정 보 보 호 학 회 지
제28권 제1호, 2018. 2

모바일 환경의 사용자 인증 기법에 대한 Usable Security 연구 동향

김 승 연*, 권 태 경**

요 약

패스워드, PIN, 패턴 락, 지문 인증 등은 현재 가장 널리 사용되고 있는 모바일 장치의 사용자 인증 수단이다. 그러나 사용자가 기억의 편의성을 위해 쉬운 패스워드를 반복 사용한다는 것은 널리 알려진 사실이며 이를 보완하기 위해 개발된 그래픽 패스워드, 또는 지문 등 생체 인증은 사용성 개선을 이루어냈으나 여전히 사용성, 안전성에서 많은 취약점이 보고되고 있다. 본 논문에서는 모바일 장치에서의 인증 기법에 관한 연구동향을 살펴보고 분석한다.

Ⅰ. 서 론

사용자 인증 기법은 지식 기반, 소지 기반, 생체 기반으로 나눌 수 있다. 이 중 지식 기반은 PIN, 패스워드와 같이 사용자가 기억하고 있는 정보로 인증하는 것을 의미한다. 소지 기반 인증은 OTP, 스마트 카드 등 사용자의 소유물을 통해 인증을 수행하는 것을 의미한다. 그러나 모바일 장치의 경우 그 자체가 PC 등의 이중 요소(two-factor) 인증 용도로 활용 되거나 다른 IoT 장치와 연계하여 후술할 행위 기반 인증을 수행하는 경우가 많으므로 본 논문에서는 소지 기반 인증에 대해서는 특별히 분리하여 다루지 않는다. 생체 인증은 사용자의 생득적이고 일반적으로 불가변한 신체적 특징(지문, 홍채 등)을 인증 요소로 하는 생물학적 생체 인증과 키스트로크, 걸음걸이 등 사용자의 동작으로부터 특징을 추출하여 인증 요소로 하는 행위 기반 인증으로 나눌 수 있다[표 1].

태블릿, 스마트폰 등 모바일 기기의 사용이 급증함에 따라 이용 가능한 서비스도 다양해졌다. 모바일 기기는 금융 거래, 소셜 네트워크 등 많은 분야에서 사용자의 편의성을 증가시키고 있으므로 사용자의 많은 민감한 데이터가 모바일 기기에 저장된다. 모바일 기기에 저장된 사용자의 민감한 정보를 악용하는 피해를 예방하고 보호하기 위해서는 안전할 뿐 아니라 편리한 사용자 인증이 필수적이다. 이는 인증 방식의 불편함이 결과적으로 안전성을 낮출 가능성이 있기 때문이다. 예를 들어 수많은 패스워드를 모두 기억할 수 없으므로 여러 웹사이트에 동일 패스워드를 중복하여 사용하며 자주 바꾸지도 않거나[6, 14], 매우 자주 인증을 통과해야하는 스마트폰의 특성상 아예 스마트폰 잠금 기능을 사용하지 않는 경우[13] 등이 이에 해당한다.

본 논문에서는 스마트폰 인증 기법을 지식 기반, 생물학적 생체, 행위 기반 인증으로 구분하여 사용성과 안전성 문제에 대해 연구 동향을 분석한다.

본 논문의 구성은 다음과 같다. 2절에서 모바일 환경

〔표 1〕 인증 기법 분류

인증 기법	기존 방식 단점	최근 연구 동향
지식 기반	사용자의 기억 부담, 부채널 공격에 취약	부채널 공격 원천 봉쇄
		코드 외 추가 인증 요소
생물학적 생체 기반	위조 공격에 취약, 템플릿 변경 불가	위조 여부 판별력 강화
행위 기반	PC 등에서의 물리적 행위에 집중	모바일 환경의 물리적 행위
		행동 프로파일링

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00380, 차세대 인증 기술 개발)
* 연세대학교 정보대학원 정보보호연구실 (tribunus000@yonsei.ac.kr)
** 교신저자, 연세대학교 정보대학원 정보보호연구실 (taekyoung@yonsei.ac.kr)

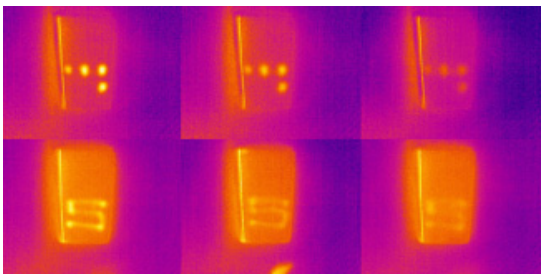
의 지식 기반 인증, 생물학적 생체 인증, 행위 기반 인증에 대해 각각이 가지고 있는 문제점과 그 문제점을 보완하기 위한 연구들의 동향을 분석한다. 3절에서 인증 솔루션을 상용화한 사례에 대해 다루며 4절에서 결론을 맺는다.

Ⅱ. 모바일 환경에서의 인증 기법

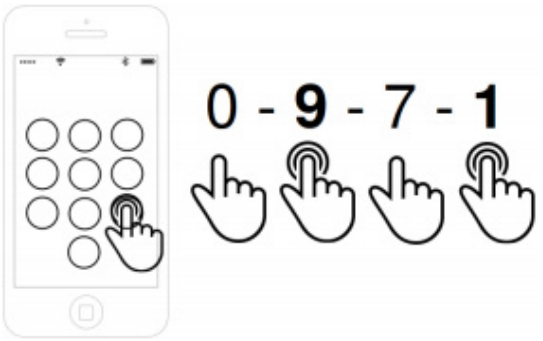
2.1. 지식 기반 인증

패턴 락(Pattern Lock)은 현재 안드로이드 모바일 장치에서 가장 널리 쓰이는 그래픽 패스워드로 PIN, 패스워드와 함께 모바일 장치에서의 대표적인 지식 기반 인증 사례이다. 텍스트를 기억하는 것보다 그림을 기억하는 것이 더 쉽다는 점에서[4] 사용자의 기억 부담을 크게 덜어주었으나 많은 취약점이 보고되고 있다. 사용자가 패스워드를 입력하는 동안 공격자가 직접, 또는 카메라 등을 활용하여 이를 훔쳐보는 숄더 서핑 공격에 취약하다는 점은 패스워드의, 특히 그래픽 패스워드의 대표적인 단점이다[10]. 또한 Aviv 등은 패턴 락 잠금 해제 후 남은 흔적(Smudge)을 바탕으로 패턴을 추측할 수 있는 스머지 공격을 제시하였으며[3], Abdelrahman 등은 [그림 1]과 같이 스마트폰 사용 후 남은 체온의 흔적을 시각화한 서멀(thermal) 이미지를 통해 패턴의 형태뿐 아니라 점을 거쳐간 순서까지 알아낼 수 있음을 보였다[1]. 이러한 취약점은 Andriotis 등이 보인 바와 같이 사용자들이 대체로 쉬운 패턴을 사용하는 것[2, 22]에 의해 더욱 큰 위험성을 가지고 있다.

이러한 기존의 패스워드 인증을 보완하는 연구는 크게 두 가지 방향으로 나눌 수 있다. 첫 번째는 단순히 패턴의 모양, 패스워드의 숫자열과 같은 코드의 일치 여부뿐만 아니라 다른 인증 요소를 추가하는 방향이다.



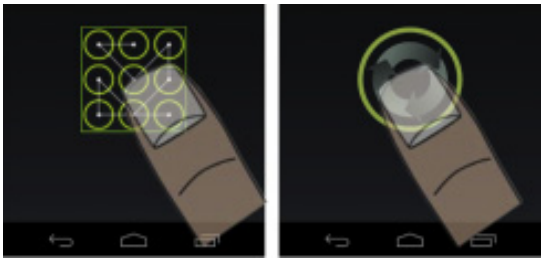
〔그림 1〕 PIN 또는 패턴 입력 후 0초, 30초, 60초 후의 열 추적 이미지〔1〕



〔그림 2〕 force-PIN의 인증 통과를 위해서는 숫자 키 값 외에 키를 누르는 압력의 순서도 일치해야 함〔17〕

De Luca 등은 패턴 락의 패턴 입력 시 손가락 압력, 넓이, X좌표 및 Y좌표를 활용하여 패턴 일치여부 외에도 등록 된 사용자가 패턴을 입력하는 방식과 유사한지를 추가로 확인하는 인증 기법을 제안했다[7]. Krombholz 등은 [그림 2]와 같이 기존 PIN 인증 방식에 키를 누르는 압력을 추가 인증 요소로 사용하는 force-PIN을 제안했다[17]. 예를 들어 사용자가 4자리 PIN 0-9-7-1을 사용한다면, 인증을 통과하기 위해 숫자열 뿐만 아니라 각 숫자키를 입력할 때 키에 가해진 압력(강, 약으로 구분)의 순서도 일치해야 한다. 50명의 사용자를 대상으로 한 실험에서 62%의 사용자들이 단순한 4자리 PIN 및 6자리 PIN보다 62%의 force-PIN이 더 안전하다고 여겼다. 또한 50개의 PIN 입력을 직접 관찰하는 숄더 서핑 공격 실험에서 단 하나의 PIN도 완벽하게 추측해 내지 못하였다. 이러한 방법들은 정당한 사용자가 올바른 코드값을 입력하였음에도 인증이 거부될 가능성(FRR)이 존재하여 사용자 불편을 초래할 가능성이 있으나 코드 입력 방식이 기존의 것과 크게 달라지지 않아 사용자 적응이 비교적 쉽다는 장점이 있다.

두 번째는 코드 입력 방식에서 기존 인증의 위협 요인을 원천 봉쇄하는 방향이다. 예를 들어 Kwon 등은 패턴 입력 시 [그림 3]과 같이 기존 패턴 락 인터페이스보다 훨씬 작은 영역에서 패턴을 그린 후 패턴을 그린 영역을 가상 휠을 따라 문질러서 패턴 입력 후 남은 스머지를 없애는 인증 방식을 제안했다[18]. 패턴을 그리는 영역이 손가락으로 가려질 만큼 작아서 숄더 서핑 공격에 저항할 수 있으며 패턴 입력 후 남는 스머지도 가상 휠을 돌리는 동작에 의해 지워진다. 그러나 입력 시간이 일반적인 패턴 입력에 비해 조금 더 길어질 수 있다. Khamis 등은 PIN 입력 시 손가락과 시선을 함께



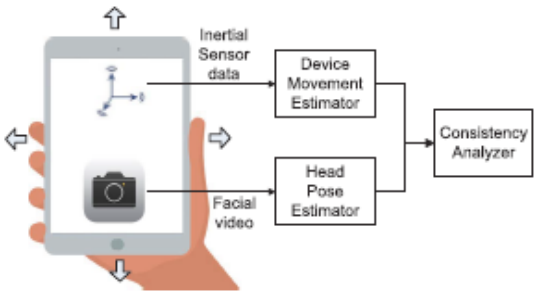
〔그림 3〕 TinyLock은 패턴 입력 후 가상 휠을 따라 스머지를 지우게 됨〔18〕

사용하여 숄더 서핑 공격에 안전한 인증 기법을 제안했다[15]. 사용자는 손가락으로 두 개의 숫자가 좌우에 배치된 총 5개의 숫자 묶음 중 필요한 숫자 묶음을 손가락으로 선택한 후 시선을 왼쪽 또는 오른쪽으로 향해서 최종적으로 숫자를 선택한다. 이 방법은 사용자의 화면 및 시선을 동시에 관찰 하는 측면 공격(Side Attack)과 사용자의 눈과 터치스크린을 각각 집중해서 관찰한 후 이를 결합하는 반복 공격(Iterative Attack) 모두에 대해 매우 뛰어난 안전성을 보였으나 사용자들은 입력이 매우 불편했다는 반응을 보였다. 이러한 인증 기법들은 코드 입력이 기존 방식보다 지연되거나 불편해지는 사용성 측면의 단점이 있을 수 있으나 안전성 면에서는 직관적이고 분명한 개선이 있으므로 특히 강력한 안전성이 요구되는 상황에서 사용하는 인증 방식으로 적합하다[15].

2.2. 생물학적 생체 인증

지식 기반 인증의 사용성을 낮추지 않으면서 안전성을 증가시키기 위한 많은 연구들이 있으나 대부분의 방법은 여전히 기존 인증 방식에 비해 입력시간 지연 등의 사용성 감소 요인을 가지고 있다. 시장조사업체 Acuity Market Intelligence가 모바일 생체 인식 시장은 2022년까지도 지속적인 성장을 이룰 것으로 전망한 것[25]과 De Luca 등이 밝힌 바와 같이 사용자들이 생체 인식을 선택하는 가장 중요한 이유 중의 하나가 안전성이 아니라 편리함[8]임을 고려한다면 점점 더 많은 사용자들이 편리한 인증을 위해 생체 인증을 사용할 것으로 예상된다.

생체 인증의 대표적인 사례로는 지문 인식, 홍채 인식, 안면 인식 등이 있다. 그러나 이러한 기존 생체 인증에는 여러 취약점 또는 불편함이 보고되고 있다. 예를



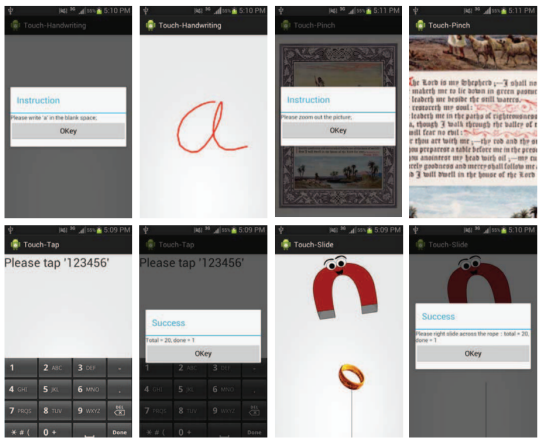
〔그림 4〕 장치의 움직임과 머리의 움직임을 각각 측정한 후 일관성 분석으로 위조 여부(liveness) 판정함〔20〕

들어 Lee 등은 스마트폰에 탑재되는 지문 인식의 경우 작은 센서로 인해 충분히 정밀한 인식이 수행되기 어려우며 스마트폰 표면에 스머지가 남는 특성을 이용하여 스머지로부터 지문 이미지 복원 후 지문 인식을 우회할 수 있음을 보였다[19]. 또한 안면 인식의 경우 최근 아이폰 X에 탑재된 Face ID에 대해 본인이 아닌 가족이 인증을 통과할 수 있음이 보고되었으며[24] 셀프 카메라(Selfie)를 찍는 인증 방식은 사회적인 불편함을 초래하여 사용자들이 안면 인식을 사용하지 않는 주된 원인인 것으로 나타났다[8].

이러한 기존 생체 인증의 취약점, 또는 불편함을 개선하기 위한 연구로는 Kim이 제안한 지문 위조 여부 판별 기술이 있다[16]. Kim은 지문의 전체적인 방향의 패턴(Local Coherence Pattern)을 특징 요소로 하여 기계학습 알고리즘 SVM (Support Vector Machine)으로 분류한 후 젤라틴, 실리콘 등으로 만든 위조 지문과 실제 지문을 구별할 수 있는 기법을 제안하였다. 비슷한 분야의 연구에서 널리 사용되는 LivDet 데이터세트들을 대상으로 성능을 평가한 결과 평균 78%의 정확도를 보였으며 모바일 장치에서도 적용 가능한 속도를 갖도록 구현되었다. 얼굴 인식에 대해서도 사진 및 비디오를 활용한 위조 공격이 가능하다는 취약점을 보완하기 위해 [그림 4]와 같이 장치 움직임 및 머리 자세 변화의 일관성에 기반 하여 위조 여부를 판단하는 기술이 연구되었다[20].

2.3. 행위 기반 인증

생물학적 생체 인증에서 지문이나 얼굴 등의 인증 수단의 위조를 방지하기 위한 연구들이 꾸준히 이루어지고 있음에도 불구하고, 한정된 계산 자원을 가진 모바일



〔그림 5〕 필기, 확대/축소, 키스트로크, 슬라이딩에서 터치 행위 수집 앱〔23〕

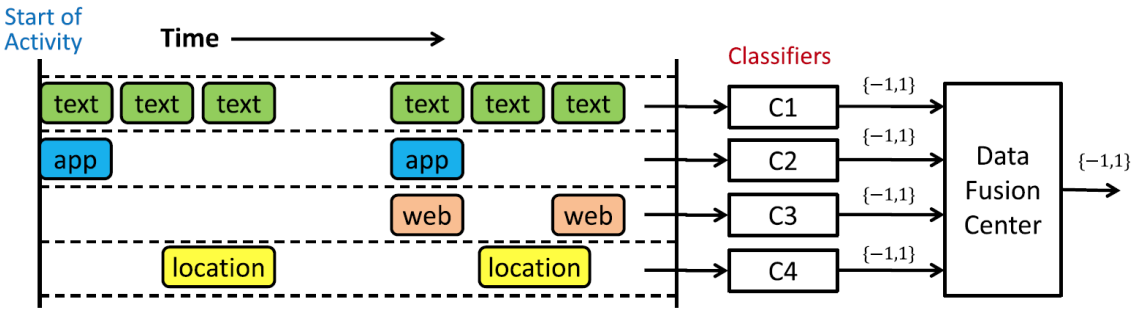
장치의 특성상 이에 전적으로 의존하기도 어렵다. 이는 인증 템플릿이 유출 되도 변경할 수 없다는 생물학적 생체 인증의 약점을 더욱 위험하게 한다. 이를 보완하기 위해 사용자의 신체적 특징이 아닌 행위적 특징을 인증 요소로 하는 행위 기반 인증에 대해 활발한 연구가 진행되고 있다.

초기 행위기반 인증은 Gaines 등이 각각 300~400개의 단어로 된 단락을 타이핑하는 방식을 분석하여 전문적인 비서 6명을 구별하려는 시도로부터 시작되었다[12]. 최근에는 스마트 기기를 중심으로 터치 행위, 시선 기반 입력, 걸음걸이 등 사용자의 물리적 행위[9]와 앱 이름, 전화 번호, GPS 위치, 브라우징 히스토리 등 행동 프로파일링을 인증요소로 활용하는 연구들이 이루어지고 있다[21].

물리적 행위에 기반 한 인증으로는 스마트 기기의 특성상 터치가 가장 활발하게 연구되고 있다. 예를 들어 Xu 등은 키스트로크, 슬라이드, 필기, 확대 및 축소 등 스마트폰 터치스크린에서 발생할 수 있는 행동을 인증 요소로 하여 인증이 가능한지 32명을 대상으로 [그림 5]에 나타난 것과 같은 실험용 앱을 구현하여 실험하였고 3명을 대상으로 21일간의 실험을 진행하였다[23]. 단일 종류의 터치만으로 완벽에 가까운 인증을 하기는 어렵고 여러 터치 동작을 복합적으로 사용해야한다는 것을 밝혔다. Crawford 등은 키스트로크를 통해 사용자를 인증하되, 자이로스코프 센서를 활용하여 사용자가 어떤 자세로 스마트폰을 사용하는지(앉아서, 서서, 걸으면서)를 먼저 식별하고 그런 후 각 상황에 맞는 분류 모델로 인증할 경우 인증 정확도가 크게 향상됨을 보였다[5].

행동 프로파일링에 기반 한 인증의 예로는 Fridman 등이 제안한 문체(Stylometry), 앱 사용 형태, 웹 브라우징, GPS Location을 인증 요소로 사용하여 사용자를 식별하는 인증 스킴이 있다[11]. 검증을 위해 200명 사용자에게 30일 동안 실제로 사용하는 스마트폰을 대상으로 데이터를 수집하였다. 매우 상이한 형태를 가진 인증 요소들(텍스트, 앱 사용, 웹 브라우징, 위치)을 통합적으로 의사 결정에 활용하기 위해 [그림 6]과 같이 개별 분류자(Classifier)의 의사 결정을 가중치를 반영하여 종합하는 방식을 채용하였다. 결과적으로 1분 정도의 훈련을 거쳐 EER 5%의 성능을 달성하였고 30분 훈련 후 EER 1%를 달성하였다.

이러한 행위 기반 인증이 가진 공통적인 특성은, 사용자의 기억 부담이 최소화되고, 위조가 어려우며, 특수한 생체 인증 요소를 활용하기 위한 고가의 장비가 필요치 않고 특히 지속적인 인증이 가능하다는 점이다. 지식 기반 인증이나 생물학적 생체 인증의 방식은 기본적



〔그림 6〕 상이한 데이터 형식을 다루는 분류자들의 의사 결정을 종합하여 최종 의사 결정을 내리는 DFC(Data Fusion Center)는 각 분류자의 의사 결정을 이전의 분류 실적에 따라 가중치 부여 후 최종 결정에 반영함〔11〕

〔표 2〕 각 인증 스킴의 사용성, 안전성 특징 요약

인증 기법	인증 스킴	사용성 특징	안전성 특징
지식 기반	Pattern Lock	텍스트 패스워드에 비해 기억하기 쉬움	숄더 서핑, 스머지, 서멀 이미지 공격 등에 취약함
	TinyLock〔18〕	기존 패턴 락에 비해 입력이 간편함, 패턴 입력이 손가락에 가려질 수 있음	숄더 서핑, 스머지, 서멀 이미지 공격 등에 안전함
	GazeTouchPIN〔15〕	손가락과 시선을 동시에 사용하여 입력이 어려움	
생물학적 생체 기반	지문 인식	패스워드의 기억 부담이 없음, (얼굴인식의 경우) 사회적 불편함 있음	위조 공격에 취약함
	얼굴 인식		
행위 기반	물리적 행위 〔23〕	패스워드의 기억 부담이 없음, 정당한 사용자가 통과하지 못하는 경우가 존재할 수 있음(EER 〈 0.01)	숄더 서핑, 위조 공격에 안전함, 지속적 인증이 가능함
	행동 프로파일링〔11〕		

으로 Unlock 방식이다. 한번 인증을 통과하면 몇몇 특수한 경우가 아니라면 추가 인증을 요구하지 않는다. 그러나 행위 기반 인증은 지속적인 모니터링을 통해 사용자의 자각 없이 인증이 이루어지므로 극대화된 사용성을 통해 결과적으로 더 높은 안전성을 확보하는 인증 방식이라 할 수 있다. [표 2]에 각 인증 스킴의 사용성, 안전성 특징이 요약되어 있다.

Ⅲ. 상용화된 인증 기술

인증 솔루션 업체 BehavioSec은 키스트로크, 걸음걸이, 제스처 패턴을 통해 앱 사용 또는 온라인에서의 묵시적 인증을 제공한다[26]. 예를 들어 온라인의 경우, 사용자는 ID와 패스워드를 입력하는 과정을 10번 반복하여 훈련 데이터를 생성하고 이후 로그인 시 ID와 패스워드를 입력하면 등록 했던 사용자가 입력한 것인지도 추가로 검증한다. 2017년 RSA 컨퍼런스에서 가장 혁신적인 스타트업으로 선정된 UnifyID는 걸음걸이를 포함한 100개 이상의 속성을 조합한 인증 방식으로 99.999%이상의 TRR(True Rejection Rate)를 달성한 인증 솔루션을 상용화하였다[27].

Ⅳ. 결 론

기존 인증 방식들은 사용자의 기억에 크게 의존하여 사용성을 저해함으로써 결과적으로 안전성을 낮추거나 변경 불가하며 위조가 쉬운 생체 인증 방식에 의존하고 있었다. 본 논문에서는 기존 인증을 지식 기반, 생물학적 생체 기반, 행위 기반으로 나누어 연구 동향을 분석하였다. 지식 기반 인증은 사용성 개선을 위해 많은 노력이 이루어지고 있으나 여전히 사용성 저해 문제를 근본적으로 해결하기 어려우며 생체 인증은 높은 사용성을 지닌 반면 위조 공격에 취약한 면이 있다. 이러한 단점들을 보완한 행위 기반 인증은 차세대 인증 기술로 각광 받고 있으며 이미 여러 인증 솔루션 업체에서 상용화를 시도하고 있다.

추후 연구로는 차세대 인증 기술로 주목받고 있는 행위 기반 인증 연구를 분석하고 그 과정에서 드러난 문제점의 보완을 통해 최소 자각 인증 방법을 도출해낼 수 있을 것이다.

참 고 문 헌

[1] Y. Abdelrahman, M. Khamis, S. Schneegass and F. Alt, “Stay cool! understanding thermal attacks on mobile-based user authentication,” In Proc. of CHI 2017.

[2] P. Andriotis, T. Tryfonas, G. Oikonomou and C. Yildiz, “A pilot study on the security of pattern screen-lock methods and soft side channel attacks,” In Proc. of Wisec 2016.

[3] A.J. Aviv, K.L Gibson, E. Mossop, M. Blaze, and J.M. Smith, “Smudge Attacks on Smartphone Touch Screen,” In Proc. of WOOT 2010.

[4] R. Biddle, S. Chiasson, and P.C. Van Oorschot, “Graphical passwords: Learning from the first twelve years,” In ACM Computing Surveys,

Aug., 2012.

[5] H. Crawford and E. Ahmadzadeh, “Authentication on the Go: Assessing the Effect of Movement on Mobile Device Keystroke Dynamics,”

[6] A. Das, J. Bonneau, M. Caesar, N. Borisov and X. Wang, “The Tangled Web of Password Reuse,” In Proc. of NDSS 2014.

[7] A. De Luca, A. Hang, F. Brudy, C. Lindner and H. Hussmann, “Touch me once and I know it’s you!: implicit authentication based on touch screen patterns,” In Proc. of CHI 2012.

[8] A. De Luca, A. Hang, E. Von Zezschwitz, and H. Hussmann, “I Feel Like I’m Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones,” In Proc. of CHI 2015.

[9] S. Eberz, K.B. Rasmussen, V. Lenders and I. Martinovic, “Evaluating behavioral biometrics for continuous authentication: Challenges and metrics,” In Proc. of ASIACCS 2017.

[10] M. Eiband, M. Khamis, E. von Zezschwitz, H. Hussmann and F. Alt, “Understanding shoulder surfing in the wild: Stories from users and observers,” In Proc. of CHI 2017.

[11] L. Fridman, S. Weber, R. Greenstadt and M. Kam, “Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location,” In IEEE Systems Journal, 2017.

[12] R.S. Gaines, W. Lisowski, S.J. Press and N. Shapiro, “Authentication by keystroke timing: Some preliminary results,” Rand Report R-2526-NSF, Rand, Santa Monica, CA. 1980.

[13] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca and M. Smith, “It’s a hard lock life: A field study of smartphone (un) locking behavior and risk perception.” In Proc. of SOUPS 2014.

[14] B. Ur, F. Noma, J. Bess, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, ““I added ‘!’ at the End to Make It Secure”: Oberving Password Creation in the Lab,“ In Proc. of SOUPS 2015.

[15] M. Khamis, M. Hassib, E.V. Zezschwitz, A. Bulling and F. Alt, “GazeTouchPIN: protecting sensitive data on mobile devices using secure multimodal authentication,” In Proc. of ICMI 2017.

[16] W. Kim, “Fingerprint Liveness Detection Using Local Coherence Patterns,” In IEEE Signal Processing Letters, 2017.

[17] K. Krombholz, T. Hupperich and T. Holz, “Use the force: Evaluating force-sensitive authentication for mobile devices,” In Proc. of SOUPS 2016.

[18] T. Kwon and S. Na, “TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems,” In computers & security, May, 2014.

[19] H. Lee, S. Kim, and T. Kwon, “Here Is Your Fingerprint!: Actual Risk versus User Perception of Latent Fingerprints and Smudges Remaining on Smartphones,” In Proc. of ACSAC 2017.

[20] Y. Li, Y. Li, Q. Yan, H. Kong and R.H. Deng, “Seeing your face is not enough: An inertial sensor-based liveness detection for face authentication,” In Proc. of ACM CCS 2015.

[21] A. Mahfouz, T.M. Mahmoud and A.S. Eldin, “A survey on behavioral biometric authentication on smartphones,” In Journal of Information Security and Applications, 2017.

[22] Y. Song, G. Cho, S. Oh, H. Kim, J.H. Huh, “On the effectiveness of pattern lock strength meters: Measuring the strength of real world pattern locks. In Proc. of CHI 2015.

[23] H. Xu, Y. Zhou, M.R. Lyu, “Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones,” In Proc. of SOUPS 2014.

[24] Ten-Year-Old’s Face Unlocks Face ID on His Mom’s iPhone X : https://youtu.be/dUMH6DVYskc

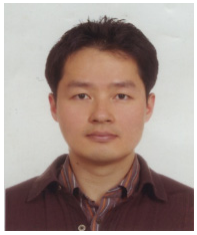
[25] The Global biometrics and Mobility Report: http://www.acuity-mi.com/GBMR_Report.php

[26] Behaviosec: https://www.behaviosec.com
[27] UnifyID: https://unify.id/

〈저 자 소 개〉

김 승 연 (Seungyeon Kim)
학생회원

2015년 2월 : 세종대학교 응용통계학 및 컴퓨터공학 학사
2015년 3월~현재 : 연세대학교 정보대학원 석사과정
관심분야 : Usable Security



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 : 세종대학교 컴퓨터공학과 교수
2007년~2008년 : Univ. Maryland at College Park 교환교수
2013년 9월~현재 : 연세대학교 정보대학원 교수
관심분야 : 암호 프로토콜, Usable Security, 사물인터넷 보안, 소프트웨어 보안 등