Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.4, Aug. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.4.843

모바일 핀테크 서비스에서 이용 가능한 인증 수단의 사용성, 안전성 분석 연구*

김 경 훈,† 권 태 경‡
연세대학교 정보보호 연구실

Usability and Security Analysis of Authentication Methods for Mobile Fin-Tech Services*

KyoungHoon Kim,† Taekyoung Kwon‡
Information Security Lab., Graduation School of Information, Yonsei University

요 약

"공인인증서 의무 사용" 폐지에 따라 모바일 기반 금융 서비스의 자율성이 높아지면서 다양한 인증 수단이 제공되고 있다. 대표적인 인증 수단으로는 SMS, ARS, PIN, 텍스트 패스워드, 지문 등이 있다. 본 연구에서는 통일된 모바일 환경에서 인증수단의 사용성, 안전성을 분석하였다. 사용성 평가에 있어서 SUS (System Usability Scale), 인터뷰를 통해 평가를 진행하였으며, NIST에서 제시한 전자인증가이드라인을 이용하여 각 인증 수단에 대한 안전성을 평가하였다. 연구 결과 지문 인식 기반 인증 수단이 가장 높은 사용성 등급을 나타내는 Excellent로 평가되었으며, 안전성 분석 결과에서도 지문 인식 기반 인증 수단이 Security Level 4를 획득하여 가장 안전한 인증 수단으로 평가되었다.

ABSTRACT

In the case of electronic payment, the obligation to use the certificate-based authentication was abolished. As Fin-tech service providers gain autonomy, various authentication methods are provided. SMS, ARS, PIN, Text-passwords, Fingerprints are popular authentication methods in the mobile Fin-tech services. In this study evaluate the usability and security of authentication methods in a unified mobile environment. We evaluate the usability through SUS and interview. Also we evaluate the security level of authentication methods through NIST guideline. At the result of the usability evaluation, Fingerprint authentication method had been determined as the highest usability, also Fingerprint authentication method had been determined as the safest authentication method by obtaining Security Level 4.

Keywords: Fin-tech, Authentication, Usability, Security.

I. 서 론

오늘날 스마트 폰, 웨어러블 기기 보급이 확산됨과 동시에 금융 서비스도 다양한 결제 환경 변화가 이루어지고 있다. 스마트 폰 보급률이 80%를 넘음에 따라[9], 금융 서비스 이용자들은 모바일 기기에 대한 의존도가 높아지고 있다. 보급률 상승과 더불어 2014년 5월 〈전자금융감독규정 시행세칙〉에서는 30만원이상 전자결제 시 '공인인증서 등'의 의무사용 규정을 폐지하여, 금융 서비스 제공자의 자율성에 의해 자연스럽게 모바일 핀테크 기반의 다양한 서비스가 출시되고 있다.

모바일 핀테크 서비스에서 중요한 핵심인 인증 수

Received (02. 28. 2017), Modified (05. 30. 2017), Accepted(05. 30. 2017)
* "본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2017-2012-0-00646)
† 주저자, rickyboss@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac..kr(Corresponding author)

단은 금융 서비스에서 본인 확인, 거래 부인 방지, 데이터 무결성 확보, 기밀성 확보 등 신뢰성과 안전성을 담보하는 중요한 역할을 하고 있다. 인증 수단으로는 SMS 본인 인증, ARS 인증, 지문 인증, PIN 인증, 비밀번호 인증, 목소리 인증 등이 있다. 다양한 인증 수단이 제공되고 있는 환경에서 각 인증 수단에 대한 사용성, 안전성 분석이 필요한 시점이다. 본 논문은 다음과 같은 공헌을 한다.

- 모바일 기반 인증 수단의 다양성을 반영한다.
- 현재 활발히 사용되고 있는 주(主) 인증 수단에 대한 분석에 의의가 있다.
- 인증수단 서비스 제공자들에게 실무적 의의를 제공할 수 있다.

II. 연구 배경 및 관련 연구

2.1 연구 배경

핀테크(Fin-tech)는 금융(Finance)과 기술(Tech nology)이 결합한 서비스를 의미한다. 핀테크 서비스는 송금, 결제, 크라우드 펀딩, P2P 대출 등 다양한 형태로 우리 주변에 존재하고 있다. 국내외 적으로 금융업과 더불어 기기 제조사, SNS 등 다양한 산업이 핀테크 서비스에 참여하고 있다. 이들 중 모바일 디바이스 기반 인증을 통한 모바일 간편 결제에 대한 동향을 분석한다. 간편 결제 서비스는 본인 명의의 신용카드/체크카드, 계좌, 휴대폰 결제 정보를 어플리케이션을 통해 인증 절차를 완료한 후, 이용하는 서비스이다.

국내의 대표적으로, 삼성페이, 카카오페이, 네이버 페이가 존재한다.

- 삼성페이 : 2015년부터 개시된 서비스로, MST 바코드 방식뿐만 아니라 근거리 무선통신을 통해 사용자들이 편리하게 사용할 수 있는 서비스이다. 결제 인증은 본인의 지문을 이용하여 가능하며, 설정에 따라 비밀번호로도 이용가능하다.
- 카카오페이 : 2014년에 출시한 간편 결제로, 카카오톡 플랫폼을 이용하기 때문에 어플리케이션 설치 없이 이용할 수 있는 편리성이 존재한다. 기존 SNS 플랫폼을 이용하여 빠르게 성장이 가능하다는 특징을 가지고 있고, 결제 인증은 6자리 PIN 번호 입력을 통해 가능하다.
- 네이버 페이 : 웹 포털 서비스가 추진한 서비스로, 2015년에 출시하여, 이미 확보된 가맹점이 네이버 페이의 강점이다. 네이버 아이디를 이용하여 간편하게 결제가 가능한 장점을 가지고 있고, 6자리 PIN 번호 입력을 통해 인증이 가능하다.

국외의 대표적으로, 애플페이, 알리페이 페이팔이 존재한다.

- 애플페이 : 2014년 아이폰 6를 발표하면서, NFC의 탑재와 함께 지문인식 인증 기능을 탑재하면서 출시되었다. 이미 아이튠스에 저장되어 있는 카드 정보를 이용하여 금융 서비스를 이용하는 특징이 있다.
- 알리페이 : 알리바바 전자상거래 서비스에서 출시한 서비스로, 인행 계좌, 신용카드를 연동하여 이용가능한 모바일 간편 결제이다. 충전 계좌를 이용하여 자금 이용이 편리해지면서 충전율이 늘어나고, 전자화폐로 인정받는 특징이 있다.
- 페이팔 : 페이팔 계정을 사용해 대금 결제나 송금을 할 수 있다. 선불 형태의 계좌 혹은 신용카드 등록을 통해 이용할 수 있으며, 온/오프라인과 더불어 기존 금융 서비스 영역에서 모두 사용 가능한 특징이 있다.

국내외 적으로 다양한 형태의 핀테크 서비스가 있음과 동시에 금융 서비스 전문 회사가 아닌 플랫폼 지원이 가능한 서비스업에서도 금융 서비스에 활발히 발을 들이고 있음을 알 수 있다. 이를 통해 앞으로 핀테크 서비스에서는 다양한 플랫폼과 방법을 이용하여 다양한 서비스가 출시 될 것으로 예상할 수 있다. 이와 더불어, IoT, 스마트 기기가 많이 출시가 예상됨에 따라 기기 특성에 따라 인증 수단의 다양화도 예상해 볼 수 있다.

2.2 관련연구

2015년 Micallef 등의 연구에서는 모바일 환경에서 PIN 인증과 텍스트 패스워드 인증에 대한 연구를 진행하였다 [5]. 사용자의 편의성과 효율성을 측정하기 위하여 SUS 평가 방법을 이용하였다. 그 결과 PIN 인증 방법과 Password 인증 중 상대적으로 PIN 기반 인증이 사용성이 떨어지고 있음을 밝혔다. 이와 더불어 인증 과정에 있어서 사용자가 표출하는 괴로움 감정은 PIN 기반 인증이 패스워드 인증 기반에 비해 더 높은 결과를 보였다.

사용자 인증 방법에 대하여 패턴 인증과 PIN 인

증에 대하여 비교 연구가 진행되었다. 총 37명의 실험 참여자를 모집하였으며, 데이터 클리닝을 통해 34명의 참가자 데이터를 분석하였다 [3]. 사용자들은 패턴 인증에 비해 PIN 인증이 불편하다고 53%가 응답하였다 (Fisher's Exact Test, p-value=0.028). Trewin 등의 연구에서는 목소리 기반 인증, 안면 인식 인증, 행동 기반 인증에 대하여 텍스트 패스워드 기반 인증 방식과 비교하는 사용성 연구를 진행하였다 [5]. 텍스트 패스워드 기반 인증보다 목소리 기반, 안면 인식 기반 인증이 인증 과정에서 짧은 시간이 걸렸다. 하지만, 생체 정보 기반 인증 방식은 패스워드 인증 방식에 비해 오류가 더 높게 나타남을 밝혔다. 이와 더불어 SUS 평가에 의해 텍스트 패스워드 기반 인증 방식은 SUS 점수 78을 획득함에 따라 사용성 등급 C를 획득하였고, 목소리 기반 인증은 SUS 66점, D 등급, 안면 인식은 SUS 75점으로 C 등급으로 평가 되었다.

Toledano 등의 연구에서는 생체 정보 기반 인증 시스템에 대하여 ISO 사용성 요소를 이용하여 사용성 연구를 진행하였다 [2]. 연구에서 사용한 ISO 사용성 요소로 유효성, 효율성, 만족도를 이용하였다. 연구 결과 유효성에 대해서는 지문 인식이 목소리 기반 인증에 비해 더 높은 오류율을 가지고 있음을 밝혔다(지문 인증: FMR: 0.00, FNMR: 40.74%, FTER: 2.32%, 목소리 인증: FMR: 8.66%, FNMR: 37.86%, FTER: 0%). 효율성 측면에서는 목소리 기반 인증이 지문 인식 기반 인증에 비해 빠른 인증 시간을 가지고 있음을 밝혔다. 유효성과 효율성 측면에서는 차이가 있었지만, 사용 만족도에서는 지문 인식과 목소리 기반 인증은 큰 차이를 보이지 않았다. (지문 인증: 5.81, 목소리 인증: 5.58)

Prabhakar 등의 연구에서는 인증 수단이 될 수 있는 지문, 안면인식, 손모양, 홍채, 목소리 인증에 대하여 사용자의 인식에 대한 연구를 진행하였다 [6]. 연구 결과 인증 수단의 성능 부분에서는 지문 인증과 홍채 인증이 다른 수단보다 높은 성능을 보여주고 있었고, 안면 인식과 목소리 인증에 대해서는 높은 수용성을 보이고 있었지만, 홍채 인식 방법에 대해서는 수용성이 낮음을 보여주고 있었다. 해당 연구에서는 각 인증 수단의 사용성에 대해 비교 분석을 진행하였지만, 저자의 생각에 의해 각 인증 방법에 대한 사용성에 대해 평가를 진행했다는 큰 문제를 가지고 있었다.

Braz 등의 연구에서는 사용자 인증 방식들에 대한 사용성 연구를 진행하였다 [1]. 연구 대상의 사용자 인증 방식은 패스워드, PIN, OTP, 공인 인증, 케르베로스, 목소리, 지문, 홍채, 키 스트로크 등이 있다. 해당 연구에서는 목소리 기반 본인 인증이 가장 높은 사용성을 보이고 있음을 밝혔고, PIN, 패스워드 인증, 홍채 인증이 사용성에 많이 뒤처지고 있음을 밝혔다. 인증을 완료하기까지 걸리는 시간으로는 지문 인식, 홍채 인식이 가장 적은 시간이 걸렸고, 공인 인증, 패스워드 인증이 상대적으로 더 오랜 시간이 걸림을 밝혔다.

Furnell 등은 텍스트 패스워드, 키스트로크, 안면인식, 목소리, 마우스, 서명, 지문, 홍채 인식 등에 대하여 비교 분석하는 연구를 진행하였다 [7]. 연구 결과 본인 인증을 위한 수단으로 사용자들은 패스워드 기반 인증을 가장 많이 선호하고 있음을 알 수 있었다. 패스워드 기반 인증 이후, 안면 인식, 목소리 기반 인증, 지문 인증 순으로 사용자들은 선호하고 있음을 알 수 있다. Furnell은 5년 후 추가 연구를 진행하였다 [4]. 추후 연구결과에서 사용자들은 지문 인식 기반 본인 인증을 가장 많이 선호하고 있었으며, 목소리 인증, 홍채 인식이 그 뒤를 이었다. 시간이 지남에 따라 인증 수단에 대한 선호가 변화되고 있음을 알 수 있다. 이와 더불어 지문 인식 기반 본인 인증은 목소리 기반 인증에 비해 높은 정확성을 보이고 있음을 밝혔다.

III. 연구방법

3.1 연구 목표

본 연구의 목표는 "인증 수단에 대한 사용성, 안전성 분석"에 있다. 사용성, 안전성 분석을 통해 어떠한 인증 수단이 높은 사용성, 안전성을 가지고 있는지 알아보며, 사용성이 뒤처지는 인증 수단의 문제점이 무엇인지 알아보기 위한 연구 목표를 가지고 있다. 기존 연구에서는 모바일 기기에서 특화한 사용성 및 안전성 평가가 동시에 진행된 연구가 미비하다. 이와 더불어 기존 연구에서는 모바일 기반 인증 수단의 다양성을 반영하지 못하고 있는 한계점을 보이고 있었으며, 인증수단 사용성 평가 진행시, 양적 데이터 분석과 질적 데이터 분석을 함께 진행한 연구가 미비하다. 사용성 평가와 더불어 NIST의 안전성 평가 요소를 이용하여 각 인증 수단에 대한 안전성 평

가를 진행한다. 이에 본 연구는 다음과 같은 실험 환경과 실험 방법을 구축하였다.

3.2 실험 환경

통일된 인증 수단 사용 환경을 구축하기 위하여 삼성 갤럭시 S6 기기만을 이용한다. 기존 연구에서는 실험 환경에 대한 구체적인 내용을 밝히지 않은 점에 보완하기 위함이다. 이와 더불어 모바일 기반의 핀테크 서비스라는 점을 감안하여 해당 기기는 충분히 실험 환경에 알맞은 선택이라 할 수 있다. 해당 기기를 이용하여 실험 참여자가 직접 사용해보면서 각 인증 수단에 대한 평가를 진행한다. 실험 참여자에게 소정의 선물을 전달한다.

3.3 사용성 실험 방법

본 연구의 실험 대상으로는 SMS 본인 인증, ARS 인증, PIN 인증, 지문 인증, 목소리 인증, 공인인증서 인증, TinyLock 인증[1]이 있다.

인증 수단 중에서 경제성을 고려하여 홍채 인식은 제외하였다. 지문 인식기반 인증 수단은 대부분의 모바일 기기에서 인식 센서를 탑재하였고, 많은 사람들이 실생활에 많이 사용하고 있음에 경제성이 있다. 하지만 홍채인식 인증 수단의 경우 최근 출시된 갤럭시 노트7에서 사용이 가능하지만, 대부분의 사용자들이 사용하고 있지 못하기에 경제성을 가지지 못하여 해당 연구의 실험 대상에서 제외하였다.

실험 참여자들이 해당 인증 수단을 직접 사용 후, 각 인증 수단 별 5점 척도로 구성된 SUS(System Usability Scale) 설문지에 응답하며, 각 인증 수단을 사용해 본 경험 및 금융 서비스 사용 의도 파악 등과 같은 행위를 알아보기 위하여, 짧은 인터뷰를 같이 진행한다. 사용성 평가에 있어서 기존 연구 방법과 더불어 인터뷰를 통해 양적, 질적 데이터를 함께 분석한다.

3.4 안전성 평가 방법

NIST(National Institute of Standards and Technology)에서 제시한 전자인증가이드라인을 이용하여 평가를 진행한다. NIST 전자 인증 가이드라인은 전자 인증 지침으로, 전자 인증 과정, 토큰 및 인증에 대한 위협요소, 등에 대한 가이드라인이다. 해당 내용은 OMB 가이드의 3번째 단계를 중점으로 두고 있다. OMB 가이드는 인증 오류의 가능성 영향 측면에서 인증 보장의 요구 수준을 정의하는 것으로, 전자 인증의 보장을 위하여 기준을 제시하고 있다. OMB에서 제시하고 있는 단계 3에 대한 내용은 전자 인증 기술 가이드를 기반으로 인증 수단 선택에 관한 내용을 포함하고 있다.

안전성 평가를 진행함에 있어서, 선입견을 최소화를 위해 총 3명의 연구원이 참여한다. 참여를 통해 각 인증수단 프로세스에 따라 안전성 요소 추출과 더불어 각 인증 수단에서 발생할 수 있는 취약점을 도출한다. 도출한 요소들을 이용하여 인증 수단에 대한 안전성 평가를 진행한다. 각 인증 수단에 대한 보안 등급을 판별하기 위해 3명의 연구원이 합의 하에 진행한다.

IV. 인증수단 평가 결과

4.1 사용성 실험 참여자 정보

본 실험은 한 사람당 대략 40분에서 1시간 소요되었다. 사용성 실험을 진행함에 있어서 각 인증 수단에 대한 설명과 더불어 SUS 기반 설문, 인터뷰를 진행하였고, 가장 마지막 문항으로 사용자 선호도 조사를 진행하였다. 실험 참여자에게는 소정의 선물을 증정하였다. 실험 참여자의 정보는 〔Table 1〕과 같다.

Table 1. Experiment Participant Information

Total Participant: 30		
Gender	Male	19
	Female	11
Age	20s	19
	30s	7
	40s or older	4
Education	Attended Univ.	4
	Graduated Univ.	1
	Attended Graduate Univ.	22
	Graduated Graduate Univ.	3
IT marjors or job classes	Yes	18
	No	12

1) 패턴 기반의 인증 수단으로, 스머지 공격에 대응하기 위한 인증수단이다 〔8〕. 작은 입력공간을 이용하여 패턴을 입력하고, 문지르는 행위를 통해 본인이 사용한 패턴의 흔적을 지우는 행위를 통해 인증이 완료 된다.

사용성 평가 실험에 참여한 인원은 총 30명이며, 남성 19명, 여성 11명이 참여하였다. 참여자의 나이는 20대 19명, 30대 7명, 40대 이상 4명으로, 평균 연령 30.96세, 중앙 나이 28세이다. IT 전공 및 직업군 참여자는 18명, 비전공자 및 비 직업군 참여자는 12명이다.

4.2 SUS(System Usability Scale) 기반 사용성 평가 결과

SUS 기반 사용성 평가 결과는 〔Figure 1〕, 〔Table 3〕와 같다(통계 결과 〔Table 2〕). SUS 점수는 실험 참여자가 응답한 SUS 설문지에 기반한 인증 수단 각각에 대하여 계산하였다. 점수 계산 방법은 홀수 문항과 짝수 문항이 서로 상이 하다. 홀수 문항의 경우, 5점 척도 기준 -1점을 한다. 짝수 문항의 경우, |응답 문항 점수 -5점|을 계산한다. 해당 방식으로 총 10개의 문항에 대하여 점수를 모두 합한 후에 곱하기 2.5점을 한다. 이를 통해 해당 인증 수단이 어느 정도의 사용성을 가지고 있는지 알 수 있다.

지문 인증 수단이 가장 높은 사용성 등급을 받았으며, 뒤를 이어 PIN 인증 수단이 B 등급을 받았다. 뒤이어 스마트 간편 인증 수단과 TinyLock 인증 수단이 C 등급을 받았다. 나머지 인증 수단 모두 D 등급을 받았다. 지문 인증 수단의 경우 Excellent 사용성 평가 결과를 받았다. PIN, 스마트 간편 인증, TinyLock의 경우 Good 사용성 등급 결과를 받았다. 나머지 4개의 인증 수단은 OK 사용성 평가 결과를 받았다.해당 결과를 도출하기 위한 각 문항 별 비교는 다음과 같다.

- ***Q.1.*** *해당 인증 방식을 자주 사용할 것이다.*

해당 문항은 평균 2.4점을 획득한 문항으로, 지문 인식 기반 인증 수단이 가장 높은 점수(3.3점)를 획득하였다. 반면 동일한 생체 정보 기반 인증 수단인

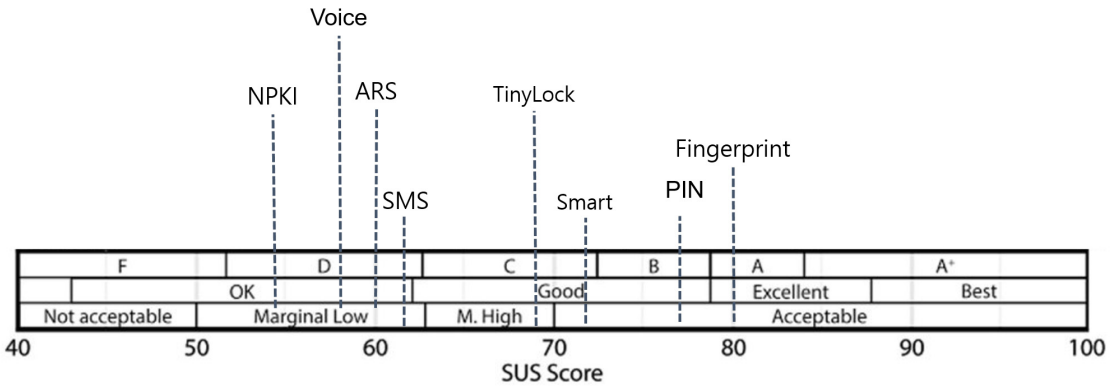


Fig. 1. The usability grade of authentication methods

Table 2. t-test results with SUS score

구분	A1	A2	A3	A4	A5	A6	A7	A8
A1	·	-1.062	4.971***	4.641***	4.587***	1.381	7.203***	2.289*
A2	·	·	6.198***	6.692***	6.659***	2.569*	8.393***	2.787**
A3	·	·	·	-.868	-.453	-3.517*	1.031	2.350*
A4	·	·	·	·	.715	-3.160*	2.633*	-1.505
A5	·	·	·	·	·	-3.813*	2.001	-2.062*
A6	·	·	·	·	·	·	4.800***	.781
A7	·	·	·	·	·	·	·	-3.460*

A1 : PIN ***A2*** : Fingerprint ***A3*** : Voice ***A4*** : SMS ***A5*** : ARS ***A6***: Smart ***A7*** : NPKI ***A8*** : TinyLock
P<0.001***, P<0.01**, P<0.05*, ns : insignificant at the 0.05 level

Table 3. Usability rating by means of authentication SUS Average score results

	SUS score	Grade	Results
Fingerprint	80	A	Excellent
PIN	77	B	Good
Smart	72.5	C	
TinyLock	68.9	C	
SMS	62.6	D	Ok
ARS	60.6	D	
Voice	58.8	D	
NPKI	54.3	D	

목소리 기반 인증 수단이 가장 낮은 점수(1.5점)를 획득하였다.

• *Q.2. 해당 인증 수단은 불필요하게 복잡하다.*

해당 문항은 평균 2.5점을 획득한 문항으로, 스마트 간편 인증이 가장 높은 점수(2.5점)를 획득하였다. 반면 공인 인증서 기반 인증 수단이 가장 낮은 점수(1.5점)를 획득하였다.

• *Q.3. 해당 인증 방식은 사용하기 편리하다.*

해당 문항은 평균 2.5점을 획득한 문항으로, 지문 인식 기반 인증 수단과 PIN 인증 수단이 가장 높은 점수(3.4점)를 획득하였다. 반면 SMS 기반 인증 수단이 가장 낮은 점수(1.5점)를 획득하였다.

• *Q.4. 해당 인증 수단은 사용하기 위해서 숙련자로부터의 도움이 있어야 한다.*

해당 문항은 평균 3.0점을 획득한 문항으로, 지문 인식 기반 인증 수단과 PIN 인증 수단이 가장 높은 점수(3.7점)를 획득하였다. 반면 공인인증서 기반 인증 수단이 가장 낮은 점수(2.1점)를 획득하였다.

• *Q.5. 해당 인증 수단은 다양한 요소를 잘 고려하고 있다.*

해당 문항은 평균 2.0점을 획득한 문항으로, 지문 인식 기반 인증 수단이 가장 높은 점수(2.4점)를 획득하였다. 반면 PIN 인증 수단이 가장 낮은 점수(1.6점)를 획득하였다.

• *Q.6. 해당 인증 수단은 비일관적이다.*

해당 문항은 평균 2.9점을 획득한 문항으로, 스마트 간편 인증 수단이 가장 높은 점수(3.2점)를 획득하였고, 목소리 기반 인증이 가장 낮은 점수(2.4점)를 획득하였다.

• *Q.7. 해당 인증 수단은 사용자들이 쉽게 배울 수 있다.*

해당 문항은 평균 3.1점을 획득한 문항으로, 지문 인식 기반 인증 수단이 가장 높은 점수(3.7점)를 획득하였다. 반면 공인인증서 기반 인증 수단이 가장 낮은 점수(2.1점)를 획득하였다.

• *Q.8. 해당 인증 수단은 사용하기 어렵다.*

해당 문항은 평균 3.0점을 획득한 문항으로, 지문 인식 기반 인증 수단이 가장 높은 점수(3.7점)를 획득하였다. 반면 공인인증서 기반 인증 수단이 가장 낮은 점수(2.1점)를 획득하였다.

• *Q.9. 해당 인증 수단은 사용함에 있어 확신(사용성에 대하여)을 느꼈다.*

해당 문항은 평균 2.3점을 획득한 문항으로, 지문 인식 기반 인증 수단이 가장 높은 점수(2.9점)를 획득하였다. 반면 동일한 생체 정보 기반 인증 수단인 목소리 기반 인증 수단이 가장 낮은 점수(1.5점)를 획득하였다.

• *Q.10. 해당 인증 수단을 이용에 앞서 많은 것을 학습해야 한다.*

해당 문항은 평균 3.0점을 획득한 문항으로, 지문 인식 기반 인증 수단과 PIN 인증 수단이 가장 높은 점수(3.3점)를 획득하였다. 공인인증서 기반 인증이 가장 낮은 점수(2.3점)를 획득하였다.

문항별 비교 결과, 6번 문항을 제외한 모든 문항에서 지문 인식 기반 인증 수단이 가장 높은 사용성을 가진 인증 수단으로 평가되었다. 6번 문항의 경우, 인증 결과에 대하여 오작동에 관련한 문항으로, 생체 정보기반 인증 수단의 특성에 따라 낮은 점수로 평가되었다. 반대로 공인인증서 기반 인증 수단의 경우 다수의 낮은 점수를 받은 인증 수단이다. 공인 인증서 기반 인증 수단의 경우 가장 낮은 사용성을 가지고 있음을 알 수 있다.

4.3 인증 수단 안전성 평가 결과

분석 결과 도출에 있어서 동일한 매커니즘을 가지고 있는 인증 수단, 예를 들어 PIN 번호, 텍스트 패스워드 인증 수단은 그룹으로 묶어 평가를 진행하였다. 안전성 평가 결과는 〔Table 4〕와 같다.

PIN, 텍스트 패스워드(**A1**)는 NIST 안전성 평가 기준에서는 엄격한 신분 증명이 요구 되지 않는 인증 수단으로, 오랫동안 사용된 인증 비밀 값이 신원확인자에게 노출될 위험이 여전히 존재하고 있다. 이와 더불어 Security Level 2에서 제시하고 있는 외부에 유출되지 않아야하는 항목에 적합하지 않은 인증 수단이다. 텍스트 패스워드의 경우 다양한 경로로 유출된 경험 및 사건 사고가 있었으며, PIN 번

Table 4. Results of the evaluation of the security measures of the authentication methods

Security Level	Requirements	A1	A2	A3	A4	A5	A6
Level 1	With the lowest security level, no rigorous identification is required.	○					
	It ensures that the same user has access to protected information or work, and does not require the use of cryptographic techniques.	○					
	The long-secret authentication value used may be exposed to identity verifier.	○					
Level 2	It can prevent eavesdropping, reuse attacks, and online guessing attacks.	X	○				○
	The authentication secret value used for a long time should not be leaked to the outside.		○				○
	Use a cryptographic technique approved by NIST.		○				○
Level 3	Based on proving the possession of a secret key or disposable password through a cryptographic protocol.		X	○			X
	There is a cryptographic mechanism that can prevent an authentication token from being leaked by various attacks.			○			
	Use a cryptographic technique approved by NIST.			○			
Level 4	Transmission of data must also be authenticated.				○	○	
	Require strong cryptographic authentication, use symmetric key, public key technology.				○	○	
	Password leakage due to malicious code can be prevented.			X	○	○	
	Use a cryptographic technique approved by NIST.			X	○	○	
Result		Level 1	Level 2	Level 3	Level 4	Level 4	Level 2

A1 : PIN, PWD ***A2*** : ARS ***A3*** : SMS ***A4*** : Biometric ***A5*** : NPKI ***A6*** : Smart

호의 경우도 마찬가지로 유출 경험이 존재한다.

ARS 인증 수단(**A2**)은 SSL/TLS을 이용하여 통신하기 때문에 NIST에 의해 승인된 기술을 사용하고 있다. 이와 더불어 OTP 값을 이용하기 때문에 재사용 공격, 온라인 추측공격을 방지할 수 있다. 하지만 Security Level 3의 일회용 비밀번호의 소유를 증명하는 것에 기반 한 것이 아니기 때문에 Level 3을 획득할 수 없다.

SMS 인증 수단(**A3**)은 엄격한 신분이 증명이 요구 되며, OTP 값은 한번만 사용되는 난수로 오랫동안 사용되는 인증 비밀 값이 아니기 때문에 Security Level 1을 만족한다. Security Level 2의 재사용 공격, 온라인 추측 공격에 대해서는 OTP 난수 값을 사용하기 때문에 어느 정도 방지 할 수 있으며, 도청에도 OTP 값을 사용하기 때문에 어느 정도 방지 할 수 있다. SMS 인증의 경우, 비밀키나 일회용 비밀번호의 소유를 증명하는 것에 기반한 인증 수단이며, 인증토큰이 유출되는 것을 막을 수 있는 암호 매커니즘을 사용하고 있으며, NIST에 의해 승인된 암호 기술을 사용하고 있다. 이로써 SMS 인증 수단은 NIST의 Security Level 3를 부여받을 수 있다.

생체 정보 인식 기반 인증 수단(**A4**)은 생체 정보 기반 인증 수단으로 지문 인식 기반 인증, 목소리 인식 기반 인증 수단이 있다. 모바일 내의 Knox와 TEE를 이용하기에 다른 인증 수단에 비해 안전한 환경에 기반 한다. Knox, TEE 기반의 모바일 센싱 기술을 통해 인증 관련 기록의 보존 및 변경에 대한 보호대책을 제공에 따라 인증정보 생성 값 유출을 방지 할 수 있다. 이와 더불어 FIDO 기반의 서버를 이용하기에 전자 서명 값 생성을 통한 부인 방지 할 수 있으며, FIDO 개인키를 이용하여 전자서명을 생성함에 따라 안전성을 제공하고 있다. 중간자 공격에 대응할 수 있는 세션 값, 암호화 데이터 생성 등을 진행하고 있다. 개인 생체 정보를 가지고 있기 때문에 인증수단의 비밀정보의 물리적 유출 방지할 수 있는 생체 정보 특징을 가지고 있다.

공인인증서 기반 인증수단(**A5**)은 안전한 CA 기관으로부터 인증서를 발급을 받으며, 발급 후, 배포 과정에서도 안전한 장치를 이용하여 스마트 폰에 복사를 진행하며, 1년 주기로 재발급 절차를 진행한다. 이와 더불어 모바일 기기를 분실 하였을 경우에도 PC 환경에서 재발급 신청을 진행하면 모바일에 저장되어 있는 공인인증서를 사용할 수 없는 보호대책을 가지고 있다. 또한 보안 카드를 통해 2중 인증을 진행할 수 있기 때문에 더욱 안전하게 이용할 수 있다. 전자 서명을 통해 부인 방지 기능을 제공하고 있다. 인증 과정에 있어서 비밀번호 몇 회 이상 틀리면 공인 인증서를 사용할 수 없게 되기 때문에 추측을 방지 할 수 있으며, 공인 인증서 위조 및 변조 방지를 위해 복사 불가 및 백신 프로그램 제공의 보안 사항을 진행하고 있다. 인증 정보 생성 값을 유출 방지를 위하여 NIST에서 인증된 암호 기술을 사용하고 있다. 대칭키, 공개키 기술을 이용하여 강력한 암호학적 인증을 진행하며, SSL/TLS를 이용하여 전송 과정에 있어서도 인증이 된다.

스마트 간편 인증수단(**A6**)은 스마트 간편 기반 인증은 소유와 본인 인증을 동시에 진행하는 인증 방법이다. 기존의 인증 수단과 달리 비밀번호 입력이 없음에 3등급에 해당하는 추측 방지에 대한 안전성 평가는 고려 대상이 되지 않는다. 점유 인증에서 USIM 정보와 기기정보를 통해 통신사의 DB 검증을 통해 인증을 진행하기 때문에 도용에 대한 안전성이 높다. 또한 서비스 제공자의 서버에서 생성된 OTP를 활용하기 때문에 스미싱 등에 대한 안전성을 보장한다. 고유키 값 생성을 통해 중간자 공격에 대해 안전성을 보장한다. 점유 인증을 통해 신분 증명이 요구되며, 인증 비밀 값이 외부에 유출되지 않는 안전성을 가지고 있다. NIST Security Level 3에서 제시하는 OTP 소유를 증명하는 것에 기반 한 인증 수단이 아니기 때문에 NIST 안전성 등급에서는 Security Level 2 등급을 부여한다.

이처럼 다양한 기준을 이용한 인증 수단 안전성 평가 결과 생체 정보 인식 기반 인증수단과 공인인증서 기반 인증수단이 높은 안전성이 있는 것으로 분석하였다.

4.4 인터뷰 기반 인증 수단 평가 결과

인터뷰를 통해 사용자들이 느끼는 의견에 대하여 질적 데이터를 획득하였고, 각 인증 수단별 금융서비스 사용 의향, 안전성에 대한 생각을 분석하였다.

- PIN 인증 : 대부분의 사용자들이 금융 서비스에서 사용의도에는 부정적 의견을 많이 비추고 있다. 하지만 과거 사용한 경험 및 사용하고 있는 경험을 바탕으로 대부분 사람들이 금융 서비스에서 사용할 것이라 밝혔다. 안전성 측면에 대해서

사용자들은 여전히 안전하지 않다는 생각을 많이 하고 있다.

- 지문 인식 인증 수단 : 지문 인증 수단의 경우, 불편한 점은 대부분 인증에 사용되는 손가락 및 날씨에 큰 영향을 받는 경향을 보였다. 하지만, 편리한 점에 사용자들은 짧은 인증 시간과 비롯해 즉각성이 있기 때문에 편리함을 밝혔다. 또한 금융 서비스에 인증 수단으로 사용함에 있어서 매우 긍정적이다. 하지만 안전성 측면에서는 미디어의 영향으로 불안감을 가지고 있음을 밝혔다.
- 목소리 인식 인증 수단 : 목소리 인증 수단에 대해서는 다른 인증 수단과 달리 안전성에 대해 매우 부정적인 결과를 사용자들은 의견을 표출하였다. 대부분 목소리 녹음, 변조에 대한 위험성을 인식하고 있었다. 또한 다른 인증 수단에 비해 상대적으로 자신의 감정 혹은 행동이 많이 반영되고 있었다. 예를 들어 부끄러움, 민망함, 자신이 어떠한 행동을 하고 있음을 표출하는 등에 대하여 이야기를 하였다. 모바일 금융에서의 인증 수단으로서의 사용 의향은 매우 부정적인 결과를 내비치고 있었다. 목소리를 통해 자신의 행동 노출에 대한 우려를 나타내고 있다.
- SMS 인증 수단 : SMS 인증 수단은 사용자들이 가장 많이 사용해본 경험이 있는 인증 수단 중 하나로, 어느 정도 훈련이 많이 되어 있는 인증 수단이다. Auto-Filling과 같은 기능이 없다면 불편함을 느끼지만, 그 외에 큰 불편함 없이 사용자들은 편리함을 느끼고 있다. 또한 금융 서비스에서도 사용 의향은 긍정적이며, 안전성을 느끼기에는 적당한 절차를 지니고 있음을 밝혔다.
- ARS 인증 수단 : 대체로 인증 완료까지 걸리는 시간이 다른 인증 수단에 비해 오래 걸리는 부분을 가장 많이 불편해 하고 있음을 밝혔다. 하지만, 사용 경험에 의하여 금융 서비스 사용 의향에서는 긍정적인 답변을 보이고 있으며, 모바일 기기를 본인이 소지해야 함이 전제가 되고 있기 때문에 안전성에 대해 사용자들은 긍정적인 반응을 비췄다.
- 스마트 간편 인증 : 스마트 간편 인증은 이전에 저장되어 있는 정보(USIM, 공인인증서)를 이용한 인증 수단으로, 실험자 대부분이 처음 사용해본 인증 수단이기에 부정적인 사용 의향을 밝히고 있었다. 해당 인증 수단에 대해 안전성 우려와 더불어 너무 쉽게 인증이 완료된다는 점을 바탕으로 거부감을 나타냈다. 하지만 사용의 편리성에서는 사용자들의 불편함은 나타나지 않았다.
- 공인인증서 인증 수단 : 공인인증서 기반 인증 수단은 모바일 기반 이전에 PC 환경에서 많이 사용한 경험을 가지고 있다. 하지만, 공인인증서의 특성상 1년 주기로 갱신하는 불편함을 내포하고 있다. 하지만 사용자들은 안전성에 대해서는 긍정적으로 생각하고 있다. 결과적으로 공인인증서 인증 수단에 대해서 사용자들은 안전함 대비 불편함이 많이 있음을 이야기 하지만, 사용 경험에 의한 성숙에 따라 모바일 금융에서도 사용할 의향이 있음을 밝혔다.
- TinyLock 인증 수단 : 기존의 패턴 잠금을 응용했다는 점에 대하여 거부감을 느끼지 못하고 있었다. 하지만 입력하는 공간에 대한 불편함을 많이 느끼고 있었다. 입력하는 공간이 일정 정도 이상의 크기로 확보가 된다면, 사용자들이 입력했을 때의 오류를 많이 줄일 수 있을 것으로 예상한다. 이와 더불어 안전성에 대해서는 기존 패턴 잠금 자체의 안전성에 대한 우려를 보이고 있지만, 패턴 흔적을 지우는 과정이 있기 때문에 어느 정도 우려를 잠식시킬 수 있는 장치가 존재하기 때문에 안전성에서 큰 거부감은 없다.

인터뷰를 통한 인증 수단 평가결과 사용자들은 특정 목적에 취합되고 있음을 알 수 있었다. 어느 정도 친숙한 인증 수단에 대해서는 긍정적 영향을 보이고 있음을 알 수 있다. 하지만, 미디어의 영향에 의해 사용자들은 안전성에 대해서 경각심을 가지고 있는 인증 수단이 존재하고 있다. 따라서 금융 서비스 이용 시, 지문인증에 대해 사용자들은 가장 큰 사용성을 보이고 있음을 밝혔다.

4.5 인증 수단 선호도 분석 결과

사용성 중심 사용 선호도([Table 5]), 안전성 중심 사용 선호도([Table 6]) 조사 결과는 와 같다. 사용자들은 지문 인식 기반 인증(15명, 50%), 패턴 기반 TinyLock 인증(10명, 33%)에 대해 사용성 중심에서 선호도가 높음을 알 수 있다. 안전성 중심 사용자 선호도는 지문 인식 기반 인증(11명, 36.7%), 공인인증서 인증(11명, 36.7%)에 대해 선호하고 있음을 알 수 있다. 공통적으로 지문 인식 기반 인증 수단이 가장 높은 사용자 선호도가 있음을

Table 5. Usability-based user preference

구분	Authentication Methods	Answer (%)
Priority 1.	Fingerprint	15명(50%)
Priority 2.	TinyLock	10명(33%)
Priority 3.	PIN	3명(10%)
Priority 4.	NPKI	1명(3.3%)
	Smart	1명(3.3%)
Priority 6.	Voice	-
	SMS	-
	ARS	-

Table 6. Security-based user preference

구분	Authentication Methods	Answer (%)
Priority 1.	Fingerprint	11 (36.7%)
	NPKI	11 (36.7%)
Priority 3.	TinyLock	2 (6.7%)
	Smar	2 (6.7%)
Priority 5.	PIN	1 (3.3%)
	Voice	1 (3.3%)
	ARS	1 (3.3%)
	SMS	1 (3.3%)

알 수 있다.

V. 결 론

SUS 기반 사용성 평가를 통해 지문 인식 기반 인증 수단이 가장 사용성이 높은 등급의 인증 수단으로 평가되었다. 반대로, 공인 인증서는 가장 사용성이 낮은 등급의 인증 수단으로 평가되었다. 안전성 평가에서는 지문 인식 기반 인증수단과 공인 인증서 기반 인증 수단이 안전성이 높은 인증 수단으로 평가되었다. 반면, PIN, 텍스트 패스워드가 가장 낮은 안전성 등급으로 평가되었다. 모바일 금융 핀테크 서비스 이용 시 사용자들은 지문 인식 인증 수단에 대하여 가장 높은 선호도를 보임에 따라 사용자들은 사용성 및 안전성이 높은 인증 수단을 선호하고 있음을 알 수 있다.

본 연구 결과를 통해 각 인증 수단에 대한 사용자 인식과 더불어 금융서비스 의향, 안전성에 대한 생각을 알 수 있었다. 본 연구를 통해 핀테크 서비스 제공자들은 지문 인증 서비스 기반의 다양한 서비스를 제공한다면, 긍정적 효과를 도출 할 것으로 예상된다. 해당 연구는 적은 수의 참여자 모집과 더불어, 특정 학력에 편중되고 있는 한계점이 있다. 안전성에 대한 사용자 인식 도출, 평가 지표에 의거한 평가에서 확장하여 시뮬레이션을 통한 안전성 평가를 진행이 확장연구로 진행 되어야한다. 이를 통해 사용자 인식과 실제 안전성에 대한 비교를 통해 사용자 인식과 실제 안전성의 차이에 대한 연구 결과 도출이 필요하다.

References

[1] C. Braz, and J. M. Robert, *"Security and usability: the case of the user authentication methods,"* *In Proc. of IHM '06,* pp. 199-203, 2006.

[2] D. T. Toledano, R. F. Pozo, A. H. Trapote and L. H. Gomez, *"Usability evaluation of multi-modal biometric verification systems,"* *Interacting with Computers,* 18(5), vol. 18, no. 5, pp. 1101-1122, Sept, 2006.

[3] H. Khan, A. Atwater, and U. Hengartner, "A comparative Evaluation of Implicit Authentication Schemes," In Proc. of RAID, pp. 255-275, Sep. 2014.

[4] N. L. Clarke, and S. M. Furnell, *"Authentication of users on mobile telephones - A survey of attitudes and practices,"* *Computers & Security,* vol. 24, no. 7, pp. 519-527, 2005.

[5] N. Micallef, M. Just, L. Baillie, M. Halvey, and H. G. Kayacik, *"Why aren't users using protection? Investigating the usability of smartphone locking,"* *Iin Proc. of MobileHCI,* 2015.

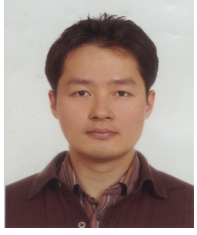
[6] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. B. David, *"Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption,"* *In Proc. of ACSAC,* pp. 159-168, Dec. 2012.

[7] S. Prabhakar, S. Pankanti, and A. K.

Jain, *"Biometric Recognition: Security and Privacy Concerns," In Proc. of IEEE S&P,* vol. 99, no. 2, pp. 33-42, 2003.
〔8〕 S. M. Furnell, P. S. Dowland, H. M. Illingworth, and P. L. Reynolds, *"Authentication and Supervision: A Survey of User Attitudes," Computers & Security,* vol. 19, no. 6, pp. 529-539, Oct., 2000.
〔9〕 K. Taekyoung, and N. Sarang *"TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems." computers & security,* vo. 42, pp. 137-150, 2014.
〔10〕 DIGIECO report, "2016 Mobile Trend Forecast," 2016.

〈저자소개〉

김 경 훈 (KyoungHoon Kim) 학생회원
2017년 2월: 연세대학교 정보대학원 석사
〈관심분야〉 Authentication, Usable Security 등



권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkely Post-Doc.
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호프로토콜, 네트워크 프로토콜, 사물인터넷 보안, HCI 보안 등