한국산학기술학회논문지
Vol. 11, No. 4, pp. 1301-1306, 2010

효율적인 OTP 기반의 인증 프로토콜

신승수[1*], 한군희[2]
[1]동명대학교 정보보호학과, [2]백석대학교 정보통신학부

Authentication Protocol based on Efficient OTP

Seung-Soo Shin[1*] and Kun-Hee Han[2]
[1]Dept. of Information Security, College of Information & Communication, Tongmyong University
[2]Division of Information & Communication Engineering, Baekseok University

요 약 패스워드 기반의 프로토콜은 패스워드가 가지는 제약으로 인한 공격에 대하여 안전해야 할 뿐 아니라 사용자의 작업량을 줄이기 위한 효율성도 매우 중요한 요건이다. 패스워드를 기반으로 하는 사용자 인증 프로토콜은 사용자들이 쉽게 기억할 수 있는 패스워드를 사용하기 때문에 대부분의 경우에 패스워드 추측공격에 취약한 문제점이 있다. S/KEY 시스템의 문제점을 개선한 새로운 메커니즘을 송유진 등이 제안하였다. 송유진 등이 제안한 프로토콜은 등록과정에서 문제점이 있고 악의적인 목적을 갖는 있는 서버에 의해 사용자의 정보를 악용할 수 있다. 이러한 문제점이 개선된 효율적인 OTP 기반의 인증 프로토콜을 제안한다.

Abstract The protocol based on password have very important qualifications that not only satisfy against attacks cause of restricting that have, but also efficiency of reducing users' workload. It has a problem of speculative attacks for the user authentication protocol based on password with most case, because users use password that can remember easily. Song and Etc. have proposed new mechanism that improved the problem of S/KEY system. The protocol proposed by Song has a problem in registration process, and user information can be abused by the malevolent server. We propose a new authentication protocol based on efficient OPT, that improved above problems.

Key Words : S/KEY, OTP, Seed, Authentiaction, Discrete logarithm

1. 서론

현대사회는 컴퓨터 및 통신망의 보급이 확대되고, 분산처리 시스템과 개방형 시스템의 응용이 활발히 진행되면서 수많은 정보들이 교환되고 있다. 우리나라는 인터넷 강국으로 불리며 초고속 인터넷의 보급과 유·무선 전화의 사용 등에서 선진국 못지않게 인프라가 잘 구축하고 있다. 전자 금융의 가입자가 해마다 늘어나고 있고 많은 사람들이 사용하고 있는 인터넷 뱅킹 서비스는 유비쿼터스 시대와 맞물려 우리 생활 깊숙이 자리 잡았다[1].

그러나, 인터넷은 개방형 네트워크이기 때문에 악의적인 공격자에 의한 시스템 침입, 불법 해킹, 도청 등과 같은 다양한 형태의 공격에 취약하다. 악의적인 행위를 방지하기 위한 보안 시스템의 구성 요소 및 동작의 완결성이 보장되어야만 시스템의 안전성을 보증할 수 있게 된다. 어느 한 부분의 약점은 전체 시스템의 완결성에 치명적 결과를 발생하게 된다.

기존의 오프라인 상에서 이루어지던 은행 거래와 상거래가 인터넷 뱅킹과 전자상거래와 같은 온라인상에서 이루어짐에 따라 그 위험 수준은 더욱 높아지고 있다. 이러한 환경에서 사용자 인증은 안전한 통신을 위한 필수적인 요소라 할 수 있다. 개인 정보 유출로 인한 전자금융 사고의 발생을 줄일 수 있는 방법 중의 하나로 강력한 사용자 인증을 수행하는 것이다. 이러한 보안의 중요성을 기반으로 사용자 인증을 위한 다양한 연구가 진행되어 있다[2,3].

*교신저자 : 신승수(shinss@tu.ac.kr)
접수일 10년 02월 01일 수정일 (1차 10년 03월 19일, 2차 10년 04월 05일) 게재확정일 10년 04월 09일

인증(Authentication)이란 요구된 실체의 신원에 대한 보증 기능으로 현재 ID/패스워드를 기반으로 한 인증 메커니즘이 가장 많이 사용되고 있다. 하지만, ID/패스워드 인증 방식은 패스워드와 같은 단순한 인증 정보를 활용하기 때문에 네트워크 환경에서 커다란 문제점을 가지고 있다[4]. 이러한 단점을 극복할 수 있는 인증 기법이 매번 새롭게 패스워드를 생성하는 일회용 패스워드(OTP : One time Password)이다. 일회용 패스워드 기술은 이러한 단점을 극복할 수 있는 인증 기법이다[5,6].

OTP는 매번 새로운 패스워드를 생성함으로서 아이디와 비밀번호 기반 방식의 문제점을 보완하고 있다. 이러한 OTP는 주로 인터넷 뱅킹에서 사용되어 왔으나 최근에는 온라인상의 다양한 형태의 상거래에서 활용하고 있다. 최근에는 강력한 개인 인증요소인 지문정보를 이용하여 가변적이고 안전한 일회용 암호화키를 생성한다[7]. 이러한 2-Factor 인증방식은 OTP 토큰의 분실 또는 도난과 같은 물리적 공격에 대한 방어책이 미비한다. 이러한 문제를 해결하기 위해서 H- MAC를 이용한 3-Factor 인증 방식 등이 제안되고 있다[8].

본 논문에서는 OTP 생성 기법 보다는 OTP 기반의 인증 메커니즘에 대하여 분석한다. OTP 기반의 초기 인증 방식에는 S/KEY 시스템을 이용한 인증 방식이 제안되었다[9]. S/KEY 시스템은 사용 횟수에 따라 반복적인 초기화 과정이 필요하며 이러한 초기화 과정에서 비밀 패스워드가 노출되게 되고 인증과정에서는 일회용 패스워드와 seed가 함께 노출되는 경우에 오프라인 사전 공격(dictionary attack)의 위험성이 존재한다. 이러한 S/KEY 시스템의 문제점을 개선한 새로운 메커니즘을 송유진[10] 등이 제안하였다. 송유진 등이 제안한 프로토콜은 등록과정에서 문제점이 야기 된다. 또한 인증 과정에서 서버는 초기화 과정에서 사용자로부터 받은 정보를 저장하고 있어야 하기 때문에 서버의 내부자가 악의적인 의도를 가졌다면 서버의 디렉토리에서 사용자의 정보를 악용할 의도가 있다. 이러한 문제점을 개선한 효율적인 OTP 기반의 인증 프로토콜을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대하여 알아보고, 3장에서는 효율적인 OTP 기반의 인증 프로토콜에 대하여 알아본다. 그리고 4장에서 안전성을 분석하고, 5장에서 결론을 맺는다.

2. 관련 연구

S/KEY 기반 인증 프로토콜은 일반적인 패스워드 인증 방식보다 패스워드가 노출이 되더라도 스니핑이나 재연 공격을 방지할 수 있으며 패스워드는 사용자만이 알고 있으며 서버에는 패스워드가 저장되지 않기 때문에 공격자가 서버의 데이터베이스에 접근을 하고 그 데이터를 알아내더라도 그 결과는 무의미하다는 장점은 있다. 그러나 초기화 과정에서 사용 횟수가 제한적이며 인증과정에서 일회용 패스워드와 seed가 함께 노출되는 경우에는 오프라인 사전 참조식 공격의 위험성이 존재한다. 이러한 문제점을 개선한 새로운 프로토콜을 송유진[10] 등이 제안하였다. 본 절에서는 송유진[10]등이 제안한 프로토콜을 분석한다.

2.1 인증 절차

송유진 등이 제안한 인증 절차는 초기화 단계, 인증단계로 구성된다.

2.1.1 초기화 단계

초기화 단계는 사용자와 서버 상호간 기본 인증 정보를 확립하기 위한 단계이며 최초 1회만 실행된다. 초기화 단계에서 필요한 절차는 다음과 같다. 사용자가 서버에 로그인하게 되면 서버는 사용자에게 초기 seed를 사용자에게 전달하고 사용자는 seed와 한 쌍의 패스워드를 기반으로 K_3를 계산하여 서버에게 전달한다. 그리고 서버는 사용자로부터 전송된 K_3와 초기 seed를 보관한다. 이러한 과정을 간단히 표시하면 다음과 같다.

① Message : U → S : ID

② Message : U ← S : S_{int}
(S_{int} 은 임의로 생성한 값)

③ Message : U → S : K_3 ($K_3 = H(K_1)_{K2}$:
$K_1 = H(P_1 \| S_{int})_{P2}$, $K_2 = H(P_2 \| S_{int})_{P1}$)
여기서, S :서버, K_N : OTP(N번째), ‖ : 합성연산자이다.

④ 서버는 K_3를 K_S로 S_{int}를 S_S로 각각 저장한다.
여기서, K_S은 서버에 보관된 OTP값이고 S_S은 저장된 seed 값이다.

2.1.2 인증단계

초기화 단계 이후 사용자가 서버로부터 인증 받는 과정이며 인증에 필요한 메시지의 전달 과정을 간단히 표시하면 다음과 같은 과정으로 진행된다.

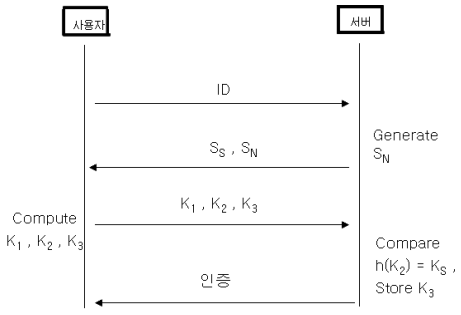
① Message : U → S : ID

② 서버는 S_N(신규 seed값)를 생성한다.

③ Message : U ← S : S_S, S_N

④ Compute : U : $K_1 = H(P_1 \| S_S)_{P2}$,
$K_2 = H(P_2 \| S_S)_{P1}$, $K_3 = H(K_{N1})_{KN2}$
$(K_{N1} = H(P_1 \| S_N)_{P2}$, $K_{N2} = H(P_2 \| S_N)_{P1})$
⑤ Message : U → S : K_1, K_2, K_3
⑥ Compare : $H(K_2)_{K1} = K_S$?
⑦ Store : S Store $K_3 \rightarrow K_S$, $S_N \rightarrow S_S$
⑧ Authenticate : U ← S

송유진 등이 제안한 프로토콜에 대한 인증에 필요한 메시지 전달 과정을 간단히 표시하면 다음 그림 1과 같다.



[그림 1] 인증 프로토콜

2.2 관련 연구 분석

송유진 등이 제안한 프로토콜은 초기화 단계에서 로그인 할 때 ID와 한 쌍의 적절한 패스워드를 생성한다. 생성된 패스워드는 사용자만 알고 있고 어느 곳에도 노출되거나 저장되지 않기 때문에 인증단계에서 $K_1 = H(P_1 \| S_S)_{P2}$, $K_2 = H(P_2 \| S_S)_{P1}$, $K_3 = H(K_{N1})_{KN2}$, $K_{N1} = H(P_1 \| S_N)P_2$, $K_{N2} = H(P_2 \| S_N)_{P1}$ 로부터 K_1, K_2, K_3를 얻을 수 없다. 따라서 등록과정에서 문제점이 야기 된다. 또한 인증 과정에서 서버는 초기화 과정에서 사용자로부터 받은 정보 $K_3 \rightarrow K_S$와 $S_{int} \rightarrow S_S$를 저장하고 있어야 하기 때문에 서버의 내부자가 악의적인 의도를 가졌다면 서버의 디렉토리에서 사용자의 정보를 악용할 의도가 있다. 이러한 문제점을 해결하기 위해 새로운 OTP 기반의 인증 프로토콜을 제안한다.

3. 제안된 프로토콜

기존 프로토콜은 부수적인 전송 횟수나, 지수승 계산 비용에 대하여 효율성 개선의 여지가 있다. 본 논문에서는 보안 요구사항들을 만족하면서도 OTP를 사용하여 인증의 효율성을 증대시킨 프로토콜을 제안하고자 한다.

3.1 시스템 파라미터

제안된 프로토콜에 사용할 파라미터에 대하여 표 1과 같이 정의한다. 프로토콜 기술 중 'mod p' 표기는 생략하기로 한다. 충돌이 없는 일방향 해시함수를 $h: \{0,1\}^* \rightarrow \{0,1\}^n$로 표기한다. 여기서, $\{0,1\}^*$는 유한한 이진문자열의 집합이고, $\{0,1\}^n$는 길이가 n인 이진문자열의 집합이라 하자. 즉, 임의의 길이의 문자열을 필요한 길이의 문자열로 변환할 수 있다.

[표 1] 표기

기호	설명
p, q	강한 소수, $p = 2q+1$
G_q	위수 q를 갖는 $\mathbb{Z}_p^*$의 부분군 (보통 160 비트)
g	G_q의 생성자, p의 원시근
A, S	사용자 아이디, 서버 아이디
$h(\cdot), h'(\cdot)$	충돌이 없는 일방향 해시함수
K	세션키
π_A, π_S	각각 사용자와 서버의 패스워드
x_A, v_A	서버에 저장되는 사용자의 검증자 값
a, b	G_q의 랜덤 정수
$\approx$	두 값의 비교

3.2 프로토콜 제안

사용자 ID와 패스워드를 설정하는 등록단계는 사용자가 서버로부터 서비스를 받기 위하여 서버에 ID와 패스워드를 등록하는 단계이다. 사용자는 서비스를 받기 전에 다음과 같은 과정을 통해 서버에 등록한다.

① 사용자는 패스워드를 선택한 후 $h^n(pwd) = \pi_A$ 를 계산한다. $x_A = h'(A, S, \pi_A)$, $v_A = g^{h'(A, S, \pi_A)^{-1}}$를 계산하고 x_A, v_A 를 안전한 채널(secure channel)을 통해 서버에 전송한다.
② 서버는 사용자에게 받은 x_A, v_A 를 패스워드 디렉토리내에 저장한다.

여기에서 $\pi_A = h^n(pwd)$ 는 사용자의 패스워드에 일방향 해시함수를 n번 적용하여 얻은 값이다. $\pi_A = h^n(pwd)$ 는 원타임 패스워드 방식처럼 패스워드를 설정한 후 i번째 통신에서 $h^{n-i+1}(pwd)$ 를 사용하며 설정한 패스워드를 $n-1$번 사용한 후에는 새로운 패스워드를

설정한다.

본 논문에서 제안하는 효율적인 OTP 기반의 인증 프로토콜은 서버와 패스워드를 설정 한 후 i 번째 인증에 대한 수행과정은 다음과 같은 절차로 수행한다.

① 사용자는 $a \in [1, q-1]$ 을 선택하고 $X_A = g^a$ 을 계산하고 서버에게 ID와 X_A을 전송한다.

② 서버는 패스워드 디렉토리로부터 x_A, v_A 을 검색하고 $b \in [1, q-1]$를 선택한 후 $X_{SA} = (v_A)^b \oplus x_A$를 계산한다. 사용자로부터 받은 랜덤수를 이용하여 $K_{AS} = (X_A)^b = g^{ab}$, $V_{SA} = h^{n-i+1}(S, X_A, K_{AS})$를 계산하여 사용자에게 보낸다.

③ 사용자는 $K_{SA} = (X_{SA} \oplus x_A)^{h(A,S,\pi_A)a} = g^{ab}$을 계산하고 $V_{SA} \approx h^{n-i+1}(S, X_A, X_{SA}, K_{AS})$을 검사하여 일치하면 서버 S를 인증한다.

④ 사용자는 $V_{AS} = h^{n-i+1}(A, X_A, X_{SA}, K_{AS})$을 계산하여 서버에게 전송하면 서버는 $V_{AS} \approx h^{n-i+1}(A, X_A, X_{SA}, K_{AS})$를 확인한다. 서버는 사용자를 인증하고 사용자의 정보를 $\pi_A = h^{n-1}(pwd)$를 교체 한다. 서버는 새로운 값 $x_A = h'(A, S, \pi_A)$, $v_A = g^{h(A,S,\pi_A)^{-1}}$ 을 계산하고 패스워드 디렉토리에 저장한다.

다음은 제안한 OTP 기반의 인증 프로토콜에 필요한 인증 과정을 간단히 표시하면 그림 2과 같다.

단계	User	메시지	Server
1	Choose a $X_A = g^a$	$ID,\ X_A$ $\rightarrow$	Choose b
2	$h(g^s),\ K = g^{ab},$ $K^* = g^{as}$	$X_{SA},\ V_{SA}$ $\leftarrow$	$X_{SA} = (v_A)^b \oplus x_A,$ $K_{AS} = (X_A)^b = g^{ab},$ $V_{SA} = h^{n-i+1}(S, X_A, K_{AS})$
3	$K_{SA} = g^{ab},$ $V_{SA} \approx$ $h^{n-i+1}(S, X_A, X_{SA}, K_{AS})$	V_{AS} $\rightarrow$	$V_{AS} \approx$ $h^{n-i+1}(A, X_A, X_{SA}, K_{AS})$

[그림 2] 제안한 인증 프로토콜

4. 안정성 분석

본 장에서는 제안한 인증 프로토콜에 대하여 안전성을 검증한다. 제안한 프로토콜의 안전성은 산술 시간에 풀기 어렵다고 알려져 있는 이산대수문제와 Diffie- Hellman 문제의 어려움 그리고 해시함수의 암호학적 강도에 근거를 둔다.

OTP 기반의 인증 프로토콜에 대한 도청 공격, 재전송 공격, 오프라인 패스워드 추측 공격, Denning -Sacco 공격, 완전한 전방향 보안성 제공 등 다양한 공격에 대하여 안전성을 분석한다.

① 도청공격 :

제안한 프로토콜은 전송되는 메시지들이 추측 불가능한 임의의 난수들이기 때문에 단순한 도청만으로 유용한 정보를 얻을 수 없다. 즉 전송되는 메시지를 도청하였다면 X_A, X_{SA}, V_{SA}, V_{AS}값들을 얻을 수 있다. 그러나 이러한 값들로부터 패스워드 $h^n(pwd) = \pi_A$ 나 세션키 K에 대한 정보를 얻을 확률은 사용된 해시함수의 특성과 이산대수 문제, Diffie-Hellman 문제의 어려움 때문에 무시할만하다.

② 재전송공격 :

프로토콜 단계별 과정에서 같은 메기지가 연속적으로 전송되지 않으므로 한 세션 내에서 같은 메시지를 전송하는 공격을 수행할 수 없다. 또한 매 세션마다 새로 생성되는 랜덤 수와 새로운 π_A를 사용하기 때문에 공격자가 이전 세션에서 전송된 메시지를 가지고 있어도 다음 세션에서 그 메시지를 사용할 수 없으므로 재전송 공격을 할 수 없다.

③ 오프라인 패스워드 추측 공격 :

오프라인 패스워드 추측공격을 수행하기 위해서는 메시지를 도청하거나 사용자나 서버로 위장하여 정보를 수집하여야 한다. 그러나 패스워드 후보자들 중에서 정확한 패스워드를 찾아내는 것이 제안된 프로토콜에서는 해시함수의 특성과 이산대수 문제 그리고 Diffie-Hellman 문제의 어려움 때문에 불가능하다.

④ Denning-Sacco 공격 :

Denning-Sacco 공격에 안전하기 위해서는 공 격자가 이전의 세션키를 안다 할지라도 사용자의 패스워드를 구할 수 없어야 한다. 세션키에는 사용자의 패스워드에 관한 정보를 포함하고 있지 않기 때문에 세션키가 노출된다고 할지라도 사용자의 패수워드나 패스워드의 정보를 알 수 없다. 만약, 공격자가 세션키를 안다고 가정하자. 공격자는 이 값과 이전 세션에서 도청한 정보들을 이용

하여 패스워드를 계산 하거나 패스워드 추측공격을 하려고 할 것이다. 그러나 성공할 확률은 아주 희박하다.

⑤ 완전한 전방향 보안성을 제공한다.

완전한 전방향 보안성은 공격자가 임의의 시점에서 패스워드를 알게 된다고 할지라도 이전 세션키들을 계산할 수 없을 때 제공된다. 제안한 프로토콜에서의 세션키의 안정성은 해시함수의 특성과 이산대수문제[11]의 어려움 때문에 패스워드가 노출되어도 과거에 사용되었던 세션키의 값들은 알 수 없다.

전통적인 패스워드 방식은 1회의 메시지만으로도 인증을 받을 수 있어 사용이 편리하고 절차가 간단하는 장점이 있으나 정보가 노출될 경우 악의적인 공격자가 모든 권한을 얻을 수 있다는 단점을 가지고 있다. 제안한 프로토콜은 송유진 등이 제안한 프로토콜과 마찬가지로 동일한 1회의 등록과정이 필요하며 또한 해쉬함수 연산 횟수도 1회 정도 단축하기 때문에 오버헤드에 대한 부담도 없다. 또한 인증과정에서 사용자의 정보인 어떠한 정보도 서버에 저장하지 않기 때문에 악의적인 서버의 내부자 공격에도 안전하다고 할 수 있다.

5. 결 론

본 논문에서는 패스워드가 노출이 되더라도 스니핑이나 재연 공격을 방지할 수 있으며 패스워드는 사용자만이 알고 있으며 서버에는 패스워드가 저장되지 않기 때문에 공격자가 서버의 데이터베이스에 접근을 하고 그 데이터를 알아내더라도 그 결과는 무의미하다는 장점을 가지고 있는 OTP 기반 인증 프로토콜을 제안하였다. 제안된 프로토콜은 패스워드 기반의 인증 프로토콜로서 여러 종류의 다양한 공격에 안전할 뿐만 아니라 완전한 전향 보안성을 제공한다. 또한 제안된 프로토콜을 간단히 수정함으로써 서버에 저장된 패스워드 디렉토리에 있는 패스워드 파일의 노출에도 패스워드 추측공격에 안전한 프로토콜이다. 공격자는 사용자와 서버 사이의 공유된 세션키를 알 수 없기 때문에 통신은 매우 안전하게 유지 된다. 제안한 프로토콜에서는 서버의 공개키를 사용하지 않기 때문에 기존의 OTP 프로토콜 환경에서 보다 성능 면에서 효율성을 가진다. 본 프로토콜은 안전한 통신을 위하여 인증, 세션키 공유 및 확인이 요구 되는 여러 분야 활용될 것으로 기대된다.

참고문헌

[1] 서승현, 강우진, “OTP 기술 현환 및 금융권 OTP 도입사례”, 정보보호학회지, 제17권, 제3호, 2007.

[2] 백미연, “전자상거래의 보안 강화 방법 및 OTP 이용 현황”, 지급결제와 정보기술, pp. 71-100, April 2006.

[3] 최동현, 김승주, 원동호, “일회용 패스워드 기술 분석 및 표준화 동향”, 정보보호학회지, 제17권, 제3호, 2007.

[4] 박중길, 장태주, 박봉주, 류재철, “시간을 이용한 효율적인 일회용 패스워드 알고리즘”, 정보처리학회논문지C, 8(4), Aug 2001.

[5] Rubin, A. D., Independent One time Passwords, Proc. 5th UNIX Security Symposium, USENIX Association, 1995.

[6] Rolf Oppliger, "Security Technologies for the World Wide Web," Artech House, 2000.

[7] 차병래, 고일석, “지문 특징을 이용한 일회용 암호키 생성기법”, 한국전자거래학회지, 제13권, 제1호, 2007.

[8] 신승수, 한군희, “OTP를 이용한 HMAC 기반의 3-Factor 인증", 한국산학기술학회논문지, 제10권, 제12호, 2009.

[9] N. Haller, "The S/KEY One-Time Password System", RFC 1760, 1995.

[10] 송유진, 이동혁, “OTP 기반의 웹서비스 인증 메커니즘 설계 및 구현”, 한국전자거래학회지, 제10권, 제2호, 2005.

[11] D. R. Stinson, Cryptography Theory and Practice, CRC, 1995.

신 승 수(Seung-Soo Shin) **[정회원]**

- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

<관심분야>
암호프로토콜, 무선 PKI, 네트워크 보안, USN, 스마트카드,

한 군 희(Kun-Hee Han) **[종신회원]**

- 2008년 8월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
암호프로토콜, 네트워크 보안, 영상처리