단일 제어 모바일 일회용 패스워드 기법

준회원 최 종 석*, 종신회원 김 호 원*°

One-Handled The Mobile One-Time Password Scheme

Jongseok Choi* *Associate Member*, Howon Kim*° *Lifelong Member*

요 약

E-비즈니스의 발전으로 온라인 서비스가 증가하면서, 금융이나 게임업체 등에서 정적 패스워드에 대한 취약성을 보완하기 위해서 OTP(One-Time Password)를 사용하고 있다. 기존의 OTP는 전용토큰을 이용하는데, 토큰을 이용한 OTP 기술은 항상 전용토큰을 소지하여야 한다. 이러한 단점을 보완하기위해 스마트폰과 같은 모바일 기기를 이용한 모바일 OTP를 제안한다. 본 논문에서 제안하는 모바일 OTP 기법은 범용적으로 사용되고 있는 해쉬함수를 이용한 S/KEY OTP 기법의 해쉬 충돌성에 대한 문제를 해결하기 위해 Pairing 기법을 이용한 비선형적 함수를 이용하여 OTP를 생성한다. 제안한 Pairing 기반의 비선형 함수를 이용한 모바일 OTP 기법은 기존의 해쉬충돌성을 보완할 수 있으며, 금융업체 및 다양한 서비스에서 보안안전성을 강화하기 위해 폭넓게 응용될 수 있을 것이다.

Key Words : OTP, Mobile, Privacy, Pairing, Banking

ABSTRACT

While increasing online services with developing e-businesses, finance, game companies and others have employed OTP(One-Time Password) to overcome vulnerabilities of static passwords. Existing OTP technology has inconvenience that customers always possess reserved token since requiring the token to generate OTP. In order to supplement the issue we propose mobile OTP generated by mobile devices such as smart phones. Our mobile OTP scheme generates OTP by using a non-linear function based on pairing to eject the collision problem of S/Key scheme universally used to design OTP schemes. Our scheme based on a non-linear function over pairing can complements the collision problem and widely applied to finance and various services to increase security level of the services.

Ⅰ. 서 론

최근에 통신기술이 발전하면서 e-비즈니스, 뱅킹 서비스 등과 같이 온라인을 이용한 서비스가 늘어나고 있다. 다양한 서비스의 온라인 활성화에 따라 사용자의 개인정보에 대한 도청 및 악용되는 사례가 늘어나고 있다. 개인정보를 얻기 위해서 많이 사용되는 공격방법으로 웹 아이디와 비밀번호를 추측하거나 다른 방법으로 취득하여 정당하지 않은 서비스를 이용하는 것이다. 금융서비스를 이용하기 위해서 보안카드를 이용하는데, 보안카드는 사용횟수가 누적될수록 악의적인 사용자가 상대의 보안카드에 대한 정보를 축적할 수 있다는 문제가 있다. 다양한 온라인 서비스에서는 이러한 정적 패스워드의

※ 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)의 일환으로 수행하였음. [10039953, 네트워크 중심의 차세대 능동형 RFID 기술 개발]
* 부산대학교 컴퓨터공학과 정보보호 및 시스템 LSI 연구실(jschoi85, howonkim@pusan.ac.kr) (° : 교신저자)
논문번호 : KICS2012-03-123, 접수일자 : 2012년 3월 16일, 최종논문접수일자 : 2012년 6월 5일

단점을 보완하기 위해서 높은 보안성을 요구하는 서비스의 경우 OTP(One-Time Password) 사용을 권장하고 있다. 하지만 기존의 사용되고 있는 OTP 기술[1-2,5-8]은 전용토큰을 사용하여 생성하고 있으므로, 항상 전용토큰을 소지해야하는 불편함이 있다. 이러한 단점을 보완하기 위해서는 대중적으로 사용되고 있는 휴대폰을 사용할 수 있다. 현재 국내 휴대폰 가입자 수가 4,000만명 이상이며, 그 중에서 스마트폰 사용자는 2,000만명을 초과하였다. 스마트폰은 다양한 앱을 개발하기 용이하며 설치 및 제거할 수 있는 특징을 가지고 있지만, 그만큼 보안 취약성이 많기 때문에 OTP 토큰으로 대중적으로 이용되지 못하고 있었지만, 스마트폰 보안을 강화하기 위한 많은 연구로 인해 뱅킹 및 전자거래등과 같은 높은 보안성을 요구하는 다양한 서비스를 스마트폰을 통해서 제공하고 있다. 뱅킹업무를 하기 위해 각 은행사나 증권사마다 정해진 금액을 초과할 시에는 OTP사용을 권장하고 있다. 이처럼 OTP는 보안카드나 다른 인증수단보다 높은 보안성을 제공하고 있지만, 휴대가 용지하지 않은 OTP토큰을 항상 소지해야 한다는 단점 때문에 대중화되지 못하고 있다.

OTP 및 모바일 OTP에 대한 연구는 수년 동안 활발하게 진행되고 있으며, 대표적인 모바일 OTP 기법으로 [3]가 있다. 기존 기법[3]은 타원곡선에 기반하여 S/KEY 기법의 횟수제한과 유추에 대한 문제점을 해결하였지만, OTP를 생성하기 위해 모바일 디바이스와 서버가 2-way handle이 필요하다는 단점이 있다.

본 논문에서는 스마트폰의 보안취약성을 보완하고 1-way handle 통신을 위해 Pairing 기반의 모바일 OTP 기법을 제안함으로써, OTP 기술의 대중화에 기여하고자 한다. 모바일 OTP 기법에 대한 보안성을 강화하기 위해 스푸핑, 재전송공격, 세션하이재킹과 같이 세가지 문제점을 중점적으로 해결할 수 있도록 설계한다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구로써 S/Key 방식을 살펴보고 3장에서 제안한 모바일 OTP 기법을 설명한다. 4장에서는 제안한 기법에 대해 분석하고 5장에서 결론을 맺는다.

Ⅱ. S/Key 방식

S/Key 방식[4]은 1994년에 처음 제안되었으며, 암호학적 일방향 해쉬함수를 이용한 기법이다. S/Key 방식은 현재 OTP 토큰에는 사용되고 있지 않지만, 기존의 OTP 방식은 대부분 S/Key 방식과 같은 해쉬함수를 이용하여 해쉬체인으로부터 얻어진 값을 OTP로 사용하고 있다. S/Key 방식에서는 최초 등록과정에서 OTP를 사용할 수 있는 횟수가 정해진다. S/Key 방식은 등록단계와 인증단계로 크게 나누어질 수 있다.

2.1. 등록단계

최초의 사용자를 등록하는 단계로써 안전한 채널을 통해서 이루어진다.

Step 1. $U \rightarrow S: x$

사용자가 임의의 x를 생성하여 서버에게 전송한다.

Step 2. $S \rightarrow U: H^n(x), n$

서버는 x를 일정횟수 해쉬연산을 수행하고 사용자에게 결과값과 해쉬횟수를 알린다.

2.2. 인증단계

사용자가 서버에 서비스를 제공받고자 할 때 수행되며, 안전하지 않은 채널을 통해서 이루어진다.

Step 1. $U \rightarrow S: OTP = h^{n-1}(x)$

사용자는 등록시 생성한 x를 $n-1$번 해쉬연산하고 그 값을 OTP로 서버에게 전송한다.

Step 2. $S: H^n(x) = ?H(OTP)$

서버는 받은 OTP값을 한 번 더 해쉬연산하여 저장되어 있는 값과 같은지 확인한다.

Step 3. $S \rightarrow U: accept$ or $reject$

서버는 사용자에게 인증여부를 전송한다. 이 때 인증을 성공할 경우에는 수행하고 $h^n(x)$ 대신 전송받은 OTP를 저장한다. 사용자는 n값을 1씩 감소시킨다.

Ⅲ. 모바일 OTP 기법

본 장에서는 Pairing 기반의 모바일 OTP 기법을 제안한다. 제안한 기법은 기존의 기법[5]의 2-way handle 통신에 대한 취약점을 개선하고 스마트폰에서의 스푸핑, 재전송공격, 세션하이재킹 공격에 대해 안전하도록 설계되었다. 제안한 모바일 OTP 기법은 겹선형사상을 이용한 Pairing 연산으로 1-way handle 통신으로 모바일 디바이스와 서버 간에 OTP를 인증할 수 있으며, 등록단계, 인증단계로 이루어진다.

3.1. 등록단계

등록단계는 사용자가 모바일 OTP를 사용하기 위해 최초 모바일 디바이스 등록을 수행하는 단계이다. 등록단계는 오프라인 또는 안전한 통신을 사용하여 이루어 질 수 있다.

Prestep.

서버(S)가 최초로 서비스를 개시하기 위해서 겹선형 사상을 선택하는 단계이며, 겹선형 사상 ($\hat{e}: G_1 \times G_1 \rightarrow G_2$)은 아래와 같은 세가지 특징을 만족해야 한다.

(1) 겹선형성

$\forall P, Q \in G_1, \forall a, b \in Z_q^*, \quad \hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$

(2) 비퇴보성

$\forall P \in G_1, P \neq 0 \Rightarrow \langle \hat{e}(P,P) \rangle = G_2$

(3) 계산효율성

$\hat{e}$는 효율적으로 계산될 수 있어야 한다.

Step 1. $S \Rightarrow U$: $\hat{e}$

서버(S)는 사용자(U)에게 겹선형 사상을 전송한다.

Step 2. $U \Rightarrow S$: $\hat{e}(M, R_U)^{MPIN}$

사용자(U)는 서버(S)에게 선택메세지(M)와 난수(R_U)를 모바일 디바이스의 고유번호(MPIN)로 페어링 연산한 값($\hat{e}(M, R_U)^{MPIN}$)을 전송한다.

Step 3. $S \Rightarrow U$: $\hat{e}(M, R_U)^{MPIN \cdot X \cdot R_S}$

서버(S)는 사용자(U)에게 받은 값에 서버의 비밀키(X)와 난수(R_S)를 곱한 값으로 페어링 연산하여 전송한다.

Step 4. $S \Rightarrow U$: $OTP, MPIN$

사용자(U)는 서버(S)에게 전송받은 값을 모바일 디바이스의 고유번호($MPIN$)으로 페어링 연산한 값(OTP)과 고유번호($MPIN$)를 전송한다.

Step 5. $S \Rightarrow U$: $Accept$ or $Reject$, T

서버(S)는 일회용패스워드(OTP)에 대한 검증을 완료하고, 검증을 성공하면 사용자의 고유번호($MPIN$)을 저장하고 사용자에게 검증여부와 타임스탬프(T)를 전송한다.

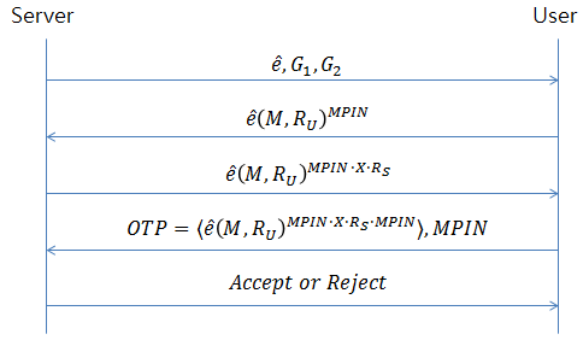

그림 1. 등록단계 흐름도
Fig. 1. Flow of registration phase

3.2. 인증단계

인증단계는 등록된 모바일 디바이스를 통해서 사용자 인증을 수행하고자 할 때 안전하지 않은 채널을 통해서 수행한다. 제안한 기법의 인증단계는 1-way handle로 이루어진다.

Step 1. $U \rightarrow S$: OTP', $OTP \oplus T_U$

사용자(U)는 등록단계 및 이전세션에서 갱신된 일회용패스워드(OTP)와 현재 타임스탬프(T_U)를 모바일 디바이스의 고유번호($MPIN$)로 페어링 연산을 수행하고, 연산된 값($OTP' = \hat{e}(OTP, T_U)^{MPIN}$)과 일회용패스워드($OTP$)로 타임스탬프($T_U$)를 배타적 논리합(XOR)하여 전송한다.

Step 2. S: $Accept$ or $reject$

서버(S)는 사용자의 이전 일회용패스워드(OTP)를 이용하여 전송받은 값으로부터 사용자의 타임스탬프(T_U)를 계산하고, 사용자의 타임스탬프(T_U)와 서버의 타임스탬프(T_S)를 비교하여 타임스탬프의 차이가 일정시간(ΔT)보다 작으면 사용자의 타임스탬프(T_U)를 통과시킨다. 사용자의 타임스탬프(T_U)를 이용하여 새로운 일회용패스워드(OTP')를 계산하여 전송받은 값과 같으면 서버(S)는 사용자(U)를 인증한다.

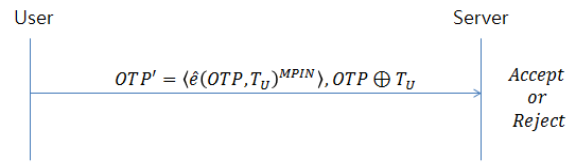

그림 2. 인증 단계 흐름도
Fig. 2. Flow of authentication phase

Ⅳ. 분 석

본 장에서는 제안한 기법을 해쉬 충돌쌍, 위장공격에 대해 각각 분석한다.

4.1. 해쉬 충돌쌍

S/Key 방식과 같이 해쉬함수를 이용한 해쉬체인을 OTP로 이용하는 경우에는 암호학적 일방향 해쉬함수의 충돌내성에 따라서 해쉬의 충돌쌍이 생길 수 있다. 그리고 이러한 충돌쌍에 대해서 이후의 OTP 값이 모두 동일해 지는 문제가 발생한다. 예를 들어 S/Key 방식에서 n값을 100이라고 하고, 두 사용자가 각각 초기 값으로 x,y를 선택했다고 하자. 그리고 $H^{10}(x)$와 $H^{20}(y)$가 동일한 해쉬값을 생성한다면, $H^{10\sim 90}(x)$와 $H^{20\sim 100}(y)$에 대한 모든 OTP값은 두 사용자가 동일하게 생성될 것이다. 따라서 S/Key 방식 뿐만 아니라 해쉬체인을 이용하는 OTP 방식에서는 상호 사용자간의 도청으로 인해 동일한 OTP가 전송되었을 경우 다음 OTP를 추측할 수 있는 심각한 문제를 초래한다. 본 논문에서 제안한 OTP방식은 해쉬함수의 충돌쌍에 대한 문제를 해결하기 위해 겹선형 사상에서 비선형함수를 이용하여 OTP를 생성한다. 제안한 기법에서는 모바일 디바이스의 고유번호를 이용하여 페어링 연산을 수행한다. 따라서 두 사용자의 디바이스가 각각 $MPIN_1, MPIN_2$라고 가정했을 때, 두 디바이스의 10번째 OTP가 동일해도 각 디바이스의 고유번호를 페어링 연산한 11번째 OTP는 동일해질 수 없다. 따라서 해쉬의 충돌쌍에 대한 문제점을 해결할 수 있다.

4.2. 위장 공격

공격자가 같은 서버에 등록된 사용자일 경우에는 인증단계에서 $OTP \oplus T_U$를 도청하여, 자신의 타임스탬프 T_A를 이용하여 사용자의 이전 OTP를 구할 수 있다. 공격자가 사용자의 OTP를 위장하기 위해서는 해당 OTP를 이용하여 $\hat{e}(OTP, T_U)^{MPIN}$을 계산할 수 있어야 한다. 공격자가 매번 OTP를 계산하기 위해서는 해당 사용자의 모바일 디바이스 고유번호를 알아야 한다. $\hat{e}(OTP, T_U)^{MPIN}$에서 $MPIN$을 계산할 수 있으면 위장공격이 가능하지만, $MPIN$을 계산하는 것은 페어링 연상에서의 이산대수 문제에 해당한다. 따라서 일정비트 이상이 되면 안전하다고 할 수 있다.

Ⅴ. 결 론

웹이나 전자금융거래에서 주로 사용되고 있는 보안카드나 정적패스워드 기반 보안기술에는 보안안전성에 한계가 생긴다. 금융업체 및 보안을 요구하는 다양한 서비스 제공업체들은 이러한 보안 문제점을 보완하기 위해서 높은 보안안전성을 요구하는 서비스의 경우에는 동적 패스워드 기반인 일회용패스워드를 사용할 것을 권장하고 있다. 일회용패스워드를 사용하기 위해서는 일회용패스워드를 생성하기 위한 전용토큰기기가 필요하다. 이러한 기기를 항상 소지하고 다니는 것은 사용자의 휴대에 용이하지 않으며 이러한 문제점 때문에 대중화되지 못하고 있는 것으로 분석된다. 토큰기기의 휴대성을 강화하기 위해서 모바일 단말을 OTP 토큰으로 사용하는 모바일 OTP에 대한 연구는 최근 수년간 진행되고 있지만, 모바일 기기의 보안 취약성 때문에 현재는 크게 상용화되지 못하고 있다.

본 논문에서는 스마트폰과 같이 모바일 단말을 OTP토큰으로 사용할 경우 생길 수 있는 보안문제점을 스푸핑, 재전송공격, 세션하이재킹으로 크게 분류하여 이러한 보안취약성을 해결할 수 있도록 Pairing 기반의 모바일 OTP 기법을 제안하였다. 제안한 모바일 OTP 기법은 다음과 같은 방법으로 세 가지 보안 문제점을 해결하고 있다.

* 스푸핑 : OTP 값을 스푸핑한다고 하더라도 모바일 디바이스의 고유번호를 알 수 없기 때문에 새로운 OTP를 생성할 수 없다.
* 재전송공격 : OTP를 저장해두었다가 재전송을 통해서 인증을 시도할 경우에는 타임스탬프의 범위를 초과하기 때문에 인증을 성공할 수 없으며, 모바일 디바이스의 고유번호를 모르면 갱신된 타임스탬프를 이용하여 새로운 계산을 할 수 없다.
* 세션하이재킹 : 본 기법에서는 겹선형 함수의 이산대수 문제에 기반하고 있으므로 세션하이재킹을 성공하더라도 중간자가 정보를 수정하기는 어렵다.

제안한 기법은 OTP 기법에서 주로 사용되고 있는 해쉬함수의 충돌쌍에 대한 문제를 해결하고 있으며, 금융서비스, 게임보안 등과 같이 높은 보안안전성을 요구하는 다양한 서비스에 폭넓게 적용될 수 있다.

References

[1] Soo-Young Kang and Im-Yeong Lee, “A Study on UICC(Universal IC Card)-based Authentication Mechanism using OTP,” Korea Institute of Information Security and Cryptology, Journal of the Korea Institute of Information Security and Cryptology, 21(5), pp.21-31, 2008.

[2] Youngjin Kim, Kiyoung Baek , Younggil Kim , Jaecheol Ryou , Gyutae Baek and Junggil Park, “The Development of a One-time Password Mechanism Improving on S/KEY,’’ Korea Institute Of Information Security And Cryptology, Journal of the Korea Institute of Information Security and Cryptology, 9(2), pp. 25-35, 1999.

[3] Hong Gi Kim and Im Yeong Lee, “A Study on One-Time Password Authentication Scheme in Mobile Environment,’’ Korea Multimedia Society, JOURNAL OF KOREA MULTIMEDIA SOCIETY, 14(6), pp. 785-793, 2011

[4] Neil M. Haller, ″The S/KEY One-Time Password System″, edited by Dan Nesset and Robj Shirey, Proceedings of the Symposium on Network and Distributed Systems Security, pp.151-157, 1994.

[5] Donghyun Choi, Seungjoo Kim, Dongho Won, “One-Time Password Technical Analysis and Standard Trends,” Korea Institute Of Information Security And Cryptology, REVIEW OF KIISC, Vol.17 No.3, pp.12-17, 2007.(원동호, 최동현, 김승주, “일회용 패스워드(OTP: One-Time Password)기술 분석 및 표준화 동향”, 한국정보보호학회, 정보보호학회지, 제17권 제3호, pp.12-17, 2007.)

[6] Seung-Hyun Seo , Woojin Kang, “OTP Condition and Instance of OTP in Korea”, Korea Institute Of Information Security And Cryptology, REVIEW OF KIISC, Vol.17 No.3, pp.18-25, 2007.(서승현, 강우진, “OTP 기술현황 및 국내 금융권 OTP 도입사례”, 한국정보보호학회, 정보보호학회지, 제17권 제3호, pp.18-25, 2007.)

[7] Yeon-Ho Ryu, “User-Authentication Server Mutual Authentication Model using OTP concept,” The Korean Institute of Information Scientists and Engineers, Proceedings of fall conference, pp.652-654, 2003.(류연호, “OTP 개념을 이용한 사용자-인증 서버의 상호 인증 모델,” 한국정보과학회, 2003년도 가을 학술발표논문집, pp.652-654, 2003.)

[8] Ki Young Kim, “A Study of Authentication System Based on One-time Password,” Korea Institute Of Information Security And Cryptology, REVIEW OF KIISC, Vol.17 No.3, pp.26-31, 2007.(김기영, “일회용 패스워드를 기반으로 한 인증 시스템에 대한 고찰”, 한국정보보호학회, 정보보호학회지, 제17권 제3호, pp.26-31, 2007.)

최 종 석 (Jongseok Choi) 준회원

2011년 2월 동명대학교 정보보호학과 졸업

2011년 3월~현재 부산대학교 컴퓨터공학과 석사과정

<관심분야> 모바일 보안, 페어링 암호, 분산시스템 보안

김 호 원 (Howon Kim) 종신회원

1999년 2월 포항공과대학교 전자전기공학과 박사(공학박사)

1998년 12월~2008년 2월 한국전자통신연구원(ETRI) 정보보호연구단 선임연구원/팀장

2008년 3월~현재 부산대학교 정보컴퓨터공학부 부교수

<관심분야> RFID/USN 정보보호 기술, 공개키 암호, Cyber-Physical Security, VLSI 설계