편집위원 : 원유재 (충남대학교)

차세대 핀테크 인증 기술

김수형, 노종혁, 김영삼
한국전자통신연구원

요 약

모바일 결제, 스마트 뱅킹 등 우리 생활의 일상적인 금융 업무에서 차별화된 편의성을 제공하기 시작한 핀테크 서비스는 사람들의 높은 관심을 받고 빠르게 확산되고 있다. 고도화된 해킹, 정보 유출 등 보안사고가 빈번하게 발생하고 있는 현재의 ICT 서비스 환경에서도 전자금융 서비스가 보안 이외에 소비자의 이용 편의에 관심을 갖고 서비스할 수 있도록 지원한 대표적인 보안 기술은 글로벌 표준으로 자리잡은 FIDO 인증 기술이다. FIDO는 지문, 홍채, 정맥 등 높은 보안성과 편의성을 갖춘 다양한 인증 수단을 지원하여 패스워드와 같은 기존 인증 수단을 빠르게 대체하고 있는 중이다. 본고에서는 현재 상용화 적용되어 보편적인 인증플랫폼으로 자리잡기 시작한 FIDO의 추가적인 인증 요소로서 활용되어 보안을 좀 더 강화할 수 있는 상황인지 기반 인증 기술에 대해 소개하고자 한다. 본 고에서 소개되는 상황인지 기반 인증 기술은 사용자의 고유한 행동적 특징과 환경적 특징을 기계학습 기법을 통해 분석하여 사용자 본인여부를 확인할 수 있는 기술로 사용자에게 명시적인 인증 절차를 요구하지 않아 이용 불편 없이 기존 서비스에 쉽게 적용될 수 있고, 타인이 위조하기 어려운 행동 및 환경적 특징을 활용하는 장점을 갖고 있어 향후 핀테크 서비스의 보안을 한단계 끌어 올려줄 기술로 활용이 기대된다.

Ⅰ. 서 론

오늘날 사람들이 정보를 소비하고 세상과 소통하는 방식은 ICT의 급격한 발전을 통해 지난 10년전과는 많이 달라져 있다. 전자금융 서비스도 예외가 아니어서 '안전'만을 강조했던 불편한 서비스들은 점차 사라지고, '안전'에 '편리'함을 더한 핀테크 서비스가 등장하여 금융소비자들의 환영을 받으며 빠르게 확산되고 있다. 핀테크 서비스의 급격한 확산은 금융정책과 제도가 소비자들의 변화된 요구와 시대적 상황에 맞춰 변화된 것이 주요한 영향을 미쳤지만, 변화된 정책을 뒷받침할 수 있었던 ICT 기술의 발전도 크게 기여하고 있다고 보여진다. 특히, 다른 어떤 기술보다도 인증 기술의 발전으로 새로운 인증 경험을 제공한 것이 일반 금융소비자들에게는 가장 큰 변화로 체감할 것이다.

사용자의 본인여부를 확인하는 인증 기술은 지난 몇 십년 동안 패스워드 기술에 많이 의존하고 있었다. PC 키보드를 이용하는 인터넷 서비스 환경에서는 패스워드만큼 편리하면서도 보편적으로 사용할 수 있는 인증 기술은 찾아보기 어려웠기 때문이다. 하지만 오늘날처럼 스마트폰 금융 서비스가 주류로 자리잡고 있는 시대에서는 패스워드 입력이 그리 편리 하지도 않으면서 패스워드의 보안취약성으로 인한 금융 사고가 증가하는 추세에 있어 이에 대한 대안이 요구되었다. 사람의 기억에만 의존하는 패스워드는 생성 복잡도를 높이거나 수시로 변경하는 보안 정책을 반영한다고 하더라도 지능화된 해커의 공격을 막아 내기에는 효과적이지 않았다. 오히려 사용자의 불편을 초래함으로써 보안을 약화시킨다는 보고도 존재한다. 예를 들어, 영국 사이버보안센터(NCSC)의 조사에 따르면, 정기적인 패스워드 변경을 강요하는 것은 보안 취약성을 증가시킨다고 지적한다[1]. 사용자의 기억력 한계로 짐작 가능한 생성 규칙을 만들거나 변경된 패스워드를 어딘가에 메모하기 때문에 결과적으로는 보안이 더 취약해진다는 것이다. 따라서 인증 기술에 있어 사용자 편의성은 보안을 위해서도 매우 중요한 평가 요소로 인식되는 현실이다.

인증 기술의 두가지 핵심 평가 요소인 보안성과 편의성을 모두 만족시키기 위해 등장한 기술이 FIDO(Fast IDentity Online) 국제표준 기술이다[2][3][4]. FIDO는 금융과 ICT 의 대표적인 글로벌 기업들이 FIDO 연합체(Alliance)에 참여하여 보안성과 편의성을 모두 만족하는 기술 개발을 목표로 개발되었으며, FIDO 1.0 정식 규격이 2014년 12월에 처음으로 일반에 공개되었다. FIDO 표준이 공개 된지 약 2년밖에 안 지났지만 다양한 간편 결제 및 스마트 뱅킹 서비스 등이 FIDO 표준 기술을 활용하여 서비스를 제공하고 있을 정도로 전세계적인 관심과 사업화가 계속적으로 증가하고 있다. 또한 FIDO 표준

을 준용하는 인증 제품과 솔루션들이 국내외에서 출시되고 있고 국내에서만 '17년 1월 현재 28개의 업체가 FIDO 공식 인증(certification)을 받고 서비스 적용을 준비하고 있다.

FIDO 기술의 성공 요인을 어느 한가지로 정의할 수는 없을 것이다. 글로벌 영향력을 갖는 기업들의 참여, 금융 사고 증가로 인한 금융 기업들의 보안 강화 필요성, FIDO 표준을 구현할 수 있게 한 최신의 ICT 기술이 사용자 기기에 적용되는 등 다양한 요인들이 복합적으로 작용하여 FIDO의 성공을 견인 하였다고 보여진다. 하지만 이러한 다양한 요인들 중에서도 특히, 핀테크 서비스에 대한 사용자들의 기대, 즉 예전보다 간편하게 금융 서비스를 이용하고자 하는 사용자들의 요구가 매우 강렬했던 것이 확산 시기를 조금 더 앞당긴 계기로 작용했을 것이다. 많은 연구 보고서를 통해 설명되고 있어 본 고에서는 간단하게 언급만 하고 있지만, FIDO는 현재 FIDO 2.0[4]으로 발전하고 있어 FIDO 기술이 적용되는 범위를 스마트폰에서 PC/브라우저까지 확대해 나가고 있다. FIDO 2.0 기술을 주도하는 구글과 마이크로소프트는 브라우저 환경에서도 바이오 인증, USB 토큰 등 다양한 인증 수단을 지원하기 위해 기술 개발과 함께 W3C 웹 표준화를 진행 중에 있다. 사용자의 아이덴티티를 다루는 인증 기술은 범용성을 확보하는 것이 매우 중요하여 일부 업체의 독자적인 기술로는 성공하기가 어렵다. 따라서 IT공룡인 구글과 마이크로소프트는 협업을 통해 관련 생태계를 조성하기 위한 지난한 과정을 거치고 있는 것이다.

FIDO가 차세대 인증을 위한 새로운 무대를 마련했다고 한다면, 향후 전개될 무대에서 소비자에게 선택되는 인증 수단은 어떠한 방향성을 가지고 준비가 되고 있는지 궁금한 것이 사실이다. 최근 적용되기 시작한 바이오 인증 수단들은 계속적으로 유효하게 사용될 것으로 보이지만, 본 고에서는 최근 연구가 진행되고 있는 몇 가지 연구 사례를 통해 새롭게 선보이게 될 인증 기술에 대해 살펴 보고자 한다. 현재 인증 분야의 최신 연구들은 기계 학습 기법을 활용해 사용자 행위와 환경 정보의 고유한 특성을 파악하고자 노력하고 있다. 어떻게 보면 사람이 사람을 식별하는 것과 동일한 방법을 인증 기술에 채택하고 있다고 볼 수 있다. 사람은 눈과 귀를 통해 바깥 세상에 대한 정보를 획득하고 획득된 정보에 대한 종합적인 분석을 통해 가족과 친구, 직장 동료들을 구분하고 있다. 최신의 인증 기술 연구도 이와 유사하다. 스마트 기기들에 탑재된 빛, 소리, 압력, 가속도 센서들을 이용해 스마트 기기의 소유자가 고유하게 가지고 있는 행동적 또는 환경적 패턴을 분석하고 이를 통해 기기의 주인을 식별하고자 하는 것이 최신의 연구 주제들이다. 이러한 연구들 중에 대표적으로는 구글의 Abacus 프로젝트가 있다. 구글은 사용자의 스마트폰에서 센싱된 다양한 정보를 분석하여 사용자를 식별하고 최종적으로는 패스워드와 같은 명시적 인증 수단을 완전히 대체하고자 하는 목표를 가지고 있다. 스마트폰 센서들을 통해 지속적으로 획득된 정보들로 사용자의 얼굴과 음성, 걸음걸이, 화면 터치 패턴 등을 종합적으로 분석하고 분석된 정보에 기반해 스마트폰의 소유자를 식별하고자 한다. 또한 이렇게 식별된 정보는 현재의 지문인식 기술보다 더 높은 엔트로피(entropy)를 가지고 있다고 주장하기도 한다. 위와 같은 연구들을 바이오 인증 분야에서는 신체적 특징에 기반한 바이오 인증과 구분하여 행위적(behavioral) 특징 기반 바이오 인증이라고 하기도 하고 기계 학습 기법을 이용해 보안을 자동화(automation) 한다는 측면에서 인지 보안(cognitive security)이라는 용어로 설명되기도 한다. 본고에서는 사용자의 현재 상황을 규정하는 행위와 환경정보를 통해 사용자를 인식한다는 측면에서 상황인지(context-aware)라는 용어를 사용해 기술을 정의하고자 한다.

상황인지 기반 인증 기술의 현재 수준은 인식률에 있어서 아직 지문, 홍채 등과 같은 신체적 특징에 기반한 바이오 인증 기술에 비해 부족한 것이 사실이다. 하지만 아래와 같은 세 가지 측면에서 차세대 인증 수단의 후보 기술로 평가할 수 있다. 첫 번째는 무엇보다도 사용자 편의성 측면에 있다. 상황인지 기반 인증 기술은 사용자의 과거 행위/환경 패턴이 현재의 행위/환경 패턴과 유사 한지 분석하는 것에 기반을 두고 있기 때문에 사용자에게 별도의 인증 절차를 요구하지 않는다. 즉, 사용자는 서비스를 이용하는 중에도 본인임을 입증할 수 있는 큰 장점을 갖고 있다. 두 번째는 사용자의 편의성을 훼손하지 않기에 다양한 인증 요소를 함께 적용 가능하다는 것이다. 기존 서비스에서는 사용자 불편이 증가하여 두 개 이상의 서로 다른 인증 요소들을 함께 사용하는 멀티팩터(multi-factor) 인증을 적용하기 쉽지 않았다. 하지만 상황인지 기반 인증 기술에서는 사용자의 다양한 행위 패턴과 환경 패턴을 적용하더라도 큰 불편 없이 보안을 강화할 수 있는 장점이 있다. 마지막으로 세 번째는 지속적인 인증(continuous authentication)이 가능하다는 것이다. 인증 기술은 통상적으로 중요 리소스나 서비스에 접근하는 시점마다 적용되어 사용자를 확인하는 것이 중요한데, 인증 횟수가 늘어날수록 사용자 불만이 증가하게 되어 주요 시점마다 인증을 계속적으로 요구하는 것은 쉽지 않다. 그러나 상황인지 기반 인증은 사용자가 서비스를 이용하는 중에 본인임을 확인할 수 있기에 사용자에게 요구하는 인증 횟수를 줄여줄 수 있는 장점을 갖는다. 예를 들어, 한번 지문 인증을 수행하여 모바일 결제를 완료하면, 이후에는 추가적인 인증 절차 없이도 소유자가 계속적으로 스마트폰을 이용하는 것만 확인이 되면 결제를 수행할 수 있게 하는 것이다. 이러한 시나리오는 EMV와 같은 신

용카드 관련 표준화 기구에서도 최근에 논의하고 있는 주제이기도 하다.

본고에서는 위와 같이 사용자의 행위 패턴과 환경 패턴을 이용해 사용자 본인여부를 확인하는 기술들 중에서 크게 두가지 주제에 대해 소개하고자 한다. 제2장에서는 행위 패턴 중에서 키입력 패턴과 관련된 연구 사례를 소개한다. 제3장에서는 사용자 위치에 기반한 인증 기술의 동향과 연구 사례를 소개한다. 마지막으로 제4장에서 결론을 맺는다.

Ⅱ. 키입력 패턴 기반 인증

바이오 인증은 지문, 홍채, 정맥 등 사용자의 고유한 신체적 특징을 분석하여 인증하는 기술과 키 입력, 화면 터치, 마우스 움직임, 걸음걸이 등 사용자의 행위적 특징을 분석하는 인증 기술로 크게 구분된다. 신체적 특징을 이용한 바이오 인증 기술은 행위적 특징을 이용한 바이오 인증 기술보다 오랜 연구 경험을 통해 높은 인식률을 가지는 상업적 솔루션들이 많이 선보이고 있으나, 고가의 인식 센서 적용에 따른 비용문제로 인해 일반적인 서비스 적용에 어려움이 있어 왔다. 하지만 최근 바이오 인식 센서가 탑재된 스마트 기기들이 보급되기 시작하면서 점차 보편적인 기술로 활용되는 추세에 있다. 행위적 특징을 이용한 바이오 인증 기술은 본격적인 연구가 진행된 것이 오래지 않아, 현재까지는 낮은 인식률로 인한 상용화 적용이 어려웠던 것이 사실이다. 하지만 신체적 특징에 기반한 바이오 인증 기술이 위조, 도용 등의 공격에 취약하고 사용자에게 명시적인 인증 행위를 요구하는 한계가 있다면, 행위적 특징에 기반한 인증 기술은 사용자에게 별도의 인증 행위를 요구하지 않으면서도 위조, 도용에 강한 장점을 갖는다. 또한 최신의 스마트폰 센서들과 기계 학습 기술의 발전은 행위 기반 인증 기술의 성능을 획기적으로 끌어올려 곧 상업적인 적용이 가능한 수준으로 발전할 것으로 기대되고 있다.

본 고에서는 행위 기반 인증 기술에 대한 이해를 돕고자 키 입력 패턴에 기반한 인증 기술을 예로 들어 좀 더 자세히 설명하고자 한다. 스마트폰의 잠금 해제 또는 금융 관련 앱들은 사용자 인증의 일환으로 사용자에게 PIN 번호를 입력하도록 요구하고 있다. 그러나 개방된 스마트폰 사용 환경으로 인하여 사용자 PIN 번호가 쉽게 노출될 위험이 존재한다. 이러한 위험은 키 입력 패턴 기반 인증 기술을 함께 적용하면 극복이 가능하다. 동일한 PIN 번호가 입력되더라도 키 입력 패턴을 분석하여 현재의 사용자가 실제 스마트폰의 소유자인지를 구분이 가능하기 때문이다.

키를 입력하는 행위를 패턴화하여 사용자를 인증하는 기법은 키스트로크 다이나믹스 인증(keystroke dynamics authentication) 이라고 표현된다. 키입력 행위 기반 인증은 1970년대부터 컴퓨터와 키보드 환경에서 연구가 진행되어 왔다[5]. 최초의 연구는 키보드에서 하나의 키가 입력되고 다음 키가 입력되는 동안의 시간 차이를 특징으로 하여 사용자의 타이핑 리듬을 패턴화 하였다. 이후에는 키 시간 특징을 활용한 연구가 활발히 진행되어 왔고, 2000년 후반에 스마트폰이 등장하면서 전통적인 키 시간 특징 이외에 스마트폰에 내장된 여러 센서들을 활용한 키스트로크 연구가 진행되어 왔다.

기존 키스트로크 연구에서는 키스트로크에 사용된 특징들을 비교, 분석하여 효율적인 특징을 추출하기 보다는 전통적으로 사용되어 왔던 특징들을 사용하고, 분류기(classifier)를 이용하여 분류 성능을 향상시키는 연구들이 대부분이었다. 이에 본 고에서는 전통적인 키 시간 특징 이외에 스마트폰 환경에서 활용되고 있는 센서 기반 특징들을 활용하는 연구들에 대해서도 소개하고자 한다.

1. 키보드 입력 패턴 분석

1977년에 Alan S.는 IBM 컴퓨터에서 사용자가 키보드를 통해 입력한 키들 간의 시간 차를 특징으로 이용하는 연구를 처음으로 시도하였다[6]. Alan S.는 〈그림 1〉과 같이 키를 누르는 이벤트 down(D)와 키가 떼어지는 이벤트 up(U)를 이용하여 DU(Down-UP), UD(Up-Down), DD(Down-Down), UU(Up-Up) 등 4가지 특징을 추출하고, 연속된 키 입력 간의 연관성을 파악하고자 하였다. 키보드 입력 패턴을 분석할 때 아래 〈그림 1〉처럼 전체 입력 시간(Tot)을 이용하기도 한다.

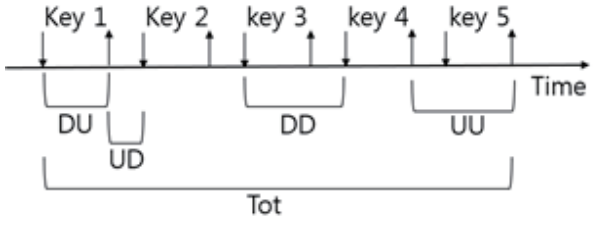

그림 1. 키 입력 시간 특징[7]

2. 스마트폰 센서 기반 입력 패턴 분석

최근 스마트폰에는 여러 가지 다양한 센서들이 내장되어 있다. 가속, 자이로스코프, 오리엔테이션, 중력 센서 등을 활용하면 기기의 미세한 상태 변화를 감지할 수 있다. 최근의 키 입력 패턴 연구는 이러한 센서들을 이용하여 〈그림 2〉와 같이 사용자가 키를 누르고 뗄 때 발생하는 변화를 특징으로 이용한다.

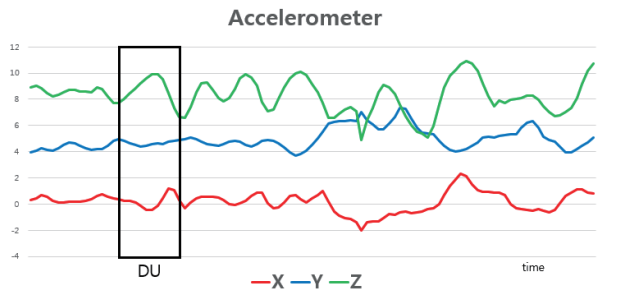

그림 2. 가속도 센서에서 추출되는 특징들

또한 스마트폰의 터치 스크린에서의 터치 크기와 터치 압력, 터치 좌표(x,y)를 특징으로 활용하기도 한다. Buchoux[8]는 〈그림 3〉과 같이 윈도우 모바일 폰에서 사용자 등록 및 인증 프로그램을 구현하여 실험하였다. 16명의 사용자에게 간단한 PIN 번호를 입력하게 하고, 마할라노비스 거리(Mahalanobis distance) 알고리즘 분류기를 이용하여 평균적으로 FRR(False Rejection Rate) 20.63%, FAR(False Acceptance Rate) 53.13%의 결과를 얻었다. 20명의 사용자를 대상으로 30번의 입력 데이터를 수집하여, 20번의 입력 데이터는 학습 데이터로 활용하고 나머지 10번의 입력 데이터는 실험 데이터로 사용한 결과이다.

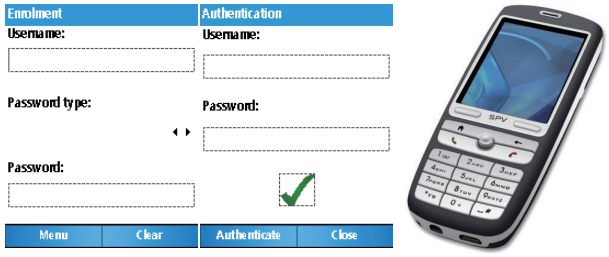

그림 3. 윈도우 폰에서의 입력 패턴 분석 [8]

Saevanee와 Bhatarakoso[9]는 기존의 키 시간 특징보다 터치 압력(pressure)의 특징을 이용하여 99%의 정확도를 얻었고, 키 시간 특징보다 터치 압력이 사용자의 패턴을 더 잘 나타낸다고 주장하였다. 터치 압력은 〈그림 4〉와 같이 계산하여 특징으로 활용한다. 남자 4명 여자 6명(총 10명)으로부터 10자리 핀 번호를 30번 연속으로 입력 받아 데이터를 수집하였다. 20개 데이터는 학습 데이터로 사용하고, 10개의 데이터는 실험 데이터로 사용하여 EER 1%의 결과를 얻었다. 작은 샘플을 대상으로 동일한 시간에 반복적으로 실험 데이터를 입력 받았기 때문에 좋은 결과를 얻었다고 추측해 볼 수 있다.

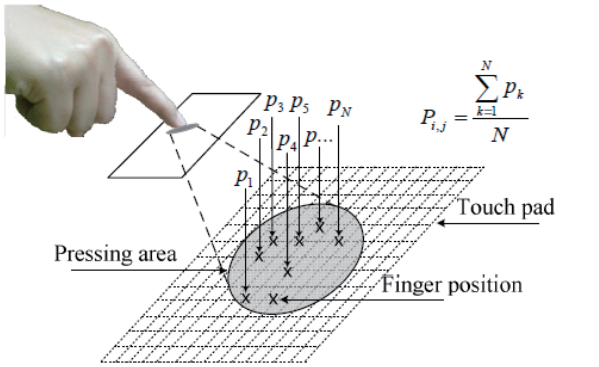

그림 4. 터치 압력 값 계산 방법[9]

Zheng[10]은 스마트폰 센서로부터 가속도(accelerometer), 터치 압력(pressure), 터치 크기(size) 특징을 추출하였다. 80명의 사용자들로부터 4-PIN, 8-PIN 데이터를 수집하여 EER 3.65%의 결과를 얻었다. 수집한 데이터 가운데 매끄럽지 않은 데이터는 아웃라이어(outlier)로 간주하여 제외하고 학습을 진행하였다. 사용한 특징은 〈그림 5〉와 같이 가속도 센서 값과 터치 압력 값, 터치 사이즈 값, 그리고 키 시간 특징에서 key hold time과 inter-key time(DU)을 사용하였다. 가속도 센서는 x, y, z축의 값을 갖는데, 해당 연구에서는 벡터 값으로 전환하여 사용하였다.

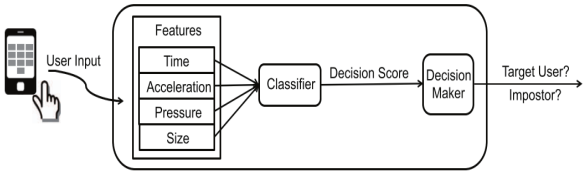

그림 5. 시스템 구조

ETRI에서는 키입력 특징 별 성능 평가 및 사용자 자세 기반 키입력 연구를 수행하였다[11]. 스마트폰은 이동성으로 인해 키보드 환경과는 다르게 여러 자세에서 사용이 가능하기에, PIN을 입력하는 자세를 손에 쥐고 입력하는 경우, 테이블 위에 두고 입력하는 경우, 걷는 상태에서 입력하는 경우로 구분하여 연구를 진행하였다. 15명의 실험 참가자로부터 15일간 각 자세 별로 5회씩 PIN을 입력하도록 하여 실험 데이터를 수집하였고, 수집한 특징 데이터는 키 입력 시간, 가속 센서, 자이로스코프 센서, 터치 사이즈, 터치 좌표이며, 이에 대하여 통계적 기법을 이용하여 사용자 패턴 특징을 분류하였다. 실험 결과 EER은 손에 쥐고 입력할 경우 7.35%, 테이블에 올려놓고 입력할 경우 10.81%, 걸으면서 입력할 경우 6.93% 이었다. ETRI의 연구는

학습 시간과 평가 시간을 달리하였고 입력 자세를 다양하게 연구하여 현실적인 인식률 평가가 가능하였다. 〈그림 6〉은 6자리 PIN을 입력한 사용자가 등록된 사용자인지 아닌지를 시연하는 동작 화면이다. 스마트폰 화면에서 분석결과를 그래프로 확인할 수 있도록 하고 있다.

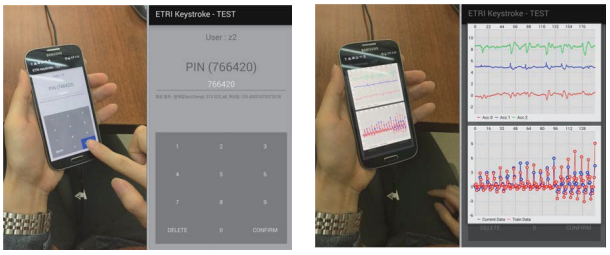

그림 6. 키입력 패턴 분석 화면

Ⅲ. 위치 기반 인증

스마트폰을 활용하여 지속적(continuous)이고 묵시적(implicit)으로 수집 및 활용이 가능한 위치정보는 사용자 인증의 한 요소로서 최근에 활발히 연구되고 있는 주제이다. 구체적으로, 위치 기반 인증 기술에 대한 연구는 두 가지로 분류해 볼 수 있다. 하나는 위치 정보에 기반하여 사용자의 컨텍스트(context)를 식별하고 안전성을 분석하는 연구이고, 다른 하나는 사용자의 위치 이력(location history)을 활용해 이동 행위 패턴(mobility behavioral pattern)을 분석하고 이를 사용자 식별 및 인증에 활용하는 연구이다.

1. 위치 컨텍스트 기반 인증

위치 컨텍스트 기반 인증 연구는 주로 스마트폰 잠금 해제의 사용성(usability)을 개선하기 위한 목적으로 연구되고 왔다. Marian Harbach[12]는 스마트폰의 잠금 해제를 위해 PIN, 패턴, 패스워드 등의 지식기반 인증을 사용하지 않는 비율이 약 57% 에 달하는데, 그 이유는 긴 인증 시간, 잦은 폰의 사용 등 사용성 문제가 큰 비중을 차지한다고 주장한다.

Markus Miettinen[13]와 Aditi Gupta[14]는 스마트폰의 GPS, Wi-Fi, Bluetooth 를 활용하여 사용자의 위치 컨텍스트에 대한 CoI(Context of Interest)를 생성하고 CoI에 대한 안전도를 분석하는 방법을 제안하였다. 구체적으로, CoI는 GPS 또는 Wi-Fi 데이터를 이용하여 생성되는데 임의의 위치에 머무르는 시간과 빈도가 CoI를 결정하는 특징이 된다. 예를 들어 GPS기반 CoI의 경우, 최대 100m 범위의 영역을 기준으로 지역을 분할하고 각각에 대해 방문 횟수와 방문 시간을 분석하여, 임의의 임계치 범위 내에 있는지를 기준으로 CoI 여부를 판단한다.

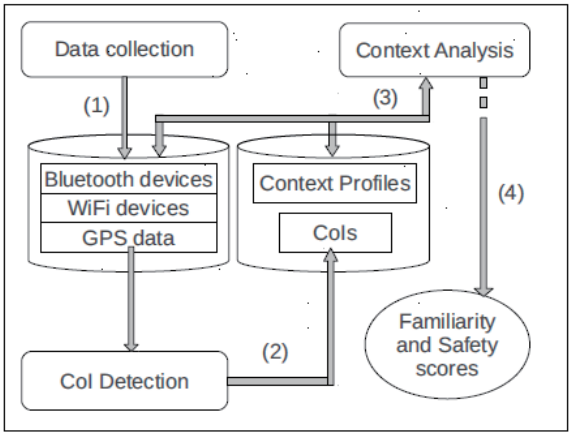

그림 7. 컨텍스트 분석 시스템 구성도[14]

위치 기반 인증을 위해서는 임의의 위치에 대한 안전도를 정량화하는 방법이 요구되는데, Aditi Gupta [14]는 컨텍스트 친숙도(context familiarity) 개념을 정의하고 CoI에 대한 친숙도 및 안전도를 정량화 하였다. 컨텍스트 친숙도는 〈그림 8〉과 같이 기기 친숙도(device familiarity), 순간 친숙도(instant familiarity), 집합 친숙도(aggregated familiarity)의 계층 구조를 기반으로 계산된다. 기기 친숙도는 사용자 주변의 블루투스 기기에 대해 독립적으로 계산되며, T개의 기기에 대한 기기 친숙 도를 평균하여 순간 친숙도를 계산하고, 여기에 smoothing 함수를 적용하여 최종적인 집합 친숙도를 얻게 된다. 그러나 친숙도는 단순히 주변 기기의 발견 빈도를 의미하기 때문에 그것을 안전도로 단순 매핑하는 것은 한계가 있다. 예를 들어 임의의 장소에서 자주 발견되는 기기라고 해서 그 기기를 신뢰한다고 평가하기는 어렵기 때문이다.

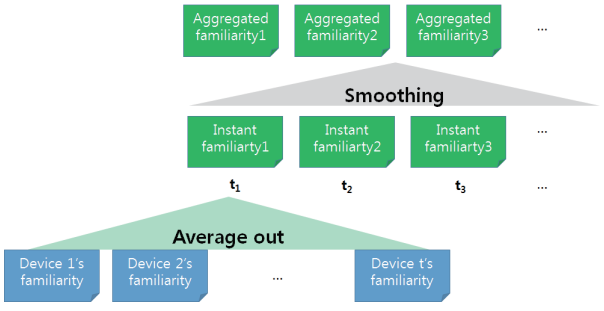

그림 8. Context familiarity 개념도[14]

Eiji Hayashi[15]는 필드 스터디를 통해 위치 기반 인증의 인증 강도를 정량화하고자 하였다. 36명의 참가자를 대상으로 위치 데이터를 수집하였으며, 수집한 기간은 최소 7일에서 최대 140일까지 다양하였다. 실험 결과, 집과 직장에서 보내는 시간이 38.9%, 18.7%로 나왔으며 익명의 세 곳의 위치 및 기타 위치에 대해 각각 9.9%, 5.5%, 4.3%, 22.6%가 나왔다. 이러한 통계치를 바탕으로 특정 위치에 대한 인증 강도를 계산하고자 하였다.

2. 위치 이력 기반 인증

위치 이력(location history) 기반 인증은 시간에 따른 위치의 변화를 관찰함으로써 사용자의 이동 행위 패턴을 모델링하고 이를 기반으로 사용자를 인증하는 방법이다. 구글의 ATAP(Advanced Technology and Projects) 프로젝트에서 진행되고 있는 관련 연구[16][17]가 대표적이다.

위치 기반 인증 연구는 실험적으로 성능 평가가 이루어지기 때문에 연구와 관련된 양질의 데이터를 확보하는 것은 매우 중요하다. 구글은 스마트폰에서 수집 가능한 각종 센서 데이터, 카메라를 통한 이미지, GPS 데이터, Wi-Fi 데이터, 키입력 데이터 등 다양한 데이터를 수집하여 데이터 셋을 구축하였다[16]. Upal Mahbub[16]에 의하면, 구글은 1500명으로부터 5개월간 수집한 27.62TB의 데이터 셋을 가지고 있으며 연구용으로는 48명으로부터 2개월간 수집한 141.14GB의 UMDAA-02 데이터셋을 확보하고 있다. Upal Mahbub는 사용자 인증에 관해서는 얼굴과 스와이핑 패턴을 이용한 결과를 제시하였으며, 위치 정보에 관해서는 다음 이동 장소를 예측하는 방법에 관해서만 언급하였다. 위치 이력 기반 인증에 관한 연구는 이후 발표한 PATH[17]를 통해 공개되었다.

Upal Mahbub[17]가 제안한 PATH(Person Authentication using Trace Histories) 시스템은 〈그림 9〉와 같이 구성되며 위치 군집 모델(Location Cluster Model)과 사용자 검증 모델(User Verification Model)을 생성하여 사용자 인증이 이루어지는 구조이다. 위치 군집 모델은 DBSCAN[18] 알고리즘을 사용하고 있으며, 사용자 검증 모델은 위치 군집 정보에 관측 시각(주중, 주말, 오전, 오후, 밤)을 결합한 순차 데이터를 HMM(Hidden Markov Chain) 알고리즘에 적용하고 있다. UMDAA-02 데이터 셋에 대한 성능평가를 통해 약 20%의 EER이 실험적으로 증명되었다.

위치 이력 기반 인증은 위치 데이터의 시간적인 변화를 고려하기 때문에 위치 기반 인증에 비해 강한 인증 강도를 제공할 수 있다. 그러나 키스트로크, 스와이프 패턴 등의 타 행위 인증에 비해 상대적으로 높은 EER은 개선해야 할 문제이다.

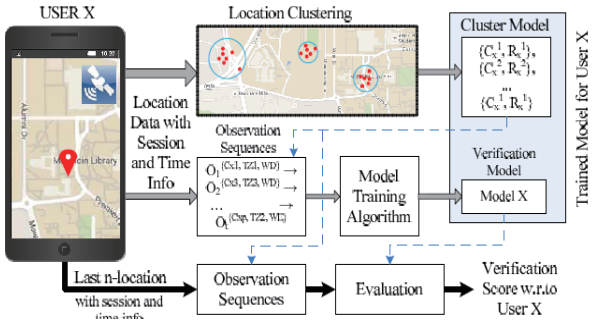

그림 9. PATH 시스템 개념도[6]

3. 실내위치 기반 인증 기술

기존의 위치 기반 인증 연구는 스마트폰의 GPS 또는 Wi-Fi를 이용하여 수집한 위치 정보를 이용하였다. PATH[17] 시스템은 집, 직장, 학교, 쇼핑몰 등 건물 단위의 실외 위치 이력 데이터를 활용한 사용자 인증에 대해 연구하였고, CoI 및 친숙도 기법[13][14]은 Wi-Fi AP 목록에 기반한 실내 위치를 활용하여 위치 컨텍스트의 안전도를 분석하고자 하였다. 최근에는 실내 위치를 활용하여 좀 더 세밀한 위치 이력을 수집하고 이를 기반으로 실내 위치 이력 기반 인증 방법에 대해 연구가 진행 중이다. 실내 위치 및 위치 이력 기반 인증의 기반이 되는 Wi-Fi 핑거프린트 기반의 실내 측위 기술에 대해 살펴본다.

Wi-Fi 핑거프린트는 스마트폰에서 스캔 가능한 Wi-Fi AP 목록과 해당 AP로부터의 신호 세기 정보로 정의된다. Wi-Fi 핑거프린트 기반 실내 측위 기술은 Wi-Fi 핑거프린트 데이터를 위치 별로 수집하여 데이터베이스를 구축하고 이를 기계 학습 기법을 통해 학습한다. 지도 학습의 특성상 학습을 위한 데이터베이스를 확보하는 것이 일차적으로 중요하지만 사람이 직접 위치 별로 이동하며 데이터를 수집해야 하기 때문에 수집 위치가 많아질수록 데이터베이스 구축 비용이 증가하는 문제가 있다. 즉, Wi-Fi 핑거프린트 데이터베이스는 다양한 날짜와 시간대에 걸쳐 다양한 환경 변화 요소들을 담아내는 데 한계가 있다. 이를 극복하기 위해서 Wi-Fi 핑거프린트 데이터베이스의 분석을 통해 중요한 특징만을 선택적으로 사용하는 특징 선택 방법이 요구되는데, 최근 연구 결과[19]에서는 탐지 빈도가 높고 신호세기가 강한 AP만을 특징으로 선택하고 있다. 구체적으로는 탐지 빈도와 신호 세기를 계산하고 계산된 수치를 기준으로 선택하는 특징의 수를 조절함으로써 측위 정확도를 향상시킬 수 있음을 보였다. 해당 연구의 평가는 실험 건물의 사무실을 대상으로 1개월간 수집한 Wi-Fi 핑거프린트 데이터베이스를 활용하였으며 특징 선택 적용 전에 93.5%의 정확도와 특징

선택 적용 시에 95.15%의 정확도를 확인할 수 있었다.

구글에서 진행하고 있는 위치 이력 기반 사용자 인증 기술은 GPS 또는 Wi-Fi, 기지국 데이터 기반의 실외 위치를 활용하고 있으며 20%대의 EER로 낮은 성능을 보여준다. [19]와 같은 실내 측위 연구 결과를 활용하여 사용자의 이동 행위의 패턴을 세밀하게 모델링함으로써 위치 이력 기반 사용자 인증의 인식률을 향상시킬 수 있다.

Ⅳ. 결론

지금까지 핀테크 서비스를 위한 차세대 인증 기술에 대해 살펴보았다. 특히, 사용자마다 고유하게 가지고 있는 행동적 또는 환경적 패턴을 통해 본인여부를 확인하는 상황인지 기반 인증 기술에 대해 소개하고 상황인지 기반 인증 기술의 많은 연구 주제들 중에서 키입력 패턴과 위치 패턴에 기반한 인증 기술의 연구 내용을 주로 설명하였다.

차세대 인증 기술로 각광을 받고 있는 현재의 FIDO 기술은 주로 사용자의 신체적 특징들을 이용한 인증 수단을 채택하고 서비스하고 있지만 향후에는 상황인지 기반 인증 기술과 결합되어 현재의 FIDO 기술이 가지고 있는 한계들을 극복해 나갈 것으로 보인다. 예를 들어, 신체적 특징에 기반한 인증 기술은 특징 패턴들이 유출되고 유출된 패턴을 통해 복제된 위조 생체를 사용한 공격에 일부 취약점이 있다. 상황인지 기반 인증 기술은 이를 극복할 수 있는 수단으로 사용될 수 있다. 상황인지 기반 인증 기술에서 사용되는 패턴 정보는 유출된다고 하더라도 위조 자체가 어려우며, 편의성 측면에서도 많은 장점을 가지고 있어 상호보완적인 기술로 활용이 가능하다.

기계 학습 기술의 발전으로 ICT 기술은 점차적으로 사람만이 가지고 있었던 고유한 기능들을 흉내내기 시작하고 있으며, 인증 기술 분야에서도 유사한 발전이 진행되고 있는 것을 확인할 수 있다. 사용자를 지속적으로 대면하는 스마트 기기는 자신이 가지고 있는 다양한 센서들을 통해 사용자를 모니터링하고 또는 주변 기기와의 협업을 통해서 현재의 사용자가 기기 소유자가 맞는지를 확인할 수 있게 되는 것이다. 이러한 기술 발전을 통해 향후 핀테크 서비스는 사람이 서비스를 이해하려고 노력하는 것 보다는, 서비스가 사람을 이해하기 위한 방향으로 발전하여, 편리하면서도 안전성이 담보되는 핀테크 환경을 구축해 갈 것으로 기대되고 있다.

Acknowledgement

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발 사업의 일환으로 하였음[B0126-15-1007, "상황인지 기반 멀티팩터 인증 및 전자서명을 제공하는 범용 인증 플랫폼 기술 개발"].

참고문헌

[1] National Cyber Security Center, "The problems with forcing regular password expiry," https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry, 2016

[2] 김수형, "FIDO 기반 핀테크 인증 기술," 한국통신학회, 한국통신학회지(정보와통신) 33(2), 2016.1, 59-65 (7 pages)

[3] 김수형 외, " 핀테크 시대: 새로운 인증 기술을 요구하다," 정보과학회지 제33권 제5호, 2015.5, 17-22.

[4] 조상래 외, " FIDO 2.0 범용인증기술 소개," 정보보호학회지 제26권 제2호, 2016.4, 14-19.

[5] GAINES, R. Stockton, et al. Authentication by keystroke timing: Some preliminary results. RAND CORP SANTA MONICA CA, 1980.

[6] ALAN S. NEAL, Time Intervals between Keystrokes, Records, and Fields in Data Entry with Skilled Operators. HUMAN FACTORS, 19(2), pages 163-170. 1977.

[7] Sung-Hoon Lee, Jong-hyck Roh, Soohyung Kim, Seung-Hun Jin, A study on feature of keystroke dynamics for improving accuracy in mobile environment, 17th WISA, August, 2016.

[8] A. Buchoux and N.L. Clarke. Deployment of keystroke analysis on a smartphone. In Australian Information Security Management Conference, 2008. p.48.

[9] H. Saevanee and P. Bhatarakosol. User authentication using combitnation of behavioral biometrics over the touchpad acting like touch screen of mobile device. In International Conference on Computer and Electrical Engineering (ICCEE), pages 82-86, 2008.

[10] N. Zheng, K. Bai, H. Huang, and H. Wang. You are how you touch: user verification on smartphones via tapping behaviour. IEEE 22nd International Conference

on Network Protocols. pages 221–232. 2014.
[11] Jong-hyuk Roh, Sung-Hun Lee, and Soohyung Kim. "Keystroke dynamics for authentication in smartphone." Information and Communication Technology Convergence (ICTC), 2016 International Conference on. IEEE, 2016.
[12] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith, "It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception," SOUPS 2014, pp. 213–230, Menlo Park, CA, July, 2014.
[13] Markus Miettinen, Stephan Heuser, Wiebke Kronz, Ahmad-Reza Sadeghi, and N. Asokan, "ConXsense - Context Profiling and Classification for Context-Aware Access Control," ASIACCS 2014, Kyoto, Japan, June, 2014.
[14] Aditi Gupta, Markus Miettinen, N. Asokan and Marcin Nagy, "Intuitive Security Policy Configuration in Mobile Devices using Context Profiling," SocialCom 2012, pp. 471–480, Jan. 2013.
[15] Eiji Hayashi, Sauvik Das, Shahriyar Amini, Jason Hong, and Ian Oakely, "CASA: Context-Aware Scalable Authentication," SOUPS 2013, pp. 1–10, Newcastle, UK, July, 2013.
[16] Upal Mahbub, Sayantan Sarkar, Vishal M. Patel, and Rama Chellappa, "Active User Authentication for Smartphone: A Challenge Data Set and Benchmark Results," BTAS 2016, Sept. 2016.
[17] Upal Mahbub and Rama Chellappa, "PATH: Person Authentication using Trace Histories," UEMCON 2016, New York, USA.
[18] J. Sander, M. Ester, H.-P. Kriegel, and X. Xu. Density-based clustering in spatial databases: The algorithm gdbscan and its applications. Data Min. Knowl. Discov., 2(2):169 - 194, June 1998.
[19] Youngsam Kim and Soohyung Kim, "Rethinking of Feature Selection Method for Room-Level Localization using Public APs," ICACT 2017, Pyeongchang, Korea, Feb. 2017.

약 력

김 수 형

1996년 연세대학교 공학사
1998년 연세대학교 공학석사
2016년 학국과학기술원 공학박사
1998년~2000년 한국정보통신 연구원
2000년~현재 한국전자통신연구원 인증기술연구실 실장
관심분야: 인증, 금융보안, ID관리 등

노 종 혁

1996년 인하대학교 공학사
1998년 인하대학교 공학석사
2006년 인하대학교 공학박사
2000년~현재 한국전자통신연구원 정보보호연구본부 책임연구원
관심분야: 정보보호, 기계학습, 패턴인식

김 영 삼

2009년 충북대학교 공학사
2011년 UST 공학석사
2010년~2013년 수리과학연구소 미래인터넷연구팀 연구원
2014년~2015년 ㈜엠투브 S/W 개발팀장
2015년~현재 한국전자통신연구원 정보보호연구본부 연구원
관심분야: 상황인지 기반 인증, 인증 프로토콜