Journal of The Korea Society of Computer and Information
Vol. 22 No. 9, pp. 65-71, September 2017

www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.09.065

A Secure Authentication Method for Smart Phone based on User's Behaviour and Habits

Geum-Boon Lee*

Abstract

This paper proposes a smart phone authentication method based on user's behavior and habit that is an authentication method against shoulder surfing attack and brute force attack. As smart phones evolve not only storage of personal data but also a key means of financial services, the importance of personal information security in smart phones is growing. When user authentication of smart phone, pattern authentication method is simple to use and memorize, but it is prone to leak and vulnerable to attack. Using the features of the smart phone pattern method of the user, the pressure applied when touching the touch pad with the finger, the size of the area touching the finger, and the time of completing the pattern are used as feature vectors and applied to user authentication security. First, a smart phone user models and stores three parameter values as prototypes for each section of the pattern. Then, when a new authentication request is made, the feature vector of the input pattern is obtained and compared with the stored model to decide whether to approve the access to the smart phone. The experimental results confirm that the proposed technique shows a robust authentication security using subjective data of smart phone user based on habits and behaviors.

▸Keyword: Touch pressure, Size of contact area, Pattern input time, User habits and behaviors, smart phone authentication

I. Introduction

오늘날 스마트폰은 통화 외에 지급결제, 대출, 송금, 증권, 사용자 인증 등과 같은 다양한 용도로 사용되고 있으며, 인공지능과 결합하여 초개인화, 예측 및 셀프 서비스의 핵심 기능을 장착해 가고 있다. 초고속, 초저지연, 초연결을 지향하는 5세대 이동통신(5G)과 결합하게 되는 스마트폰은 가상현실(Virtual Reality: VR)과 증강현실(Augmented Reality: AR) 나아가 혼합현실(Mixed Reality: MR) 서비스는 물론 음성비서와 결합된 무인자동차(Self-Driving Car) 제어, 실시간 동시 통역 등 다양한 목적으로 진화하고 있다. 이에 따라 개인 정보와 재산에 대한 중요한 정보를 담고 있는 스마트폰의 중요성이 더욱 커짐에 따라 스마트폰의 해킹 및 분실의 위험으로부터 이들을 보호하려는 강인한 보안 요구가 증대하고 있다.

최근 스마트폰 상의 본인 인증을 위해 지문, 음성, 홍채 등의 생체인식 방법들이 활용되고 있으나 처리 비용이 높고 인식률이 낮으며 사용자 거부감 등의 문제가 제기되어[1], 사용자의 일상적인 행위와 습관을 보안에 적용하려는 연구가 대두되고 있다. 이를 위해 기계학습 알고리즘을 적용하여 특정 로그인 시간과 위치, 키스트로크 동작과 특성 등을 파악하고 화면에서 입력 버튼을 클릭하는 위치, 입력 시 상호작용하는 방법, 응용 프로그램에서 동작하는 방식 등을 분석하여 보안 위협과 비정상적인 행위를 탐지하려는

• First Author: Geum-Boon Lee, Corresponding Author: Geum-Boon Lee
*Geum-Boon Lee (goldpalm@cst.ac.kr), Dept. of Computer Security, Chosun College of Science & Technology
• Received: 2017. 08. 16, Revised: 2017. 08. 25, Accepted: 2017. 09. 18.

노력이 있으며[2-5]. 또한 스마트 시계에 저장된 사용자의 심장 박동수, 사물인터넷 기기의 위치 정보 등을 결합하여 비밀번호를 사용하지 않고도 사용자를 인증하는 방법을 적용하여 보안을 강화하려는 연구도 지속되고 있다[6].

본 논문은 스마트 기기를 다루는 사용자의 행위와 습관에 기반한 스마트폰 인증 방법으로 스크린을 터치하는 사용자의 손가락 끝의 압력과 굵기, 키가 눌려진 상대적 위치 그리고 패턴을 입력하는 시간을 고려하여 사용자를 인증하는 방법을 제안함으로써 훔쳐보기 공격(Shoulder Surfing Attack)과 전사적 대입 공격(Brute Force Attack)에 강인하고 사용자 편의성을 확대하는 스마트폰 패턴 인증 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 최근까지 연구되었던 스마트폰 사용자 인증 방법들을 살펴보고, 3장에서는 제안하는 사용자의 행위와 습관에 기반한 스마트폰 인증 방법을 논의한다. 4장에서는 스마트폰 어플리케이션으로 개발하여 제안하는 방법에 대한 실험 결과를 보여주며, 5장에서는 결론 및 향후 연구방향을 제시한다.

II. Related Works

스마트폰 사용자 인증 방법은 생체인증, 패스워드와 SMS 인증, 그래피컬 패스워드 인증, 행동 특성에 따른 인증 등으로 나누어 볼 수 있다.

1. Biometric authentication

생체 인증은 다른 사람과 구별되는 고유한 특성을 기반으로 신원을 확인하는 것으로 얼굴 특징이나 음성, 지문, 홍채, 심전도(ECG: Electrocardiogram) 등과 같은 생체 특성이 적용된다[7-8]. 개인 고유의 특징 정보로 인증함으로써 개인식별번호(Personal Identification Number: PIN)나 토큰 또는 암호를 사용할 때 발생되는 분실이나 기억나지 않는 단점을 극복할 수 있다. 또한 스마트폰 인증 시 사용자의 선호에 맞게 설정 및 조정 가능하므로 개인화된 보안 서비스 제공이 가능하다. 그러나 생체 인증을 위해 별도의 장치를 장착해야 하며 처리 비용이 높고 낮은 인식률 등의 문제가 발생할 수 있다.

2. Password and SMS authentication

스마트폰 이용 시 회원 가입 및 지불 관련 애플리케이션에서 널리 사용되는 암호 또는 SMS 인증 코드를 이용한 인증 방법은 전통적인 방법으로 사용자의 암호가 유출되거나 악의적인 소프트웨어에 의해 SMS 인증 번호가 가로채기 공격을 당하였을 경우 개인 정보 유출과 더불어 지속적인 보안 위협이 될 수 있다. 문자 패스워드에 기반하므로 훔쳐보기, 레코딩, 사전 공격, 키 로거, 스파이웨어 등의 공격에 취약하고 이는 모바일 환경에서 텍스트 기반의 패스워드를 대체할 새로운 시스템이 요구되는 이유이다.

3. Graphical password authentication

기존 텍스트 기반 패스워드의 보안상 문제점을 개선하기 위해 제시된 인증 방법 중 하나인 그래피컬 패스워드는 숫자나 문자열을 입력하는 대신 이미지를 사용한다. 그래픽 사용자 인터페이스로 표현된 사용자 이미지를 사용하는 인증 방식으로 인증 시 사용자가 자신의 패스워드를 격자 등과 같은 일정한 공간위에 그려 저장한 후 인증 시 일치되는 지 판별하여 인증을 수행하는 방법과 여러 개의 그림을 패스워드로 등록한 후 인증 시 해당하는 그림들을 선택하거나 그림의 조합을 이용해서 인증하는 방법이 있다[9-11]. 그래피컬 패스워드는 텍스트 기반 패스워드보다 사람들이 기억하기 쉽고 안전하지만 훔쳐보기, 레코딩, 스머지(Smudge) 공격 등에 취약하다.

4. Authentication based on behavioral characteristics

사용자가 패스워드를 입력할 때의 행동 특성을 분석하여 본인 인증에 적용하는 방식이 사용자의 편리성과 안전성을 제공하는 중요한 수단이 되고 있다. 행동 특성에 따른 사용자 인증으로 키스트로크의 패턴을 분석하는 방법과 필기체 서명을 분석 방법 등이 사용된다. 키스트로크 리듬 기반 패턴인식은 사용자가 문자열을 타이핑할 때의 입력 패턴을 고려한 인식 방법으로 개인마다 키스트로크 패턴이 다르다는데 착안하여 암호의 내용뿐만 아니라 암호의 키스트로크 패턴까지 이용함으로써 패스워드 공격을 방지하고자 하는 사용자 인증 방식이다[5]. 키스트로크 인증은 공격자가 사용자의 암호를 획득하였을 경우에도 사용자의 키스트로크 지속 시간, 키누름과 키누름 사이의 지연 시간, 공분산 등을 계산하여 키스트로크의 패턴 일치 여부를 검사한다[3]. 필기체 서명은 다른 사람과 본인을 확인하기 위한 수단으로 평소에 사용하는 임의의 서명 문구를 사용하여 암호키 또는 해쉬값으로 시스템 보안에 사용하거나[12]. 스마트폰이나 태블릿의 터치 스크린에서 글쓰기 또는 서명하는 동안 사용자의 손가락 움직임의 특성으로 사용자를 인증하는 방법이 있다[13].

III. The Proposed Method on Smart Phone User Authentication

터치스크린 장치는 키를 누르거나 패턴을 만들 때 손가락 끝 압력, 손가락 끝 크기 또는 키가 눌려진 상대적 위치와 모바일 장치를 다루는 손(왼손, 오른손) 등을 특징으로 갖는다. 터치 패드에는 기기의 표면에 얼마나 많은 압력을 가했는지 정보를 얻을 수 있는 센서가 있으며, 손가락 끝 전체를 사용하여 패턴을 완성하는 경우과 손가락 끝의 일부분만으로 패턴을 만드는 경우가 있으므로 터치 면적의 크기는 중요한 특징이 될 수 있다. 또한 패턴을 입력할 때 기본 설정되는 손도 하나의 특징값으로

적용될 수 있으며, 인증 시 사용자가 스마트 폰을 잡고 있는 기울기도 인증을 위한 특징으로 계산될 수 있다.

본 논문의 사용자 패턴인증 시스템에서는 패턴 인증모델을 구축하기 위해 터치 패널에서의 사용자가 패턴을 그려서 완성하는 시간적 특성과 키 누름의 압력 그리고 패턴을 그리는 손가락이 스크린에 닿는 면적을 구간별 특징벡터로 계산하여 사용자의 행위와 습관에 기반한 스마트폰 사용자 인증방법을 제안코자 한다.

1. User Pattern Authentication System

행위와 습관에 기반한 사용자 인증은 생체 인식(Biometry)과 같이 인간의 고유한 행동 및 생리적인 특성에 대한 정보이다. 스마트폰에서 패턴 인증을 위해 사용자 등록 및 인증 두 단계로 나누어 시스템을 구성한다. 등록은 인증에 앞서 사용자의 행위의 고유 특징을 추출하여 저장하는 단계이다. 공격자가 사용자의 스마트폰 입력 행위를 엿보거나 녹화하여 패턴을 그대로 따라해도 접근이 허용되지 않는 특징을 추출하여 원시데이터로 등록한다. 인증은 등록 프로세스와 동일한 방식으로 사용자의 특징 데이터를 추출하여, 등록 시 저장된 원시 데이터(참조 패턴)와 비교한다. 데이터가 일치하지 않으면 등록되지 않은 사람이거나 공격 의도의 접근으로 보고 인증을 거부한다.

스마트폰 패턴 기반의 사용자 인증 시스템 구축을 위해 개인마다 입력하는 패턴 모양이 다르고 터치하는 방식이 다르다는 점에 착안하여 키 누름의 정도와 시간 그리고 눌린 면적을 특징으로 추출하여 참조 패턴으로 등록한다. 이러한 특징들은 훔쳐보기 공격과 전사적 공격에 의해 패턴이 유출되더라도 사용자의 행위와 습관에 기반한 특징으로 저장된 참조 패턴과 일치하지 않으므로 불법적인 접근 및 해킹을 방지하기 위한 보안 도구로 사용될 수 있다. 제안하는 스마트폰 사용자 패턴 인증 시스템은 Fig. 1과 같다.

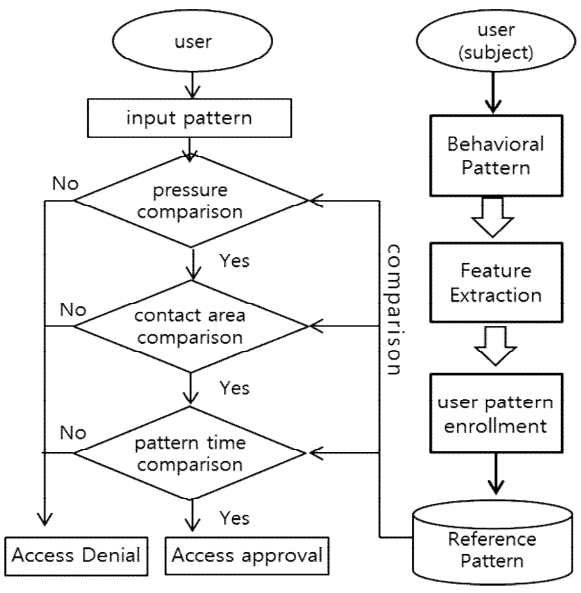


Fig. 1. Smart Phone User Authentication Modeling by Pattern

Fig. 1은 스마트폰 패턴 인증 모델링 과정으로 사용자 본인의 패턴을 등록하는 과정과 이후 사용자를 인증하는 과정으로 나뉜다. 사용자 패턴의 등록을 위하여 여러 번에 걸친 입력을 받아 특징을 추출하고 다른 사용자와 구별할 수 있는 값으로 등록하여 참조 패턴을 만든다. 이후 스마트폰 인증이 발생할 시 참조 패턴과 비교하여 터치 스크린에 눌려진 압력과 영역의 크기 그리고 시간을 참조 패턴과 순서대로 비교해 가면서 접근 승인 및 접근 거부를 결정한다.

2. Authentication Process

2.1 Feature Extraction

패턴 기반의 스마트폰 사용자 인증의 방법은 공격 의도의 접근과 정상적인 접근을 판별하기 위해 파라미터를 학습하여 결정자(discriminator)를 찾는 문제가 아닌 스마트폰 사용자 본인의 고유한 행위와 습관을 표현할 수 있는 특징벡터를 찾는 문제로 보고 이를 해결하기 위해 특징벡터로 구간별 압력과 면적 그리고 시간으로 구성한다.

등록할 사용자 본인의 패턴은 x_i, $i=1,\cdots,n$ 로 나타내며, 등록된 참조 패턴 $R=[P\ S\ T]$ 의 특징 벡터로 구성되어 있다.

$$\begin{aligned} P_1 &= \frac{1}{n}\sum_{i=1}^{n} p_1(x_i) \\ P_2 &= \frac{1}{n}\sum_{i=1}^{n} p_2(x_i) \\ &\vdots \\ P_{k-1} &= \frac{1}{n}\sum_{i=1}^{n} p_{k-1}(x_i) \end{aligned} \quad (1)$$

이다. 식 (1)에서 P_j, $j=1,\cdots,k-1$ 는 구간별 평균 압력으로 n 번의 사용자 패턴을 입력받아 k 개의 문자열을 거치면서 패턴을 완성할 시 $k-1$ 구간이 생기므로 각 구간마다 상이한 평균 압력을 계산한 것이다.

$$\begin{aligned} S_1 &= \frac{1}{n}\sum_{i=1}^{n} s_1(x_i) \\ S_2 &= \frac{1}{n}\sum_{i=1}^{n} s_2(x_i) \\ &\vdots \\ S_{k-1} &= \frac{1}{n}\sum_{i=1}^{n} s_{k-1}(x_i) \end{aligned} \quad (2)$$

식 (2)의 S_j, $j=1,\cdots,k-1$ 는 n 번의 사용자 패턴 입력에 대해 손가락으로 터치되는 면적의 구간별 평균을 나타내고, 식 (3)의 T_j, $j=1,\cdots,k-1$ 는 패턴을 입력하는데 걸린 구간별 평균

시간이다.

$$T_1 = \frac{1}{n}\sum_{i=1}^{n} t_1(x_i)$$
$$T_2 = \frac{1}{n}\sum_{i=1}^{n} t_2(x_i) \quad (3)$$
$$\vdots$$
$$T_{k-1} = \frac{1}{n}\sum_{i=1}^{n} t_{k-1}(x_i)$$

각각의 특징벡터로 참조 패턴을 완성한 후 새로운 입력 y가 입력되면 본인 인증 여부를 판별하기 위해 다음과 같이 거리를 계산한다.

$$dist(P, p_j(y)) < \theta, \quad j = 1, \cdots, k-1 \quad (4)$$

$$dist(S, s_j(y)) < \varepsilon, \quad j = 1, \cdots, k-1 \quad (5)$$

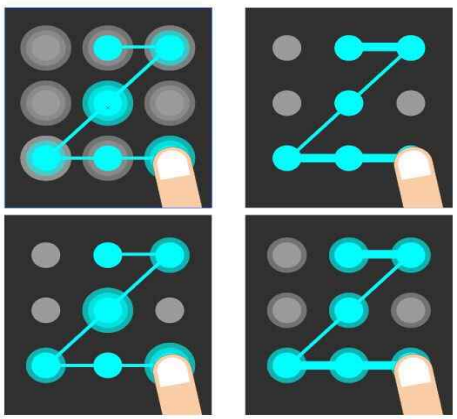
$$dist(S, t_j(y)) < \tau, \quad j = 1, \cdots, k-1 \quad (6)$$

식(4)~(6)에서 $p_j(y)$는 테스트 패턴 입력 시 구간 압력이며, $s_j(y)$는 터치 면적이고, $t_j(y)$는 패턴을 입력하는데 소요된 구간 시간으로 등록된 참조 패턴과 거리를 계산한다. 여기서 두 패턴 사이의 거리는 식 (7)과 같다

$$dist(x_i, y_j) = \sqrt{(x_i - y_j)^T (x_i - y_j)} \quad (7)$$

2.2 Pattern Authentication

스마트폰 사용자가 훔쳐보기 공격 등으로 패턴이 노출되어 공격자에 의해 침입 시도가 있을 시 인증되지 않도록 등록된 참조 패턴과 비교하여 접근 여부를 결정한다.



(a) user's pattern (b) attacker'pattern

Fig. 2. Pattern comparison between user and attacker

Fig. 2(a)는 사용자 본인 패턴으로 평소의 습관대로 패턴을 사용하여 인증하는 과정으로 Fig. 2(b)에서 공격자가 패턴을 해킹하여 동일한 패턴을 입력하더라도 스마트폰에 등록된 참조 패턴 R과 비교하여 인증 여부를 결정한다. Fig. 2는 각 구간의 압력의 세기, 손가락이 닿는 구간 영역의 크기, 그리고 구간에 도달하는 시간이 다름을 보여주고 있다.

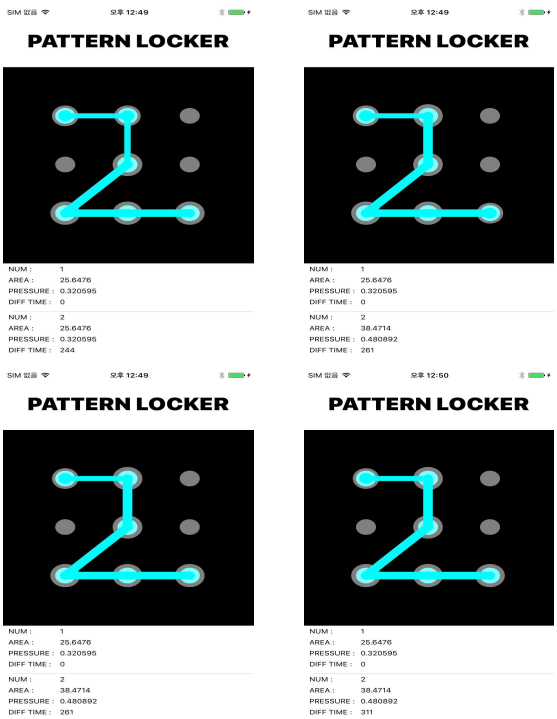
IV. Experiment Result

사용자의 행위와 습관에 기반한 스마트폰 사용자 인증을 위한 개발 환경과 테스트 환경은 Table. 1과 같다.

Table 1. Development Environment

Environment	item	Development Resource
Development	OS	maxOSX 10.12.6
	Tool	Xcode 8.3.3
	Programming	Swift 3.0
Test	Smart Phone	iPhone 7s
	OS version	10.3.3

Fig. 3은 참조 패턴을 등록하기 위해 사용자 본인으로부터 5번의 패턴 입력을 받은 데이터이다. 빠른 참조 패턴 등록을 위해 5회 입력에서 추출된 특징값으로 참조 패턴을 구성하였으나 입력 패턴의 수가 많을수록 인증의 정확도가 높아진다.



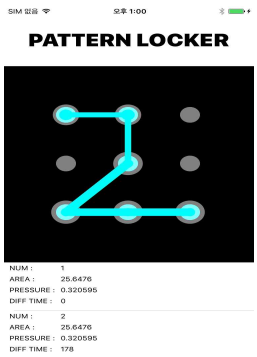


Fig. 3. User(subject) input patterns for reference model

식(1)~(3)에서와 같이 구간별(1-2-5-7-8-9) 특징 벡터를 구하기 위해 각 구간의 $[P\ S\ T]$를 구하였다.

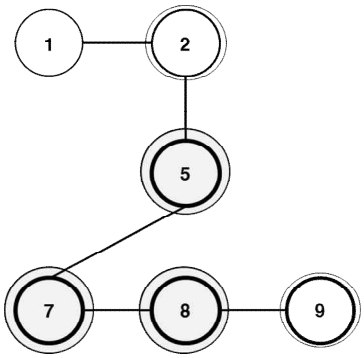


Fig. 4. Path of user pattern

Fig. 4는 사용자 패턴의 경로를 그래프로 표현한 것으로 5회의 입력을 받아 노드와 노드 사이의 압력(P), 손가락이 닿는 영역의 크기(S), 그리고 시간(T)를 Table. 2와 같이 구간별 평균값을 구하였다. 압력은 0.0~1.0 사이의 값으로 정규화 하였으며, 시간은 ms 단위로 나타내었다.

Table 2. Pressure, Area, and Diff_Time for node to node

Node	1	2	5	7	8	9
P	0.3206	0.4168	0.4809	0.4809	0.4809	0.4488
S	25.6476	33.3418	38.4714	38.2714	38.4714	38.9067
T	0	251	290	400	327	163

Table 2의 값들을 참조 패턴로 등록하고 스마트폰 사용자 인증에 사용한다. 훔쳐보기 공격에 의해 사용자 패턴이 해킹되어도 인증 시 Table 2에서 제시된 값들과 비교하여 인증 여부를 결정한다.

step 1. Refer to the enrolled pattern

$$R = [P\ S\ T]$$

step 2. Decide the authentication

$$if\ \ dist(P, p_j(y)) < \theta$$

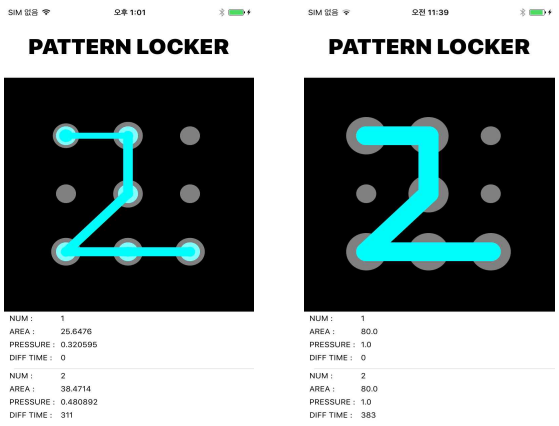
$$then\ \ if\ \ dist(S, s_j(y)) < \varepsilon$$

$$then\ \ if\ \ dist(T, t_j(y)) < \tau\ ,\ \ accept$$

$$else\ \ reject$$

Fig. 5. Authentication process

새로운 패턴 y가 입력되면 각 구간별 압력, 영역, 시간의 데이터 $p_j(y)$, $s_j(y)$, $t_j(y)$를 구하여 참조 패턴과 각 구간 거리를 계산한다. y가 인증되는 프로세스는 Fig. 5와 같다. 임계치 θ, ε, τ에 대하여 최적화(optimization)나 일반화(generalization) 문제로 해결하기 보다는 스마트폰 사용자 본인의 데이터에 기반한 개인화(personalization) 문제로 보고 작은 값으로 결정하였다. 임계 파라미터 θ는 0.2를 적용하고, ε는 5.0 이하로 사용하며 τ는 200(ms)으로 인증 여부를 실험하였다. 임계 파라미터 θ, ε, τ는 참조 패턴 등록 시 사용자 입력 패턴의 수가 많을수록 작은 값을 적용할 수 있다.



(a) user's pattern (b) attacker'pattern

Fig. 6. Pattern authentication between user and attacker

Fig. 6은 (a) 사용자 본인의 패턴과 (b) 훔쳐보기 공격으로 패턴을 획득한 공격자가 인증을 시도하고 있다.

Table 3. Pressure, Area, and Diff_Time of user

Node	1	2	5	7	8	9
P	0.3206	0.4809	0.4809	0.4809	0.4809	0.4488
S	25.6476	38.4714	38.4714	38.4714	38.4714	38.4714
T	0	311	366	434	350	217

Table 4. Pressure, Area, and Diff_Time of attacker

Node	1	2	5	7	8	9
P	1.0	1.0	1.0	1.0	1.0	1.0
S	80.0000	80.0000	80.0000	80.0000	80.0000	79.1542
T	0	383	400	499	334	683

Table 3은 사용자의 데이터이며, Table 4는 공격자의 데이터로 Table 2의 참조 패턴 데이터와 거리를 계산하여 인증 여부를 판별할 때 Fig. 6(a)는 접근이 승인되었으며 (b)는 접근이 거부되었다.

실험에서 사용된 파라미터는 사용자의 행위와 습관에 기반하여 평소 습관대로 입력하면 인증될 수 있도록 설계한 것으로 별도의 조작이나 복잡한 절차 없이 보안이 강화된 인증을 할 수 있다. 인위적인 패턴의 등록도 가능하며 특정한 구간에서 본인이 행위 했던 패턴의 절차를 기억하면 공격자를 비롯한 다른 사용자와 구별되는 강력한 보안을 할 수 있다.

V. Conclusions

스마트폰은 기본적인 통화 목적 외에 대출, 지불, 결제, 국내외 송금 등 다양한 금융활동이 가능케 되면서 사용자 인증의 중요성이 강조되고 있다. 사용자 패턴 인증의 경우 기억하기 쉽고 접근하기 쉬워 많은 사용자가 인증 수단으로 사용하는 반면 외부에 패턴 노출로 훔쳐보기 공격과 전사적 공격에 취약하였다. 본 논문에서는 사용자의 습관과 행위에 기반한 사용자 인증으로 이러한 공격에 강인한 스마트폰 보안을 논의하였다. 평소 습관대로 입력을 하는 것만으로 본인 인증이 가능하도록 하기 위해 스마트폰을 다루는 사용자의 터치 시 압력, 패턴을 그리는 손가락이 닿는 영역 그리고 패턴을 완성하는 시간을 사용하여 각 구간별 특징값으로 사용자 인증이 가능함을 보여주었다.

향후 사용자의 습관과 행위에 기반한 보안 영역은 확대될 것으로 보이며, 다른 사람과 구별하여 본인임을 인증할 수 있는 특징에 대한 연구와 지속적으로 수요가 증가되고 있는 개인화에 대한 연구가 필요하겠다.

REFERENCES

[1] N. Clarke, S. Furnell, P. Rodwell, and P. Reynolds, "Acceptance of Subscriber Authentication Methods For Mobile Telephony Device," Computer & Security, Vol. 21, No. 3, pp. 220-228, June 2002.

[2] H. Zhang, C. Yan, P. Zhao, and M. Wang, "Model construction and authentication algorithm of virtual keystroke dynamics for smart phone users," 2016 IEEE International Conference on Systems, Man, and Cybernetics, pp. 000171-000175, October 2016.

[3] M. Trojahn, and F. Ortmeier, "Toward mobile authentiction with keystroke dynamics on mobile phones and tablets," 27th International Conference on Advanced Information Networking and Applications Workshops, pp. 697-702, 2013.

[4] K. D. Rajat, M. Sudipta, and B. Puranjoy, "User Authentication Based on Keystroke Dynamics," IETE Journal of Research, Vol. 60, No. 3, pp. 229-239, July 2014.

[5] S. Hwang, S. Cho, and S. Park, “Mobile User Authentication using Keystroke Dynamics Analysis,” Conference Korea Operations Research And Management Society, pp. 652-655, Nov. 2006.

[6] T. Shari, S. Cal, and K. Larry et al., "Biometric authentication on a mobile device: a study of user effort, error and task disruption," Proceedings of the 28th Annual Computer Security Applications Conference, pp. 159-168, 2012.

[7] J. S. A-Falconi, H. A. Osman and A. E. Saddik, "ECG Authentication for Mobile Devices," IEEE Transactions on Instrumentation and Measurement, Vol. 65, Issue. 3, pp. 591-600, 2016.

[8] Y. Zheng and Z. Sihui, "A Usable Authentication System Based on Personal Voice Challenge," Proceeding of 2016 International Conference on Advanced Cloud and Big Data, pp. 194-199, Aug. 2016.

[9] T. Ko, T. Shon, and M. Hong, ”A Study on the Korean-Stroke based Graphical Password Approach,” Journal of the Korea Institute of Information Security & Cryptology, Vol. 22, No. 2, pp. 189-200, April 2012.

[10] W. Hu, X. Wu, and G. Wei, "The security analysis of graphical passwords," Proceedings of 2010 International Conference on Communications and Intelligence Information Security, pp. 200-203, Oct. 2010.

[11] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, “A new graphical password scheme resistanct to shoulder-surfing,” Proceedings of International Conference on Cyberworlds, pp. 194-199, Oct. 2010.

[12] L. Ballard, D. Lopresti, and F. Monrose, "Evaluating the Security of Handwriting Biometrics," Proceedings of 10th International Workshop on Frontiers in Handwriting Recognition, pp. 461-466, Oct. 2006.

[13] A. Buriro, B. Crispo, F. Delfrari, and K. Wrona, "Hold and Sign: A Novel Behavioral Biometrics for Smartphone User Authentication," Proceedings of 2016 IEEE Security and Privacy Workshops, pp. 276-285, May 2016.

Authors

Geum Boon Lee received the M.S. and Ph.D. degrees in Computer Engineering from Daejeon University and Chosun University, Korea, in 2002 and 2010, respectively Dr. Lee joined the faculty of the Department of Computer Security at Chosun College of Science & Technology, Gwangju, Korea, in 2013. She is currently a Professor in the Department of Computer Security, Chosun College of Science & Technology. She is interested in machine learning, computer security and embedded computing.