이체정보를 활용한 강화된 모바일 OTP 생성기 설계

박범수*, 조상일**, 김태용**, 이훈재**

*동서대학교 일반대학원, **동서대학교 컴퓨터정보공학부

On a Enhanced Mobile OTP generator design using Transaction

Beum-Su Park*, Sang-Il Cho**, Tae Yong Kim, Hoon Jae Lee**

*Department of Ubiquitous and IT Graduate School of General, Dongseo University, Busan, 617-716, South Korea, Tel: +82-51-320-1730

**Div. of Computer and Information Engineering, Dongseo University

BeumSuPark@hotmail.com, i3011@lycos.co.kr, kim2k@paran.com, hjlee@dongseo.ac.kr

요 약

일회용 암호는 동일한 암호를 반복해서 사용하는 방법에 비해 생성된 암호를 한번만 사용하는 특성을 가져 보다 안전하다. “휴대폰 상에서 특정 트랜잭션용 추가 인증을 제공하는 일회용 암호 생성기 설계 방안”에서는 챌린지 교환방식을 활용한 일회용 생성기를 제안하였다. 하지만 챌린지값 교환의 문제점과 기존과 동일한 암호비도 수준을 보인다. 본 논문에서는 제시된 일회용 암호 생성기 설계 방안에 대해 분석하고 해결방안과 새로운 방안을 제시하여 중간자 공격과 재사용 공격에 강화되면서 보다 높은 수준의 암호비도수준을 보여주는 방법을 제안한다.

ABSTRACT

Generated One-Time Password (OTP) is used only once. This attributes is to safety than to repeated use the same password. Recently, Park’s proposed on “Design of A One-time Password Generator on A Mobile Phone Providing An Additional Authentication for A Particular Transaction” use challenge-response based one-time password generator. However, Challenge exchange problem and currently OTP the same security level. In this paper, Park’s proposed OTP generator design for us analysis. And then presents a resolution to the problem and new system logic. New system strong to Man-In-Middle attack and replay attack. In addition, OTP security level is higher.

키워드

OTP(One Time Password), SHA-256, 시간동기화, 챌린지동기화

Ⅰ. 서 론

최근 보고되고 있는 전형적인 인터넷 뱅킹의 해킹 방법은 특정 사용자 PC에 키보드 로거나 스크린 그래버 같은 스파이웨어를 사용자 몰래 설치하여 오랜 기간에 걸쳐 사용자의 인터넷 뱅킹용 비밀 정보를 수집을 하고, 수집된 정보를 이용해 공격자가 자신이 원하는 계좌로 공격 대상자의 예금을 이체 시키는 것이다. 이러한 공격에 대비해 인터넷 뱅킹 솔루션을 개발하는 은행 및 공급업체는 방화벽, 키보드 보안 및 암호화 솔루션 등을 인터넷 뱅킹 사용자에게 제공하고 있다. 하지만 이런 노력에도 불구하고, 보안에 무관심하거나 또는 공공에게 노출된 PC로 인터넷 뱅킹을 하는 경우 해킹을 통한 금전적 피해의 가능성은 여전히 남아있다. 이에 최근에는 Two Factor 인증[1]을 위해 OTP(One-Time Password)[2],[3] 생성기를 사용해서 보이는 숫자 암호를 사용자가 입력하도록 하는 방식이 더 안전하다고 판단되어 많이 사용하고 있다.

이것에 관한 연구 논문 중 “특정 트랜잭션용 추가 인증을 제공하는 휴대폰상의 일회용 암호 생성기 설계”[4] 에서는 현재 쓰이는 OTP의 보안상 문제점들을 제시하고, 이에 대한 대안으로 개인 휴대폰 상에서 보안성이 강화된 OTP생성기를 설

계하였다. 제시된 방안은 중간자 공격에 대비 할 수 있고 휴대성이 뛰어나며, 도난의 경우에도 안전하고, PC에 설치된 키보드 로거 등의 스파이웨어를 통한 공격 대상자의 다른 인증 정보가 노출되더라고 불법 이체 행위를 막을 수 있다고 하였다. 하지만 본 논문에서는 제시된 OTP 생성기의 보안상 문제점을 보이는 챌린지 값 재전송 횟수 제한의 관리와 HMAC(SHA-256)를 통해 나온 값을 base-64로 인코딩하여 기존 사용 중에 있는 OTP 생성기와 동일한 암호 비도수준을 가지는 OTP 값에 대하여 기존 제안한 방법을 수정하고 새로운 방안을 제안함으로써 보안상 문제점을 개선하고자 한다.

II. 문제점 분석

본 장에서는 앞서 제안된 OTP생성기 설계구조와 중요기술에 대해 알아보고, OTP생성기 설계에서의 문제점에 대한 분석결과는 표 1. 과 같다.

표 1. 제안된 OTP 생성기의 문제점 분석

주요기술	모바일상에서 특정 트랜잭션을 활용한 OTP값 생성하고, 이를 이용하여 재전송 공격 및 중간자공격을 방지한다.
OTP 생성기 구조	OTP 생성기의 내부적인 값, 챌린지값 그리고 특정 트랜잭션(이체정보, 사용자PIN)값들을 HMAC(SHA-256)의 키값으로 사용하여 랜덤한 키스트림을 생성, base64로 인코딩된 4digit을 인증키로 사용된다.
챌린지값 생성방식	HC-256 사용하여 랜덤스트림값을 생성, 24bit 단위로 사용자에게 배부.
챌린지값의 문제점	재전송 횟수에 대한 제한이 없어, 재전송 공격에 노출됨.
OTP값의 문제점	기존에 사용하는 OTP와 동일한 암호비도를 가지면서 약 30번의 모바일패드 입력은 가용성이 떨어짐.

III. 문제점 해결방안

본 장은 2장에서 유추된 OTP생성기 설계상의 문제점에 대하여 해결방안을 제시하고, 제안된 설계안을 수정 및 보안하여 새로운 설계 방안을 제안하고자 한다.

3.1. 챌린지 값 관리 문제

챌린지 값의 재요청 시도에 대한 횟수 제한을 적용하여 반복적인 재요청 시도를 방지 할 수 있어야 한다. 또한, 챌린지 값으로 OTP를 생성함으로 OTP 오류입력 횟수와는 별개의 값으로 카운트 되어야 한다.

3.2. OTP값의 보안성 강화를 위한 제안

현재 사용중인 공인 인증서 인증과정 후에 OTP에 의한 인증과정 부분은 그림 1. 에서와 같이 특정트랜잭션을 활용한 시간동기화 방식을 이용하여 OTP코드와 별개의 은행코드를 최종 입력하는 인증키로 사용하여 보다 높은 보안성을 가지는 OTP 생성기를 제안한다.

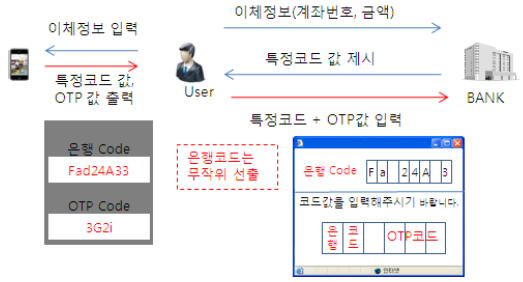

그림 1. OTP의 강화된 인증 방안

IV. 결 론

본 논문에서는 사용자와 은행 간의 이체정보를 이용한 은행코드를 이용하여 중간자 공격의 근원적 차단이 가능하게 하였다. 또한, 생성된 은행코드값과 OTP코드값을 최종 인증키 값으로 사용하여 암호비도 수준을 향상 시키고 중간자 공격에 강함을 가진다. 또한 사용자가 직접 은행에서 OTP 생성기를 휴대폰에 받아 사용함으로써 공유키에 대한 공격은 휴대폰 분실 시 일어 날 수 있으나, 휴대폰을 분실하였을 경우 휴대폰에 설치된 프로그램의 PIN값을 미리 설정하여 불법적인 OTP 생성시도를 막으며 별도의 OTP생성 장치를 구비하는데 드는 비용이나 배터리 교체 및 휴대의 부담에서 이득을 가진다.

참고문헌

[1] B. Schneier, “Two-Factor Authentication, Too little, Too Late”, Communications of the ACM, vol48, no4, April 2005.

[2] L. Lamport, “Password Authentication with Insecure Communication”, Communications of the ACM, vol24, no11, pp770-772, 1981.

[3] N. Haller, C. Metz, P. Nesser, and M. Straw, “A One-Time Password System”, RFC 2289, IETF, 1998.

[4] 박준철, “특정트랜잭션용 추가 인증을 제공하는 휴대폰 상의 일회용 암호 생성기 설계”, 정보과학회논문지, vol36, no6, Dec 2009.