워터마킹 기반 모바일 3-Factor OTP 인증

최종석*, 신승수*, 한군희**
*동명대학교 정보보호학과
**백석대학교 정보통신학부
e-mail:shinss@tu.ac.kr

3-Factor OTP Authentication based on Water-Marking

Jong-Seok Choi*, Seung-Soo Shin*, Kun-Hee Han**
*Dept of Information Security, TongMyoung University
**Division of Information & Communication Engineering, Baekseok University

요 약

정보통신기술의 발달로 온라인으로 많은 서비스가 이루어지면서 온라인을 통해서 송·수신 되는 정보들의 가치도 높아지고 있다. 현재 전자금융거래의 보안을 향상시키기 위해서 금융기관은 OTP 인증을 사용한다. OTP 인증은 패스워드 기반의 인증기술이며, OTP 토큰을 이용하여 OTP를 생성한다. 이러한 인증은 일방향 해시함수의 충돌성, OTP 토큰에 대한 물리적 공격, OTP 토큰의 전력소모에 따른 동기화 문제를 가지고 있다. 따라서 본 논문에서는 모바일 기기를 이용한 워터마킹 기반 3-Factor OTP 인증을 제안한다. 제안한 인증에서는 OTP를 생성하기 위해 사용자의 생체정보를 사용하며, 서비스 제공자는 사용자의 생체정보에 서버의 비밀정보를 워터마킹 기법을 이용하여 숨긴다. 워터마킹된 생체정보를 사용자의 모바일 기기의 저장하고, 이 정보를 통해 사용자는 생체정보를 인증하고, OTP를 생성한다. 제안한 인증기술은 OTP토큰을 휴대해야 하는 불편 대신에 대부분 성인이 휴대한 휴대폰과 같은 모바일 기기를 통해 OTP를 생성하고 인증을 할 수 있으며, 생체정보를 이용함으로써 다른 사용자가 OTP를 생성할 수 없도록 한다. 이러한 기법은 안전한 인증을 요구하는 모든 온라인 서비스에서 사용될 수 있다.

1. 서론

최근 컴퓨터와 정보통신기술의 급속한 발달로 온라인으로 많은 서비스들이 이루어지면서 온라인을 통해서 송·수신 되는 정보들의 가치도 더욱 높아지고 있다. 특히 인터넷 뱅킹과 전자상거래와 같은 전자금융거래에 대한 정보의 보안수준을 향상하기 위해 인증이 필요하다. 그래서 금융기관은 전자금융거래의 안전성을 강화하기 위한 수단으로 일회용패스워드(OTP)를 도입하여 사용하고 있다. OTP는 인증 시마다 새로운 비밀번호를 생성하고 한 번 사용한 비밀번호를 다시 사용하지 않으며, 인터넷에서 주로 사용되는 정적인 Password와는 달리 동적인 Password이다. 따라서 스니핑이나 스푸핑과 같은 공격을 당해도 그 OTP는 다시는 사용되지 않기 때문에 이와 같은 문제를 해결할 수 있다.

여러 금융기관에서는 OTP 토큰을 이용한 2-Factor 인증을 기반으로 하여 OTP 인증 서비스가 시행되고 있다. 그러나 OTP 토큰 분실 및 도난에 따른 여러 가지 문제점이 제기되고 있다.

이러한 문제점을 해결하기 위해서 생체정보를 이용한 3-Factor OTP 인증을 생각할 수 있다. 이러한 생체인식 기술을 사용하기 위해서는 몇 가지 제약된 환경이 필요하며, 생체정보를 보호할 필요가 있다.

따라서 본 논문에서는 모바일 기기를 이용한 워터마킹 기반 3-Factor OTP 인증을 제안한다.

워터마킹 기법은 데이터를 은닉하는 기법으로 Embedding 알고리즘이 알려지지 않는다면, 은닉된

데이터의 안전성을 보장할 수 있다[1]. 워터마킹 기법과 지문인식 기술의 효율적인 처리를 위해서 필요한 제약적인 환경을 위해서 우리나라 인구 4500만명 중 4000만명이 소유[2]하고 있는 핸드폰과 같은 모바일 기기를 이용할 수 있다.

본 논문은 2장에서 관련연구를 살펴보고, 관련연구에 대한 분석을 한다. 3장에서는 워터마킹 기반 모바일 3-Factor OTP 생성 방식을 제안하고, 제안한 구조를 분석한다. 마지막 4장에서 결론을 맺는다.

2. 관련연구 및 분석

관련연구로 인증과 OTP 생성방식에 대해서 살펴보고, 기존에 OTP 인증의 취약한 해시함수의 충돌성, OTP 토큰에 대한 물리적 공격과 같은 문제점에 대해서 분석한다.

2.1 개체 인증

개체 인증(entity authentication)이란 한 개체가 다른 한 개체의 신원을 증명할 수 있도록 설계된 기술을 말한다.[3, 4] 개체 인증을 하기 위해서는 다음과 같은 세 가지 정보를 사용할 수 있다.

(가) 알고 있는 것(something known)

주장자만 알고 있는 비밀로서 검증자에 의해 검증될 수 있다. 예를 들면 패스워드, PIN, 비밀키 등이 있다.

(나) 소유하고 있는 것(something possessed)

주장자의 신원을 증명할 수 있는 것을 말한다. 예를 들면 운전 면허증, 신분증, 여권, 신용카드, 현금 인출용 카드 등이 있다.

(다) 태생적으로 가지고 있는 것(something inherent) 주장자의 타고난 특성을 말한다. 예를 들면 지문, 음성, 홍채 패턴 등이 있다.

2.2 OTP(One-Time Password)

일반적인 패스워드는 정적인 패스워드로 네트워크 도청으로 인해 패스워드를 알아냈을 경우 불법적으로 재사용할 위험이 있다. OTP는 필요에 따라 새로운 패스워드를 생성하기 때문에 네트워크 도청을 통하여 패스워드를 알아내더라도 더 이상 사용할 수 없으므로 이러한 위험을 방지 할 수 있다. 따라서 OTP는 정적인 패스워드 사용에 따른 위험을 해결하고 개인정보 유출에 따른 사용자 인증을 강화하기 위해 도입 되었다. OTP는 동적인 패스워드로 사용하기 위해서는 별도의 매체가 요구된다. 이 매체는 OTP를 생성할 수 있는 기능을 가지는 장치로 OTP 토큰이라고 한다. OTP는 OTP 생성매체에 의해 필요한 시점에 발생되고 매번 새로운 번호를 생성한다.

2.2.1 OTP 생성 방식

OTP 생성 방식에는 입력 값에 따라 질의-응답방식, 시간동기화 방식, 이벤트동기화 방식, 조합방식으로 나누어진다.

(가) 질의-응답 방식

질의-응답 방식은 사용자가 서버가 제시한 질의 값을 OTP 토큰에 입력해 응답 값을 얻고 그 응답의 해당 값을 서버에 전송하여 사용자를 인증하는 방식이다[5]. 질의-응답 방식은 OTP 토큰과 인증서버 간에 동기화해야할 기준 정보가 없기 때문에, 동기화할 필요가 없으며, 사용자와 서버 간에 상호 인증을 제공하는 방식으로 쉽게 확장이 가능하다는 장점을 가진다. 그러나 사용자가 직접 질의 값을 OTP 토큰에 입력해야한다는 불편이 있으며, 인증서버도 해당 사용자의 질의 값을 관리해야 하는 부담이 있다.

(나) 시간동기화 방식

시간 동기화 방식은 서버와 OTP 토큰 간에 동기화된 시간 정보를 기준으로 특정 시간간격(보통 1분)마다 새로운 비밀번호를 생성하는 방식이다.[6]

(다) S/Key 방식

S/Key OTP 시스템에 대한 상세한 설명은 국제단체인 IETF(Internet Engineering Task Force) 표준 RFC1320에 소개 되었다. 이 방식은 MD4 메시지 다이제스트 알고리즘을 기반으로 하는 시스템이다.[7]OTP는 일방향 해시함수를 여러 번 적용함으로 계속해서 생성되어진다.

2.3 관련연구 분석

관련연구 분석으로 기존의 OTP 인증방식이 취약한 일방향 해시함수의 충돌성과 OTP 토큰의 물리적 공격에 대해 분석한다.

(가) 일방향 해시함수의 충돌성

기존의 OTP 생성알고리즘은 일방향 해시함수를

사용한다. 이때 일방향 해시함수 f는 $f: X \rightarrow Y$ ($|X| > |Y|$)이다. 따라서 우리는 비둘기집의 원리를 생각해볼 수 있다. 즉, n개의 집에 $2n$마리의 비둘기가 모두 들어가기 위해서는 평균 2마리의 비둘기가 1개의 집에 들어가야 한다. 일방향 해시함수는 이와 같은 성질을 가지는데 이 성질을 일방향 해시함수의 충돌성[4]이라고 한다.

(나) OTP 토큰의 물리적 공격

만약 OTP 토큰을 분실 또는 도난당한다면 OTP 토큰을 취득한 사람은 OTP 토큰의 주인과 같은 OTP를 생성할 수 있게 된다. 서버 측에서는 이 OTP가 인증자와 같은 것으로 인증하게 되고 커다란 문제점이 생기게 된다.

(다)OTP 토큰의 전력소모

OTP 토큰과 서비스 제공자 간에는 타임클럭과 같은 동기화된 값이 필요하다. 이 값은 일정시간에 따라 OTP 토큰에서 변하게 되지만, 전력소모 또는 기계적 오차에 의해서 허용 윈도우의 범위를 벗어날 수도 있다.

3. 워터마킹 기반 모바일 3-Factor OTP

최근 모바일 서비스에 대한 연구가 활발하게 진행중이다. 따라서 본 논문에서는 OTP 토큰을 이용한 OTP 인증의 취약점을 보완하기 위해 모바일 기기를 이용한 워터마킹 기반 3-Factor OTP 인증 방식을 제안한다. 본 논문에서는 [표 1]과 같은 표기법을 사용한다.

[표 1] 표기법

기호	설명
U	사용자
S	서비스 제공자 또는 서버
x	S의 비밀정보
PIN	모바일 기기 또는 고유번호
ID	사용자 식별번호
fin	생체정보
TH	생체정보를 검증하기 위한 값
Wx()	x를 이용한 Embedding 함수
trunc()	OTP 추출함수
pos()	위치추출함수
extp()	p위치의 일정길이 비트추출
T	동기화된 타임클럭
C	동기화된 계수기
->	공개된 채널
=>	안전한 채널

3.1 제안한 인증구조

제안한 인증구조는 등록, 생성, 인증, 동기화와 같이 4과정으로 이루어진다.

3.1.1 등록

Step 1. U => S : ID, PIN, fin

사용자는 안전한 채널을 통해서 자신의 ID, PIN, 생체정보를 S에게 등록한다.

Step 2. S => U : Wx(fin), T, C, pos(), extp(), trunc()

S는 동기화된 클럭 T, C와 워터마킹 기법을 적용한 생체정보 w(fin)을 U의 모바일 기기에 저장해준다.

이 때 U는 워터마킹 Embedding 함수 Wx()에 대해서 알 수 없으므로 Wx(fin)으로부터 S의 비밀정보 x를 추출할 수 없다.

3.1.2 OTP 생성

Step 1. U -> PIN : fin

U는 PIN에 지문인식을 한다.

Step 2. PIN은 Wx(fin)와 fin을 비교하여 검증한다. 이 때 PIN은 TH를 이용하여 Wx(fin)과 fin의 동일여부를 검증한다.

Step 3. p = pos(T, C)를 계산한다. 이때 p는 생체정보의 비트길이 내의 위치를 가르치기 위한 임의의 위치 값이다.

Step 4. t = extp(Wx(fin))을 계산한다. 워터마킹이 적용된 생체정보의 p위치부터 20비트를 추출한다.

Step 5. OTP = trunc(t)를 계산한다.

일반적으로 워터마킹을 할 때 상위비트를 바꾸면 비가시성을 유지하기 어렵기 때문에 MSB에 워터마킹 기법을 사용하지는 않는다. 지문과 같은 생체정보는 흑백으로 표현될 수 있으며 Wx(fin)에서 TH보다 큰 값을 생체정보의 실제 값으로 하여 지문에 대한 인증을 할 수 있다.

3.1.3 OTP 인증

Step 1. U -> S : ID, OTP

U는 공개된 채널을 통해서 OTP 값을 전송한다.

Step 2. S는 OTP 생성과정과 같이 계산을 통해 U의 OTP를 생성하여 검증한다.

3.1.4 동기화과정

Step 1. U와 S는 각각 pos(T, C)로 생성된 값을 다음 OTP 인증을 위한 C 값으로 사용한다. T값은 국제표준 또는 국내표준의 타임클럭에 따른다.
Step 2. 각 시간의 30초와 0초를 기준으로 C값을 0으로 초기화 한다.

3.2 제안한 구조 분석

본 논문에서 제안한 모바일 기기를 이용한 워터마킹 기반 3-Factor OTP 인증을 OTP 토큰의 물리적 공격과 전력소모, 전방향 안전성, 서버 비밀정보 추측 공격에 대해서 분석한다.

3.2.1 OTP 토큰의 물리적 공격

본 논문에서 제안한 구조는 OTP토큰 대신 핸드폰과 같은 모바일 기기를 사용한다. 정당한 사용자가 모바일 기기를 분실 또는 도난당할 수 있다. 그러나 정당한 사용자가 아닌 악의적인 사용자가 모바일 기기를 획득한다고 해도 정당한 사용자의 지문과 같은 생체정보를 흉내낼 수 없다면 인증을 통과 할 수 없다.

3.2.2 OTP 토큰의 전력소모

제안한 구조에서 사용하는 모바일 구조는 기존의 OTP 토큰과는 달리 반영구적으로 사용될 수 있다. 사용자의 부주의로 모바일 기기의 전원이 꺼진다해도 동기화 클럭 C는 매시간 30초와 0초에 0으로 초기화되며, T는 표준 클럭을 따르므로 모바일 기기 자체적으로 동기화를 되찾을 수 있다.

4. 결론

최근 컴퓨터통신 기술의 발달로 전자상거래와 같은 온라인 서비스가 상용화 되고 있다. 이러한 온라인 서비스를 안전하게 제공하기 위한 방법으로 많은 전자금융기관들은 OTP를 이용하고 있다. 그러나 기존의 OTP 토큰을 이용한 OTP 생성방식은 OTP 토큰에 대한 물리적 공격과 전력소모에 따른 동기화 재설정에 대한 문제점을 가지고 있다. 따라서 본 논문에서는 이러한 문제점을 해결하기 위해 모바일 기기를 이용한 워터마킹 기반 3-Factor OTP 인증 방식을 제안한다. 제안한 인증구조는 생체정보를 이용하여 모바일 기기를 분실한다고 해도 다른 사람이 자신의 OTP를 생성하지 못하도록 막을 수 있으며, 지문인식 센서와 같은 고가의 장비를 OTP토큰에 장착해야 한다는 부담을 줄일 수 있다. 이와 같은 인증구조는 전자상거래, 인터넷 뱅킹, 폰뱅킹 등과 같이 안전한 서비스를 제공하기 위한 분야에서 폭넓게 이용될 수 있다.

참고문헌

[1] 김태해, 정승환, 정용화, 문대성, 문기영, “워터마킹 기법을 이용한 생체정보 보호”
[2] 강수영, 이임영, “OTP를 활용한 UICC 기반의 인증 메커니즘에 관한 연구”, 한국정보보호학회, 2008.4.
[3] Bruce Schneier, ″Applied cryptography″ John Wiley & Sons, 1996.
[4] Behrouz A. Forouzan, ″Cryptography and Network security″ McGraw-Hill, 2008.
[5] 최동현, 김승주, 원동호, “일회용 패스워드(OTP: One-Time Password)기술 분석 및 표준화 동향”, 한국정보보호학회, 2007.6.
[6] 서승현, 강우진, “OTP 기술현황 및 국내 금융권 OTP 도입사례”, 한국정보보호학회, 2007.6.
[7] 류연호, “OTP 개념을 이용한 사용자-인증 서버의 상호 인증 모델”, NuriMedia, 2005.
[8] 히로시 유키, “알기 쉬운 정보보호 개론” 인피니티 북스, 2008. 1.
[9] 김기영, “일회용 패스워드를 기반으로 한 인증 시스템에 대한 고찰”, 한국정보보호학회, 2007.6.