검증자를 사용한 패스워드 기반의 인증 및 키 교환 프로토콜

반정^{O} 이재욱 김순자
경북대학교 전자공학과
{bahn^{O}, llkkllkk}@palgong.knu.ac.kr, snjkim@ee.knu.ac.kr

Password-based Authentication and Key Agreement Protocol using Verifier

Jung bahn^{0} Jae-Wook Lee Soon-Ja Kim
Dept. of Electronics Engineering, Kyungpook National University

요 약

패스워드 기반의 키 교환 프로토콜들은 참여자들이 쉽게 기억할 수 있는 자신의 패스워드를 사용하므로 단순성, 편리성, 이동성의 장점 때문에 광범위하게 사용되지만 완전한 전방향 보안성(perfect forward secrecy), 패스워드 추측공격과 Denning-Saccon 공격에 취약하다. 본 논문에서 제안한 검증자(verifier)를 사용한 패스워드 기반의 인증 및 키 교환 프로토콜은 키 교환 프로토콜 요구 사항을 만족하고, 알려진 공격으로부터 안전하며 DH(Diffie-Hellman) 키 교환 방법과 해쉬 함수만을 사용하기 때문에 기존의 프로토콜보다 구조가 간단하며 높은 효율성을 가진다.

1. 서 론

인터넷과 같이 개방형 네트워크 상에서 사용자와 서버간의 안전한 통신을 보장하기 위해서 인증, 기밀성, 무결성 등과 같은 보안서비스의 필요성이 증대하여 키 교환 프로토콜이 큰 관심을 얻고 있다. 대칭키나 공개키 기반의 키 교환 프로토콜([1])을 수행하기 위해서는 대칭키나 공개/개인키를 소유 하고 하고 있어야 하는데 키는 사람이 기억할 수 없기 때문에 안전한 저장장치에 보관해야하는 문제점이 있다. 그러나 패스워드 기반의 키 교환 프로토콜은 사람이 기억할 수 있는 패스워드를 사용하는 간단한 프로토콜이므로 널리 사용되고 있다. 패스워드 기반의 키 교환 프로토콜은 낮은 엔트로피를 가지기 때문에 패스워드 추측 공격에 취약하다.

패스워드 기반의 인증 프로토콜은 크게 평문 등가 기법과 검증자 기반 기법으로 나누어진다([2]). 평문 등가 기법은 사용자와 서버가 패스워드만으로 인증하기 때문에 효율적일 수 있지만 서버가 공격당해 공격자에게 패스워드가 노출되면 안전성은 크게 떨어진다. 평문 등가 기법에는 EKE([3]), DH-EKE([4]), SPEKE([5])등이 있고, 이 프로토콜들은 패스워드 추측공격과 Denning -Sacco 공격에 취약하다. 그러나 검증자 기반 기법은 서버에 패스워드로부터 생성된 검증자를 저장하고 사용자는 패스워드를 사용하여 인증하는 방법을 사용함으로써 서버의 패스워드 파일이 노출될 위험은 없다. 검증자 기반 기법에는 B-SPEKE([6]), SRP([2]), PAK([7]), AMP([8])등이 있다.

본 논문에서는 검증자를 사용한 패스워드 기반의 인증 및 키 교환 프로토콜을 제안한다. 제안한 프로토콜은 패스워드 추측공격, 재 전송 공격, Denning-Sacco 공격, 중간자 공격, Stolen-verifier 공격에 안전하면서도 완전한 전방향 보안성을 가지며 기존의 프로토콜과 비교하여 높은 효율성을 제공한다. 2장에서는 기존의 패스워드 기반 키 교환 프로토콜들에 대해 살펴보고, 3장에서는 제안한 프로토콜에 대해서 살펴보고 4장에서는 제안한 프로토콜의 안정성에 대해서 살펴보고 효율성을 기존의 프로토콜과 비교해서 알아본다. 끝으로 5장에서는 결론을 내린다.

2. 기존 연구

기존의 패스워드 기반의 키 교환 프로토콜의 종류가 여러 가지가 있지만 본 논문에서는 EKE와 AMP의 안전성 및 성능에 대해서 간략하게 살펴보고 필요한 요구 사항에 대해 설명한다([9]).

2.1 EKE

EKE는 서버가 패스워드를 저장함으로써 서버 손상시 패스워드가 직접적으로 노출된다. 그리고 사용자의 공개키로 암호화한 서버가 생성한 세션키를 사용자에게 보내기 때문에 세션키가 드러나게 되면 공격자는 이미 교환된 메시지를 이용하여 패스워드를 추측할 수 있다. 즉 Denning-Sacco공격에 취약하다.

2.2 AMP

AMP는 검증자를 서버에 저장하기 때문에 서버가 공격당하더라도 패스워드가 노출될 위험이 없다. 그리고 DH(Diffie-Hellman) 키 교환 방식을 이용하여 서버와 사용자가 같이 참여하여 세션키를 생성하고, 세션키에는 패스워드에 대한 정보가 없기 때문에 Denning-Sacco공격에 안전하다. 매 세션마다 새로운 N_A와 N_S 를 사용하여 세션키를 생성하므로 전방향 보안성이 제공된다. 그러나 AMP는 지수 연산량, 통신회수, 해쉬 함수 사용 회수등의 연산량이 많고, AMP상의 파라미터 ς를 안전하게 저장하기 위해서 스마트카드 같은 안전한 저장장치에 저장하가나 서버의 개인키(private key)로 암호화하여 저장해야 한다. 그리고 ς와 관련된 동작이 실행 될 때마다 서버의 런-타임 메모리에만 남아 있어야한다.

2.3 요구사항

• 객체 인증

실시간에 프로토콜에 참여하는 사용자와 서버가 서로 상대방에 대한 신원 확인하는 과정으로 공격자가 서버나 사용자로 가장하는 것을 방지하기 위하여 필요다.

• **키 신규성**
이전의 세션키로부터 현재의 세션키가 만들어 진다면 이전의 세션키를 알게 되면 현재의 세션키가 드러나게 되므로 매 세션마다 새로운 키의 생성이 요구 된다.

• **키 동의**
사용자와 서버는 세션키 생성에 함께 참여하고 3자는 세션키를 생성 할 수 없어야 한다. 이것은 키 교환 프로토콜의 기본 요구 사항이다.

• **키 확인**
정당한 사용자가 자신이 의도한 서버와 동일한 세션키를 공유하고 있다는 것이 확인 가능해야 한다. 이것은 중간자 공격에 의해 서로 다른 세션키를 공유 하는 것을 막을 수 있다.

3. 제안하는 프로토콜

이번 장에서는 앞으로의 프로토콜에 사용되는 용어를 정의하고 제안한 프로토콜에 대해 설명한다.

3.1 용어 정의

제안한 프로토콜에 공통적으로 사용되는 용어를 정리하면 표 1과 같다.

표 1 용어 정의

기 호	의 미
S, A	서버, 사용자
P_A	A의 패스워드
N_A, N_S	A, S에 의해 선택되는 랜덤 수
p, g	큰 소수, 생성자
$h(), H()$	일방향 해쉬함수
x	$h(A, P_A)$
V_A	서버에 저장되는 A의 검증자 (g^x)
K_{AS}, K_{SA}	A와 S사이의 세션키
$A \Rightarrow S : M$	A는 메시지 M을 S에게 전송

프로토콜의 두 참여자인 사용자(A)와 서버(S)는 Z_p^*상의 생성자인 g와 큰 소수 p를 미리 공유하고 있다. $h()$, $H()$는 암호학적으로 강한 일방향 해쉬 함수이다. 제안한 프로토콜은 DH(Diffie-Hellman)기반의 키 교환방식을 사용하고, 프로토콜이 성공적으로 완료되면 A와 S는 $K_{SA} = K_{AS} = H(g^{N_S N_A} \bmod p)$인 동일한 세션키를 공유하게 된다.

3.2 제안 프로토콜의 단계

• **설정단계**
먼저 사용자 A는 검증자 값인 $V_A = g^x \bmod p$,를 계산한 후 서버에 사전 등록한다. 이후 A와 S사이의 인증 및 키 교환은 다음과 같이 실행된다.

• **실행단계**
[1단계] $A \Rightarrow S$: A, R_A
A는 랜덤 수 N_A를 선택하고 Z_p상의 x의 덧셈에 대한 역원을 구한 후 $R_A = g^{N_A - x} \bmod p$를 계산한 다음 S에게 A, R_A 메시지를 전송한다.

[2단계] $S \Rightarrow A$: $S, R_S, h(S, A, K_{SA})$
S는 A에서 받은 R_A 에 서버가 저장하고 있는 A의 검증자 (V_A)를 곱한 후 세션키 $K_{SA} = H((R_A V_A)^{N_S} \bmod p) = H(g^{N_A N_S} \bmod p)$를 계산한다. S는 랜덤 수 N_S를 선택한 후 $R_S = V_A^{N_S} \bmod p = g^{xN_S} \bmod p$ 계산한 후 A에게 $S, R_S, h(S, A, K_{SA})$를 전송한다.

[3단계] $A \Rightarrow S$: $h(A, S, K_{AS})$
A는 S에서 넘어온 R_S에 Z_p^*상의 x의 곱셈에 대한 역원을 구한 후 $w = N_S x^{-1} \bmod p$계산한다. 그리고 세션키 $K_{AS} = H(R_S{}^w \bmod p) = H(g^{N_A N_S} \bmod p)$와 $h(S, A, K_{AS})$를 계산한 후 S에서 넘어온 $h(S, A, K_{SA})$와 $h(S, A, K_{AS})$를 비교 하여 같다면 A는 S를 정당한 서버임을 인증하게 되고, 동일한 세션키를 공유한 것을 확인할 수 있다. 그리고 A는 $h(A, S, K_{AS})$계산한 값을 S에게 전송한다.

[4단계]
S는 $h(A, S, K_{SA})$를 계산한 후 A에서 넘어온 $h(A, S, K_{AS})$를 비교 하여 같다면 S는 A를 정당한 사용자로 인증하게 되고, 동일한 세션키를 공유한 것을 확인할 수 있다.
이후 S와 A는 동일한 세션키를 공유한다.

4. 제안한 프로토콜의 안전성 및 성능 분석

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

4.1 안전성 분석

• **요구 사항**
서버와 사용자는 미리 설정한 패스워드와 검증자로 서로를 인증한다. 매 세션마다 새로운 사용자의 N_A와 서버의 N_S를 이용하여 세션키를 생성하므로 키 동의와 키 신규성을 제공한다. 마지막으로 해쉬함수를 이용하여 동일한 세션키가 생성되었는지 확인한다.

• **패스워드 추측공격**
패스워드 추측공격은 공격자가 추측한 패스워드 (P_A')를 메시지 $R_S, h(S, A, K_{SA}), R_A, h(A, S, K_{AS})$에 대입하여 비교함으로써 P_A'가 정확한지 비교한다. 그러나 제안한 프로토콜에서는 P_A'를 대입하더라도 이산대수 문제의 어려움 때문에 P_A'가 정확한 패스워드(P_A)인지 검증할 방법이 없다.

• 재전송 공격

사용자와 서버사이에 이미 교환한 메시지를 이용하여 공격한다. 제안한 프로토콜은 매 세션마다 임의의 값 R_A, R_S를 사용하기 때문에 새로운 세션키가 생성되고, 공격자는 이산대수문제의 어려움으로 N_A, N_S를 알 수 없어서 새로운 세션키를 알지 못하므로 재전송 공격이 불가능하다.

• 완전한 전방향 보안성

패스워드가 노출되더라도 세션키들은 안전해야 한다. 제안한 프로토콜은 임의의 값 g^{N_A}, g^{N_S}를 이용하여 세션키 $(K_{AS}= K_{SA} = h(g^{N_AN_S} \bmod p))$를 생성하므로 패스워드를 알아도 세션키를 알 수 없으므로 완전한 전방향 보안성을 만족한다.

• Denning-Sacco 공격

세션 키가 노출되었을 경우 공격자는 이 세션키로부터 패스워드를 얻으려는 공격이다. 제안한 프로토콜은 세션키 $(K_{AS}= K_{SA} = h(g^{N_AN_S} \bmod p))$를 생성할 때 패스워드에 관한 정보를 포함하고 있지 않으므로 이 공격으로부터 안전하다.

• 중간자 공격

수동적인 공격자가 사용자와 서버사이에서 메시지를 가로채어 공격한다. 제안한 프로토콜에서 공격자가 R_A, R_S, $h(S, A, K_{SA})$, $h(A, S, K_{AS})$ 값을 얻을 수 있지만, 이산 대수 문제와 일방향 해쉬의 성질로부터 세션키를 계산할 수 없다. 적극적인 공격자가 R_A, R_S를 수정하여 상대방에게 전송한다면 이 수정된 값들은 A와 S에 의해 K_{AS}, K_{SA}를 생성 하는데 각각 사용된다. 그러나 공격자는 패스워드와 검증자를 알 수 없으므로 동일한 세션키를 생성할 수 없다. 그러므로 중간자 공격으로부터 안전하다.

• Stolen-verifier 공격

공격자가 V_A값을 알면 자신이 만든 N_A'를 이용하여 R_A'를 얻을 수 있지만 패스워드를 모르기 때문에 Z_b*상의 x의 곱셈에 대한 역원을 계산 할 수 없어서 3단계 메시지를 만드는데 필요한 세션키를 계산할 수 없다. 그러므로 Stolen-verifier 공격에 안전하다.

4.2 성능 분석

이번 절에서는 기존의 프로토콜과 제안한 프로토콜을 비교하여 성능 및 효율성에 대해 알아본다.

표 2 기존 프로토콜들과의 성능 비교

	통신	지수 연산		랜덤 수		해쉬 함수	
	회수	A	S	A	S	A	S
B-SPEKE	4	4	4	1	2	2	2
SRP	4	3	3	1	2	4	3
PAK	3	3	2	1	1	3	2
AMP	4	2	4	1	1	4	3
제안 프로토콜	3	2	2	1	1	2	2

제안한 프로토콜, PAK과 AMP는 곱셈에 대한 역원을 한번씩 계산하지만 지수 연산량에 비교하면 전체 프로토콜 연산량에 큰 영향을 미치지 않으므로 고려하지 않아도 된다. 표2에서 보는 바와 같이 기존의 다른 프로토콜들의 지수 연산, 통신 회수, 랜덤 수 생성 회수와 해쉬 함수 사용회수 등을 비교하면 제안한 프로토콜이 효율성이 높다는 것을 확인 할 수 있다.

5. 결 론

정보화 사회에서 인터넷이 발달됨에 따라 인터넷을 통한 주요 문서 및 정보의 유통이 급격히 증가하였다. 따라서 온라인상에 노출되는 정보들에 대한 불법적인 위·변조 및 신분위장 등 각종 위협이 예상되고 있다. 그러므로 인터넷상에서 사용자와 정보 제공자간의 정보보호를 위해 상호간의 인증(authentication)과 메시지의 암호화가 중요한 문제로 대두되었다.

본 논문에서는 패스워드를 이용하여 생성한 검증자를 서버에 저장하는 검증자 사용한 패스워드 기반의 인증 및 키 교환 프로토콜을 제안하였다. 이산대수 문제의 어려움과 일방향 해쉬 함수를 사용하여 안전하며, DH(Diffie-Hellman) 키 교환 방법과 해쉬 함수만을 사용하여 구조가 간단하고 연산량이 적어 기존의 프로토콜과 비교하면 제안한 프로토콜이 높은 효율성을 가진다.

참고문헌

[1] C. Body, "Towards a classification of key Agreement Protocols", Computer Security Foundations WorkShop, Proceeding., eighth IEEE 13-15, pp. 38-43, 1995.

[2] T.wu, "Secure remote password protocol", In Network and Distributed System Security Symposium (NDSS), pp.97-111, 1998.

[3] 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.

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

[5]D.P. Jablon, "Strong password-only authenticated key exchange", ACM Computer Communications Review, pp. 5-26, 1996.

[6] D.P. Jablon, "Extended password key exchange protocol", WETICE Workshop on Enterprise Security, pp. 248-255,1997.

[7] V. Boyko, P. Mackenzie and S. Patel, "Provably secure password key exchange using Diffie-Hellman", Advances in Cryptology-EUROCRYPT'2000 pp. 156-171, 2000.

[8] T. Kwon, "Ultimate Solution to Authentication via Memorable Password", Presented to IEEE P1363a, 2000

[9] C. Boyd and D. Park, "Public Key Protocols for Wireless Communications", in the 1st International Conference on Information Security and Cryptology(ICISC'98), pp.47-57, 1998.