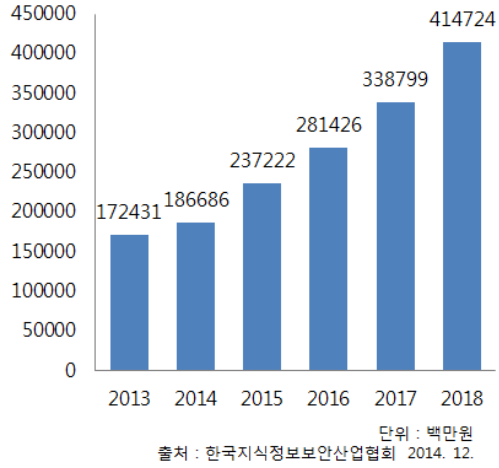
정맥을 이용한 생체인증 방식의 동향☆

유 동 현* 김 경 한* 김 수 형** 윤 봉 중*** 염 흥 열*

목 차

1. 서 론

언제 어디서든 사용자가 원하는 정보와 자원을 이용할 수 있게 되면서, 정당한 서비스 사용자임을 인식하고 인증하기 위한 방식의 중요성이 강조되고 있다. 과거에는 업무서비스를 사용하기 위해 사용자가 직접 방문하여 본인임을 증명하지 않고도 원격지에서 본인임을 증명할 수 있는 비대면 인증방식으로 아이디와 비밀번호를 이용하는 방식을 가장 선호했다. 하지만, 분실과 도난의 위험성이 제기되면서 비밀번호를 사용하지 않는 인증방식을 지향하는 다양한 방법들이 등장하였다. 최근에는 사용자 신체에 존재하는 생체정보를 이용하여 사용자 본인임을 증명하는 FIDO(Fast IDentity Online)방식이 등장하였고 이는 현재 다양한 분야에 도입되어 연구개발이 진행되고 있다. FIDO를 이용한 산업시장은 점차 성장할 것으로 보이며, 시장이 성장함에 따라 기존에 사용되던 생체정보가 아닌 새로운 생체정보를 이용하여 사용자를 인증하는 다양한 방식이 등장할 것으로 보인다. 이전의 생체인증 방식은 큰 단말기를 이용하여 생체정보를 수집했지만, 생체인식 장치 소형화에 관한 연구를 통해 점차 단말기의 크기가 작아지고 있다. 생체인식 단말기의 크기가 작아지면서 스마트폰과 같은 모바일 장치에 생체인증 방식이 도입되는 사례가 증가하였고, 다양한 생체정보를 활용하여 금융거래, 스마트폰 잠금 해제, 사생활 보호 등을 위한 사용자 인증이 가능해졌다.



(그림 1) 국내 생체인식산업 매출 전망

생체인증을 통해 접근할 수 있는 자원과 서비스가 다양해지면서, 인증과정에 취약점이 존재할 경우 발생할 수 있는 피해도 커지고 있다. 공격자들은 인증과정을 공격하기 위해 다양한 공격을 시도한다.

본 논문에서는 생체인증에 사용되는 생체정보의 유형과 특징 및 보안위협을 알아보고, 그 중 정맥인증 방식의 특징과 다른 생체정보를 이용하는 방식과의 차이점에 대해 소개한다.

* 순천향대학교 정보보호학과
** ETRI 인증기술 연구실
*** 금융결제원 표준화팀

2. 비 생체기반 사용자 인증

생체인증 방식이 보편화되기 이전의 온라인을 통해 비대면 방식의 사용자 인증방식에는 지식기반 방식과 소지기반 방식이 주로 사용되었다. 지식기반 방식은 사용자의 기억에 의존하는 인증방식이며, 소지기반 방식은 사용자가 가지고 있는 물건을 이용하는 방식이다.

(표 1) 지식기반 인증방식과 소지기반 인증방식의 예

유형	소지기반	지식기반
이용사례	OTP, 보안토큰, 스마트카드,	아이디, 비밀번호, PIN번호, 패턴인식

지식기반의 인증방식은 단일요소로도 인증에 사용되지만, 소지기반의 인증방식은 주로 다중요소의 인증방식 중 하나로 사용된다.

2.1 비밀번호를 이용한 방식

비밀번호를 이용한 방식은 웹 사이트에서 사용자를 인증할 때 자주 사용되는 방식 중 하나이다. 지식기반의 방식으로, 사용자는 원하는 문구나 단어를 이용하여 아이디와 비밀번호를 설정하여 사용한다. 사용자가 설정한 비밀번호는 해시(Hash)화 과정을 거친 뒤 인증 시스템의 데이터베이스에 저장되고 인증 프로세스가 시작되면 사용자로부터 입력받은 비밀번호의 해시 값과 데이터베이스 내에 저장 된 해시 값을 비교하여 사용자를 인증하는 원리로 이루어진다.

2.1.1 보안위협

비밀번호 방식의 보안강도는 사용자가 지정한 문자의 복잡성에 있다. 숫자만을 사용하여 비밀번호를 만든 경우와 영문을 섞어서 만든 경우, 특수문자를 섞어서 만든 경우 등으로 분류 할 수 있다. 또한 비밀번호의 문자길이 역시 비밀번호 방식의 보안강도에 영향을 끼친다. 비밀번호는 보안강도가 낮을수록 무차별 대입공격(Brute-Forcing)에 취약한 것으로 알려져 있다. 무차별 대입공격은 가능한 경우의 수를 모두 대입하여 비밀번호를 무작위로 추측하는 형태의 공격이다. 비밀번호 입력횟수의 제한이 없고 사용자 비밀번호의 강도가 약할 경우, 공격자는 무차별 대입공격을 통해 사용자인증의 성공가능성이 존재한다.

2.2 OTP(One Time Password)

OTP는 인증을 위한 프로세스가 시작될 때마다 새로운 비밀번호를 생성하여 사용하는 일회용 비밀번호 방식이다. 사용자 인증을 위해 OTP기기나 스마트폰과 같은 모바일 장치에 애플리케이션을 설치하여 서버와의 동기화를 통해 실시간으로 생성된 비밀번호를 사용자에게 노출시킨 뒤, 사용자는 노출된 비밀번호를 온라인상 입력화면에 입력하여 본인인증을 완료하는 프로세스로 작동한다. 금융보안연구원을 통해 2007년 처음 국내에 도입되어 시행되었으며, 현재 금융거래와 온라인게임 서비스 등에서 사용자 인증에 활발히 사용 중이다.

(그림 2) OTP기기

2.2.1 보안위협

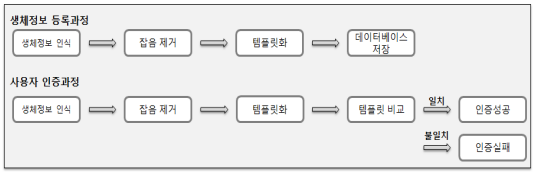
OTP방식은 소지기반의 장치를 통해 비밀번호를 입력하는 방법이기 때문에 공격자는 사용자인증을 위한 정보를 알고 있어도 인증에 성공하지 못한다. 하지만, 공격자가 OTP를 사용하는 사용자 컴퓨터에 키로거(Key Logger)악성코드를 설치하여 입력되는 OTP번호를 갈취할 수 있는 상태가 되거나, 패킷스니핑(Packet Sniffing)과 같은 공격에 노출될 경우 중간자 공격을 통해 OTP의 재생성주기 동안에는 사용자인증에 성공할 가능성이 존재한다.[1]

3. 생체인증 방식의 종류와 문제점

인증시스템은 생체인증을 위해 사용자 신체로부터 생체정보를 수집한다. 인증에 사용하는 생체정보의 종류와 유형에 따라서 해당 생체정보를 사용자로부터

얻어내는 방식이 다를 수 있다. 지문인식처럼 신체를 직접 인식장치에 가져다 대는 행위를 통해 생체정보를 수집하는 접촉식 방식이 있으며, 얼굴인식과 음석인식처럼 카메라나 마이크 등을 사용하여 생체정보를 포착하는 방식의 비접촉식 방식이 있다. 생체인증의 특성 상 하나의 인증시스템에 불특정 다수가 동일한 인식장치를 사용하기 때문에 접촉식 방식을 사용하는 경우 사용자의 위생 문제와도 연관될 수 있으며, 접촉된 신체의 정보를 수집하지 않고 일정 거리에 존재하는 정보를 수집하여 인증을 하는 비접촉식 방식의 경우에는 빛의 세기와 방향, 잡음 등의 인증할 당시의 주변 환경에 따라서 인증의 실패확률이 높아질 수 있다.[2]

생체정보의 경우 사용자 신체를 이용하는 만큼 인식 당시 사용자의 몸 상태나 주변 환경에 영향을 많이 받는다. 따라서 일반적인 생체인증 시스템의 경우 사용자의 신체로부터 수집한 생체정보를 그대로 사용하지 않고, 잡음을 제거한 뒤 템플릿(Template)화 알고리즘을 통해 가공한다. 최종적으로 만들어진 생체정보 템플릿은 데이터베이스에 저장되어 인증 시 만들어진 템플릿과 비교하는 방식을 사용한다.[3]



(그림 3) 생체정보를 이용한 사용자 인증과정

3.1 지문인식

개인이 가지고 있는 지문의 차이점을 포착해서 사용자를 인증하는 방법으로 가장 보편화된 생체인증 방식 중 하나로 알려져 있다. 일반적인 생체정보는 신체의 유실이나 변형이 일어나기 전까지는 데이터의 분실가능성이 없다고 알려져 있다. 지문정보의 경우에는 손가락을 많이 사용하는 사람일수록 지문의 훼손가능성이 높기 때문에 다른 생체정보보다는 정보의 변형가능성이 비교적 높다고 할 수 있다. 또한 지문의 경우 손으로 만지는 모든 사물에 흔적을 남기기 때문에 공격자는 사용자가 신체에 가지고 있는 정보를 직접 사용하지 않고도 흔적들을 이용하여 지문정보의 도용이 가능하다.

지문정보와 같은 생체정보는 한번 유출이 되면 평생동안의 위험을 감수해야 하는 만큼 템플릿이 아닌 지문 이미지 전체가 공격자에게 노출되는 사고는 사용자에게 치명적이다. 최근 지문인식 장치를 탑재한 스마트폰이 대거 등장하면서, 잠금 해제나 간편 결제에 지문정보를 이용하는 사례가 급증하고 있으며, 스마트폰 내에 저장된 생체정보의 유출 가능성이 제기되고 있다.[4][5][6]

(표 2) 지문인식을 지원하는 모바일 결제방식의 종류

종류	애플 페이	삼성 페이	안드로이드 페이
출시	2014. 10.	2015. 09.	2015. 10.
지원 기기	iPhone6/6+, iPhone6S/6S+, Apple Watch	Galaxy S6, Galaxy S6 Edge/Edge+, Galaxy Note5	NFC 기능이 탑재된 모든 안드로이드
지문 인증	지원	지원	지원

보안업체 '파이어아이(FireEye)'의 연구원들은 스마트폰 악성코드를 통해 기기 내 지문인식 장치에 접근하여 지문정보 템플릿이 아닌 고해상도의 원본 지문이미지를 탈취시나리오를 발표하면서 스마트폰 지문인식 방식의 위험성을 제기하였다.[7]

3.2 홍채인식

사람 눈의 동공 주변의 홍채패턴의 차이점을 포착해서 사용자를 인증하는 방법으로 홍채의 모양과 모세혈관의 구조를 분석하여 홍채정보 템플릿을 생성하고 사용한다. 인식장치는 카메라를 통해 사람의 눈에 존재하는 홍채이미지를 인식하기 때문에 손을 사용할수록 지문이 닳아 정보의 변형가능성이 높은 지문인식보다는 비교적 유실과 변형가능성이 적다.

최근 홍채인식 기술의 소형화가 가능해지면서 홍채를 통한 사용자인증 방식이 스마트폰 뿐 만 아니라 금융거래 ATM기기에도 적용되는 추세이다. 국내 제조사 S사의 경우 2016년 상반기에 홍채인식 기능을 탑재한 스마트폰을 출시 할 계획이라고 밝혔으며, 국내 금융권

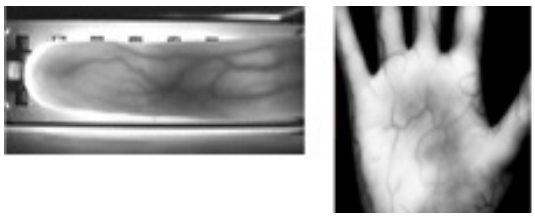
I은행의 경우 현재 홍채인증 방식의 ATM기기를 설치하여 시범운영을 통해 확대의사를 밝혔다.[8]

(그림 4) 국내 I은행의 시범운영중인 홍채인증 ATM

모바일에서 사용되는 지문인식 방식은 카메라를 통해 이미지를 입력받지 않고 반도체 형태의 인식센서를 이용하여 지문 이미지를 입력받는 반면 홍채인식 방식은 카메라를 통해서만 이미지를 입력받을 수 있다. 이러한 특징을 이용하여 스페인의 마드리드 자치대학교(UAM)의 과학자들은 실제 데이터베이스에 저장되어있는 홍채이미지를 복제 후 합성하여 얻어낸 가짜 이미지로 인식기를 통과하는 시나리오를 통해 홍채인식 시스템의 도용가능성을 제기하였다.[9]

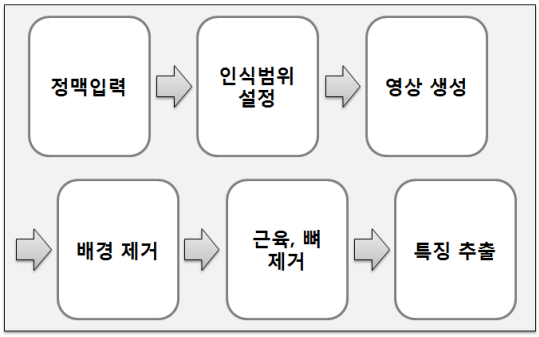
4. 정맥인식을 통한 생체인증

생체인증에 사용되는 사용자의 지문정보는 손가락에만 존재하고 홍채정보는 안구에만 존재한다. 이와는 다르게 정맥정보 같은 경우는 사용자 신체부위 모두에 존재하기 때문에 정맥을 이용하는 인증시스템에도 손가락 정맥과 손등 정맥, 손바닥 정맥을 이용하는 방식 등 여러 종류가 있다.



(그림 5) 지정맥(좌)과 손바닥 정맥(우)

인식장치는 사용자 신체로부터 정맥의 생김새를 추출해 내기 위해 적외선을 투과시켜서 헤모글로빈의 움직임을 촬영한다. 인증시스템은 촬영된 영상으로부터 정맥 부분을 추출해내며, 추출된 정맥의 생김새는 템플릿 화를 거쳐 데이터베이스에 저장되게 된다.[10]



(그림 5) 정맥정보의 추출과정

정맥을 입력하는 과정은 혈액이 순환하며 발생하는 헤모글로빈의 움직임을 이용하여 정맥의 생김새를 추출하기 때문에 죽은 사람의 신체를 가지고 정맥인식에 도용을 하는 것은 불가능하다.

4.1 지정맥 인식

지정맥 인식은 사용자 손가락에 존재하는 정맥을 이용하는 방식이다. 사용자 신체에 존재하는 혈관 중 가장 인식시키기 쉬운 부위를 사용한다는 장점이 있다. 또한, 기존에 존재하는 지문인식 방식과 사용법이 유사하기 때문에 처음 사용하는 사용자의 거부감도 적은 편이다. 지정맥 인식은 현재 해외 금융권에서 활발히 사용 중이며, 국내 금융권에서도 지정맥 인식을 도입을 추진 중에 있다.[11]

(그림 6) 일본 Y은행의 지정맥 ATM 사용법

4.2 손바닥정맥 인식

사용자의 손바닥에 존재하는 정맥을 이용하는 방식은 다른 신체부위의 정맥에 비해 포함하고 있는 정맥정보가 많다. 손바닥 정맥은 신체부위의 너비가 넓기 때문에 지정맥과는 다르게 비접촉식 생체인증이 가능하다. 지정맥 방식은 접촉식 방식이기 때문에 위생상의 문제로 사용자의 거부감이 생길 수 있지만 손바닥 정맥은 위생상의 문제가 없다는 장점이 있다. 국내 금융권 S은행은 2015년 12월부터 손바닥 정맥을 이용한 ATM 기기 서비스를 시작하였다.[12]

(그림 7) S은행의 손바닥 정맥인증 ATM

5. 결 론

본 논문에서는 예전부터 사용된 사용자 인증방식과 최근 화두가 되고 있는 생체인증 방식의 차이점 및 동향 대하여 설명하였다. FIDO 방식의 등장으로 사용자의 생체정보를 이용한 인증이 다양한 분야에서 활용되고 있지만 생체정보를 활용하는 인증방식에도 보안위협의 가능성이 존재하는 것을 확인하였다. 최근 정맥인식을 통한 사용자 인증방식이 국내 금융권 등에 활발하게 도입되어 사용되고 있으며, 향후 보다 많은 분야에서 사용될 것으로 보인다.

생체정보는 한 번 형성되면 죽기 전까지는 변하지 않는다는 특성이 있기 때문에 공격자에게 유출될 경우 해당 사용자가 사용하는 모든 생체인증에 대해 도용이 가능하며, 금융권의 경우 공격자가 사용자의 계좌에 접근하여 금전적인 피해를 입힐 수도 있다. 따라서 사용자의 생체정보를 저장하는 프로세스와 데이터베이스에 접근에 관해 엄격한 관리가 필요하다고 생각한다.

참 고 문 헌

[1] 김기영. 일회용 패스워드를 기반으로 한 인증 시스템에 대한 고찰, 정보보호학회지, 17(3), 26-31, 2007

[2] 유동현, 김경한, 염흥열, 김수형, 윤봉중, 생체정보를 이용한 인증방식의 유형과 동향, 정보보호학회 동계학술대회, 2015.12

[3] 신용녀, 이용준, 전명근, 개인정보 보호를 위한 바이오인식 템플릿 보안, 한국지능시스템학회 논문지, 18(4), 437-444, 2008

[4] 삼성 페이, http://www.samsung.com/sec/samsung-pay/

[5] 에플 페이, http://www.apple.com/apple-pay/

[6] 안드로이드 페이, https://www.android.com/pay/

[7] Yulong Zhang, Zhaofeng Chen, Hui Xue, Tao Wei, Fingerprints On Mobile Devices: Abusing and Leaking, Blackhat, 2015

[8] 카드없이 눈으로 돈 찾는다…'홍채인증 ATM' 등장, http://news.donga.com/Economy/3/all/20151214/75353318/1, 뉴스1, 2015.12.14

[9] Ruiz-Albacete, Virginia, et al, Direct attacks using fake images in iris verification, Biometrics and identity management, Springer Berlin Heidelberg, 181-190, 2008.

[10] 정진철, 고명철, 손병준, 손가락 정맥 기반 생체인식, 한국정보과학회 학술발표논문집, 34(1D), 41-45, 2007

[11] http://www.yachiyobank.co.jp/kojin/kouza/ic_card.html

[12] 신한銀, 디지털 키오스크 써보니, http://www.asiae.co.kr/news/view.htm?idxno=2015120313300749131, 아시아경제, 2015.12.03.

[13] 이의철, 조명 정규화를 통한 정맥인식 성능 향상 기법, 한국정보통신학회논문지, 17(2), 423-430, 2013

◐ 저 자 소 개 ◑

유 동 현

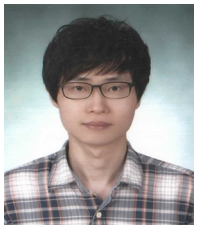
2015년 8월 순천향대학교 정보보호학과 졸업
2005년 8월 ~ 현재 순천향대학교 대학원 정보보호학과 석사과정
관심분야 : 정보보호, 악성코드, 웹, 서비스보안

김 경 한

2015년 순천향대학교 정보보호학과 학사
2015년~ 현재 순천향대학교 정보보호학과 석사과정
관심분야 : International Standards, Social Engineering, Cryptography, Financial Security, etc...

김 수 형

2000년~ 현재 한국전자통신연구원 인증기술연구실 실장 / 책임연구원
1998년~ 2000년 한국정보통신 연구소 연구원
2016년 한국과학기술원 전산학부 박사
1998년 연세대학교 컴퓨터과학과 석사
1996년 연세대학교 컴퓨터과학과 학사
관심분야 : 사용자인증, 개인정보보호, 전자금융 보안, 모바일 보안, IoT 보안 등



윤 봉 중

2004년 고려대학교 컴퓨터학과(이학사)
2015년 고려대학교 대학원 컴퓨터·전파통신공학과(공학석사)
2004년~현재 금융결제원
관심분야: 금융보안

염 흥 열

1990년 한양대학교 대학원 전자공학과 박사
1982년 ~ 1990년 8월 한국전자통신연구원 선임연구원
1990년 9월 ~ 1990년 현재 순천향대학교 공과대학 정보보호학과
2011년 1월 ~ 12월 한국정보보호학회 회장 (현) 명예회장
2007년 7월 ~ 현재 ISMS/PIMS 인증위원회 위원장
2014년 12월 ~ 현재 정보보호 준비도 평가 심의위원회 위원장
관심분야 : IoT 보안, 클라우드 보안, 개인정보보호 관리체계, 모바일 보안 등