OTP 통합인증과 안전성 분석

김인석* · 강형우* · 임종인**

요 약

최근 개인용 컴퓨터 및 네트워크의 발전과 보급 확대 등으로 인하여 인터넷뱅킹과 같은 전자금융의 사용이 급속도로 증가하고 있다. 전자금융의 활성화가 금융권의 업무 효율성과 고객의 금융거래의 편의성 측면에서 상당히 큰 기여를 하고 있지만, 전자금융거래가 갖는 비대면성의 특성으로 인하여 이에 대한 보안 문제가 점차 증대되고 있다. 따라서 최근 금융권에서는 전자금융 거래시 본인확인 강화를 위하여 OTP(One Time Password)를 도입하고, 고객이 하나의 OTP 기기를 이용하여 금융권에서 공동으로 사용하기 위한 OTP 통합인증센터를 구축하였다. 본 논문에서는 전자금융의 보안강화를 위하여 금융권에서 추진 중인 OTP 통합인증센터의 주요 업무를 살펴보고 OTP 통합인증센터의 핵심 기능인 OTP 통합인증 서비스에 대한 안전성 분석을 제시한다.

Integrated OTP Authentication and Security Analysis

In Seok Kim* · Hyung Woo Kang* · Jong In Lim**

ABSTRACT

In recent years, electronic financial services, such as internet banking, come into wide use since the personal computer and network technology have made reasonably good progress. The growth of electronic financial service contributes to promoting the business efficiency of financial institution and promoting the convenience of financial customer, while the security on electronic financial service is getting more important because it is not face-to-face financial service. Therefore, the financial sector had decided to introduce the OTP (One Time Password) in order to authenticate the identification of customer and has built the Integrated OTP Authentication Center for a customer being able to use only one OTP token in electronic financial transaction with several financial institution. In this paper, we introduce the business of Integrated OTP Authentication Center and present the security analysis on integrated OPT authentication service, which is the main function of Integrated OTP Authentication Center.

Key words : Electronic Finance, OTP(One Time Password), Authentication, MITM(Man-In-The-Middle) Attack, Phishing

* 금융감독원
** 고려대학교 정보경영공학 전문대학원 원장

1. 서 론

인터넷뱅킹서비스 등록 고객수가 3천만명을 넘어서고 전자금융서비스를 이용한 자금이체 건수가 전체 이체건수의 75%를 넘어서는 등 사람들이 금융업무를 위해 인터넷에 의존하는 빈도가 점점 높아지고 있다. 이러한 전자금융의 활성화 이면에 전자금융의 보안 허점을 노린 해킹시도가 끊이지 않고 있다. 2005년 5월에는 시중은행의 인터넷뱅킹에서 해킹사고가 처음으로 발생하였다. 이를 계기로, 금융감독원은 산업자원부, 정보통신부 등 유관기관과 공동으로 “전자금융 보안 종합대책”[1]을 수립하여 2005년 9월 경제정책조정회의에 보고하였다.

“전자금융 보안 종합대책”은 개인 정보유출로 인한 전자금융사고의 피해를 최소화하고, 안전한 전자금융거래를 위한 대책을 제시하고 있으며, 특히 인터넷뱅킹과 같은 전자금융거래시 본인확인을 강화하기 위하여 OTP 기기를 도입하도록 하였다. 이와 함께, OTP 통합인증센터를 설립하여 금융권에서 공동으로 사용할 OTP 통합인증시스템을 구축하고 운영 및 관리를 전담하도록 하였다.

OTP 인증 기술은 강력한 보안성과 편의성으로 인해서 활발한 연구들이[2-6] 진행되고 있으며, 최근에는 전 세계적으로 널리 보급되고 있으므로, 수많은 보안전문가들이 OTP 인증 기술의 안전성을 분석하여 검증하였다. 하지만, 사용자가 하나의 OTP 기기를 여러 기관에 공동으로 사용하기 위한 OTP 통합인증시스템은 전 세계적으로 구축 사례가 없으며, 이에 대한 안전성 분석 또한 전무한 상태이다. 따라서 국가 공공의 목적으로 전자금융에 적용할 OTP 통합인증서비스에 대한 안전성 분석은 반드시 필요하다.

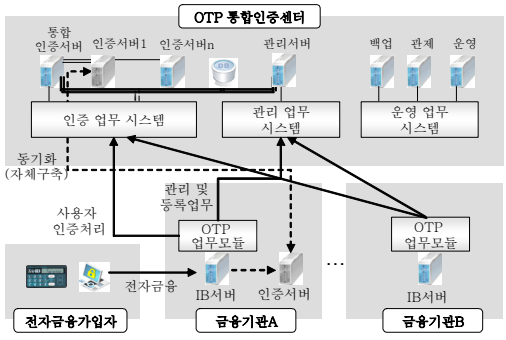
본 논문의 구성은 다음과 같다. 제 2장에서는 OTP 통합인증센터에서 수행하는 주요 업무를 살펴보고, 제 3장에서는 OTP 통합인증센터의 핵심기능인 OTP 통합인증서비스에 대해서 안전성을 분석하며, 마지막으로 제 4장에서는 결론을 내린다.

2. OTP 통합인증센터

OTP 통합인증이란 사용자가 하나의 OTP 기기를 가지고서도 자신이 거래하는 모든 금융기관의 전자금융 서비스를 이용할 수 있도록 통합된 OTP 인증이 제공됨을 의미한다. 즉 금융기관 공동으로 구축하는 OTP 통합인증센터를 통해 전자금융 사용자의 OTP 인증이 모든 금융기관에 통합적으로 수행하게 된다.

2.1 OTP 통합인증센터 업무

OTP 통합인증센터는 금융기관의 요청에 의한 OTP 인증업무와 금융기관과의 OTP 업무를 위한 관리업무 및 통합인증센터 고유의 운영업무 3가지로 구성되며, OTP 통합인증센터의 구성도는 (그림 1)과 같다. 인증 업무는 통합인증센터의 핵심 업무로서 금융기관이 요청한 전자금융가입자의 식별자와 OTP값을 받아서 OTP값의 유효성을 확인하여 인증을 제공하는 것이며, 관리 업무는 인증업무를 제외한 금융기관과 통합인증센터 간에 연동이 필요한 업무로서 OTP 기기의 발급 및 재발급, 등록 및 폐기 등의 업무가 이에 해당된다. 운영 업

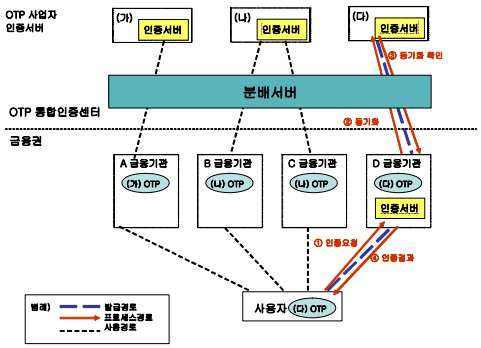


(그림 1) OTP 통합인증센터 구성도

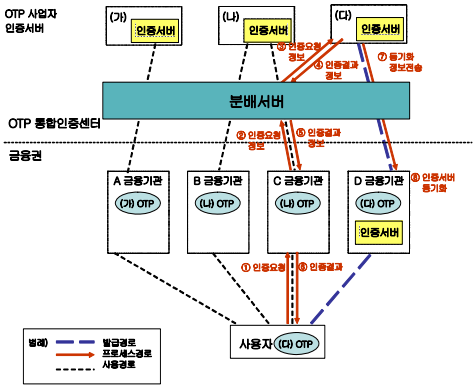
무는 금융기관과의 연동이 필요 없는 통합인증센터 내부의 업무로서 시스템 운영, 정보시스템 감사, 관제 및 모니터링 및 비상대응 등이 해당된다.

2.2 OTP 통합인증 절차

OTP 통합인증센터에서 제공하는 인증서비스는 금융기관이 대체인증서버를 이용하는 경우(그림 2)와 대체인증서버를 이용하지 않는 경우(그림 3)로 나뉘어 진다. 대체인증서버는 금융기관이 개별적으로 OTP 인증서버를 구축하여 발행한 OTP 기기에 대해서 자체적으로 인증서비스를 제공하며, OTP 정보의 동기화를 위해 OTP 통합인증센터로 동기화 전문을 전송한다. 반면에 대체인증서버가 구축되지 않은 금융기관은 OTP 통합인증센터를 통하여 모든 OTP 인증 처리를 수행하게 된다. 금융기관이 대체인증 서버를 보유했다 하더라도 타 금융기관에서 발급된 OTP를 등록하여 사용하는 경우에는 OTP 통합인증센터를 통하여 인증처리를 하게 되며, OTP 통합인증센터에서는 해당 토큰의 발급기관에 역방향으로 동기화 통지 전문을 전송한다. 인증 실패가 발생할 경우 OTP 통합인증센터에서는 오류횟수 등을 통합관리 한다. 대체인증서버를 이용한 인증방식은 OTP 통합인증센터의 부하를 분산시키는 효과가 있으며, OTP 통합인증센터의 비상시에도 별도의 인증경로의 전환작업 없이 정상적으로 거래될 수 있다는 점에서 상대적으로 안정성이 높다.



(그림 2) 발급 금융기관의 대체인증서버를 통한 인증절차



(그림 3) 발급 금융기관이 아닌 타 금융기관을 통한 인증절차

3. OTP 통합인증의 안전성 분석

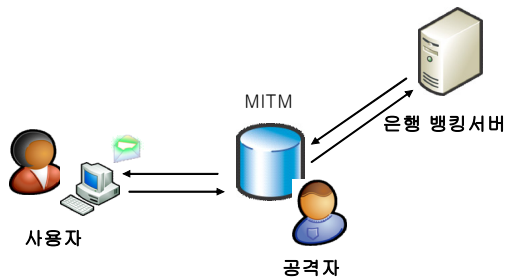
이 장에서는 OTP 통합인증센터에서 제공하는 OTP 통합인증서비스에 대한 안전성을 분석해 본다. 현재 대부분의 금융권에서는 시간동기화 방식 OTP 기기를 사용하므로 본 장에서는 시간동기화 방식에 초점을 맞춰서 OTP 통합인증에 대한 안전성을 분석한다.

3.1 MITM(Man-In-The-Middle) 공격 관련 안전성 분석

공격자가 사용자와 인터넷뱅킹서버의 중간에서 상호간이 통신을 중개하면서 사용자의 정보를 유출 또는 변조하여, 공격자가 인터넷뱅킹서버에 사용자의 신분인 것처럼 위장하는 공격기법이다. (그림 4)는 전형적인 MITM[7] 공격을 보여준다.

MITM 공격의 경우 네트워크로 전송되는 데이터 내용이 평문으로 전송되는 경우에만 가능하다.

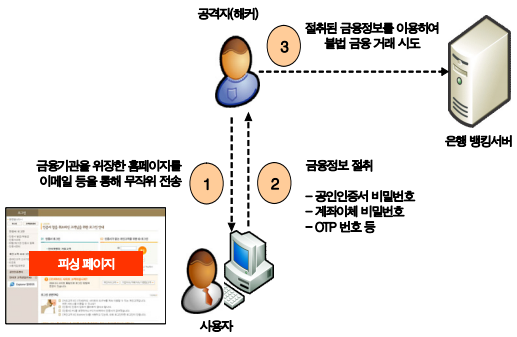
하지만 현재 모든 전자금융거래는 PKI 기반의 암호화를 통해 전송데이터가 보호되고 있으므로 MITM 공격을 시도하여도 정보를 유출 또는 변조하는 것이 불가능하다.



(그림 4) MITM 공격기법

3.2 피싱 사이트 + MITM 공격 관련 안전성 분석

공격자가 사용자의 각종 비밀번호를 절취하기 위하여 피싱 사이트를 개설한 후 이 비밀번호를 이용하여 MITM 공격을 수행하면 보다 강력한 공격기법이 된다. (그림 5)는 피싱 기법과 연계한 MITM 공격 기법을 보여준다.

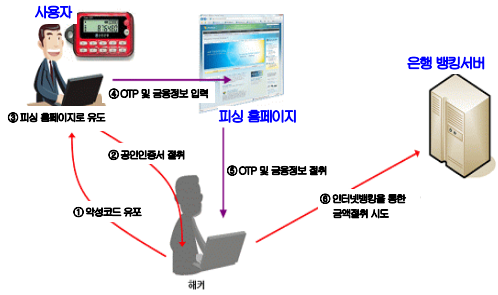


(그림 5) 피싱사이트 + MITM 공격기법

공격자가 피싱 사이트를 이용하여 전자금융거래에 필요한 각종 비밀번호와 OTP값을 알아낸 후 사용자를 가장하여 사용자의 금액을 절취하려는 공격수법 이다. 하지만 전자금융거래에서는 사용자의 각종 비밀번호와 더불어 공인인증서가 필요하다. 피싱 기법을 이용하여 각종 비밀번호와 OTP값을 획득하였다 하더라도 공인인증서가 없으므로 공격자는 공격에 성공할 수 없다.

3.3 피싱 사이트 + 공인인증서 절취 + MITM 공격 관련 안전성 분석

공격자가 사용자의 PC 해킹 등을 통하여 사용자의 공인인증서를 절취하고, 피싱 사이트 개설 후 사용자의 각종 금융 비밀정보를 알아내어, 이 정보를 이용하여 MITM 공격을 수행하면 가장 강력한 공격기법이 된다. (그림 6)은 사용자 PC 해킹 기법(공인인증서 절취), 피싱 기법, 그리고 MITM 기법을 연계한 공격 기법을 보여준다.



(그림 6) 피싱사이트 + 공인인증서 절취 + MITM 공격기법

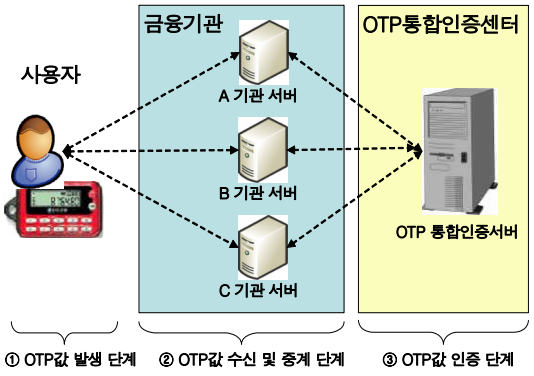
이와 같은 공격 기법은 다음의 두 가지 이유로 인해 실현이 불가능하다. 첫째, 유효한 OTP값은 기술적으로 1분마다 자동 변경되며, 공격자가 알아낸 OTP값은 1분 동안만 유효하므로 재사용이 불가능하다. 따라서 공격자가 OTP값을 알아냈다 하더라도 사용자의 OTP값이 생성된 순간부터 1분 이내에 공격을 성공하는 것은 현실적으로 불가능하다. 둘째, 금융권에서는 사용자의 PC 해킹에 대응하기 위하여 전자금융 거래시 PC 보안프로그램이 자동으로 설치되어 사용자의 PC 해킹에 대비하고 있으며, 또한 현재 피싱 공격에 대응하기 위

하여 피싱 차단리스트와 각종 피싱 대응솔루션으로 대응하고 있거나 준비하고 있으므로 이런 유형의 공격이 성공하기는 상당히 어렵다.

3.4 OTP 통합사용 관련 안전성 분석

본 절에서는 OTP 통합인증의 각 인증 단계에서 OTP값 노출시 발생 가능한 취약요소를 분석하여 OTP 통합사용에 대한 안전성을 진단한다. OTP를 통합하여 사용할 경우 인증을 처리하는 과정은 (그림 7)과 같이 3단계로 구분된다. 첫째, 1단계(OTP값 발생단계)에서의 OTP값 노출시에 대한 안전성 분석이다. 사용자가 A기관에 사용할 목적으로 발생한 OTP값을 공격자가 불법적으로 획득할 경우, 공격자가 이 OTP값을 A기관뿐 아니라 C기관에서도 사용이 가능하다는 문제이다. 이 경우 공격자는 사용자의 공인인증서와 A와 C기관의 모든 금융 비밀정보를 확보해야하며, 또한, 공격자가 OTP값을 획득하였다 하더라도 사용자가 OTP값을 입력한 순간부터 약 30초~1분 이내에 공격을 성공한다는 것은 현실적으로 불가능하다. 둘째, 2단계(OTP값 수신 및 중계단계)에서의 OTP값 노출시에 대한 안전성 분석이다. 사용자가 A기관에서 사용한 OTP값을 공격자가 불법적으로 알아내어 다른 C기관에서 사용할 경우 발생하는 문제[8]이다. 이 경우 OTP값은 원칙적으로 재사용이 금지되도록 OTP 통합인증 프로토콜이 설계되어 있으므로 인증을 처리하는 OTP 통합인증센터에서 수신한 OTP값은 전체 금융기관에서 사용이 불가능하다. A기관에서 수신한 OTP값을 OTP 통합인증센터로 전송하여 사용자를 인증하는데 소요되는 시간은 1초 이내이다. 따라서 사용자가 A기관에 제출한 OTP값을 공격자가 알아냈다 하더라도 1초 이내에 C와 같은 다른 기관에서 재사용하는 것은 불가능하다. 셋째, 3단계(OTP값 인증단계)에서의 OTP값 노출시에 대한 안전성 분석이다. 이 경우 OTP 통합인증센터에서 OTP값을 이미 수신하였으므로 공격자가 OTP값을 타 기관에 재사용하는 것은 불가능하다.

지금까지 OTP값 처리 과정을 3단계로 구분하여 OTP값 노출에 대한 안전성을 분석하였다. 1단계에서의 OTP값 노출은 위험성이 있지만, 다른 보안수단을 통하여 사고발생 가능성을 낮추고 있다. 또한, 이 문제점은 OTP를 개별적으로 사용해도 발생할 수 있는 위험성이다. 2, 3단계에서의 OTP값 노출은 타 기관에 대한 재사용 가능성이 없으므로 OTP 통합사용에 따른 취약요소는 전혀 없다. 따라서 OTP의 통합사용은 금융기관의 보안성을 하향평준화 하지 않으며, OTP 기술의 안전성을 모든 금융기관이 활용하므로 금융기관의 보안성이 상향평준화 되는 효과가 있다.



(그림 7) OTP 통합인증 개념 및 인증처리 단계

지금까지 OTP 통합인증 서비스에 대해서 발생할 수 있는 취약점을 위주로 안전성을 분석하였다. 지금부터는 OTP 통합인증 서비스에 대한 장점을 살펴본다. OTP 인증기술 자체에 대한 장점은 기존의 연구[9, 10]에서 알려져 있으므로, 본 논문에서는 전자금융에서 본인 확인을 위해 OTP를 통합하여 사용하는 OTP 통합인증 서비스에 대한 장점을 살펴본다. 첫째, 금융기관들에서 제공하는 전자금융서비스의 보안강도가 상향평준화 된다. 고객에게 발급된 OTP 기기를 공동 사용하며, OTP 인증센터를 통합적으로 운영함으로써 비용이 절감되기 때문에, 중소형 금융기관들도 OTP 도입을 적

〈표 1〉 인증처리 단계별 위험도 분석

OTP값 노출 단계	사고 발생 가능성	타기관 사용 가능성	비고
1단계	매우 낮음	있음	◦A, B, C 모든 기관에서 사용 가능 ◦하지만, 공인인증서, 금융비밀정보 등 다른 보안수단으로 필요하므로 사고 발생 가능성은 없음
2단계	없음	없음	◦이론적으로 타 기관에서 사용이 가능하지만, ◦1초 이내에 타기관에서 재사용하는 것은 불가능하므로 실제로는 A, B, C 모든 기관에서 사용 불가능
3단계	없음	없음	◦A, B, C 모든 기관에서 사용 불가능

극적으로 추진하여 사용할 수 있다. 이는 전체 금융기관에 OTP가 보편화됨으로써 전자금융 안전성이 몇몇 대형 금융기관에 편중되지 않고 전반적으로 향상되는 효과가 있다. 둘째, 전자금융 사용자의 편의성이 증대된다. 금융기관이 개별적으로 OTP를 구축한다면, 기존의 보안카드와 마찬가지로 고객들은 거래하는 금융기관별 OTP를 별도로 소지해야만 한다. 하지만, OTP 통합인증을 통해 하나의 OTP로 전 금융기관을 사용한다면, 사용자 편의성 증가로 인한 OTP 이용활성화를 기대할 수 있다. 셋째, 전문화된 통합관리로 인하여 보안이 향상된다. 보안의 통합관리는 개별관리에 비해 전문화된 인력으로 적절한 통제에 의해 관리하게 되므로 더욱 안전하며, 국가 공공의 PKI를 발급 및 관리하는 공인인증센터에서 그 사례가 있듯이 통합관리는 개별 기관의 안정성이 모두 상향되는 효과가 있다.

4. 결 론

컴퓨터와 인터넷의 보급으로 인하여 인터넷뱅킹, 홈트레이딩 시스템과 같은 전자금융거래가 활성화되어 우리 생활에 많은 혜택을 주고 있지만, 이와 동시에 컴퓨터 해킹 및 바이러스와 같은 정보화의 역기능에 대한 준비 또한 필요하게 되었다. 이와 같은 정보화 역기능에 대비하기 위하여, 금융권에서는 전자금융거래의 본인 확인을 강화하기 위하여 OTP 통합인증센터를 구축하여 사용자가 하나의 OTP를 이용하여 다수의 금융기관에 사용할 수 있는 OTP 통합인증서비스를 제공하였다. 본 논문에서는 금융권에서 제공하는 OTP 통합인증서비스에서 발생 가능한 취약점에 초점을 두고 안전성을 분석하였으며, 분석 결과 OTP 통합인증서비스가 피싱, 해킹 등의 다양한 공격기법으로부터 안전한 서비스인 것으로 확인되었다. 또한 OTP 기술은 기존의 금융권에서 제공하는 보안성을 크게 향상시키며 OTP 통합인증센터를 통한 인증서비스는 금융기관의 예산 절감 효과와 함께 사용자 편의성, 시스템 보안성, 그리고 시스템 안정성을 증대시킬 것으로 분석됐다. 향후에는 전자금융서비스의 보안 강화를 위하여 OTP를 이용한 양방향 인증을 위한 인증프로토콜 등에 대해서 추가적으로 연구를 진행할 예정이다.

참 고 문 헌

[1] 금융감독원, “전자금융 보안 종합대책”, 2005.
[2] N. Haller, “A One-Time Password Standard”, IETF RFC 1938, 1996.
[3] OATH, http://www.openauthentication.org.
[4] RSA, http://www.rsa.com.
[5] Akihiro Shimizu, “A One-Time Password Authentication Method”, Kochi University of Technology Master’s thesis, January 2003.
[6] T. Tsuji, T. Kamioka, and A. Shimizu, “Simple and secure password authentication protocol”, Ver.2 (SAS-2), IEICE Technical Report, OIS2002-30, Vol. 102, No. 314, September 2002.

[7] A. Menezes, P. Oorschot and S. Vanstone, “Handbook of applied cryptography”, CRC Press, 2001.
[8] 김기영, “일회용 패스워드를 기반으로 한 인증 시스템에 대한 고찰”, 정보보호학회지, 제17권, 제3호, 2007.
[9] Joel Dubin, “One-time password tokens : Best practices for two-factor authentication”, Information Security Magazine, 2006.
[10] FFIEC, “Authentication in an Internet Banking”, 2001.

김 인 석

1980년 홍익대학교 전자계산학과
2001년 동국대학교 국제정보 대학원 석사(이학석사)
2006년 고려대학교 정보보호 대학원 박사(수료)
현재 금융감독원 IT 감독팀장

강 형 우

1997년 고려대학교 전산과
1999년 고려대학교 전산과 석사
2006년 고려대학교 정보보호대학원 박사
1999년~2006년 ETRI 부설 국가보안기술연구소 선임연구원
현재 금융감독원 IT 감독팀 선임조사역

임 종 인

1980년 고려대학교 수학과
1982년 고려대학교 수학과 석사
1986년 고려대학교 수학과 박사
2000년 고려대학교 자연과학대학 정교수
현재 고려대학교 정보경영공학 전문대학원 원장,
고려대학교 정보보호기술 연구센터 센터장