오프라인 패스워드 추측 공격에 강한 키 교환 프로토콜

김우헌[0*] 김현성** 이성운* 유기영*
*경북대학교 컴퓨터공학과 정보보호연구실
**경일대학교 컴퓨터공학과
{whkim[0], hskim, staroun, yook}@purple.knu.ac.kr

Authenticated Key Exchange Protocol against Off-line Password Guessing Attack

Woo-Hun Kim[0*] Hyun-Sung Kim** Sung-Woon Lee* Kee-Young Yoo*
*Information Security Lab. Dept. of Computer Engineering, Kyungpook National University
**Dept. of Computer Engineering, Kyungil University

요 약

Lin 등이 제안한 키 교환 프로토콜 및 SAKA 변형 키 교환 프로토콜은 오프라인 패스워드 추측 공격에 대응하지 못했다. 본 논문에서는 기존의 SAKA 변형 키 교환 프로토콜의 취약점을 해결하기 위한 새로운 키 교환 프로토콜을 제안한다. 제안한 프로토콜은 키 검증단계에서 일방향 해쉬 함수를 이용함으로서 기존 프로토콜의 문제점들을 해결하였다. 본 논문에서 제안한 프로토콜은 키 교환 프로토콜에서 요구되는 재전송 공격과 오프라인 패스워드 추측 공격에 강한 특징을 갖고 완전한 전방향 보안(perfect forward secrecy)을 제공한다.

1. 서론

Diffie-Hellman은 안전하지 않는 통신망상에서 사용될 수 있는 세션키 교환방식을 제안하였다[1]. 그러나 Diffie-Hellman 키 교환 프로토콜에서는 송·수신자 상호간의 인증 수단을 유효하게 제공하지 못했기 때문에 중간자 공격(Man in the middle attack)에 취약하였다. Seo, Sweeney는 Diffie-Hellman 키 교환 프로토콜에 인증수단을 제공하기 위해서 SAKA (Simple authenticated key agreement protocol)를 제안했다[2]. SAKA는 인증수단으로 패스워드를 기반으로 하는데, 프로토콜 수행전에 패스워드 교환을 필요로 한다. 이 프로토콜은 Diffie-Hellman 프로토콜과 비슷한 수행 시간을 필요로 하고, 인증을 위해 한번의 추가적인 메시지 교환만을 필요로 하는 장점이 있다. 그러나 Tseng은 SAKA의 키인증 단계에서 발생할 수 있는 취약점을 제시하고 이 취약점에 대처할 수 있는 개선된 프로토콜을 제안하였다[3]. 그 후 Ku와 Wang은 Tseng의 개선책 또한 재전송 공격에 취약하다는 것을 보이고 그 해결책을 제안하였다[4]. 한편 Lin 등은 SAKA의 세 가지의 취약점을 언급하고 그들 또한 SAKA를 개선한 새로운 프로토콜을 제시하였는데, Hsieh 등은 Lin등의 개선된 프로토콜이 오프라인 패스워드 추측 공격에 취약하다는 것을 제시하고 안전성에 의문을 제기하였다[5][6].

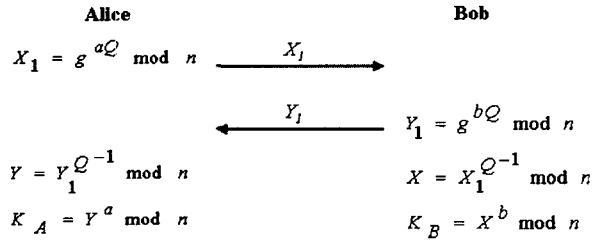
본 논문은 기존의 SAKA 변형 프로토콜의 취약성들을 해결할 수 있는 프로토콜을 제안한다. 인증을 위해서 제안된 프로토콜은 일방향 해쉬 함수(One-way hash function)를 이용한다. 이 해쉬 함수는 충돌이 배제된 해쉬 함수(Collision-free hash function)와 충돌이 포함된 해쉬 함수(Collisionful hash function)의 두 가지 형태로 이용된다. 해쉬 함수에 충돌성을 제공하기 위해서 충돌이 배제된 해쉬 함수를 먼저 적용하고 그 결과에 모듈러 연산을 적용하여 충돌성을 제공한다. 본 논문에서는 이 두 가지 종류의 해쉬 함수를 혼용하여 새로운 인증수단을 제공한다. 제안한 프로토콜은 중간자 공격과 오프라인 패스워드 추측 공격에 강하고 완전한 전방향 보안을 제공하는 보안에 강한 특징이 있다.

본 논문의 구성은 2장에서 SAKA 프로토콜을 기술하고, SAKA의 개선점과 문제점을 설명하며, 3장에서 새로운 프로토콜을 제안하고 암호학적 강도를 분석한다. 마지막으로 4장에서는 결론을 내린다.

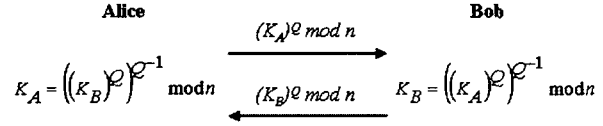
2. 관련연구

2.1 SAKA(Simple Authenticated Key Agreement)

Seo, Sweeney는 Diffie-Hellman 키 교환 프로토콜에 인증 수단을 제공하기 위해서 SAKA (Simple authenticated key agreement protocol)를 제안했다[2]. 프로토콜을 위한 가정은 다음과 같다. 사용자 A와 B는 프로토콜을 시작하기 전에 패스워드 P를 알고 있어야 한다. 또한, Diffie-Hellman 키 교환 프로토콜에서와 같이 원시근(Primitive root) g와 큰 소수 n을 사용한다. 키 교환 단계는 다음 그림 1 (가)와 같다.



(가) 키 교환



(나) 키 인증

그림 1. SAKA 프로토콜

그림 1에서 사용된 변수 a는 참여자 A의 랜덤 값, b는 참여자 B의 랜덤 값, K_A는 A의 세션 키, K_B는 B의 세션 키, P는 세션이 시작하기 전에 교환한 패스워드이고, Q는 사전에 정의된 방법으로 P로부터 유추된 값이다.

SAKA 프로토콜에서 $K_A = K_B = g^{ab} \bmod n$ 이므로, A와 B사이에 공동의 세션 키가 성립된다. 교환된 세션 키의 유효성을 확인하기 위해 A와 B는 그림 1 (나)의 단계를 수행한다.

2.2 SAKA의 개선 프로토콜

Lin, Chang, Hwang 은 SAKA가 중간자 공격과 패스워드 추측 공격(password guessing attack)에 취약함을 보이고, 완전한 전방향 보안을 제공하지 못함을 제기했다. 그림 2는 Lin등이 개선한 SAKA의 키 인증 과정이다[5].

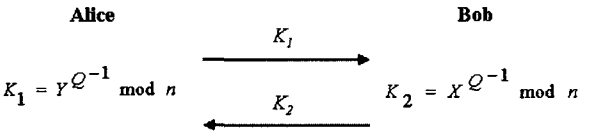


그림 2. Lin등의 개선된 키 인증 프로토콜

이 인증 프로토콜에서 A는 $K_2 = (g^a)^{Q^{-1}} \bmod n$을 통하여 키 검증을 하며, B는 $K_1 = (g^b)^{Q^{-1}} \bmod n$으로 검증한다.

Hsieh 등은 Lin 등의 프로토콜에서 전송되는 키 교환 단계의 X_1 과 키 인증 단계의 K_2 를 저장해두고, 다음과 같이 오프라인 패스워드 추측공격이 가능하다는 것을 보였다[6].

(1) 공격자가 패스워드 P를 추측하여 이와 연관된 Q와 $Q^{-1} \bmod n$ 을 구한다.

(2) 공격자는 자신이 추측한 패스워드 P 를 $X_1^{Q-1} = K_2^{Q}$ 연산을 통하여 검증한다.

오프라인 패스워드 추측공격은 전송된 메시지에 $X_1^{Q^{-1}} = K_2^{Q} = g^a \bmod n$의 성질을 이용하여 가능하다. 전술한 바와 같이 SAKA와 SAKA 변형 프로토콜은 여전히 프로토콜에 취약점이 존재한다. 특히 모든 프로토콜에서 오프라인 패스워드 추측공격이 가능함을 알 수 있다.

3. 오프라인 공격에 강한 키 교환 프로토콜

본 장에서는 기존의 SAKA와 SAKA 변형 프로토콜의 문제점을 해결할 수 있는 새로운 프로토콜을 제안한다. 특히, 제안된 프로토콜은 오프라인 패스워드 추측공격에 강하다.

3.1 키 교환 프로토콜

프로토콜을 제안하기 위해서 먼저 키를 이용한 일방향 해쉬 함수(Keyed one-way hash function)를 정의한다[7]. 본 논문에서 사용되는 해쉬 함수는 크게 다음의 두 가지 형태로 사용된다.

(1) 충돌이 배제된 해쉬 함수 :

$$f(m,t,k) = h(m|t,k)$$

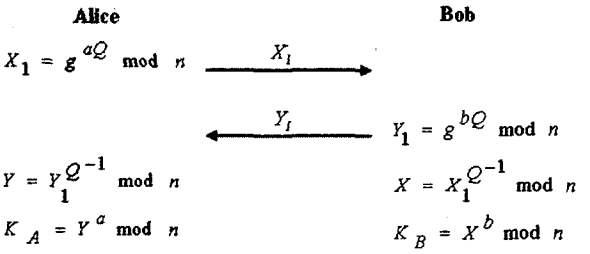
(2) 충돌이 포함된 해쉬 함수 :

$$c(m,t,k) = f((f(m,t,k) \bmod 2^n), t, k)$$

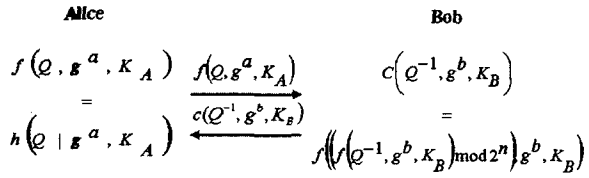
여기서 $f()$ 함수의 첫 번째 인자 m은 해쉬 될 메시지이며 패딩 값인 두 번째 인자 t와 접합연산(|)을 취한 후 해쉬 한다. 세 번째 인자 k는 해쉬 함수의 패스워드가 된다. 즉 패스워드를 아는 사용자만이 메시지를 해쉬 할 수 있다. 충돌이 포함된 해쉬 함수 $c()$는 해쉬가 적용된 결과 값의 범위보다 작은 범위의 n을 선택해서 모듈러 연산을 취한 후 다시 해쉬를 적용한다.

여기서 정의된 일방향 해쉬 함수는 생성된 세션키의 검증 단계에서 사용된다. 본 논문에서 제안한 새로운 키 교환 프로토콜은 그림 3과 같다.

제안한 인증 프로토콜에서는 비대칭(Asymmetric) 메시지를 이용하여 키 인증을 제공한다. 먼저 첫 단계에서 A가 충돌이 배제된 해쉬 함수를 이용하여 통신 쌍방만이 아는 정보 Q와 g^a를 이용하여 해쉬하여 B에게 전송한다. B는 받은 정보가 올바른 정보인지 확인하고, 충돌이 포함된 해쉬 함수를 이용하여 비밀정보 Q^{-1}와 g^b를 해쉬하여 A에게 전송한다. A는 받은 정보를 확인하여 키 인증을 수행한다.



(가) 키 교환



(나) 키 인증

그림 3. 제안한 키 교환 프로토콜

키 인증 단계에서 사용된 모든 정보는 세션 키 설립단계에서 주고받은 정보를 이용해서 추측하는 것이 불가능하다. 다음절에서는 제안한 프로토콜의 좀더 상세한 분석을 제시한다.

3.2 암호학적 프로토콜 분석

본 절에서는 제안한 프로토콜의 암호학적 분석을 위하여 세 가지 공격, 중간자 공격과 완전한 전방향 보안 및 오프라인 패스워드 추측공격, 측면에서 기술하고자 한다.

먼저, 제 3자가 중간자 공격을 하기 위해서는 패스워드로부터 유도한 Q와 Q^{-1} 값을 알아야 한다. 그러나 제 3자는 전송된 메시지로부터 패스워드를 알아낼 수 있는 방법이 없고, 임의의 Q'을 이용하여 중간자 공격을 수행한다면 키 인증 과정에서 공격의 여부를 확인할 수 있다.

완전한 전방향 보안은 현재의 세션키를 제 3자가 알게 되더라도 그 이전의 세션키를 추측할 수 없을 때 제공된다. 제안한 프로토콜에서 전방향 보안에 대한 공격을 위해서는 네트워크 상에서 획득 가능한 전송된 메시지로부터 Q와 Q^{-1}를 유추할 수 있어야 한다. 그러나 제안한 프로토콜에서는 전송된 메시지를 통하여 Q와 Q^{-1}추측은 이산대수의 어려움에 기반 한 문제이다.

오프라인 패스워드 추측공격은 한 세션의 세션 키를 알 때 그 세션 키 정보를 이용하여 통신 쌍방이 공유하고 있는 패스워드를 추측하는 공격이다. 논문 [8]에서 Bakhtiari는 Anderson 프로토콜 [7]의 키 인증 단계에서 사용된 정보를 통하여 패스워드 공격이 가능함을 보였다. 그러나 본 논문에서 제안한 프로토콜은 키 인증 단계에서 패스워드로부터 유도한 정보와 현재 세션의 키 생성을 위한 난수 값의 조합을 이용한다. 공격이 가능하기 위해서 제 3자는 키 교환 단계에서 주고받은 정보인 g^{aQ}나 g^{bQ}로부터 값 g^a과 g^b을 계산 할 수 있어야 한다. 그러나 이 문제는 이산대수 문제이므로 불가능하다.

4. 결론

본 논문에서는 패스워드 기반의 키 교환 프로토콜을 제안하였다. 제안된 프로토콜의 분석을 통하여 기존의 SAKA 및 SAKA관련 프로토콜의 취약성인 재전송 공격과 오프라인 패스워드 추측 공격에 강한 특징을 갖고 완전한 전방향 보안을 제공함을 보였다. 제안된 프로토콜은 공개키 기반구조로 사용될 수 있을 것이다.

참 고 문 헌

[1] W. Diffie, and M. E. Hellman, "New direction in cryptography", *IEEE Trans, IT*-22, pp. 644-654, 1976.

[2] D. H. Seo, and P. Sweeney, "Simple authenticated key agreement algorithm", *Electronic Letters*, 35(13), pp. 1073-1074, June. 1999.

[3] Y. M. Tseng, "Weakness in simple authenticated key agreement protocol", *Electronic Letters*, 36(1), pp. 48-49, January. 2000.

[4] W. C. Ku, and S. D. Wang, "Cryptanalysis of modified authenticated key agreement protocol", *Electronic Letters*, 36(21), pp. 1770-1771, October. 2000.

[5] I. C. Lin, and C. C. Chang, and M. S. Hwang, " Security Enhancement for the Simple Authentication Key Agreement Algorithm", *24th Ann. Int. Computer Software and Applications Conf*, pp. 113-115, 2000.

[6] B. T. Hsieh, and H. M. Sun, and T. Hwang, "Cryptanalysis of enhancement for simple authentication key agreement algorithm", *Electronic Letters*, 38(1), pp. 20-21, January. 2002.

[7] R. J. Anderson, and T. M. A. Lomas, "On Fortifying Key Negotiation Schemes with Poorly Chosen Passwords", *Electronic Letters*, 30, pp. 1040-1041, June. 1994.

[8] S. Bakhtiari, and R. Safavi-Naini, and J. Pieprzyk, "On Password-Based Authenticated Key Exchange using Collisionful Hash Function", *Australasian Conference on Information Security and Privacy*, 1996.