韓國컴퓨터情報學會 論文誌
第14卷 第6號, 2009. 6.

2009-14-6-1-4

HMAC 기반의 일회용 패스워드를 이용한 3-Factor 인증

김 지 홍*, 오 세 웅**

3-Factor Authentication Using HMAC-based One-Time Password

Jihong Kim*, Seiwoong Oh**

요 약

최근 컴퓨터 통신 기술이 발달함에 따라 대부분의 정보 서비스가 온라인으로 이루어지고 있으며, 온라인 정보들의 가치 또한 높아지고 있다. 그러나 정보 기술의 발달과 더불어 이를 공격하기 위한 다양한 공격 기법들도 생기고 있으며, 이러한 공격으로부터 안정한 온라인 서비스를 제공하기 위해서 일반적인 ID/Password 방식의 정적인 Password를 이용하는 것이 아니라 매번 새로운 Password를 생성하는 OTP를 이용하게 되었다. 현재는 OTP 토큰을 이용한 2-Factor OTP 생성 방식이 주로 이용되고 있다. 그러나 2-Factor 인증 방식은 OTP 토큰의 분실 또는 도난과 같은 물리적 공격에 대한 방어책을 제시하지 못한다. 본 논문에서는 이와 같은 문제를 해결하기 위해 HMAC을 이용한 3-Factor 인증 방식을 제안하며, 이와 함께 제안한 인증 방식에 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.

▸ Keyword : 일회용 패스워드(One-Time Password), 인증(Authentication), 인터넷 피싱(Internet Pishing), 해시 메시지 인증 부호(Hash Message Authentication Code, HMAC)

• 제1저자 : 김지홍 교신저자 : 오세웅
• 투고일 : 2009. 06. 11, 심사일 : 2009. 06. 11, 게재확정일 : 2009. 06. 18.
* 동의대학교 영상정보공학과 **동의대학교 게임공학과

Ⅰ. 서 론

최근 인터넷과 같은 통신 기술이 급속도로 발전함에 따라 많은 정보 서비스들이 온라인을 통해서 이루어지고 있다. 그러나 이전에 오프라인 상에서 이루어지던 은행 거래와 상거래가 인터넷 뱅킹과 전자 상거래와 같이 온라인 상에서 이루어지면서 많은 문제점들이 노출되고 있다. 인터넷은 개방형 네트워크이기 때문에 인터넷 뱅킹이나 전자 상거래는 편리성 못지 않게 공격자에 의한 시스템 침입, 불법 해킹, 인터넷 피싱 등의 피해에 대해 노출되어 있다. 예를 들어 2005년 5월 인터넷 뱅킹 사고, 2007년 1월 대형 은행 고객 정보 유출, 2007년 2월 공인 인증서 유출로 인한 은행 불법 인출 사건 등과 같은 불법 피해 사례가 늘고 있다. 이러한 사고로 인해 막대한 금전적 손해 뿐만 아니라 이로 인해 겪는 정신적 피해도 증가하여 산업자원부, 정보통신부, 금융감독위원회, 금융감독원은 공동으로 "전자 금융 거래 안전성 강화 종합 대책"을 수립하였다[1].

개인 정보 유출로 인한 전자 금융 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(One-Time Password, OTP) 기반 인증 기법이 인터넷 뱅킹, 전자 상거래에 사용되어 왔으며, 최근에는 게임, 음악, 동영상등 다양한 분야에서 활용되고 있다. 그러나 질의-응답방식, 이벤트 동기화 방식, 시간 동기화, 조합 방식과 같은 기존의 OTP 인증 방식은 일방향 해시함수의 충돌성과 OTP 토큰에 대한 물리적 공격에 대해 취약하다.

본 논문에서는 이러한 기존 OTP 인증 방식의 문제점을 해결하기 위해 HMAC 기반 3-Factor OTP인증 방식을 제안한다. 제안된 프로토콜은 OTP를 생성하기 위해 생체 정보를 이용하여 OTP 토큰에 대한 물리적 공격을 해결하며, HMAC을 기반으로 하여 일방향 해시함수의 충돌성에 대한 문제점에 대해 더 효율적이다.

본 논문의 구성은 다음과 같다. II장에서는 관련 연구로서 질의-응답방식, 이벤트 동기화 방식, 시간 동기화 방식, 조합 방식에 대해 살펴보고, 이들의 문제점을 분석한다. III장에서는 이러한 문제점을 해결하기 위한 새로운 OTP 인증 프로토콜을 제안하고, 그 안전성을 평가한다. IV장에서는 기존 OTP 인증 프로토콜과 본 논문에서 제안한 프로토콜을 비교 분석하며, V장의 결론으로 논문을 맺는다.

Ⅱ. 관련 연구

이 장에서는 기존의 OTP 생성 방식을 살펴보고, 기존 OTP 생성 방식의 문제점을 분석한다.

1. OTP 생성 방식

OTP 인증이란 매 세션마다 변하는 동적 패스워드를 이용하여 개체를 인증하는 방식을 의미한다[4]. 이 방식에서는 개체 인증을 위한 요소로서 알고 있는 것(지식 기반), 소유하고 있는 것(소유 기반), 태생적으로 타고난 것(생체 기반)과 같은 3가지 요소를 주로 이용한다. 기존 OTP 인증 방식은 지식-소유기반의 2-Factor 인증 방식을 사용하고 있으며, 입력값에 따라 질의-응답 방식, 이벤트 동기화 방식, 시간 동기화 방식, 조합 방식으로 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].

1.1 질의-응답 방식

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

1.2 이벤트 동기화 방식

대표적인 이벤트 동기화 방식으로는 S/Key 방식이 있다. 이 방식은 국제 단체인 IETF(Internet Engineering Task Force) 표준 RFC1320에 소개되었으며, MD4 메시지 다이제스트 알고리즘을 기반으로 하는 시스템이다[6].

S/Key OTP 시스템의 동작 절차는 클라이언트와 서버 측의 두 가지 측면에서 볼 수 있다. n = 4 라고 가정하면, 첫 번째로 서버는 $X_{n+1} = f(f(f(f(f(x)))))$ 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 생

성한다. 그리고 동기화된 n 값을 1씩 증가시킨다.

1.3 시간 동기화 방식

시간 동기화 방식은 서버와 OTP 토큰 간에 동기화된 시간 정보를 기준으로 특정 시간 간격(보통 1분)마다 새로운 비밀번호를 생성하는 방식이다[7].

1.4 조합 방식

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

2. 관련 연구 분석

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

2.1 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 입증되었다[8].

2.2 OTP 토큰에 대한 물리적 공격

OTP 토큰은 사용자가 항상 소지하여야 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 인증 방식에서는 OTP 토큰을 도난당하면 악의적인 사용자에 의한 사용을 막을 수 없다.

III. 제안 프로토콜

이 장에서는 본 논문에서 제안한 인증 방식의 구조를 살펴보고, 제안한 인증 방식을 재전송 공격, 일방향 해시함수의 충돌성, OTP 토큰 물리적 공격 등에 대해 분석한다. 본 논문에서는 표 1과 같은 표기법을 사용한다.

표 1. 표기법
Table 1. Notations

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( )	해시함수
HMACK( )	HMAC 함수
trunc( )	6자리 OTP값 추출함수

1. 제안 프로토콜의 구조

본 논문에서 제안하는 인증 방식은 등록 단계, OTP 생성 단계, OTP 인증 단계로 구성되며, 동작 과정은 그림 1과 같다.

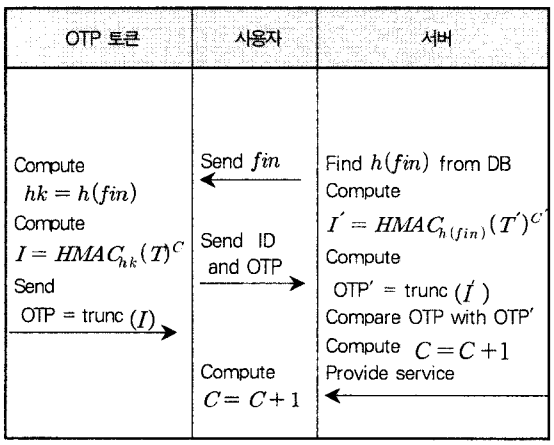

그림 1. 제안 프로토콜
Fig. 1. Proposed protocol

1.1 등록 단계

U가 S에 최초 등록 또는 재등록하고자 할 때 수행한다.

Step 1. U ⇒ S : ID, fin, UPIN

Step 2. S는 데이터베이스에 U의 ID, h(fin), UPIN을

저장한다.

Step 3. S는 U에게 OTP 토큰을 발급한다.

1.2 OTP 생성 단계

U가 서비스를 제공받기 위해 OTP를 생성하고자 할 때 OTP토큰에 지문을 입력하면 다음과 같이 수행한다.

Step 1. $hk = h(\text{fin})$을 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, OTP

1.3 OTP 인증 단계

U가 S에게 생성한 OTP를 보내면 S가 U로부터 받은 OTP를 통해 U를 인증하고자 할 때 수행한다.

Step 1. S는 U의 ID를 이용하여 데이터베이스에서 U의 $h(\text{fin})$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. U로부터 받은 OTP와 S가 만든 OTP'을 비교하여 서로 동일하면 서비스를 제공하고, 동일하지 않으면 서비스를 제공하지 않는다.

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

2. 제안 인증 방식 분석

이 절에서는 제안된 인증 방식에 대한 재전송 공격, 일방향 해시함수의 충돌성, OTP 토큰 물리적 공격 등을 분석한다.

2.1 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 인증 방식은 재전송 공격으로부터 안전하다.

2.2 일방향 해시함수의 충돌성

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

2.3 OTP 토큰에 대한 물리적 공격

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

IV. 안전성 및 효율성 분석

본 장에서는 제안한 메커니즘을 기존의 OPT를 이용한 방식들과 비교하여 안전성 및 효율성을 검증한다. 제안된 인증 방식은 지수 연산이나 암호화 연산과 같은 현대 컴퓨팅 기술에 영향을 줄 정도로 비용 부담이 큰 연산이 없으므로 성능적 측면에 대한 분석은 의미가 없다. 기능적 측면에서 볼 때 제안된 프로토콜은 사용자의 생체 정보와 HMAC을 사용하여 OTP를 생성하기 때문에, 표 2와 같이 제안한 프로콜에 대한 효율성을 일방향 해시함수의 충돌성과 OTP토큰에 대한 물리적 공격에 대해 일반 패스워드 방식, S/KEY 시스템보다 더 효율적임을 보여주고 있다.

표 2. 기능성 비교분석
Table 2. Performance Comparison

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

× : 안전하지 않음 △ : 부분적으로 안전함 ○ : 안전함

1. 안전성 분석

1.1 패스워드 추측 공격

패스워드 추측 공격은 온라인과 오프라인 패스워드 추측 공격으로 나눌 수 있다. 온라인 패스워드 추측 공격은 U에게 받은 OTP와 S가 만든 OTP'을 비교하여 같으면 서비스를 제

공하고, 같지 않으면 서비스를 제공하지 않기 때문에 온라인 패스워드 추측 공격에 안전하다. 본 논문에서 제안한 프로토콜에서 패스워드를 유추하는 것은 해시함수의 일방향성 때문에 불가능하다.

1.2 서버의 비밀 키 추측 공격

서버의 비밀 키 추측 공격 또한 패스워드 추측 공격에서와 마찬가지로 공격자가 합법적인 사용자에 대하여 도청한 메시지들로부터 서버의 비밀 키에 관한 정보를 유추하는 것이다. 그러나 이들 정보로부터 서버의 비밀 키를 유추하는 것은 해시함수의 일방향성 때문에 불가능하다.

1.3 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 OPT값을 계산할 수 없다. 왜냐하면 등록 단계에서 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 인증 방식은 재전송 공격으로부터 안전하다.

1.4 위장 공격

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

2. 효율성 분석

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

표 3. 효율성 비교 분석
Table 3. Efficiency Comparison

	일반패스워드	S/KEY	제안메커니즘
사용 횟수	제한 없음	n회	제한 없음
해시 연산	없음	n-1회	4회
메시지 전송 횟수	1회	3회	2회
초기화 횟수	1회	다수	1회

V. 결 론

기존 OTP 인증 방식은 지식-소유 기반의 2-Factor 인증 방식을 사용하고 있으며, 이러한 인증 방식은 일방향 해시함수의 충돌성과 OTP 토큰에 대한 물리적 공격으로부터 안전하지 않다. 따라서 본 논문에서는 이러한 문제점을 해결하기 위해 HMAC 기반의 인증 방식을 제안하였다. 제안된 인증 방식은 3-Factor 인증 방식으로서 OTP를 생성하기 위해 사용자의 생체 정보를 이용한다. 따라서 기존 인증 방식이 가지고 있던 다양한 문제점을 해결할 수 있으며, 전자 상거래, 인터넷 뱅킹, 게임, 음악 등과 같은 다양한 응용 분야에서 활용할 수 있다.

참고문헌

[1] 금융감독원, "*전자상거래 안전성 강화 종합대책*," 2005년.
[2] 백미연, "전자상거래의 보안 강화 방법 및 OTP 이용 현황," 지급결제와 정보기술, 71-100쪽, 2006년.
[3] 박중길, 장태주, 박봉주, 류재철, "시간을 이용한 효율적인 일회용 패스워드 알고리즘," 한국정보처리학회논문지 Part C, 제 8(C)권, 제 4호, 373-378쪽, 2001년 8월.
[4] N. Haller, "A One Time Password Standard," IETF RFC 1938, 1996.

[5] 금융보안연구원, "*금융보안 추간 정보*," 2006년.
[6] 서승현, 강우진, "OTP 기술현황 및 국내 금융권 OTP 도입사례," 한국정보보호학회, 제 17권 제3호, 18-25쪽, 2007년 6월.
[7] 류연호, "*OTP 개념을 이용한 사용자-인증 서버의 상호 인증 모델*," NuriMedia, 2005년.
[8] 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.

저 자 소 개

김 지 홍(Jihong Kim)

1988년: 경북대학교 대학원 전자공학과 졸업(석사)
1996년: 포스텍 대학원 전자전기공학과 졸업(박사)
현 재: 동의대학교 영상정보공학과 부교수
관심분야: 영상처리, 컴퓨터 네트워크 등

오세웅(Seiwoong Oh)

1987년: 한양대학교 대학원 전자공학과 졸업(석사)
1998년: 일본 오사카대학교 정보공학과 졸업(박사)
현 재: 동의대학교 게임공학과 부교수
관심분야: 온라인 게임, 정보보호, 유비쿼터스 컴퓨팅 등