를 풀지 않고는 이를 행할 수 없다. 그러므로 SEKA-H는 Denning-Sacco 공격에 안전하다.

SEKA-H와 비슷하게 SEKA-E는 중간 침입자 공격과 패스워드 추측 공격, 그리고 Denning- Sacco 공격에 안전하고 전방향 보안성을 제공한다. 이들에 대한 분석은 SEKA-H의 경우와 비슷하므로 생략한다.

V. 성능 분석

키 동의 프로토콜의 성능은 통신 부하와 계산 부하 측면에서 측정될 수 있다. 통신 횟수는 통신 부하를 측정하는 기준이고 랜덤 정수 생성 횟수, 지수 연산 횟수, 해쉬 연산 횟수, 대칭키 연산 횟수는 계산 부하를 측정하기 위한 기준들이다. 그리고 프로토콜의 또 다른 성능 측정 기준으로 전체 수행 시간을 고려해 볼 수 있다. 이 전체 수행 시간은 프로토콜의 첫 연산을 수행하기 시작하면서부터 마지막 연산이 수행되기까지 걸리는 전체 시간으로, 프로토콜에서 수행되어야 할 연산 횟수들의 합으로 계산될 수 있다. 프로토콜의 실질적인 전체 수행 시간을 계산하기 위하여 같은 시간에 중복되어 수행되는 연산들은 더 오랜 시간이 걸리는 연산만을 포함하기로 한다. 예를 들어, 각 참여자들이 같은 시간에 지수 연산을 수행한다면 한 번의 지수 연산만이 전체 수행 시간에 포함되고, 한 참여자가 메시지를 전송한 직후 해쉬 연산을 수행한다면 전체 수행 시간에는 통신 시간만 포함된다. [표 2]은 이러한 성능 평가 기준들, 즉 통신 횟수, 랜덤 정수 생성 횟수, 지수 연산 횟수, 해쉬 연산 횟수, 대칭키 연산 횟수, 그리고 전체 수행 시간의 측면에서 기존의 잘 알려진 프로토콜들인 PAK,[3] AKE,[4] 그리고 KS[5]들과 비교하여 제안된 프로토콜들의 성능을 보여준다.

〔표 2〕 잘 알려진 프로토콜들과의 비교

분석요인 \ 프로토콜		PAK	AKE	KS	SEKA-H	SEKA-E
통신(C) 횟수		3	3	4	4	4
랜덤정수(R)생성횟수		2	2	4	2	2
지수연산(E)	A	3	2	4.5	2	4
횟수	B	3	2	4.5	2	4
해쉬연산(H)	A	4	3	4	2	0
횟수	B	4	3	4	2	0
대칭키연산(S) 횟수		0	4	0	0	0
전체수행시간		3C+1R+4E+3H	3C+1R+3E+4H+4S	4C+2R+4.5E+ 4H	4C+1R+2E+1H	if(2C<E) 2C+1R+4E else 4C+1R+3E

[표 2]에서 보는 바와 같이 SEKA-H 프로토콜은 각 참여자가 수행해야 할 각 연산 횟수나 전체 수행 시간 측면에서 가장 효율적이다. 통신 횟수 측면에서는 SEKA-H 프로토콜이 PAK과 AKE 프로토콜들보다 많은 4회의 통신을 수행한다. 적은 통신 부하를 요구하는 응용들에서는 이러한 통신 횟수가 적은 프로토콜들이 효과적일 수 있다. 이와 같은 환경에 사용하기 위하여 SEKA-H 프로토콜을 3회의 통신을 수행하는 프로토콜로 변형하기는 매우 쉽다. 즉 연산들에 대해서는 아무런 변경 없이 각 참여자들이 $A \rightarrow^{X_A} B$, $B \rightarrow^{X_B, V_B} A$, $A \rightarrow^{V_A} B$형태로 통신을 하도록 통신 흐름만 변형하면 된다. 이 변형 프로토콜에서 각 참여자가 수행해야 하는 각 연산의 수는 SEKA-H 프로토콜과 동일하며 전체 수행 시간은 3C+1R+3E+2H가 되어 다른 프로토콜들에 비해 가장 효율적이다.

[표 2]에서 보는 바와 같이 SEKA-E 프로토콜은 다른 프로토콜들과는 달리 해쉬 연산이나 대칭키 연산을 필요로 하지 않는다. 그러나 각 참여자는 총 4번의 지수 연산을 수행해야 한다. 이것은 KS 프로토콜보다는 적고 PAK과 AKE 프로토콜에 비해서는 많은 횟수이다. 그러나 SEKA-E 프로토콜에서 각 참여자는 다른 참여자의 응답을 기다리는 대기 시간을 이용하여 몇몇 지수 연산들을 수행한다. 이 때문에 상대적으로 많은 시간이 소요되는 지수 연산을 적은 비용으로 효율적으로 수행할 수 있다. [표 2]에서 SEKA-E 프로토콜의 전체 수행 시간은 통신 시간과 지수 연산 시간의 관계에 따라 두 측면으로 나누어 측정되었다.

Ⅵ. 결 론

패스워드 기반의 프로토콜은 사람들이 패스워드와 같은 작은 지식만을 기억하면 되기 때문에 간단성, 편의성, 적응성, 이동성, 그리고 하드웨어 사용의 불필요 등의 장점을 가지고 있어 널리 이용되고 있다. 본 논문에서는 상호 인증 가능한 패스워드 기반의 키 동의 프로토콜들인 SEKA-H와 SEKA-E를 제안하였다. SEKA-H 프로토콜은 프로토콜을 수행하는 중에 공유된 세션키를 검증하기 위하여 해쉬 함수를 사용하고 SEKA-H 프로토콜의 다른 변형인 SEKA-E 프로토콜은 지수 연산을 사용한다. 제안된 프로토콜들은 중간 침입자 공격, 패스워드 추측 공격, 그리고 Denning-Sacco 공격에 안전하고 완전한 전방향 보안성을 제공한다. SEKA-H 프로토콜은 기존에 잘 알려진 프로토콜들과 비교하여 구조가 매우 간단하며 좋은 효율성을 갖는다. SEKA-E 프로토콜은 다른 프로토콜들과 비교하여 비슷한 전체 수행 시간을 필요로 한다.

참 고 문 헌

[1] W. Diffie, M. E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, Vol.IT-22, No.6, pp.644~654, 1976.

[2] S. M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", *IEEE Symposium on Research in Security and Privacy*, pp.72~84, 1992.

[3] V. Boyko, P. MacKenzie, and S. Patel, "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman", *Advances in Cryptology-EUROCRYPT'2000*, pp.156~171, 2000.

[4] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attacks", *Advances in Cryptology-EUROCRYPT'2000*, pp.139~155, 2000.

[5] T. Kwon and J. Song, "A Study on the Generalized Key Agreement and Password Authentication Protocol", *IEICE TRANS. COMMUN.*, Vol.E83-B, No.9, pp.2044~2050, SEP 2000.

[6] R. Anderson and M. Lomas, "Fortifying Key Negotiation Schemes with Poorly Chosen Passwords", *Electronics Letters*, Vol.30, No.13, pp.1040~1041, 1994.

[7] S. Lucks, "Open key exchange: How to defeat dictionary attacks without encrypting public keys", *Proceedings of the Security Protocol Workshop '97*, pp. 7~9, April 1997.

[8] P. MacKenzie, S. Patel, and R. Swaminathan, "Password-Authenticated Key Exchange based on RSA", *Advances in Cryptology-ASIACRYPT'2000*, pp.599~613, 2000.

[9] D.H. Seo and P. Sweeney, "Simple authenticated key agreement algorithm", *Electronics Letters*, Vol. 35, No.13, pp.1073-1074, 1999.

[10] B. W. Simon, and M. Alfred, "Authenticated Diffie-Hellman Key Agreement Protocols", *Proceedings of SAC 98*, LNCS, 1998

[11] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols". In *ACM security '93*, pp.62~73, 1993.

[12] M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution", *Advances in Cryptology-CRYPTO'93*, Vol.773, pp.232~249, 1994.

[13] D. R. Stinson, *Cryptography Theory and Practice*, CRC, 1995.

〈著者紹介〉

이 성 운 (Sung-Woon Lee) 정회원
1993년 8월 : 전남대학교 전산통계학과 학사졸업
1996년 8월 : 전남대학교 전산통계학과 석사졸업
2001년 3월~현재 : 경북대학교 컴퓨터공학과 박사과정
<관심분야> 정보보호, 암호학, 네트워크 보안

유 기 영 (Kee-Young Yoo) 정회원
1978년 2월 : 경북대학교 수학교육과 학사졸업
1980년 2월 : 한국과학기술원 컴퓨터공학과 석사졸업
1993년 2월 : Rensselaer Polytechnic Institute, New York, 컴퓨터공학과 박사졸업
1980년 2월~현재 : 경북대학교 컴퓨터공학과 교수
<관심분야> 정보보호, 암호학, 암호칩 설계, 스마트카드 보안