ETRI

2018
Electronics and
Telecommunications
Trends

4차 산업혁명 사회의 초연결 지능과 신뢰 인터넷 기술 특집

무자각 지속인증 기술 동향

Trends in Implicit Continuous Authentication Technology

김승현 (S.H. Kim, ayo@etri.re.kr) 정보보호연구본부 선임연구원
김수형 (S.H. Kim, lifewsky@etri.re.kr) 정보보호연구본부 책임연구원/기술총괄
진승헌 (S.H. Jin, jinsh@etri.re.kr) 정보보호연구본부 책임연구원/본부장

Modern users are intensifying their use of online services every day. In addition, hackers are attempting to execute advanced attacks to steal personal information protected using existing authentication technologies. However, existing authentication methods require an explicit authentication procedure for the user, and do not conduct identity verification in the middle of the authentication session. In this paper, we introduce an implicit continuous authentication technology to overcome the limitations of existing authentication technology. Implicit continuous authentication is a technique for continuously authenticating users without explicit intervention by utilizing their behavioral and environmental information. This can improve the level of security by verifying the user's identity during the authentication session without the burden of an explicit authentication procedure. In addition, we briefly introduce the definition, key features, applicable algorithms, and recent research trends for various authentication technologies that can be used as an implicit continuous authentication technology.

* DOI: 10.22648/ETRI.2018.J.330106

* 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임[No. 2015-0-00168, 상황인지기반 멀티팩터 인증 및 전자서명을 제공하는 범용인증플랫폼기술 개발].

Ⅰ. 개요

현대 사용자들의 온라인 서비스 사용이 심화되고 있다. 인터넷 서비스뿐만 아니라, 최근의 O2O(Online-to-Offline) 서비스를 통해 대부분의 활동을 온라인으로 수행할 수 있게 되었다. 이러한 변화로 사용자가 검색한 정보, 소셜네트워크 활동과 같은 온라인 사용 이력이나 결제정보 등의 다양한 개인정보가 온라인 서비스에 저장된다. 저장된 개인정보는 해커의 타켓이 되기 때문에, 사용자 본인만 접근 가능하기 위한 인증 절차가 매우 중요하다. 하지만 기존 인증기술의 허점을 노리는 해커의 공격이 고도화되고 있다.

인증은 〈표 1〉과 같이 지식 기반, 소유 기반 및 생체인식 기반 인증으로 나눌 수 있다. 지식 기반 인증은 암호 또는 PIN과 같은 기억 정보를 통해 사용자 신원을 확인한다. 지식 기반 인증은 사용하기에 편리하지만, 무차별(Brute force) 공격, 사전(Dictionary) 공격, 어깨너머(Shoulder surfing) 공격 및 얼룩(Smudge) 공격에 취약하다.

소유 기반 인증은 OTP(One Time Password)나 공인인증서처럼 사용자가 소지한 객체를 기반으로 사용자를 인증하는 방식을 말한다. 소유 기반 인증은 사용자가 인증토큰을 소유하고 있어야 하기 때문에 지식 기반 인증보다 보안성이 높다. 그러나 인증시스템 구축이 어렵고, 사용자가 서비스 신청을 위해 CA(Certification Authority) 또는 RA(Registration Authority)와 최소 1번의 대면으로 본인 확인이 필요하며 항상 소유하고 있어야 하므로 편리성이 낮다는 단점이 있다.

생체인식 기반 인증은 사용자의 생체 인식 특성을 통해 사용자의 신원을 확인한다. 생체인식은 물리적 유형과 행동적 유형으로 구분된다. 물리적 생체인식에는 얼굴, 음성, 손바닥 등이 포함되며, 행동적 생체인식에는 서명, 키스트로크 다이나믹스, 걸음걸이 등이 포함된다. 생체인식 기반 인증은 고유성으로 인해 분실, 도용 또는 모방하기가 어렵다. 또한, 사용자가 별도의 지식정보를 기억하거나 인증토큰을 소유하지 않아도 되기 때문에 편리성이 높다.

〈표 1〉 기존 인증기술

방법	사례	속성
지식	ID, 패스워드, PIN 번호	공유가능, 망각
소지	카드, 열쇠, 토큰, 인증서	공유가능, 복제
생체	얼굴, 음성, 지문	공유불가능, 부인방지

생체인식 기반 인증 중에서 물리적 생체 인식이 가장 우수한 식별 성능을 나타낸다. 하지만 높은 식별력을 얻기 위해서는 전용 스캐너와 같은 최신 장비가 필요하다. 또한, 사용자의 고유한 생체정보의 비밀성과 무결성이 훼손될 경우에 큰 문제가 발생할 수 있다. 대조적으로, 행동적 생체인식은 사용자의 행동 패턴이 일관되는지와 타 사용자와 큰 차별성을 보이는가에 따라서 식별 성능이 변동한다. 하지만 인증 절차가 명시적이지 않고 별도 장비를 요구하지 않을 수 있다. 이 때문에 다른 인증 방식과 함께 연동될 수 있고 지속적으로 사용자의 신원을 검증하는 데 사용할 수 있다.

FIDO(Fast IDentity Online) 얼라이언스(Alliance)는 2012년 7월 설립된 협의회로 온라인 환경에서 생체인식기술을 활용한 인증방식인 FIDO 기술표준을 정의하였다[1]. FIDO 기술은 패스워드 인증의 문제점을 해결하기 위해 제안된 사용자 인증 프레임워크로, 사용자를 인증하는 방법과 그 인증 정보를 주고받기 위한 인증 프로토콜을 분리하였다. FIDO 표준은 패스워드 없는 인증을 수행하는 Universal Authentication Framework (UAF) 프로토콜과 소지기반 인증을 위한 Universal 2nd Factor(U2F) 프로토콜로 구성된다[2]. FIDO 프레임워크 하에서 기존인증 기술인 지식 기반, 소유 기반 및 생체인식 기반 인증을 모두 적용할 수 있다.

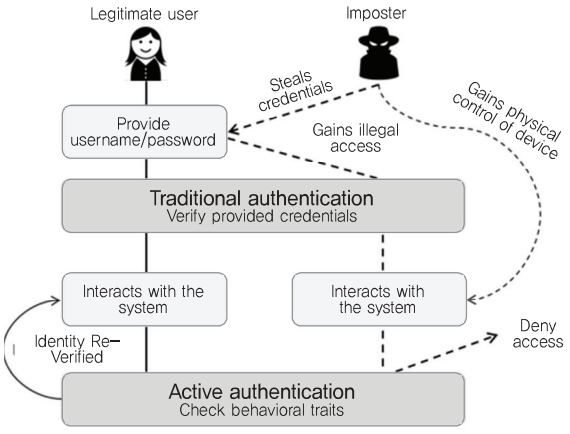
Ⅱ. 무자각 지속인증 기술

기존 인증방식은 사용자의 신원을 검증해야 할 때마다 명시적인 인증 절차를 거쳐야 한다. 명시적 인증은

사용자에게 불편한 인증 절차를 정기적으로 요구하기 때문에 편의성 문제가 있다. 또한, 명시적 인증을 통과한 이후의 신원점검이 이루어지지 않기 때문에 해커의 인증수단 도용이나 인증세션을 가로채는 공격에 취약하다.

이 때문에 원래 인증된 사용자의 신뢰성을 지속적으로 검증할 수 있는 새로운 인증 방법이 연구 중이다. 이러한 유형의 인증은 일반적으로 다양한 시점에서 시스템이 현재 사용자의 신원을 명시적이지 않은 방법으로 검증하려고 시도한다. 본 논문에서 우리는 이러한 유형의 인증을 무자각 지속인증이라고 부르고, '행위 및 환경 정보를 활용하여 사용자의 명시적 개입 없이 지속적으로 신원을 검증하는 기술'로 정의하였다.

무자각 지속인증은 전통적인 명시적 인증의 한계를 극복한다. (그림 1)은 기존 인증과 무자각 지속인증의 차이점을 보인다. 지속적으로 사용자의 신원을 검증하기 때문에, 명시적 인증절차를 통과하거나 인증세션을 가로챈 해커일지라도 접근을 차단할 수 있다. 예를 들어, 사용자가 시스템에 로그인 한 다음 로그아웃이나 화면 잠금없이 본인의 컴퓨터에서 멀어지는 상황을 고려해보자. 기존 인증방식에서는 해커가 사용자인 것처럼



(그림 1) 기존 인증과 무자각 지속인증의 차이점

[출처] A.A. El Masri, "Active Authentication Using Behavioral Biometrics and Machine Learning," PhD Thesis, George Mason University, 2016.

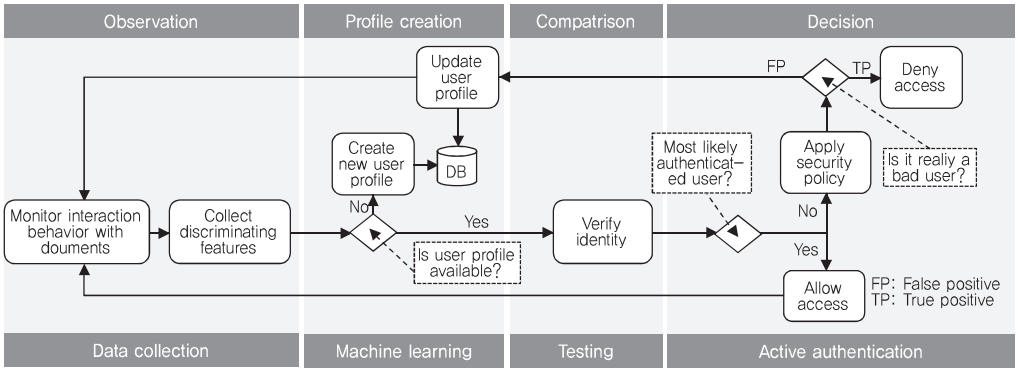
시스템 내에서 자유롭게 행동할 수 있지만, 무자각 지속인증에서는 해커가 시스템에 의해 감지되어 명시적인 인증방식을 요구받게 된다. 또한, 사용자는 일정 시간 또는 이벤트마다 시스템에 명시적으로 인증할 필요가 없어진다. 시스템은 무자각 지속인증으로 사용자의 신원을 검증하고, 검증이 실패한 경우에만 명시적 인증을 요청할 수 있다.

무자각 지속인증을 제공하는 시스템은 두 가지 주요 특성을 충족해야 한다.

- 무자각 인증: 시스템은 현재 사용자에게 명시적인 고지없이 사용자의 신원을 모니터링하고 확인함으로써 정상적인 서비스 흐름을 방해하지 않고 작동해야 함. 무자각적인 속성을 충족시키기 위해, 무자각 인증 기술은 대부분 생체인식 기반 인증을 사용.
- 지속 인증: 시스템은 지속적으로 해당 사용자의 신원을 확인해야 함. 사용자 신원 검증은 시간 또는 이벤트를 기반으로 시작될 수 있음. 시간 기반 모델에서, 시스템은 사전에 정의된 시간 간격에 따라 현재 사용자의 신원을 확인하려고 시도함. 이벤트 기반 모델에서, 시스템은 특정 이벤트 발생 또는 시스템의 상태정보 변경에 따라 현재 사용자의 신원을 확인하려고 시도.

무자각 지속인증의 기본 프로토콜은 다음과 같다[(그림 2) 참조].

1. 관찰 단계: 시스템은 사용자와의 상호 작용에서 무자각적으로 모니터링하고, 사용자 특화된 속성으로 알려진 데이터 요소를 수집.
2. 프로파일 생성/업데이트 단계: 시스템은 사용자 프로파일 저장소를 참조하여 현재 사용자 프로필이 있는지 확인. 이전에 시스템과 상호 작용한 사용자 프로파일이 없으면, 새 사용자 프로파일



(그림 2) 무자각 지속인증의 기본 프로토콜

[출처] A.A. El Masri, "Active Authentication Using Behavioral Biometrics and Machine Learning," PhD Thesis, George Mason University, 2016.

을 작성사고 수집된 데이터로 갱신. 사용자 프로파일이 발견되면 수집된 데이터로 검색한 뒤 갱신.

3. 비교 단계: 시스템은 사용자가 실제로 사용자 본인이 맞는지를 판단. 저장된 사용자 프로파일과 새로 수집된 데이터 간에 기계 학습 알고리즘을 적용하여 결정을 내릴 수 있음.
4. 결정 단계: 시스템은 사용자와 계속 상호작용할지를 결정. 기계학습 알고리즘이 현재 데이터를 인증된 사용자에 속하는 것으로 분류하면 승인 결정을 내리고, 아니라면 거부 결정을 내림. 거부 결정인 경우, 시스템은 사용자의 시스템 접근 잠금, 시스템 관리자에게 경고, 사용자에게 재인증 요청 등의 다양한 조치를 정책에 따라 수행할 수 있음.

인증된 사용자가 액세스가 부당하게 거부된 경우(False Positive), 시스템은 오분류한 상호작용 데이터로 사용자 프로파일을 업데이트함으로써 해당 오류에 적응할 수 있어야 한다. 시스템은 사용자의 상호작용 동작 변화를 재학습하여 향후 오탐지를 줄인다.

Ⅲ. 무자각 지속인증용 인증수단

본 장에서는 무자각 지속인증에 사용 가능한 인증수단을 열거하고, 각 인증수단의 특징 및 연구 동향을 간략히 소개한다. 무자각 지속인증에 사용 가능한 인증 수단의 선별을 위해 다음의 기준을 따른다. 첫째, 별도의 인증용 추가단말을 사용자에게 요구하지 않는다. 가령, 다른 용도로도 활용되는 스마트워치와 같은 기존 웨어러블의 센서를 활용한 인증수단은 포함하지만, 뇌파인증의 경우 사용자가 전용의 뇌파 장치를 장착해야 하기 때문에 제외한다. 둘째, 인증을 위해 사용자에게 명시적인 행동을 요구하거나 명시적 인증과 결합하여 동작하지 않는다. 가령, 온라인 서명에서의 필적 검증, 패스워드 입력에 대한 키스트로크 다이나믹스, 패턴암호에 대한 터치 다이나믹스는 해당 시점에서만 인증을 수행하기 때문에 제외한다.

1. 얼굴

얼굴(또는 안면) 인식은 안면 특징을 사용하여 디지털 이미지 또는 비디오 프레임에서 사람을 식별하는 인증 방식이다. 얼굴 특징적 요소로는 각 부분(눈, 코, 입, 광대뼈 및 턱)의 위치/크기/모양, 피부나 머리카락의 질감(주름, 패턴, 반점)이 주로 사용된다[3]. 일반적인 얼굴 인식 시스템은 세 가지 주요 단계로 구성된다. 첫 번째 단계에서는 카메라로 촬영한 이미지 또는 비디오에서 얼굴을 감지한다. 그런 다음 얼굴의 전체적인 특징 또는

얼굴 일부의 특징을 추출한다. 마지막으로 추출된 얼굴 특징을 분류기로 전달하고, 기등록된 사용자의 특징 정보와 일치 여부에 따라 인증 여부를 결정한다.

안면 인식을 무자각 지속인증에 활용하기 위해서는 얼굴의 전체적인 특징보다 부분의 특징을 더욱 중요하게 고려해야 한다. 무자각 상황에서 지속적으로 획득하는 이미지에는 사용자의 얼굴이 온전히 표현되지 않고 일부분만 존재하는 경우가 많기 때문이다. Google ATAP 부서의 연구원들은 머신러닝 기술을 사용하여 핸드폰의 전면 카메라로 획득한 부분 얼굴 이미지를 사용해 실시간 안면 인식을 수행할 수 있게 하는 가벼운 알고리즘을 개발했다[4]. 이 기술은 FSFD(Facial Segment-based Face Detector)이라 불리며, 사람의 다양한 얼굴 이미지를 얼굴 요소들로 조각내고 얼굴 영역을 추정하는 단계, 부분 얼굴 이미지와 실제 사용자를 패턴화하는 머신러닝 단계, 안면 인식 시스템이 얼굴의 부분적 이미지들에 신뢰도 레벨을 할당하는 단계를 가진다. 테스트 결과, FSFD는 부분 얼굴과 전체 얼굴을 탐지할 수 있었고 조명과 포즈의 변화에 거의 영향을 받지 않았다.

무자각 상황에서 수집하는 얼굴 영상은 사용자의 자세나 조명 변화에 따라 전혀 다른 성능을 보일 수 있다. 이 문제를 해결하기 위해 최근에는 DNN(Deep Neural Network) 기반의 얼굴 인식 방법이 연구되었다[5]. 제안된 방법은 임베디드 환경에서 구동할 정도로 모델의 복잡도가 낮고 자세와 조명 변화에 강하며 Android 기반 모바일 임베디드 플랫폼에서 실시간으로 실행할 수 있음을 입증했다. 다른 연구에서는 DCNN(Deep Convolutional Neural Network) 기반의 방법이 개발되었다[6]. 이 방법은 먼저 Alexnet[7]의 처음 다섯 레이어를 사용하여 깊은 피쳐를 추출하고, 특정 크기의 얼굴 이미지를 감지하기 위해 각 창 크기에 대해 SVM(Support Vector Machine)으로 학습했다. 이 검출기는 조명 변화에 매우 견고하며 얼굴 일부 이미지만으로도 신원을 검증했다.

2. 음성

화자(Speaker) 인식은 목소리의 특징을 활용하여 말하는 사람을 식별하는 인증 방식이다. 이 개념은 관절 기관(성대의 구조, 비강의 크기, 성대 특성) 및 말하기 방식의 고유한 차이에 따라 다른 음성 서명을 가지고 있으며, 동일한 단어가 다른 억양이나 다른 상황으로 말하면 다른 의미를 가질 수 있다는 특징에 기반한다. 화자 인증 시스템은 발화하는 문장에 따라서 텍스트 의존적과 텍스트 독립적으로 나뉘는데, 무자각 지속인증을 위해서는 등록 및 검증 중에 임의의 텍스트를 사용하는 텍스트 독립적인 방식이 요구된다.

화자 인식 시스템에서 사용하는 음성 특징적 요소는 사용자 간에는 큰 차이가 있지만, 동일 사용자의 다른 세션에서는 작은 변화를 가져야 한다. 또한, 모방, 재현, 잡음 및 채널 효과에 강건해야 한다. 초기의 화자 인식 기법은 스펙트럼 표현과 피치와 같은 음향 특징의 장기적인 평균값을 사용했으나, 긴 음성 데이터를 요구하여 화자의 많은 의존 정보가 손실된다. 성대 특성을 모델링한 LPC(Linear Predictive Coefficient) 매개 변수, 스피커의 성문 정보를 나타내는 LPC 잔여 신호, 필터 뱅크 기법을 모델로 한 MFCC(Mel Frequency Cepstral Coefficient), PCA(Principal Component Analysis)를 사용한 특성추출 방법[8]이 연구되었다.

일단 특징 피쳐 세트가 생성되면 학습 데이터로 화자 모델을 훈련한다. 화자 모델은 템플릿 모델과 확률 모델로 분류할 수 있다. VQ(Vector Quantization) 접근법은 텍스트 독립적인 화자 인식에 사용되며 기본적으로 클러스터링 절차로 모든 스피커에 대한 코드북을 만든다. 확률 모델은 GMM(Gaussian Mixture Model)과 HMM(Hidden Markov Model)을 포함한다. GMM은 화자 인

식 시스템에서 거의 표준화된 방법으로, 목소리 확률적 모델로 표현한다. 또한 화자 인식 목적으로 사용되는 일부 보컬 트랙 특성 및 스펙트럼 모양은 개별 가우스 성분으로 나타낸다.

신경망 기법의 모델은 특정 화자를 표현하기 위해 개별 모델을 훈련하는 대신, 알려진 세트와 가장 잘 구분되는 의사 결정 기능을 모델링한다. 이 접근법은 각 화자에게 자신의 발화에 의해서만 활성화되는 개인화 된 신경망을 제공한다. MLP(Multi-Layer Perceptron), GRNN(General Regression Neural Network), RBF (Radial Basis Function) 등의 모델이 화자 인식 시스템에 적용되었다.

3. 걸음걸이

걸음걸이(또는 보행, Gait) 인식은 사람의 걸음걸이 형태의 특징을 추출해 사용자를 인증하는 방식이다. 이는 의학계에서 오래전부터 연구한 기법으로, 신경이나 근육, 뼈 등에 이상이 있으면 비정상적인 걸음걸이가 나타난다는데서 착안했다. 보행은 골격이나 근육 등의 체격적인 특징 또는 걷는 방법 등의 동적인 특성으로 개인을 식별할 수 있다.

보행 인증에는 머신 비전 기반, 바닥 센서 기반, 웨어러블 센서 기반의 세 가지 주요 유형으로 구분된다[9]. 머신 비전 기반 접근법에서 보행 동작은 비디오로 캡처되어 신호 처리, 이미지 처리 및 기계 학습 기술로 보행 정보 및 개인을 식별한다. 바닥 센서 기반 접근법에서는 바닥에 설치된 센서로 개인이 걸어올 때의 힘이나 압력을 측정하여 개인 식별에 활용한다. 웨어러블 센서 기반 접근법에서 사용자는 보행을 측정하고 패턴을 인식할 수 있는 장치를 착용한다. 이 접근법은 속도, 가속도계, 자이로스코프 및 입력 센서와 같은 다양한 유형의 센서를 사용할 수 있다. 장소에 무관하게 무자각 지속인증을 수행하기 위해서는 웨어러블 센서 기반 접근법이 적합하다. 요즘 대부분 스마트폰에는 3축 가속도계가 내장되어 있기 때문에 스마트폰 기반 보행 인증이 활발하게 연구된다.

보행 인증을 결정하는 방식은 데이터의 특징 분석 또는 인증 알고리즘의 유형에 따라 다르다. 예를 들어, 상관관계, 주파수 영역 분석 및 데이터 분포 통계에 기반한 방법, 동적 시간 왜곡에 기반한 방법, 보행주기를 특징으로 사용할 수 있다. 인증 알고리즘으로는 KNN(K-Nearest Neighbors), HMM 등이 사용되었다.

수집 자세에 따라 걸음걸이의 인식 성능이 다르게 나타날 수 있다. 관련 연구에 따르면 인간의 팔다리 운동마다 특이성과 보편성의 수준이 다르다. 예를 들어, 벨트, 바지 앞주머니, 뒷주머니, 발목, 손 등에 장치를 부착하고 측정한 걸음걸이는 저마다 다른 신호를 보인다. [10]은 방향 센서를 사용하여 각 동작의 피치, 롤 및 제목을 수집하고 보행 자세의 특성을 활용하여 6.85%의 EER(Equal Error Rate)를 달성했다. [11]은 보행 인식을 위해 HMM의 적용과 함께 GDI(Gait Dynamic Images)라 불리는 센서 방향 불변 보행 표현 기법을 제안했다. GDI는 센서 방향과 관련하여 불변하므로 센서 회전 전후에 기존 방식에 비해 더 일관적인 결과를 보였다.

4. 키스트로크 다이나믹스

키스트로크(KeyStroke) 다이나믹스는 키보드 또는 키패드에 문자를 입력하는 방식과 리듬으로 사람을 식별하는 인증 방식이다. 이 개념은 타이핑 패턴이 학습된 운동 기술이며 행동 특성이 된다는 사실에 기인한다. 키스트로크 다이나믹스는 텍스트 입력 길이에 따라 단문(패스워드, 단어, 문장)과 장문(에세이, 산문)으로 구분 가능하다. 또한, 타이핑 패턴을 추출하기 위한 단어의 동일성 여부에 따라 정적 방법과 동적 방법으로 구분된다. 동적 방법은 일정한 단어에 국한하지 않고 일정시간 동안의 키보드 입력으로부터 지속해서 패턴을 분석하는

방법으로 무자각 지속인증에 적합하다.

키스트로크 다이나믹스의 특징적 요소로는 단일 키 동작(키 다운 이벤트와 키 업 이벤트 사이의 시간 차이), 키 다이그래프(Digraph) 동작(총 지속시간, 키를 눌렀다 놓은 시간(Down-Up Time), 두 개의 연속 키가 눌러진 시간(Down-Down Time) 사이의 경과 시간, 키가 다음 키로 해제될 때까지의 시간(Up-Down Time), 두 개의 연속 키가 해제되는 시간(Up-Up Time), 양극 활자, 삼중 그래프 및 사중 그래프가 사용되었다. 분류기를 구축하는 방법에는 통계적 방법, 퍼지 논리, 신경망, 유클리드 거리, SVM 알고리즘 방법이 사용되었다.

최근 연구에서는 사용자가 특정 단어에 대해 보이는 인지적 타이핑 리듬을 관찰하기 위해 SVM과 KRR (Kernel Ridge Regression) 알고리즘을 적용한 CTR (Cognitive Typing Rhythm) 인증 시스템이 제시되었다. 이 개념은 사용자에 따라 특정 단어에 대해 인지하는 시간 차이가 발생할 수 있고, 타이핑 패턴에 반영될 수 있다고 가정한다. 1,977 명의 사용자를 대상으로 실시한 실험 결과에 따르면 FRR(False Rejection Ratio)은 0.7%이고 FAR(False Acceptance Ratio)은 5.5%라는 성능을 보였다[12].

5. 마우스 다이나믹스

마우스(Mouse) 다이나믹스는 마우스를 움직이는 방식으로 사람을 식별하는 인증 방법이다. 마우스의 이점은 키보드보다 물리적 구조가 훨씬 간단하다는 것으로, 마우스 유형과 마우스 사용 환경에 덜 의존적이다.

마우스 다이나믹스의 특징적 요소로는 마우스 이동, 클릭, 더블클릭, 드래그 앤 드롭 및 동작 특성(각도, 속도, 이동 거리) 등과 같은 다양한 동작 범주로 나눠진다. 기존 특징적 요소를 분석하여 평균 이동 속도, 클릭 기반 간격 시간, 동작 막대 그래프 및 이동 거리당 평균 이동 속도를 특징적 요소에 추가로 포함할 수 있다.

[13]은 사용자가 일상적으로 컴퓨터를 사용하는 동안 수집한 마우스 데이터에 신경망을 사용하여 2.46%의 EER을 달성했다. [14]는 ANN(Artificial Neural Network)과 SVM를 통해 마우스 특징적 요소를 선택하고 계산을 보정한 결과, 1.86%의 FAR 및 3.46 %의 FRR을 달성했다. [15]는 사용자가 마우스로 클릭한 지점의 각도 기반 특징을 계산하여, 사용자 당 마우스 스트로크가 적지만 유사한 분류 결과를 얻는 방안을 제안하고 1.3%의 EER을 달성했다.

6. 터치 다이나믹스

터치(Touch) 다이나믹스는 터치스크린 장치를 터치하는 방식으로 사람을 식별하는 인증 방식이다. 터치 다이나믹스는 모바일 장치에서 가장 일반적으로 사용되는 지속 인증 방법 중 하나로, 화면 터치 동작(사용자가 모바일 장치의 터치스크린에서 손가락을 스와이프하는 방식)으로 스마트폰을 사용하는 동안 사용자를 무자각으로 지속 인증할 수 있다.

터치 다이나믹스의 특징적 요소에는 시간적 요소(터치 이벤트의 종류, 지속 시간(Dwell Time), 이벤트 사이 시간(Flight Time), 이벤트 길이(*n*-graph)), 공간적 요소(터치 위치, 터치 크기, 터치 압력), 동적 요소(가속도, 자이로스코프) 등이 사용된다. 사용자를 모델링하는 방식으로는 거리 측정(Euclidean, Manhattan, Mahalanobis, Bhattacharyya), 통계적(평균 및 표준편차, 편차 내성), 확률론적(Bayes, Naïve Bayes, GMM), 클러스터(*k*-means, *k*-Star, KNN), 의사결정 트리(J48, RF(Random Forest), SVM, RBFN(Radial Basis Function Network), MLP)가 사용되었다.

[16]은 기존의 터치 다이나믹스 특징적 요소와는 달리 GTGF(Graphical Touch Gesture Feature)라는 이미지 기반 기능을 제안했다. 이 접근법에서 스와이프 형상 특성은 이미지 공간으로 변환되어, 스와이프의 동적, 압력

특성을 명시적으로 모델링한다. 이 모델은 통계 분석 모델을 적용해 이미지 영역에 있는 GTGF의 사용자 동작 편차를 학습하고, 새로 추가된 스와이프에 따라 새로운 인스턴스를 합성하여 기존보다 더 나은 성능을 보였다.

7. 문체

문체(Stylometry)는 언어학적 형태에 기반하여 사람을 식별하는 인증 방식이다. 이 개념은 모든 사람이 서로 다른 작가를 구별하기 위해 계량화되고 측정될 수 있는 고유한 언어 스타일을 가정한다. 많은 연구자가 텍스트 분류, 저자 식별 및 저자 확인과 같은 여러 목적을 위해 언어 프로파일링의 타당성을 조사했다. 문체 기법은 긴 문서에 대해 높은 정확도를 달성할 수 있지만, 많은 저자 중에서 짧은 문서의 작성자를 식별하는 것은 어려운 것으로 알려져 있다. 무자각 지속인증을 위해서는 장문에 비해 단문에서의 문체 인증이 요구된다.

문체의 특징적 요소는 잠재적으로 무궁무진하며, 기존 연구에서는 기능(Function) 단어, 문법, 문자 n-gram 등을 사용했다. 원시 데이터는 모든 키 입력으로 구성되기 때문에, 맞춤법 오류나 삭제 패턴(문장을 선택하고 삭제를 누를 때, 백 스페이스를 반복적으로 누를 때)과 같은 언어 및 입력 특성을 추출할 수 있다.

문체 인증 방법으로는 각 특징적 요소들의 주기(Frequency) 측정 또는 빈도 평가를 주로 사용한다. 단문을 활용한 기존 연구들은 주로 전자메일의 저자 확인을 목표로 했다. [17]은 292개의 다른 특징을 추출하고 독자적인 분류 및 회귀 알고리즘을 적용했다. [18]은 150개의 문체 특징을 추출하여 n-gram 분석과 결합된 감독 학습 기법을 사용했다.

8. 위치

위치 기반 인증은 사람이 주로 생활하는 장소의 패턴으로 사람을 식별하는 인증 방식이다. 사용자의 이동성 정보를 통해 일상 활동에서의 사회적 패턴을 인식하고, 사회적으로 중요한 위치를 파악하고, 패턴화된 리듬을 모델링 할 수 있다. 스마트폰과 태블릿 같은 모바일 기기의 확산으로 인해 이동성 데이터를 정확하고 쉽게 장기간 수집할 수 있으며, 생활 패턴을 추론하기 위해 이동성 데이터를 마이닝하는 연구 활동이 증가 중이다.

위치의 특징적 요소로는 GPS 신호(시간, 고도, 위도, 경도), 자이로스코프, 가속도계, 자력계, 블루투스, WiFi, 셀 안테나 등이 일반적이며, 컨텍스트 정보(직장, 집, 쇼핑, 관광, 스포츠 활동) 등이 추가로 고려될 수 있다. 위치 데이터로부터 분류기를 구축하는 방법으로는 지리적 위치를 몇 가지 특성으로 클러스터링한 다음 상태 전이 궤도의 순차적 패턴 마이닝을 수행하는 방법, 템플릿 매칭 접근법, 문자열 일치 알고리즘, MMC (Mobility Markov Chains), MMM(Mixed Markov chain Model), HMM으로 상태 공간 모델을 구축하는 방법 등이 사용된다.

무자각 지속인증을 위한 위치 기반 검증 접근법으로 최근에 연구된 PATH(Person Authentication using Trace Histories)는 사용자의 기록 추적 데이터를 기반으로 최근 위치 추적을 사용하여 스마트폰의 현재 사용자를 인증하기 위한 신뢰도 점수를 생성한다. 연속적으로 사용자의 과거 위치 데이터로부터 사용자 검증을 수행하여 위치 정보에 기초한 검증 스코어를 연속적으로 획득한다. 새로운 위치를 처리하기 위해 사용자 데이터 클러스터링을 위한 고유한 방법이 도입되었고, 수정된 HMM 기반의 사용자 검증 방법인 MSMM(Marginally Smoothed HMM)을 제안했다[19].

9. 앱 사용습관

앱 사용습관에 기반한 인증은 사용자 행동, 습관 및 관심사에 따라 앱이나 웹에서의 동작이 차별화되는 특성으로 사람을 식별하는 인증 방식이다. 이 개념은 다른

사람들이 동일한 핵심 작업을 수행하기 위해 서로 다른 명령 세트를 사용한다는 사실에 기반한다. 이 연구 분야는 과거 유닉스와 같은 명령행 기반 시스템에서 사용자가 입력하는 명령을 모니터링하여 프로파일링하였으나, GUI(Graphic User Interface) 기반 시스템이 등장함에 따라 사용자의 GUI 상호 작용 스타일을 프로파일링하는 것으로 발전되었다.

앱 사용습관의 특징적 요소는 명령행 인터페이스와 GUI에 따라 서로 다른 요소를 가진다. 공통적으로는 사용자의 동작, 컨트롤 유형(스크롤 막대 사용, 버튼 클릭), 메모리 및 CPU 소비와 같은 정보가 활용될 수 있다. GUI에서는 열려있는 창의 수, 새 창 사이의 시간 및 창 제목의 단어 수, 열린 시간, 열린 상태의 앱, 열린 상태와 닫힌 상태 등의 특징적 요소가 활용된다. 또한, 컨텍스트 요소를 반영하여 시간(주중/주말, 시간대), 활용하는 동작 종류(운영 체제 상호 작용 동작, 웹 브라우징 동작, 이메일 확인, 워드 프로세싱 동작, 미디어 상호 작용 동작, 사진 편집 동작, 게임에서의 플레이 전략, 목적에 따른 소프트웨어 선택 여부)가 특징적 요소로 사용될 수 있다.

앱 사용습관에서 분류기를 구축하는 방법으로는 SVM, AdaBoost, KNN, Naïve Bayes, 결정트리, ANN, HMM, RF, k-means 클러스터링이 사용되었다. 최근 연구에서는 특징 벡터를 모델링하기 위해 앱 사용습관의 피쳐에 n-gram 시퀀싱 기법을 고유하게 적용함으로써 빠르게 앱 사용습관을 기반으로 사용자를 인증할 수 있다[20].

10. 모바일 장치 사용

모바일 장치 사용 기반 인증은 사람들이 모바일 장치(스마트폰, 웨어러블)의 서비스와 상호 작용하는 방식에 따라 사람을 식별하는 인증 방식이다. 최근의 모바일 장치는 다양한 센서가 장착되어 미세한 레벨에서 사용자의 활동을 암시적이고 지속적으로 관찰할 수 있다.

모바일 장치 사용 기반 인증은 가속도계 및 자이로 스코프와 같이 내장된 다양한 센서를 활용한다. 또한, 현재 급속히 증가하고 있는 웨어러블 기기(스마트워치)의 블루투스 연결성과 다중 센서를 활용한다. 일반적으로 모바일 장치 사용 기반 인증은 스마트 폰 및 스마트 워치로부터 센서 데이터를 수신한 뒤, 미가공 데이터로부터 세분된 시간-주파수 특성을 추출하고 두 개의 특성 벡터(컨텍스트 특성 벡터, 인증 특성 벡터)를 생성하여 각각 컨텍스트 검색 구성 요소와 인증 구성 요소로 변환한다. 컨텍스트 검출 컴포넌트는 사용자가 어느 컨텍스트에 있는지를 결정하고 검출된 컨텍스트를 인증 컴포넌트로 보내어 사용자의 최종 인증 여부를 결정한다.

모바일 장치 사용 기반 인증에서 분류기를 구축하는 방법으로 k-means 클러스터링, RF, Logistic regression, 신경망, KNN, SVM, KRR, Gaussian kernel SVM이 사용되었다. 최근에는 딥러닝 AutoEncoder를 특징 추출 프로세스에 활용하여 감소된 피쳐 그룹을 사용하고, 숨겨진 계층의 수가 더 많은 자동 인코딩 아키텍처가 사용자와 공격자의 특징을 명확히 구분 지었다. 이를 통해 오랜 시간 뒤에 더 작은 데이터 세트로 모델을 재훈련하여도 더 높은 정확도 수준을 달성함을 보였다[21].

Ⅳ. 결론

세계적인 조사기관인 IDC는 전 세계 보안 시장이 2016년 737억 달러에서 2020년에는 1,016억 달러로 증가할 것으로 예측하면서, 가장 빠르게 성장하는 보안 제품 시장 중 하나로 '사용자 행위 분석 기술'(연평균성장률 12.2%)을 지목했다[22]. 또한, 인터넷진흥원은 2017년 산업체가 주목해야 할 정보보호 10대 기술 중 하나로, '행동패턴 기반 무자각·무인지 인식기술'을 제시했다[23]. 무자각 지속인증 기술은 주로 학계에서

연구되었지만, 수년 내에 급성장하여 신시장을 창출할 것으로 예상한다.

본 논문에서는 무자각 지속인증에 대한 정의와 함께, 무자각 인증기술로 활용 가능한 여러 인증기술에 대하여 정의, 주요 특징요소, 적용 가능한 알고리즘, 최신 연구 동향을 간략히 소개했다. 각 인증기술로는 얼굴, 음성, 걸음걸이, 키스트로크 다이나믹스, 마우스 다이나믹스, 터치 다이나믹스, 문제, 위치, 앱 사용습관, 모바일 장치 사용으로 상세히 구분하였다. 향후 연구로는 각 방식 간의 장단점을 비교하고, 단일 팩터의 인증 기술을 결합한 멀티모달 기법의 연구들을 조사할 예정이다. 또한, 무자각 지속인증 기술 연구에서 고려해야 할 요소들을 고찰할 것이다.

약어 정리

ANN	Artificial Neural Network
CA	Certification Authority
CTR	Cognitive Typing Rhythm
DCNN	Deep Convolutional Neural Network
DNN	Deep Neural Network
EER	Equal Error Rate
FAR	False Acceptance Ratio
FIDO	Fast IDentity Online
FRR	False Rejection Ratio
FSFD	Facial Segment-based Face Detector
GDI	Gait Dynamic Images
GMM	Gaussian Mixture Model
GRNN	General Regression Neural Network
GTGF	Graphical Touch Gesture Feature
GUI	Graphic User Interface
HMM	Hidden Markov Model
KNN	K-Nearest Neighbors
KRR	Kernel Ridge Regression
LPC	Linear Predictive Coefficient
MFCC	Mel Frequency Cepstral Coefficient
MLP	Multi-Layer Perceptron
MMC	Mobility Markov Chains
MMM	Mixed Markov Chain Model
MSMM	Marginally Smoothed HMM
O2O	Online-to-Offline
OTP	One Time Password
PATH	Person Authentication using Trace Histories
PCA	Principal Component Analysis
RA	Registration Authority
RBF	Radial Basis Function
RBFN	Radial Basis Function Network
SVM	Support Vector Machine
U2F	Universal 2nd Factor
UAF	Universal Authentication Framework
VQ	Vector Quantization

참고문헌

[1] FIDO Alliance, Accessed 2017. https://fidoalliance.org/

[2] FIDO Specifications, Accessed 2017. https://fidoalliance.org/download/

[3] W. Meng, D.S. Wong, S. Furnell, and J. Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones," *IEEE Commun. Surveys Tutorials*, vol. 17, no. 3, 2015, pp. 1268-1293.

[4] U. Mahbub, S. Sarkar, and R. Chellappa, "Partial Face Detection in the Mobile Domain," arXiv preprint arXiv: 1704.02117, 2017.

[5] S.H. Oh, G.W. Kim, and K. Lim, "Compact Deep Learned Feature-Based Face Recognition for Visual Internet of Things," *J. Supercomput.*, 2017, pp. 1-13.

[6] S. Sarkar, V.M. Patel, and R. Chellappa, "Deep Feature-Based Face Detection on Mobile Devices," in *Proc. IEEE Int. Conf. Identity Security Behavior Anal.*, Sendai, Japan, 2016, pp. 1-8.

[7] A. Krizhevsky, I. Sutskever, and G.E. Hinton, "Imagenet Classification with Deep Convolutional Neural Networks," in *Adv. Neural Inform. Process. Syst.*, Lake Tahoe, NV, USA, Dec. 2012, pp. 1097-1105.

[8] K.S. Ahmad, A.S. Thosar, J.H. Nirmal, and V.S. pande, "A Unique Approach in Text Independent Speaker Recognition Using MFCC Feature Sets and Probabilistic Neural Network," In *Int. Conf. Adv. Pattern Recogn.*, Kolkata, India, Jan. 2015, pp. 1-6.

[9] M. Muaaz and R. Mayrhofer, "Smartphone-Based Gait Recognition: From Authentication to Imitation," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, 2017, pp. 3209-

3221.

[10] CC. Lin, C.C. Chang, D. Liang, and C.H. Yang, "A New Non-intrusive Authentication Method Based on the Orientation Sensor for Smartphone Users," In *IEEE Int. Conf. Softw. Security Reliability*, Gaithersburg, MD, USA, June 2012, pp. 245-252.

[11] Y. Zhong, Y. Deng, and G. Meltzner, "Pace Independent Mobile Gait Biometrics," In *IEEE Int. Conf. Biometrics Theory, Applicat. Syst.*, Arlington, VA, USA, Sept. 2015, pp. 1-8.

[12] C. Jien, "Capturing Cognitive Processing Time for Active Authentication," Iowa State University of Science and Technology, USA, AFRL-RI-RS-TR-2014-035, Feb. 2014.

[13] A.A.E. Ahmed and I. Traore, "A New Biometric Technology Based on Mouse Dynamics," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 3, 2007, pp. 165-179.

[14] C. Shen, X. Guan, and J. Cai, "A Hypo-Optimum Feature Selection Strategy for Mouse Dynamics In Continuous Identity Authentication and Monitoring," In *IEEE Int. Conf. Inform. Theory Inform. Security*, Bejing, China, Dec. 2010, pp. 349-353.

[15] N. Zheng, A. Paloski, and H. Wang, "An Efficient User Verification System via Mouse Movements," In *ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, Oct. 2011, pp. 1-12.

[16] X. Zhao, T. Feng, and W. Shi, "Continuous Mobile Authentication Using a Novel Graphic Touch Gesture Feature," In *IEEE Int. Conf. Biometrics: Theory, Applicat. Syst.*, Arlington, VA, USA, 2013, pp. 1-6.

[17] F. Iqbal, H. Binsalleeh, B.C. Fung, and M. Debbabi, "Mining wRiteprints from Anonymous E-Mails for Forensic Investigation," *Digital Investigation*, vol. 7, no. 1-2, Oct. 2010, pp. 56-64.

[18] X. Chen, P. Hao, R. Chandramouli, and K.P. Subbalakshmi, "Authorship Similarity Detection from Email Messages," In *Int. Conf. Mach. Learning Data Mining Pattern Recogn.*, vol. 6871, 2011, pp. 375-386.

[19] U. Mahbub and R. Chellappa, "PATH: Person Authentication Using Trace Histories," In *IEEE Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf.*, New York, USA, Oct. 2016, pp. 1-8.

[20] A.A. El Masri, "Active Authentication Using Behavioral Biometrics and Machine Learning," PhD Thesis, George Mason University, 2016.

[21] M.P. Centeno, A. van Moorsel, and S. Castruccio, "Smartphone Continuous Authentication Using Deep Learning Autoencoders," In *Privacy, Security Trust*, Aug. 2017.

[22] IDC, "Worldwide Revenue for Security Technology Forecast to Surpass $100 Billion in 2020, According to the New IDC Worldwide Semiannual Security Spending Guide," 2016, Accessed 2017. https://www.idc.com/getdoc.jsp?containerId=prUS41851116

[23] 한국인터넷진흥원, "2017년, 보안이 4차 산업혁명 플랫폼으로 자리 잡을 것," 2016 Accessed 2017. https://www.kisa.or.kr/notice/press_View.jsp?mode=view&p_No=8&b_No=8&d_No=1518&ST=total&SV=