스마트폰에서 Two-Factor 인증 기술을 활용한 사용자 인증 방식

박정훈, 김강석, 최옥경, 손태식, 홍만표, 예홍진
아주대학교 일반대학원 지식정보보안학과
e-mail : pjh112@ajou.ac.kr, kangskim@ajou.ac.kr, okchoi@ajou.ac.kr,
tsshon@ajou.ac.kr, mphong@ajou.ac.kr, hjyeh@ajou.ac.kr

User Authentication Method with Two-Factor Authentication Technology on Smartphone

Junghun Park, Kangseok Kim, Okkyung Choi,
Taeshik Shon, Manpyo Hong, Hongjin Yeh
Dept. of Knowledge Information Security, Graduate School of Ajou University

요 약

스마트폰의 보급으로 인해 이를 이용한 전자금융거래가 빠르게 확산되고 있다. 대부분의 금융회사가 스마트폰을 이용한 전자금융거래 서비스를 시행하고 있으며, 장소와 시간의 제약이 없는 스마트폰의 특성으로 인해 이용자 수는 계속 증가하고 있다. 그러나, 현재의 스마트폰은 전자금융거래에서 가장 중요하게 처리해야 할 인증 단계에서 보안 취약점을 보유하고 있으며, 이에 대한 보안 대책 기술이 강력하게 마련되지 못하고 있는 실정이다. 따라서 본 연구에서는 기존 연구가 가지고 있는 인증 방식의 취약점을 보안하기 위해 2팩터 인증기술과 인증 이미지 사진의 GPS정보를 활용하여 본인 인증 절차를 강화시키고, 전자금융거래에서 부인방지 기능을 제공한다. 또한, 단계별 시나리오 및 설계 방안을 제시하고 이를 바탕으로 보안 모듈을 설계 및 구현하여 연구의 효율성 및 타당성을 증명해 보이고자 한다.

1. 서론

전자금융거래란 금융기관 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고, 이용자가 금융기관 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 않으면서 현금자동지급기, 컴퓨터, 전화기 등 자동화된 방식으로 이를 이용하는 거래를 말한다[1]. 2007년 시행된 전자금융거래법 제 9조는 접근매체의 위·변조, 해킹 등으로 전자금융 사고 발생 시 금융기관 등이 이용자의 고의·중과실을 입증하지 못하는 경우 금융기관이 책임을 부담하게 하는 등 전자금융거래 이용자를 보호하기 위한 조치가 크게 강화되었다[2].

스마트폰 이용자 수의 증가로 인해 스마트폰 전자금융거래 환경이 신속하게 조성되고 있지만, 현재 전자금융거래 법제도가 PC에 국한되는 기준을 적용하고 있기 때문에 PC와는 다른 특성을 지닌 스마트폰이라는 새로운 전자금융거래 매체에 대해 현행의 전자금융거래 법제도를 그대로 적용시키려면 사회적으로 많은 문제점이 나타날 것이다. 따라서 근본적인 스마트폰 전자금융거래 보안 대책이 요구되고 있으며 보안 인증 기술에 대한 체계적이고 강화된 방식의 개발이 시급한 실정이다[3].

또한, 인증기술의 특성으로, 국내 전자금융에 새로운 인증기술을 도입하기 위한 기술적 요건으로 사용자인증, 전자금융서버의 인증, 거래내역에 대한 무결성 기능, 전자금융 이용사실에 대해 부인방지기능을 제공하여야 하며, 추가적으로 전송구간의 암호화 기능이 제공되어야 한다[4].

본 연구에서는 기존 전자 금융 인증 기술의 적용 현황을 알아보고, 보안 검토 사항을 고려하여 전자금융에 적용 가능한 인증기술을 제안하고자 한다. 제안하는 인증기술의 핵심은 2팩터 인증기술과 인증 이미지 사진의 GPS정보를 활용하여 강력한 본인인증과 함께 전자금융거래에서 부인방지 기능을 제공한다. 또한, 인증기술의 효율성과 타당성을 증명해 보이기 위해 보안 모듈을 직접 설계 및 구현하였다.

2. 관련 연구

2.1 인증기술 분류

전자금융에 사용할 수 있는 인증기술을 인증 팩터(Authentication factor) 관점으로 분류한다면, <표 1>과 같이 '지식기반'(What you know), '소지기반' (What you have), '특징기반'(What you are)으로 분류하는 것이 일반적이다.

이밖에도 개인 간의 비밀번호 입력패턴 차이, 전자적인 서명필체 등을 이용하는 인증 팩터를 '행동기반'(What you do)으로 분류하기도 하며, 사용자의 전자금융 이용패턴, 이용위치 등 사용자의 알려진 사실에 기반 한 인증 팩터를 '알려진 사실기반'(What known about you)으로 세분화하여 분류하기도 하지만 아직까지는 일부에서만 적용하여 분류하고 있다[5].

<표 1> 인증 수단의 분류

분류	지식기반 (what you know)	소유기반 (what you have)	특징기반 (what you are)
내용	사용자가 알고 있는 지식 기반	사용자가 소지 하고 있는 인증매체 기반	바이오정보를 이용
종류	비밀번호, PIN번호, 사전 등록된 질의응답방식 등	OTP발생기, HSM, 휴대폰, 보안카드, 스마트카드 등	지문, 홍채, 얼굴, 음성 등
장점	- 별도의 HW/SW 필요 없음 (저비용) - 사용, 변경, 대체 용이 - 고객의 거부감 적음	- 사용, 변경, 대체용이 - 복제, 수정이 어려워 비교적 안전	- 정확한 본인인증 - 도난, 분실, 수정 등의 위험이 없음 - 사용이 편리
단점	- 해킹에 취약 - 명의 도용이 간단 - 개개인의 기억력에 크게 의존	- 도난, 분실 위험 - 추가기기 휴대의 번거로움으로 고객 거부감 유발	- HW/SW가 필요하여 도입 비용 높음 - 생체정보 저장에 따른 프라이버시 문제로 고객 거부감

이들 중 하나의 요소만 이용하는 단일 인증은 보안에 매우 취약한 편이다. 패스워드 등 자신이 아는 정보만을 사용할 경우 분실 여부를 인지하기 어려우며, 토큰, 키 등 자신이 소유한 것만을 사용할 경우 분실 시 습득자의 즉각적인 사용이 가능하다. 따라서 이러한 단일 인증의 보안 취약성을 보강하기 위하여 이들 중 서로 다른 2개의 인증을 조합하여 채택한 방식이 이중 인증 즉, 2팩터 인증이다.

- **공인인증서** : 전자금융 거래 시 거래 당사자인 사용자의 신원확인 기능, 거래 내역에 대한 위·변조 방지, 거래사실의 부인 방지 등의 목적으로 신뢰된 공인인증기관이 발행하는 전자적 정보로서, 일종의 전자금융거래용 인감 증명서이다.

- **OTP발생기** : 인터넷, 휴대폰, 전화 등을 다양한 매체를 이용하여 은행, 증권, 선물사의 전자금융 거래 시에 고정된 비밀번호 대신 사용되는 매번 새롭게 바뀌는 비밀번호이다.

- **보안카드** : 35개 이내의 난수가 적혀진 카드로, 전자금융 거래 시 사용자가 카드에 인쇄된 번호를 직접 입력하고, 응답번호와 일치여부를 판단하여 전자금융거래를 수행한다.

- **HSM (Hardware Security Module)** : 전자서명 생성키 등 비밀정보를 안전하게 저장·보관 및 키 생성, 전자서명 생성 등이 기기 내부에서 처리되도록 구현된 스마트칩을 내장한 하드웨어 모듈로 휴대가 가능한 인증서 보안기술이다.

- **2채널인증** : OTP발생기, HSM방식 공인인증서와 같이 1등급 보안매체로 분류되는 2채널인증은 전자금융거래 채널 이외에 거래승인을 위한 채널을 분리하여 이용하는 기술이다.

- **휴대폰 SMS (거래내역통보)** : 인터넷뱅킹, 텔레뱅킹 등의 전자금융 서비스를 이용한 자금이체내역을 휴대폰으로 통지하는 서비스이다.

- **바이오인증** : 현재 금융 거래 시 비밀번호와 사진이 있는 ID로 본인 확인을 하는 것 대신에 금융 거래 시 지문 인식, 눈동자 확인 등 생체적인 본인입증 자료를 토대로 금융거래에 대한 인증을 하는 것이다.

2.2 국내 전자금융 인증기술 적용 현황

국내 전자금융 현황을 살펴보면 2008년 4월 발표된 보안등급별 이체한도 차등화 정책에 따라 전자금융거래의 안전성 강화를 위하여 인터넷뱅킹이나 텔레뱅킹 이용 시 거래수단별로 보안등급을 부여하고, 부여된 보안 등급에 따라 이체한도를 적용하고 있다.

<표 2>에서 보듯이 보안등급은 총 3개의 등급으로 분류되며 공인인증서와 일회용 비밀번호(보안카드 포함)를 사용해야 하며, 조합되는 인증수단에 따라 등급을 구분하고 있다. 보안 1등급으로 OTP발생기, HSM, 2채널인증이 사용되고, 2등급으로는 휴대폰 SMS(거래내역통보), 그리고 보안카드는 3등급으로 분류된다.

기업, 법인의 경우에는 1등급 보안매체를 사용해야 하는 대상으로 분류되어 반드시 OTP등을 사용해야 한다. 개인은 보안 2·3등급의 보안매체를 사용해도 되지만 이체한도와 보안성이 떨어지게 된다.

<표 2> 전자자금이체한도별 거래이용수단
(전자금융감독규정, '08.07.31)

거래이용수단	보안등급
OTP발생기 + 공인인증서	1등급
HSM 방식 공인인증서 + 보안카드	
보안카드 + 공인인증서 + 2 channel 인증*	
보안카드 + 공인인증서 + 휴대폰 SMS (거래내역통보)	2등급
보안카드 + 공인인증서	3등급

* 2 channel 인증 : 두 개의 서로 다른 통신경로 (예, 인터넷과 전화, 전화와 FAX)를 이용하여 본인을 인정하는 방식

3. 설계 방안 및 구현

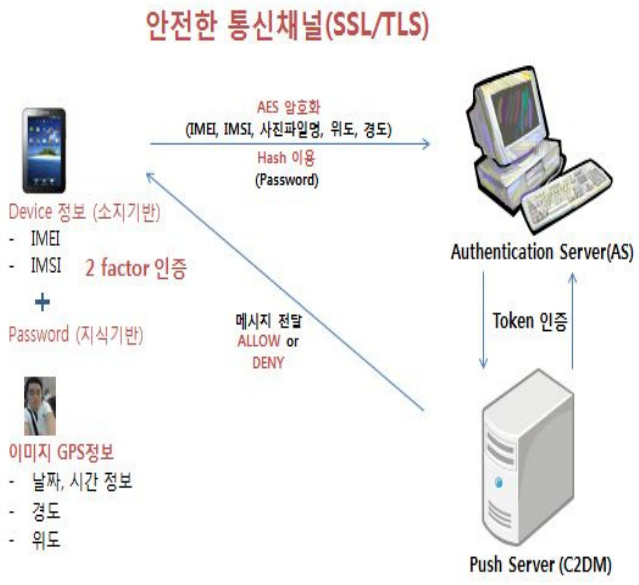
3.1 설계 방안

자신이 가진 스마트폰에는 기기에 대한 IMEI넘버가 존재한다. IMEI(International Mobile Equipment Identity)는 제조사가 전 세계의 수많은 휴대전화를 구별하기 위해 만든 휴대전화의 고유번호이며, 제조사, 제조 시기별로 만들어지는 규칙이 있으며 개인이 인위적으로 바꾸지 않는 이상 IMEI넘버가 겹치는 기기는 없을 것이다[6].

IMSI(International Mobile Subscriber Identity)는 GSM 서비스 가입 시에 이동 단말기에 할당되는 고유 15자리 식별번호로써, 이 번호는 이동 국가 코드, 이동 네트워크 코드, 이동 가입자 식별번호 및 국가 이동가입자 식별 번호로 구성된다[7].

로그인을 할 때 사용자 인증은 IMEI와 IMSI는 사용자가 소지하고 있는 Device정보를 나타내주므로 '소지기반'(What you have)팩터와 사용자 본인만이 알고 있는 Password는 '지식기반'(What you know)팩터의 결합으로 2팩터 인증을 이용한다.

로그인 이전 가입을 할 때 IMSI를 이용한 ID란에는 이동 가입자 식별자 번호를 디폴트로 설정하고, 비밀번호를 입력 후 이메일 인증을 통해 Authentication Server에 사용자 등록을 한다. AS는 사용자가 입력한 이메일 주소로 인증 번호를 보내는데 인증 번호는 난수 생성 알고리즘을 이용해서 사용한다. 사용자는 난수 입력을 하고 난 후 로그인 화면에서 비밀번호 입력과 함께 본인의 이미지 사진을 찍어서 로그인을 한다. 본인의 이미지 사진에는 지금 현재 있는 위치 즉, GPS정보가 들어있는데 그 정보의 사진 파일은 현재 사진이 찍힌 날짜, 시간이 나오며 위도, 경도가 표시되면서 구글맵을 이용하여 본인의 위치를 나타낼 수 있기 때문에 전자금융거래에서 부인방지 기능을 한다. (그림 1)은 제안방식의 전체적인 구성을 보여준다.

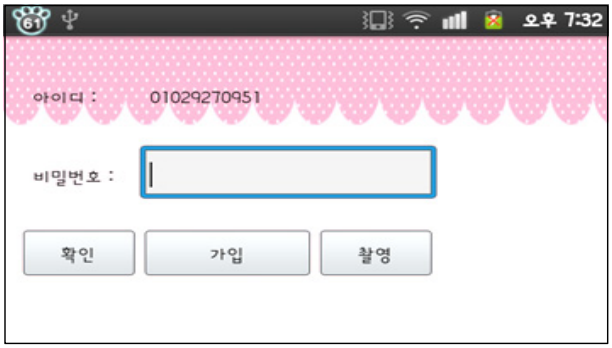


(그림 1) 제안방식

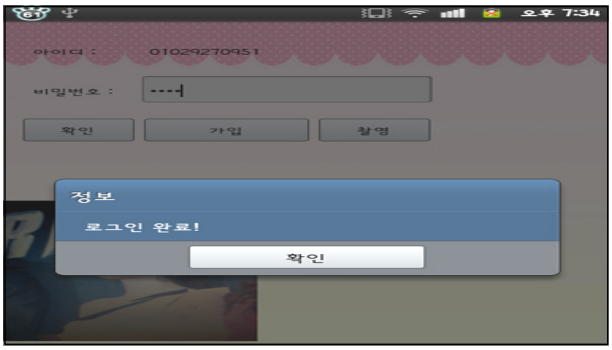
3.2 구현

3.2.1 App 구현

(그림 2)에서 ID부분은 USIM칩을 통한 IMSI값 중 핸드폰 번호를 추출하여 Default로 설정하고, 회원가입은 회원정보 목록을 모두 채우고, Email 확인버튼을 누르게 되면 서버에서 생성된 난수를 사용자 인증을 위해 SMTP메일 서버를 통해 발송 하게 된다. 메일 서버로부터 전송 받은 난수를 복사하여 붙여 넣어 확인 버튼을 누르게 되면 서버에서는 이 난수 값을 비교하여 같을 경우 인증에 성공하여 정상적으로 회원가입을 완료할 수 있게 된다. 그리고 로그인 시 비밀번호 또는 사진이 없을 경우 해당 정보를 입력하라는 경고 창을 띄우도록 한다. (그림 3)은 비밀번호와 얼굴을 정확히 입력을 하게 되면 로그인이 성공적으로 이루어진다. 촬영된 얼굴이미지는 DB에 저장되면서 스마트폰에서는 자동 삭제된다.



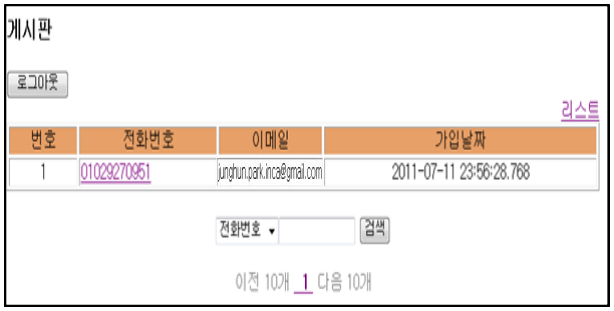
(그림 2) 로그인



(그림 3) 완료

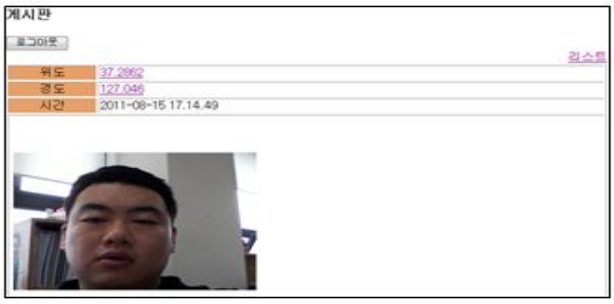
3.2.2 관리자 페이지 구현

관리자 페이지는 관리자만 로그인이 가능하다. 관리자 아이디 / 비밀번호 입력하면 (그림 4)처럼 가입된 사용자들의 리스트를 보여주는 화면이 보이며, 전화번호와 이메일로 검색 가능하다. 그리고 전화번호 링크를 클릭하면 (그림 5)와 같이 특정 사용자(T01029270951)의 로그인 리스트를 보여준다. 시간 링크를 클릭하면 (그림 6)처럼 로그인 리스트 중 하나의 사진파일 보기가 가능하며, 위도 또는 경도 링크를 클릭하면 (그림 7)과 같이 사진이 찍힌 로그인 위치를 표시한다.



(그림 4) 사용자 리스트

(그림 5) 특정 사용자 로그인 리스트



(그림 6) 파일보기

(그림 7) 로그인 위치 표시

4. 결론

스마트폰은 기존의 휴대전화와는 다른 PC급 성능을 보유한 전화기로 기존의 모바일 금융거래에 비해 높은 보안 위협이 존재하는 것이 사실이다. 따라서 스마트폰 기반의 모바일 금융에서는 기존 PC에서 제공돼 왔던 금융거래 수준 이상의 보안 대책이 필요하다. 그러나 보안등급 1 ~ 3등급을 보면 OTP발생기 + 공인인증서, HSM방식 공인인증서 + 보안카드, 보안카드 + 공인인증서 + 2채널인증을 사용한 1등급 매체라 하더라도 부인방지 기능을 하지 못한다.

본 논문에서 제안한 방식은 스마트폰에서 IMEI, IMSI를 이용한 '소지기반' 팩터를 사용한다. 대부분 '소지기반' 팩터는 HSM이나 OTP발생기를 이용하는데 반해 제안 방법에서는 적용성, 편의성, 보안성 측면을 고려하여 스마트폰 자체를 '소지기반' 팩터로 이용한다. 또한, 전자금융 거래에서 중요한 부인방지 기능을 이미지 GPS정보를 이용하여 위도, 경도를 통해 자신이 로그인한 위치를 DB에 저장하고, 구글맵을 통해 나타냄으로써 부인방지 기능을 가정보에 대한 이슈가 남아 있기 때문에 위치 정보 수집에 있어서 미리 사용자의 동의를 구해야한다.

스마트폰은 최신의 IT기술들이 결합된 휴대전화 기기로써 IT기술 발전과 소비자 요구의 변화로 인해 다양한 형태로 변화될 수 있으며, 소비자들에게 보다 널리 보급될 경우 금융 거래에 있어서 새로운 형태의 보안위협이 발생할 수 있으므로, 향후 예상되는 보안 취약점을 모니터링하여 스마트폰 보안위협에 범 금융권이 공동으로 대응하는 것이 필요하다. 또한, 전자금융 인증기술은 적용성, 편의성, 보안성을 갖추어야 한다.

향후 연구 계획으로는 GPS정보만을 저장한 이미지가 아닌 얼굴매칭알고리즘을 적용해서 GPS정보뿐만 아니라 DB에 가입할 경우, 저장한 이미지를 인증 할 때 처음 이미지랑 현재 이미지랑 매칭 시켜 어느 정도 이상의 일치도가 나오면 사용자 인증을 할 수 있게 만들 예정이다. 또한, GPS같은 경우 건물 실내 또는 지하에서 안 잡히는 경우도 있기 때문에 네트워크 기반 서비스로 이동통신 중계기 및 주변 무선 공유기 AP들을 이용해서 사용자의 위치를 정확히 찾아낼 수 있는 방안을 연구할 것이다.

참고문헌

[1] 곽창규, "전자금융 新인증기술 연구보고서", 103page, 금융보안연구원, 2011.01.

[2] 김보라, "비대면 지급결제서비스에서의 본인인증수단 현황과 전망", 27page, 금융결제원, 2009.04.

[3] 금융감독원, "10. 3월말 현재 스마트폰 전자금융 서비스 현황 및 향후 제공계획", 금융감독원 보도자료, 2010.04.

[4] 금융보안연구원, "전자금융 이용자 보안가이드", 2007.10.

[5] CA technologies, Managing Strong Authentication: A Guide to Creating an Effective Management System, 2007.

[6] Fadi Aloul, Syed Zahidi, Wassim El-Hajj, "Two factor authentication using mobile phones," aiccsa, pp.641-644, 2009.

[7] Fadi Aloul, Syed Zahidi, and Wassim El-Hajj, "Multi Factor Authentication Using Mobile Phones", International Journal of Mathematics and Computer Science, vol. 4, no. 2, pages 65-80, 2009.