속성 기반 암호화 방식을 이용한 다중 서버 패스워드 인증 키 교환

박민경, 조은상, 권태경
서울대학교

mkpark@mmlab.snu.ac.kr, escho@mmlab.snu.ac.kr, tkkwon@snu.ac.kr

Multi Server Password Authenticated Key Exchange Using Attribute-based Encryption

Minkyung Park, Eunsang Cho, Ted "Taekyoung" Kwon
Seoul National University

요 약

패스워드 인증 키 교환 프로토콜(Password Authenticated Key Exchange: PAKE)은 서버와 클라이언트가 서로를 인증하고 키를 교환하는 알고리즘이다. 패스워드를 여러 개의 서버에 나누어 저장해서, 모든 서버가 손상되지 않으면 패스워드나 키가 유출되지 않는 알고리즘은 다중 서버 PAKE (Multi Server-PAKE: M-PAKE)이다. 속성 기반 암호화 방식에서는 암호화 하는 주체가 원하는 속성을 모두 만족하여야 복호화가 가능한 특징이 있다. 본 논문에서는 속성 기반 암호화 방식의 속성 값을 패스워드로 보아, 공개키/비밀키를 별도로 생성하지 않고 공개키 기반 암호화가 가능한 M-PAKE 프로토콜을 제안한다. 제안한 프로토콜은 서버 당 한번의 메시지 교환만이 필요하며 사전(dictionary) 공격에 안전하다. 또한 사전 공격에 대한 위협 모델을 제시하고 보안 분석을 통하여 안전성을 검증하였으며, 사용한 암호 알고리즘의 수행시간 측정을 통해 제안한 프로토콜의 실현가능성(feasibility)을 검토하였다.

Ⅰ. 서 론

패스워드 기반 인증 키 교환 프로토콜(Password Authenticated Key Exchange: PAKE)은 패스워드를 이용하여 서버와 클라이언트가 서로를 인증하고 키를 교환하는 알고리즘이다. 패스워드 방식은 사전(dictionary) 공격에 취약하기 때문에 PAKE 프로토콜은 이에 안전해야 한다. 인증서나 다른 방식을 이용한 방식과 비교 하였을 때, 패스워드 기반 인증 방식은 사용자가 쉽게 읽고 사용할 수 있는 특성으로 인해 여전히 많이 이용되고 있다. 그러나 서버가 손상되면, 패스워드가 모두 노출이 될 수 있다는 단점도 가지고 있다. 이를 극복한 것이 다중 서버 PAKE(Multi Server-PAKE: M-PAKE)이다. M-PAKE 는 클라이언트의 패스워드를 여러 개의 서버에 저장하여, N 개의 서버 중 N-1 개의 서버가 손상되어도 이를 탐지하는 것이 가능하여야 한다.

Bellovin 과 Merritt[1]이 처음으로 사전 공격에 안전한 PAKE 알고리즘을 발표하였다. 그 이후 단일 서버에서는 PKI 기반 PAKE [2], ID 기반 PAKE[3]이 발표되었고, 멀티 서버에서는 threshold 를 이용한 PAKE[4]과 2 개의 서버를 이용한 PAKE[5] 등이 꾸준히 발표되고 있다. 그러나 위의 프로토콜들은 메시지 교환이 많이 발생하고, 특정 서버의 개수에만 적용할 수 있다는 한계가 있다. 본 논문에서는 속성 기반 암호화 기법을 사용하여 이러한 한계점을 극복하려고 한다.

속성 기반 암호화 기법(Attribute-based encryption: ABE)[6]은 ID-based encryption 에서 파생되었다. Bilinear pairing 에서 $e(g^a,g^b) = e(g,g)^{ab}$ 라는 pairing 특징을 이용하면, 암호화를 하는 주체가 원하는 속성값을 모두 만족해야 복호화(Attribute-based decryption: ABD)가 가능한 기법이다. public parameter 리스트(속성 리스트) $\{g^{t1}, \cdots, g^{tn}\}$에 대해 각 속성 g^{tk} 에 대응하는 값을 yk 라 하면, 해당 속성 가진 주체는 비밀키 $g^{yk/tk}$ 를 갖게 된다. 따라서 암호화를 할 때 속성과 속성 값으로 암호화를 하면, 복호화를 할 때에도 해당 속성에 대한 값이 일치해야 복호화가 가능해 진다. 다중 속성을 만족해야 하는 ABE 의 특성을 이용해 서버의 개수에 상관 없이 메시지 교환에 효율적이고, 사전 공격에 안전한 M-PAKE 프로토콜을 제안한다.

Ⅱ. 제안하는 M-PAKE 프로토콜

이번 장에서는 제안하는 M-PAKE 프로토콜에 대해 설명한다. 클라이언트 C 의 패스워드를 pw_C 이고, 서버 K 에 저장된 클라이언트의 패스워드를 pw_K 라 하자. 이는 $pw_C=pw_1+\cdots+pw_N$ 의 조건을 만족하도록 N 개의 서버에 각각 패스워드를 저장한다.

속성 기반 암호화 기법에서, 클라이언트 C 와 N 개의 서버를 N+1 개의 속성 리스트라고 볼 수 있다. 따라서, 서버 k 라는 속성(속성 g^{tk})에는 pw_k 이라는 속성 값을 갖고, 이로부터 도출되는 비밀키는 분배된 클라이언트의 패스워드를 이용한 $g^{pwk/tk}$ 이다. 이는 패스워드가 저장된 서버 k 만이 알고 있다. 클라이언트도 마찬가지로 g^{tc} 의 속성에는, 서버에 나뉘어진 N 개의 패스워드를 모두 만족하는, 속성 값 pw_C 와 비밀키 $g^{pwc/tc}$ 를 가지고 있다. 따라서 공개키/비밀키를 패스워드로부터 도출해 낼 수 있다.

Figure1 에 프로토콜 흐름을 명시했다. 초기에 클라이언트는 서버에게 패스워드를 안전하게 배포하고, public parameter 는 안전하게 전달했다고 가정한다.

클라이언트는 ABE 과정에서 $s*pw_k$ 을 일회용 비밀번호(One time password: OTP)로 사용하여 서버에게 보낸다. 이 때 서버가 메시지를 ABD 하게 되면, 서버는 클라이언트를 인증할 수 있게 된다. 또한

클라이언트는 각 서버에게 받은 $x*pw_k$ 를 가지고 $x*pw_C$ 를 정확하게 도출해 내면 서버를 인증할 수 있다. 양방향 인증이 성공하면 클라이언트와 서버 k 간에는 $X^{r'_k} = W'_k{}^{r_k} = g^{r_k r_k'}$라는 세션키를 갖게 된다.

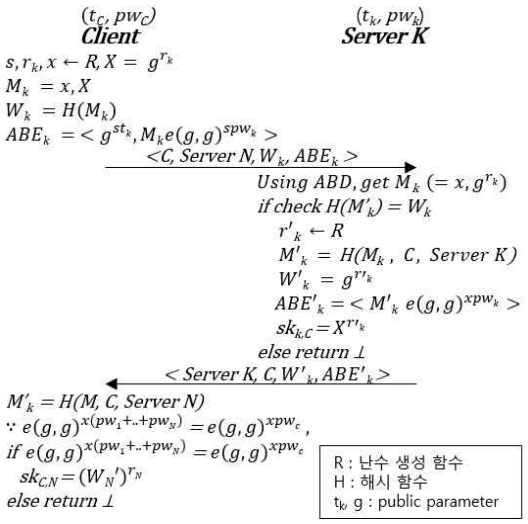

Figure 1. 제안하는 M- PAKE 프로토콜

Ⅲ. 위협 모델과 보안 분석

사전 공격은 온라인 사전공격과 오프라인 사전공격이 있다. 온라인 사전 공격은 brute-force 공격의 일종으로 탐지가 쉽다. 반면 오프라인 사전 공격은 공격자가 클라이언트와 서버 간에 메시지 흐름을 관찰하며, 최종적으로는 클라이언트의 키를 탈취하는 공격이다. 서버 N 개 중에 N-1 개의 서버만 손상되었다고 가정한다.

서버가 클라이언트를 인증하는 과정에서 클라이언트가 자신의 패스워드 일부인 pw_k 를 이용해 메시지를 암호화하고, 해쉬 함수의 사용으로 서버 k 의 패스워드를 알지 못하면 M_k 를 얻지 못하게 된다. 공격자는 N-1 개의 서버의 패스워드를 알더라도, $e(g,g)^{ab}$ 와 b 를 알 때 a 의 값을 구하는 것이 어려운 것처럼 pwc 의 값을 구하는 것은 어려운 문제이다. 키 교환 방법은 Diffie-Hellman 방식을 사용하지만 암호화 되어있어서 중간자 공격에 안전하며 교환되는 키 값을 알 수 없다. $s*pw_k$ 를 OTP 로 사용해서, s 를 알 지 못하면 pw_k가 노출이 되지 않고, ABD 에서도 이 s 를 노출시키지 않고 복호화를 하기 때문에, s 자체를 알 수 없다. 따라서 N-1 개의 서버가 손상되어도 오프라인 사전 공격에 안전하다.

Ⅳ. 실험

제안한 프로토콜에서 사용되는 ABE 는 bilinear pairing 연산을 사용하기 때문에 다른 공개키 기반 암호화 방식인 RSA 나 ElGamal 에 비해 속도가 느리다. ABE 와 RSA 의 속도를 비교하여 Table 1 에 나타내었다. Intel i7-4770 CPU, 8G RAM 에서 측정하였고, JPBC library(http://gas.dia.unisa.it/projects/jpbc)를 이용하여 구현하였다. ABE 는 224bit curve 를 RSA 는 2048bit 의 키를 이용하였고, 메시지 길이는 동일하게 16byte 로 하였다. Table 1 에서 볼 수 있듯이 ABE 와 RSA 의 속도 차이는 상당하다. 하지만, pairing 연산이나 ABE 의 성능을 향상시키려는 연구가 지속적으로 있고 이에 따라 제안한 알고리즘의 성능 향상을 기대할 수 있다. 또한 제안한 알고리즘에서는 메시지 교환이 한 번만 이루어지기 때문에, 기존 다른 PAKE 알고리즘 보다 네트워크 시간을 단축시켜 속도 성능의 향상을 기대할 수 있다.

Table 1 ABE, RSA 1000 회 수행 결과 평균 (괄호는 표준편차)

	암호화	복호화
ABE	106,297us (3521 us)	68,320 us (2,249 us)
RSA	227 us (86 us)	5,483 us (885 us)

Ⅴ. 결론

기존 PAKE 프로토콜은 다수의 메시지 교환이 필요했고, 공개키 기반 암호화 방식을 위해 별도의 공개키를 생성해야 했다. 이에 따라 trust anchor 나 revocation 등의 부가적인 이슈가 있을 수 있다. 하지만 제안한 M-PAKE 프로토콜에서는 속성 기반 암호화 방식을 이용해 클라이언트의 패스워드를 비밀키로 사용할 수 있게 되었다. 또한 서버의 개수에 상관 없이 적용이 가능하여, N-1 개의 서버가 손상되어도 사전 공격에 안전하다. 또한 서버의 개수 당 한번의 왕복으로 인증과 키 교환이 가능해 진다.

그러나 제안한 프로토콜에서 패스워드와 public parameter 가 안전하게 분배/전송된다고 가정하였다. 하지만 이 과정에서 key escrow 문제가 있을 수 있다. 이에 대해 차후에 안전하게 패스워드와 public parameter 를 분배/전송하는 문제를 연구할 예정이다.

ACKNOWLEDGMENT

이 논문은 2014 년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구 결과물임을 밝힙니다. (No.2013R1A2A2A01016562)

참 고 문 헌

[1] Bellovin, S.M., Merritt, M. "Encrypted key exchange: Password-based protocol secure against dictionary attack." In: Proc. IEEE Symposium on Research in Security and Privacy, pp. 72-84 (1992)

[2] Halevi, S., Krawczyk, H. "Public-key cryptography and password protocols." ACM Transactions on Information and System Security 2(3), 230-268 (1999)

[3] Yi, X., Tso, R., Okamoto, E. "Identity-based password-authenticated key exchange for client/server model." In: SECRYPT 2012, pp. 45-54 (2012)

[4] Ford, W., Kaliski, B.S. "Server-assisted generation of a strong secret from a password." In: Proc. 5th IEEE Intl. Workshop on Enterprise Security (2000)

[5] Yi, X., et al. "ID-Based Two-Server Password-Authenticated Key Exchange." Computer Security-ESORICS 2014, Springer: 257-276 . (2014).

[6] Goyal, V., et al. "Attribute-based encryption for fine-grained access control of encrypted data." In: Proc. of the 13th ACM conference on Computer and communications security, ACM. (2006)