KIPS Tr. Comp. and Comm. Sys.
Vol.7, No.5 pp.127~136 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2018.7.5.127

A Study of User Behavior Recognition-Based PIN Entry Using Machine Learning Technique

Changhun Jung† · Zayabaatar Dagvatur†† · RhongHo Jang† · DaeHun Nyang††† · KyungHee Lee††††

ABSTRACT

In this paper, we propose a PIN entry method that combines with machine learning technique on smartphone. We use not only a PIN but also touch time intervals and locations as factors to identify whether the user is correct or not. In the user registration phase, a remote server was used to train/create a machine learning model using data that collected from end-user device (i.e. smartphone). In the user authentication phase, the pre-trained model and the saved PIN was used to decide the authentication success or failure. We examined that there is no big inconvenience to use this technique (FRR: 0%) and more secure than the previous PIN entry techniques (FAR : 0%), through usability and security experiments, as a result we could confirm that this technique can be used sufficiently. In addition, we examined that a security incident is unlikely to occur (FAR: 5%) even if the PIN is leaked through the shoulder surfing attack experiments.

Keywords : Smartphone, Authentication Protocol, User Behavior Recognition, Machine Learning, PIN

머신러닝을 이용한 사용자 행동 인식 기반의 PIN 입력 기법 연구

정 창 훈† · Zayabaatar Dagvatur†† · 장 룡 호† · 양 대 헌††† · 이 경 희††††

요 약

이 논문에서는 스마트폰에서 사용자 인증 프로토콜에 머신러닝을 사용하는 기법을 제안한다. 우리가 제안하는 기법은 사용자가 PIN을 입력할 때, PIN 뿐만 아니라 추가적으로 스크린을 터치하는 시간 간격 및 위치를 인증 정보로 수집하여 식별자로 사용하는 기법이다. 먼저 사용자 등록 단계에서 다수의 사용자 터치 시간 및 위치 데이터를 수집 한 다음, 그 데이터로 머신러닝을 이용하여 모델을 제작한다. 그리고 사용자 인증 단계에서 사용자가 입력한 PIN을 비교하고, PIN이 일치하면 사용자의 터치 시간 및 위치 데이터를 모델에 입력하여 기존에 수집한 데이터와 거리를 비교하여, 그에 따라 인증 성공 여부가 결정된다. 우리는 사용성 실험과 보안성 실험을 통하여 이 기법을 사용하는데 큰 불편이 없다는 것(FRR : 0%)과, 이전의 사용되고 있던 PIN 입력 기법보다 안전하다는 것(FAR : 0%)을 보였고, 그에 따라 충분히 사용될 수 있는 기법이라는 것을 확인하였다. 또한 숄더 서핑 공격 실험을 통하여 PIN이 유출되어도 보안 사고가 발생하기 힘들다는 것(FAR : 5%)을 확인하였다.

키워드 : 스마트폰, 인증 프로토콜, 사용자 행동 인식, 머신러닝, 핀

1. 서 론

모바일 간편 결제 서비스란 스마트폰 상에서 금전적인 거래를 간편하게 진행해주는 서비스로서, 결제 카드를 선택하고, 사용자 인증만 하면 결제가 완료되는 서비스이다. 한국소비자원 시장조사국 거래조사팀의 2016년 8월 보도자료[1]에 따르면, 국내 모바일 간편 결제 서비스는 국민앱카드, 하나앱카드, 카카오페이, 삼성페이 등이 있으며, 2014년 2분기에는 약 3조였던 시장규모가 2015년 2분기에는 5조로 증가하였다. 모바일 간편 결제 서비스에서 사용될 수 있는 인증 수단으로는 비밀번호, 지문 정보, 홍채 정보, PIN(Personal Identification Number)[2] 등이 사용될 수 있으며, 특히 숫자 4자리로 구성되어 있어서 간편한 PIN은 스마트폰의 보급률[3]과 스마트폰에서의 결제 서비스량[1]이 많아짐에 따라, 모바일 간편 결제 서비스에서 주로 사용되고 있는 인증 수단이다. 간편한 PIN은 사용성이 높지만, 보안이론에서의 사용성과 보안성은 트

※ 이 논문은 2016년도 정부(과학기술정보통신부)의 재원으로 한국연구재단-글로벌연구실사업의 지원을 받아 수행된 연구임(NRF-2016K1A1A2912757). 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.B0717-16-0114, 비대면 본인확인을 위한 바이오 공개키 기반구조 기술 개발).
† 준 회 원 : 인하대학교 컴퓨터공학과 박사과정
†† 비 회 원 : 인하대학교 정보통신공학과 석·박사통합과정
††† 정 회 원 : 인하대학교 컴퓨터공학과 교수
†††† 종신회원 : 수원대학교 전기공학과 부교수
Manuscript Received : November 20, 2017
First Revision : January 9, 2018
Accepted : February 23, 2018
* Corresponding Author : KyungHee Lee(khlee@suwon.ac.kr)

레이드 오프 관계이기 때문에, 해커들로부터 쉽게 공격당할 수도 있는 인증 수단이다[1].

사용자들이 모바일 간편 결제 시스템을 이용하려면 PIN을 입력해야 하고, 이를 위해 스마트폰 스크린의 특정 위치를 터치해야 하는데, 이러한 사용자의 행동은 스머지(Smudge) 공격[4], 키로깅(Keylogging) 공격[5], 숄더 서핑(Shoulder Surfing) 공격[6] 등으로부터 공격당해 보안 사고가 발생 할 수 있으며, 이로 인해 더 안전하게 PIN을 입력할 수 있는 방법이 필요한 상황이다.

이 논문에서는 머신러닝을 이용한 사용자 행동 인식 기반의 PIN 입력 기법을 제안한다. 이 기법은 스마트폰 금융 관련 어플리케이션에서 계좌이체 등의 서비스를 사용하기 위해 원격 인증을 할 때 PIN 뿐만 아니라, 추가적으로 스크린을 터치하는 시간 간격 및 위치를 인증 정보로 수집하여, 머신 러닝의 로지스틱 리그레션(Logistic Regression) 기술을 이용하여 사용자 식별을 수행하는 것이 특징이다. 우리는 사용성 실험을 통하여 사용자가 사전 훈련을 20번 정도만 한다면, 우리가 제안하는 기법에 익숙해져서 사용하는데 큰 불편함이 없다는 것을 알게 되었으며, 그 사용성 실험의 FRR(False Reject Rate, 오거부률)[7]은 0%였다. 그리고 사용자의 PIN이 유출되었거나, 숄더 서핑 공격을 당했을 때를 가정하여 보안성 실험을 진행하였고 각각의 FAR(False Acceptance Rate, 오인식률)[7]은 0%, 5%였으며, 이를 통해 우리가 제안하는 기법을 사용하면 보안 사고가 발생하기 힘들다는 것도 확인하였다.

이 논문의 구성은 다음과 같다. 2장에서는 이전에 사용되고 연구되었던 PIN 입력 기법과 머신러닝에 대해서 알아보고, 3장에서는 우리가 제안한 기법을 소개한다. 4장에서는 우리가 제안한 기법에 대하여 사용성 실험과 보안성 실험을 진행한 후 결과를 분석한다. 마지막 5장에서는 결론과 향후 연구에 대해 논의한다.

2. 관련 연구

2.1 랜덤 숫자 키패드를 이용하는 PIN 입력 기법

랜덤 숫자 키패드를 이용하는 PIN 입력 기법은 사용자가 인증을 위해 PIN 입력을 시도할 때마다, Fig. 1처럼 0부터 9까지인 10개의 숫자들이 키패드에 랜덤하게 배치된다. 이에 따라 사용자는 매번 PIN을 입력하려고 숫자 버튼을 터치할 때, 일반적인 숫자 키패드와 다른 위치를 터치해야 한다. 이 기법은 이러한 특징으로 인해 일반적인 숫자 키패드를 이용하여 PIN을 입력하는 기법보다 낮은 사용성을 가지고 있다. 사용자는 매번 같은 PIN을 입력하더라도 매번 다른 위치의 숫자 버튼을 터치하여 PIN을 입력해야 하기 때문이다.

그러나 이러한 특징은 한편으로 일반적인 숫자 키패드 보다 높은 보안성을 가질 수 있게 해주는 특징이기도 하다. 공격자가 스머지 공격을 이용하여 스마트폰 스크린 표면의 묻은 지문의 흔적을 통해 사용자가 터치한 위치를 알 수 있지만 랜덤 숫자 키패드이기 때문에 어떠한 번호를 터치하였는지는 정확하게 알 수 없으므로 스머지 공격에는 강한 특징을

Fig. 1. PIN Entry Using the Randomly Placed Numeric Keypad

가지고 있다. 또한 공격자가 키로깅 공격을 이용하여 사용자가 스마트폰 스크린상의 터치한 위치 데이터를 탈취한다고 하더라도, 랜덤 숫자 키패드이기 때문에 사용자가 터치한 위치에 어떤 번호가 위치해 있었는지는 정확하게 알 수 없으므로 키로깅 공격에도 강한 특징을 가지고 있다.

그러나 숄더 서핑 공격에는 여전히 약한 특징을 가지고 있는데, 사용자가 지하철, 버스, 강의실 등의 공개된 장소에서 결제를 하려고 PIN을 입력할 때, 공격자가 숄더 서핑 공격으로 사용자가 PIN을 입력하는 과정을 훔쳐본다면, 공격자는 사용자가 터치한 PIN을 탈취할 수 있기 때문에 숄더 서핑 공격에 약한 특징을 가지고 있다. 그러므로 숄더 서핑 공격에도 강한 PIN 입력 기법이 필요 되고 있는 실정이다. 이 키패드는 2017년 국내 여러 은행의 어플리케이션이나 여러 모바일 간편 결제 서비스에서 사용되고 있다.

2.2 터치 위치 기반의 PIN 입력 기법

김진복[8] 등은 사용자 인증을 위해 PIN을 입력할 때 터치 위치 데이터를 사용하여 안전성을 높인 PIN 입력 기법을 제안하였다. 터치 위치 데이터는 Fig. 2와 같이 하나의 숫자 버튼을 기준으로 좌측상단의 (0, 0)부터 우측하단의 (X_MAX, Y_MAX)로 표현된다.

이 기법은 먼저 올바른 사용자가 여러 번 PIN을 입력하여 하나의 숫자 버튼에 대하여 여러 개의 터치 위치 데이터를

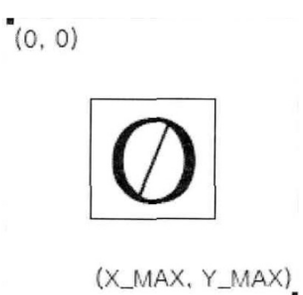


Fig. 2. Touch Location Data on a 0 Button

저장시킨 후, 그 데이터들의 평균값을 기준으로 정의한다. 그리고 사용자 인증을 위해 PIN을 입력할 때 터치 위치 데이터도 같이 입력으로 받아서, 터치 위치 데이터들이 기준이 되는 터치 위치 데이터의 평균값보다 어느 정도 떨어져 있는지 확인하여, 인증 성공 여부를 판단한다. 그러므로 공격자가 숄더 서핑 공격 등으로 사용자의 PIN을 탈취하여도, 사용자가 PIN을 입력할 때의 터치한 위치 데이터를 모르고 있으면 인증을 할 수 없게 된다.

이 기법은 PIN 외에도 터치 위치 데이터를 사용자 인증 식별자로 사용하고 있는데, 우리는 보안성을 더욱 높이기 위하여 터치 위치 데이터뿐만 아니라 터치 시간 데이터까지 식별자로 사용한다. 또한 기준이 되는 터치 위치 데이터, 터치 시간 데이터와 사용자가 PIN을 입력할 때의 입력으로 받는 터치 위치 데이터, 터치 시간 데이터를 비교할 때 머신러닝 이론 중 로지스틱 리그레션을 이용하여, 인증 성공 여부를 판단한다.

2.3 머신러닝(Machine Learning)

머신러닝이란, 인공지능의 한 분야로서 사람이 컴퓨터에 일일이 명시적인 코드로 프로그래밍을 하지 않아도, 컴퓨터가 데이터로부터 학습하여 새로운 지식을 얻어내거나 자동적으로 프로그램을 실행시키는 것을 말한다[9]. 머신러닝은 50년대 이후부터 시작되어 오래되었지만 80~90년대까지 발전 후 제자리걸음을 하다가 2000년대 들어와서 빅데이터(Big Data)와 결합되었고, 그로인해 엄청난 발전을 보였다. 머신러닝은 빅데이터로부터 학습에 필요한 많은 데이터를 얻음으로서 딥러닝(Deep Learning)으로 이어졌고, 딥러닝은 컴퓨터공학 분야 내에서 주목할 만한 분야 중 하나로 인식되고 있다.

우리는 이러한 머신러닝의 특징을 이용하여 사용자가 스마트폰에서 PIN을 입력할 때, PIN뿐만 아니라 스마트폰 스크린을 터치하는 시간 데이터와 위치 데이터를 입력으로 받아들여서, 서버가 자동적으로 올바른 사용자인지 올바르지 않은 사용자인지 판단한 후, 그 결과를 사용자에게 출력해주는 기법을 제안한다. 그리고 이를 위해 머신러닝 이론 중 다양한 방면에서 사용되고 있는 로지스틱 리그레션[10]을 사용한다. 로지스틱 리그레션이란 여러 데이터에 TRUE 또는 FALSE라고 라벨을 붙인 후 시그모이드 함수(Sigmoid Function)를 사용하여 학습을 시키고 모델을 만든 다음, 그 모델을 이용하여 새로운 입력 값이 TRUE에 근접한 것인지 FALSE에 근접한 것인지 계산하여 0과 1 사이에 있는 소수 값으로 출력을 해주는 이론이다. TRUE에 근접한 것이면 1에 가까운 소수 값이 출력된다[11, 12].

2.4 키 입력 패턴 인식(Keystroke dynamics)

키 입력 패턴 인식이란, 사용자가 데스크탑 또는 랩탑에서 키보드를 이용하여 사용자 인증을 수행할 때 키보드를 입력하는 패턴이 개인마다 다르다는데 기초한 기술이다. 예를 들어 비밀번호가 '7890'일 때, '7890'를 0.1초 간격으로 입력하는 사용자가 있을 수도 있고, 0.8초마다 입력하는 사용자가 있을 수도 있고, 또는 어떠한 리듬을 기반으로 입력하는 사용자가 있을 수도 있다. 이러한 시간 간격이나 리듬을 모르는 사용자는 인증이 되지 않으며, 이러한 특징을 이용하여 보안성을 높일 수 있다. 그리고 입력 패턴의 특징으로는 키를 입력하는 간격, 키를 누르고 있는 시간 등이 사용될 수 있다.

기존의 키 입력 패턴 인식에 대한 연구는 주로 데스크탑 또는 랩탑의 키보드를 이용한 연구가 있었으며[13-15], 입력한 패턴이 옳은지 옳지 않은지를 판단하는 시스템은 일반적으로 입력한 특징을 평균 내어 비교하는 방식이었다. 이 논문에서는 데스크탑, 랩탑의 키보드가 아닌 스마트폰 환경에 초점을 맞추고 있으며, 비교하는 방법을 일반적인 평균을 이용하는 것이 아니라 머신러닝을 이용하여 사용자가 입력한 특징이 옳은지 옳지 않은지 판단한다.

3. 머신러닝을 이용한 사용자 행동 인식 기반의 PIN 입력 기법

3.1 머신러닝을 이용한 사용자 행동 인식 기반의 PIN 입력 기법

이 논문에서는 머신러닝을 이용한 사용자 행동 인식 기반의 PIN 입력 기법을 제안한다. 이 기법은 스마트폰 상에서 사용자 인증이 진행될 때, 사용자 식별자로 PIN 뿐만 아니라 사용자가 PIN을 입력할 때의 스마트폰 스크린을 터치하는 시간 데이터와 위치 데이터도 식별자로 사용하여 올바른 사용자인지 올바르지 않은 사용자인지를 판단하는 기법이다.

여기서 시간 데이터는 PIN을 입력할 때, PIN의 첫 자리를 입력하기 위해 숫자 버튼을 터치하는 시간을 시작 기준으로 하여, PIN의 마지막 자리 숫자 버튼을 터치할 때까지, 숫자 버튼의 터치와 터치 사이의 시간을 기록한 데이터이다. 첫 번째 시간 데이터는 기준이기 때문에 항상 0.0초이다. 그리고 위치 데이터는 PIN을 입력하려면 숫자 버튼을 터치해야 하는데, 이때 각 숫자 버튼 범위 내의 사용자가 터치한 위치의 x, y 좌표를 기록한 데이터를 의미한다.

그리고 우리는 올바른 사용자인지 올바르지 않은 사용자인지를 판단(분류)하기 위해 머신러닝 이론 중 로지스틱 리그레션을 사용한다. 로지스틱 리그레션을 이용하여 올바른 사용자를 판단하려면 올바른 사용자의 행동 특징인 터치 시간 데이터와 터치 위치 데이터를 추출하여 TRUE 또는 FALSE로 라벨을 붙여서 학습 모델을 만든 후 그것을 사용해야 하는데, 학습 모델을 만들 때 사용자의 행동 특징을 조금 더 명확하게 그리고 더 많이 추출하기 위하여 일반적으로 사용하는 네 자리 또는 여섯 자리 PIN이 아닌 여덟 자리 PIN을 사용한다.

Fig. 3은 우리가 고안한 키패드이며 사용자가 PIN을 입력하기 위해 숫자 버튼을 터치하면, 자동으로 시간 데이터와 위치 데이터가 기록되는 키패드이다. 또한 스머지 공격, 키로깅 공격에 강한 특징을 갖기 위하여 일반 숫자 키패드보다 보안성이 더 높은 랜덤 숫자 키패드를 사용하며, 이 키패드의 랜덤한 숫자 배치는 사용자 의존성을 가지고 있어서 사용자 마다 숫자 키가 다르게 배치된다. Fig. 3의 파란색 숫자 및 문자들은 예를 들어 사용자가 05461467인 PIN을 입력하였을 때, 기록된 터치 시간 데이터와 터치 위치 데이터의 예시이다. 원

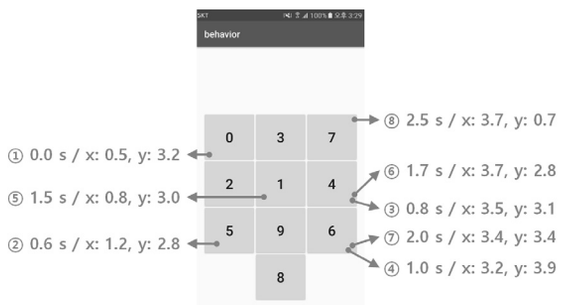


Fig. 3. Proposed Keypad with an Example of Touch Time and Location Data

문자는 터치한 순서를 의미하고, 끝에 s가 붙은 숫자는 시간 데이터, 그리고 나머지는 위치 데이터를 의미한다.

3.2 인증 프로토콜

이 기법은 사용자 등록 단계와 사용자 인증 단계로 나뉜다. 사용자 등록 단계는 인증 서버가 머신 러닝을 이용하여 인증을 시도하는 사용자가 올바른 사용자인지 올바르지 않은 사용자인지를 판단하기 위하여, 사용자가 인증 서버에 학습을 위한 데이터를 전송하고, 인증 서버는 그 데이터로 학습 한 후, 학습 모델을 추출하는 단계이다. 사용자 인증 단계는 인증 서버가 추출한 모델을 가지고 인증을 시도하는 사용자가 올바른 사용자인지 올바르지 않은 사용자인지를 판단하는 단계이다.

1) 사용자 등록 단계

먼저 사용자는 자신의 데이터를 인증 서버가 학습할 수 있도록, 회원 가입 단계에서 여러 개의 PIN, 터치 시간 데이터, 터치 위치데이터를 서버로 전송해야 한다. 이를 위해 사용자는 우리가 고안한 키패드를 이용한 사전훈련이 필요한데, 이 사전훈련은 사용자가 어느 정도 일정한 터치 시간 패턴과 터치 위치를 가지게 하기 위함이다. 일단 등록하려고 하는 PIN을 스마트폰에서 20번 정도 반복하여 입력한다. 이 때 사용자는 매번 최대한 비슷하게 터치 시간 패턴과 터치 위치를 유지하면서 PIN을 입력함으로서 이 터치 시간 패턴과 터치 위치에 익숙해지게 한다. 참고로 이 기법을 사용하기 위해서는 사용자가 PIN을 입력하기 위해 스마트폰 스크린을 터치할 때, 자신만의 터치 시간 패턴과 터치 위치 패턴을 인지하고 있어야 한다.

사용자가 어느 정도 익숙해졌다면 사전훈련과 같은 방식으로 20번의 PIN 입력을 통해 사용자로부터 만들어진 20개의 PIN, 터치 시간 데이터, 터치 위치 데이터를 인증 서버로 전송한다. 인증 서버는 전송받은 PIN을 데이터베이스에 저장하고, 터치 시간데이터와 터치 위치 데이터에 TRUE라고 라벨을 붙인다. 그리고 사용자의 데이터와 다른 80개의 랜덤한 터치 시간 데이터, 터치 위치 데이터를 생성한 후 FALSE라고 라벨을 붙인다. 그 다음 머신러닝 이론 중 시그모이드 함수를 이용하고 레이어 하나로 구성된 로지스틱 리그레션을 사용하여 학습을 시작하고, 학습이 완료되면 모델을 추출한다. 로지스틱 리그레션을 사용할 때, 우리는 오픈소스 소프트웨어인 텐서플로우(TensorFlow)[16]를 이용한다.

이를 도식화하면 Fig. 4와 같고, 의사코드 알고리즘으로 나타내면 Fig. 5와 같다. 여기서 T와 L은 각각 터치 시간 데이터와 터치 위치 데이터를 의미한다.

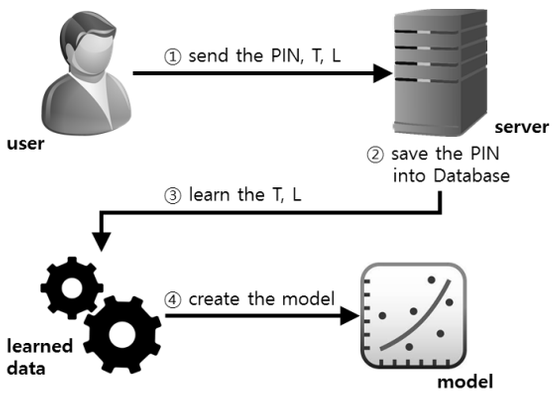


Fig. 4. User Registration Phase

Input: PIN, T, L
Output: MODEL

```
save(PIN)
var_L = Learning(sigmoid(T, L))
var_M = Modeling(var_L)
return var_M
```

Fig. 5. Pseudo Code Algorithm of User Registration Phase

2) 사용자 인증 단계

사용자 등록 단계가 완료되면, 사용자는 인증을 시도할 수 있다. 사용자는 인증을 하기 위해 스마트폰 상에서 PIN을 입력한다. 이 때 인증 설정 단계에서 PIN을 입력할 때와 비슷한 터치 시간 패턴과 터치 위치 패턴을 인지하면서 입력을 진행한다. 입력이 완료되면 사용자가 입력한 PIN과 입력할 때의 기록된 터치 시간 데이터와 터치 위치 데이터가 서버로 전송된다.

인증 서버는 사용자로부터 전송받은 데이터로부터 PIN이 인증 서버 데이터베이스에 저장되어 있는 PIN과 일치하는지 비교한다. 만약 일치한다면, 터치 시간 데이터와 터치 위치 데이터를 추출된 모델로 보내고, 모델은 사용자의 데이터가 TRUE에 근접한 것인지 FALSE에 근접한 것인지 계산한 후 모델 결과로서 0과 1 사이의 소수 값을 서버로 되돌려준다. 서버에서는 0과 1 사이에서 인증 성공과 실패를 나눌 기준인 소수 값을 정한 후, 모델 결과를 그 기준에 적용시켜서 그에 따라 결정된 인증 성공 여부를 사용자에게 알려준다. 예를 들어 서버에서 인증 성공 기준이 0.9이고, 모델 결과가 0.6이면 인증 실패이며, 모델 결과가 0.95이면 인증 성공이 될 것이다. 이 기준은 사용자에 따라서 정해질 수 있다. 예를 들어 인증 성공 기준이 0.9인 사용자가 0.98의 모델결과로 인증을 다수 성공한다면, 서버는 그에 따라 동적으로 인증 성공 기준을 0.9에서 0.97로 변경하여 보안성을 더 높일 수 있다.

이를 도식화하면 Fig. 6과 같고, 의사코드 알고리즘으로 나타내면 Fig. 7과 같다. 여기서 T와 L은 각각 터치 시간 데이터와 터치 위치 데이터를 의미한다. 그리고 Fig. 7의 'PIN′'은 데이터베이스에 저장되어 있는 사용자의 PIN을 의미하고, 'Θ'는 0과 1 사이의 소수 값으로서 서버에서 정한 인증 성공 기준을 의미한다.

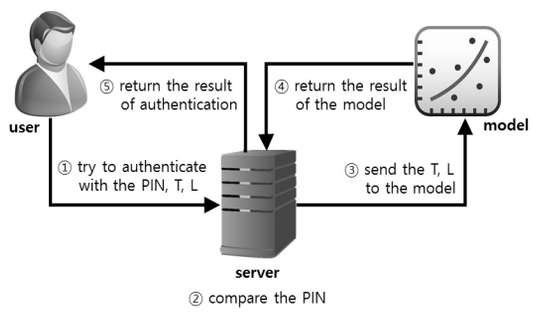


Fig. 6. User Authentication Phase

```
Input: PIN, T, L
Output: SUCCESS, FAIL

if PIN = PIN′
  var_Result = var_M(T, L)
  if var_Result ≥ Θ
    return SUCCESS
  else
    return FAIL
```

Fig. 7. Pseudo Code Algorithm of User Authentication Phase

4. 사용자 실험 및 결과

4.1 실험 환경 설정

이 논문에서는 우리가 제안한 기법의 사용성과 보안성을 알아보기 위하여 실험을 진행하였다. 이 두 가지 실험을 위해서 Fig. 8과 같이 PIN을 입력할 때 터치 시간 데이터와 터치 위치 데이터를 수집할 수 있는 어플리케이션을 고안하였다.

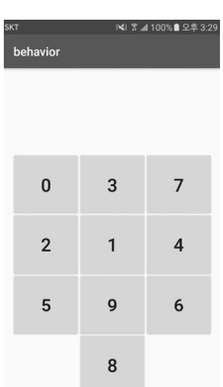


Fig. 8. Application We Made for Experiment

실험을 위해 20대 7명, 30대 7명, 총 14명의 피험자를 모집하였다. 그리고 그 중 7명은 남성, 나머지 5명은 여성이었다. 14명 중, 20대 남성 1명, 30대 남성 1명, 20대 여성 1명, 30대 여성 1명이 올바른 사용자를 담당하게 하였고, 나머지 20대 남성 5명, 30대 남성 5명을 올바르지 않은 사용자, 즉, 공격자를 담당하도록 하였다.

그리고 모델 결과가 인증 성공인지 실패인지 결정하기 위하여 서버에서 정한 인증 성공 기준은 0.9로 설정하였다. 실험에 사용된 스마트폰은 갤럭시 S7이었으며, 사용된 서버의 스펙은 Intel Xeon E5-2620, 64G Memory, 512G SSD, Ubuntu 16.04, NVIDIA TITIAN X Pascal이었고, 서버에서는 머신러닝의 로지스틱 리그레션을 사용하기 위하여 텐서플로우를 이용하였다.

다음으로는 실험에 사용할 모델을 만들기 위해서 데이터 학습에 필요한 TRUE 데이터와 FALSE 데이터를 수집하였다. 먼저 올바른 사용자들을 대상으로 TRUE 데이터를 모으기 전에 사전훈련을 시행하였다. 올바른 사용자들에게 임의의 8자리의 PIN, 임의의 터치 시간 패턴, 임의의 터치 위치 패턴을 정하라고 한 후에, 그것을 이용하여 20번 반복해서 입력하라고 하여 사용자가 임의의 PIN과 터치 시간 및 위치 패턴에 익숙해지도록 하였다.

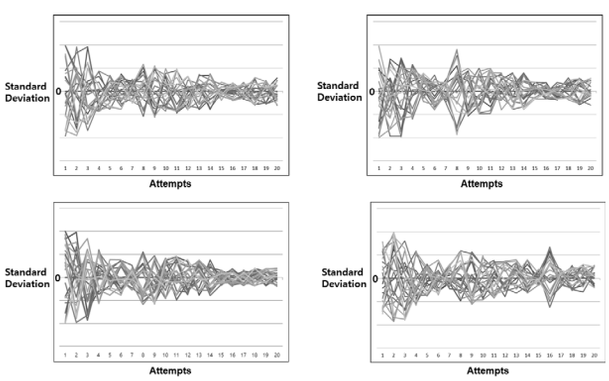


Fig. 9. Standard Deviation of Pre Training

Fig. 9는 4명의 올바른 사용자들이 사전훈련을 진행한 결과의 표준편차이다. 왼쪽 상단은 20대 남성, 오른쪽 상단은 30대 남성, 왼쪽 하단은 20대 여성, 오른쪽 하단은 30대 여성의 결과를 의미하고, 각 그래프의 y축은 표준편차, x축은 사전 훈련 횟수를 의미한다. 이를 통해 사전 훈련 횟수가 20번에 가까워질수록 표준편차가 0에 가까워진다는 것을 알았고, 20번의 사전 훈련이 충분하다는 것도 알 수 있었다. 또한 이러한 표준편차 데이터들을 기반으로 휴리스틱 방법으로 사용자를 판단하기에는 어렵기 때문에, 머신러닝이 필요하다는 것도 알 수 있었다.

그 다음으로는 사전훈련 때와 같은 방식으로 PIN을 20번 입력하게 함으로서, 올바른 사용자의 터치 시간 데이터와 터치 위치 데이터를 수집하였고, 이때 각각 49초, 56초, 42초, 54초였다. 그러므로 사용자 등록을 위해서는 약 1분 정도의 시간이 필요했다.

4명의 올바른 사용자들로부터 수집된 데이터에 TRUE라고 라벨을 붙인 다음, 공격을 담당하는 피험자 10명에게 임의의 8자리의 PIN을 8번씩 임의대로 입력하게 함으로서, 올바르지 않은 사용자의 터치 시간 데이터와 터치 위치 데이터를 수집한 뒤, 그 데이터에는 FALSE라고 라벨을 붙였다.

20대 남성 사용자(올바른 사용자)가 임의로 정한 PIN에 대하여, 수집된 TRUE 데이터와 FALSE 데이터는 Table 1과 같았고, 두 데이터 사이에 차이가 존재한다는 것을 알 수 있었다. Table 1의 첫 번째 행의 #1부터 #8은 PIN 번호의 첫 번째 숫자부터 마지막 숫자까지를 의미하고, 'T'는 TRUE 데이터를 의미하고, 'F'는 FALSE 데이터를 의미한다. 그리고 시간의 단위는 초이다.

Table 1. Average Time and Location Data We Collected for First Person(20's Man)

	Average	#1	#2	#3	#4	#5	#6	#7	#8
T	Time(s)	0.0	0.5	0.7	1.0	1.5	1.7	2.0	2.5
	Location(x)	0.7	1.0	3.3	3.1	1.0	3.3	3.4	3.4
	Location(y)	3.2	3.2	3.2	3.2	3.3	3.2	3.2	0.7
F	Time(s)	0.0	0.5	1.0	1.5	2.0	2.5	3.0	3.4
	Location(x)	2.0	2.2	2.4	2.2	2.3	2.4	2.2	2.5
	Location(y)	2.0	2.3	2.2	2.3	2.3	2.2	2.3	2.0

20대 남성뿐만 아니라, 30대 남성, 20대 여성, 30대 남성이 임의로 정한 TRUE 데이터(시간 데이터, 위치 데이터)는 FALSE 데이터와 차이를 보였다. 이 데이터로 보아 TRUE 데이터와 FALSE 데이터는 차이가 있으나, 휴리스틱으로 번류하기에는 쉽지 않다는 것을 알 수 있었다.

다음으로 우리는 로지스틱 리그레션을 이용하여 각각 올바른 사용자로부터 수집한 20개의 TRUE 데이터와 올바르지 않은 사용자로부터 수집한 80개의 FALSE 데이터를 학습시킨 후 4개의 모델을 만들었고, 실험 환경 설정을 완료하였다.

4.2 사용성 실험 방법

우리가 제안한 기법의 사용성을 알아보기 위해서는 우선 4명의 올바른 사용자들에게 인증을 시도할 때 터치 시간 데이터와 터치 위치 데이터도 인증을 위한 식별자로 사용된다는 것을 알려준 다음, 연속으로 2일 동안 하루에 10번씩 PIN을 입력하게 하고, 3일 뒤에 연속으로 3일 동안 하루에 10번씩 PIN을 입력하게 하였다. 그리고 5일 뒤에 연속으로 5일 동안 하루에 10번씩 PIN을 입력하여 하였다. 결과적으로 한명의 사용자 마다 총 100번의 PIN 입력을 하게 하였다. 우리는 올바른 사용자들이 인증을 시도하였을 때의 인증에 성공한 횟수와 인증에 걸린 시간, 모델 결과를 기록함으로서 실생활에서 충분히 사용될 수 있는 기법인지 아닌지를 확인하였다.

4.3 사용성 실험 결과

Table 2는 4명의 올바른 사용자들이 처음 2일 동안 하루에 10번씩 인증을 시도하고, 3일 뒤에 연속 3일 동안 하루에 10번씩 인증을 시도하고, 5일 뒤에 연속 5일 동안 하루에 10번씩 인증을 시도 했을 때의 모델 결과이다. 첫 번째 행의 #1은 20대 남성, #2는 30대 남성, #3은 20대 여성, #4는 30대 여성을 의미한다.

Table 2. Results of the Usability Experiment

	#1 Average of Model Result	#2 Average of Model Result	#3 Average of Model Result	#4 Average of Model Result
1st	0.979	0.992	0.969	0.968
2nd	0.991	0.972	0.987	0.972
after 3 days...				
3rd	0.984	0.994	0.957	0.975
4th	0.988	0.993	0.981	0.979
5th	0.983	0.983	0.957	0.991
after 5 days...				
6th	0.994	0.957	0.953	0.953
7th	0.990	0.993	0.958	0.990
8th	0.992	0.986	0.996	0.977
9th	0.989	0.985	0.968	0.959
10th	0.992	0.968	0.952	0.991
Aver.	0.988	0.982	0.968	0.976
Min.	0.952	0.957	0.952	0.953
Var.	0.00002	0.00014	0.00021	0.00016
StDe.	0.00451	0.01197	0.01462	0.01246

올바른 사용자들은 각각 총 100번의 시도를 하였고, 각 사용자들마다 평균 모델 결과는 0.988, 0.982, 0.968, 0.976, 분산은 0.00002, 0.00014, 0.00021, 0.00016, 표준편차는 0.00451, 0.01197, 0.01462, 0.01246, 최소 모델 결과는 0.952, 0.957, 0.952, 0.953이였으며, 서버에서 설정한 인증 성공 기준인 0.9보다 모델 결과가 낮은 경우는 한 번도 없었다. 이에 대한 그래프는 다음의 Fig. 10과 같다.

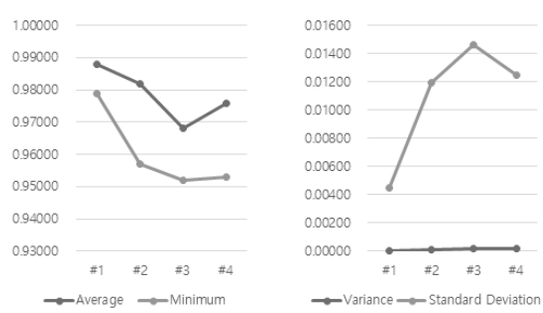


Fig. 10. Average, Minimum, Variance and Standard Deviation of Results of the Usability Experiment

위 결과로 보아 인증 성공 기준인 0.9가 적절한 기준이라고 확인되었으며, 실험 결과를 바탕으로 인증 성공 기준을 동적으로 0.95로 변경하여도 인증하는데 문제가 없다는 것을 알 수 있었다.

이에 따라 인증에 실패한 적이 없었으며, 인증하기 위하여 사용자가 여덟 자리의 숫자 버튼을 터치하는 시간은 평균 약

2.5초 정도였고, 서버에서 사용자의 데이터를 받아서 모델 결과로 인증 성공 여부를 판단하는 시간은 평균 약 0.2초였다. 그러므로 인증에 걸리는 시간은 약 2.7초정도였다. 이를 통해 우리는 올바른 사용자가 인증을 시도할 때 PIN 뿐만 아니라 터치 시간 데이터와 터치 위치 데이터도 식별자라는 것을 인지하고 있으면, 큰 불편 없이 인증에 성공할 수 있다는 것을 알았다.

그런데 한편으로는 이렇게 터치 시간과 터치 위치를 인지하는 것 자체가 사용자에게 부담이 될 수도 있다고 생각하였다. 그러나 실험 첫째 날에 무리 없이 10번 모두 인증에 성공했다는 것과, 중간에 쉬었다가 3일 뒤에 실험을 진행하였을 때에도, 그리고 5일 뒤에 실험을 진행하였을 때에도 10번 모두 인증에 성공했다는 것을 바탕으로 이 부담은 사용하는데 큰 문제가 되지 않는다는 것을 확인할 수 있었다. 또한 사전 훈련을 통해서 올바른 사용자가 일관적인 터치 시간 패턴과 터치 위치에 익숙해지도록 하게 하여 이에 대한 부담을 줄이려고 노력하였고, PIN 입력을 하면 할수록 점점 더 익숙해질 것이므로 그 부담은 점점 줄어들 것이라고 생각하며, 이를 통해 우리가 제안한 기법은 충분히 사용될 수 있다는 것을 확인하였다.

4.4 보안성 실험 방법

보안성을 알아보기 위해서는 20대 남성(올바른 사용자)의 PIN은 이미 10명의 공격자들에게 유출이 되었지만, 터치 시간 데이터와 터치 위치 데이터는 공격자가 여전히 모른다고 가정하였다. 그리고 공격자들은 올바른 사용자의 PIN만 알고 있는 상태에서 20번씩 인증을 시도하는 방법으로 보안성 실험을 진행하였다. 또한 Fig. 11처럼 우리는 숄더 서핑 공격에 대하여 보안성 실험도 진행하였는데, 이전에 실험을 진행한 공격자들에게 인증에 필요한 식별자로 터치 시간 데이터와 터치 위치 데이터도 필요하다는 사실을 알려 준 다음, 올바른 사용자가 PIN을 3번 연속으로 입력할 때, 공격자들에게 숄더 서핑 공격을 실행하게 한 후 20번씩 인증을 시도하게 하였다. 이러한 실험에서 우리는 공격자들이 인증에 성공하는지 실패하는지를 기록하고, 모델 결과를 기록하여 이 기법이 안전한지 아닌지를 확인하였다.

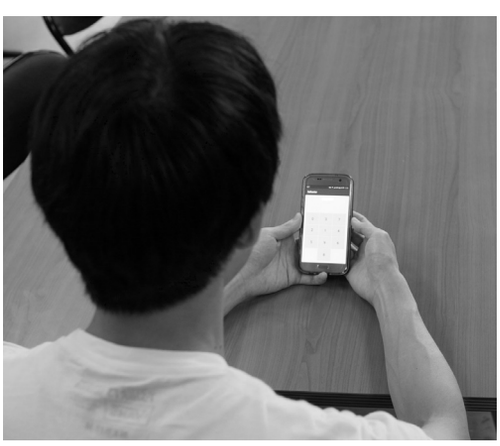


Fig. 11. The View from a Shoulder Surfing Attacker

마지막으로 우리는 공격자가 올바른 사용자의 PIN과 터치 시간만을 알고 있을 때, 또는 올바른 사용자의 PIN과 터치 위치만을 알고 있을 때, 즉, 3가지 식별자인 PIN, 터치 시간, 터치 위치 중 2가지 식별자만 알고 있었을 때를 가정하고, 그 경우의 인증이 성공하는지를 알아보기 위한 실험도 진행하였다. 이 실험은 올바른 사용자를 공격자라고 가정한 후, PIN과 올바른 터치 시간만을 고려하여 또는 PIN과 올바른 터치 위치만을 고려하여 각각 20번씩 인증을 시도함으로서 실험을 진행하였다. 우리는 여기서 인증 성공 여부와 모델 결과를 기록하여, 2가지의 식별자로만 인증이 되는지 안 되는지를 확인하였다.

4.5 보안성 실험 결과

Table 3은 10명의 공격자(Att.)들이 이미 올바른 사용자의 PIN을 알고 있다는 가정 하에 진행한 보안성 실험의 결과이다.

Table 3. Results of the Security Experiment

	Number of attempts	Average of Model Result	Number of Auth. Succ.
Att. 1	20	0.035	0 / 20
Att. 2	20	0.008	0 / 20
Att. 3	20	0.200	0 / 20
Att. 4	20	0.105	0 / 20
Att. 5	20	0.022	0 / 20
Att. 6	20	0.045	0 / 20
Att. 7	20	0.091	0 / 20
Att. 8	20	0.204	0 / 20
Att. 9	20	0.169	0 / 20
Att. 10	20	0.090	0 / 20
Aver.	-	0.091	-
Max.	-	0.798	-

10명의 공격자들은 각각 20번씩 총 200번의 PIN 입력시도를 하였고, 평균 모델 결과는 0.091, 최대 모델 결과는 0.798이었다. 서버에서 설정한 인증 성공 기준은 0.9였고, 모델 결과가 0.9 이상인 경우는 한 번도 없었으며, 그에 따라 인증에 성공한 공격자는 아무도 없었다.

Table 4는 공격자(Att.)들에게 인증에 필요한 식별자로 터치 시간 데이터와 터치 위치 데이터도 필요하다는 사실을 알려준 후, 올바른 사용자가 PIN을 3번 연속으로 입력할 때, Fig. 11처럼 공격자들이 숄더 서핑 공격을 실행한 후 20번씩 인증을 시도한 보안성 실험의 결과이다.

공격자들의 평균 모델 결과는 0.261이었으며 공격자들이 올바른 사용자의 PIN만 알고 있다는 가정하에 진행된 실험의 모델 결과인 0.091보다 증가했다는 것을 알 수 있었다. 그리고 4번, 5번, 6번 공격자는 숄더 서핑 공격을 할 때 올바른 사용자가 입력하는 터치 시간과 터치 위치를 잘 파악하여 각각 7번, 1번, 2번의 성공을 하였다. 이 공격자들로부터 성공에 대한 의견을 들어보면, 올바른 사용자가 PIN을 입력하는 특징을 잘 파악하여 공격에 성공할 수는 있었지만, 한번 성공을 하더라도 특히 공격 시간 패턴을 잘 파악하고 있는 것이 어

려워서, 계속해서 성공을 유지하기에는 어렵다는 의견이 공통적이었다. 4번, 5번, 6번 공격자를 제외하면 숄더 서핑 공격 후에도 인증에 성공한 공격자는 없었고, 결과적으로 10명의 공격자가 20번씩 총 200번의 공격을 하였고, 그 중에 5%만이 성공했다는 것을 알 수 있었다.

Table 4. Results of the Security Experiment after 3 Times of Shoulder Surfing Attack

	Number of attempts	Average of Model Result	Number of Auth. Succ.
Att. 1	20	0.305	0 / 20
Att. 2	20	0.011	0 / 20
Att. 3	20	0.090	0 / 20
Att. 4	20	0.827	7 / 20
Att. 5	20	0.370	1 / 20
Att. 6	20	0.306	2 / 20
Att. 7	20	0.308	0 / 20
Att. 8	20	0.121	0 / 20
Att. 9	20	0.056	0 / 20
Att. 10	20	0.219	0 / 20
Aver.	-	0.261	-
Max.	-	0.938	-

보안성 실험의 결과인 Table 3과 Table 4를 통해서, 공격자가 우리가 제안한 기법을 사용하는 올바른 사용자의 PIN을 탈취하여 알고 있더라도, 터치 시간 데이터와 터치 위치 데이터를 모른다면 인증하기 어렵다는 것을 알 수 있었다. 또한 숄더 서핑 공격을 몇 차례 시도하더라도, 공격자가 올바른 사용자의 터치 시간 데이터와 터치 위치 데이터를 쉽게 탈취할 수 없다는 것도 알 수 있었다.

Table 5는 인증 성공 기준을 0.9로 설정한 상태에서 사용성 실험 결과와 보안성 실험 결과를 바탕으로 FAR, FRR을 분석한 결과이다.

Table 5. Analysis of the FAR and FRR Using Number of Authentication Success on Table 2, Table 3, and Table 4

	Number of Auth. Succ.	FAR	FRR
Table 2	100 / 100	-	0%
Table 3	0 / 200	0%	-
Table 4	10 / 200	5%	-

올바른 사용자의 사용성 실험을 진행한 결과인 Table 2에서 총 100번의 시도 중 인증 성공 횟수는 100번 모두였다. 이를 통해 FRR은 0%라는 것을 알게 되었다. 다음으로 공격자가 올바른 사용자의 PIN만 알고 있는 상태에서 보안성 분석을 진행한 결과인 Table 3에서는 총 200번의 시도 중 인증 성공 횟수는 0번이었으며, 이를 통해 이 실험의 FAR은 0%라는 것을 알게 되었다. 또한 공격자들이 숄더 서핑 공격을 실행한 후의 보안성 분석을 진행한 결과인 Table 4에서 총 200번의 시도 중 인증 성공 횟수는 10번이었으며, 이를 통해 이 실험의 FAR은 5%라는 것을 알게 되었다.

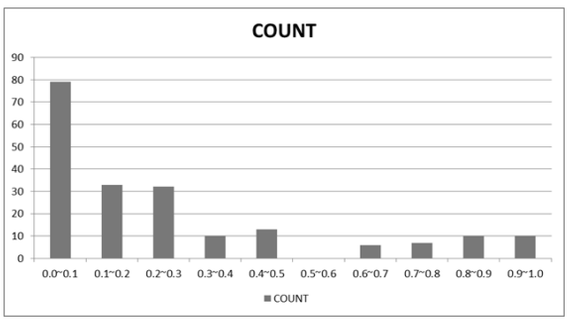


Fig. 12. Graph for Table 4

Fig. 12는 숄더 서핑 공격의 결과인 Table 4에 대한 그래프이다. 모델 결과가 0.0부터 0.9 사이일 때는 총 190번, 0.9부터 1.0 사이일 때는 10번의 결과가 있었고, 이를 통해 설정한 인증 성공 기준인 0.9는 적절한 기준이었다고 생각하였으며, 인증 성공 기준을 0.9이하로 설정하면 공격당할 확률이 증가한다는 것을 알 수 있었다. 더 나아가 숄더 서핑 공격에 성공한 공격자들의 모델 결과의 최대값이 0.938이었고, 올바른 사용자가 인증에 성공한 모델 결과의 최소값은 0.952였기 때문에, 인증 성공 기준을 0.95로 설정한다면 더욱 더 안전한 기법이 된다는 것도 알 수 있었다.

Table 6은 공격자가 올바른 사용자의 PIN과 터치 시간만을 알고 있을 때, 또는 올바른 사용자의 PIN과 터치 위치만을 알고 있을 때를 가정한 실험의 결과이다.

Table 6. Results of the Experiment When We Try to Authenticate with Only Two Identifiers

PIN, Time	Number of attempts	20
	Average of Model Result	0.062
	Maximum of Model Result	0.326
	Number of Auth. Succ.	0/20
PIN, Location	Number of attempts	20
	Average of Model Result	0.080
	Maximum of Model Result	0.247
	Number of Auth. Succ.	0/20

각 경우에 대해서 20번씩 인증 시도를 하였고, PIN과 터치 시간만 알고 있을 때의 평균 모델 결과는 0.062, 최대 모델 결과는 0.326, PIN과 터치 위치만 알고 있을 때의 평균 모델 결과는 0.080, 최대 모델 결과는 0.247이었다. 이에 따라 인증에 성공한 경우는 한 번도 없었다. 이를 통해 우리는 성공적인 인증을 하기 위해서는 PIN 뿐만 아니라 정확한 터치 시간과 터치 위치도 모두 함께 알고 있어야 한다는 것을 알 수 있었다.

4.6 보안성 분석

우리는 사용자가 스마트폰 상에서 비밀번호 또는 PIN을 입력할 때, 공격자들이 주로 사용하는 공격 방법인 스머지 공격, 키로깅 공격, 숄더 서핑 공격에 대한 보안성 분석을 진행하였다.

1) 스머지 공격 및 키로깅 공격

공격자가 일반적인 숫자 키패드를 사용하는 사용자를 스머지 공격으로 공격한다면, 스마트폰 스크린 표면의 묻은 지문의 흔적으로부터 사용자의 PIN을 알아낼 수 있을 것이다. 그러나 우리가 제안하는 기법은 일단 사용자 마다 다른 랜덤 숫자 키패드를 사용하고 있기 때문에, 공격자가 스머지 공격을 이용하여 사용자가 어느 숫자 키를 터치했는지 알기 어렵다. 뿐만 아니라 스머지 공격으로는 터치 시간 데이터까지 알아낼 수 없으므로, 우리가 제안하는 기법은 일반적으로 사용되는 숫자 키패드보다 스머지 공격에 강한 특징을 가지고 있다고 말할 수 있다.

공격자는 사용자가 PIN을 입력하기 위해 스마트폰을 터치할 때에 키로깅 공격으로 터치 위치 데이터를 탈취할 수 있다. 그러나 우리가 제안하는 기법은 일단 사용자 마다 다른 랜덤 숫자 키패드를 사용하고 있기 때문에, 탈취당한 터치 위치 데이터에 어떤 번호가 위치해 있었는지 알 수 없으므로 공격자는 사용자의 PIN을 정확히 알아 낼 수 없을 것이다. 뿐만 아니라 공격자는 사용자가 PIN을 입력할 때 숫자 버튼을 터치한 시간 데이터를 여전히 모르고 있기 때문에, 공격자는 인증에 성공할 수 없을 것이며, 그러므로 우리가 제안하는 기법은 일반적으로 사용되는 숫자 키패드보다 키로깅 공격에 강한 특징을 가지고 있다고 말할 수 있다.

2) 숄더 서핑 공격

우리가 제안하는 기법을 사용하는 사용자가 PIN을 입력하려고 할 때, 공격자는 숄더 서핑 공격으로 사용자가 어떤 번호를 터치하였는지 쉽게 알 수 있으며 그로인해 사용자의 PIN을 알아낼 수 있다. 그러나 공격자가 PIN을 쉽게 알아내더라도, 사용자가 정확히 어떠한 시간 패턴으로 터치를 했는지, 정확히 어느 위치를 터치 했는지 기억하지 못한다면 공격을 성공시키기 어려울 것이다. 그렇기 때문에 우리가 제안하는 기법은 숄더 서핑 공격에 강한 특징을 가지고 있으며, 보안성 실험 통해서도 숄더 서핑 공격에 강한 특징을 가지고 있다는 것을 한 번 더 확인할 수 있었다.

5. 결 론

이 논문에서는 머신러닝을 이용한 사용자 행동 인식 기반의 PIN 입력 기법을 제안하였다. 기존 키 입력 패턴 인식 연구는 주로 키보드를 이용하였지만, 우리는 스마트폰 금융 관련 어플리케이션에서 계좌이체 등의 서비스를 사용하기 위해 원격 인증을 이용하는 것을 목적으로 하였다. 이 기법은 사용자가 인증을 시도 할 때, PIN 뿐만 아니라 PIN을 입력하기 위해 스마트폰 스크린을 터치하는 시간과 위치까지 식별자로 사용한다. 그리고 이 식별자를 이용하여 올바른 사용자인지 아닌지는 머신러닝의 로지스틱 리그레션을 이용하여 판단한다. 우리는 사용성 실험과 보안성 실험을 통해서, 사용자들이 큰 불편함 없이 우리가 제안한 기법을 사용할 수 있다는 것(FRR : 0%)과 PIN이 공격자에게 탈취당해도 보안 사고가 발생하기 힘들다는 것(FAR : 0%)을 알 수 있었다. 또한 숄더 서핑 공격으로 공격을 당해도 보안 사고가 발생하기 힘들다는 것(FAR : 5%)을 알 수 있었다.

이 기법을 사용할 때에 사용자는 터치 시간과 터치 위치가 식별자로 사용된다는 것을 인지하고 있어야 하며 이것은 사용자에게 부담이 될 수도 있다. 이와 관련하여 사용자 등록 단계의 진행 시간을 줄이거나, 사용성을 높이기 위해 다양한 환경에서 다양한(더 많은) 사람들을 대상으로 사용성 실험을 추후 진행할 예정이다. 그리고 요즘에는 안경에 소형 카메라가 부착되어 있는 제품을 이용하여, 레코딩 공격을 할 수 있는 방법도 있기 때문에, 터치 시간과 터치 위치뿐만 아니라 사용자의 행동을 인식할 수 있는 요소인 가속도 센서, 자이로 센서 등의 스마트폰에서 사용할 수 있는 각종 센서를 이용하여 사용성과 보안성을 동시에 높이는 연구도 추후 연구 주제로 남긴다. 또한 머신러닝이 아닌, 딥러닝의 개념을 이용하여 렐루(ReLU), 멀티 레이어, 초기화, 드롭아웃 등의 기법을 가지고 올바른 사용자인지 판단하는 정확도를 높이는 연구도 추후 연구 주제로 남긴다.

References

[1] E. Jang, S. Oh, and J. Park, “Press release about simple mobile payment,” Korea Consumer Agency, Aug. 2016.

[2] C. Adams, “Personal Identification Number (PIN),” Encyclopedia of Cryptography and Security, p.927, 2011.

[3] S. Mun, “2017. 5. Wireless communication service subscriber statistics,” Ministry of Science, ICT and Future Planning, Jun. 2017.

[4] A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith, “Smudge Attacks on Smartphone Touch Screens,” *WOOT '10 Proceedings of the 4th USENIX Conference on Offensive Technologies*, 2010.

[5] F. Mohsen and M. Shehab, “Android Keylogging Threat,” *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Dec. 2013.

[6] W. Goucher, “Look behind you: the dangers of shoulder surfing,” *Computer Fraud & Security*, Vol.2011, Iss.11, pp.17-20. Nov. 2011.

[7] F. Cherifi, B. Hemery, R. Giot, M. Pasquet, and C. Rosenberger, “Performance Evaluation Of Behavioral Biometric Systems,” Book on Behavioral Biometrics for Human Identification: Intelligent Applications, 2009.

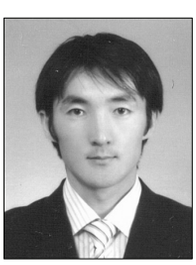
[8] J. Kim and M. Lee, “User authentication using touch positions in a touch-screen interface,” *Journal of the Korea Institute of Information Security & Cryptology*, Vol.21, pp.135-141, Feb. 2011.

[9] David E. Goldberg and John H. Holland, “Genetic Algorithms and Machine Learning,” *Machine Learning*, Vol.3, Iss.2-3, pp.95-99, 1988.

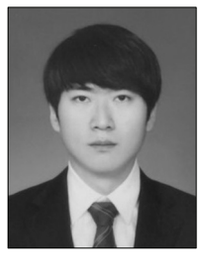
[10] S. Kim, Y. Kim, and D. Kim, “A Method of Activity Recognition in Small-Scale Activity Classification Problems via Optimization of Deep Neural Networks,” *KIPS Transactions on Software and Data Engineering*, Vol.6, No.3, pp.155-160, 2017.

[11] Yejin Yoon, Jong-Hyuk Im, and Mun-Kyu Lee, “Secure power demand forecasting using regression analysis on Intel SGX,” *Next Generation Computing Conference 2017*, Aug. 2017.
[12] Xinyou Yin, Jan Goudriaan, Egbert A. Lantinga, Jan Vos, and Huub J. Spiertz, “A Flexible Sigmoid Function of Determinate Growth,” *Annals of Botany*, Vol.91, Iss.3, pp.361-371, 2003.
[13] Lívia C. F. Araújo, Luiz H. R. Sucupira Jr., Miguel G. Lizárraga, Lee L. Ling, and João B. T. Yabu-uti, “User Authentication Through Typing Biometrics Features,” *IEEE Transactions on Signal Processing*, Vol.53, No.2, pp.851-855, 2005.
[14] P. Panasiuk and K. Saeed, “A Modified Algorithm for User Identification by His Typing on the Keyboard,” *Image Processing and Communications Challenges 2*, Springer, Berlin, Heidelberg, pp.113-120, 2010.
[15] S. J. Shepherd, “Continuous authentication by analysis of keyboard typing characteristics,” Security and Detection 1995, May. 1995.
[16] “TensorFlow,” Wikipedia, 2017.

정 창 훈
https://orcid.org/0000-0001-6299-1207
e-mail : jcptk677@gmail.com
2017년 인하대학교 컴퓨터정보공학과(석사)
2017년～현 재 인하대학교 컴퓨터공학과 박사과정
관심분야 : 인증 프로토콜, 네트워크 보안, 정보보호



Zayabaatar Dagvatur
https://orcid.org/0000-0003-1735-2099
e-mail : zayabaatar@gmail.com
2007년 인하대학교 컴퓨터정보공학과 (학사)
2007년～현 재 인하대학교 정보통신공학과 석・박사통합과정
관심분야 : 인증 프로토콜, 네트워크 보안, 암호학



장 룡 호
https://orcid.org/0000-0002-3417-6851
e-mail : jiyoo@seclab.inha.ac.kr
2013년 인하대학교 컴퓨터정보공학과 (학사)
2015년 인하대학교 컴퓨터정보공학과 (석사)
2015년～현 재 인하대학교 컴퓨터공학과 박사과정
관심분야 : 네트워크 보안, 무선 인터넷 보안, SDN

양 대 헌
https://orcid.org/0000-0001-5183-891X
e-mail : nyang@inha.ac.kr
1994년 한국과학기술원 전기 및 전자공학과(학사)
1996년 연세대학교 컴퓨터과학과(석사)
2000년 연세대학교 컴퓨터과학과(박사)
2000년～2003년 한국전자통신연구원 정보보호연구본부 선임연구원
2003년～현 재 인하대학교 컴퓨터공학과 교수
관심분야 : 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안, 네트워크 보안

이 경 희
https://orcid.org/0000-0001-5669-1216
e-mail : khlee@suwon.ac.kr
1993년 연세대학교 컴퓨터과학과(학사)
1998년 연세대학교 컴퓨터과학과(석사)
2004년 연세대학교 컴퓨터과학과(박사)
1993년～1996년 LG 소프트(주) 연구원
2000년～2005년 한국전자통신연구원 선임연구원
2005년～현 재 수원대학교 전기공학과 부교수
관심분야 : 바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식