사전공격에 안전한 패스워드 기반 키 분배 프로토콜에 관한 연구

원동규*, 정영석*, 오동규*, 곽 진*, 원동호*

*성균관대학교, 컴퓨터공학과

A study on the Safe Password based Key Distribution Protocol against Dictionary Attack

Dongkyu Won*, Youngseok Chung*, Dongkyu Oh*, Jin Kwak*, Dongho Won*

*Department of Computer Engineering, Sungkyunkwan Univ.

요 약

본 논문에서는 사용자 인증에 사용되는 패스워드 검증자의 안전성을 더욱 보강한 새로운 패스워드 검증자 기반 키 분배 프로토콜을 제안한다. 기존 패스워드 기반 키 분배 프로토콜 방식은 네트워크 상에서 패스워드의 안전한 전송이 어려웠고, 패스워드 파일의 안전한 보호가 어렵다는 문제가 있었다. 이에 패스워드 파일을 그대로 서버에 저장하지 않고 패스워드를 사용하여 생성한 검증자(verifier)를 저장하게 함으로써 패스워드 파일을 보다 안전하게 보호할 수 있게 되었으며, 서버가 사용자의 패스워드를 알지 못하더라도 검증자를 사용한 증명방식을 통해 사용자를 인증할 수 있게 되었다. 본 논문에서는 사용자와 서버의 비밀정보로 만든 새로운 형태의 검증자를 사용하고, 사용자는 다른 저장정보 없이 기억하고 있는 ID와 패스워드만을 사용하여 키 분배를 수행하는 패스워드 검증자 기반 키 분배 프로토콜을 제안한다. 제안하는 프로토콜의 안전성 분석을 위해 active impersonation과 forward secrecy, man-in-the-middle attack, off-line dictionary attack 등의 공격 모델을 적용하였다.

I. 서론

사용자 인증(User Authentication)은 네트워크 상에서 통신하는 상대방의 신원을 확인하는 것이다. 이는 통신 개체들이 동일한 세션키를 공유하기 위해 수행하는 키 분배 과정에 반드시 필요하다. 패스워드 기반 키 분배 프로토콜[1]은 개체 인증을 제공하며, 세션키를 생성하는 프로토콜로, 대칭키나 비대칭키와 같이 긴 길이의 키를 사용하는 키 분배 프로토콜에 비해 사용자가 기억하기 용이한 길이의 비밀정보를 사용하기 때문에 하드웨어의 요구사항이 적고 편리하며, 간편하다는 장점 때문에 널리 사용되고 있다. 하지만 패스워드 기반 인증 방법은 정보량적인 측면에서 낮은 엔트로피(Low Entropy)를 가지기 때문에 패스워드에 대한 추측 공격(Guessing Attack)에 취약하며, 서버에 저장되어 있는 패스워드 파일이 공격자에게 노출되었을 경우, 사전공격(Dictionary Attack)이 가능하다는 문제점을 가지고 있다. 이에 패스워드 파일을 그대로 사용했던 EKE[2], DH-EKE[2], SPEKE[3] 등과 같은 키 분배 프로토콜에서 패스워드 파일을 그대로 서버에 저장하지 않고 패스워드를 사용하여 생성한 검증자를 저장한 후 이를 인증에 사용하는 방식의 프로토콜들이 등장했다. (B-SPEKE[4], PAK-X[5], SRP[6], AMP[7]) 본 논문에서는 사용자에 의해서만 검증자가 계산되어 전송되고, 서버는 그 검증자를 사용자 인증에 사용하는 방식과 다르게 서버와 사용자 양쪽의 비밀정보로 검증자를 생성한 후 공개 정보로 사용하

고, 서버와 사용자는 서로의 인증을 위해 서버의 비밀키와 사용자의 패스워드를 사용하는 키 분배 프로토콜을 제안한다. 제안한 키 분배 프로토콜은 Active Impersonation, Forward Secrecy, Man-in-the-middle Attack, Off-line Dictionary Attack에 안전하며, 계산량적 측면에서 효율적인 프로토콜이다.

II. 제안하는 키 분배 프로토콜

1. 시스템 파라미터

본 논문에서 사용되는 시스템 파라미터는 다음과 같다.

- π : 사용자 A의 패스워드(Password)
- V : 서버 B의 검증자(Verifier)
- w : 서버 B의 비밀키
- p : $GF(p)$를 정의하는 큰 소수
- q : $q \mid p-1$
- g : Z_p에서 위수 $p-1$을 갖는 원시원소
- r_X : 개체 X가 생성한 랜덤수
- $h(\ )$: 일방향 해쉬 함수
- $\|$: 연접(concatenation)

2. 등록과정

제안하는 프로토콜에서 사용자는 자신의 ID와 패스워드 정보만으로 사용자 인증과정과 키 분배 과정을 동시에 수행한다. 사용자 A와 서버 B사이의 사용자 인증과 키 분배 프로토콜을 안전하게 수행하기 위해 사용자의 패스워드를 검증하는 검증자 V를 서버에 저장하는 등록과정이 필요하다. 등록과정에서 중간값 R과 사용자의 ID는 안전한 채널(secure channel)을 통해 전달되어진다. 안전한 채널은 사용자와 서버간에 오프라인(offline)을 통한 전달이나 안전한 서명과 암호알고리즘을 사용하여 전달하는 방식을 의미한다. 등록과정은 초기에 한번만 수행한다. 등록과정은 다음과 같다.

① 사용자 A는 ID와 원시원소 g에 패스워드 π의 역수를 지수승하여 생성한 중간값 R을 안전한 채널을 통해 서버 B에 전송한다.

$$R = g^{\pi^{-1}} \pmod{p}$$

② 서버 B는 자신의 비밀키 w의 역수값을 계산한 후, 수신한 중간값 R에 지수승 해주어 검증자 V를 생성한다. 생성한 검증자 V와 서버 B의 비밀키 w를 각각 다른 안전한 장소에 저장한다.

$$V = R^{w^{-1}} \pmod{p}$$

3. 키 분배 프로토콜

제안하는 패스워드 검증자 기반 키 분배 프로토콜은 검증자 V가 사용자의 패스워드 π만으로 생성되어 서버에게 전송해 주는 기존의 키 분배 프로토콜과는 다르게, 사용자의 패스워드 정보 π와 서버의 비밀키 정보 w로 검증자를 생성하여 서버에 저장하는 방식이다. 서버와 사용자의 비밀정보로 이루어졌기 때문에 검증자 V가 공격자에게 노출이 된다 하더라도, 공격자가 정당한 사용자로 위장하거나 사용자와 서버의 비밀정보를 계산할 수 없다. 또한 사용자는 기억하고있는 자신의 ID와 패스워드로만 키 분배 프로토콜을 수행하기 때문에 데이터 저장매체 등을 가지고 다닐 필요없이 암호연산이 가능한 곳이면, 어느곳에서도 키 분배

사용자 A		서버 B
$R = g^{\pi^{-1}} \pmod{p}$	$\xrightarrow{\quad id,\ R \quad}$ (Secure Channel)	$R = g^{\pi^{-1}} \pmod{p}$ $V = R^{w^{-1}} \pmod{p}$

그림 1: 등록 과정

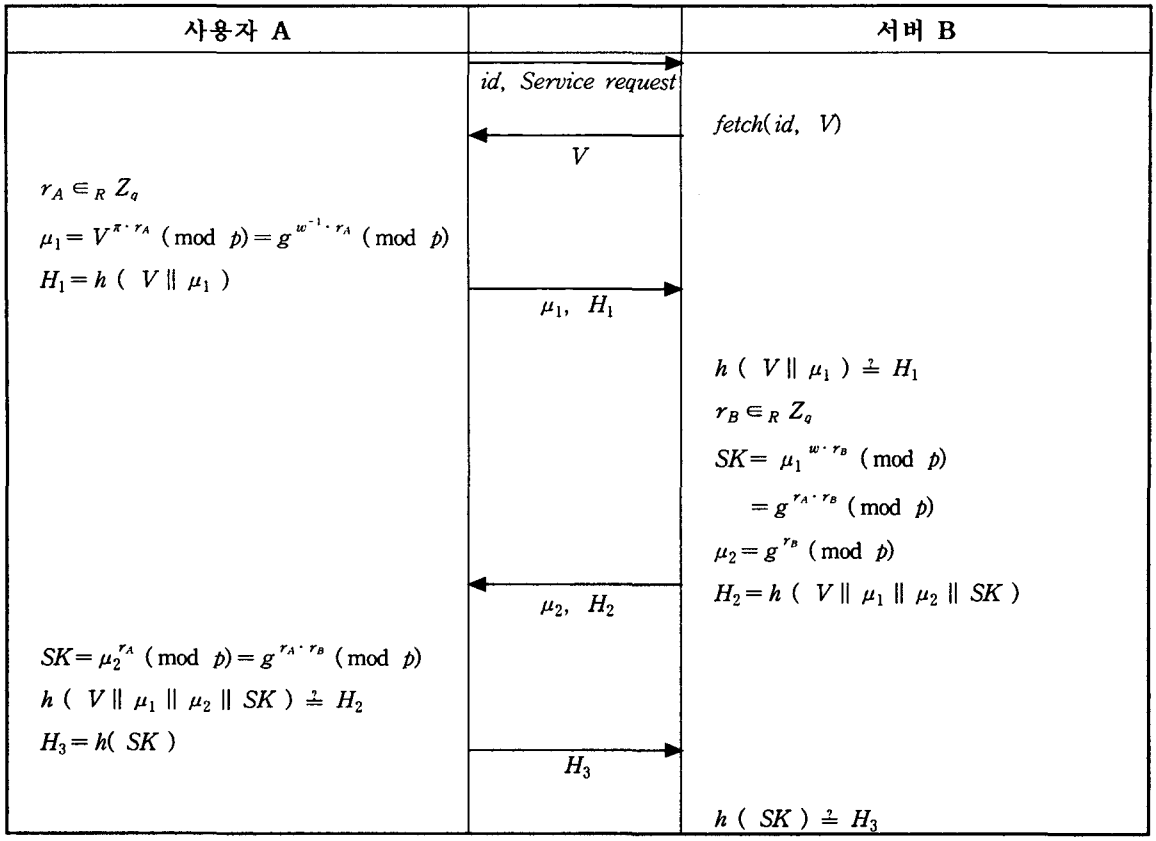

그림 2: 패스워드 기반 키 분배 프로토콜

프로토콜을 수행할 수 있다.

본 논문에서 제안하는 패스워드 검증자 기반 키 분배 프로토콜의 수행동작 과정은 다음과 같다.

① 사용자 A는 자신의 ID와 함께 서버 B에게 서비스 요청 메시지를 보낸다.

$$id,\ Service\ request$$

② 서버 B는 사용자 ID의 정보에 상응하는 검증자 V를 찾아 사용자 A에게 전송해 준다.

$$fetch(id,\ V)$$

③ 사용자 A는 자신이 선택한 랜덤수 r_A와 패스워드 π의 곱을 검증자 V에 지수승하여 중간값 μ_1을 생성한다. 전송정보의 메시지 인증을 위해 검증자 V와 생성된 중간값 μ_1을 연접하고 해쉬하여 H_1를 생성한다. 생성한 중간값 μ_1과 H_1을 서버 B에게 전송한다.

$$r_A \in_R Z_q$$

$$\mu_1 = V^{\pi \cdot r_A} \pmod p = g^{w^{-1} \cdot r_A} \pmod p$$

$$H_1 = h(V \| \mu_1)$$

④ 사용자 B는 전송정보 검증자 V와 수신한 중간값 μ_1을 연접한 값을 해쉬하고, 그 값을 수신한 H_1과 비교하여 메시지의 무결성을 검사한다. 서버 B는 선택한 랜덤수 r_B를 비밀키 w와 곱하여, 수신한 중간값 μ_1에

지수승 해주어 세션키 SK를 계산한다. 랜덤수 r_B를 원시원소 g에 지수승 하여, 중간값 μ_2를 생성한다. 전송정보의 메시지 인증을 위해 이전의 전송정보 μ_1, 검증자 V, 생성된 중간값 μ_2와 세션키 SK를 연접하고 해쉬하여 H_2를 생성한다. μ_2, H_2을 사용자 A에게 전송한다.

$$h(V \| \mu_1) \stackrel{?}{=} H_1$$

$$r_B \in_R Z_q$$

$$SK = \mu_1^{w \cdot r_B} \pmod{p}$$

$$= g^{r_A \cdot r_B} \pmod{p}$$

$$\mu_2 = g^{r_B} \pmod{p}$$

$$H_2 = h(V \| \mu_1 \| \mu_2 \| SK)$$

⑤ 사용자 A는 수신한 중간값 μ_2에 자신이 생성한 랜덤수 r_A를 지수승하여 세션키 SK를 생성한다. 사용자 A는 검증자 V와 전송정보 μ_1, μ_2, 생성한 세션키 SK를 연접한 값을 해쉬하고, 그 값을 수신한 H_2과 비교하여 메시지의 무결성을 검사한다, 생성된 세션키 SK를 해쉬한 값인 H_3를 서버 B에게 전송한다.

$$SK = \mu_2^{r_A} \pmod{p} = g^{r_A \cdot r_B} \pmod{p}$$

$$h(V \| \mu_1 \| \mu_2 \| SK) \stackrel{?}{=} H_2$$

$$H_3 = h(SK)$$

⑥ 서버 B는 사용자 A로부터 수신한 H_3와 자신이 생성한 세션키 SK를 해쉬한 값을 비교하여 키 확인을 한다.

$$h(SK) \stackrel{?}{=} H_3$$

III. 프로토콜의 안전성 분석

본 논문에서 제안한 패스워드 검증자 기반 키 분배 프로토콜의 안전성은 이산대수 문제와 Diffie-Hellman 문제에 기반 하므로 전송정보를 이용하여 세션키를 구하는 어려움은 이산대수 문제와 Diffie-Hellman 문제를 푸는 어려움과 동일하다.

1. Active Impersonation에 대한 안전성

공격자가 사용자 A로 위장하여 서버 B와의 세션키를 설정하는 것은 이산대수와 Diffie-Hellman 문제를 푸는 어려움과 동일하다. 공격자가 패스워드 π나 서버 B의 비밀키 w를 알지 못한다면, 사용자 인증에 사용되는 정당한 μ_1과 세션키 SK를 계산해 낼 수 없으므로 정당한 사용자로의 위장이 불가능하다. 이는 서버 B가 자신이 생성한 세션키 SK와 수신한 세션키의 해쉬값 H_3을 비교하는 과정을 통해 발견될 수 있다.

공격자가 서버 B로 위장하였을 경우 공격자는 비밀키 w을 알지 못하므로 서버 B로 위장할 수 없다. 이는 사용자 A로부터 수신한 중간값 μ_1으로부터 정당한 세션키 SK를 생성해 낼 수 없기 때문에 키 확인 과정에서 쉽게 검출할 수 있다.

2. Forward Secrecy에 대한 안전성

사용자 A의 비밀정보인 패스워드 π가 노출된 경우 공격자는 과거의 세션키 생성에 사용된 랜덤수 r_A, r_B를 알지 못하기 때문에 과거의 세션키 SK를 생성해 낼 수 없다. 또한 서버 B의 비밀정보인 비밀키 w가 노출되었을 경우에도, 사용자 A의 패스워드 π가 노출된 경우와 마찬가지로 과거에 사용된 랜덤수 r_A, r_B를 알지 못하기 때문에 과거의 세션키 SK를 생성해 낼 수 없다.(Half Forward Secrecy).

공격자가 사용자 A와 서버 B의 패스워드와 검증자가 모두 노출되었다 하더라도 과거의 랜덤수 r_A, r_B를 계산해낼 수 없으므로 과거의 세션키 SK를 구할 수 없는 Diffie-Hellman 문제의 어려움과 동일하다.(Full Forward Secrecy)

3. Man-in-the-middle Attack에 대한 안전성

공격자가 사용자 A와 서버 B 사이에 개입하여 서버에겐 정당한 사용자로 사용자에게는 정당한 서버로 위장하는 공격은 패스워드 π를 알지 못하는 공격자는 서버 B의 Challenge에 대한 정당한 Response를 생성해 낼 수 없기 때문에 불가능하다. 즉 전송정보 μ_1을 수정하거나 새로 생성하여 전송해 주는 경우, 이를 수신한 서버 B가 정당한 세션키 SK를 생성해 낼 수 없기 때문에 세션키 SK를 확인하는 과정에서 쉽게 검출해 낼 수 있다.

4. Off-line Dictionary Attack에 대한 안전성

Off-line dictionary attack은 키 교환 과정 동안 수행한 사용자들간에 전송정보를 이용하여 공격자가 패스워드 π나 세션키 SK를 구하는 방법이다. 첫 번째, 제안한 프로토콜에서 공격자가 패스워드 π에 대해 off-line-dictionary attack을 수행하려는 경우, 검증자 V로부터 패스워드 π를 계산하기 위해서는 사용된 랜덤수 r_A의 정보와 서버 B의 비밀키 w를 알아야 가능하며, 이 정보를 계산하는 것은 이산대수문제의 어려움과 동일하다.

VI. 프로토콜의 특징 및 효율성 분석

1. 프로토콜의 특징 분석

제안한 프로토콜은 세션키를 설정하는 과정에서 사용자 A와 서버 B가 각각 생성한 랜덤수 r_A, r_B를 이용하여 계산하므로 키 동의와 Key freshness을 보장한다. 그리고 사용자 A는 서버 B가 자신이 전송해준 중간값 μ_1으로부터 계산한 세션키 SK와 자신이 생성한 세션키 SK의 비교검증을 통해 서버 B임을 인증하고, 서버 B도 사용자 A가 전송해준 세션키의 해쉬 값 H_3와 서버가 생성한 세션키 SK의 해쉬값과의 비교를 통해 사용자 A임을 인증한다. 이 과정을 통해서 사용자 A와 서버 B는 양방향 개체 인증뿐 아니라 양방향 명시적 키 인증과 키 확인을 제공한다.

제안한 프로토콜에 대한 특징 분석을 정리하면 아래 표 1 과 같다.

표 1: 제안한 프로토콜의 특징 분석

특징 \ 항목	제안한 프로토콜
통신횟수	5 pass
개체인증	양방향
키 인증	양방향 명시적
키 확인	양방향
key freshness	양방향

2. 프로토콜의 효율성 분석

본 논문에서 제안하는 키 분배 프로토콜의 계산량적 측면에 대해 분석하였다. 이의 분석을 위해 키 분배 프로토콜의 분배 과정 및 검증과정에서 수행되는 지수 연산과 해쉬함수 연산을 기준으로 기존 프로토콜과 제안한 프로토콜의 계산량을 비교한다.

B-SPEKE는 사용자 3번/서버 4번의 지수연산을 수행하고, PAK-X는 사용자 4번/서버 4번의 지수연산을 수행한다. SRP는 사용자 3번/서버 3번 AMP는 사용자 2번/서버2번의 지수 연산을 수행한다. 제안한 프로토콜은 AMP 프로토콜의 지수연산처럼 사용자 2번/서버2번의 지수 연산을 수행한다.

내용을 정리하면 아래 표 2와 같다.

표 2: 계산량 비교

특징 \ 항목	지수연산		해쉬연산	
	사용자	서버	사용자	서버
B-SPEKE	3	4	-	-
PAK-X	4	4	4	3
SRP	3	3	3	2
AMP	2	2	3	3
제안한 프로토콜	2	2	3	3

V. 결론 및 향후 연구 방향

본 논문에서는 새로운 패스워드 기반 키 분배 프로토콜에 대해 제안하였다. 이 프로토콜은 공개정보로 검증자를 사용하는 새로운 방식으로써, 기존의 프로토콜이 검증자에 대한 서버의 안전성을 요구했다면, 제안한 방식은 서버의 비밀키의 안전한 저장이 요구된다. 기존의 프로토콜 방식과 같이 사용자는 자신이 기억하는 패스워드만을 사용하여 프로토콜의 수행이 가능하도록 하였다. 제안한 프로토콜은 양방향 명시적 키 인증과 양방향 키 확인, 양방향 개체인증, key freshness 등의 요구사항을 만족하며, 기존 프로토콜과 비교해 AMP와 같은 계산량을 요구한다.

본 논문에서 제안하는 키 분배 프로토콜의 안전성은 이산대수 문제와 Diffie-Hellman 문제에 기반하고 있으며, active impersonation attack, forward secrecy, man-in-the-middle attack에 대한 안전성을 분석하였다. 그러나 본 논문에서 기술한 안전성은 경험적 안전성에 기반한 것이므로 향후 formal 모델에서의 안전성 증명이 이루어져야 할 것으로 본다. 또한 무선환경에 적용하기 위해 계산량적 측면을 고려한 연구가 진행되어야 할 것이다.

참고문헌

[1] Bellare, Jablon, Krawczyk, MacKenzie, Rogaway, Swaminathan & Wu, "Proposal for P1363 Study Group on Password-Based Authenticated-Key-Exchange methods", February. 2000

[2] Steven M. Bellovin, M. Merritt "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", *Proceedings of the IEEE Symposium on Research in Security and Privacy*, May. 1992

[3] David P. Jablon, "Strong Password-Only Authenticated Key Exchange", *ACM Computer Communication*, October. 1996

[4] David P. Jablon, "Extended Password Key Exchange Protocols Immune to Dictionary Attack*", *Proceedings of the WETICE*, June. 1997

[5] Victor boyko, Philip MacKenzie, Sarvar Patel, "Provably Secure Password-authenticated key Exchange Using Diffie-Hellman", *Proc. of Eurocrypt '01, LNCS 1807*, pp 156-171, July. 2000

[6] Thomas Wu, "The Secure Remote Password Protocol", *In Network and Distributed System Security Symposium*, 1998

[7] Taekyoung kwon, "Authentication and Key Agreement via Memorable Password", *In Proc. of NDSS 2001 Symposium Conference*, 2001.

[8] M.Lomas, L.Gong, J.Saltzer, and R.Needham, "Reducing risks from poorly chosen keys", *Proceeding of the 12th ACM Symposium on Operating System Principles, ACM Operating Systems Review*, pp. 14-18, 1989

[9] 안상만, 오수현, 원동호, "효율적인 1-pass 패스워드 기반 키 분배 프로토콜에 관한 연구", *한국정보처리학회 추계학술발표대회 논문집 제 9권 2호*, pp. 1119-1122, 2001. 1