검증자 기반의 Three-Party 키 교환 프로토콜

김해문[O] 최영근 김순자
경북대학교 전자공학과
{seadoor[O], ind}@palgong.knu.ac.kr, snjkim@ee.knu.ac.kr

Three-Party Key Exchange Protocol based Verifier

Haemun Kim[0] Yeonggeun Choe Soonja Kim
Dept. of Electronics Engineering, Kyungpook National University

요 약

패스워드 기반 키 교환 프로토콜은 참여자들이 쉽게 기억할 수 있는 자신의 패스워드를 사용하므로 단순성, 편리성, 이동성의 장점 때문에 광범위하게 사용된다.

2000년에 Lin, Sun, Hwang[1]이 Steiner, Tsudik, Waidner[2]가 제안한 three-party EKE 프로토콜(STW-3PEKE)이 패스워드 추측 공격에 취약함을 증명하고 이를 개선한 서버의 공개키를 이용한 새로운 three-party EKE 프로토콜(LSH-3PEKE)을 제안했다. 2001년에는 Lin, Sun, Steiner, Hwang[3]이 서버의 공개키를 사용하지 않는 새로운 three-party EKE 프로토콜(LSSH-3PEKE)을 제안했다. 본 논문에서는 검증자(verifier) 기반 즉 서버가 사용자의 패스워드를 저장하지 않고 패스워드에 의해 생성되는 검증자를 가지는 프로토콜을 제안하며 이전에 제안한 프로토콜의 안전성을 그대로 유지하면서 좀 더 간단하며 효율적인 프로토콜을 제시한다.

1. 서 론

인증은 안전성과 많은 서비스 시스템들의 평가에 중요하다. 인증은 두 참여자가 나중에 암호학적인 연산에 사용할 수 있는 공통의 세션 키를 얻기 위해 사용된다. 패스워드 기반 기법은 생성 또는 저장 장치의 도움 없이 자신이 선택한 패스워드를 가지고 인증 및 키 교환에 사용되므로 널리 사용되는 방법이다. 그러나 패스워드의 선택범위와 길이는 사용자의 기억력에 의해 제한되는 낮은 엔트로피(entropy)를 가지므로 공격자가 패스워드로 유추되는 단어들을 사전화하고, 오프라인에서 이 단어들을 차례로 대입하여 정당성을 확인하는 오프라인 사전공격에 취약하다.

1992년 Bellovin과 Merritt[4]는 사전공격[5]으로부터 보호되는 사용자가 쉽게 기억할 수 있는 패스워드를 사용한 encrypted key exchahge(EKE)를 제안했다. EKE 프로토콜은 사전에 두 참여자 사이에 안전하게 공통의 패스워드를 공유하며, 이후 인증과 두 참여자 사이의 공통의 세션키를 얻는다.

1995년 Steiner등은 모든 참여자들은 신뢰된 서버 S와 패스워드를 사전에 서로 공유하고 서버 S는 두 참여자 사이의 양방향 인증이 가능하도록 조정하는 three-party EKE 프로토콜 STW-3PEKE을 제안했다.

그러나 [1]에서 Lin, Sun, Hwang은 STW-3PEKE 프로토콜이 온라인 패스워드 추측 공격, 오프라인 패스워드 추측 공격[6]에 취약함을 지적했으며 이러한 공격을 예방하기 위해 서버가 영구적이며 공개적으로 알려진 공개키를 가지는 프로토콜 LSH-3PEKE를 제안했다. 하지만 통신에 참여하는 사용자는 서버의 공개키를 얻어야 하며 검증해야 되는데 이는 사용자에게 큰 부담을 준다. 2001년에 Lin등은 서버의 공개키가 필요없는 새로운 프로토콜 LSSH-3PEKE를 제안했다. LSSH-3PEKE는 서버의 공개키를 사용하지 않으므로 LSH-3PEKE가 가지는 부담을 줄였다.

패스워드 기반의 인증 기법은 평문-등가 기법과 검증자 기반 기법으로 나눌 수 있는데, 평문-등가 기법은 서버가 사용자의 패스워드나 비밀키를 복사하여 저장하는 방식이고 검증자 기반 기법은 서버는 사용자의 패스워드를 모르고 패스워드에 의해 생성되는 임의의 값(검증자)을 저장한다.

본 논문에서는 검증자 기반의 three-party 패스워드 프로토콜을 제안한다. 서버는 각 사용자의 패스워드는 모르면서 패스워드를 이용해서 생성된 값인 검증자를 가진다. 그리고 암호화를 사용하지 않으며 단지 Diffie-Hellman과 해쉬함수에 의해서만 프로토콜을 구성한다. 이렇게 함으로써 프로토콜이 간단해지며 좀 더 향상된 효율성을 가질 수 있다. 2장에서는 제안한 프로토콜에 대해서 살펴보고 3장에서는 제안한 프로토콜의 안정성에 대해서 살펴보고 효율성 측면에서 기존의 프로토콜과 비교해서 알아본다. 끝으로 4장에서는 결론을 내린다.

2. 제안하는 프로토콜

이번 장에서는 프로토콜에 사용되는 표기법과 제안한 프로토콜에 대해 자세히 설명한다.

2.1 용어 정의

프로토콜에 공통적으로 사용되는 용어와 표기법은 표 1에서 정의한다.

기호	내용
A,B	통신 참여자
S	인증 서버
P_A, P_B	$A(B)$의 패스워드
N_A, N_B, N_S	A, B, S에 의해 선택되는 랜덤 수
p, g	큰 소수, 생성자
$f_K(M)$	의사 난수 함수(PRF), MAC과 유사
K_{AB}, K_{BA}	A와 B사이의 공통의 세션키
$h(), H_1(), H_2()$	일방향 해쉬함수
$A \Rightarrow B : M$	A는 메시지 M을 B에게 전송

표 1 용어와 표기법

2.2 제안 프로토콜의 단계

● 설정단계

먼저 사용자 A, B는 검증자 값인 $V_A = h(A, P_A)$, $V_B = h(B, P_B)$ 를 계산한 후 서버에 사전 등록한다. 그리고 서버는 $R_S = g^{N_S} \bmod p$ 를 계산한 후 공개한다. 이후 A, B, S사이의 인증 및 키 교환은 다음과 같이 실행된다.

● 실행단계

[1단계] $A \Rightarrow B : A, R_A$

A는 랜덤한 수 N_A를 선택하고 $R_A = g^{N_A} \bmod p$ 를 계산한 다음 B에게 A, R_A 메시지를 보낸다.

[2단계] $B \Rightarrow A : A, B, X_B, R_B$

B는 $K_{B,S} = R_S^{N_B} \bmod p$ 를 계산한 후 $X_B = f_{K_{B,S}}(A, B, v_B')$ 를 계산한다. 여기서 $v_B' = h(B, P_B)$ 이다. 랜덤한 수 N_B를 선택하고 $R_B = g^{N_B} \bmod p$ 를 계산한다.

[3단계] $A \Rightarrow S : A, B, R_A, X_A, R_B, X_B$

A는 $K_{A,S} = R_S^{N_A} \bmod p$ 를 계산한 후 $X_A = f_{K_{A,S}}(A, B, v_A')$ 를 계산한다. 여기서 $v_A' = h(A, P_A)$ 이다. 계산한 값과 B로부터 받은 메시지를 포함해서 인증 서버 S에게 전송한다.

[4단계] $S \Rightarrow B : Y_{A,S}, Y_{B,S}$

S는 $K_{S,A} = R_A^{N_S} \bmod p$ 를 계산한 후 $X_A' = f_{K_{S,A}}(A, B, V_A)$ 를 계산한다. A로부터 받은 메시지 X_A와 같은지를 비교한다. 두 값이 같다면 S는 정당한 참여자 A임을 인증한다. 마찬가지로 S는 $K_{S,B} = R_B^{N_S} \bmod p$ 를 계산한 후 $X_B' = f_{K_{S,B}}(A, B, V_B)$ 를 계산한다. A로부터 받은 메시지 X_B와 같은지를 비교한다. 두 값이 같다면 B도 정당한 참여자임을 인증한다.

S는 $Y_{A,S} = h(g^{N_A}, g^{N_A N_S}, V_A)$ 와 $Y_{B,S} = h(g^{N_B}, g^{N_B N_S}, V_B)$를 계산한 후 B에게 전송한다.

[5단계] $B \Rightarrow A : Y_{A,S}, K_B'$

B는 $Y_{B,S}' = h(g^{N_B}, g^{N_S N_B}, v_B')$ 를 계산 후 S로부터 받은 메시지 $Y_{B,S}$와 비교한다. 두 값이 같다면 B는 정당한 인증 서버 S임을 인증한다.

B는 세션 키인 $K_{BA} = H_1(A, B, R_A^{N_B} \bmod p)$ 와 키 확인을 위한 값인 $K_B' = H_2(R_A^{N_B}, R_A) \bmod p)$를 계산한 다음 A에게 $Y_{A,S}, K_B'$ 를 전송한다.

[6단계] $A \Rightarrow B : K_A'$

A는 세션 키인 $K_{AB} = H_1(A, B, R_B^{N_A} \bmod p)$ 를 계산한다. 그리고 $H_2(R_B^{N_A}, R_A)$를 계산한 후 B로부터 받은 K_B'와 비교한다. 두 값이 같다면 A는 B가 정당한 참여자이며 동일한 세션키를 생성했음을 확인한다. 그런다음, A는 $K_A' = H_2(R_B^{N_A}, R_B)$ 를 계산 후 B에 전송한다. B는 $H_2(R_A^{N_B}, R_B)$를 계산 후 A로부터 받은 K_A'와 비교한다. 두 값이 같다면 B는 A가 정당한 참여자이며 동일한 세션키를 생성했음을 확인한다. 이후 A, B 는 동일한 세션키를 가지게 된다.

3. 제안한 프로토콜의 안전성 및 성능 분석

이번 장에서는 제안한 프로토콜의 안전성에 대해서 분석하고 기존의 몇 가지 프로토콜들과의 효율성 및 성능을 비교한다.

3.1 안전성 분석

• 사전 공격

사전공격은 공격자가 사용자나 서버로 위장해 패스워드 추측에 필요한 정보를 획득한 후 임의의 패스워드를 대입하여 획득한 정보와 비교하여 패스워드를 추측해낸다. 제안한 프로토콜에서 공격자가 $h(A,P')$ 를 대입하여 공격하더라도 $K_{A,S}, K_{B,S}$ 값을 구할 수 없기 때문에 사전 공격에 안전하다.

• 재전송 공격

사용자와 서버사이에 이미 주고 받은 메시지를 이용하여 공격한다. 제안한 프로토콜은 매 세션마다 임의의 값 g^{N_A}, g^{N_B}를 사용하기 때문에 재전송 공격이 불가능하다.

• 완전한 전방향 보안성

현재의 세션키가 노출되더라도 이전의 세션키들은 안전해야 한다. 제안한 프로토콜은 임의의 값 g^{N_A}, g^{N_B}를 사용하며 이전의 키 생성과는 독립적으로 생성되기 때문에 완전한 전방향 보안성이 제공된다.

• Denning-Sacco 공격

세션키가 노출되었을 경우 공격자는 이 세션키로부터 패스워드를 얻으려는 공격이다. 제안한 프로토콜은 세션키 생성시 패스워드에 관한 정보를 포함하고 있지 않으므로 이 공격으로부터 보호된다.

• 중간자 공격

공격자가 사용자와 서버사이에서 메시지를 가로채어 공격한다. 제안한 프로토콜에서 공격자가 X_A, X_B , $Y_{A,S}, Y_{B,S}$ 값을 얻을 수 있지만, 이산 대수 문제와 일방향 해쉬의 성질로부터 $K_{A,S}, K_{B,S}$ 값을 계산할 수 없으므로 이 공격으로부터 보호된다.

3.2 성능 분석

이번절에서는 기존의 프로토콜(LSH-3PEKE, LSSH-3PEKE)과의 비교를 통한 성능 및 효율성에 대해 알아본다.

	LSH-3PEKE			LSSH-3PEKE			제안 프로토콜		
	A	B	S	A	B	S	A	B	S
대칭키 암(복)호	2	2	2	1	1	2	0	0	0
지수 연산	2(7)	2(7)	0(6)	3	3	4	3	3	2
PRF 연산	0	0	0	4	4	4	1	1	2
랜덤 수	2	2	0	1	1	2	1	1	0
Hash	1	1	0	2	2	0	5	5	2
프로토콜 단계	5			7			6		

표 2 기존 프로토콜들과의 성능 비교

표 2는 기존 프로토콜들과 제안한 프로토콜의 통신 회수 및 연산량을 비교한 것이다. LSH-3PEKE와 LSSH-3PEKE는 패스워드 자체를 서버가 저장하는데 비해 제안한 프로토콜은 검증자 기반으로 프로토콜 실행시 서버의 연산 부담을 줄였다. 그리고 기존 프로토콜과는 다르게 암(복)호화를 사용하지 않았으며, 해쉬의 연산이 늘어났지만 이것은 연산량에 크게 영향을 미치지 않으므로 고려하지 않아도 된다.

4. 결 론

본 논문에서는 패스워드를 이용하여 생성한 검증자를 저장하는 검증자 기반의 three-party 키 교환 프로토콜을 설계하였다. 이산대수 문제의 어려움과 일방향 해쉬 함수를 이용하면서 서버측의 연산량 부담을 줄였으며, 암(복)호화를 사용하지 않았다. 그리고 기존 프로토콜의 안전성을 그대로 유지하면서 효율성이나 성능면에서 기존의 프로토콜들과 비교할 때 보다 효과적이다. 이후 추가적인 연구 방향은 참여자들측의 연산량 또한 줄이는 것이다.

5. 참고문헌

[1] C. L. Lin, H.M. 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.

[2] M. Steiner, G. Tsudik and M. Waidner, "Refinement and Extension of Encrypted Key Exchange", ACM Operating Systems Review, 29(3), pp. 22-30, 1995.

[3] C.L. Lin, H.M. Sun, M. Steiner and T. Hwang, "Three-party encrypted key exchange Without Server Public-Keys", Communications Letters, IEEE , vol. 5, no. 12, pp. 497-499, 2001.

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

[5] R. Morris and K. Thompson, "Password Security: A Case History", Communications of the ACM, 22(11), pp. 594-597, 1979.

[6] Y. Ding and P. Horster, "Undetectable On-line Password Guessing Attacks", ACM Operating Systems Review, 29(4), pp. 77-86, 1995.