모바일 환경에서 OTP기술과 얼굴인식 기술을 이용한 사용자 인증 개선에 관한 연구★

허승표*, 이대성**, 김귀남*

요 약

모바일 기술의 급격한 발전으로 스마트폰 사용이 확산되고 있다. 미래의 모바일 뱅킹 시장 활성화를 위해서 무엇보다 중요하고 우선시되는 것은 안전한 금융 거래이다. 그러나, 스마트폰 확산에 비례하여 검증되지 않은 많은 앱들이 개발되고 있는 상황에서 보안 위협은 높아질 수 밖에 없다. 현재 스마트폰 금융 거래 방식은 기존 공인인증서나 OTP기술을 그대로 모바일 환경에 적용하고 있으나, 많은 보안 문제점이 꾸준히 지적되고 있다. 본 논문은 다단계 인증 방법을 통해 보안성을 강화하고 물리적 부인방지 기능을 제공함으로써 기존의 인증 방식의 보안성을 개선하고자 한다.

A Study on The Improvement of User Authentication using the Facial Recognition and OTP Technique in the Mobile Environment

Seung Pyo Huh*, Daesung Lee**, Kui Nam Kim*

ABSTRACT

With the rapid development of mobile technology the use of smartphone is spreading. In order to activate mobile banking and market in the future, the most important key is a secure financial transactoin. However, because many apps are developed without security check in proportional to the spread of smartphone, security threat is inevitably high. Current smartphone banking is processed as the way of the existing public certificate or OTP technique in the mobile environment, but many security hole about current technology is pointed out steadily. Therefore, in this paper we are to improve a existing security hole by reinforcing the security through multi-factor authentication and providing a physical non-repudiation.

Key words : User Authentication, Facial Recognition and Mobile OTP

접수일(2011년 06월 07일), 수정일(1차: 2011년 06월 17일), 게재확정일(2011년 6월 24일)

★ 본 연구는 지식경제부 지역혁신센터사업인 산업기술보호특화센터 지원으로 수행되었음.

* 경기대학교/산업보안학과

** 경기대학교/산업기술보호특화센터

1. 서 론

정보 기술과 모바일 기술의 발전으로 인하여 핸드폰과 스마트폰의 사용이 대중화 되었으며 오늘날 스마트폰의 시대라고 해도 과언이 아닌 세상이 되었다. 스마트폰의 강력한 하드웨어와 소프트웨어 기술 때문에 일반 PC에서만 사용했던 많은 응용프로그램들을 스마트폰에서 사용할 수 있게 되었으며, 스마트폰만의 특징으로 인하여 다양한 응용 콘텐츠들이 생겨나고 급속도록 증가하고 있다. 이러한 시대적 변화에 맞게 많은 금융기관에서도 스마트폰을 이용한 금융 거래(모바일 뱅킹)가 이루어질 수 있도록 다양한 기술과 응용 콘텐츠를 선보이고 있다.

한국은행이 최근 내놓은 1분기 국내 인터넷뱅킹서비스 이용현황에 따르면 올해 1분기 스마트폰 기반 모바일뱅킹 등록고객 수는 422만7000명을 기록했고 이는 전분기의 1.6배, 전년도 같은 기간의 45.5배에 이른다고 보고했다. 해당 등록고객 수는 관련 통계를 집계하기 시작한 2009년 4분기 1만3000명에서 2010년 1분기 9만3000명, 2분기 54만명, 3분기 136만9000명, 4분기 260만9000명으로 매년 큰 폭 증가했다[1].

이렇게 모바일 뱅킹 사용자는 스마트폰의 대중화로 인하여 지속적으로 증가할 것으로 예상되고 있으며, 현재 모바일 뱅킹은 단순 조회 및 간단한 이체 서비스에 머물고 있지만 스마트폰의 발전과 더불어 다양한 서비스들이 생길 것으로 예상된다.

이렇게 모바일 뱅킹은 고객에 대한 다양한 서비스와 편리성을 제공하기 때문에 많은 잠재적인 부가가치를 창출할 수 있으며, 모바일 뱅킹을 통하여 금융상품과 금융 거래를 활성화 시킬 수 있을 것으로 예상이 된다.

따라서, 현재 스마트폰을 이용한 금융 거래는 공인인증서나 금융기관에서 발행하는 사설인증서를 이용하고 있다. 인증서를 이용한 금융거래는 현존하는 금융 거래 방법 중 가장 안전한 방법으로 손꼽히고 있으며, 인증서를 통하여 인증, 기밀성, 부인방지, 무결성을 제공하기 때문에 안전한 금융 거래를 할 수 있다. 하지만, 현재 일부 연구기관이나 단체에서 인증서를 이용한 모바일 금융 거래에 대해서 몇 가지 우려의 반응과 문제점을 지적하고 있다[2].

본 연구는 기존의 공인 인증서를 사용하지 않고 모바일 OTP와 스마트폰의 카메라를 이용한 얼굴인증 기술을 이용하여 TypeII + TypeIII 인증을 제공함으로써 사용하기 편리하고 안전한 모바일 뱅킹이 이루어지도록 하는데 있다<표 1>.

<표 1> 식별과 인증 방식

구 분	기술(아이디어) 내용
TypeI	비밀번호, PIN, Passphrase, 계좌번호 등의 지식기반 인증
TypeII	스마트카드, 토큰, OTP 등의 소유기반 인증
TypeIII	홍채, 망막, 지문, 얼굴 등의 존재기반 인증
TypeIV	음성, 서명 Keystroke

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로써 국내·외 모바일 전자결제 기술과 인증 기술 현황을 조사하고 2 factor 인증 기술과 얼굴인식 인증 기술을 설명하고 분석한다. 3장에서는 모바일 뱅킹 공격에 대한 유형을 조사하고 분석하며 해당 공격에 대한 대응 방안을 설명한다. 4장에서는 본 논문이 제안하는 모바일 OTP와 얼굴인식 기술을 이용한 금융거래 사용자 인증 방법에 대해 제안하고 설명한다. 5장에서는 금융보안연구원에서 제시한 모바일OTP 보안성 분석서의 보안 검토사항과 본 논문이 제안하는 인증 체계의 분석을 통해 검증하며, 6장에서 결론을 맺는다.

2. 관련연구

2.1 다중요소(Multi Factor)를 이용한 모바일 인증 기술

2.1.1 치열영상과 음성 인증 연구

이동단말 장치에서 개인의 신원을 인증하는 수단으로 치열영상과 음성을 생체정보로 이용한 멀티모달(Multimodal) 화자인증 방법에 대한 제안 방법으로서 치

열영역을 검출하기 위하여 최근에 가장 널리 사용되는 Haar-like 특징 기반의 AdaBoost 학습 알고리즘을 사용하여 치열을 검출하고 치열영상의 특징 성분을 잘 표현하며 데이터의 중복성을 효율적으로 제거할 수 있는 2D-DCT를 치열영상의 특징 파라미터로 사용하였다. 또한 치열인증 뿐만 아니라 사용자의 음성을 이용하여 음성인증 시스템을 구성하는 연구를 제안하였다[3]. 하지만 음성인식의 단점은 항상 조용한 환경에서 인식률이 높기 때문에 소음이 발생한다면 인식률이 떨어지는 단점이 있다.

2.1.2 2차원바코드와 모바일 OTP 인증 연구

또 다른 방법으로 2차원 바코드와(QR-Code) 모바일 OTP를 이용한 온라인 뱅킹 인증 방법으로 스트림 암호 기반의 모바일 OTP와 함께 국제 및 국내 표준 2차원 바코드를 이용하여 보안카드의 항시 소지하는 불편함을 해소하고 편의성을 제공하는 인증 시스템을 제안하였다[4]. 하지만 기존 공인인증서의 사용자 인증을 수행함으로써 공인인증서가 갖고 있는 문제점을 그대로 안고 가기 때문에 앞서 지적한 형태의 문제점을 보일 수 있는 단점이 있다.

2.1.3 지문인식과 OTP 인증 연구

휴대 단말기에서 OTP를 생성하고 지문인식 기술을 이용한 2 factor 인증 연구이다. 기존 OTP Token에서 공유된 값을 생성하는 방식과 달리 단문 메시지 기반(SMS-based) OTP와 지문인식 기능을 이용한 인증 방법이다. 이 방식은 전통적인 Username/Password 비해 훨씬 안전한 방법이고 비용 절감 면에서도 최소화 할 수 있는 수단이다. 또한 지문인식기술을 함께 적용하기 때문에 사용자 인증에 있어 견고하고 보안 향상에 좀 더 강화할 수 있는 장점이 있다[5]. 생체정보 중 지문인식은 높은 인식률과 사용자의 거부감이 가장 없는 부분으로 자리 잡고 있지만 휴대 단말기에서 별도의 지문인식 장치가 필요하거나 추가적인 장치가 내장돼 있어야만 가능하다. 때문에 비용면에서 문제가 지적되고 있다.

2.1.4 모바일 폰을 이용한 두 단계 연구

모바일 폰을 사용하여 인터넷 뱅킹과 ATM기계와 같은 서비스에서 인증을 하기 위해 비 접속(Connection-less) 인증 시스템으로 서버, 클라이언트 접속 없이 OTP 생성하는 메커니즘을 제안하였고, 사용자의 신원을 확인하기 위하여 문자 메시지(SMS-based)를 통해 사용자의 고유 정보를 서버로 보내는 방법이다[6].

2.2 OTP 기술 정의 및 특징

2.2.1 비동기식 방식

비동기화 방식의 OTP는 OTP 기기와 인증 서버간에 미리 설정되어 있는 동기화 기준 정보가 없어, 인증 요청시 사용자가 직접 임의의 난수 값을 OTP 기기에 입력하여 OTP 값을 생성하는 방식을 말한다. 비동기화 방식의 대표적인 예가 질의-응답(Challenge-Response)방식이며, 금융권에서 OTP 도입 초기에 주로 사용되었다. 질의-응답 방식은 사용자가 OTP 인증 요청시 인증서버로부터 받은 질의 값을 직접 OTP 기기에 입력하여 응답 값(난수 형태)을 생성하는 방식으로, 사용자가 로그인 화면에 생성된 응답 값을 입력한다[7].

2.2.2 동기식 방식

동기화 방식의 OTP는 OTP 기기와 인증 서버 간에 미리 공유된 비밀정보와 동기화 정보에 의해 OTP 값이 생성되는 방식이다. 비동기화 방식에 비해, OTP 기기와 인증 서버 간에 반드시 동기화가 이루어져야 올바른 인증 처리가 된다는 제약점이 있으나, 사용자 입력 불편, 기존 ID/PW 어플리케이션(Application)과의 호환 어려움 등 비동기화 방식의 단점을 개선하였다. OTP 입력 값의 하나인 동기화 정보에 따라 시간 동기화(time-synchronous), 이벤트 동기화(event-synchronous), 조합 방식으로 나눌 수 있으며, OTP 입력 값으로 시간 동기화 방식은 현재시간, 공유된 비밀키 값을 받고, 이벤트 동기화 방식의 경우, 이벤트 카운터 값과 공유된 비밀키 값을, 조합방식의 경우, 시간값, 이벤트 카운트 값, 공유된 비밀키 값을 받는다[7].

(1) 시간동기화 방식

시간 동기화 방식은 서버와 OTP 기기 간에 동기화된 시간 정보를 기준으로 특정 시간간격(보통 1분)마

다 변하는 비밀번호를 생성하는 방식이다. 이 방식은 사용자의 인증요청과 상관없이 1분 간격마다 OTP값이 매번 바뀌므로, 1분 동안 입력하지 못 할경우, 중간에 패스워드가 바뀌어 다시 입력해야 하고, 실수로 OTP값을 잘못 입력하면 인증 재시도를 위해 특정 시간 동안 기다려야하는 불편이 있다. 그러나 이러한 특성은 MITM (Main-In-The-Middle)공격으로 공격자가 의미있는 OTP 값을 얻어냈다 하더라도 1분이내에 사용해야 공격에 성공할 수 있다는 제약점이 되고, 타인의 OTP 값을 기록하였다가 이후에 재사용하여 성공할 가능성이 희박하다는 점 등 보안성을 향상시킬 수 있는 장점이 된다[7].

(2) 이벤트 동기화 방식

이벤트 동기화 방식은 서버와 OTP 기기가 동일한 카운트 값을 기준으로 비밀번호를 생성하는 방식이다. 동기화 기준 값으로 사용되는 카운트 값은 현재 시간 정보와 달리, OTP 기기와 인증 서버만 알 수 있는 값이기 때문에, OTP 입력 값으로 비밀키 이외에 또 하나의 비밀정보가 입력되는 형태라 볼 수 있다. 이 방식은 OTP 값을 얻은 후, 다시 OTP 생성 요청을 할 때까지 비밀번호가 바뀌지 않기 때문에, 사용자가 입력하는데 편리한 측면은 있으나, 실수로 여러번 OTP 값을 생성시키고 나면, 서버와 OTP 기기 간에 카운트 값이 동기화되지 않아 이를 보정해야하는 문제가 있다. 또한, MITM 공격으로 공격자가 의미있는 OTP 값을 얻어냈을 경우, 혹은 타인의 OTP 값을 생성하여 기록하였을 경우, 정상적인 사용자가 다음번 인증요청을 수행하기 전까지 이를 재사용하여 공격을 성공할 수 있다. 다음번 인증요청이 즉시 이루어진다면 공격의 성공가능성이 희박하나, 그렇지 않은 경우, 성공할 가능성이 존재한다[7].

(3) 조합방식

시간 동기화 방식과 이벤트 동기화 방식의 장점을 조합하여 구성한 방식으로, 시간 동기화 중심의 조합방식과 이벤트 동기화 중심의 조합방식으로 구분된다. 시간 동기화 중심의 조합 방식은 특정 시간간격(보통24초~32초)마다 비밀번호가 다시 생성되며, 같은 시간간격 내에서 재시도시에는 카운트 값을 증가시켜서 비밀번호가 바뀌도록 하는 방식이다. 따라서 1분 동안은 생성된 OTP 값이 바뀌지 않는 시간 동기화 방식에 비해 1분 이내에도 여러번 다른 비밀번호를 생성하여 활용할 수 있다[7].

2.3 OTP 기술 정의 및 특징

최근 보안의 필요성에 대한 인식이 증대되면서 다양한 생체 인식 기술 연구가 활발히 진행되고 있다. 일상생활에서 널리 사용되고 패스워드 등 사용자가 알고 있는 정보 또는 소지하고 있는 장치를 이용한 사용자 인증 방법은 망각, 분실 또는 도난의 이유 등으로 높은 보안 성능을 제공하지 못할 수 있는 문제가 있다. 반면에 생체인식 기술은 개인별로 차이가 있는 사용자의 고유한 생체정보 또는 독특한 행동을 이용하는 것으로, 사용자가 기억하거나 소지할 필요가 없으므로 분실 및 도난 등의 문제가 전혀 없어 기존의 방법에 비해 높은 보안 성능을 제공할 수 있다[9]. 최근 전자여권에 추가된 비접촉식 IC칩을 내장한 바이오인식정보(Biometric Data)와 신원정보를 저장한 여권이 도입되었듯이 전자 정부, 전자 상거래, 정보통신 등 넓은 인프라에서 빠르게 보급되고 쓰이고 있다[8].

3. 모바일 폰 보안 위협 유형

앞으로 급속도로 확장될 모바일 인터넷 환경에서도 인터넷 침해공격, 바이러스·웜 감염, 정보유출 등 기존의 보안 위협이 재현될 수 있다. 특히, 해외의 모바일 악성코드 유포 사례를 통해 유추해 볼 때 국내의 경우도 2011년 하반기부터 금전적 이득을 노리는 스마트폰 악성코드의 출현이 예상되고 2012년부터 본격적으로 악성코드가 유포될 것으로 전망된다. 2010년 4월, 윈도 모바일 운영체제를 사용하는 스마트폰을 대상으로 국제전화 무단발신을 유발하는 모바일 악성코드가 국내에서 처음 발견되었으나, '스마트폰 정보보호 민·관 합동대응반'의 사전조치 및 신속한 대응으로 다행히 피해를 사전에 예방하였던 사례는 우리의 경각심을 일깨우기에 충분하였다. 또한, 새로운 서비스

도입에 따른 신규 보안 위협이 출현할 수 있다. 단말기기에 무선랜(Wi-Fi), 블루투스, 이동통신서비스(3G), GPS통신 등 복수의 통신기능이 기본 탑재됨에 따라 침해경로가 다변화 되고 IPTV, 클라우드 컴퓨팅 등 유선망의 신규 서비스가 무선 환경으로 이용됨에 따라 안전성을 위협하는 요인도 증가하고 있다. 또한 중요한 개인정보를 담고 있는 모바일 기기의 분실·도난 시 개인정보 노출, 사기범죄에 악용 등의 피해가 우려되고, 정품 스마트폰을 변형(예: jailbreak, rooting)할 경우 해킹에 노출될 위험성도 크다. 그 밖에도 위치기반 서비스(LBS)에 의한 개인 위치 노출 및 사생활 침해 가능성 및 모바일 단말기를 통한 불건전 정보 및 유해 사이트 접근의 위험성도 우려되고 있다[9].

이번 장에서는 모바일 보안 위협 공격 유형에 대해 분석하고 대응 할 수 있는 방법들에 대해 살펴본다.

3.1 모바일 폰 보안 위협 분석

3.1.1 정보 노출 및 손실

모바일 뱅킹은 무선 네트워크를 통해 정보를 전송한다. 무선 네트워크는 전기 신호를 이용해 데이터를 조절하고 송, 수신을 한다. 하지만 수 많은 전기 신호를 공존함에 있어 서로 간섭할 수 있다. 현재 무선 네트워크 기술은 무선 전송 미디어를 보호할 수 있는 툴이 극히 제한적이다. 때문에 뱅킹 정보는 매일 매일 거래 장치에서 누설 될 수 있고 손실 될 수 있다. 공격자는 위와 같은 허점으로 모바일 환경에서 전송되는 정보를 가로채거나 시스템에 접근하여 정보를 추가, 삭제, 수정을 함으로서 합법적으로 이용하는 사용자들에게 큰 피해를 줄 수 있다[10].

3.1.2 불완전한 정보

모바일 장치 운영 및 전송 채널의 불안정 때문에 쉽게 불완전한 통신 데이터를 야기 할 수 있다. 사용자는 통신 서비스가 좋지 않은 지역에서 모바일 서비스를 이용할 경우 서비스 지연 및 신호 간섭이이 일어남에 따라 뱅킹 거래는 쉽게 불완전한 데이터 야기하거나 데이터를 손실 시킬 수 있다[10].

3.1.3 DDoS 공격

DDoS공격은 네트워크 상의 활성 모바일 세션을 증가시킨다. 소량의 데이터를 보내 세션이 끊어지면 다시 연결하고, 연결되면 끊고 하는 공격을 반복해 RNC(radio network controller)의 혼잡을 유발하며, RNC의 과부하는 곧 일반 가입자에 대한 서비스 거부로 이어진다[10].

3.1.4 바이러스 공격

현재 모바일 운영에서 발견되는 바이러스 형태는 주로 모바일 폰 기능을 파괴함에도 불구하고 기기의 전기를 소모하고 폰의 기록 및 정보를 지우기도 한다. 모바일 뱅킹의 잠재적인 위협은 네트워크 뱅킹의 위협보다 훨씬 더 위협적이다. 바이러스는 모바일 단말기에서 무선 네트워크 단말기의 운영체제를 감염시킬 수 있을 뿐만 아니라 고정된 네트워크 단말기도 감염시킬 수 있다.또한 모바일 기기 제약에 대해 안티바이러스 소프트웨어를 쓰는 것이 어렵고 많은 무선 네트워크는 안티바이러스 예방 정책을 갖고 있지 않다. 최근 러시아에서 모바일 네트워크를 통해 확산된 컴퓨터 바이러스가 최초 발견되었다. 바이러스는 무선 네트워크를 통해 블루투스 기술에게까지 확산 시킬 수 있어 그 피해는 점점 심각해지고 있다[10].

3.1.5 크로스 플랫폼형 악성코드

모바일 단말을 통해 PC를 감염시키는 공격 유형이다. 2005년에 발생된 Cardtrap.A가 최초의 크로스 플랫폼형 악성코드로써 폰의 메모리 카드에 윈도웜을 복사하여, 감염된 폰 메모리 카드를 PC에 장착 했을 때 autorun를 통해 PC를 자동으로 감염시켜 데이터를 삭제하거나 성능을 저하시킨다. 모바일 기기간의 확산이 아닌 모바일 기기에서 PC를 감염시킨다는 점에서 새로운 형태의 공격 유형이라 할 수 있다[10].

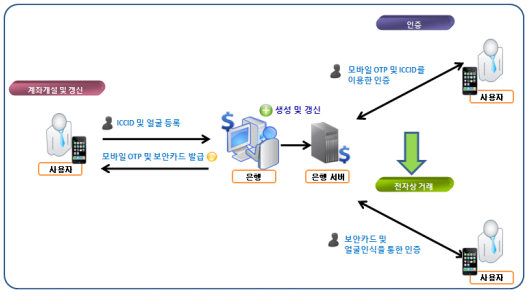
4. 모바일 OTP와 얼굴인식 기술을 이용한 금융거래 사용자 인증 방법

본 연구는 보다 세부적으로 살펴보면 기존의 은행

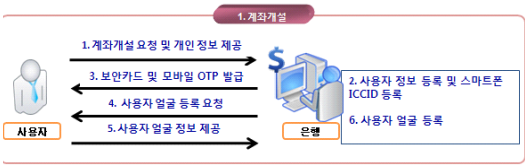
에서 제공하고 있는 인증서를 이용한 온라인 거래 방법 및 절차와 동일하게 스마트폰 사용자를 등록하고 스마트폰의 전용 소프트웨어를 제공하여 안전한 온라인 금융 거래가 가능하게 하는데 있다. 본 연구는 기존의 스마트폰 인증서를 이용한 온라인 거래와 다른 점은 인증서를 사용하지 않고 모바일OTP와 ICCID를 이용하여 사용자와 스마트폰을 인증하고, 생체인증 기술 중 하나인 얼굴인식 기술을 이용하여 실질적인 사용자를 인증하는데 있다.

4.1 사용자 등록

스마트폰을 이용하여 은행 업무를 할 경우 우선 사용자를 등록해야 한다. 사용자 등록은 스마트폰의 특성상 사용자 및 스마트폰 정보 등록, 모바일 OTP 및 보안카드 발급, 사용자 얼굴등록의 3단계로 이루어지며, 각각의 세부 단계는 (그림1)와 같다.



(그림 1) 스마트폰 전자상거래 절차

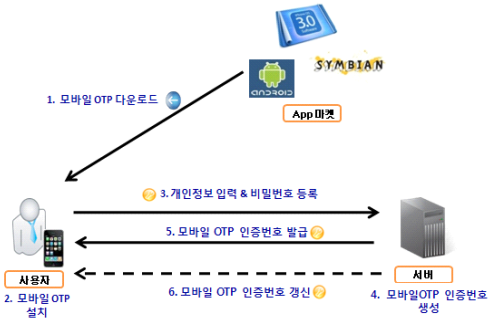


(그림 2) 사용자 계좌 개설

4.1.1 사용자 및 스마트폰 정보 등록

스마트폰 사용자는 은행에 방문을 해서 개설하고자 하는 계좌와 사용자 신상에 대한 정보를 등록한다. 스마트폰의 특성상 3G/4G나 Wi-Fi와 같은 무선 데이터를 이용하고 접속 위치가 항상 변하기 때문에 은행은 스마트폰의 기본 정보와 인증이 필요하다.

따라서 스마트폰을 인증할 수 있는 고유 정보가 필요한데, 최근의 모든 스마트폰에는 개인 사용자를 식별하고 정보를 저장할 수 있는 U-SIM 카드가 기본적으로 내장되어 있으며, U-SIM에는 고유 식별번호(ICCID)가 존재한다. ICCID라 불리는 이 번호는 USIM카드에 인쇄되어지며 이 값을 보고 국가나 이동통신 사업자를 구분하는 이동 통신사는 고객을 구분하는 데이터로 사용된다. (그림 3)과 같이 최초의 3자리는 국가코드를 나타내며, 다음 2자리는 이동 통신사코드를 나타낸다. 다음 12자리는 시리얼 번호로 일부 통신사는 좌측 두 자리를 HLR을 식별시키는데 사용하며, 20번째 자리는 체크 섬으로 사용되어진다. ICCIS는 국제표준인 ISO/iEC 7812에 근거한 번호체계로 최대 20자리가 가능하나 19자리 ID가 선호되어 사용되고 있다[11]. 이렇게 스마트폰을 은행서버에 등록하게 됨으로써 사용자가 다른 스마트폰에서 이용하지 못하도록 하는 장점이 있다.

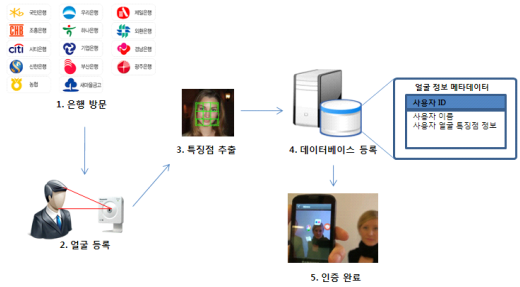


(그림 3) 모바일 OTP 인증키 발급절차

4.1.2 보안카드 발급 및 모바일OTP 발급

사용자 및 스마트폰 정보의 등록이 완료되면 은행은 스마트폰 사용자에게 모바일 OTP와 보안카드를 발급해준다. 모바일 OTP는 사용자가 스마트폰을 이용하여 은행에 접속할 때 초기 사용자 인증과 공유키(대칭키) 생성을 위해 사용되며, 보안카드는 은행 금융 거래(입출금 및 이체 등)에 사용된다. 본 연구는 언급한 모바일 OTP는 스마트폰에는 충분한 연산 처리 기능이 있기 때문에 스마트폰의 응용 어플리케이션으로 S/W PIN 방식의 모바일 OTP를 제공하며, 모바일 OTP 초기 사용에 대한 인증은 SMS 문자를 이용하여 인증한다. 보다 자세한 모바일 OTP 발급에 대한 방법은

<그림 4>와 같으며, 이러한 방법은 최근 일부 업체에서 많이 사용되고 있다[12].



(그림 4) 사용자 얼굴 인증 등록 절차

① 사용자는 모바일 OTP를 해당 기기의 스토어에서 해당은행에서 제공한 모바일 OTP 애플리케이션을 다운받는다.
② 사용자는 모바일 OTP 애플리케이션을 자신의 기기에 설치한다.
③ 사용자는 인증 서버와 인증하기 위해 개인정보 입력 및 비밀번호를 등록한다.
④ 인증 서버는 초기 모바일 OTP 사용에 대해 SMS-based 기반으로 대면인식을 통해 본인확인을 한다.
⑤ 은행 인증 서버는 사용자가 설치한 모바일OTP App에 인증번호를 발급 및 갱신한다.

4.1.3 사용자 얼굴 등록

모바일 OTP와 보안카드가 발급되면 다음으로 본 기술의 핵심으로 다음 (그림 5)와 같이 스마트폰의 사용자 얼굴을 등록한다. 은행에는 스마트폰과 동일한 화소를 가진 카메라를 통하여 사용자 얼굴을 촬영하고 사용자 얼굴 이미지를 은행 전산시스템에 등록한다. 은행 전산 시스템은 등록된 이미지를 전처리 및 얼굴 특징점 추출을 통하여 사용자의 얼굴 정보를 메타 데이터화하여 저장하며, 추후 스마트폰 사용자 얼굴 인증에 사용되도록 한다. 또한, 사용자 얼굴 이미지는 은행 서버에서 실시간으로 처리하기 때문에 사용자의 얼굴 사진 재사용에 대한 문제점을 방지 할 수 있다.

① 사용자는 사용자 등록 및 스마트폰 등록과 함께 사용자 얼굴 등록하기 위해 은행을 방문한다.
② 사용자는 자신의 스마트폰을 갖고 은행에 방문하여 별도의 얼굴 등록 서버 장치로부터 독립적으로 전송 받는다.
③,④ 스마트폰 자체에 내장된 카메라로 (해상도 640 × 480, 렌즈 35mm, Apple 아이폰4 기준) 얼굴 영상을 획득하고 얼굴 특징점(눈, 코, 입)을 추출하여 은행 DBMS에 등록 관리하게 된다.
④ 등록된 사용자 정보는 메타데이터화여 저장된다. 메타데이터는 사용자의 간단한 개인정보(ID, 사용자 이름, 얼굴특징점 정보로 구성)가 기록되고 저장된다.
⑤ 마지막으로 사용자 얼굴 인증 등록이 완료된다.

(그림 5) 비밀번호&OTP 값을 이용한 공유키(대칭키) 생성

4.2 스마트폰을 이용한 금융 거래

4.2.1 모바일OTP및 ICCID를 이용한 사용자 인증

본 연구는 초기 사용자의 스마트폰과 은행 전산시스템간의 접속이 이루어지면 사용자는 기존에 등록한 비밀번호와 모바일 OTP 기기에서 생성된 OTP 값을 입력하여 인증을 수행한다. 비밀번호와 OTP의 두 가지 비밀 값이 모두 올바른 경우에만 인증이 이루어지며, 인증이 완료되면 암호화 통신에 사용되는 공유된 공유키(대칭키)를 생성한다[7].

OTP 생성 방식은 비동기화 방식과 동기화 방식으로 나누어지며, 동기화 방식에도 시간동기화 방식, 이벤트 동기화 방식, 조합 방식으로 나누어진다. 비동기화 방식은 OTP 기기와 인증 서버 간에 미리 설정되어 있는 동기화 기준 정보가 없어, 인증 요청시 사용자가

직접 임의의 난수 값을 OTP기기에서 입력하여 OTP 값을 생성하는 방식이다. 동기화 방식의 OTP는 OTP 기기와 인증 서버 간에 미리 공유된 비밀정보와 동기화 정보에 의해 OTP 값이 생성되는 방식으로 대부분 동기화 방식을 사용하고 있다. 동기화 방식은 OTP 기기와 인증 서버간의 반드시 동기화가 되어야 올바른 인증 처리가 된다는 제약점이 있으나, 사용자 입력 불편, 기존 ID/PW 어플리케이션(Application)과의 호환 어려움 등 비동기화 방식의 단점이 개선된 방식이다. 이러한 OTP 생성 방식은 은행 및 스마트폰 환경에 알맞게 적절한 방식으로 채용하여 OTP를 생성시키면 된다. 아래 (그림 7)는 시간동기화 방식을 사용할 경우 1차 인 증시에 사용되어 지는 모바일 OTP를 이용한 초기 접속의 절차를 나타낸 것이다. 이렇게 모바일 OTP를 통하여 공유키가 생성되면 공유키와 대칭 암호 알고리즘을 이용하여 스마트폰의 ICCID를 암호화시켜 은행 전산 서버로 전송한다. 그러면 은행 전산 서버는 서버에 등록된 사용자의 ICCID와 비교를 수행한다. 비교하여 정보가 올바르면 비로소 안전한 암호화 통신 세션이 이루어지며, 그 후 스마트폰 폰을 이용하여 금융 거래를 수행할 수 있다.

(그림 6) 모바일 OTP를 이용한 인증 절차 예

4.2.2 보안카드를 이용한 인증

현재 국내에서 보편적으로 가장 많이 쓰고 있는 개인용 인터넷 뱅킹 보안 카드를 이용해 스마트폰에서도 같이 적용해 2Factor(Type Ⅰ+TypeⅡ)인증과 같이 활용함으로써 보안 안전에 안심할 수 있는 구조이다. 또한 인터넷 뱅킹에서 발견됐던 키로거 해킹으로 사용자가 보안 카드의 숫자 입력 시에 입력 값을 가로챌 수 있는 단점을 스마트폰에서는 터치 방식의 숫자를 입력하고 항시 랜덤으로 나타나는 숫자 구조이기 때문에 위치 값을 파악할 수 없는 장점이 있다.

4.2.3 얼굴인식 알고리즘을 이용한 물리적 부인 방지

본 연구는 2차 인증에서 보안카드 인증이 완료되면 최종적으로 스마트폰의 카메라를 이용하여 TypeIII의 생체 인증인 사용자 얼굴 인증을 수행한다. 얼굴 인증은 생체 정보 인식 중 가장 자연스러운 방법으로 사용자의 편의성이 뛰어나며 거부감이 없다는 장점으로 인하여 생체 인식 분양 중 적용 범위가 가장 넓고 다양하다. 얼굴 인식을 통한 인증 방법에는 다양한 접근방법과 알고리즘이 존재하지만, 일반적으로 얼굴 이미지의 특징 매칭 방법을 많이 사용하고 있다. 특징 기반 매칭 방법은 공간 특징(눈, 코, 입)을 먼저 추출한 뒤, 공간 특징들의 위치와 공간 특성(기하학과 외형)이 인식 시스템이 입력된다. 일반적으로 얼굴 인식은 특징들을 매칭 하여 정확도를 측정하는 방법으로 볼 수 있기 때문에, 순수 기하학적(Pure Geometry Methods)방법에서는 실제적인 얼굴 특징(눈, 코, 입)을 사람 얼굴의 관점과 이런 특징들을 기하학적인 관점의 설계로 정보가 구축하여 매칭 하여 활용한다.

5. 보안성 분석

인터넷 뱅킹 시스템에서 보고된 공격 사례들을 토대로 분석하고자 한다. 2006년 발생한 미국의 시티은행에서 발생된 해킹 사례로 중간자 공격(Man-in-The-Middle-Attack)이 보고되었다. 공격자는 피싱 사이트로 고객을 유도하고 고객의 중요 정보를 입력하게 하고, 탈취된 정보를 실제 시티은행 서버로 공격을 시도하였다. 중간자 공격은 중간에서 공격 대상자의 기본 정보를 입력받고 서버에 전달해서 이체를 실행시키는 기법으로써 본 연구가 제시하는 모바일 OTP인증 방법은 암호화 통신을 수행하기 때문에 중간자 공격에 대비해 안전하게 방어할 수 있다. 또한, Replay공격으로부터 OTP 및 time salt 값을 이용하기 때문에 방어가 가능하고 얼굴인식 기술을 이용하기 때문에 Cloning 공격 및 Key Substitution 공격에 강함을 보여준다.

<표 5> 제안 인증 방법의 보안성 분석

공격유형	보안성 분석
MITM 공격	OTP를 이용하여 암호화 통신을 수행하기 때문에 Man-In-the-Middle 공격에 강함
Replay 공격	OTP 및 Time salt 값을 이용하기 때문에 Replay공격에 강함
Cloning 공격	얼굴인증을 하기 때문에 Cloning 공격에 강함
Key Substitution 공격	얼굴인증을 사용하기 때문에 대리 사용 및 인증 공격에 강함

6. 결 론

최근 스마트폰 사용자가 증가함에 따라 모바일 뱅킹 수도 비례적로 늘고 있는 추세이다. 스마트폰에서 모바일 뱅킹 서비스의 다양한 인증 방법에 대한 지적이 늘고 있고 관계 부처에서는 보안성이 높고 편리성을 강조하는 연구에 중점을 두고 있다.

따라서, 본 논문은 스마트폰 등 모바일 환경에서의 안전한 금융거래를 위해서 기존의 기술(TypeⅡ)을 활용하고 TypeⅢ의 생체정보를 추가하여 2Factor 인증 서비스를 제공함으로써, 비교적 강인한 인증 방식과 유연한 접근 방식을 제시하고 있다. 스마트폰의 고유번호인 ICCID와 생체정보인 얼굴 인식 기능과의 접목으로 자신만의 유일한 데이터를 인증하기 때문에 실질적인 무결성 및 부인방지를 보장할 수 있다. 이에 따라, 현재 공인 인증서의 금융 결제 방식의 기술을 대체할 수 있는 기술 중 한가지로 기대해 볼 수 있다. 또한 사용자는 별도의 OTP를 소지하거나 공인 인증서 복사 없이 쉽게 이용할 수 있는 인증 방법에 따른 불편함을 해소하고 각 은행마다 각기 다른 기준을 따르지 않고도 유연하게 스마트폰 하나로 사용자 인증을 할 수 있는 방법을 제안한다. 또한, 사용자 생체정보인 얼굴인식기술을 이용함에 따라 제 3 자가 모바일 뱅킹을 사용할 수 없도록 부인방지를 할 수 있고 스마트폰 자체 내장돼 있는 카메라를 이용하기 때문에 결제 시스템의 비용절감 효과 및 중복 투자에 따른 손실을 미연에 방지 할 수 있다. 비단 얼굴인식 기능뿐만 아니라 다양한 생체정보를 이용할 수 있다는 것을 관련연구를 통해 알아보았고 그 중 본 연구가 제안한 얼굴인식 기능을 이용한 인증 체계는 국내 금융 거래 체계에 안전하고 새로운 인증체계로서 중추적인 역할을 할 것이다. 향후, 보완해야 할 점은 사용자의 생체정보를 이용하기 때문에 노출 된다면 심각한 개인정보침해를 초래할 수 있다. 따라서, 이에 대한 대비책 마련할 수 있도록 추가적인 심도 있는 연구가 필요하다.

참고문헌

[1] “모바일 뱅킹 시장 현황과 사용행태 분석”, http://mobizen.pe.kr/910, 2011년 3월 30일

[2] http://news.mt.co.kr/mtvview.php?no=2010011516371705850&ERV2, 2011년 4월 1일

[3] 김동주, 하길람, 홍광석, “이동환경에서 치열영상과 음성을 이용한 멀티모달 화자인증 시스템 구현”, 전자공학회논문지-CI 제45권 제5호, pp162-172, 2008년

[4] 이영실 외 4명 “Online Banking Authentication System Mobile OTP with QR-code”, ICCIT, pp644-648, Nov. 30 2010

[5] Gaizhen Yang, Fen Zhou, "Trusted Computing-Based Double Factor Authentication for Mobile Terminals", IPTC '10, pp683-685, 2010

[6] Fadi Aloul, Syed Zahidi, Wasim El-Hajj, “Multi Factor Authentication Using Mobile Phones“, International Journal of Mathematics and Computer Science, no. 2, pp65-80, 2009

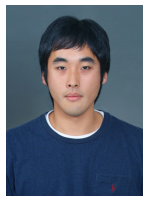
[7] 서승현, 강우진 “OTP 기술현황 및 국내 금융권 OTP 도입사례”, 정보보호학회지 제17권 제3호, pp. 18-25, 2007년 6월

[8] 외교통상부, “전자여권의 개념”, 2011년 4월 7일

[9] TTA 박철순. “스마트폰 모바일 정책 방향”, TTA

journal vol.33,
[10] Jin ,Nie and Xianling,Hu, "Mobile Banking Information Security and Protection Methods", International Conference on Computer Science and Software Engineering, pp587-590, Dec. 2008
[11] wikipedia, http://en.wikipedia.org/wiki/Subscriber_Identity_Module, 2011년 4월 15일
[12] http://www.zdnet.co.kr/news/news_view.asp?artice_id=20090305135215&type=det, 2011년 4월 16일
[13] http://www.u-otp.co.kr/blog/43, 2011년 4월 16일

[저 자 소 개]



허 승 표 (Seung-pyo Huh)

2009년 2월 남서울대학교
컴퓨터학과 학사
2011년 현재 경기대학교 산업보안
석사 과정

email : huhspunk@naver.com

이 대 성 (Dae-sung Lee)

1999년 2월 인하대학교
전자계산공학과 학사
2001년 2월 인하대학교
전자계산공학과 석사
2008년 2월 인하대학교
정보공학과 박사

email : xdillema@naver.com

김 귀 남 (Kui-nam Kim)

1989 Univ. of Kansas 수학과 학사
1993 Colorado State Univ
통계학과 석사
1994 Colorado State Univ
산업공학과 박사

email : harap@hanmail.net