한국산학기술학회논문지
Vol. 10, No. 12, pp. 3708-3714, 2009

OTP를 이용한 HMAC 기반의 3-Factor 인증

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

HMAC-based 3-factor Authentication using 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 최근 컴퓨터 통신 기술이 발달함에 따라서 대부분의 정보 서비스가 온라인으로 이루어지고 있으며, 온라인 정보들의 가치 또한 높아지고 있다. 그러나 정보 기술의 발달에 따라 이를 공격하기 위한 다양한 공격 기법들도 생기고 있으며, 이 공격들로부터 안전한 온라인 서비스를 제공하기 위해서 일반적인 ID/Password 방식의 정적인 Password를 이용하는 것이 아니라 매번 새로운 Password를 생성하는 OTP를 이용하게 되었다. 현재 OTP 토큰을 이용한 2-factor OTP 생성방식이 주로 이용되고 있다. 그러나 이 2-Factor 인증방식은 OTP 토큰의 분실 또는 도난과 같은 물리적 공격에 대한 방어책을 제시하지 못한다. 본 논문에서는 이와 같은 문제를 해결하기 위해 HMAC을 이용한 3-factor 인증방식을 제안하며, 이와 함께 제안한 인증방식에 대한 안전성을 평가한다.

Abstract Recently, most of information services are provided by the computer network, since the technology of computer communication is developing rapidly, and the worth of information over the network is also increasing with expensive cost. But various attacks to quietly intercept the informations is invoked with the technology of communication developed, and then most of the financial agency currently have used OTP, which is generated by a token at a number whenever a user authenticates to a server, rather than general static password for some services. A 2-factor OTP generating method using the OTP token is mostly used by the financial agency. However, the method is vulnerable to real attacks and therefore the OTP token could be robbed and disappeared. In this paper, we propose a 3-factor OTP way using HMAC to conquer the problems and analyze the security of the proposed scheme.

Key Words : One Time Password, Authentication, HMAC, S/Key, One-way Hash Function

1. 서론

정보통신의 발달로 현대사회는 일명 정보화 사회라고 불릴 정도로 우리는 수많은 정보에 둘러 싸여있다. 특히, 최근 인터넷이 발달하면서 인터넷을 통한 서비스가 다양해지고 있을 뿐만 아니라 정보의 손쉬운 접근과 이용이 주는 편리함으로 인해 인터넷 서비스를 사용하는 사람들이 갈수록 크게 늘어나고 있다. 또한 통신기술이 급속도로 발전함에 따라 많은 정보 서비스들이 온라인을 통해서 이루어지고 있다. 기존에 오프라인 상에서 이루어지던 은행거래, 상거래가 인터넷 뱅킹과 전자상거래와 같이 온라인상에서 이루어지면서 많은 문제점에 노출되고 있다. 인터넷은 개방형 네트워크이기 때문에 인터넷 뱅킹이나 전자 상거래는 편리성 못지않게 공격자에 의한 시스템 침입, 불법 해킹 및 인터넷 피싱 등의 피해에 대해 노출되어 있다. 인터넷 뱅킹 사고, 대형은행 고객정보 유출 및 공인인증서 유출로 인한 은행 불법 인출 사건 등과 같은 불법 피해 사례가 늘고 있다. 이러한 사고로 인해 막대한

*교신저자 : 신승수(shinss@tu.ac.kr)
접수일 09년 11월 19일 수정일 09년 12월 02일 게재확정일 09년 12월 16일

금전적 손해뿐만 아니라 이로 인해 겪는 정신적 피해도 증가하여 산업자원부, 정보통신부, 금융감독위원회 및 금융감독원은 공동으로 “전자금융거래 안전성 강화 종합대책”을 수립하였다[1].

개인정보 유출로 인한 전자금융 사고를 줄일 수 있는 방법 중 하나는 강력한 사용자 인증을 수행하는 것이다[2]. 사용자 인증은 안전한 인터넷 사용을 위한 필수적인 요소이며, 대표적인 방식으로 ID/Password 인증 방식이 있다. 그러나 ID/Password 인증 방식은 정적 패스워드를 사용하기 때문에 도청에 의해 노출되면 악의적인 공격자가 이를 이용하여 정당한 사용자로 위장할 수도 있다[3]. 이러한 문제점을 해결하기 위해 매번 새로운 패스워드를 생성하는 일회용 패스워드(OTP : One-Time Password) 기반 인증기법이 인터넷 뱅킹 및 전자상거래에 사용되어 왔으며, 최근에는 게임, 음악 및 동영상등 다양한 분야에서 활용되고 있다.

OTP 인증이란 매 세션마다 변하는 동적 패스워드를 이용하여 개체를 인증하는 방식을 의미한다[4]. 이러한 개체를 인증하기 위한 요소로서 알고 있는 것(지식기반), 소유하고 있는 것(소유기반), 태생적으로 타고난 것(생체기반)과 같은 3가지 요소를 주로 이용한다. 기존 OTP 인증 방식은 지식-소유기반의 2-factor 인증방식을 사용하고 있으며, 입력값에 따라 질의-응답 방식, 이벤트 동기화 방식, 시간 동기화방식 및 조합방식으로 나눌 수 있다. 이러한 OTP를 생성하기 위한 OTP 생성 매체는 전용 H/W OTP 토큰과 OTP 생성 기능을 소프트웨어로 탑재한 모바일 OTP, 카드형 OTP 등이 있다[5].

기존의 OTP 인증 방식은 일방향 해시함수의 충돌성과 OTP 토큰에 대한 물리적 공격에 대한 문제점들이 나타나고 있다. 본 논문에서는 이러한 문제점을 분석하고 패스워드 방식, S/Key OTP 방식과 제안한 방식을 안전성과 효율성 측면에서 비교 분석하고자 한다. 비교 분석한 결과 새로 제안한 OTP 인증 방식의 문제점을 해결하기 위해 HMAC 기반 3-factor OTP인증 방식이 우수하다는 것을 알 수 있었다. 제안된 프로토콜은 OTP를 생성하기 위해 생체정보를 이용하여 OTP 토큰에 대한 물리적 공격을 해결하며, HMAC을 기반으로 하여 일방향 해시함수의 충돌성에 대한 문제점에 대해 더 효율적임을 알 수 있다.

2. 개요

본 장에서는 본 논문에서 사용할 용어들을 정의하고 OTP를 이용한 HMAC 기반의 3-factor 인증 구조를 만족해야 하는 기본적인 보안 요구사항들을 기술한다.

2.1 용어 정의

본 논문에서는 표 1과 같은 여러 가지의 표기법을 사용한다.

[표 1] 표기법

표 기	정 의
U	사용자
S	서비스 제공자 또는 서버
ID	사용자의 식별자
FIN	사용자의 지문
UPIN	사용자의 개인정보
T	동기화된 시간 클럭
C	동기화된 계수기
OTP	6자리 OTP 값
h( )	해쉬함수
$HMAC_K$( )	HMAC 함수
trunc( )	6자리 OTP값 추출함수

2.2 보안 요구사항

패스워드 기반의 프로토콜들이 고려해야 할 보안 특성과 요구조건은 다음과 같다[6,7]. 본 논문에서 제안한 프로토콜은 이러한 요구 조건들을 만족시키도록 설계하고 그에 대한 검증을 5장에서 서술한다.

1) 수동적 공격(passive adversary)은 도청공격에 안전해야한다. 도청공격(eavesdropping)은 온라인상의 통신 내용을 도청하여 세션키의 정보를 알아내거나 통신에서 사용되는 유용한 정보를 알아내는 공격이다.
2) 능동적 공격(active adversary)은 재전송 공격과 중간 침입자 공격에 안전해야 한다.
   - 재전송 공격(replay attack) : 재전송 공격은 합법적인 사용자가 과거에 통신했던 메시지를 공격자가 저장했다가 이후의 통신에 재전송하는 공격이다.
   - 중간 침입자 공격(man in the middle attack) : 중간 침입자 공격은 통신 선로상의 중간에 위치한 공격자가 서버와 사용자 사이에 전송되는 정보들을 불법으로 도청·변경하여 전송함으로써 합법적인 사용자들 간의 세션키를 구해내는 공격이다.
3) 오프라인 추측 공격(off-line password guessing attack)에 안전해야 한다.
   오프라인 패스워드 추측 공격은 공격자가 사용자에 의해 자주 선택되는 패스워드들에 대한 사전을 가지고 있다고 할 때 수행되는 공격이다. 공격자가

사용자들 간의 통신을 저장한 후 패스워드 사전으로부터 과거 통신에 사용된 패스워드와 일치하는 값을 비교하여 찾아낸다.

4) Denning-Sacco 공격에 안전해야 한다.
Denning-Sacco 공격은 세션키가 노출되었을 때 공격자가 그 동안 도청한 정보들을 기반으로 사용자의 패스워드에 대한 정보나 앞으로 진행될 세션에서 사용될 세션키에 대한 정보를 얻고자 하는 공격이다.

5) Perfect Forward Secrecy를 만족해야 한다.
Perfect Forward Secrecy란 공격자가 사용자의 패스워드나 서버의 장기(long-term) 패스워드 확인자를 알아냈다 할지라도 이전에 사용되었던 세션키에 대한 정보는 알아낼 수 없다는 성질이다.

3. 관련 연구

본 장에서는 2-factor OTP 생성 방식을 살펴보고, 기존 2-factor OTP 생성 방식에서 일방향 해시함수의 충돌성과 OTP 토큰에 대한 물리적 공격에 대해서 분석하고 이를 해결할 수 있는 OTP를 이용한 HMAC 기반의 3-factor 인증 구조를 제안한다.

3.1 OTP 생성방식

1) 질의-응답 방식

질의-응답 방식은 사용자가 OTP 인증 서버로부터 받은 질의 값을 직접 입력하여 OTP를 생성하므로 보안사고 발생 시 책임 소재를 명백히 가릴 수 있으며, 서로 질의 값과 응답 값을 주고받으므로 상호 인증이 가능하다[2]. 대표적인 질의-응답 방식으로는 폰뱅킹이나 인터넷 뱅킹을 이용할 때 보안 카드를 사용하는 것이다.

2) 이벤트동기화 방식

대표적인 이벤트 동기화 방식으로는 S/Key 방식이 있다. 이 방식은 국제단체인 IETF (Internet Engineer -ing Task Force) 표준 RFC1320에 소개 되었으며, MD4 메시지 다이제스트 알고리즘을 기반으로 하는 시스템이다[8].

S/Key OTP 시스템의 동작 절차는 클라이언트와 서버 측의 두 가지 측면에서 볼 수 있다. n = 4 라고 가정하면, 첫 번째로 서버는 $X_{n+1} = f(f(f(f(x))))$ 값을 저장한다. 클라이언트는 $X_n = f(f(f(f(x))))$ 값을 OTP로 생성하여 서버에게 보낸다. 서버는 $X_{n+1} = f(X_n)$을 계산하여 검증을 하게 된다. 마지막으로, 서버는 인증이 성공하면 X_{n+1}을 X_n으로 하여 다시 $X_{n+1} = f(X_n)$을 생성한다. 그리고 동기화된 n값을 1씩 증가 시킨다.

3) 시간동기화 방식

시간 동기화 방식은 서버와 OTP 토큰 간에 동기화된 시간 정보를 기준으로 특정 시간 간격은 보통 1분마다 새로운 비밀번호를 생성하는 방식이다[9].

4) 조합방식

조합방식은 새로운 OTP를 생성하기 위해 1분을 기다려야 하는 시간동기화 방식의 단점과 카운터 값의 동기화가 잘못되었을 때 재동기화를 해야 하는 이벤트동기화 방식의 단점을 보완하기 위해 시간동기화방식과 이벤트 동기화 방식을 같이 사용하는 방식이다. 조합방식은 현재 OTP를 이용한 인증에서 가장 많이 사용되고 있는 방식이다.

3.2 관련연구 분석

이 절에서는 기존에 사용되고 있는 OTP 인증 방식을 일방향 해시함수의 충돌성과 OTP 토큰에 대한 물리적 공격에 대해 분석한다.

1) 일방향 해시함수의 충돌성

일방향 해시함수 f는 $f : X \rightarrow Y$ ($|X| > |Y|$)이다. 따라서 일방향 해시함수의 충돌쌍이 존재한다. 기존 OTP 토큰은 SHA-1과 HAS-160이 사용하고 있지만, 최근 중국의 암호학자인 WANG 교수의 차분 공격에 의해서 현재 전 세계에서 보편적으로 사용하고 있는 해시 알고리즘인 SHA-1과 HAS-160의 해독 가능성이 입증 되었다[10].

2) OTP 토큰에 대한 물리적 공격

OTP 토큰은 사용자가 항상 소지 하여야 하며 인증 요청 시 반드시 가지고 있어야 한다. 만약 OTP 토큰의 분실 또는 도난발생 시 이를 취득한 악의적인 사용자는 OTP 토큰의 실제 사용자와 같은 OTP를 생성할 수 있게 된다. 따라서 2-factor 인증방식에서는 OTP토큰을 도난당하면 악의적인 사용자에 의한 사용을 막을 수 없다.

4. 제안 프로토콜

본 장에서는 기존 2-factor OTP 생성 방식에서 일방향 해시함수의 충돌성과 OTP 토큰에 대한 물리적 공격을 해결할 수 있는 새로운 인증 방식의 구조를 살펴보고, 제

안한 인증 방식을 보안 요구 사항인 재전송 공격, 일방향 해시함수의 충돌성 및 OTP 토큰 물리적 공격 등에 대해 분석하고, 보안 요구사항들을 만족하면서도 원타임-패스워드를 사용하여 효율성을 증대시킨 OTP를 이용한 HMAC 기반의 3-factor 인증 구조를 제안한다.

4.1 제안 프로토콜

본 논문에서 제안하는 인증 방식은 등록단계, OTP 생성단계, OTP 인증 단계로 구성되며 다음과 같은 순서로 진행된다.

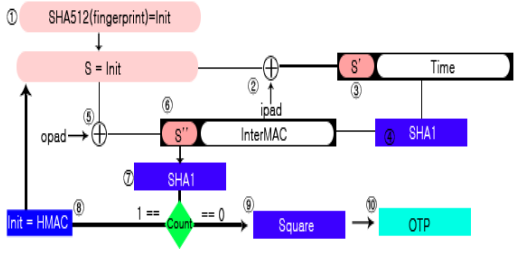
1) 등록단계

U가 S에 최초 등록 또는 재등록하고자 할 때 수행한다. 등록절차에서는 사용자에 대한 정보를 은행에 등록하는 절차로 생각할 수 있으며, 사용자의 정보, 즉 이름, 주민등록번호, 핸드폰번호, 이메일주소와 같은 정보를 은행이나 기타 업무의 필요에 따라 입력받게 되며 3-factor 인증을 위해서 지문을 추가적으로 등록 시에 입력받아야 한다. 또한 서버측은 인증과정에서 부하를 줄이기 위해서 지문에 대한 해시값을 보관하게 된다. 다음은 단계별 등록 과정을 나타낸 것이다.

Step 1. U ⇒ S : ID, fin, UPIN
Step 2. S는 데이터베이스에 U의 ID, h(fin), UPIN을 저장한다.
Step 3. S는 U에게 OTP 토큰을 발급한다.

2) OTP 생성단계

OTP 생성은 클라이언트 즉 OTP 생성기에서 수행하게 되는 과정을 뜻한다. 3-factor 인증과정에서는 지문과 시간, 카운트 값을 사용하고 HMAC 알고리즘을 사용한다. 또한 이때 지문을 해시한 값을 HMAC의 키처럼 사용할 것이다. 그리고 Square 함수를 통해 6자리의 OTP값이 생성된다. 그림 1은 사용자 측에서의 OTP 생성과정을 보여준다.



[그림 1] OTP 생성과정

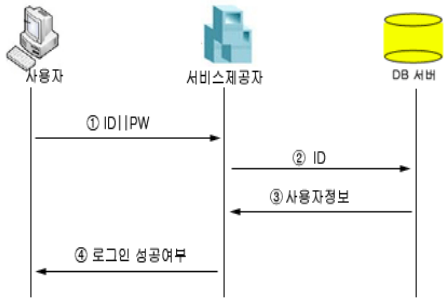
사용자 U가 서비스를 제공받기 위해 OTP를 생성하고자 할 때 OTP 토큰에 지문을 입력하고 다음과 같은 단계로 수행한다.

Step 1. hk = h(fin)를 계산한다.
Step 2. I = HMAC $_{hk}$(T)^{C}를 계산한다. 이 때 T는 S와 동기화된 시간 클럭이며, C는 S와 동기화된 계수기 값이다.
Step 3. OTP = trunc(I)를 추출한다.
Step 4. U → S : ID, OTP를 보낸다.

3) OTP 인증단계

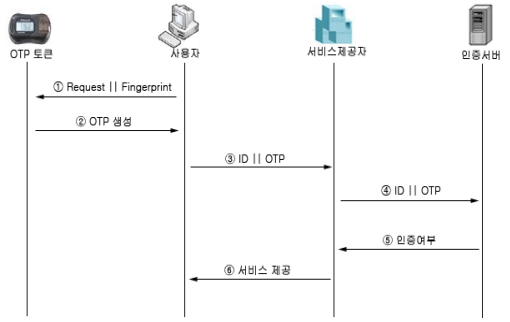
OTP 인증은 서버에서 수행하게 되는 과정이다. 서버측에서도 클라이언트 측과 마찬가지로 미리 등록된 지문을 이용하여 Square함수를 통하여 OTP 값을 생성한다. 인증실패 시에는 서버에서 카운트 값이 바뀌기 전까지 더 이상 해당 사용자에 대해 반응하지 않게 된다.

그림 2는 로그인 절차 과정을 나타낸 것이다. 로그인 과정이 끝나면 서비스 제공자가 사용자를 인증하기 위하여 그림 3과 같은 OTP 인증절차를 거친다.



[그림 2] 로그인 절차

① 사용자가 ID, 비밀번호와 같은 로그인정보를 보낸다.
② 서비스제공자는 ID에 해당하는 정보를 DB 서버에게 요청한다.
③ 서비스제공자가 보낸 ID가 존재하는지 여부를 체크하고 해당정보를 서비스제공자에게 보낸다.
④ DB서버에게 받은 사용자정보를 이용하여 ID와 PW가 정확한지 검사하고 사용자에게 로그인 성공여부를 알린다.



[그림 3] OTP 인증절차

사용자 U가 서버 S에게 생성한 OTP를 보내면 서버 S가 사용자 U에게 받은 OTP를 통해 사용자 U를 인증하고자 할 때 수행한다.

Step 1. S는 U의 ID를 이용하여 데이터베이스에서 U의 h(fin)값을 얻는다.

Step 2. I' = HMAC $_{h(fin)}(T')^{C'}$을 계산한다. 이 때 T'은 U와 동기화된 시간 클럭이며, C'는 U와 동기화된 계수기 값이다.

Step 3. OTP' = trunc(I')을 추출한다.

Step 4. U에게 받은 OTP와 S가 만든 OTP'을 비교하여 같으면 서비스를 제공하고, 같지 않으면 서비스를 제공하지 않는다.

Step 5. 인증이 성공하면 U와 S는 C = C +1을 계산하여, 계수기를 새롭게 동기화 한다. 이 때 S와 U의 ΔT를 초과하면 동기화된 계수기 C는 0으로 초기화 한다.

4.2 제안 인증방식 분석

이 절에서는 제안된 인증 방식에 대하여 보안 요구사항인 재전송 공격, 일방향 해시함수의 충돌성, OTP토큰 물리적 공격 등을 분석한다.

1) 재전송 공격

제안된 인증 방식은 기존 인증 방식과 같이 동기화된 시간 클럭 T와 동기화된 계수기 C를 사용하기 때문에 생성된 OTP는 ΔT 내에서 동기화된 계수기 C가 같을 때만 사용 가능하다. 따라서 제안한 인증방식은 재전송공격으로부터 안전하다.

2) 일방향 해시함수의 충돌성

제안한 인증방식은 HMAC을 기반으로 하여 주어진 MAC 값으로부터 사용된 키나 충돌쌍을 찾는 것은 계산적으로 어렵다. 이 때 HMAC의 해시함수로는 암호학적으로 안전한 어떠한 해시함수도 사용가능하다.

3) OTP 토큰에 대한 물리적 공격

제안한 인증방식은 사용자의 지문 또는 생체정보를 이용하여 OTP를 생성한다. 만약 악의적인 사용자가 다른 사용자의 OTP 토큰을 얻는다고 해도, 지문이나 생체정보를 완벽하게 흉내 낼 수 없기 때문에 OTP 토큰의 주인과 같은 OTP를 생성할 수 없다. 따라서 제안한 방식은 물리적 공격을 해결할 수 있다.

5. 안전성 및 효율성 분석

본 장에서는 제안한 프로토콜을 일반패스워드 사용, S/Key방식과 제안한 OTP를 이용한 방식들을 비교 분석하여 안전성 및 효율성을 검증한다.

제안한 프로토콜을 성능적 측면과 기능적 측면에서 분석하고자 한다. 먼저 제안한 프로토콜은 지수 연산이나 암호화 연산과 같은 현대 컴퓨팅 기술에 영향을 줄 정도로 비용부담이 큰 연산이 없으므로 성능적 측면에 대한 분석은 의미가 없다. 기능적 측면에서 볼 때 제안한 프로토콜은 사용자의 생체 정보와 HMAC을 사용하여 OTP를 생성하기 때문에 표 2와 같이 제안한 프로토콜에 대한 기능성을 일방향 해시함수의 충돌성과 OTP토큰에 대한 물리적 공격에 대해 일반 패스워드방식, S/KEY 시스템보다 더 효율적임을 보여주고 있다.

[표 2] 효율성 비교분석

	재전송 공격	해시함수 충돌성	물리적 공격
일반패스워드	×	×	×
S/KEY	○	△	×
제안 인증방식	○	○	○

× : 안전하지 않음 △ : 부분적으로 안전함 ○ : 안전함

또한 OTP를 이용한 HMAC 기반의 3-factor 인증에 대한 패스워드 추측공격, 서버 비밀키 추측공격, 재전송공격 및 위장공격과 같은 여러 가지 공격에 대하여 안전성을 분석한다.

1) 도청 공격

제안한 프로토콜 상에서 전송되는 메시지들이 추측 불가능한 HMAC에 의해서 생성된 OTP값이기 때문에 단순

한 도청만으로는 유용한 정보를 얻을 수가 없다. 따라서 제안한 인증 구조는 도청공격에 안전하다.

2) 패스워드 추측공격

패스워드 추측공격은 오라인과 오프라인 패스워드 추측공격으로 나눌 수 있다. 온라인 패스워드 추측공격은 사용자 U에게 받은 OTP와 서버 S가 만든 OTP'을 비교하여 같으면 서비스를 제공하고, 같지 않으면 서비스를 제공하지 않기 때문에 온라인 패스워드추측공격에 안전하다. 본 논문에서 제안한 프로토콜에서 패스워드를 유추하는 것은 해시함수의 일방향성 때문에 불가능하다.

3) 서버의 비밀키 추측 공격

서버의 비밀키 추측공격 또한 패스워드 추측공격에서와 마찬가지로 공격자가 합법적인 사용자에 대하여 도청한 메시지들로부터 서버의 비밀키에 관한 정보를 유추하는 것이다. 그러나 이들 정보로부터 서버의 비밀키를 유추하는 것은 해시함수의 일방향성 때문에 불가능하다. 따라서 제안한 인증 구조는 서버의 비밀키 공격에 안전하다.

4) 재전송 공격

만약 공격자가 이전 세션에서 획득한 메시지를 가지고 사용자 A로 가장하여 서버에게 그 메시지를 전송하고 사용자 B가 사용자 A에게 보내는 메시지를 가로챘다 하더라도 공격자는 이전 OTP값을 계산할 수 없다. 왜냐하면 등록단계에서 사용자가 서버에게 제공한 ID, fin, UPIN 값을 알 수 없기 때문이다. 따라서 제안된 인증 방식은 기존 인증 방식과 같이 동기화된 시간 클럭 T와 동기화된 계수기 C를 사용하기 때문에 생성된 OTP는 ΔT 내에서 동기화된 계수기 C가 같을 때만 사용 가능하다. 따라서 제안한 인증방식은 재전송 공격으로부터 안전하다.

5) 위장공격

적법한 사용자나 공격자가 타인을 위장하기 위해서는 위장하고자하는 사용자의 아이디와 패스워드를 알아야 한다. 사용자의 공개된 정보이기 때문에 쉽게 알 수 있지만, 사용자의 패스워드는 $I = HMAC_{h(fin)}(T)^C$를 계산하고 OTP' = trunc(I')을 추출하여야 하기 때문에 해시함수의 일방향성으로 인하여 추측하기 어렵다. 따라서 위장공격은 불가능하다.

제안한 프로토콜에 대한 효율성 분석은 표 3에서 나타난 것과 같이 일반 패스워드 방식과 동일한 1회의 초기화 과정이 필요하며, 사용 횟수에 제한 없이 사용할 수 있다는 장점이 있다. 또한 해시연산 횟수도 4회로 고정됨으로써 오버헤드에 대한 부담도 없음을 알 수 있다. S/Key 시스템은 일련번호를 사용하여 OTP를 생성하므로 사용 횟수가 초기화 과정에서 설정한 n회로 제한되기 때문에 설정한 범위를 초과 할 경우 다시 초기화 과정을 거치게 되는 번거로움이 있으며 초기화 과정에서의 비밀 패스워드 노출에 따른 위험이 존재한다. 제안 프로토콜에서는 일련번호를 사용하지 않고 U와 S는 C = C + 1을 계산하여, 계수기를 새롭게 동기화 한다. 이 때 서버 S와 사용자 U의 ΔT를 초과하면 동기화된 계수기 C는 0으로 초기화 한다.

[표 3] 효율성 비교분석

	일반패스워드	S/KEY	제안메커니즘
사용회수	제한 없음	n회	제한 없음
해쉬연산	없음	n-1회	4회
메시지 전송 회수	1회	3회	2회
초기화회수	1회	다수	1회

6. 결론

안전한 온라인 서비스를 제공하기 위해서 일반적인 ID/Password 방식의 정적인 패스워드를 이용하는 것이 아니라 매번 새로운 패스워드를 생성하는 OTP를 이용하게 되었다. 현재 OTP 토큰을 이용한 2-factor OTP 생성방식이 주로 이용되고 있다. 그러나 이 2-factor 인증방식은 OTP 토큰의 분실 또는 도난과 같은 물리적 공격에 대한 방어책을 제시하지 못한다. 이러한 인증 방식은 일방향 해시함수의 충돌성과 OTP 토큰에 대한 물리적 공격으로부터 안전하지 않다. 따라서 본 논문에서는 이러한 문제점을 해결하기 위해 HMAC 기반의 인증방식을 제안하였다. 제안된 인증 방식은 3-factor 인증방식으로서 OTP를 생성하기 위해 사용자의 생체 정보를 이용한다. 따라서 기존 인증 방식이 가지고 있던 다양한 문제점을 해결할 수 있으며, 전자상거래, 인터넷 뱅킹, 게임, 음악 등과 같은 다양한 응용 분야에서 활용할 수 있을 것으로 본다.

참고문헌

[1] 금융감독원, “전자상거래 안전성 강화 종합대책,” 9월, 2005.

[2] 백미연, “전자상거래의 보안 강화 방법 및 OTP 이용 현황,” 지급결제와 정보기술, pp. 71-100, 2006.
[3] 박중길, 장태주, 박봉주, 류재철, “시간을 이용한 효율적인 일회용 패스워드 알고리즘,” 한국정보처리학회 논문지 C, 8(4), 2001.
[4] N. Haller, "A One Time Password Standard," IETF RFC 1938, 1996.
[5] 금융보안연구원, “금융보안 주간 정보,” 2006.
[6] M. Bellare, D. Jablon, H. Krawczyk, P. Mackenzie, P. Rogaway, R. Swaminathan and T. Wu, "Proposal for P1363 study group on password-based authenticated key exchange methods," 2000.
[7] 박왕석, 정종필, 박창섭, 이동훈, “패스워드를 이용한 인증 프로토콜에 대한 고찰”, 통신정보보호학회 학술지 제9권 제4호, 1999.
[8] 서승현, 강우진, “OTP 기술현황 및 국내 금융권 OTP 도입사례,” 한국정보보호학회, 6월, 2007.
[9] 류연호, “OTP 개념을 이용한 사용자-인증 서버의 상호 인증 모델,” NuriMedia, 2005.
[10] X. Wang, Y. L Yin, and H. Yu, "Finding collisions in the full SHA-1," Advances in Cryptology Crypto'05, Lecture Notes in Computer Science 3621, Springer-Verlag, pp. 17-36, 2005.

신 승 수(Seung-Soo Shin) **[정회원]**

- 1988년 2월 : 충북대학교 수학과 (이학사)
- 1993년 2월 : 충북대학교 수학과 (이학석사)
- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

<관심분야>
암호프로토콜, 무선 PKI, 네트워크 보안, USN.

한 군 희(Kun-Hee Han) **[종신회원]**

- 2008년 8월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
RFID, 경영정보컨설팅