일회용 패스워드를 기반으로 한 3-factor 인증 시스템

김동관*, 신승수*
*동명대학교 정보보호학과
e-mail: kwandk@nate.com

Three-Factor authentication system based on one time password

Donk-Kwan Kim*, Seung-Soo Shin*
*Dept of Information Security, Tong-Myong University

요 약

최근 인터넷과 같은 통신 기술 및 컴퓨터의 계산 능력이 급속도로 발전함에 따라, 많은 업무들이 온라인을 통해서 이루어지고 있다. 온라인 서비스의 편리함 이면에는, 전자 금융의 보안 허점을 노린 해킹시도가 끊이지 않고 있으며 금전적인 이득을 노린 금융 보안 사고들이 자주 발생하고 있다. 이러한 보안 사고를 막기 위해서 사용되는 기존의 인증 방식을 확인하고 인증 방식의 문제점을 분석한다. 본 논문에서 새로운 3-factor 인증 방식을 제안함으로써 기존의 인증 방식의 문제점을 해결하고, 기존 인증 방식보다 보안성이 강화된 인증 체계의 구현과 다양한 보안 서비스 제공, 안전한 금융 서비스 제공이 가능할 것으로 기대 된다.

1. 서 론

최근 인터넷과 같은 통신 기술 및 컴퓨터의 계산 능력이 급속도로 발전함에 따라, 많은 비지니스들이 온라인을 통해서 이루어지고 있다. 이에 따라 지식 및 정보 등 다양한 분야에 있어서 누구나 많은 혜택을 누릴 수 있게 되었다. 온라인 서비스의 편리함 이면에는, 전자 금융의 보안 허점을 노린 해킹시도가 끊이지 않고 있으며, 2005년 5월 인터넷 뱅킹 사고를 시작으로 2007년 1월 대형 은행 고객 정보 대량 유출 피싱사건, 2007년 2월 공인인증서 유출로 인한 은행 불법 인출 사건, 2008년 5월 인터넷 경매 사이트 '옥션' 개인정보 유출 사건 등 금전적인 이득을 노린 금융 보안 사고들이 발생하고 있다.[1]

이러한 환경에서 사용자 인증은 안전한 인터넷 사용을 위한 필수적인 요소라고 할 수 있다. 사용자 인증이란, 어떤 사용자가 실제로 정당한 사용자인지를 판단하는 과정으로, 대표적인 방식으로 아이디와 패스워드 방법이 있다. 하지만 이 인증 방식은 패스워드와 같은 단순한 인증 정보를 활용하기 때문에 네트워크 환경에서 커다란 문제점을 가지고 있다. 사용자가 아이디와 패스워드를 외우기 쉬운 정보로 설정하고, 다른 인증에도 고정된 아이디와 패스워드를 사용하기 때문에 공격자에 의해서 쉽게 추측될 수 있는 문제점이 있다.

또한 도청이나 스니핑 같은 공격에 쉽게 노출될 가능성이 높기 때문에 악의적인 공격자가 이를 이용하여 정당한 사용자로 위장할 수도 있다. 이러한 단점을 극복할 수 있는 방법으로 사용자만이 알고 있는 패스워드 이외에 사용자가 가지고 있는 매체나 사용자의 고유한 생체 정보를 결합 시켜 사용자 인증에 적용하는 방법과, 스마트 카드와 PIN(Personal- Identification Number) 패스워드의 사용, 패스워드와 공인인증서의 사용 등이 이에 해당한다. 두 개 또는 여러 개의 인증 수단을 사용하는 이중 요소 인증, 다중 요소 인증(Multi-Factor Authentication)을 도입하여 보안성을 강화하고 있으며 전자금융거래에서는 이중 요소 인증을 도입하여 사용자 인증을 강화 하였다.

최근 보안카드나 공인인증서 이외의 2-factor 인증의 한 수단으로 일회용 패스워드(One-Time Password)를 도입하였다. 그러나 OTP 토큰은 분실 및 도난시 불법 사용자의 의도적인 불법인증에 관한 취약점이 있다. 불법적인 사용자의 인증을 막기 위해 새로운 3-factor의 인증 방식을 제안한다.

2. 관련 연구

2.1 인증

인증(Authentication)이란 시스템 또는 네트워크에 액세스 하고자 하는 사용자를 확인하는 과정을 말한다.[2] 즉, 원격접속 환경에서의 인증이란 허용된 사용자인지 인증 절차를 확인 하는 것이다. 따라서 인증 절차는 컴퓨터나 네트워크와 같은 주요 전산 자산을 보호하는데 있어서 정보보안의 가장 기초적이면서도 필수적인 과정이다.

2.1.1 사용자 인증

사용자를 인증 하는 세 가지 방법 (ⅰ)알고 있는 것을 확인하는 방법 “What you know?” (패스워드, PIN 번호 등), (ⅱ)소유하고 있는 것을 확인하는 방법 ”What you have?” (스마트카드, 보안카드, OTP 토큰, 신용카드, 핸드폰 등), (ⅲ)사용자 자신을 확인하는 방법 “What you are?” (지문, 음성, 맥박, 홍채 등) 세 가지로 구성된다.[3]

2.1.2 이중 요소 인증(2-Factor Authentication)

2-factor 인증 방식이란 단일 인증의 보안 취약성을 보완하기 위하여 사용자 인증 방법의 세 가지 방법들 중에서 서로 다른 두 개의 인증을 조합하여 채택한 방식이 이중 요소 인증이다. 이중 요소 인증의 가장 보편적인 방법은 “알고 있는 것”과 “지니고 있는 것”을 동시에 사용하는 것이다. 신용카드 또는 현금인출용 카드가 이중 요소 인증 방식의 대표적인 예라고 할 수 있다. 즉 카드 자체를 물리적으로 사용자가 소유하고 있는 것이고, 이 카드에 대응되는 암호(4자리 숫자)는 사용자가 알고 있는 것이다. 이 두 요소가 동시에 제시되어야만 인증 과정을 통과 할 수 있다. 이중 요소 인증 방식은 원격접속 및 온라인 ID 도용 피해를 현격하게 줄여 주고 있다. 단, 카드에 대응되는 암호가 정적인 패스워드이기 때문에 그에 따르는 취약성이 있다. 이러한 방식의 한계를 극복하기 위해서는 패스워드의 개수를 굉장히 많이 늘리거나 매번 바뀌는 패스워드를 생성해야 한다. 여기서, 매번 바뀌는 비밀번호를 생성하는 방법이 일회용 패스워드이다.

2.2 OTP(One-Time Password)

일반적인 패스워드는 정적인 인증 수단으로 네트워크 도청으로 인해 패스워드를 알아냈을 경우 불법적으로 재사용할 위험이 있다. 그러나 OTP는 이미 사용된 패스워드는 재사용하지 않으므로 네트워크 도청을 통하여 패스워드를 알아냈다 할지라도 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 장치(Device)로 OTP 토큰(Token)이라고 한다. OTP는 OTP 생성매체에 의해 필요한 시점에 발생되고 매번 다른 번호를 생성한다.

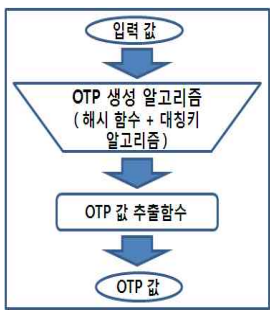
2.2.1 OTP 토큰

OTP 생성매체는 전용 하드웨어 OTP 토큰과 OTP 생성 기능을 소프트웨어로 탑재한 모바일 OTP, 카드형 OTP 등이 있다. 전용하드웨어 OTP 토큰은 OTP 자체를 생성할 수 있는 연산 기능, 암호 알고리즘 등이 내장되어 별도의 하드웨어 매체로 [그림1]과 같이 호출기 모양, 카드형 등이 있다.[4] OTP 생성 기능만을 지닌 전용 토큰이므로 추가 장비 필요 없이 사용이 가능하며 시스템 적용에 용이하여 많이 사용되고 있다. 그러나 사용자가 별도로 토큰을 구입해야 하므로 구입비용에 대한 부담과 휴대에 대한 불편함이 있다.

[그림 1. 전용 OTP토큰]

2.2.2 OTP 생성 과정

OTP 값의 생성은 [그림 2]와 같은 순서에 의해 생성된다.



[그림 2. OTP값 생성과정]

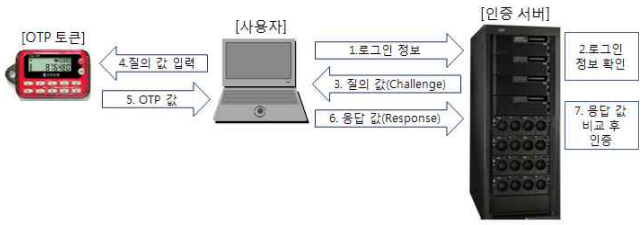
(가)입력 값 : OTP 생성알고리즘의 입력 데이터
(나)OTP 생성알고리즘 : 입력 값으로부터 OTP 값을 생성하는 알고리즘으로, 일방향 해시함수(현재 SHA-1, HAS-160이 사용 됨)와 대칭키 암호화알고리즘 (현재 블록암호 알고리즘이 사용됨)에 기반 한다.
(다) OTP 값 추출 알고리즘(Truncate 함수) : OTP 생성 알고리즘을 통해 출력된 값 으로부터 실제 패스워드로 사용할 OTP 값 6~8자리 숫자를 뽑아내는 알고리즘

2.2.3 OTP 생성 방식

(가) 비동기화 방식

비동기화 방식의 OTP는 OTP 토큰과 인증 서버간에 미리 설정되어 있는 동기화 기준 정보가 없어, 인증 요청시 사용자가 직접 임의의 난수 값을 OTP 토큰에 입력하여 OTP 값을 생성하는 방식을 말한다.[4] 비동기화 방식의 대표적인 예가 질의-응답(Challenge-Response) 방식이며, 인터넷 뱅킹에서 사용되는 보안카드가 바로 질의-응답 방식이다.

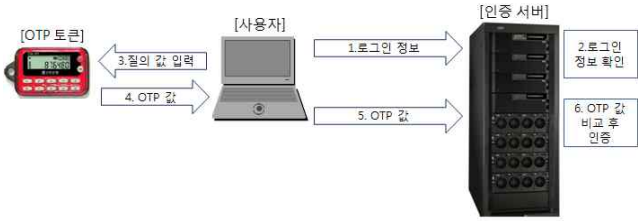
질의-응답 방식은 사용자가 OTP 인증 요청시 인증서버로부터 질의 값을 직접 OTP 토큰에 입력하여 응답 값(난수 형태)을 생성하는 방식으로, [그림 3]과 같이 사용자가 로그인 화면에 생성된 응답 값을 입력한다. 질의-응답 방식은 OTP 토큰과 인증 서버 간에 동기화해야할 기준 정보가 없기 때문에, 동기화할 필요가 없으며, 사용자와 서버 간에 상호인증을 제공하는 방식으로 쉽게 확장이 가능하다는 장점을 가진다. 그러나, 사용자가 직접 질의 값을 OTP 토큰에 입력해야한다는 불편이 있으며, 인증 서버도 해당 사용자의 질의 값을 관리해야 하는 부담이 있다. 또한 일반적인 패스워드 인증 어플리케이션과 호환이 쉽지 않다.



[그림 3. 비동기화 방식]

(나)동기화방식

동기화 방식은 OTP 토큰과 OTP 인증 서버 사이에 미리 공유된 비밀정보와 동기화 정보에 의해 OTP 값이 생성 되는 방식이다. 비동기화 방식에 비해, OTP 토큰과 인증 서버간에 반드시 동기화가 이루어져야 올바른 인증 처리가 된다는 제약점이 있으나, 사용자 입력 불편, 기존 ID/PASSWORD 어플리케이션과의 호환 어려움 등 비동기화 방식의 단점을 개선하였다.[5] OTP입력 값의 하나인 동기화 정보에 따라 시간동기화(Time-Synchronous) 방식, 이벤트 동기화(Event-Synchronous) 방식, 시간-이벤트 조합(Time-Event-Synchronous) 방식으로 구분된다. OTP 입력 값으로 시간 동기화 방식은 현재시간, 공유된 비밀키 값을 받고, 이벤트 동기화 방식은 이벤트 카운터 값과 공유된 비밀키 값을, 조합방식은 시간 값 + 이벤트 카운터 값, 공유된 비밀키 값을 받는다.



[그림 4. 동기화 방식]

2.2.4 OTP 취약점

(가) 해시함수의 안전성 문제 제기

기존의 OTP 토큰에 내장되어 있는 알고리즘으로 일방향 해시 함수인 SHA-1과 HAS-160이 사용되고 있다. 일발향 해시 함수는 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해시 값 또는 해시 코드라 불리는 값을 출력한다. 해시 함수 h는 임의의 길이의 문자열을 고정된 길이를 갖는 n비트 문자열로 대응시킨다. 정의역을 D, 치역을 R 이라 할 때 해시 함수 $h: D \rightarrow R$ ($|D| > |R|$)는 다대일 대응 함수이다. 이것은 충돌이 반드시 있음을 의미한다. 최근 중국의 암호학자인 WANG 교수의 차분 공격에 의해서 현재 전 세계에서 보편적으로 사용하고 있는 해시 알고리즘인 'SHA-1'과 'HAS-160'의 해독 가능성이 입증 되었다.[6]

(나) OTP 토큰의 오프라인 공격

OTP 토큰은 사용자가 항상 소지 하여야 하며 인증 요청시 반드시 가지고 있어야 한다. 만약 OTP 토큰의 분실 또는 도난발생시 이를 이용한 악의적인 사용자에 의해서 OTP 토큰의 사용을 막을 수 없다. 이는 사용자 본인이 아니더라도 누구나 OTP 값을 생성할 수 있다는 것이다. 이러한 문제점들을 해결하기 위해서 다음 장에서 새로운 3-Factor 인증 방식을 제안한다.

3. 3-Factor 인증 시스템

3.1 삼중요소 인증(Three-Factor Authentication)

앞 장에서 제시한 두 가지 문제점을 해결하고 보안성을 높일 수 있는 인증 시스템으로 3-Factor 인증 시스템을 제안한다.

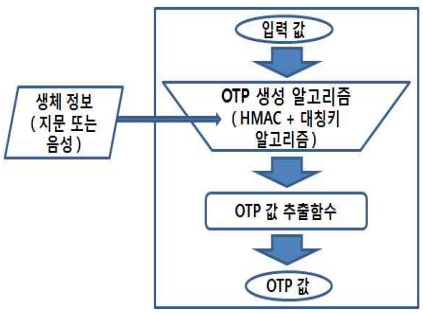
[표 1. 인증 요소의 예]

요소 구분	사용 예
알고 있는 것	암호, PIN 등
지니고 있는 것	OTP 토큰, 핸드폰 등
신체의 일부	지문, 음성패턴, 맥박, 홍채 등
할 수 있는 것	서명, 음성인식, 걸음걸이 등

위 [표 1]에 나타난 사용자 인증 요소의 3가지를 조합하여 이전의 이중요소 인증에 대한 오프라인 공격의 취약점을 해결 할 수 있다.[7] OTP 값 생성시 사용자의 유일한 생체정보를 해시함수의 입력 값이 아닌 HMAC[8]의 키 값으로 하여 OTP 토큰의 정당한 사용자를 인증 한다.

3.2.3-factor기반 OTP

3-factor 기반 OTP 값의 생성 과정은 아래 [그림 5]와 같이 구성된다.[9]



[그림 5. 3-factor OTP 생성 과정]

본 논문에서 제안한 3-factor기반 OTP는 지식기반 + 소유기반 + 생체정보 기반으로 구성 된다.

3.3 비교 분석

현재 금융권에서 사용하는 인증 방식과 본 논문에서 제안하는 3-factor 인증 방식의 OTP를 비교하고 안전성 및 보안성을 분석한다.

[표 2. 기존 인증 방식과 제안 OTP 방식 비교]

인증 방식	인증 요소	비밀번호구성	스니핑 공격	분실 및 도난	사용자 인증	악의적 사용
보안 카드	지식+소유	고정된 35개의 4자리숫자	o	o	x	o
기존 OTP	지식+소유	일회용 6자리의 숫자	1 회	o	x	o
제안 OTP	지식+소유+ 신체정보(지문,음성)	일회용 6자리의 숫자	1 회	o	o	x

4. 결론

본 논문에서는 현재 금융권에서 사용하는 2-factor 인증 방식인 OTP의 문제점을 제시하고 이를 해결 할 수 있는 3-factor 인증 시스템을 제안 하였다. 3-factor 인증 시스템은 현재 널리 사용되는 해시 함수의 안전성을 상기시키고 안전한 해시 함수로의 신속하고 체계적인 교체를 위해서 HMAC을 이용한 OTP 값 생성을 제안하였다. 또한 사용자의 유일한 생체 정보를 OTP 값 생성시 HMAC의 키 값으로 사용하여 OTP의 오프라인 공격을 통한 악의적인 사용을 막을 수 있다. 이는 기존 인증 방식보다 보안성이 강화된 인증 체계의 구현과 다양한 보안 서비스 제공, 안전한 금융 서비스 제공이 가능할 것으로 기대 된다.

향후 3-factor 인증 시스템이 가능한 저렴하고 사용자에게 편의성을 제공할 수 있는 OTP 토큰의 개발과 3-factor 인증 통합인증시스템 구축이 이루어져야 할 것이다.

참 고 문 헌

[1] www.boannews.com, 인터넷 보안뉴스
[2] 원동호, “현대암호학”, 그리출판, 2006. 8
[3] 서승현, 강우진, “OTP 기술현황 및 국내 금융권 OTP 도입사례“ 정보보호학회지, 2007. 6
[4] 금융보안연구원, “금융보안 주간정보”, 2006
[5] 백미연, “전자금융거래의 보안 강화 방안 및 OTP 이용현황“, 지급결제와 정보기술, pp.71-100, 2006. 4
[6] 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
[7] NetworkTimes, "OTP 솔루션“, 2006. 10
[8] 히로시 유키, “알기쉬운 정보보호 개론” 인피니티 북스, 2008. 1
[9] MRaihi, D., "HOTP: An HMAC-Based One Time Password Algorithm", IETF RFC 4226, 2005. 12