효율적인 일회용 패스워드 인증 스킴

류은경*, 윤은준*, 유기영*
*경북대학교 컴퓨터공학과
e-mail:{ekryu, ejyoon}@infosec.knu.ac.kr, yook@knu.ac.kr

An Efficient One-Time Password Authentication Scheme

Eun-kyung Ryu*, Eun-jun Yoon*, Kee-young Yoo*
*Dept. of Computer Engineering, Kyungpook National University

요 약

최근에 YEH-SHEN은 스마트 카드를 이용한 일회용 패스워드 인증 스킴을 제안했다. 본 논문에서는 YEH-SHEN의 인증 스킴이, 사용자 등록 단계에서 로그인 사용 횟수를 N번으로 제한하고 있으며 또한 로그인 단계서 일회용 패스워드를 계산할 때 일방향 해쉬 함수를 (N-로그인 횟수)번 만큼 반복 수행해야 한다는 문제점을 지적한다. 또한 본 논문에서는 이를 개선한 보다 효율적인 새로운 인증 스킴을 제안하고 제안된 스킴이 여러 보안 요구사항에 안전함을 보인다.

1. 서 론

패스워드 기반의 사용자 인증은 현재 가장 일반적으로 사용되는 인증 방법이다. 하지만 전통적인 패스워드 기반의 인증 스킴은 다음과 같은 공격에 취약함을 보일 수 있다. 첫째, 사용자는 일반적으로 쉽게 기억할 수 있는 단순한 패스워드를 선택하는 경향이 있다. 이러한 패스워드는 낮은 엔트로피를 갖기 때문에 공격자의 사전 공격에 취약하다는 문제점이 있다. 둘째, 대부분의 인증 스킴이 오직 사용자만 인증을 하기 때문에 서버 스푸핑 공격의 가능성이 있다. 셋째, 공격자는 네트워크 상에서 이전에 사용한 사용자의 패스워드를 가로채기 할 수 있기 때문에 재전송 공격과 같은 다른 위협들이 존재한다. 위와 같은 보안상의 문제점들을 해결하기 위해서, 현재까지 패스워드 기반의 안전한 인증 스킴에 대한 많은 연구들이 이루어져왔다.[1]-[6].

특히, Lamport [1]는 재전송 공격에 안전한 일회용 패스워드 개념을 제안하였으며 Haller는 Lamport의 스킴을 응용한 S/KEY 일회용 패스워드 스킴 [7][8]을 제안하여 RFC 1760 [9]에 표준화되었다. 그러나, [10][11]에서 S/KEY 스킴이 재전송 공격의 특별한 경우인 재시도 공격과 오프라인 사전 공격과 같은 몇몇 강화된 공격에 안전하지 못함을 지적되었다. 이에 최근에 YEH-SHEN [12]은 RFC 1760 표준 S/KEY 일회용 패스워드 스킴의 보안 취약점을 강화한 스마트 카드를 이용한 새로운 일회용 패스워드 인증 스킴을 제안하였다. YEH-SHEN이 제안한 스킴은 서버 스푸핑 공격, 재시도 공격, 오프라인 패스워드 공격 등 여러 가지 공격에 안전하고 상호인증이 제공되는 스킴이다.

본 논문에서는 YEH-SHEN이 제안한 스킴이 등록 단계에서 로그인 사용 횟수를 N번으로 제한하고 있으며 로그인 단계에서 일방향 함수를 (N-로그인 횟수)번 만큼 반복 수행하여 일회용 패스워드를 계산해야 하는 비효율성을 지적하며 이를 개선한 보다 효율적인 새로운 인증스킴을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 기존의 YEH-SHEN이 제안한 스킴에 대해 살펴보고, 3장에서는 본 논문에서 제안하는 효율적인 일회용 인증 스킴을 기술하고, 제안한 스킴에 대한 안전성과 효율성을 분석한다. 마지막으로 4장에서 결론을 맺는다.

2. 관련 연구

이 장에서는 본 논문에서 사용할 용어들을 정의하고, YEN-SHEN의 일회용 패스워드 인증 스킴을 소개하고 스킴이 가지는 기능과 효율성 측면을 분석한다.

2.1 용어 정의

- N : 전체 로그인 횟수
- t : t번째 로그인
- C : N-t로 계산되며, 남은 로그인 횟수
- SEED : 사용자 및 서버에서 패스워드 생성시 사용하는 사전 공유 비밀값으로 아주 큰 랜덤 수

- H(·) : 일방향 해쉬 함수(one-way hash function)
- ⊕ : 배타적 논리합 연산(Exclusive OR operation)
- D : 서버가 생성하는 랜덤 수(random number)
- K : 사용자 비밀키
- p : 일회용 패스워드(one-time password)

2.2 YEH-SHEN의 인증 스킴

YEH-SHEN의 일회용 패스워드 인증스킴은 등록 단계, 로그인 단계, 인증 단계로 구성되며 각 단계는 다음과 같다.

등록 단계:

User ← Server: SEED

User ← Server: N, SEED⊕D, H(D)

User → Server: p_0⊕D

(1) 서버는 사용자와의 사전 공유 비밀값인 큰 랜덤 수 SEED를 생성하여 스마트 카드에 저장한 후 안전한 채널을 통하여 사용자에게 전달한다.
(2) 서버는 랜덤 수 D를 생성한 후 SEED⊕D와 H(D)를 계산하여 N과 함께 사용자에게 전송한다.
(3) 사용자는 스마트 카드에 저장된 SEED로 수신한 SEED⊕D를 XOR 연산하여 랜덤 수 D를 추출한다. 추출한 D를 한번 해쉬한 후 수신한 H(D)와 비교한다. 만약 두 값이 같으면, 사용자는 서버를 인증하여 초기 패스워드 $p_0=H^N(K⊕SEED)$를 계산한 후 D와 XOR하여 서버에 응답한다. 서버는 사용자의 ID와 초기 패스워드 p_0를 데이터베이스에 저장한다.

로그인 단계:

User ← Server: C, SEED⊕D, H(D)⊕p_{t-1}

User → Server: p_t⊕D

(1) 사용자가 t번째 로그인을 요청한다고 가정하면, 서버는 랜덤 수 D를 생성하여 SEED⊕D와 H(D)⊕p_{t-1}을 계산한 후 C=N-t와 함께 사용자에게 보낸다.
(2) 사용자는 스마트 카드에 저장된 SEED로 수신한 SEED⊕D를 XOR 연산하여 랜덤 수 D를 추출한다. 추출한 D를 한번 해쉬한 후 H(D)와 비교하기 위해서 스마트 카드에 저장된 t-1번째 일회용 패스워드 p_{t-1}로 수신한 H(D)⊕p_{t-1}과 XOR 연산하여 H(D)를 추출하여 비교한다. 만약 두 값이 같으면, 사용자는 서버를 인증하여 t번째 일회용 패스워드 $p_t=H^C(K⊕SEED)$를 계산한 후 D와 XOR하여 서버에 응답한다.

인증 단계:

서버는 사용자로부터 받은 p_t⊕D와 소유하고 있던 D를 XOR 연산하여 t번째 일회용 패스워드 p_t를 추출한다. 추출한 t번째 일회용 패스워드 p_t를 한번 해쉬한 후 서버에 저장되어 있는 t-1번째 일회용 패스워드 p_{t-1}과 비교한다. 만약 두 값이 같으면, 서버는 사용자를 인증하게 된다. 또한 데이터베이스에 저장되어 있는 t-1번째 일회용 패스워드 p_{t-1}을 t번째 일회용 패스워드 p_t로 업데이트하고 저장되어 있는 일련 번호를 C로 갱신한다.

2.3 YEH-SHEN의 스킴 분석

YEH-SHEN의 스킴은 기존의 RFC 1760 표준 S/KEY 일회용 패스워드 스킴이 갖는 문제점을 개선하기 위해 스마트카드를 이용하며, 카드내에 저장된 SEED와 난수를 이용하여 사용자 인증뿐만 아니라 서버인증기능을 제공한다. 하지만 YEH-SHEN의 일회용 패스워드 스킴은 다음과 같은 비효율성을 가진다. 첫째, 등록 단계에서 로그인 사용 횟수를 N번으로 제한하고 있다. 둘째, 로그인 단계에서 일회용 패스워드를 계산할 때 일방향 해쉬 함수를 (N-로그인횟수)번 만큼 반복 계산해야 한다.

본 논문에서는 이러한 비효율성을 개선하는데 초점을 맞춘다.

3. 제안한 스킴

이 장에서는 YEN-SHEN의 스킴을 개선한 보다 효율적 일회용 패스워드 인증 스킴을 제안하며 제안된 스킴에 대해서 안전성과 효율성을 분석한다.

3.1 인증 스킴

본 논문에서 제안한 스킴의 구성은 앞에서 살펴본 YEN-SHEN의 스킴과 같이 등록, 로그인, 인증의 3단계로 구성되며 각각의 단계는 다음과 같다.

등록 단계:

User ← Server: SEED

User → Server: ID, p_0

(1) 서버는 사용자와의 사전 공유 비밀값인 큰 랜덤 수 SEED를 생성하여 스마트 카드에 저장하고, 안전한 채널을 통하여 SEED가 저장된 스마트카드를 사용자에게 전달한다.
(2) 사용자는 스마트 카드에 저장된 SEED와 함께 자신의 임의의 길이의 비밀 패스워드 K를 이용하여 초기 패스워드 $p_0=H(K⊕SEED)$를 계산한 후 ID와 함께 안전한 채널을 통하여 서버에 응답한다. 서버는 사용자의 ID와 초기 패스워드 p_0를 데이터베이스에 저장한다.

로그인 단계:

User → Server: Login request, ID

User ← Server: SEED⊕D, H(D⊕p_{t-1})

User → Server: $p_t \oplus D$

(1) t번째 로그인을 위해 사용자는 서버에게 로그인 요청을 한다.
(2) 서버는 ID의 유효성을 검사한 후, 랜덤 수 D를 생성한다. 생성한 D를 이용하여 SEED⊕D와 $H(D \oplus p_{t-1})$을 계산하여 사용자에게 챌린저로 보낸다.
(3) 사용자는 자신의 스마트 카드에 저장된 SEED로 수신한 SEED⊕D를 XOR 연산하여 랜덤 수 D를 추출한다. 추출한 D와 스마트 카드에 저장된 p_t을 이용하여 $H(D \oplus p_{t-1})$을 계산한 후 수신한 $H(D \oplus p_{t-1})$과 같은지를 비교한다. 만약 두 값이 같으면, 사용자는 서버를 인증하여 t번째 일회용 패스워드 $p_t=H(p_{t-1})$를 계산한 후 D와 XOR하여 서버에 응답한다.

인증 단계:

서버는 사용자로부터 받은 $p_t \oplus D$와 자신이 생성한 난수 D를 XOR 연산하여 t번째 일회용 패스워드 p_t을 추출한다. 서버에 저장되어 있는 t-1번째 일회용 패스워드 p_{t-1}을 한번 해쉬한 값과 추출한 t번째 일회용 패스워드 p_t를 비교한다. 만약 두 값이 같으면, 서버는 사용자를 적법한 사용자임을 인증하고 데이터베이스에 저장되어 있는 t-1번째 패스워드 p_{t-1}을 p_t로 갱신한다.

3.2 안전성 분석

■서버 스푸핑 공격: 로그인 단계에서 사용자는 SEED, D, p_{t-1}을 통하여 서버를 인증하며, 서버는 p_t에 의해서 사용자를 인증한다. 이러한 상호 인증은 공격자의 서버 스푸핑 공격을 방지할 수 있다.

■재시도 공격: 서버의 챌린저를 미리 예측할 수 없기 때문에 공격자는 서버로 위장할 수 없다. 일회용 패스워드를 사용함으로 사용자를 속일 수 있는 다음 챌린저를 미리 예측할 수 없다. 따라서 공격자가 이전의 챌린저 메시지를 가지고 있어도 다음 챌린저에서 그 메시지를 사용할 수 없으므로 재시도 공격을 수행할 수 없다.

■오프라인 사전공격: RFC 1760 표준 S/KEY 스킴의 안전성은 오직 사용자의 비밀키 K에 의존한다. 하지만 사용자는 일반적으로 쉽게 기억 가능한 간단한 패스워드를 선택한다. 공격자는 올바른 일회용 패스워드를 찾기 위해 사용자가 선택한 비밀키 K를 찾는 오프라인 사전공격을 할 수 있다. 이것을 고려해서 본 논문에서는 서버에서 아주 큰 랜덤 수의 SEED를 생성함으로 인해서 사용자의 비밀키 K를 보호하는데 사용하였다. 그러므로 공격자가 오프라인 사전 공격을 시도하려면 K와 SEED를 동시에 결정하여야 함으로 공격이 어려우며 사용자 비밀키 K는 서버로 인해 안전하게 보호되어 오프라인 사전공격에 안전하다.

■능동적 공격: 능동적 공격에 안전하고 메시지 내용이 누설되지 않는 비밀성을 가지기 위해서는 세션 암호를 사용하는 것이 필요하다. 제안한 스킴에서는 통신 당사자간에 주고받는 메시지를 암호화하기 위해 인증 과정에서 서버가 생성한 랜덤값 D에 일방향 해쉬 함수를 적용하여 세션키로 사용하여 능동적 공격에 대응할 수 있다.

표1은 기존의 일회용 패스워드 스킴과 제안한 스킴의 안전성 및 효율성을 비교 분석한 결과이다. 표 1에서 보는 바와 같이 본 논문에서 제안한 인증스킴은 YEH-SHEN의 인증 스킴과 같은 안전도를 갖으면서, 보다 나은 효율성을 갖는다. 제안한 스킴에서 일회용 패스워드가 $p_0=H(K \oplus SEED)$, $p_1=H(p_0)$, $p_2=H(p_1)$의 형태로 생성되기 때문에 RFC 1760 표준 S/Key 스킴이나 YEH-SHEN이 제안한 스킴에서처럼 사용 횟수에 대한 제한이 없을 뿐 아니라 로그인 단계에서 매번 필요한 횟수만큼의 일방향 해쉬 함수를 계산하지 않아도 된다는 장점이 있다.

표 1 제안된 스킴의 안전성 및 효율성 비교

	RFC 1760 표준 S/KEY	YEH-SHEN 스킴	제안한 스킴
사용횟수	N회	N회	제한없슴
해쉬횟수	C회	C회	1회
서버 스푸핑 공격 방지	O	O	O
재시도 공격 방지	X	O	O
오프라인 사전공격 방지	X	O	O
능동적 공격 방지	X	O	O
메시지 엿보기 방지	X	O	O
안전성	일방향 해쉬 함수	일방향 해쉬 함수	일방향 해쉬 함수
상호인증 기능	X	O	O

4. 결 론

본 논문에서 제안한 스킴은 일회용 패스워드 방식을 이용하여 안전하고 효율적인 상호 인증을 가능하게 하는 방식이다. 스마트 카드와 일방향 해쉬 함수에 의존한 여러 가지 안전성은 기존의 S/KEY 방식의 문제점을 완전하게 개선하고 있으며 또한 YEH-SHEN이 제안한 스킴에서처럼 사용 횟수에 대한 제한이 없을 뿐 아니라 로그인 단계에서 매번 필요한 횟수만큼의 일방향 해쉬 함수를 계산하지 않아도 되는 효율적이고 간편한 구조로 이루어져 있다. 본 논문에서 제안한 새로운 스킴이 가지는 이러한 장점들은 보안이 요구되는 온라인 뱅킹, 온라인 계약, 온라인 협약과 같은 민감한 통신 환경에서 이상적으로 사용 될 수 있다.

참 고 문 헌

[1] L. Lamport, "Password authentication with insecure communication," Communications of ACM, Vol. 24, pp.770-772, 1981.

[2] T.Kwon, "Authentication and key agreement via memorable password," Proc. 2001 Internet Society Network and Distributed System Security Symposium, San Diego, CA, Feb. 2001.

[3] T.Wu, "Secure remote password protocol," Proc. 1998 Internet Society Network and Distributed System Security Symposium, San Diego, CA, March 1998.

[4] S.M. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," Proc. IEEE Symposium on Research in Security and Privacy, pp.72-84, Oakland, May 1992.

[5] S.M. Bellovin and M. Merritt, "Augmented encrypted key exchange: A Password-based protocols secure against dictionary attacks and password file compromise," AT&T Bell Laboratories, 1994.

[6] L. Gong, M.Lomas, R. Needham, and J, Saltzer, "Protecting poorly chosen secrets from guessing attacks," IEEE J.Sel. Areas Commun., vol.11,no.5, pp.648-656, June 1993.

[7] N.M. Haller, "A one-time password system," RFC 1938, May 1996.

[8] N.M. Haller, "On internet authentication," RFC 1704, Oct. 1994.

[9] N.M. Haller, "The S/KEY one-time password system," RFC 1760, Feb. 1995.

[10] C.J. Mitchell and L. Chen, "Comments on the S/KEY user authentication scheme," ACM Operation Systems Review, vol.30, no.4, pp.12-16, Oct. 1996.

[11] S.M. Yen and K.H. Liao, "Shared authentication token secure against replay and weak key attacks," Information Processing Letters, vol.62, pp.77-80, 1997.

[12] T.C.YEH, H.Y.SHEN and J.J.HWANG. "A Secure One-Time Password Authentication Scheme Using Smart Cards," IEICE Trans. Commun., vol.e85-b, no.11 November 2002.