디지털산업정보학회 논문지 제6권 제4호-2010년 12월

OTP를 이용한 인터넷뱅킹 시스템의 다중 채널 인증 기법

윤 승 구* · 박 재 표**

A Multichannel Authentication Technique In The Internet Banking System Using OTP

Yoon, Seong Gu · Park, Jae Pyo

〈Abstract〉

Due to the development of the Internet, Internet banking that we are liberated from time and space has evolved into banking system. So modern life became comfortable. However, Dysfunction (malicious Information leakage and hacking etc.) of the Internet development has become a serious social problem. According to this, The need for security is rapidly growing.

In this paper, we proposed the Internet Banking Authentication System using a dual-channel in OTP(One Time Password) authentication. This technology is that A user transfer transaction information to Bank through one Internet channel then bank transfer transaction information to user using the registered mobile phone or smart phone. If user confirm transaction information then bank request user's OTP value.

User create OTP value and transfer to bank and bank authenticate them throgth the ARS. If authentication is pass then transaction permitted.

Security assessment that the proposed system, the security requirement that the confidentiality and integrity, authentication, repudiation of all of the features provide a key length is longer than the current Internet banking systems, such as using encryption, the security provided by the Financial Supervisory Service Level 1 rating can be applied to more than confirmed.

Key Words : OTP, Authentication, Internet Banking, ARS, MultiChannel Authentication

Ⅰ. 서론

인터넷의 발달로 업무의 중심은 Off-line에서 On-line으로 옮겨가면서 금융권에서도 인터넷뱅킹이 활성화되었다. 인터넷뱅킹이란 사용자가 인터넷을 통하여 송금이나 예금 이체, 공과금 수납과 같은 은행 업무를 처리할 수 있는 것을 말한다. 이러한 인터넷뱅킹의 발달로 인하여 은행 업무를 시간·공간 등의 제약을 벗어나서 언제 어디서나 은행 업무를 볼 수 있게 되어 현대인들의 삶에 편리함을 제공해주고 있다.

그러나 해킹이나 악의적인 정보 유출과 같은 인터넷 발달의 역기능 역시 점차 다양해지면서 인터넷뱅킹 사용자들에게 심각한 불안감이 가중되어 보안에 대한 안전성 및 신뢰성에 대한 요구가 증대되고 있다. 이에 정부에서

* 숭실대학교 정보과학대학원 정보보안학과
** 숭실대학교 정보과학대학원 정보보안학과 교수(교신저자)

는 '전자금융거래 안정성강화 종합대책'을 수립하여 사용자 아이디, 비밀번호, 공인인증서와 함께 HSM을 이용한 공인인증이나 보안카드의 개선 그리고 OTP 기기를 도입하여 등급을 나누어서 금융거래의 취약점을 보완토록 하였으나 사용의 불편함 가중과 함께 근본적인 인터넷 역기능에 대한 해결책이 되지 못하고 있는 현실이다.

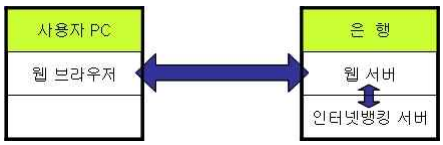
따라서 본 논문에서는 보안상의 취약점이 존재하는 기존 보안인증 체제 취약점을 해결하는 방안으로 기존에 존재하던 인증 매체들을 활용하고 추가적인 채널을 사용하여 보안이 강화된 이중채널 인증기법을 제안한다.

Ⅱ. 관련연구

2.1 인터넷뱅킹

인터넷뱅킹은 인터넷을 통해 은행 업무를 처리하는 금융시스템으로 사용자(고객)은 PC를 통해 시간과 공간의 제약 없이 인터넷에 접속하여 원하는 은행의 서비스를 이용할 수 있다.

기본적인 인터넷뱅킹 서비스는 <그림 1>과 같다.



<그림 1> 기존 인터넷뱅킹 구성도

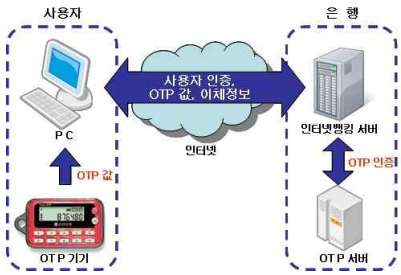
사용자PC와 은행 간에 인터넷이라는 매체를 통하여 다양한 절차를 거쳐 인증을 받아 거래가 이루어진다. 사용자가 인터넷뱅킹을 사용하기 위해서는 사전에 은행에 방문하여 통장을 개설하고 인터넷뱅킹 사용에 대한 신청을 하고 허가를 받아야 한다.

허가 과정에서 인터넷뱅킹 용도로 사용되는 비밀번호를 부여받아 보안카드 및 홈페이지의 아이디와 패스워드를 생성하고, 공인인증서도 발급받아야 한다. 은행은 사용자 정보나 거래정보를 은행들끼리 공유하고 있으나, 이 과정에서 해당 은행이 사용자에 대한 개별적 정보를 별도로 요구할 경우 사용자는 본인의 정보를 은행기관에 다시 제공해야 한다[1].

사용자는 최초 은행 홈페이지에서 접속하여 본인인증을 거쳐야 한다. 또한 서비스 요청단계로 이용하고자 하는 서비스를 실행하기 전에 시스템이 안전한지 은행에서 제공하는 보안제품으로부터 평가를 받는 과정을 거친다. 만약 이 과정(보안평가)에서 문제가 발견되면, 즉시 거래가 중지되거나 서비스 이용에 제약을 받을 수 있다.

즉 보안평가에서 문제가 없다면 은행은 이후에 서비스를 제공하게 되는데 서비스 제공에 따른 부인방지와 무결성을 위하여 다시 사용자에게 정보를 요청한다. 정보가 정확할 경우 서비스가 실행되며 실행과정이나 추가작업에 대해서는 사용자가 알 수 없다.

예를 들어 홈페이지 접속시 방화벽과 안티 바이러스 백신제품 등이 Internet Explorer의 Active X 기능을 이용하여 자동 설치되고 시스템의 이상 유무를 판단한 뒤 문제가 없다면 금융거래를 시작할 수 있다. 이때 보안제품에서 위험을 감지하거나 장애가 발생될 경우 거래가 중지되거나 더 이상 서비스를 이용할 수 없다.



<그림 2> 기존 인터넷뱅킹 개요

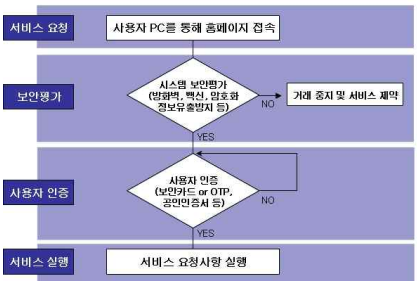
<그림 2>는 기존 인터넷뱅킹의 개요로서 사용자는 PC의 시스템에 안전도와 보안평가를 거쳐 통과 후 인터넷뱅킹 서비스를 제공받는다.

2.2 인터넷뱅킹 인증 프로세스

인터넷뱅킹에 사용하는 인증은 사용자와 은행을 동시에 인증해야하는 상호인증이다[2].

을 하고자 하는 사용자는 먼저 은행으로부터 제공된 다양한 정보를 알고 있어야 한다. 이는 사용자를 인증하기 위한 일종의 인증절차이며 은행은 이러한 절차를 통하여 허가된 사용자 인가를 판단하려 한다[3].

기존 인터넷뱅킹 인증절차는 <그림 3>과 같은 절차를 수행하고 있다.



<그림 2> 기존 인터넷뱅킹 인증절차

사용자가 서비스를 요청하기 위해서 홈페이지에 접속하면 은행은 홈페이지를 통하여 사용자가 사용하는 시스템의 보안평가를 수행하게 된다. 수행 후 보안상의 문제가 없다면 사용자가 허가된 사용자인지에 대한 정보를 요구하는데 이때 사용자는 은행이 요구하는 정보를 입력하게 된다. 제공되는 서비스는 각 은행에 따라 서비스 제공 전이나 과정에서 인증절차를 수행한다. 이 인증절차 과정에서 절차가 수행되지 않거나 문제가 발생하면 인터넷뱅킹 거래가 성립되지 않는다[4].

2.3 인터넷 뱅킹의 취약점

기존의 인터넷뱅킹은 통신하는 보안채널을 해킹하여 암호해독을 시도하거나 내부서버 및 서버 간 통신채널을 해킹하는 서버 해킹 그리고 바이러스나 웜을 사용한 사용자의 PC 해킹 그리고 가상서버로 연결하여 개인정보 수정을 유도하여 개인의 신상정보를 빼내는 피싱과 같은 취약점이 존재한다.

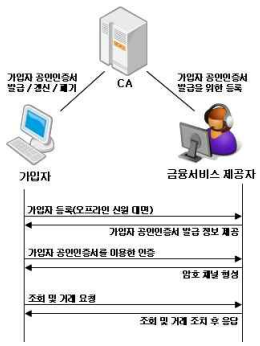
2.4 인터넷뱅킹 암호 기술

인터넷뱅킹은 웹 기반으로 이용자 등록, 인증, 조회, 거래 서비스 등 서비스들의 안전한 거래를 위해 사용자 공인인증서를 이용한 전자서명, 키 공유과정 및 암호화 채널과 같은 암호기법 등 각종 보안기술이 적용된다. 이러한 서비스는 형태에 따라 다른 암호기법을 적용한다. <표 1>은 서비스 형태에 따른 적용 암호기법이다[6].

<표 1> 인터넷뱅킹에서 사용되는 암호기법

서비스	암호 알고리즘	키길이 (bit)	Mode	패딩
인증 및 키 공유	RSA	1024	RSAES-PKCS#1(v1.5) RSAES-OAEP	
	SHA1 with RSA	1024	RSASSA-PKCS#1(v1.5)	
조회	SEED	128	CBC	PKCS#5
거래	SHA1 with RSA	1024		
	SEED	128	CBC	PKCS#5
	HMAC-SHA1			

또한 기존 사용되는 인터넷뱅킹 서비스의 흐름도는 <그림 4>와 같다.



<그림 4> 인터넷뱅킹 서비스 흐름도

2.6 OTP 인증 서비스

2.6.1 OTP의 개요

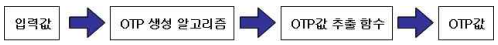
일반적인 사용자 인증방식으로 정적 패스워드를 사용해왔다. 하지만 정적 패스워드는 보통 사용자들이 기억하기 쉬운 단어들의 조합으로 이루어져있기 때문에 보안성이 낮아 추측이 쉬워 자의든 타의든 쉽게 노출될 우려가 있고, 키로거 및 스푸핑, 추측공격, 사전공격, 무차별 공격에 의하여 쉽게 공격당할 수 있는 취약성을 가진다. 그리고 이는 재사용이 가능하여 사용자에게 실질적인 피해가 가기 전까지는 해커에 의한 위험이 따르기 쉬운 불안정한 인증방식이다.

OTP(One Time Password)는 사용자가 매번 다른 비밀번호를 사하여 인증하는 일회용 비밀번호를 의미하며, 기존 사용하는 비밀번호로부터 다음번에 사용할 비밀번호를 유추하는 것이 수학적으로 불가능한 특성을 가진다[9]. OTP는 의미 있는 단어, 숫자패턴, 특정 사용자와 연관된 문자 등으로 구성돼있지 않아, 기억 가능하거나 쉽게 유추할 수 없다. 또한 매번 다른 비밀번호를 생성하는 동적인 특성을 갖기 때문에, 취득한 값을 재사용할 가능성이 희박하다. 그밖에도 PIN(Personal Identification Number)을 함께 사용하여 Two Factor 인증을 제공할 수 있기 때문에 One Factor 인증방식인 정적인 패스워드 방식에 비해 더 안전하다고 할 수 있다[7].

국내에서는 OTP 통합인증센터를 통해 2007년 6월부터 인터넷뱅킹 거래에 이를 적용하였다. 금융보안연구원에 따르면 2007년 말 기준 통합인증센터에 참여하고 있는 55개 회원사 중 45개가 서비스를 하고 있으며, 하루 평균 20만건 정도가 사용되고 있다고 한다[8].

2.6.2 OTP 생성 단계

OTP 값은 다음 <그림 5>와 같은 생성단계를 거쳐 생성된다[7].



<그림 5> OTP 생성단계

① 입력값 : OTP 생성알고리즘의 입력 데이터
- 질의·응답방식 : 질의 값, 비밀 키(서버와 OTP 기기 간에 공유된 값), 등
- 시간 동기화 방식 : 시간값, 비밀 키 등
- 이벤트 동기화 방식 : 카운터(이벤트의 횟수), 비밀 키 등
- 조합 방식 : 시간 값, 카운터, 비밀키 등

② OTP 생성알고리즘 : 입력 값으로부터 OTP 값을 생성해 내는 알고리즘으로, 일방향 해시함수(출력으로부터 입력을 유추할 수 없는 함수)와 대칭키 암호화 알고리즘(기존 블록암호 알고리즘이 사용됨)에 기반함

③ OTP 값 추출 알고리즘(Truncate 함수) : OTP 생성 알고리즘을 통해 출력된 값으로부터 실제 OTP로 사용할 OTP 값 6~8자리 숫자를 뽑아내는 알고리즘

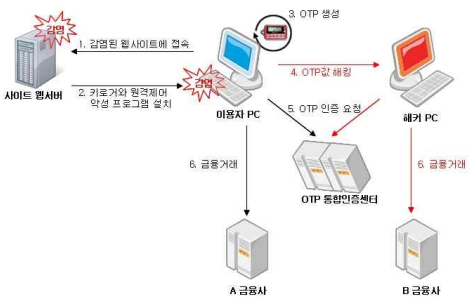
2.6.3 OTP의 보안 취약점

기존의 인터넷뱅킹 거래에서 사용했던 보안카드의 경우 항상 반복적으로 입력되는 원리이기 때문에 쉽게 노출이 되었지만 OTP의 경우에는 매번 다른 비밀번호를 생성해 내어 이러한 공격 방식들을 모두 무력화 시킨다. OTP 인증 시스템 자체에 대한 공격은 전수조사 공격을 통해 실제 사용되는 OTP 값을 얻어내는 것인데, 이는 시간적 제약이 있는 상황에서 000000~999999(6자리 OTP 값 기준)까지의 값을 대입할 수 있어야 하므로 공격 성공확률이 1/1,000,000로 이론적으로 낮다고 할 수 있다. 8자리의 OTP 값을 사용하는 경우, 이 확률은 1/100,000,000로 더 떨어지게 된다[9].

하지만 OTP 자체의 기술적 취약점을 공략하기 보다는 OTP 사용 프로세스의 가장 취약한 연결 고리인 개인 PC를 통한 해킹사고가 발생되었다. 이 방식은 피싱 사이트를 통해 OTP 키를 유출하고 중간자 공격

(Man-in-the-middle attack) 형태로 relay하여 공격하는 방법이다.

<그림 6>과 같이 해커는 사전에 사용자의 PC를 키로거 등 악성 프로그램으로 감염시킨다. 이후 사용자는 OTP 기기에서 생성한 일회용 패스워드를 OTP 통합인증센터를 통하여 입력할 것이다. 이 일회용 패스워드는 그대로 해커의 화면에 보이고, 해커는 사용자가 입력한 일회용 패스워드를 가지고 다른 금융사에 접속하여 인증을 받는 수법이다. 이는 OTP의 기술적 취약점을 찾아낸 공격이라기보다는 프로세스 전체에 걸친 취약점을 공격하는 해킹방법이다.



<그림 6> OTP 프로세스의 취약성

이처럼 날이 갈수록 해커들의 해킹수법은 점차 다양해지고 고도화되어 향후에는 인증방식의 체계를 바꾸어 인증 프로세스 자체를 강화할 개선 방안이 마련되어야 할 것이다.

Ⅲ. OTP를 이용한 보안 강화 기법

3.1 보안 강화 기법의 구성요소

3.1.1 제공자(은행) 측면의 구성요소

기존 은행에서 사용 중인 인터넷뱅킹, ARS, OTP 서버의 프로세스를 변경만으로 기존보다 보안이 강화된 인터넷뱅킹 서비스 제공할 수 있다.

1) 인터넷뱅킹 서버

인터넷뱅킹 서버는 사용자에게 웹서비스를 제공한다. 본 논문에서는 인터넷뱅킹 서버를 통하여 사용자 인증, 사용자의 인증서 인증, 거래처리 역할을 한다.

2) ARS 서버

ARS(자동응답시스템:Automatic Response System) 서버는 기존 '인터넷 뱅킹 전화승인서비스'에서 사용하는 것이지만 은행에서 사용자가 지정한 번호로 ARS가 걸려오는 것이 아니라 사용자가 ARS에게 전화를 걸도록 한다. ARS 서버는 사용자가 지정한 전화번호와 사용자 정보를 인증하고, OTP 값을 입력받아 인증을 요청하는 역할을 한다.

3) OTP 서버

OTP 값을 받아서 유효성을 확인하고 인증을 제공하기 위한 서버로 각 은행의 OTP 서버는 OTP 통합인증센터에 있는 통합인증 서버와 동기화되어 있어야 한다. 만약 은행에 별도의 OTP 인증서버가 없는 경우 OTP 값을 통합인증 서버로 보내서 인증받는다.

3.1.2 사용자(고객) 측면의 구성요소

사용자 본인만이 보유하고 있는 매체를 활용하여 사용자를 구분할 수 있으며, 사용자에 의한 요청임을 증명(부인방지)할 수 있다.

1) 개인 PC

개인 PC는 인터넷뱅킹 서비스에 접속하기 위한 수단으로 사용자는 PC를 통해 개인인증서로 암·복호화 및 전자서명을 한다.

2) OTP 생성 기기

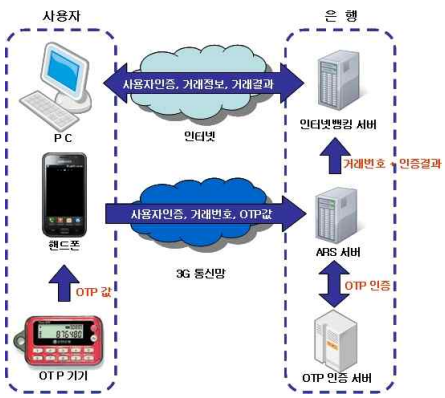
은행에서 발행한 Two Factor 인증을 제공하기 위한 인증매체로 일회용 패스워드를 생성한다.

3) 핸드폰 및 유선전화

핸드폰 및 유선전화는 사용자의 PC와는 다른 채널을 통해서 인증받는 매체로, 전화번호는 사용자를 구분하는 역할을 한다. 사용자는 인증을 위해 사용할 전화번호를 은행에 등록하고 이후 ARS에 발신된 번호를 통하여 사용자를 식별한다.

3.2 OTP를 이용한 보안 강화 기법 구조

본 논문에서는 인터넷뱅킹 환경에서 보안성이 강화된 인증기법으로 사용자의 PC에서 계좌이체 정보를 입력하고 사전에 등록된 핸드폰을 통하여 OTP 인증을 받는 이중채널 인증기법으로 다음 <그림 7>과 같다.

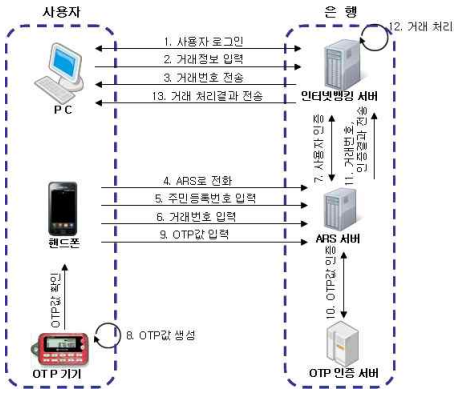


<그림 7> 제안하는 시스템의 구조

<그림 8>은 제안하는 시스템의 전체 구성도로 단계별 설명은 다음과 같다.

① 사용자 PC에서 인터넷뱅킹 웹서비스에 로그인한다.

② 사용자는 계좌이체를 하기 위하여 웹서비스에 계좌이체 정보를 입력하고 전송한다. 계좌이체 정보는 공개키 알고리즘을 이용하여 암호화하여 전송된다.



<그림 8> 제안하는 시스템의 전체 구성도

③ 은행은 사용자의 인증서에 대해 유효성을 검사하고 암호화된 정보를 복호화한다. 복호화한 계좌이체 정보를 확인하고 계좌이체 정보에 대한 거래번호를 생성하여 사용자에게 알려준다.

④ 사용자는 해당 은행의 ARS로 등록되어 있는 전화번호로 전화를 건다. (예를 들어 A은행의 ARS인증 전화번호가 '1588-1588'로 등록되어 있다면, 사용자는 은행에 등록한 핸드폰을 이용하여 '1588-1588'로 전화를 건다.)

⑤ 사용자를 확인하기 위하여 핸드폰의 버튼을 이용하여 사용자의 주민등록번호를 입력한다.

⑥ 인증받을 계좌이체 정보를 구분하기 위해서 은행에서 알려준 거래번호를 입력한다.

⑦ ARS 서버는 사용자의 핸드폰으로 걸려온 발신번호와 사용자가 입력한 주민등록번호, 거래번호를 인터넷뱅킹 서버에 전송하여 사용자인증을 한다. 거래번호와 주민등록번호를 이용하여 해당거래와 사용자를 확인하고, 주민등록번호와 발신된 전화를 비교하여 사용자가 등록한 전화번호가 맞는지 확인한다. 사용자 정보가 일치하면 'OK'값을 전송하여 ARS로 사용자에게 OTP 값을 요청하고, 일치하지 않으면 오류 카운터 값을 증가시키고 다시 인증받을 수 있도록 한다. 인증 오류 횟수에 제

한을 두어 무한으로 인증할 수 없도록 한다.

⑧ 사용자는 은행에서 인증수단으로 발급받은 OTP 기기를 이용하여 OTP 값을 생성한다.

⑨ OTP 기기에서 OTP 값을 확인한 사용자는 ARS 서버에 접속되어 있는 핸드폰으로 OTP 값을 입력한다.

ARS 서버는 입력받은 OTP 값을 OTP 서버에 전송하여, 그 값이 유효한지 인증받는다. OTP 값이 유효하면 다음단계를 진행하고 OTP 값이 틀리면 OTP 오류 카운터를 증가시키고 다시 인증을 요청한다. OTP 인증도 오류 횟수에 제한을 두어 무한으로 인증할 수 없도록 한다.

OTP 값이 인증되면 ARS 서버는 사용자에게 받은 거래번호와 OTP 인증 결과를 전송한다.

인터넷뱅킹 서버는 전송받은 거래번호와 OTP 인증결과를 확인하고, 거래번호와 일치하는 계좌이체 정보를 처리한다.

인터넷뱅킹 서버는 웹서비스에 접속해 있는 사용자에게 계좌이체 결과를 알려준다. 계좌이체 결과는 '계좌이체 완료'와 '계좌이체 실패'두 가지가 있다.

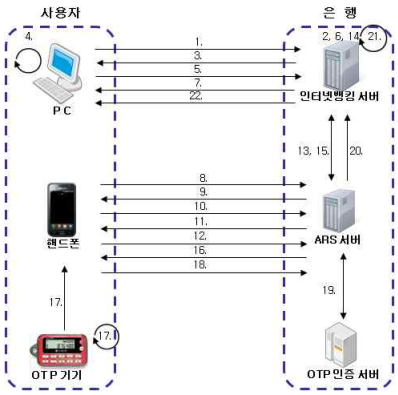
3.3 보안 강화 기법의 데이터 교환 프로토콜

본 논문에서 제안하는 방식은 기존의 인터넷뱅킹의 웹서비스를 통하여 OTP 값을 PC로 인증받는 방식에서 ARS로 인증받도록 옮겨왔다. 사용자와 ARS 서버는 사용자 인증과 OTP 인증으로 이루어진다.

<그림 9>는 제안하는 이중채널 인증방식에서 데이터 교환 프로토콜이다.

① 사용자는 인터넷뱅킹의 웹서비스에 아이디(Web-ID)와 패스워드(Web-Passwd)를 입력하여 로그인을 요청한다.
Request Login {Web-ID, Web-Passwd}

② 사용자의 아이디와 패스워드를 검증한다.
Verification {Web-ID, Web-Passwd}



<그림 9> 보안 강화 기법의 데이터 교환 프로토콜 흐름도

③ 로그인 요청에 대한 결과를 사용자에게 전송한다.
Response Login result

④ 사용자는 {자신의 계좌번호, 계좌패스워드, 입금할 계좌이체번호, 이체 금액} 정보가 들어 있는 계좌이체 정보 Transfer-Info을 대칭키(Session-Key)를 이용하여 SEED 128bit 알고리즘으로 암호화하고 대칭키는 은행의 공개키 Bank-Pub-Key을 이용하여 암호화한다. 이렇게 암호화된 계좌이체 정보 ETransfer을 생성한다.
ETransfer-Info = nvelopSession_Key(Transfer_Info)ETransfer = nvelopBank_Pub_Key(Session_Key) || Transfer_Info
계좌이체 정보의 무결성을 증명하기 위하여 암호화된 ETransfer을 사용자의 개인키 User-Pri-Key를 이용하여 서명한다.
Sig = SingUser-Pri-Key(ETransfer)

⑤ 사용자는 암호화된 계좌이체 정보와 전자서명 값, 사용자의 인증서를 인터넷뱅킹 서버에 전송한다.
Request Transaction {ETransfer || Sig || Certificate}

⑥ 은행은 사용자의 인증서에 대해 유효성을 확인하고, 인증서에서 사용자의 공개키 User-Pub-Key를 추출하

여 전자서명 값을 검증한다.

Verification CertificateVerifyUser-Pub-Key(Sig)

검증된 계좌이체 정보 ETransfer을 은행의 개인키 Bank-Pri-Key로 복호화하여 대칭키와 암호화된 정보를 추출한다.

Session-Key, ETransfer_Info = DevelopBank-Pri-Key (ETransfer)

추출한 암호화정보 ETransfer-Info는 대칭키인 Session-Key로 SEED 128bit 알고리즘을 이용하여 복호화한다.

Transfer-Info = DevelopSession-Key(ETransfer-Info)

인터넷뱅킹 서버는 복호화하여 얻는 원문정보 Transfer_Info를 유일하게 식별할 수 있는 거래번호를 생성한다.

Create Transfer-Number

⑦ 인터넷뱅킹 서버는 웹서비스를 통하여 사용자에 계좌이체 정보에 대한 거래번호 Transfer-Number를 알려주고, 사용자가 OTP 인증을 할 수 있도록 요청한다.

Send Transfer_NumberRequest OTP Authentication

⑧ 사용자는 OTP 인증을 하기 위해서 은행에 등록한 핸드폰으로 은행의 ARS 서버에 전화를 건다. ARS 서버와 연결이 되면 ARS 서버는 사용자의 발신번호 Phone-Number를 획득할 수 있다.

Call ARS (Phone-Number)

⑨ ARS는 녹음되어 있는 음성을 이용하여 사용자의 주민등록번호 RRN(Resident Registration Number)을 요청한다.

Request RRN

⑩ 사용자는 핸드폰의 키패드를 이용하여 주민등록번호를 입력한다.

Response RRN

⑪ ARS는 주민등록번호를 확인하고, 이 후 계좌이체정보를 확인할 수 있는 식별 값인 거래번호를 요청한다.

Request Transfer-Number

⑫ 사용자는 인터넷뱅킹 서버가 알려준 거래번호를 개인 PC에서 확인하고, 사용자의 핸드폰으로 입력하여 ARS 서버에 전송한다.

Response Transfer-Number

⑬ ARS 서버는 획득한 발신번호 Phone-Number와 입력받은 주민등록 번호 RRN, 거래번호 Transfer-Number를 인터넷뱅킹 서버에 전송하여 사용자 인증을 한다.

Request User Authentication {Phone-Number, RRN, Transfer-Number}

⑭ 인터넷뱅킹 서버는 거래번호 Transfer-Number에 대한 사용자를 확인하고 전송받은 주민등록번호와 매칭시킨다. 거래번호에 대한 사용자가 동일하면 발신된 Phone-Number가 사용자의 주민등록번호로 미리 등록한 번호인지 확인한다.

Verification User Authentication

⑮ 사용자 인증 결과를 ARS 서버에 전송한다. 인증 결과 값은 '인증성공'과 '인증실패'가 있다. '인증성공'은 단계 14에서 모든 인증이 정상적으로 처리되었을 때의 값이고, '인증실패'는 등록되어 있지 않은 전화번호로 발신되는 '전화번호 인증실패'와 주민등록번호와 거래번호가 매칭 되지 않는 '사용자 인증실패' 두 가지로 나뉜다.

Response User Authentication result

⑯ ARS 서버는 '인증실패' 값을 전송받으면 인증을 실패한 부분에 대해 사용자에게 다시 입력을 요청하고 '인증성공' 값을 전송받으면 OTP 값을 요청한다.

Request OTP Value

⑰ 사용자는 발급받은 OTP 기기를 이용하여 OTP 값을 생성한다.

Create OTP Value

⑱ 사용자는 OTP 값을 확인하고, ARS 서버에 연결되어 있는 핸드폰의 키패드를 이용하여 OTP값을 전송한다.

Response OTP Value

⑲ ARS 서버는 입력된 OTP 값의 인증을 요청한다.

Request OTP Authentication {OTP Value}

OTP 서버는 OTP 값에 대한 검증을 수행한다.

Verification {OTP Value}

OTP 인증 결과를 전송한다.

Response OTP Authentication result

⑳ ARS 서버는 OTP 인증결과가 '인증성공'이면 거래번호와 OTP 인증결과를 인터넷뱅킹 서버에 요청하고, 인증결과가 '인증실패'이면 사용자에게 OTP 입력을 다시 요청한다.

Send {Transfer_Number, OTP Authentication result}

㉑ 인터넷뱅킹 서버는 사용자가 OTP 값을 인증한 것을 확인하고, 거래번호 Transfer-Number로 계좌이체 정보를 확인하여 해당 계좌이체를 처리한다.

Processing Transaction

㉒ 사용자의 개인 PC로 계좌이체 처리결과를 전송한다.

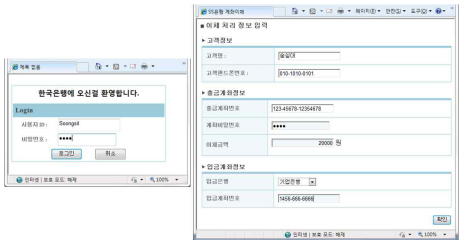
Response Transaction result

3.4 제안 시스템의 구현

제안하는 시스템의 구조는 3.2절에서 설명하였다. 핸드폰으로 OTP 값을 인증받을 때 전화통신망을 사용하도록 제안하였지만, 개인적으로 ARS 서버를 구축하는데 어려움이 있어서, 무선네트워크를 이용하여 데이터를 전송할 수 있도록 구현하였고, 실험환경은 모바일 시뮬레이터를 이용하였다. 그리고 실제 OTP 기기를 이용하여 OTP 값을 인증받기 어렵기 때문에, 개인 PC를 통하여 랜덤한 OTP 값을 생성하여 인증받도록 하였다.

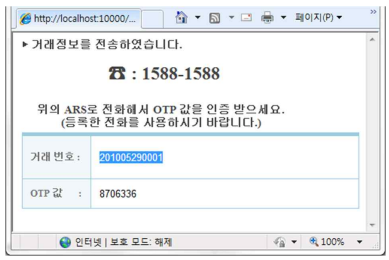
인터넷뱅킹 서버는 Windows 2003 Server 운영체제에 Apache 2.2.15 서버를 사용하였다. 인터넷뱅킹 서비스 구현은 PHP-5.2.13을 이용하였고, 핸드폰 인증은 Microsoft Visual C# 2008을 사용하였으며 데이터베이스는 MS-SQL 2008을 사용하였다. 사용자의 개인 PC는 Windows 7 Enterprise 32bit 운영 체제에서 웹브라우저 Internet Explorer를 사용하였고, 핸드폰 인증을 위해서 모바일 시뮬레이터를 이용하였다.

<그림 10>은 사용자가 웹브라우저를 통하여 인터넷뱅킹 서버에 아이디와 패스워드를 입력하여 로그인하고, 거래를 하기 위해서 계좌이체 정보를 입력한 화면이다. 계좌이체 정보 화면에서 확인버튼을 클릭하면 이체정보를 인터넷뱅킹 서버에 전송한다.



<그림 10> 인터넷뱅킹 서비스 화면

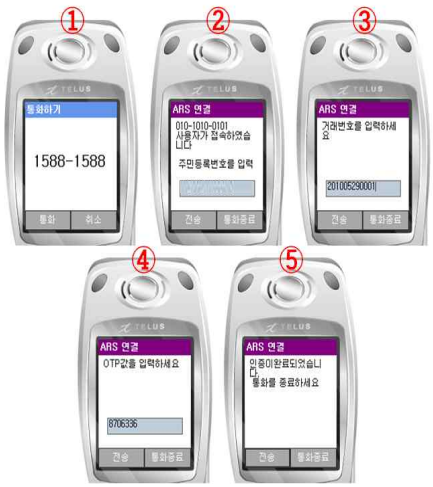
인터넷뱅킹 서버는 이체정보를 전송받고, 계좌이체에 대한 유일한 거래번호를 생성하여 사용자에게 알려준다. 실험환경에서는 실제 OTP 기기를 이용할 수 없기 때문에 거래번호를 알려줄 때 OTP값을 같이 알려주도록 하였다. <그림 11>은 거래번호와 OTP 값을 알려주는 화면이다.



<그림 11> 거래번호와 OTP 값 전송화면

<그림 12>는 사용자는 은행에 등록한 핸드폰으로 OTP 값을 인증하기 위한 과정이며 순서는 다음과 같다.

① 은행으로 전화(1588-1588)를 건다
② 본인 확인을 위한 주민등록번호 입력
③ 거래내역 확인을 위한 거래번호 입력
④ 인증을 위한 OTP 값 입력
⑤ 인증 확인을 받는다.



<그림 12> 핸드폰 인증 화면

3.5 보안 기법의 비교분석

3.5.1 필수항목에 대한 보안 평가

전자거래 금융서비스에서 보안 평가의 일반적인 요구사항인 기밀성과 무결성, 인증, 부인방지에 대해서 제안하는 시스템이 만족하는 지를 평가한다.

<표 2>는 제안하는 시스템이 제공하는 보안 요구사항을 분석하였다.

<표 2> 제안시스템의 보안 요구사항 분석

	제안 시스템
기밀성	SEED 128bit 대칭키 암호화 수행
무결성	전자서명 수행
인증	공인인증서+ ARS + OTP 다중채널 인증
부인방지	SHA256 with RSA 전자서명

제안하는 시스템은 기밀성과 무결성, 인증, 부인방지를 모두 제공하며 RSA 알고리즘에서 키 길이를 2048bit로 사용하고, 해시 알고리즘도 SHA256을 사용하여 보안 강도를 높였다.

금융감독원은 금융보안 인증요소에 따른 보안등급을 <표 3>과 같이 정의하였다.

<표 3> 거래이용 수단에 따른 보안등급

거래이용수단	보안등급
OTP발생기 + 공인인증서	1등급
HSM 방식 공인인증서 + 보안카드	
보안카드 + 공인인증서 + 이중채널 인증	
보안카드 + 공인인증서 + 핸드폰 SMS	2등급
보안카드 + 공인인증서	3등급

제안하는 시스템은 사용자의 PC에서 인증서를 이용하여 인증하고 다른 채널인 전화통신으로 OTP 인증을 하기 때문에 '공인인증서 + OTP'의 1등급 보안에 이중채널 인증까지 적용하고 있기 때문에 동일한 1등급 또는 1등급 이상으로 으로 판단할 수 있다.

4.5.2 기존 기법과 제안한 기법의 인증방식 비교분석

기존 인터넷뱅킹 서비스에서 사용하는 인증방식으로는 공인인증서와 보안카드, OTP, SMS(Short Message Service), 전화로 인증하는 이중채널 인증방식이 있다. 이러한 기존의 인터넷뱅킹 시스템의 인증방법과 제안하는 시스템에 대해서 비교하면 <표 4>과 같다.

<표 4> 기존 인터넷뱅킹의 인증방식과 비교

인증 요소	기존의 인증방식				제안 시스템
	공인 인증서	보안 카드	OTP	전화 인증	
인증할 때 입력 방식	키보드	키보드	키보드	전화 키패드	PC 키보드 핸드폰 키패드
유출 경로	PC 해킹/도난 /분실	PC 해킹/도난 /분실	PC 해킹/도난 /분실	전화 도청/도난 / 분실	PC 전화 해킹/도난/ 분실
공격 방법	키보드해킹, 원격제어, 중간자공격, 메모리해킹	키보드해킹, 패턴분석, 원격제어, 중간자공격, 메모리해킹	프로세스 취약성 이용한 공격, 메모리해킹등	전화 인증 도청, 피싱	無 유출은 가능 (공격은 불가)

그러나 공인인증서와 보안카드, OTP는 사용자의 PC에서 일반적으로 키보드를 통하여 입력한다. 이러한 방식은 개인 PC의 취약성을 이용한 해킹을 통하여 유출이 일어날 수 있다. 특히 기존에 가장 안전한 보안장치로 알려진 OTP 인증방식 역시 프로세스의 취약점을 이용한 중간자 공격과 PC의 메모리 해킹에 취약성을 보였다. 그러므로 본 논문에서 제안하는 이중채널을 이용한 인증기법은 하나의 채널이 해킹을 당해도 다른 채널의 정보가 안전하기 때문에 안전하게 거래를 할 수 있는 인증기법이다.

Ⅳ. 결론

본 논문에서는 기존의 인증매체들을 활용하여 인터넷 뱅킹 인증 시스템의 보안을 강화한 인증기법으로 사용자의 PC에서 계좌이체 정보를 입력하고 사전에 등록된 핸드폰이나 유선전화를 통하여 OTP 인증을 받는 이중채널 인증기법이다.

제안하는 시스템은 보안의 일반적인 요구사항인 기밀성과 무결성, 인증, 부인방지 기능을 제공하는지 4장에서 살펴보았다. 또한 기존 인터넷 뱅킹에서 제공하는 모든 보안기능을 제안하는 시스템에서도 제공할 수 있을 뿐 아니라, 기존 시스템보다 암호화할 때 상대적으로 긴 키를 사용함으로써 보안강도를 좀 더 높였다. 그리고 금융감독원에서 제공하는 보안등급에 따라 '공인인증서+OTP'의 1등급 보안에 +α로 이중채널 인증까지 적용하여 제공할 수 있었다.

기존 인터넷뱅킹 서비스의 인증 방식인 공인인증서, 보안카드, OTP, SMS, 이중채널 인증과 제안하는 시스템의 인증방식에 대해 취약성을 분석해 보았다. 기존의 인증방식은 개인 PC의 취약성을 이용한 해킹에 의해 유출되는 것을 확인할 수 있었고, 이에 반해 제안하는 시스템은 PC뿐 아니라 전화통신망을 이용하여 인증 받기 때문에 PC 해킹에 대해 안전성을 보였다. 그리고 전화통신망의 도청이나 피싱과 같은 해킹에 대해서도 OTP 인증을 사용함으로써 안전성을 확인하였다.

따라서 본 논문에서 제안하는 OTP를 이용한 보안 강화 기법은 기존 인증방식에 비해 보안성이 강화된 것을 확인하였으며, 향후에는 양방향 인증 거래방식을 제안하여, 기존의 전자금융거래 시스템이 일방향 거래 방식이기 때문에 드러나는 취약점을 개선하는 것이 필요할 것이다.

참고문헌

[1] 박도권, "사이버침해 위협에 관한 연구," 한양대학교 박사학위논문, 2007. 2.

[2] 이창보 · 김정재 · 박찬길 · 전문석, "Key 교환 기반의 RFID 상호 인증 프로토콜의 설계," 디지털산업정보학회논문지, 2000, pp.31-41.

[3] 이영교 · 안정희, "공인인증서를 이용한 익명 인증방법," 디지털산업정보학회논문지, 2010, pp.116-129.

[4] 김소정 · 임종인 · 오일석, "사이버범죄의 암호화된 증거 수집에 관한 연구," 한국정보보호학회논문지, 2003, pp.113-122.

[5] 금융감독원, 금융부문 암호 기술 관리 가이드, 2010.

[6] 서승형 · 강우진, "OTP 기술현황 및 국내 금융권 OTP 도입사례," 한국정보보호학회논문지, 2007, pp. 18-25.

[7] 국가정보원, 방송통신위원회, 2008 국가정보보호백서, 2008.

[8] N. Haller, "A One-Time Password Standard," IETF RFC 1938, 1996.

[9] A. J. Menezes, P. C. Oorschot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997, pp.395-397.

■ 저자소개 ■

윤 승 구
Yoon, Seong Gu

2006년 3월~ 숭실대학교 정보과학대학원 정보보안학과
2006년 2월 홍익대학교 컴퓨터정보통신학과 (공학사)

관심분야 : 컴퓨터/내트워크 보안
E-mail : koo798@nate.com

박 재 표
Park, Jae Pyo

2010년 3월~현재 숭실대학교 교수
2008년 9월~2009년 8월 숭실대학교 정보미디어기술연구소 전임연구원
2004년 8월 숭실대학교 컴퓨터학과(공학박사)
1998년 8월 숭실대학교 컴퓨터학과(공학석사)
1996년 2월 숭실대학교 컴퓨터학부(공학사)

관심분야 : 컴퓨터통신, 보안, 디지털포렌식
E-mail : pjerry@ssu.ac.kr

논문접수일 : 2010년 8월 27일
수 정 일 : 2010년 9월 15일(1차), 10월 5일(2차)
게재확정일 : 2010년 10월 27일