간단한 패스워드 검증자 기반의 키 교환 프로토콜

이성운*, 김우헌*, 김현성**, 유기영*

*경북대학교 컴퓨터공학과, **경일대학교 컴퓨터공학과

Simple Password verifier-based Key Agreement Protocol

Sung-Woon Lee*, Woo-Hun Kim*, Hyun-Sung Kim**, Kee-Young Yoo*

*Department of Computer Engineering Kyungpook Univ.
**Department of Computer Engineering Kyungil Univ.

요 약

본 논문에서는 패스워드 검증자(verifier) 기반의 인증 및 키 교환 프로토콜을 제안한다. 제안한 프로토콜은 패스워드 기반 프로토콜들의 가장 큰 문제점인 패스워드 추측 공격과 중간 침입자 공격, 그리고 Denning-Sacco 공격에 안전하며, 완전한 전방향 보안성을 제공할 수 있다. 그리고 패스워드 검증자를 기반으로 하기 때문에 서버의 패스워드 파일의 노출에도 안전하다. 제안된 프로토콜의 안전성은 이산대수 문제와 Diffie-Hellman 문제의 어려움, 그리고 해쉬 함수의 암호학적 강도에 기반을 두고 있다. 또한 제안한 프로토콜은 구조가 간단하고 병렬 처리가 가능하기 때문에 안전하다고 알려진 기존의 프로토콜들과 비교하여 효율적이다.

I. 서론

통신 및 네트워크 기술의 발전은 전자 상거래, 원격지 사용자간의 통신, 응용서버와의 통신 등의 서비스를 창출하였다. 특히 인터넷과 같은 개방형 네트워크 상에서 통신 상대간에 안전한 통신을 하기 위해서는 전송될 정보를 암호화하여야 하며, 이를 위해서 통신 상대자간에 공통으로 사용할 수 있는 키의 공유가 우선되어야 한다. 이때 통신 상대자간에는 통신을 통해 정보를 교환하고 있는 상대가 실제 의도한 상대인지를 확인하는 인증 과정이 반드시 필요하다. 또한 이러한 인증 기능은 사용자가 응용 서버로부터의 서비스를 받기 위해서도 요구된다. 따라서 암호화키를 공유하는 문제와 사용자 인증 문제는 안전한 정보 교환과 개인 정보보호를 위해 해결해야 할 중요한 문제이며, 이를 위해서는 보다 효율적인 프로토콜 개발이 절실히 요구된다.

사용자 인증 방식은 인증의 기반이 되는 요소가 무엇이냐에 따라 다음과 같이 세 가지로 분류된다. 첫째, 목소리 식별, 망막 검사 등과 같이 사용자의 물리적인 특징을 이용하는 인증 방법, 둘째, ID card나 smart card 등과 같이 사용자가 소유한 물건을 통한 인증 방법, 셋째, 패스워드와 같이 사용자가 알고 있는 지식을 통한 인증 방법이다. 첫 번째와 두 번째 방식은 강력한 보안을 위해 사용되기는 하지만 그에 따르는 부가적인 하드웨어 비용이 크다. 반면 세 번째 방식은 별도로 필요한 장비가 없기 때문에 큰 비용을 들이지 않고도 쉽게 사용될 수 있어 많이 이용되고 있으며 패스워드를 이용한 프로토콜들이 이에 해당된다. 그러나 낮은 엔트로피를 가지는, 즉 사람이 기억할 수 있는 패스워드를 이용해야 하므로 패스워드 추측공격에 취약할 수 있다.

패스워드를 기반으로 하는 인증 및 키 교환 프로토콜들은 크게 두 종류로 분류될 수 있다[8]. 첫째는 동일 패스워드(balanced password) 기반의 프로토콜로서 두 참여자는 같은 한 개의 패스워드를 사용하여 프로토콜을 수행한다. 이 방식은 피어투피어 형태의 통신에는 효율적으로 사용될 수 있지만 클라이언트 서버 환경에 사용된다면 패스워드 파일이 공격자에게 노출될 경우 모든 사용자의 패스워드들이 노출되게 되어 안전성이 크게 떨어질 수 있다. 둘째는 패스워드 검증자(password verifier) 기반의 프로토콜로서 동일 패스워드 기반의 프로토콜과는 달리 한 참여자는 클라이언트로,

다른 한 참여자는 서버의 역할을 수행하는 환경에서 사용될 수 있다. 클라이언트는 패스워드를 사용하고, 서버는 클라이언트의 패스워드를 가공한 결과 값을 패스워드 파일에 미리 저장해두고 프로토콜 수행 중에 해당 클라이언트에 대한 인증을 위한 검증 데이터로 사용한다. 서버에 저장된 패스워드를 가공한 이 정보를 검증자(verifier)라고 한다. 이 방식은 서버의 패스워드 파일에 패스워드에 대한 검증자 만이 저장되어 있기 때문에 패스워드 파일이 노출되더라도 공격자는 이 검증자만을 가지고 직접적으로 클라이언트로 위장하여 서버의 인증을 받을 수 없다. 그러나 검증자를 획득한 공격자는 서버로 위장할 수는 있고, 많은 비용이 드는 사전 공격(dictionary attack)을 수행하면 패스워드를 알아낼 수도 있다. 그러므로 이 논문에서 앞으로 사용하는 'Stolen-verifier 공격에 안전하다'는 의미는 다른 프로토콜들과 동일하게 '검증자를 얻는 공격자가 클라이언트로 직접 위장할 수 없다'는 것을 말한다. 이 프로토콜들로는 A-EKE[2], B-SPEKE[5], SRP[6], SNAPI-X[7], PAK-X[3], 그리고 AMP[4] 프로토콜 등이 있다.

본 논문에서는 패스워드 검증자를 기반으로 하는새로운 키 교환 프로토콜을 제안한다. 제안된 프로토콜의 안전성은 이산대수 문제와 Diffie-Hellman 문제의 어려움과 해쉬함수의 암호학적 강도에 기반을 두고 있다. 제안한 프로토콜은 중간 침입자 공격(man-in-the-middle attack), 패스워드 추측 공격(password guessing attack), Denning-Sacco 공격, Stolen-verifier 공격에 안전하며, 완전한 전방향 보안성(perfect forward secrecy)을 제공한다. 제안한 프로토콜은 기존의 잘 알려진 프로토콜들과 비교하여 여러 측면에서 좋은 성능을 가진다.

II. 제안한 프로토콜

본 장에서는 패스워드를 이용하여 참여자들 사이에 서로를 인증하고 세션키를 공유할 수 있는 패스워드 검증자 기반의 키 교환 프로토콜을 제안한다. 제안한 프로토콜은 Diffie-Hellman 방식[1]의 키 교환을 수행한다.

프로토콜의 두 참여자 클라이언트(A)와 서버(B)는 합법적인 참여자들이다. A와 B는 안전하게 Z_n^* 상의 생성자인 g와 큰 소수인 n를 미리 공유하고 있다고 가정한다. 또한 A는 패스워드 π를 소유하고 있고 B는 A의 id와 패스워드 검증자 $v = g^{h(A,B,\pi)}$를 패스워드 파일에 저장하고 있다고 하자. $h()$는 일방향 해쉬함수(one-way hash function)이다. 프로토콜이 성공적으로 완료하면 A와 B는 $K = h(K_A) = h(K_B) = h(g^{ab})$를 세션키로 공유하게 된다. 간편함을 위해 "mod n" 연산은 생략한다. 효율적인 수행을 위해 프로토콜이 시작하면 A는 $v' = g^{h(A,B,\pi)}$를 미리 계산하여 둔다. 제안된 프로토콜은 다음과 같이 수행한다.

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

2단계. B는 패스워드 파일로부터 A의 검증자 v를 검색한다. 그리고 임의의 정수 b를 선택하여 $X_B = (v)^b \oplus v = g^{bh(A,B,\pi)} \oplus g^{h(A,B,\pi)}$를 계산하여 A에게 전송한다. 그리고 B는 A의 응답을 기다리는 동안 다음과 같이 K_B, V_B, 그리고 V_A'를 계산한다.

$$K_B = (X_A \oplus v)^b = g^{ab}$$
$$V_B = h(X_A, K_B) = h(g^a \oplus g^{h(A,B,\pi)}, g^{ab})$$
$$V_A' = h(X_B, K_B) = h(g^{bh(A,B,\pi)} \oplus g^{h(A,B,\pi)}, g^{ab})$$

3단계. A는 B로부터 X_B를 받은 후에 $X_A \doteq X_B$인지를 검사한다. 같지 않다면 다음과 같이 K_A와 V_A를 계산하고 V_A를 B에게 전송한다.

$$K_A = (X_B \oplus v')^{ah(A,B,\pi)^{-1}} = g^{ab}$$
$$V_A = h(X_B, K_A) = h(g^{bh(A,B,\pi)} \oplus g^{h(A,B,\pi)}, g^{ab})$$

그리고 A는 B의 응답을 기다리는 동안 $V_B' = h(X_A, K_A) = h(g^a \oplus g^{h(A,B,\pi)}, g^{ab})$를 계산한다.

4단계. B는 A로부터 V_A를 받은 후에 $V_A \doteq V_A'$를 검사한다. 만약 같다면 B는 K_A가 정확하다고 확신한다. 그리고 V_B를 A에게 전송한다.

5단계. A는 B로부터 V_B를 받은 후에 $V_B \doteq V_B'$를 검사한다 만약 같다면 A는 K_B가 정확하다고 확신한다.

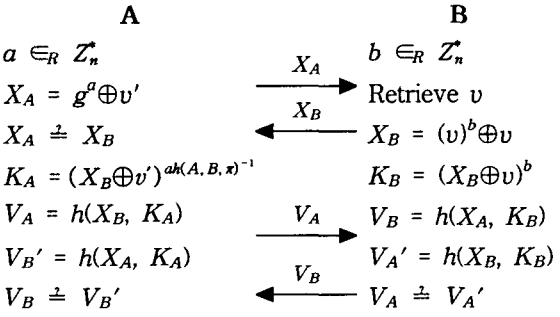

그림 1: 제안한 프로토콜

III. 안전성 분석

제안된 프로토콜의 안전성은 다음과 같은 산술시간에 풀기 어렵다고 알려진 두개의 어려운 문제

들과 사용된 해쉬함수의 암호학적 강도에 기반을 두고 있다.

이산 대수 문제. 곱셈 군 Z_n^*에서 생성자 g와 한 원소 g^a가 주어졌을 때 a를 계산하는 문제이다.

Diffie-Hellman 문제. 곱셈 군 Z_n^*에서 생성자 g와 두 원소 g^a와 g^b가 주어졌을 때 g^{ab}를 계산하는 문제이다.

우리는 제안한 프로토콜이 다양한 공격들에 대하여 안전하다는 것을 보이고자 한다.

중간 침입자 공격

일반적으로 키 교환 프로토콜은 안전하지 않은 통신상에서의 메시지 교환을 통해 서로를 인증하고 세션키를 공유한다. 그래서 공격자는 통신선로 중간에서 전송 메시지들을 도청(eavesdropping)하여 패스워드나 세션키의 정보를 알아내려고 할 수 있다. 그리고 전송 메시지들을 수정(modification), 반송(reflection), 또는 이전 세션의 메시지들을 저장해 두었다가 다음 세션들에서 재전송(replay)하는 방법 등으로 참여자들이 알지 못한 상태에서 잘못된 세션키를 공유하도록 유도할 수도 있다. 또한 정당한 참여자로 위장(impersonation)하여 다른 정당한 참여자와 정상적인 방법으로 세션키를 공유하려고 할 수 있다. 키 교환 프로토콜은 이러한 공격들에 대하여 세션키와 패스워드에 관한 정보를 노출시켜서는 안되며 잘못된 세션키의 공유를 탐지할 수 있어야 한다.

첫째로, 수동적인 공격을 고려하자. 공격자는 전송 메시지들을 도청을 하여 $X_A = g^a \oplus g^{h(A,B,\pi)}$, $X_B = g^{bh(A,B,\pi)} \oplus g^{h(A,B,\pi)}$, $V_A = h(g^{bh(A,B,\pi)} \oplus g^{h(A,B,\pi)}, g^{ab})$, $V_B = h(g^a \oplus g^{h(A,B,\pi)}, g^{ab})$를 얻을 수 있다. 그러나 공격자가 이 값들을 획득한다 하더라도 π와 K를 계산할 확률은 이산대수 문제와 Diffie-Hellman 문제 때문에 무시할만하다.

둘째로, 적극적인 공격자의 수정 공격을 고려하자. 공격자가 X_A와 X_B를 중간에서 수정하여 상대에게 전송한다면, 이 위조된 값들은 A와 B에 의해 K_A와 K_B를 생성하는데 각각 사용되게 된다. 그러나 A는 임의의 정수 a를 사용하여 K_A를 계산하고 B는 임의의 정수 b를 사용하여 K_B를 계산하기 때문에 K_A와 K_B의 값이 같게 될 확률은 무시할만하다. 결국, 검증단계에서 검증 값이 다르게 되므로 이 공격은 검증단계에서 탐지되게 된다.

셋째로, 적극적인 공격자의 재전송 공격을 고려하자. 재전송 공격은 이전 세션의 전송 메시지들을 저장해 두었다가 이후 세션들에 이용하는 공격이다. 그러나 매 세션마다 각 참여자들은 새로운 임의의 난수 a와 b를 생성하여 사용한다. 공격자가 이 값들을 알 수 있는 확률은 무시할 만하다.

넷째로, 적극적인 공격자의 반송 공격을 고려하자. 즉 공격자는 통신선로 중간에서 A가 B에게 보낸 X_A와 V_A를 A에게 되돌려 보내어 잘못된 세션키 생성을 유도하려 할 수 있다. 그러나 3단계에서 A는 B로부터 X_B를 받은 후에 $X_A \neq X_B$인지를 검사하기 때문에 이러한 공격은 성공할 수 없다.

다섯째로, 공격자는 합법적인 참여자로 위장하여 정상적인 방법으로 다른 합법적인 참여자와 세션키를 공유하려고 할 수 있다. 그러나 이러한 위장 공격은 공격자가 패스워드를 알지 못하기 때문에 검증 단계에서 탐지될 수밖에 없다.

결국 제안한 프로토콜들은 이와 같은 중간 침입자 공격들에 안전하다.

패스워드 추측 공격

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 제한함으로서 쉽게 조치될 수 있다. 그러나 공격자는 안전하지 않은 통신상의 메시지를 도청하거나 정당한 사용자로 가장하여 다른 사용자와 세션키 교환 시에 발생하는 정보들을 모아 오프라인으로 패스워드에 관한 정보를 알아내려고 할 수 있다.

먼저 도청한 메시지를 이용한 수동적인 패스워드 추측 공격을 고려하자. 공격자는 메시지 X_A, X_B, V_A, V_B를 가로채 저장하고, 패스워드로 사용될 수 있는 π'를 추측한다. 그리고 π'을 도청한 값들에 적용하여 비교함으로 검증한다. 이를 모든 패스워드 범위에 대하여 반복 수행함으로써 추측한 π'가 참여자들이 사용하고 있는 정확한 π인지를 확인해야 한다. 그러나 제안된 프로토콜들에서는 전송 메시지인 X_A, X_B, V_A, V_B에 π'를 적용하여도 π'가 정확한지를 검증할 방법이 없다.

또한 공격자가 정당한 참여자로 위장한 패스워드 추측 공격을 고려해보자. 먼저, 공격자가 A로 위장했다면 자신이 만든 a, g^a, $g^a \oplus g^{h(A,B,\pi')}$와 B로부터 받은 $g^{bh(A,B,\pi)} \oplus g^{h(A,B,\pi)}$ 값들을 얻을 수 있다. 그러나 이 자료들을 이용해서는 π'가 정확한지를 검증할 방법이 없다. 그리고, 공격자가 B로 위장했다면 자신이 생성한 b, g^b, $g^{h(A,B,\pi')}$, $g^{bh(A,B,\pi')}$와 A로부터 받은 $g^a \oplus g^{h(A,B,\pi)}$, $h(g^{bh(A,B,\pi')} \oplus$

$g^{h(A,B,\pi')}$, $(g^{b\cdot h(A,B,\pi')} \oplus g^{h(A,B,\pi')})^{a\cdot h(A,B,\pi)^{-1}}$ 값들을 얻을 수 있다. 그러나 이 값들을 이용해서도 π'가 정확한지를 검증할 방법이 없다. 그러므로 제안된 프로토콜들은 패스워드 추측 공격에 안전하다.

Denning-Sacco 공격

Denning-Sacco 공격은 세션키가 노출되었을 때 공격자가 패스워드에 관한 정보를 얻고자 하는 공격이다. 제안된 프로토콜들에서 공격자가 임의의 세션에서 도청을 통해 X_A, X_B, V_A, V_B를 얻었고, 세션키 $h(g^{ab})$가 공격자에게 노출되었다고 가정하자. 그러나 이산대수 문제와 Diffie-Hellman 문제의 어려움 때문에 이 정보들로부터 패스워드를 구하는 것은 무시할만하다.

완전한 전방향 보안성

완전한 전방향 보안성을 제공하기 위해서는 패스워드가 공격자에게 노출되었다 할지라도 이전의 세션키들은 안전해야 한다. 제안된 프로토콜들에서 공격자에게 패스워드 π가 노출되었다고 하자. 공격자는 도청을 통해 X_A, X_B, V_A, V_B를 얻을 수 있다. 그러나 이 정보들로부터 세션키인 $h(g^{ab})$를 구할 수 있는 확률은 이산대수 문제와 Diffie-Hellman 문제의 어려움 때문에 무시할만하다.

Stolen-verifier 공격

Stolen-verifier 공격은 서버로부터 패스워드 검증자를 훔친 공격자가 직접적으로 합법적인 사용자로 가장하려는 공격을 의미한다. 제안된 프로토콜에서 서버에 저장된 패스워드 검증자는 $v = g^{h(A,B,\pi)}$ 이다. 이 자료를 훔친 공격자는 새로운 세션의 3단계에서 사용해야 하는 π를 직접적으로 계산할 수 없다. 그러므로 패스워드 검증자를 도난 당했을 때 위험이 감소된다고 볼 수 있다.

V. 효율성 분석

프로토콜 / 분석요인	통신 횟수	랜덤 정수 생성 횟수	지수연산 사용횟수			해쉬함수 사용횟수			대칭키 암호화 횟수
			A	B	병렬	A	B	병렬	
A-EKE[2]	5	2	4	4	6	2	1	2	4
B-SPEKE[5]	4	3	3	4	6	2	2	2	0
SRP[6]	4	2	3	3	4	4	3	4	0
SNAPI-X[7]	5	5	5	4	7	4	3	6	0
PAK-X[3]	3	3	4	4	8	5	5	7	0
AMP[4]	4	2	2	4	5	4	3	4	0
Ours	4	2	3	2	3	3	3	3	0

표 1: 기존 프로토콜들과의 효율성 비교

우리는 제안된 프로토콜을 A-EKE, B-SPEKE, SRP, SNAPI-X, PAK-X, 그리고 AMP와 같은 기존에 잘 알려진 패스워드 검증자 기반의 프로토콜들과 표 1에서 비교한다.

VI. 결론

본 논문에서는 패스워드 검증자 기반의 새로운 키 교환 프로토콜을 제안하였다. 이 프로토콜은 중간 침입자 공격(man-in-the-middle attack), 패스워드 추측 공격(password guessing attack), Denning-Sacco 공격, Stolen-verifier 공격에 안전하며, 완전한 전방향 보안성(perfect forward secrecy)을 제공한다. 더욱이 제안한 프로토콜은 구조적으로 매우 간단하고 병렬성을 제공하기 때문에 기존의 잘 알려진 프로토콜들과 비교하여 효율적이다.

참고문헌

[1] Diffie W., and Hellman M.E., New directions in cryptography, IEEE Trans., IT-22, 1976, (6), pp. 644-654.

[2] S. Bellovin and M. Merritt. Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password-file compromise, ACM Conference 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, Advances in Cryptology-EUROCRYPT'2000, pp. 156-171, 2000.

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

[5] D. Jablon. Extended password key exchange protocols, WETICE Workshop on Enterprise Security, 1997.

[6] T. Wu. Secure remote password protocol, Internet Society Symposium on Network and Distributed System Security, 1998.

[7] P. MacKenzie, S. Patel, and R. Swaminathan. Password-authenticated key exchange based on RSA. In ASIACRYPT2000.

[8] IEEE. Standard Specifications for Public Key Cryptography, IEEE1363, 2002.