情報保護學會論文誌
第18卷 第1號, 2008. 2

두 패스워드 기반 키 교환 및 인증 프로토콜들에 대한 오프라인 패스워드 추측 공격의 취약성 분석*

심경아, 이주희, 이향숙
이화여자대학교

Vulnerability of Two Password-based Key Exchange and Authentication Protocols against Off-line Password-Guessing Attacks*

Kyung-Ah Shim, Ju-Hee Lee, Hyang-Sook Lee
Ewha Womans University

요 약

패스워드를 기반으로 하는 사용자 인증 및 키 교환 프로토콜은 사용자들이 쉽게 기억할 수 있는 패스워드를 사용하기 때문에 대부분의 경우에 패스워드 추측공격에 취약하다는 문제점이 있다. 본 논문에서는 동일 서버를 사용하는 두 사용자 간의 패스워드 기반 키 교환 프로토콜과 패스워드 기반 인증 프로토콜이 모두 오프라인 패스워드 추측공격에 안전하지 못함을 보인다.

ABSTRACT

Since a number of password-based protocols are using human memorable passwords they are vulnerable to several kinds of password guessing attacks. In this paper, we show that two password-based key exchange and authentication protocols are insecure against off-line password-guessing attacks.

Keywords : Password-Based authentication protocol, Off-line Password guessing attack

I. 서 론

패스워드 기반 인증 및 키 교환 (PAKE) 프로토콜은 인터넷과 같은 공개된 통신망에서 통신하는 두 개체가 프로토콜을 수행하기 전에 미리 공유한 패스워드를 사용하여 통신하는 상대방의 신분을 확인하고 연속되는 다음 통신에 사용될 세션 키를 동의하고자 하는 것이 목적이다. 패스워드 기반 키 교환 프로토콜은 참여자들의 수에 따라 두 참여자 환경, 세 참여자 환경, 그룹 참여자 환경 등으로 나뉠 수 있다. 두 참여자 환경이란 통신에 참여한 두 참여자들 사이에 서로를 인증하고 세션 키를 공유하는 것이고, 세 참여자 환경이란 한 서버와 그 서버에 등록한 두 사용자들이 서로를 인증하고 세션 키를 공유하는 것이다. 이때, 서버는 두 사용자를 인증하고

접수일: 2007년 12월 5일; 채택일: 2008년 1월 15일
* 저자[1]는 한국학술진흥재단 지원사업(MOEHRD) (KRF-2005-217-C00002), 저자[2]는 2단계 BK21 지원사업, 저자[3]는 한국과학재단 특정기초 지원사업(R01-2005-000-10713-0)의 연구결과로 수행되었음.
† 주저자, kashim@ewha.ac.kr
‡ 교신저자, juheelee@ewhain.net

그들이 세션 키를 공유하도록 돕는 역할을 하지만 생성된 세션 키는 알 수 없기 때문에 두 사용자들 사이에 전송되는 메시지들은 안전하게 보호된다. Bellovin과 Merritt[1]가 두 사용자 간에 패스워드 기반 키 교환(EKE) 프로토콜을 처음으로 제안한 이래 많은 2자간, 3자간의 PAKE프로토콜들이 제안되어 왔다[2, 3, 4]. 최근에 신성철 등[5]은 서버에 저장된 패스워드 파일의 노출에도 패스워드 추측 공격에 안전한 프로토콜(3PAKE)을 제시하였고 곽진 등[6]은 man-in-the-middle 공격과 사전 공격에 대해 안전하고 perfect forward secrecy를 제공하며, advanced modification 공격에 안전한 패스워드 기반 키 동의 (KOYW) 프로토콜을 제안하였다. 본 논문에서는 그들의 프로토콜은 여전히 오프라인 패스워드 추측 공격에 안전하지 못한 것임을 보인다.

본 논문의 구성은 다음과 같다. 2장에서는 세 참여자 환경의 3PAKE 프로토콜과 두 참여자 환경의 KOYW 프로토콜을 살펴보고, 3장에서는 각각의 프로토콜에서의 오프라인 패스워드 추측 공격에 대한 취약성을 분석한다. 마지막으로 4장에서 결론을 맺는다.

Ⅱ. 3PAKE와 KOYW 프로토콜

본 절에서는 다양한 공격들에 대하여도 안전하고 완전한 보안성을 제공하는 각각 다른 환경에서 설계된 두개의 프로토콜들을 살펴보고자 한다.

2.1. 3PAKE 프로토콜

신성철 등[5]은 Sun[10]의 SCH-3PEKE 프로토콜이 패스워드 추측 공격을 막기 위해 서버의 공개키 사용으로 인한 비효율성을 개선한 3PAKE 프로토콜을 제안하였다. 3PAKE 프로토콜은 서버에 자신의 아이디와 패스워드를 등록한 두 사용자가 각각 자신의 패스워드를 사용하여 서버와 상호 인증 을 수행하고 자신들만이 아는 세션 키를 공유하려는 것이 목적이다. Alice 와 Bob은 프로토콜을 수행하기 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.

〔표 1〕. 시스템 파라미터

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

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.

3PAKE 프로토콜[그림1]은 서버S에 등록되어 있는 Alice와 Bob이 세션 키 K를 공유하기 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.

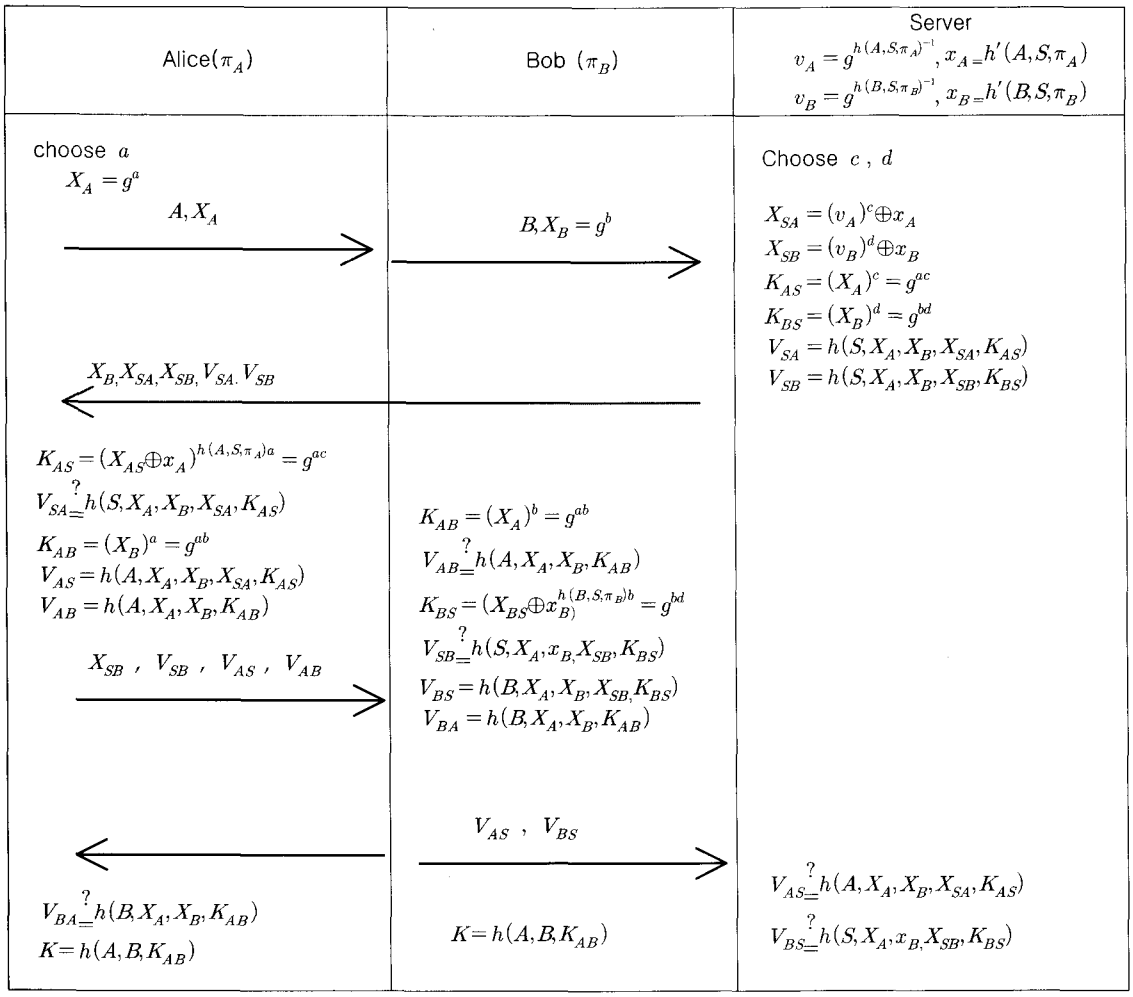
③ 서버는 패스워드 파일로부터 v_A, x_A, v_B, x_B를 검색하고 c, $d \in_R G_q$를 선택하여 다음 값들을 계산한다.

$X_{SA} = (v_A)^c \oplus x_A$, $X_{SB} = (v_B)^d \oplus x_B$,

$K_{AS} = (X_A)^c = g^{ac}$, $K_{BS} = (X_B)^d = g^{bd}$,

$V_{SA} = h(S, X_A, X_B, X_{SA}, K_{AS})$,

$V_{SB} = h(S, X_A, X_B, X_{SB}, K_{BS})$.



〔그림 1〕. 3PAKE 프로토콜

그리고 X_B, X_{SA}, X_{SB}, V_{SA}, V_{SB} 를 Alice에게 전송한다.

④ Alice는 $K_{AS} = (X_{AS} \oplus x_A)^{h(A,S,\pi_A)a} = g^{ac}$를 계산하고 $V_{SA} \stackrel{?}{=} h(S, X_A, X_B, X_{SA}, K_{AS})$를 검사함으로써 서버를 인증한다. 그리고 다음 값들을 계산한다.

$$K_{AB} = (X_B)^a = g^{ab}$$

$$V_{AS} = h(A, X_A, X_B, X_{SA}, K_{AS}),$$

$$V_{AB} = h(A, X_A, X_B, K_{AB})$$

그리고 X_{SB} , V_{SB} , V_{AS} , V_{AB}를 Bob에게 전송한다.

⑤ Bob은 $K_{AB} = (X_A)^b = g^{ab}$를 계산하고 $V_{AB} \stackrel{?}{=} h(A, X_A, X_B, K_{AB})$ 를 검사하여 Alice를 검증한다. 또한 $K_{BS} = (X_{BS} \oplus x_B^{h(B,S,\pi_B)b} = g^{bd}$를 계산하고 $V_{SB} \stackrel{?}{=} h(S, X_A, x_B, X_{SB}, K_{BS})$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 $V_{AS} \stackrel{?}{=} h(A, X_A, X_B, X_{SA}, K_{AS})$와 $V_{BS} \stackrel{?}{=} h(B, X_A, X_B, X_{SB}, K_{BS})$를 검사하여 Alice와

Bob을 인증한다.

⑦ Alice는 $V_{BA} \stackrel{?}{=} h(B, X_A, X_B, K_{AB})$를 검사하여 Bob을 인증한 후 세션 키 $K = h(A, B, K_{AB})$를 계산한다.

3PAKE 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} , V_{BA}를 검사함으로써 서로를 인증하게 된다. 이러한 인증과정들이 성공적으로 끝나면 Alice와 Bob은 세션 키 $K = h(A, B, K_{AB})$를 계산하고 프로토콜을 종료한다.

2.2. KOYW 프로토콜

곽진 등[6]은 기존에 제안된 패스워드를 기반으로 하는 SAKA(Simple Authenticated Key Agreement) 프로토콜들이 Advanced Modification 공격에 취약함을 보이고 이에 안전한 KOYW 프로토콜을 제안하였다.

KOYW 프로토콜은 두 개체가 통신을 시작하기 이전에 공통의 비밀 패스워드를 공유하고 있다는 것을 가정한다.

〔표 2〕. 시스템파라미터

기호	설명
p	큰 소수
Eve	능동적 공격자
S	공통의 비밀 패스워드
g	Z_p 상의 원시원소($\mathrm{ord}(g) = p-1$)
Alice, Bob	통신개체
H	일방향 해쉬 함수 (one-way hash function)
$SK_{A,B}$	Alice와 Bob이 세션 키
$a, b \in_R Z_p^*$	Alice와 Bob이 선택한 랜덤 수,
$\rightarrow$	메시지 전송

KOYW 프로토콜[그림2]에서 사용하는 시스템 파라미터들, 키 설정 과정 그리고 키 확인 과정은 다음과 같다.

[키 설정 과정]

① Alice와 Bob은 프로토콜을 시작하기 전에 각각 두 정수 $Q \bmod p$와 $Q^{-1} \bmod p$를 계산한다. 여기서 Q는 패스워드 S로부터 유도 된 값으로, $(p-1)$과 서로소인 값이어야 한다. 또한, 서로 다른 패스워드가 주어졌을 경우 동일한 Q 값이 나올 확률이 매우 낮아야 한다.

② Alice는 랜덤 수 a를 선택하여 $X_1 = g^{aQ} \bmod p$을 계산한 후 BOb에게 전송한다.

③ Bob은 랜덤 수 b를 선택하여 $Y_1 = g^{bQ} \bmod p$을 계산한 후 Alice에게 전송한다.

④ Alice는 Bob으로부터 수신한 Y_1을 이용하여 $SK_A = (Y_1)^{aQ^{-1}} = g^{ab} \bmod p$을 계산한다.

⑤ Bob은 Alice로부터 수신한 X_1을 이용하여 $SK_B = ((X_1)^{bQ^{-1}}) = g^{ab} \bmod p$을 계산한다.

[키 확인 과정]

⑥ Alice는 $k_1 = H(SK_A, Q)$ 을 계산하여 Bob에게 전송한다.

⑦ Bob은 $k_2 = H(SK_B, Q^{-1})$ 을 계산하여 Alice에게 전송한다.

⑧ Alice와 Bob은 각각 다음 식을 이용하여 자신들이 계산한 세션 키를 검증한다.

Alice : $H(SK_B, Q^{-1}) \stackrel{?}{=} H(SK_A, Q^{-1})$

Bob : $H(SK_A, Q) \stackrel{?}{=} H(SK_B, Q)$.

Ku-Wang 등 [8]과 Lin 등 [9]이 제안한 프로토콜에서는 공격자 Eve에 의한 Advanced Modification 공격을 통해, Alice와 Bob이 키 확인 과정을 수행한다 할지라도 잘못된 세션 키를 신뢰하도록 할 수 있다. 이것은 공격자 Eve가 프로토콜에서 X_1 또는 Y_1을 계산하지 못하고, Q 또는 Q^{-1} 값을 알지 못한다 하더라도 Alice와 Bob을 속일 수 있음을 보여준다. KOYW는 키 확인 과정에서 Eve의 공격이 성공하려면 반드시 $g^{ab} \bmod p$ 값을 계산하여 Bob에게 전송할 수 있어야 하지만 이산대수 문제를 푸는 것이 계산상 불가능하고 패스워드가 비밀리에 보관되므로 이 값을 계산하는 것은 불가능하다고 주장하였다.

Alice	공개정보 p, g	Bob
[키 설정 과정] $a \in_R Z_p^*$ $X_1 = g^{aQ} \bmod p$	X_1 →	$b \in_R Z_p^*$ $Y_1 = g^{bQ} \bmod p$
$SK_A = ((Y_1)^{aQ^{-1}}) = g^{ab} \bmod p$	← Y_1	$SK_B = ((X_1)^{bQ^{-1}}) = g^{ab} \bmod p$
[키 확인 과정]	$k_1 = H(SK_A, Q)$ →	
$H(SK_B, Q^{-1}) \stackrel{?}{=} H(SK_A, Q^{-1})$	← $k_2 = H(SK_B, Q^{-1})$	$H(SK_A, Q) \stackrel{?}{=} H(SK_B, Q)$

〔그림 2〕. KOYW 프로토콜

Ⅲ. 두개의 패스워드 기반 키 교환 및 인증 프로토콜에 대한 오프라인 패스워드 추측공격

권태경 등 [7]은 공격자의 행동 유형 측면에서 오프라인 패스워드 추측 공격은 다음과 같은 두 가지 유형으로 분류하였다.

(1) 오프라인 추측 공격(off-line password guessing attack): 공격 대상자의 패스워드를 추측한 공격자는 프로토콜의 정상적인 메시지를 도청하고 저장한 후, 저장된 메시지를 이용하여 추측에 대한 검증을 오프라인으로 반복한다. 이와 같은 형태의 추측 공격은 발견할 수 없으며, 따라서 방어하기 위한 방법은 공격자가 추측한 패스워드를 검증하는데 필요한 계산량을 늘리는 것이다.

(2) 온라인 추측 공격(on-line password guessing attack): 공격 대상자의 패스워드를 추측한 공격자는 추측에 대한 검증을 위해서 온라인으로 반복하여 프로토콜에 참여한다. 온라인 참여를 위해서는 도청한 메시지를 재전송하거나 공격 대상자를 가장하여 위조 메시지를 만든 후 프로토콜에 참여하는 방법으로 이루어질 수 있다. 프로토콜의 서버나 상대방이 검증에 직접 참여하게되므로, 따라서 방어하기 위해서는 서버나 상대방이 추측한 패스워드의 실패 여부를 신속히 발견할 수 있어야 한다.

이제, 각각의 프로토콜에 대한 오프라인 패스워드 추측 공격을 살펴보기로 하자.

3.1. 3PAKE 프로토콜에 대한 공격[그림3]

① Eve는 Alice로 가장하여 $e \in_R Z_q$를 선택하고 $X_A = g^e$를 계산하여 Bob에게 A, X_A를 전송한다.

② Bob은 $b \in_R Z_q$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, $d \in_R Z_q$를 선택하여 다음 값들을 계산한다.

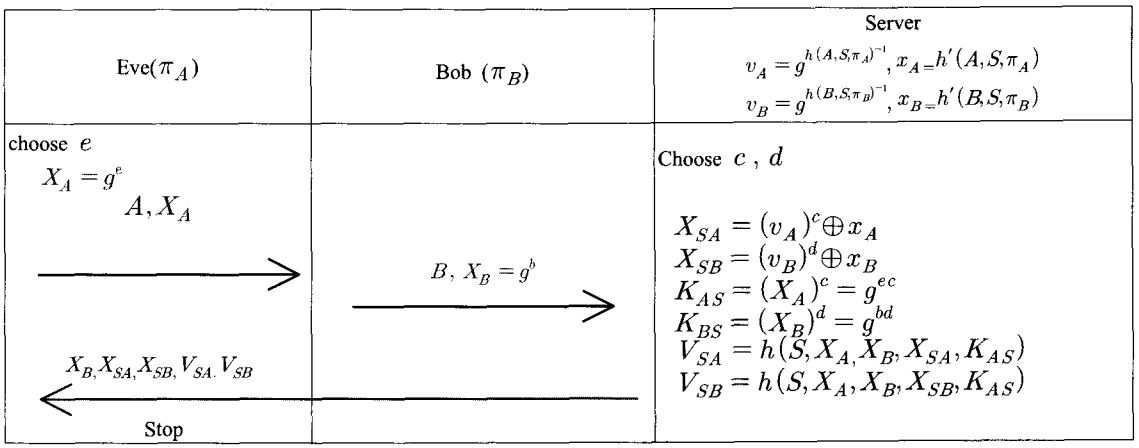
$$X_{SA} = (v_A)^c \oplus x_A, X_{SB} = (v_B)^d \oplus x_B,$$
$$K_{AS} = (X_A)^c = g^{ec}, K_{BS} = (X_B)^d = g^{bd}$$
$$V_{SA} = h(S, X_A, X_B, X_{SA}, K_{AS}),$$
$$V_{SB} = h(S, X_A, X_B, X_{SB}, K_{BS}).$$

그리고 X_B, X_{SA}, X_{SB}, V_{SA}, V_{SB}를 Alice에게 전송한다.

④ Eve는 서버가 전송한 X_B, X_{SA}, X_{SB}, V_{SA} V_{SB} 값을 받아 저장하고 프로토콜 실행을 멈춘다.

이제부터 Eve는 오프라인 추측공격을 실행하고 추측 가능한 범위 내에서 검증을 반복 시행한다.

1. 패스워드 후보 π_A'를 선택 지정한다.
2. $x_A' = h'(A, S, \pi_A')$, $K_{AS}' = (X_{SA} \oplus x'_A)^{h(A,S,\pi'_A)e}$ 와



〔그림 3〕. 3PAKE 프로토콜에 대한 공격

$V_{SA}' = h(S, X_A, X_B, X_{SA}, K_{AS}')$를 계산한다.

3. V_{SA}와 V_{SA}'을 비교한다.

마지막 3단계에서, 만약 π_A'이 Alice의 정확한 패스워드 π_A라면 V_{SA}와 V_{SA}'은 일치하게 된다. 결국 공격자는 A의 패스워드 π_A를 얻게 된다.

3.2. KOYW 프로토콜에 대한 공격[그림4]

① Eve는 Alice가 Bob에게 전송한 값 X_1을 가로 챈다.

② Eve는 직접 $Y_1' = g^b \mod p$을 계산하여 Alice에게 Bob으로 가장하여 Y_1인 것처럼 전송한다.

③ Alice는 다음을 계산하고 Bob에게 k_1을 전송한다.

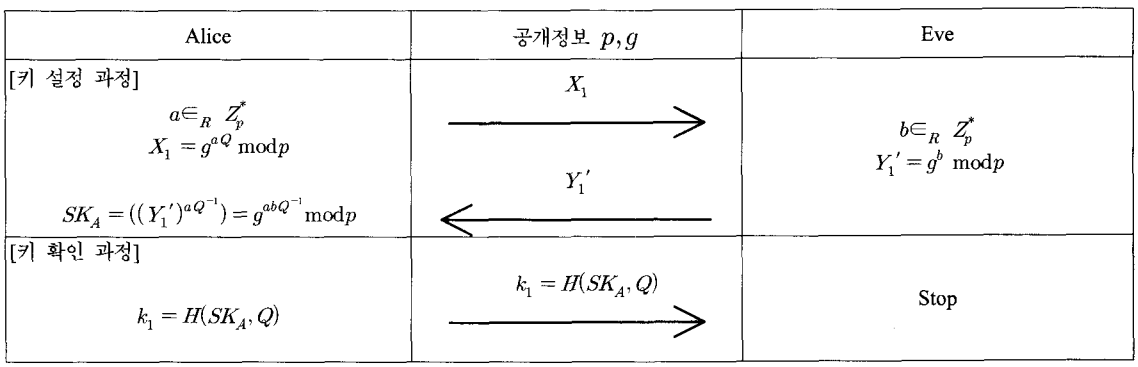
$$SK_A = (g^{bQ^{-1}})^a = g^{abQ^{-1}} \mod p$$
$$k_1 = H(SK_A, Q) \mod p$$

④ Eve는 Alice가 전송한 k_1을 받아서 저장하고 프로토콜실행을 멈춘다.

이제부터 Eve는 오프라인 추측 공격을 실행하고 추측 가능한 범위 내에서 다음과 같은 검증을 반복 시행한다.

1. 패스워드 후보 Q'을 선택 지정한다.
2. $k' = H((g^{aQ})^{b(Q'^{-1})^2}, Q')$을 계산한다.
3. k'과 k_1을 비교한다.

마지막 3단계에서, 만약 Q'이 Alice와 Bob의 정확한 패스워드 Q 라면 k'과 k_1은 일치하게 된다. 결국, 공격자는 올바른 패스워드 Q를 얻게 된다.



[그림 4]. KOYW 프로토콜에 대한 공격

Ⅳ. 결 론

본 논문에서는 3PAKE 프로토콜과 KOYW 프로토콜이 오프라인 추측 공격에 안전하지 못하다는 것을 보였다. 이러한 결과들은 경험적인 안전성(heuristic security) 분석이 아니라 제안된 환경에 적절한 안전성 모델을 정의하고 그 모델에서 안전함을 증명하는 증명 가능한 안전성 (provable security)을 갖는 프로토콜이 제안되어져야 한다는 것을 보여주고 있다.

참고문헌

[1] S. Bellovin and M. Meritt, Encrypted key exchange: password-based on protocols secure against dictionary attacks, *IEEE Computer Society Conference on Research in Security and Privacy* (1992), pp. 72-84.

[2] S. Bellovin and M. Meritt, Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password-file compromised, *ACM Conf. on Computer and Communications Security*, pp. 244-250, 1993.

[3] V. Boyko, P. MacKenzie and S. Patel, Provably secure password authenticated key exchange using Diffie-Hellman, *Advanced in Cryptography-Eurocrypt'00, LNCS 1807,* Springer-Verlag ,New York(2000), pp. 156-171.

[4] M. Bellare, D. Pointcheval and P. Rogaway, Authenticated Key Exchange secure against Dictionary Attacks, *Advanced in Cryptography -Eurocrypt'00, LNCS 1807*, Springer-Verlag, New York(2000), pp. 139-155.

[5] 신성철, 이성운, 동일 서버를 사용하는 두 사용자 간 효율적인 패스워드 기반의 키 교환 프로토콜, *한국정보보호학회논문지* , 1598-3986 , 제15권 6호, pp. 127-133 , 2005.

[6] 곽진, 오수현, 양형규, 원동호, Advanced Modification 공격에 안전한 패스워드 기반키 동의 프로토콜, *정보처리학회논문지C 제11-C권 제3호*, pp. 277-286 , 2004.

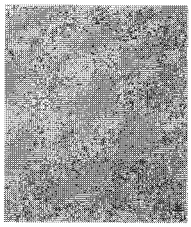
[7] 권태경, 강명호, 송주석, 패스워드 기반 시스템을 위한 효율적이고 안전한 인증 프로토콜의 설계 및 검증, *통신정보보호학회논문지 제 7권 제2호*, pp. 27-42, 1997.

[8] W. C. Ku and S. D. Wang. Cryptanaysis of modified authenticated key agreement protocol, *Electronics Letters*, Vol.36, NO.21, pp. 1770-1771, 2000.

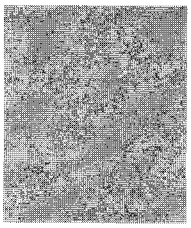
[9] I. C. Lin, C. C. Chang and M. S. Hwang, Security enhancement for the simple authentication key agreement algorithm, *24th Annual International Computer Software and Application Conference*, pp. 113-115, 2000.

[10] 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.

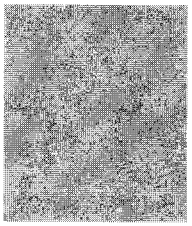
〈著者紹介〉



심 경 아 (Kyung-Ah Shim) 정회원
1992년 2월 : 이화여자대학교 수학과 졸업
1994년 2월 : 이화여자대학교 수학과 석사
1999년 2월 : 이화여자대학교 수학과 박사
2000년 2월~2004년 2월 : 한국정보보호진흥원 선임연구원
2004년 8월~현재 : 이화여자대학교 수학과 연구교수
<관심분야> 암호론, 정보보호



이 주 희(Ju-Hee Lee) 학생회원
1996년 2월 : 한남대학교 수학과 졸업
2002년 2월 : 이화여자대학교 수학과 석사
2005년 3월~현재 : 이화여자대학교 수학과 박사과정
<관심분야> 암호론, 정보보호



이 향 숙 (Hyang-Sook Lee) 정회원
1986년 2월 : 이화여자대학교 수학과 졸업
1988년 2월 : 이화여자대학교 수학과 석사
1993년 12월 : Northwestern 대학 수학과 박사
1995년 3월~현재 : 이화여자대학교 수학과 교수
<관심분야> 암호론, 정보보호