Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.1, Feb. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.1.127

행위 기반 인증을 위한 사용자 중심의 인증 요소 분석 연구*

이 영 주,† 구 예 은, 권 태 경‡
연세대학교 정보보호연구실

A Study of User Perception on Features Used in Behavior-Based Authentication*

Youngjoo Lee,† Yeeun Ku, Taekyoung Kwon‡
Information Security Lab, Yonsei University

요 약

패스워드, 패턴 락, 지문인식 등의 기존 스마트폰 인증 기술은 사용자의 높은 자각을 요구하며 한번 인증이 되면 재인증 절차 없이 모든 정보에 접근이 허용되는 일시적 인증이다. 이를 보완하기 위해 최근 스마트폰 사용자의 기기 사용 패턴 및 행동을 기반으로 한 행위 기반 인증이 주목받고 있다. 하지만 기존의 연구는 사용자 중심의 연구가 아닌 인증의 정확도를 높이는 연구가 중점적으로 수행되었다. 인증은 사람이 직접 사용하는 것이므로 사용자 인식의 분석이 필요하다. 본 연구는 인증을 강화하고 빈번히 발생하는 인증에 대한 사용 편의성을 향상시키기 위해 행위 기반 인증 기술에 대해 사용자 중심의 연구를 수행한다. 이를 위해 기존의 행위 기반 인증에 대한 연구를 바탕으로 인증 요소를 선별하고 이에 대한 인식 및 행위 기반 인증 기법의 수용에 대한 인식을 분석한다.

ABSTRACT

The growth in smartphone service has given rise to an increase in frequency and importance of authentication. Existing smartphone authentication mechanisms such as passwords, pattern lock and fingerprint recognition require a high level of awareness and authenticate users temporarily with a point-of-entry techniques. To overcome these disadvantages, there have been active researches in behavior-based authentication. However, previous studies focused on enhancing the accuracy of the authentication. Since authentication is directly used by people, it is necessary to reflect actual users' perception. This paper proposes user perception on behavior-based authentication with feature analysis. We conduct user survey to empirically understand user perception regarding behavioral authentication with selected authentication features. Then, we analyze acceptance of the behavioral authentication to provide continuous authentication with minimal awareness while using the device.

Keywords: Smartphone Authentication, Behavior-based Authentication, Authentication Features, User Perception

I. 서 론

기존의 스마트폰 인증 방법은 사용자의 높은 자각을 요구하며, 주로 패스워드, 지문 등 정적인 요소를 활용하는 일회성 인증에 불과해 지속적인 인증이 어렵다는 불편함이 있다. 이를 보완하기 위해 스마트

Received(11. 22. 2018), Modified(01. 16. 2019), Accepted(01. 17. 2019)
* 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원(No.2017-0-00380, 차세대 인증 기술 개발)과 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 지원을 받아 수행된 연구임(IITP-2018-2016-0-00304).
† 주저자, yj.lee91@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

폰 사용자의 기기 사용 패턴 및 행동 기반의 행위 기반 인증이 대두되었다. 그러나 기존의 행위 기반 인증 연구는 사용성을 고려하지 않은 채 인증의 정확도 향상을 위한 연구가 중점적으로 수행되었다는 문제점이 존재한다. 인증은 사람이 직접 사용하므로 사용자의 불편함을 감소시키고 사용 편의성을 향상시키기 위해 사용자 중심의 연구가 추가적으로 필요하다[1-2].

본 논문은 복합 행위 기반 인증 요소의 분류·분석을 바탕으로 인증요소를 선별하고 이를 활용하는 행위 기반 인증 기법에 대한 사용자 중심의 인증 수용 정도를 분석한다. 나아가, 기존 인증 방법과의 인식 비교 및 행위 기반 인증 기법에 활용되는 각각의 인증 요소에 대한 인식 분석을 바탕으로 수용 가능성을 분석하고, 수용 정도가 낮은 인증 요소에 대해 원인을 파악한다.

II. 이론적 배경

2.1 기존 스마트폰 인증 기술

초기 스마트폰에 도입된 인증 기술은 패스워드, PIN으로 사용성이 높고 메커니즘이 단순한 반면 사용자 기억에 의존해야하고 사전 공격 및 추측 공격에 취약하다[3-4]. 이후 도입된 안드로이드 패턴 락 또한 사용자 기억에 의존할 뿐만 아니라 스머지 공격(Smudge Attack)과 숄더 서핑 공격 (Shoulder Surfing Attack)에 취약하다는 단점이 있다[5-7].

이들의 한계점을 극복하기 위해 최근 사용자의 생체정보를 인증에 활용하는 지문 인식 기술, 얼굴 인식 기술, 홍채 인식 기술 등의 생체 인증 기술이 대두되었다[8-9]. 생체 인증 기술은 인증 시간이 짧아 편의성이 높고 사용자 고유의 정보를 활용하기 때문에 위조가 어려워 보안성이 높다는 장점을 가진다. 하지만, 생체 인증 기술은 개인정보 침해로 인한 사용자 거부감이 가장 큰 문제이며, 사용자가 인증을 위해 하던 일을 멈추고 인증을 수행해야하는 번거로움이 있다[10-11]. 이러한 기존 인증 기술의 근본적인 한계점은 한번 인증이 되면 이후 인증을 수행하지 않는 포인트-오브-엔트리 (point-of-entry) 방식의 일시적 인증에 불과하다는 것이다[12-13].

Table 1. Authentication Modalities for our study

Modality	Feature Examples	Performance	Risk Level
Touch	Type, Position, Direction, Pressure	EER 0.5%	1
App Usage	App name, Usage time, Location	EER 1%	2
Web Usage	IP address, URL, Time, Location	EER 1%	2
Location	Location, Moving pattern	FAR<0.1, FRR<0.05	3
Call	Phone number, Call time, Location	EER 2.2%	3
SMS	Phone number, Time, Location	EER 5.4%	3

2.2 행위 기반 인증 기술

행위 기반 인증 기술은 신체적 정보를 활용하는 기존의 생체 인증 기술과 다르게 사용자의 다양한 행동 정보를 기반으로 사용자를 인증한다. 행위 기반 인증은 일시적 인증 이후에도 사용자의 행위를 지속적으로 추적하여 인증을 수행하는 지속 인증이 가능하다는 장점을 가지고 있다. 이로 인해, 행위 기반 인증 기술의 필요성이 대두되었고 이를 위한 연구가 활발히 진행되고 있다[14].

본 연구에서는 행위 기반 인증 과정에서 사용자를 구별하는데 사용되는 행위 요소를 물리적 요소와 논리적 요소로 구분한다. 물리적 요소는 터치스크린 센서, 가속도계, 자이로스코프, 압력센서 등의 스마트폰에 내장된 센서로부터 수집되는 좌표, 압력, 면적 등의 데이터에서 추출 가능한 정보를 의미한다[15-23]. 논리적 요소는 앱 사용 방식, 웹 사용 방식, 통화 및 문자 송·수신 이력, 위치 이동 정보 등 사용자의 기기 사용에 대한 행동으로 사용된 앱 이름, 시작 시간, URL, 문자 입력 패턴 등을 추출해 낼 수 있다[4-5][22-26]. Table 1은 선별한 인증 요소의 특징 예시와 각각의 성능 및 위험도를 요약한다. 물리적 인증 요소의 경우, 터치 정보를 이용한 행위 기반 인증 기술이 주된 연구로 최대 0.5%의 정확도를 보이며 단독 인증 요소로 활용되기도 하였다. 논리적 요소의 경우, 다양한 요소들이 복합적으로 활용되는 경향을 보였으며 그 중 앱과 웹 사용 정보에 대한 연구가 활발하였다. 뿐만 아니라 전화 및 문자기록은 각각 최대 EER 2.2%, 5.4%의 높은 정확도를 보였다. 위치 정보는 대부분의 요소와 결합되어 세부 인증 요소로 활용 되거나 독립적으로는 위

치 이동 패턴으로 인증 시 활용되었다.

선행 연구의 보편성과 인증 정확도를 기준으로 6개 인증 요소를 선별하였으며 해당 인증 요소에 대한 기술적 보안 측면 및 프라이버시 측면에서의 위험도 분석을 위해 ISO/IEC 27005를 바탕으로 보안 및 개인정보보호 측면에서의 위협수준에 대해 위험도(Risk Level)를 3 단계로 평가하였다[27-28]. 위치 이동 정보, 통화기록 문자기록은 사용자에 대한 정보가 직접적으로 드러날 수 있으며 누적된 데이터와 최신 정보를 바탕으로 사용자의 행동을 추적할 수 있는 가장 민감한 정보이므로 3단계로 할당한다. 앱 사용 정보와 웹 사용 정보는 사용자에 대한 직접적인 정보는 드러나지 않지만 이용 내역의 경우 사용자가 숨기고 싶거나 공유하고 싶지 않은 정보가 있을 수 있으므로 2단계로 설정한다. 터치 정보는 사용자를 나타내는 직접적인 정보가 없을 뿐만 아니라 단편적인 터치정보가 공유되더라도 개인을 특정할 수 없으므로 1단계로 분류한다.

III. 연구 설계

본 연구는 사용자의 기존 인증에 대한 경험과 행위 기반 인증에 대한 인식이 행위 기반 인증 기법 수용에 미치는 영향을 분석하고자 한다. 독립변수는 기존 인증에 대한 경험이며, 행위 기반 인증에 대한 인식을 매개변수로 설정하여 변수 간의 관계에 대한 가설을 정립하였다. 연구모형은 Fig. 1과 같다.

3.1 가설 설정

각 가설은 행위 기반 인증 수용 여부에 영향을 미치는 요인으로 기존 인증에 대한 경험(H1)과 행위 기반 인증에 대한 인식(H3)을 제시하고 기존 인증의 경험에 따른 행위 기반 인증 인식 차이(H2) 분석을 위한 상위 가설과 세부 가설로 구성되어 있다.

- **H1**: 기존 인증에 대한 경험은 행위 기반 인증 기법 수용 여부에 영향을 미친다.

행위 기반 인증은 기존의 인증 방법에 추가되거나 이를 대체할 것으로 보이며 기존 인증을 사용하는 방식과 이에 대한 인식이 영향을 미칠 것이다. 따라서 기존의 사용자의 보안 의식과 스마트폰 인증 방식에 대한 인식 및 수용 패턴을 변수로 설정하여 가설 H1에 대해 다음을 제시한다.

- H1_1: 사용자의 보안 의식은 행위 기반 인증 기법 수용 여부에 영향을 미친다.
- H1_2: 기존 인증에 대한 인식은 행위 기반 인증 기법 수용 여부에 영향을 미친다.
  - H1_2a: 기존 인증의 사용 편의성에 대한 인식은 행위 기반 인증 기법 수용 여부에 영향을 미친다.
  - H1_2b: 기존 인증의 개인정보에 대한 인식은 행위 기반 인증 기법 수용 여부에 영향을 미친다.
  - H1_2c: 기존 인증의 안전성에 대한 인식은 행위 기반 인증 기법 수용 여부에 영향을 미친다.
- H1_3: 기존 인증의 수용 방식은 행위 기반 인증 기법 수용 여부에 영향을 미친다.
  - H1_3a: 기존 인증의 사용 패턴은 행위 기반 인증 기법 수용 여부에 영향을 미친다.
  - H1_3b: 기존 인증에 대한 선호도는 행위 기반 인증 기법 수용 여부에 영향을 미친다.

- **H2**: 기존 인증의 경험에 따라 행위 기반 인증의 인식에 차이가 있다.

기존의 지문인식, 얼굴인식, 홍채인식은 생체정보 인증 방식은 생체기반 인증이며 행위 기반 인증 또한 사용자의 행동 패턴을 인증에 활용하는 생체 기반 인증의 일부이다. 생체 정보를 활용하는 유사성을 바탕으로 기존 인증에 대한 경험에 따른 행위 기반 인증의 인식이 차이가 있을 것으로 예상하여 이를 바탕으로 가설 H2를 사용자의 보안 의식, 기존 인증에 대한 인식, 기존 인증의 수용 방식에 따른 행위 기반 인증 인식의 차이로 설정한다.

- H2_1: 사용자의 보안 의식에 따라 행위 기반 인증의 인식에 차이가 있다.
  - H2_1a: 사용자의 보안 의식에 따라 행위 기반 인증의 특징에 대한 인식에 차이가 있다.
  - H2_1b: 사용자의 보안 의식에 따라 행위 기반 인증 요소에 대한 인식에 차이가 있다.
- H2_2: 기존 인증의 인식에 따라 행위 기반 인증의 인식에 차이가 있다.
  - H2_2a: 기존의 인증의 인식에 따라 행위 기반 인증의 특징에 대한 인식에 차이가 있다.

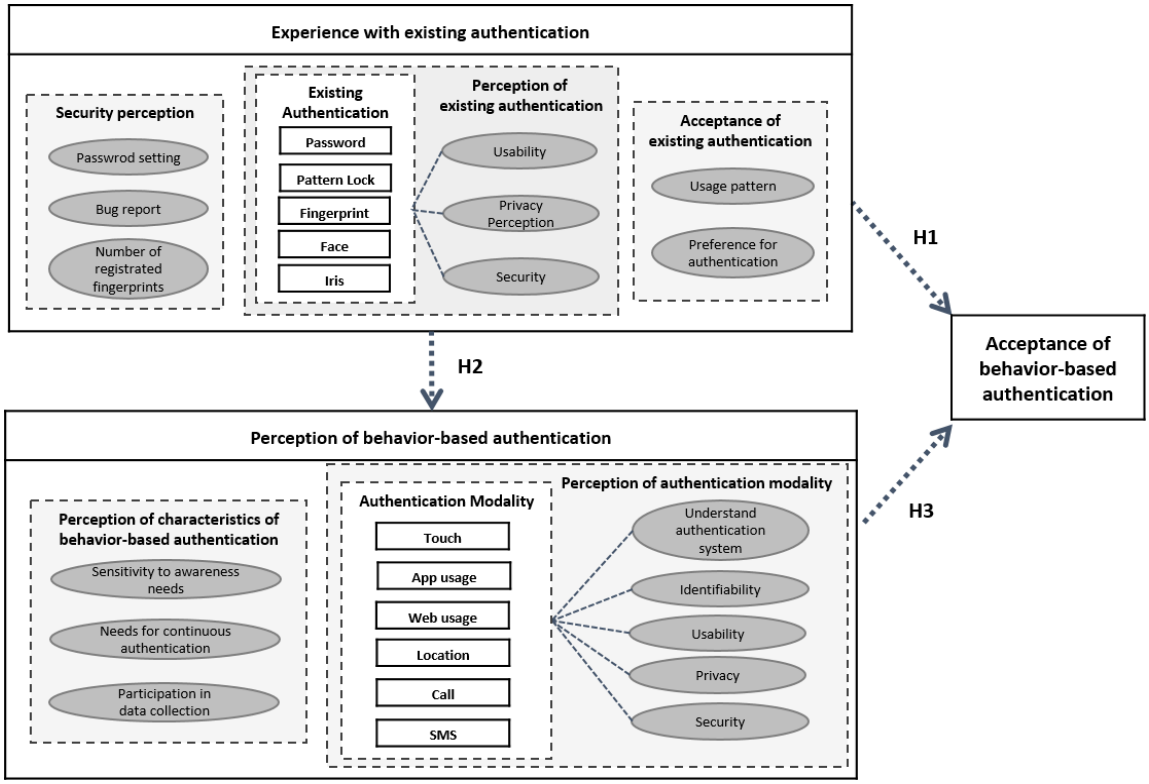

Fig. 1. Research model

- H2_2b: 기존의 인증의 인식에 따라 행위 기반 인증 요소에 대한 인식에 차이가 있다.

- H2_3: 기존 인증의 수용 방식에 따라 행위 기반 인증의 인식에 차이가 있다.
  - H2_3a: 기존의 수용 방식에 따라 행위 기반 인증의 특징에 대한 인식에 차이가 있다.
  - H2_3b: 기존의 수용 방식에 따라 행위 기반 인증 요소에 대한 인식에 차이가 있다.

- **H3**: 행위 기반 인증에 대한 인식은 행위 기반 인증 기법 수용 여부에 영향을 미친다.

행위 기반 인증 수용 여부는 이에 대한 사용자의 사전 인식이 중요한 요소라고 판단된다. 기존 인증과의 차별점인 행위 기반 인증의 특징에 대한 인식과 다양한 인증 요소를 활용하는 행위 기반 인증 기법의 인증 요소에 대한 인식이 영향을 미칠 것이다. 따라서 행위 기반 인증의 특징과 행위 기반 인증 요소에 대한 인식에 따른 행위 기반 인증 기법 수용 여부를 분석하기 위해 가설 H3을 설정한다.

- H3_1: 행위 기반 인증의 특징에 대한 인식은 행위 기반 인증 기법 수용에 영향을 미친다.
  - H3_1a: 자각 요구에 대한 민감도는 행위 기반 인증 기법 수용에 영향을 미친다.
  - H3_1b: 지속 인증의 필요성은 행위 기반 인증 기법 수용에 영향을 미친다.
  - H3_1c: 데이터 수집 참여는 행위 기반 인증 기법 수용에 영향을 미친다.
- H3_2: 행위 기반 인증 요소에 대한 인식은 행위 기반 인증 기법 수용 여부에 영향을 미친다.
  - H3_2a: 행위 기반 인증 요소의 활용에 대한 이해는 행위 기반 인증 기법 수용에 영향을 미친다.
  - H3_2b: 행위 기반 인증 요소의 식별 가능성에 대한 인식은 행위 기반 인증 기법 수용에 영향을 미친다.
  - H3_2c: 행위 기반 인증 요소의 사용 편의성에 대한 인식은 행위 기반 인증 기법 수용에 영향을 미친다.
  - H3_2d: 행위 기반 인증 요소의 개인정보 관련

인식은 행위 기반 인증 기법 수용에 영향을 미친다.

- H3_2e: 행위 기반 인증 요소의 안전성에 대한 인식은 행위 기반 인증 기법 수용에 영향을 미친다.

3.2 변수의 조작적 정의

다음은 본 연구에서 설정한 변수이다. 각 변수들의 관계는 Fig. 1에 도시되어 있다. 행위 기반 인증 수용 여부에 영향을 미치는 요인으로 기존 인증에 대한 경험과 행위 기반 인증에 대한 인식을 설정한다.

3.2.1 기존 인증에 대한 경험

사용자의 보안 의식에 관한 변수는 다음과 같이 정의한다. 보안 의식이 높은 사람은 보안이 강화된 인증 방법 또는 타인에 의해 모방이 불가능한, 위협도가 낮은 인증 방법을 사용할 것이다. 패스워드 설정 및 사용 패턴이란 사용자가 사용하는 패스워드 개수, 패스워드 길이, 패스워드 변경 주기를 말하며 패스워드가 개수가 많을수록, 길이가 길수록, 자주 변경할수록 보안 의식이 높은 사람이다[29-30]. 버그 리포트란, 스마트폰 사용 중에 발생하는 오류를 개발사에 보고하는 것으로 사용자의 기기 사용 로그 및 사용자 정보를 포함한다. 따라서 버그 리포트에 대해 동의하는 경우 자신의 사용 정보를 전송하므로 정보에 대한 보안 의식이 낮다고 판단된다. 또한 지문인식 사용을 위해 지문을 등록할 때 등록하는 지문의 개수를 1개로 설정한 경우 보안 의식이 낮다고 판단한다.

기존 인증에 대한 인식의 변수는 다음과 같이 정의 된다. 사용 편의성은 해당 인증 방식이 편리하다고 생각하는 것에 대한 인식이다. 개인정보 인식은 프라이버시 측면에서 해당 인증 방식이 민감한 사생활 정보를 포함하는 것에 대한 인식이다. 안전성은 기술적 보안 측면에서 해당 인증 방식 유출 시 타인이 이를 활용하여 인증하기 어려운 것에 대한 인식이다. 기존 인증의 수용 방식은 사용자들이 현재 실제로 사용하는 인증방식과 선호하는 인증방식으로 측정되며 지문인식, 얼굴인식, 홍채인식 등 생체인증 방식 사용 및 선호 여부로 측정된다.

3.2.2 행위 기반 인증에 대한 인식

행위 기반 인증의 특징에 대한 인식의 변수는 다음과 같이 정의된다. 자각 요구에 대한 민감도는 기존 인증의 자각 요구를 민감하게 받아들이는 정도와 행위 기반 인증 자각 최소화에 대한 인식이다. 지속 인증에 대한 필요성은 사용자들이 기존의 일시적 인증이 아닌 지속적인 인증을 필요하다고 느끼는 정도이다. 데이터 수집 참여는 데이터 수집을 위한 사용자 기기 사용 모니터링에 대한 참여 여부이다.

행위 기반 인증 요소에 대한 인식의 변수는 다음과 같이 정의된다. 인증 활용의 이해는 해당 인증 요소가 인증에 활용되는 것에 대한 이해 여부이다. 식별 가능성은 해당 인증 요소가 사용자를 식별하는 것에 대한 가능할 것으로 생각하는지 여부이다. 사용 편의성은 해당 인증 방식이 편리하다고 생각하는 것에 대한 인식이다. 개인정보 인식은 프라이버시 측면에서 해당 인증 요소가 민감한 사생활 정보를 포함하는 지에 대한 인식이다. 안전성은 기술적 보안 측면에서 해당 인증 요소 유출 시 타인이 이를 활용하여 인증하기 어려운 것에 대한 인식이다.

3.3 분석 절차 및 방법

임의추출방법을 통해 스마트폰을 사용하는 20세 이상의 사용자를 대상으로 온라인과 오프라인에서 실시하였다. 본 실험에 앞서 12명을 대상으로 예비 조사 및 인터뷰를 실시하여 문항을 보완하였고 229명을 대상으로 본 연구를 진행하였다. Table 2는 본 연구에 참여한 응답자 229명의 특성을 요약한다.

기존 인증 방식은 패스워드, 패턴락, 지문인식, 얼굴인식, 홍채인식 5개의 인증 방식을 대상으로 한다. 사용자의 보안 의식, 인증 방식에 대한 인식, 수용 방식으로 세분화하여 분석한다. 사용자의 보안 의식은 사용자의 패스워드에 대한 패스워드 사용 패턴(패스워드 개수, 길이, 변경 빈도), 버그리포트 동의 여부, 지문 사용 시 지문 등록 개수로 측정하였다. 인증의 사용 패턴 및 선호도와 사용 편의성, 개인정보 인식, 안전성의 기존 인증에 대한 인식은 5개의 기존 인증 방식에 대해 중복 선택하도록 한 후, 빈도를 측정하였다.

본 연구에서 제안하는 행위 기반 인증에 활용 가능한 행위 기반 인증 요소는 사전 연구를 통해 선별한 6가지 인증요소인 터치정보, 앱 사용 정보, 웹 사

Table 2. Characteristics of the sample

Category		Respondent
Gender	Men	127 (55.5%)
	Women	102 (44.5%)
Age	20's	37 (16.2%)
	30's	80 (34.9%)
	40's	79 (34.5%)
	50's	33 (14.4%)
Education	High school	45 (19.7%)
	Undergraduate student	25 (10.5%)
	Bachelor's degree	139 (60.7%)
	Master / doctoral degree	11 (4.8%)
	Other	10 (4.4%)
Total		229 (100%)

용 정보, 위치 정보, 통화기록, 문자기록이다. 이러한 인증 요소를 활용하는 행위 기반 인증의 특징에 대한 인식과 6가지 각각의 행위 기반 인증 요소에 대한 인식으로 나눠 평가한다.

기존 인증 경험에 따른 행위 기반 인증에 대한 인식 차이와 행위 기반 인증 기법 수용 여부를 분석하고 행위 기반 인증의 인식이 행위 기반 인증 기법 수용에 미치는 영향을 분석한다. 전자의 경우 종속변수는 행위 기반 인증에 대한 인식이며, 후자의 경우 행위 기반 인증 기법의 수용 여부이다. 독립변수는 기존 인증에 대한 경험과 관련된 변수 8개와 행위 기반 인증에 대한 인식과 관련된 변수 8개이다. 총 16개의 독립변수로 이루어진 데이터로 이에 대한 빈도 분석을 실시하고 종속변수인 행위 기반 인증에 대한 인식 또는 행위 기반 인증 기법의 수용 여부와의 관계를 통계적으로 분석한다. 독립변수들의 종속변수로의 영향 여부를 분석하기 위해 χ^2 검정을 실시하여 유의성을 검정한다. 유의한 결과를 나타내는 변수의 경우 종속 변수에 영향을 미치며 추후 행위 기반 인증 기법 개발에 고려되어야 하는 요인으로 판단한다.

IV. 결과 분석

본 장에서는 3장의 연구 방법에 따라 분석한 결과를 제시한다. 먼저 가설 검정의 결과를 기술하고 주요 연구 결과에 대해 논의한다.

4.1 가설 검정

가설 H1_1에서 보안 의식이 낮은 사용자는 행위 기반 인증 수용 의사가 더 높은 것으로 나타났다(p 〈.001). 보안 의식을 판정하기 위해, 패스워드 개수를 4개 이상, 길이는 7자리 이상, 변경 주기는 6개월 이하로 설정하는 사용자들은 보안 의식이 높다고 판단한다. 또한 버그 리포트에 동의하지 않으며 지문 등록 개수가 낮을수록 보안에 대한 의식이 높다고 판단하고 지문 등록 개수는 1로 설정하였다.

가설 H1_2에서 사용 편의성(H1_2a), 개인정보 민감도(H1_2b), 안전성(H1_2c)이 행위 기반 인증 수용 여부에 영향을 미치는지 검증한 결과 사용 편의성 면에서 유의한 결과를 보여 생체 인증을 편리하게 생각하는 사용자의 수용 의사가 더 높았다.

가설 H1_3에서 인증 사용 패턴과 인증 선호도는 행위 기반 인증 수용에 $\alpha = .05$ 수준에서 유의한 영향을 미치지 않았다.

가설 H2_1에서 보안 의식이 낮은 사용자가 자각 최소화와 지속 인증을 유의하게 더 필요로 하였고, 모니터링에 더 동의하는 것으로 나타났다(각각 p 〈.002). 즉, 사용자의 보안 의식에 따라 행위 기반 인증의 인식에 유의한 차이가 있었다(H2_1a). 또한 보안 의식이 낮은 사용자가 해당 인증 요소를 더 잘 이해하는 경향을 나타냈다(H2_1b, p〈.05). 식별 가능성 면에서는 앱 사용 정보와 웹 사용 정보만 유의한 차이가 있었다(p〈.02).

가설 H2_2에서 기존 생체 인증의 사용 편의성이 높다고 생각하는 사용자는 자각 최소화와 지속 인증을 유의하게 더 필요로 하고 모니터링에 더 동의하는 경향을 보였다(각각 p〈.05). 기존 생체 인증의 안전성을 높게 평가하는 사용자가 자각 최소화를 유의하게 더 필요로 하였다(p〈.02). 즉, 기존 인증에 대한 인식에 따라 행위 기반 인증의 특징에 대한 인식의 차이가 있었다(H2_2a). 기존 인증에 대한 인식이 행위 기반 인증 요소에 대한 인식에 영향을 주는지 분석하였으나 $\alpha = .05$ 에서 어떠한 경우에도 유의한 영향을 미치지 못하였다(H2_2b).

가설 H2_3에서 기존 인증의 수용 방식과 선호도는 어떠한 행위 기반 인증의 특징 인식에도 $\alpha = .05$ 에서 유의한 영향을 미치지 못하였다(H2_3a). 기존 인증의 수용 방식과 선호도는 행위 기반 인증 요소에 대한 인식에도 어떠한 $\alpha = .05$ 에서 유의한 영향을 미치지 못하였다(H2_3b).

가설 H3_1에서 기존 인증의 자각 요구를 불편하게 여기는 사용자와 기기 사용 중 추가 인증이 필요하다고 여기는 사용자, 그리고 모니터링에 동의하는 사용자는 각각 행위 기반 인증 수용 의사가 유의하게 더 높았다(각각 p<.03).

가설 H3_2에서 행위 기반 인증 요소에 대한 인식이 행위 기반 인증 기법 수용 여부에 영향을 미치는지 확인한 결과, 인증 요소의 활용 이해 면에서는 6가지 요소 모두에 대해 이해도가 높은 사용자가 행위 기반 인증 수용 의사가 유의하게 더 높았다(각각 p<.01). 식별 가능성 면에서는 터치 정보와 앱 사용 정보의 식별 가능성 인식이 높을수록 수용 의사가 높게 나타났다(각각 p<.05). 사용 편의성 면에서는 앱 사용 정보와 문자 기록을 편리하게 여긴 사용자가 더 유의하게 수용 의사가 높았다(p<.002). 개인정보 인식 면에서는 앱 사용 정보를 덜 민감한 사생활 정보로 여기는 사용자가 그렇지 않은 경우보다 행위 기반 인증 수용 의사가 높았다(각각 p<.03). 안전성 인식 면에서는 앱 사용 정보와 통화기록의 안전성이 높다고 여긴 경우 수용 의사가 높게 나타났다(p<.03).

Table 3. Perception and acceptance of existing authentication 1

Category		Patterns using existing biometric		
		Reject	Accept	Total
Usability	Low	86	33	119
	High	56	35	110
Total		142	87	229
χ^2-test		p<.001		
Privacy perception	Low	34	17	51
	High	108	70	178
Total		142	87	229
χ^2-test		Not significant		
Security	Low	22	19	41
	High	120	68	188
Total		142	87	229
χ^2-test		Not significant		

4.2 결과 논의

사용자의 보안의식에 따라 행위 기반 인증의 특징, 행위 기반 인증 요소에 대한 인증 활용의 이해, 행위 기반 인증 기법의 수용에 차이가 있음을 확인하였다. 보안에 의식이 낮은 사용자일수록 행위 기반 인증의 자각 최소화 필요, 지속 인증의 필요, 데이터 수집 참여에 대한 인식이 높은 경향을 보였다. 행위 기반 인증에 활용하는 행위 기반 인증요소에 대한 분석 결과, 모든 인증요소에 대해 인증 활용의 이해가 높을수록 식별 가능성에 대한 인식이 높았으며 행위 기반 인증 기법의 수용에 동의하는 경향을 보였다. 이는 보안 의식이 높은 사용자들은 기존 인증 방식 대신 쉽게 다른 인증 방식을 사용하지 않으며 보안 의식이 높은 만큼 보안에 대한 확신이 있어야 그 기술을 수용할 것이라는 결론을 도출하였다.

기존 인증의 인식에 따른 기존 인증의 수용 방식을 분석한 결과, 인증의 수용에는 사용편의성이 중요한 역할을 한다는 것을 알 수 있었다. 이와 더불어 행위 기반 인증요소에 대한 인식을 분석한 결과에서는 인증 활용의 이해와 식별가능성이 행위 기반 인증 기법 수용에 가장 중요한 영향을 있었다. 따라서 추후 사용자 중심의 행위 기반 인증을 위해서는 해당 인증요소의 활용과 식별력에 대한 이해를 바탕으로 사용편의성의 측면이 중요하게 작용할 것이다.

Table 4. Perception and acceptance of existing authentication 2

Category		Preference for existing biometric		
		Reject	Accept	Total
Usability	Low	89	30	119
	High	37	73	110
Total		126	103	229
χ^2-test		p<.001		
Privacy perception	Low	29	22	51
	High	97	81	178
Total		126	103	229
χ^2-test		Not significant		
Security	Low	21	20	41
	High	105	83	188
Total		126	103	229
χ^2-test		Not significant		

Table 6. Priority classification by perception level of behavior based authentication

Priority		Usability (+)	Understand authentication system (+)	Identifiability (-)	Privacy (-)	Security (+)
High | Low	1	Touch, Location	Touch, Location	Touch, App, Location	Touch	Touch
	2	App, Web, Call	App, Web, Call, SMS	Web, Call	App, Web	App, Web, Location, Call
	3	SMS	-	SMS	Location, Call, SMS	SMS

V. 시사점

5.1 인증 수용 동기

추후 행위 기반 인증 기법 사용에 가장 영향을 많이 미치는 인식이 무엇인지 알아보기 위해 이미 상용화된 인증의 수용 방식에서 그 경향을 분석하였다.

기존 생체 인증 방식의 인식에 따른 생체 인증 사용 패턴을 χ^2 검정으로 분석한 결과, 사용 편의성이 매우 유의한 결과를 보였으며 개인정보 인식과 안전성은 영향을 미치지 않았다(Table 3). 또한 기존의 생체 인증에 대한 인식과 이의 선호도를 χ^2 검정으로 분석결과, 사용편의성이 매우 유의한 결과를 보였으며 개인정보 인식과 안전성은 유의하지 않아 생체 인증의 사용 패턴과 같은 결과를 보였다(Table 4). 따라서 이미 상용화된 인증 방식에서의 수용 동기를 분석한 결과, 사용 편의성, 개인정보 인식, 안전성 중에서 사용 편의성만 수용 동기임을 알 수 있다.

유의한 결과를 보인 사용 편의성에 대한 이유를 분석한 결과, 짧은 인증 소요 시간이 가장 큰 이유로 인증 시간이 중요한 요인임을 알 수 있다(Table 5). 지문인식, 얼굴인식, 홍채인식과 같은 생체 인증 방법은 인증 소요 시간이 짧아 사용 시 편리하며 이러한 사용 편의성은 실제 생체 인증의 수용에 대한 동기에 영향을 미치는 것으로 보인다. 행위 기반 인증 기법의 수용 또한 기존 생체 인증의 사용 편의성과 유의한 결과를 도출하며 유사한 경향을 보였다. 생체 인증 방식의 사생활 정보 포함 유무와 안전 유무는 행위 기반 인증 기법 수용에 영향을 미치지 않았으며 이는 기존 생체 인증에 대한 개인정보 인식 및 안전성 관련 인식은 무관하다는 것을 의미한다.

Table 5. Reason for usability

Reason	Respondant
Short authentication time	130 (56.8%)
Little activity for authentication	81 (35.4%)
Familiar authentication method	59 (25.8%)
Not have to rely on memory for authentication	42 (18.3%)
Easy authentication	41 (17.9%)

5.2 행위 기반 인증 요소의 평가 및 제안

기존 인증의 수용 동기를 바탕으로 생체 정보를 이용하는 행위 기반 인증 또한 사용자의 사용 편의성에 대한 인식이 이의 수용여부에 가장 많은 영향이 미칠 것으로 예상된다. 행위 기반 인증 기법은 사용자의 기기 사용 행동 데이터를 누적하여 이를 인증에 활용하여 비사용자를 거부하고 동일한 행동 패턴을 보이는 사용자를 수용한다. 또한 기존 인증 방식과 다르게 행동 데이터로 수집 가능한 요소가 다양하여 이에 대한 이해와 사용자 식별력에 대한 인식이 추가적으로 고려되어야 한다. 특히 모든 인증 요소에 대한 인증 활용에 대한 이해는 행위 기반 인증 기법의 수용과 유의한 결과를 보였다. 또한 모든 인증 요소에 대해, 인증 활용에 대한 이해도가 높을수록 식별 가능성에 대한 인식이 높아 해당 요소가 사용자를 잘

Table 7. Unified classification result

Priority		Usability, Understand authentication system, Identifiability
High | Low	1	Touch, Location
	2	App usage, Web usage, Call
	3	SMS

Table 8. Priority of behavior-based authentication modality

Priority of modality	
High	Touch
	Location
	App usage
|	Web usage
Low	Call
	SMS

식별할 것이라고 인식하는 경향을 보이며 유의한 결과를 나타냈다. 이러한 분석을 바탕으로 행위 기반 인증 요소를 평가하고 인증 요소 적용의 우선순의를 제안한다. 본 연구에서 행위 기반 인증의 인식으로 고려한 5가지 인식인 인증 활용의 이해, 식별 가능성, 사용 편의성, 개인정보 인식, 안전성을 상대적인 수치에 따라 3단계로 분류한다. 인증 활용의 이해의 경우 모든 인증에서 인식률이 높음에 따라 2단계로 적용하여 분류한다(Table 6).

인증 수용 동기에 따른 사용 편의성과 유의미한 결과를 보인 인증 활용의 이해 및 식별 가능성을 통합하여 다음의 Table 7과 같이 3단계로 재분류한다. 또한 이 분류결과에 개인정보 인식과 안전성을 적용하여 Table 8과 같이 차세대 인증에 적용한 인증 요소에 대한 우선순위를 제안한다.

VI. 결 론

본 논문에서는 행위 기반 인증 기술에 활용되는 인증 요소에 대한 사용자 중심의 인증 수용 정도를 분석하였다. 또한, 분석 결과를 고려하여 인증 요소에 대한 우선순위를 제안하였다. 본 논문에서 제안한 인증 요소 우선순위는 행위 기반 인증 기술 개발 시 사용성 측면에서의 가이드라인으로 활용될 수 있으며, 가이드라인을 고려하지 않은 경우에 비해 행위 기반 인증 기술에 대한 사용자의 수용가능성이 높아질 것으로 예상된다.

References

[1] 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.

[2] C. Braz, and J. M. Robert, "Security and usability: the case of the user authentication methods," IHM, pp. 199-203, Apr. 2006.

[3] H. Saevanee, N. Clarke, S. Furnell, V. Biscione, "Text-based active authentication for mobile devices," IFIP, pp. 99-112, June. 2014.

[4] M. Dürmuth, D. Freeman, and B. Biggio, "Who are you? A statistical approach to measuring user authenticity," NDSS, pp. 1−15, Feb. 2016.

[5] A.H. Lashkari, S. Farmand, O.B. Zakaria, and R. Saleh "Shoulder surfing attack in graphical password authentication," IJCSIS, vol. 6, no. 2, pp. 145-154, Nov. 2009.

[6] A.J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge Attacks on Smartphone Touch Screens," WOOT, pp. 1-7, 2010.

[7] M. Shahzad, A. X. Liu, and A. Samuel, "Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it," MobiCom, pp. 39-50, Sept. 2013.

[8] A. K. Jain, K. Nandakumar, A. Ross, "50 years of biometric research: Accomplishments challenges and opportunities," Pattern Recognition Letters, vol. 79, no. 1, pp. 80-105, Aug. 2016.

[9] F. Li, N. Clarke, M. Papadaki, P. Dowland, "Active authentication for mobile devices utilising behaviour profiling," Int. J. Inf. Security, vol. 13, no. 3, pp. 229-244, Jun. 2014.

[10] A.D. Luca and J. Lindqvist, "Is Secure and Usable Smartphone Authentication Asking Too Much?," IEEE Computer, vol. 48, no. 5, pp.

64-68, May. 2015.
[11] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.
[12] N. Clarke and S. Furnell, "Authentication of users on mobile telephones - a survey of attitudes and practices," Computers & Security, vol. 24, no. 7, pp. 519 - 527, Oct. 2005.
[13] P.S. Teh, N. Zhang, A.B.J Teoh, and K. Chen, "A survey on touch dynamics authentication in mobile devices," Computers & Security, Vol. 59, pp. 210-235, June. 2016.
[14] F. Tao, L. Ziyi, C. Bogdan, B. Daining, and S. Weidong, "Continuous mobile authentication using touchscreen gestures," HST, pp. 451-456, Nov. 2012.
[15] L. Li, X. Zhao, and G. Xue, "Unobservable re-Authentication for smartphones," NDSS, Feb. 2013
[16] Xu, H., Zhou, Y., and Lyu, M, "Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones," SOUPS, pp. 187-198, July. 2014.
[17] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, K. S. Balagani, "HMOG: New behavioral biometric features for continuous authentication of smart-phone users," IEEE Trans. Inform. Forensics Security, vol. 11, no. 5, pp. 877-892, May. 2016.
[18] W.-H. Lee, X. Liu, Y. Shen, H. Jin, R. Lee, "Secure pick up: Implicit authentication when you start using the smartphone," SACMAT, pp. 67-78, June. 2017.
[19] Karapanos, N., Marforio, C., Soriente, C., & Čapkun, S. "Sound-proof: usable two-factor authentication based on ambient sound" USENIX Security, pp. 483-498, Aug. 2015.
[20] L. Zhang, S. Tan, J. Yang, Y. Chen, "VoiceLive: A Phoneme Localization based Liveness Detection for Voice Authentication on Smartphones," CCS, pp. 1080-1091, Oct. 2016.
[21] D. Liu, J. Chen, Q. Deng, A. Konate, and Z. Tian, "Secure pairing with wearable devices by using ambient sound and light," Wuhan University Journal of Natural Sciences, vol. 22, no. 4, pp. 329-336, Aug. 2017.
[22] T. Neal, D. Woodard, A. Striegel, "Mobile device application Bluetooth and Wi-Fi usage data as behavioral biometric traits," Proc. IEEE Int. Conf Biometrics Theory Applicat. and Syst., pp. 1-6, Sept. 2015.
[23] F. Li, N. Clarke, M. Papadaki, P. Dowland, "Behaviour profiling for transparent authentication for mobile devices," Proc. Euro. Conf. Inform. Warfare and Security, pp. 307-314, July. 2011.
[24] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location," IEEE Systems Journal, vol. 11, no. 2, pp. 513-521, 2017.
[25] S. Yazji, X. Chen, R. P. Dick, and P. Scheuermann. "Implicit User Re-authentication for Mobile Devices," In Ubiquitous Intelligence and Computing, Lecture Notes in Computer Science, pp. 325-339, July. 2009.
[26] Preuveneers, D., Joosen, W., " Smartauth: dynamic context fingerprinting for continuous user authentication," In Proc. of the ACM Symposium on Applied Computing, SAC, pp.

2185 - 2191, Apr. 2015
〔27〕 H. Xu, S. Gupta, M. B. Rosson, and J. M. Carroll. "Measuring mobile users' concerns for information privacy." ICIS. pp. 1-6, Dec. 2012.
〔28〕 E. Chin, A. P. Felt, V. Sekar, and D. Wagner. "Measuring user confidence in smartphone security and privacy." SOUPS, pp. 1-6, July. 2012
〔29〕 Password Selection and Use Guide, Korea Internet & Security Agency, Jan. 2010
〔30〕 A. Serwadda, V. Phoha, and Z. Wang, "Which verifiers work?: A benchmark evaluation of touch-based authentication algorithms," BTAS, pp. 1 - 8, Sept. 2013.

〈저자소개〉

이 영 주 (Youngjoo Lee) 학생회원
2016년 2월: 이화여자대학교 컴퓨터공학과 학사
2018년 2월: 연세대학교 정보대학원 석사
〈관심분야〉 Usable Security, IoT Security 등

구 예 은 (Yeeun Ku) 학생회원
2017년 2월: 세종대학교 정보보호학과 학사
2017년 9월~현재: 연세대학교 정보대학원 석사과정
〈관심분야〉 모바일-시스템 보안, 머신러닝 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〉 암호 프로토콜, 인증, Usable Security, 사물인터넷 보안, 소프트웨어 보안, 펌웨어 보안 등