제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

효율적인 1-pass 패스워드 기반 키 분배 프로토콜에 관한 연구

안상만*, 오수현*, 원동호*
*성균관대학교 정보통신공학부
e-mail: {smahn, shoh, dhwon}@dosan.skku.ac.kr

A study on the efficient 1-pass password-based key exchange protocol

*Sang-Man Ahn, Soo-Hyun Oh, Dong-Ho Won
*School of Information and Communications Engineering,
Sungkyunkwan University

요 약

본 논문에서는 Ford와 Kaliski[6]가 제안한 패스워드 은닉 기술을 적용하여 클라이언트와 서버의 은닉 변수로 은닉된 값을 서버가 패스워드 검증자로 사용하는 새로운 패스워드 기반 키 교환 프로토콜을 제안한다. 제안하는 프로토콜은 패스워드 검증자를 비밀리에 보관하여야하는 다른 검증자 기반 방식과 달리 클라이언트와 서버의 은닉 변수가 적용된 검증자를 사용하여 서버의 패스워드 검증자에 대한 안전성을 증가시켰다. 또한, Nyberg-Ruppel 방식[4]을 적용하여, 한번의 통신으로 사용자 인증과 키 교환을 할 수 있다. 본 논문에서 제안하는 프로토콜 안전성은 이산대수문제인 DLP(Discrete logarithm Problem)와 DHP(Diffie-Hellman Problem)[6]에 의존한다. 따라서 DLP와 DHP의 가정하에, 제안된 프로토콜은 오프라인 사전공격(off-line dictionary attack), 서버 데이터 도청(server data eavesdropping), 전향적 안전성(forward secrecy), Denning-Sacco 공격[1]에 대하여 안전하다.

1. 서론

사용자 인증에서 많이 사용되고 있는 패스워드 기반 인증 방법은 패스워드가 정보량적인 측면에서 낮은 엔트로피(불확실성)를 가지고 있기 때문에 패스워드에 대한 추측 공격과 서버에 저장되어 있는 패스워드 파일이 공격자에게 노출되었을 경우, 사전공격(Dictionary attack)에 약하다는 단점이 있다.

Lomas[2] 등은 off-line 사전공격을 막을 수 있는 방법을 처음으로 제안하였다. Lomas의 프로토콜은 사용자가 서버의 공개키를 사용하는 방식으로서, 엄밀한 관점에서 패스워드만을 사용하는 프로토콜은 아니다. 또한 서버의 공개키를 사용하여야 함으로, 복잡하고 비효율적인 공개키 기반 구조(PKI-Public Key infrastructure)를 사용해야만 하는 추가적인 요구사항이 있다.

Bellovin와 Merritt[3]는 서버의 공개키를 사용하지 않으며, 관용암호방식과 공개키 암호방식을 혼합하여 방식으로 인증된 패스워드 기반 키 분배를 하는 첫번째 프로토콜인 EKE(Encrypted Key Exchange)를 제안하였다. 따라서 공격자는 패스워드에 대한 추측공격으로 암호를 복호할 수 있지만, 키 교환을 위해 사용된 공개키 암호 방식을 깰 수 없어, 추측한 값을 검증할 수 없다.

EKE가 제안된 이후, EKE보다 안전하고, 새로운 특성을 만족하는 프로토콜들이 많이 제안되었다. 그러나 이전까지 제안된 패스워드 기반 키 분배 프로토콜들은 비록 검증자 기반 방식이라고 하더라도, 패스워드에 대한 검증자를 "secret public key"라고 하여 항상 비밀리에 보관되어야한다. 즉, 서버에 저장된 패스워드 검증자가 노출되면, 공격자는 서버로 위장 가능하며, 또한 노출된 검증자를 이용하여 사용자의 패스워드 추측을 위한 검증값으로 사용할 수 있다. 이를 보완하기 위해 Ford와 Kaliski는 공격자에 의한 추측공격을 방지하기 위하여 복수의 서버를 사용하였다.

본 논문에서는 Ford와 Kaliski가 제안한 방식 중,

은닉서명 방식을 응용한 "password-hardening protocol"을 이용하여 클라이언트와 서버의 은닉 변수(blinding factor)로 은닉된 패스워드 검증자를 생성하고, 이 값을 서버의 검증자로 사용함으로써, 서버 손상(Server compromise) 공격을 감소시키고, 또한 Nyberg-Ruppel 방식[4]을 응용하여, 한번의 통신으로 사용자 인증과 키 교환을 할 수 있는 효율적인 새로운 패스워드 기반 키 분배 프로토콜을 제안한다.

2장에서는 Ford와 Faliski[6]에서 사용된 패스워드 은닉 방식에 대해서 기술하고, 3장에서는 2장에서 기술된 방식을 사용하여 교환된 검증자를 이용하여 클라이언트와 서버간의 인증과 세션키을 교환하는 새로운 프로토콜에 대해서 기술한다. 4장에서는 제안한 protocol의 안전성에 대해서 기술하며, 5장에서 결론을 맺는다.

2. 패스워드 은닉 프로토콜

Ford와 Kaliski[6]는 서버에 저장된 패스워드 검증자에 대한 안전성을 보장하기 위하여 다중서버 모델을 제안하면서 패스워드 은닉 프로토콜에 대해서 기술하였다. 위 과정은 본 논문에서 제안하는 프로토콜의 검증자 교환을 위한 셋업과정으로 사용한다. 프로토콜 설명에 앞서 본 논문에서 기술되는 기호들에 대한 정의는 다음과 같다.

p	: 큰 소수 ($p=2q+1$)
q	: $p-1$의 큰 소수 원소
ID_C	: 클라이언트의 ID(이름이나 주소 스트링)
ID_S	: 서버의 ID(이름이나 주소 스트링)
V	: 서버의 패스워드 파일에 저장되는 패스워드 검증자
π	: 클라이언트의 패스워드
k	: 클라이언트의 비밀 랜덤수
$f(\pi)$	: π를 DH의 기저에 적합하도록 변환하는 함수
x, r	: 클라이언트가 선택한 랜덤수
d_C	: 서버가 생성하는 클라이언트에 대한 비밀 키
K	: 세션키

패스워드 은닉 프로토콜을 수행하는 목적은 클라이언트는 패스워드 π에 대한 서버의 은닉 서명된 값 $R=f(\pi)^{d_C} \bmod p$을 받고, 서버는 패스워드에 대한 검증자 V를 교환하기 위한 것이다. 프로토콜의 수행 과정은 다음과 같다.

1. 클라이언트는 $r \equiv f(\pi)^k \bmod p$를 계산하여 ID_C와 r을 서버에서 전송한다.

   클라이언트 → 서버 : ID_C, r (1)

2. 위 값을 전송 받은 서버는 $V=r^{d_C} \bmod p$를 계산하여 ID_S와 V를 클라이언트에게 전송한다.

   서버 → 클라이언트 : ID_S, V (2)

3. 서버의 검증자로 사용되는 V를 전송 받은 클라이언트는 r값 생성에 사용된 k의 역수를 이용하여 $R=V^{k^{-1}} \bmod p$를 계산한다.

   클라이언트 : R (3)

위 과정의 종료 후, 서버는 클라이언트의 검증자인 V를 계산하여 데이터베이스에 저장하고, 클라이언트는 강화된 패스워드 $R=f(\pi)^{d_C} \bmod p$를 계산한다. 위 과정에서 멱지수 k는 은닉 인수로 사용되어 서버는 r로부터 패스워드에 대한 어떠한 정보도 획득하지 못하고, 또한 강화된 패스워드 R을 계산할 수 없다. 서버는 클라이언트의 검증자로 각 클라이언트마다 서버가 생성한 비밀키 d_C로 서명된 V를 사용하므로 클라이언트라도 자신의 검증자를 계산할 수 없다.

그러나 위 과정은 Ford와 Kaliski가 제안한 방식을 사용하므로 자체에 포함되어 있는 제한사항 또한 존재한다. 일 예로, 클라이언트와 서버가 검증자를 교환하기 위해서는 SSL(Secure Sockets Layer)과 같은 사전 서버 인증기술을 필요로 한다. 자세한 제한사항은 Ford와 Kaliski가 제안한 방식[6]과 동일하므로 본 논문에서는 생략하도록 한다.

3. 제안하는 패스워드 기반 키 분배 방식

본 장에서는 앞에서 기술한 셋업 과정을 통하여 은닉된 검증자를 교환하고, 패스워드 검증자와 클라이언트와 서버의 비밀값을 이용하여 사용자 인증과 키 교환을 하는 새로운 프로토콜로써, 검증자를 교환하기 위한 셋업 과정은 초기 프로토콜 설정시에만 사용하므로, 실제 사용자 인증과 세션키 교환 과정은 Nyberg-Rueppel의 일방향 키 교환 방식을 사용한 검증자 기반 메커니즘을 이용하여 한번의 통신으로 클라이언트와 서버간에 수행할 수 있다.

클라이언트에 대한 인증과 세션키를 교환하기 위해서 클라이언트는 서버와 다음과 같은 과정을 수행한다.

1. 클라이언트는 $s \equiv k^{-1}r + e \bmod q$와 $e \equiv f(\pi)^{x-r} \bmod p$를 계산하여 서버에 전송한다. 단, $x, r \in Z_q$은 클라이언트가 생성한 랜덤수이다.

$$\text{클라이언트} \rightarrow \text{서버} : ID_C, (e, s) \quad (4)$$

위 과정을 수행한 후, 클라이언트는 세션키 K를 아래와 같은 계산을 수행한다.

$$K = R^x \bmod p$$
$$K = f(\pi)^{x \cdot d_C} \bmod p \quad (5)$$

2. 위 값들은 전송 받은 서버는 , $e \not\equiv 0 \bmod p$ $s \not\equiv 0 \bmod q$를 검증한 후, 아래와 같이 세션키를 계산한다.

$$K = V^s \cdot V^{-e} \cdot e^{d_C} \bmod p$$
$$K = f(\pi)^{x \cdot d_C} \bmod p \quad (6)$$

만약, 위의 모든 과정이 정확히 수행된다면, 클라이언트와 서버는 세션키 $K \equiv f(\pi)^{xd_C} \bmod p$를 얻게 된다.

위 프로토콜은 특성상 키 확인 기능을 제공하지 않지만 세션키 생성 후, 추가정보 전송을 통해 쉽게 제공할 수 있다.

3. 세션키를 계산한 서버는 세션키와 클라이언트의 전송정보를 해쉬한 값과 재전송 공격(reply attack)을 방지하기 위한 nonce의 비트연산을 하여 클라이언트에게 전송한다.

$$\text{서버} \rightarrow \text{클라이언트} : nonce \oplus h(K, e, s) \quad (7)$$

4. 위 값을 전송 받은 클라이언트는 자신이 생성한 세션키와 전송정보를 이용하여 해쉬값을 생성하고 해쉬값을 검증하고, 비트연산을 통하여 $nonce$를 추출한다. 추출한 $nonce$와 클라이언트가 생성한 K의 해쉬값을 서버에게 전송한다.

$$\text{클라이언트} \rightarrow \text{서버} : h(nonce, K) \quad (8)$$

4. 안전성 분석

본 논문에서 제안한 프로토콜에 대한 안전성은 경험적 안전성에 기인하고 있으며, 이상대수문제인 DLP(Discrete logarithm Problem)와 DHP(Diffie-Hellman Problem)에 의존하고 있다. 각각의 특성에 대한 자세한 증명은 아래와 같다.

4.1 오프라인 사전공격에 대한 안전성

키 교환 과정 동안, 수동적 공격자에게 주어지는 정보는 아래와 같다.

$$\{ p,\ q,\ f(\pi)^{x-r} \bmod p,\ k^{-1}r + e \bmod q. \}$$

만약, 공격자가 패스워드 π'를 추측한다면, $e' \equiv f(\pi')^{x-r} \bmod p$, $s \equiv k^{-1}r + e' \bmod q$를 찾을 수 있다. 또한, 세션키 $K = f(\pi')^{xd_C} \bmod p$를 추측할 수 있다. 그러나 이것은 이산대수문제(DLP)와 DHP을 풀어야만 하므로, 수동적 공격자가 추측한 패스워드를 검증할 수 있는 아무런 정보도 제공하지 않는다.

4.2 서버 데이터 도청(Server data eavesdropping) 공격에 대한 안전성

공격자에게 서버에 저장되어 있는 패스워드 검증자가 노출된 경우라도, 공격자는 사용자로 위장할 수 없다. 공격자가 세션키를 계산하기 위해서는 세션키 계산을 위한 기저 $f(\pi)$를 사용하여야 하지만, 노출된 검증자로부터 기저 $f(\pi)$를 유추해 낼 수 없다. 또한, 노출된 검증자를 추측한 패스워드의 검증값으로 이용하는 패스워드 추측 공격은, 검증자 V가 클라이언트와 서버의 비밀 랜덤값으로 은닉되어 있으므로 노출된 검증자를 추측한 패스워드를 검증하기 위한 값으로 사용할 수 없어 추측 공격 또한 불가능하다.

4.3 전향전 안전성(Forward Secrecy)

공격자에게 클라이언트의 패스워드 π가 노출되더라도, 이전 세션에서 사용되었던 세션키를 계산할 수 없다. 즉, 공격자가 도청을 통하여, 현재 세션의 전송 정보 (e, s)를 획득하고, 클라이언트의 패스워드를 알고 있더라도, 이전 세션키의 생성에 사용된 x와 d_C가 패스워드와는 독립적인 정수 값이고, 또한 x와 d_C를 구하는 것은 이산대수 문제와 동일하여 x와 d_C를 구할 수 없으므로, 이전의 세션키를 구할 수 없다.

4.4 Denning-Sacco에 대한 안전성

세션키 K는 클라이언트가 생성하는 값 x에 의해 매 세션마다 변경되므로, 이전에 노출된 세션키는 현재의 세션키로 사용할 수 없으며, 또한 추측한 패스워드에 검증값으로의 사용은 DHP로 귀착되므로 추측한 패스워드의 검증값으로도 사용할 수 없다.

5. 효율성 비교

본 논문에서 제안하는 패스워드 기반 키 분배 방식은 통신량적 측면에서 커다란 이득이 있다. 즉, 세션키 교환 시 클라이언트가 생성한 정보를 한번만 서버에게 전송함으로써, 세션키를 계산할 수 있는 효율적인 방식이다. 지금까지 제안된 검증자 기반 방식 중, IEEE P1363.2 / D2002-02-12[8]에서 표준화 작업중인 AMP, B-SPEKE, PAK-X, SRP-3 등과 멱승수와 세션키 교환만을 위한 통신회수에 대한 비교는 다음 [표 1]와 같다. IEEE P1363.2에서 제시된 각각의 프로토콜에 대한 자세한 설명은 지면관계상 생략한다.

[표 1] 효율성 비교

프로토콜	멱승수		통신회수
	클라이언트	서버	
AMP	2	2	2
B-SPEKE	3	3	2
PAK-X	2	2	2
SRP-3	2	2	2
제안하는 프로토콜	2	2	1

5. 결론

본 논문에서는 Ford와 Kaliski가 제안한 패스워드 강화 방식을 사용하여 패스워드 검증자에 대한 안전성을 증가시켰고, 검증자가 노출되어도 각 클라이언트에 대한 비밀키를 알고 있는 서버만이 세션키를 계산할 수 있는 효율적인 1-pass 패스워드 기반 키 교환 프로토콜을 제안하였다. 또한, IEEE P1363.2 / D2002-02-12에서 표준화되고 있는 검증자 기반 프로토콜을 대상으로 효율성 비교를 하였다. 대부분의 프로토콜들이 세션키 교환을 위해 2회의 통신회수를 필요로 하는 반면, 본 논문의 프로토콜은 1번의 통신으로 세션키를 교환할 수 있는 이점이 있다.

본 논문에서 제안하는 프로토콜의 안전성은 DLP와 DHP에 의존하고 있다. 따라서, 위 가정하에, 패스워드 추측 공격, Server data eavesdropping, 전향적 안전성(Forward Secrecy), Denning-Sacco attack에 대해 안전함을 증명하였다. 그러나 본 논문에서 기술한 안전성은 경험적 안전성에 기초하여 안전성이 증명되어, 향후 formal 모델에서의 안전성 증명이 이루어져야 할 것이다.

참 고 문 헌

[1] D. Denning and G. Sacco, Timestamps in key distribution. *Communications of the ACM*, August 1981.

[2] T. M. Lomos, L. Gong, J. H. Saltzer, and R. M. Needham, Reducting risks from poorly chosen keys, *ACM Operating systems Review, Proceeding of the 12th ACM Symposium on Operating systems Principles*, 23(5): Dec. 1989, pp 14-18.

[3] S.M. Bellovin, M. Merritt, Eencrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks, *Proceedings of the IEEE Symposium on Research in security and Privacy*, 1992.

[4] K. Nyberg and R. Ruppel, A new signature scheme based on DSA giving message recovery, *Proc, 1st ACM Conf, on Comput. Commun. Security*, 1986, pp. 58-61.

[5] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans. Inf. Theory*, vol.IT-22, no.6, , 1976, pp. 644-654.

[6] W. Ford & B. Kaliski, Server-Assisted Generation of a Strong Secret from a Password, *Proceedings of the IEEE 9th International Workshops on Enabling Technologies: NIST*, Gaithersburg MD, June 14-16, 2000.

[7] P. MacKenzie, On the Security of the SPEKE Password-Authenticated Key Exchange Protocol, *Cryptology Print Archive: Report* , 2001.

[8] IEEE P1363.2 / D2002-02-12 (*Standard Specifications for Public Key Cryptography: Password-based Techniques*)