KIPS Tr. Comp. and Comm. Sys.
Vol.6, No.12 pp.497~506 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2017.6.12.497

Technique for PIN Entry Using an Accelerometer Sensor and a Vibration Sensor on Smartphone

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

ABSTRACT

There have been previous researches about user authentication by analyzing the user's gait or behavior or action using the accelerometer sensor of smartphone, but there was a lack of user convenience to apply PIN entry. In this paper, we propose the technique for PIN entry without a touch on smartphone, the technique uses an accelerometer sensor and a vibration sensor built in the smartphone to enter the PIN. We conducted a usability experiment using the proposed technique and confirmed that the usability can be increased according to users become accustomed to this technique and that the users can enter PIN with 12.9 seconds and a probability of 100% on average. Also we conducted a security experiment and confirmed that an attack success rate is 0% when an attacker attacked the user using the recording attack and that it is more secure than the previous PIN entry technique. As a result, we was able to confirm that this technique can be used sufficiently.

Keywords : Authentication Protocol, PIN, Smartphone, Vibration, Accelerometer

스마트폰에서 가속도 센서와 진동 센서를 이용한 PIN 입력 기법

정 창 훈† · 장 룡 호† · 양 대 헌†† · 이 경 희†††

요 약

스마트폰의 가속도 센서로 사용자의 걸음이나 행동을 분석하여 사용자 인증을 하는 연구는 이전에도 있었으나, PIN 입력에 적용하기에는 사용자 편의성이 낮아서 부족한 면이 있었다. 이 논문에서는 스마트폰의 스크린을 직접 터치하는 것이 아니라, 스마트폰의 진동 센서와 가속도 센서를 이용하여 PIN을 입력하는 기법을 제안한다. 우리는 제안한 기법을 이용하여 사용성 실험을 진행하였고 사용자가 이 기법에 익숙해짐에 따라 사용성이 높아진다는 것과 그로인해 평균 12.9초, 100%의 확률로 PIN을 입력할 수 있다는 것을 확인하였다. 또한 보안성 실험을 통해 공격자가 촬영 공격을 이용하여 사용자를 공격했을 때 공격 성공률이 0%이였다는 것과 그로인해 기존에 존재하는 PIN 입력 기법보다 안전하다는 것을 확인하였다. 결과적으로 충분히 사용될 수 있는 기법이라는 것을 확인하였다.

키워드 : 인증 프로토콜, 핀, 스마트폰, 진동, 가속도

1. 서 론

PIN(Personal Identification Number)[1] 이란 개인 식별 번호를 의미하며 사용자 인증, 모바일 간편 결제 시스템, 모바일 뱅킹 등에서 사용되고 있다. 특히 최근 모바일 간편 결제 시스템에서 많이 사용되고 있으며, 결제 카드 선택 → 신용카드 선택 → 신용카드 유효기간 입력 → 신용카드 비밀번호 입력 → 공인인증서 비밀번호 입력 → 결제 완료를 거쳐야하는 일반 결제 시스템에 비해, 결제 카드 선택 → PIN(간편 결제 비밀번호) 입력 → 결제 완료의 절차만 거치면 되는 간편 결제 시스템은 점점 사용이 많아지고 있는 추세이다.

교보증권 리서치센터의 분석자료인 '간편결제 시장, 여전히 춘추전국시대'(2016.06.08.)[2]에 따르면 삼성전자의 간편 결제 서비스인 삼성 페이의 가입자 수는 약 500만 명이고

※ 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
†† 정 회 원 : 인하대학교 컴퓨터공학과 교수
††† 종신회원 : 수원대학교 전기공학과 부교수
Manuscript Received : July 20, 2017
Accepted : August 16, 2017
* Corresponding Author : KyungHee Lee(khlee@suwon.ac.kr)

누적결제액은 약 1조원, 네이버의 간편 결제 서비스인 네이버 페이의 가입자 수는 약 1600만 명이고 누적결제액은 약 1.8조원, SKT의 간편 결제 서비스인 시럽 페이의 가입자 수는 약 240만 명이고 누적결제액은 약 3500억 원이었으며, 가입자와 누적결제액 모두 지속적으로 증가하고 있기 때문에 PIN을 이용하는 금융 시장은 점점 커지고 있는 실정이다.

이렇게 PIN의 사용이 많아짐에 따라, PIN 사용에 따른 보안 사고도 증가하고 있는 추세이다. 그 첫 번째 이유는 PIN 입력 기법은 간단하게 네 자리 또는 여섯 자리의 숫자를 입력하는 시스템이고, PIN의 본래 취지가 사용자 편의성을 높이고 보안성을 낮춘 것이기 때문이다. 그에 따라 학교, 지하철, 버스 등의 공공장소에서는 PIN을 사용할 때 기존의 기법보다 사용성이 조금 낮더라도, 조금 더 높은 보안성을 가진 PIN 입력 기법이 필요한 실정이다.

두 번째로는 해커들의 공격 기법이 나날이 발전해가고 있기 때문이다. PIN 입력을 위하여 숫자를 입력하기 위해서는 스마트폰 스크린의 특정 위치를 터치해야 하므로, 스머지(Smudge) 공격[3] 및 키로깅(Keylogging) 공격[4]을 당할 수 있는 위험이 존재한다. 그리고 화질이 좋은 카메라를 가진 스마트폰, 액션 카메라 그리고 소형 카메라의 등장으로 숄더 서핑(Shoulder Surfing)[5] 및 촬영(Recording) 공격이 점점 간편해지고 있다. 또한 2014년 Qinggang Yue 등은 어떠한 사용자가 숫자 키패드를 이용하여 PIN을 입력할 때, 구글 글래스를 이용하여 사용자의 손동작을 분석할 수 있었고, 이를 통해 사용자의 PIN을 알아내는데 성공함으로서 보안상 취약점이 존재한다는 것을 보였다[6]. 그로인해 더 높은 보안성을 가진 PIN 입력 기법이 필요 되고 있다.

우리는 가속도 센서와 진동 센서를 이용하여 PIN을 입력하는 기법을 제안한다. 가속도 센서를 사용자 인증에 이용하는 연구는 이전에도 있었으나, 사용자의 걸음이나 행동으로 사용자를 확인하는 연구[7-9]였으며, 이는 생체 인식에 가까운 연구였고, PIN 입력에 적용하기에는 사용자 편의성이 낮아서 부족한 면이 있었다. 우리는 제안하는 기법을 직접 구현하였고, 보안성 분석을 통해 스머지 공격과 키로깅 공격에 강하다는 것을 보였다. 그리고 특히 숄더 서핑 및 촬영 공격에 대하여 공격당할 확률이 0.267%로 기존의 기법들보다 더 안전하다는 것을 확인하였다. 또한 사용성 실험과 보안성 실험을 통해, 사용자가 이 기법에 익숙해짐에 따라 사용성이 올라간다는 것과 이전에 존재하는 PIN 입력 기법보다 안전하다는 것을 알 수 있었다.

이 논문의 구성은 다음과 같다. 2장에서는 여러 가지 PIN 입력 기법에 대해서 알아보고, 3장에서는 스마트폰에서 가속도 센서와 진동 센서를 이용한 PIN 입력 기법을 알아본다. 4장에서는 사용성 실험과 보안성 실험을 진행하고 마지막 5장에서는 결론과 향후 연구에 대해 논의한다.

2. 관련 연구

2.1 공백 숫자 키패드를 사용하는 PIN 입력 기법

공백 숫자 키패드를 사용하는 PIN 입력 기법은 Fig. 1의 오른쪽 그림처럼 숫자 중간 중간에 랜덤으로 공백이 배치되어 있는 키패드를 사용하는 PIN 입력 기법이다. 이 키패드의 공백은 사용자가 PIN 입력을 시도할 때마다 숫자 중간 중간에 랜덤으로 배치가 되며, 그에 따라 1부터 0까지의 10개 숫자들은 순서대로 재배치된다. 결과적으로 사용자는 PIN 입력을 할 때마다 매번 같은 PIN을 입력하게 되더라도 이전과 다른 스마트폰 스크린의 위치를 터치해야 할 수도 있으며, 그러므로 스머지 공격과 키로깅 공격에 대해서 Fig. 1의 왼쪽 그림과 같은 일반적인 숫자 키패드를 사용하는 것보다는 강하다고 말할 수 있다. 그러나 공백을 제외한 나머지 숫자들이 오름차순으로 재배치되기 때문에 완벽히 안전하다고는 할 수 없으며[10], 숄더 서핑 및 촬영 공격에 대하여 여전히 보안상 취약점을 가지고 있다. Fig. 1의 오른쪽 그림인 공백 숫자 키패드를 사용하는 PIN 입력 기법은 2017년 국내 ㅅ은행 모바일 뱅킹 어플리케이션에서 사용되고 있다.

Fig. 1. PIN Entry Using the Normal Numeric Keypad, and PIN Entry Using the Numeric and Blank Keypad

2.2 랜덤한 숫자 키패드를 사용하는 PIN 입력 기법

랜덤한 숫자 키패드를 사용하는 PIN 입력 기법은 사용자가 PIN 입력을 시도할 때마다 Fig. 2와 같이 0부터 9까지인 10개의 숫자들이 랜덤하게 키패드에 배치된다. 그렇기 때문에 같은 PIN을 입력하게 되더라도 매번 스마트폰 스크린의 다른 위치를 터치해야 한다. 이에 따라 일반적인 숫자 키패드 또는 공백 숫자 키패드를 사용하는 PIN 입력 기법보다 사용자 편의성은 떨어지지만, 스머지 공격이나 키로깅 공격

에 대한 보안성은 강하다고 말할 수 있다. 그러나 여전히 숄더 서핑 및 촬영 공격에 대한 보안상 취약점을 가지고 있다. 2017년 국내에서는 ㄱ은행 모바일 뱅킹 어플리케이션에서 사용되고 있다.

Fig. 2. PIN Entry Using the Randomly Placed Numeric Keypad

2.3 입력할 때마다 숫자 키패드의 배치가 랜덤으로 변경되는 PIN 입력 기법

입력할 때마다 숫자 키패드의 배치가 랜덤으로 변경되는 PIN 입력 기법은 Fig. 3처럼 사용자가 PIN을 입력할 때, 숫자 한 개의 입력마다 숫자들의 배치가 랜덤으로 변경되는 키패드를 사용하는 PIN 입력 기법이다. 사용자는 PIN을 입력할 때 같은 숫자를 여러 번 입력하게 되더라도, 매번 스마트폰 스크린의 다른 위치를 터치해야 한다. 결과적으로 랜덤한 숫자 키패드를 사용하는 PIN 입력 기법보다 사용성은 떨어지지만 스머지 공격, 키로깅 공격에 대한 보안성은 강하다고 말할 수 있다. 그러나 여전히 숄더 서핑 및 촬영 공격에 대한 보안상 취약점을 가지고 있다.

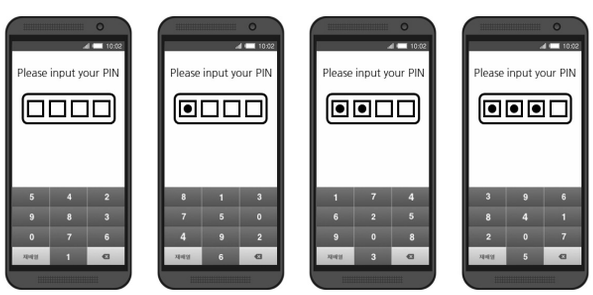


Fig. 3. PIN Entry Using Randomly Changing Numeric Keypad

2.4 검은색과 흰색을 사용하는 PIN 입력 기법

V. Roth 등은 검은색과 흰색을 사용하여 PIN을 입력하는 기법[11]을 개발하였다. 이 기법은 Fig. 4처럼 0부터 9까지의 숫자들 중 다섯 개의 배경색은 검은색으로, 나머지 다섯 개의 배경색은 흰색으로 표시되어진다. 사용자는 PIN을 입력하기 위하여 직접 숫자를 터치하는 것이 아니라, 숫자 아래쪽의 Black 또는 White 버튼으로 숫자를 입력할 수 있으며, 숫자들의 배경색은 Black 또는 White 버튼을 터치할 때마다 랜덤으로 변경된다. 하나의 숫자를 입력하기 위해서는 네 번의 Black 또는 White 버튼의 터치가 필요하며, 사용자가 원하는 숫자의 배경색을 순서대로 네 번 터치하면 된다. Fig. 4는 사용자가 3을 입력하기 위하여 순서대로 White, Black, White, Black을 터치하는 사진이다. 이 기법은 스머지 공격, 키로깅 공격에는 강하지만 숄더 서핑 및 촬영 공격에는 취약점을 가지고 있다.

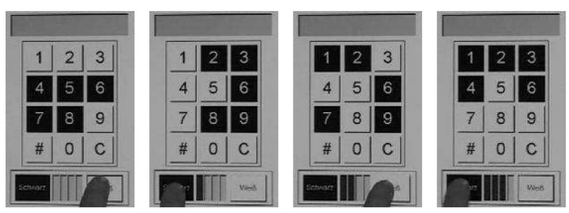


Fig. 4. PIN Entry Using Black and White Keypad

2.5 소리를 사용하는 PIN 입력 기법

A. Bianchi 등은 소리를 이용하여 PIN을 입력 할 수 있는 The Phone Lock[12]을 개발하였다. The Phone Lock은 Fig. 5처럼 0부터 9까지의 숫자와 매칭되어 있는 10개의 도형과 하나의 원으로 구성되어 있다. 사용자는 PIN을 입력하기 이전에 10개의 도형 중 하나를 터치하면 0부터 9까지의 숫자 중 하나가 영어로 재생되는 것을 들을 수 있으며, 이 도형들과 매칭되어 있는 숫자들은 시계방향의 오름차순으로 정렬이 되어 있다. 그러므로 사용자는 소리를 통해 보이지 않는 숫자들의 위치를 알 수 있게 되며, 원하는 숫자와 매칭되어 있는 도형을 드래그한 후 가운데 원으로 드롭을 하면 숫자가 입력이 된다. 이러한 과정으로 사용자는 PIN을 입력할 수 있으며, 숫자의 배치는 매번 PIN 입력을 할 때마다 변경된다. 이 기법은 스머지 공격과 키로깅 공격에는 강하지만 숄더 서핑 및 촬영 공격에는 약하고, PIN을 입력할 때마다 이어폰을 착용해야 한다는 불편함이 존재한다.

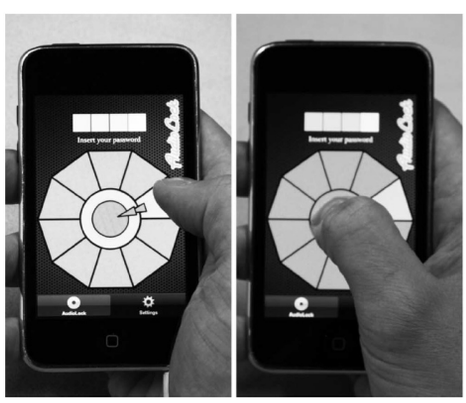


Fig. 5. PIN Entry Using the Phone Lock

3. 스마트폰에서 가속도 센서와 진동 센서를 이용한 PIN 입력 기법

3.1 스마트폰에서 가속도 센서와 진동 센서를 이용한 PIN 입력 기법

이 논문에서 제안하는 기법은 스마트폰에 내장 되어 있는 진동 센서와 가속도 센서를 이용하여 사용자가 스마트폰의 스크린을 터치하지 않으면서 PIN을 입력하는 기법이다. 진동 센서는 어떠한 이벤트가 발생하면 진동을 발생시키는 센서이고, 가속도 센서는 스마트폰의 기울기, 위치 등에 따라 중력 가속도 값을 측정하여 x, y, z값으로 출력해주는 센서이다. 여기서 x는 왼쪽과 오른쪽을 의미하고, y는 위와 아래를 의미하고, z는 앞과 뒤를 의미한다.

이 기법은 PIN 입력을 위한 모션, 랜덤한 공백 시간, 현재 상태 값의 설정이라는 특징을 가지고 있다. 먼저 PIN 입력을 위한 모션은 다음과 같다.

- 왼쪽으로 기울이기 : Fig. 6의 왼쪽 사진처럼 스마트폰을 왼쪽으로 기울이면 진동 센서가 진동을 하나씩 연속적으로 발생시키고, 진동이 한 번 발생할 때마다 현재 상태 값이 -1이 된다.
- 오른쪽으로 기울이기 : Fig. 6의 오른쪽 사진처럼 스마트폰을 오른쪽으로 기울이면 진동센서가 진동을 하나씩 연속적으로 발생시키고, 진동이 한 번 발생할 때마다 현재 상태 값이 +1이 된다.
- 정면으로 되돌리기 : Fig. 6의 가운데 사진처럼 스마트폰을 사용자의 정면으로 되돌리면 현재 상태 값이 입력된다.
- 현재 상태 값과 같은 값을 입력하기 : 스마트폰을 왼쪽 또는 오른쪽으로 기울였다가 진동이 발생하기 전에 재빨리 정면으로 되돌리면 현재 상태 값과 같은 값이 입력된다.

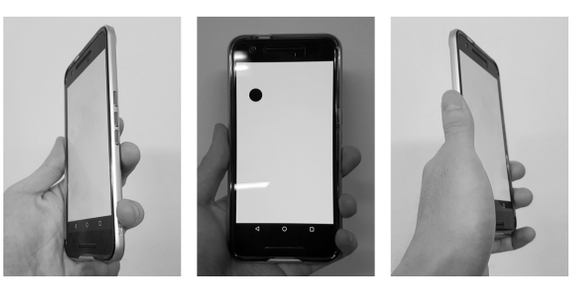


Fig. 6. Motion for PIN Entry Without Touch on Smartphone

랜덤한 공백 시간은 다음과 같다. 사용자가 PIN 입력을 위해 스마트폰을 왼쪽이나 오른쪽으로 기울이면 진동이 발생하는데, 이 때 진동은 0.3초 동안 발생하며, 하나의 진동이 발생하기 이전에는 0.3초부터 0.8초 사이에서 0.1초 단위의 랜덤으로 정해진 공백 시간이 존재한다. 그러므로 진동 이전의 랜덤한 공백 시간은 0.3초, 0.4초, 0.5초, 0.6초, 0.7초, 0.8초 중 하나가 될 수 있다. Fig. 7은 이러한 특징을 이용하여 사용자가 네 자리의 PIN 중 하나의 숫자를 입력할 때 진동이 발생하는 예시이다. 사용자가 스마트폰을 왼쪽으로 기울이면 랜덤한 공백 시간과 진동이 반복적으로 발생하며 진동이 발생할 때마다 현재 상태 값이 변경되고, 사용자가 원할 때 스마트폰을 정면으로 되돌리면 현재 상태 값이 입력된다. 랜덤한 공백 시간은 공격자가 시간 분석을 이용해 사용자를 공격할 때, 이를 어렵게 하는 것을 목적으로 한다.

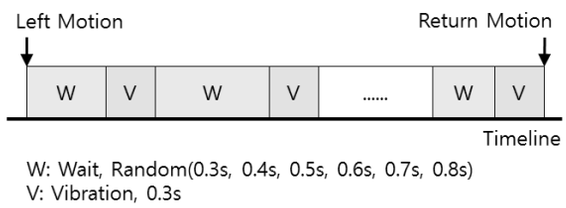


Fig. 7. An Example of Vibration Generation for Choosing the One of the PIN

현재 상태 값의 설정은 다음과 같다. 현재 상태 값은 입력하려는 값을 의미하며, 스마트폰을 왼쪽으로 기울이거나 오른쪽으로 기울이는 모션을 하면 진동이 발생하는데, 이 진동에 따라 -1이 되거나 +1이 된다. 이때 0에서 -1이 되는 경우는, -1이 되는 것이 아니라 9로 변경이 되고, 9에서 +1이 되는 경우는 10이 아니라 0으로 변경이 된다. 그리고 이렇게 현재 상태 값이 변경되는 도중에, 스마트폰을 정면으로 되돌리면 현재 상태 값이 입력된다. 현재 상태 값의 초기 값은 사용자가 직접 설정할 수 있어서 사용자 의존성을 가지며, 이는 공격자가 사용자의 PIN을 추측할 때, 추측할 수 있는 확률을 낮추는 것을 목적으로 한다.

사용자는 이러한 특징을 이용하여 PIN을 입력 할 수 있으며, PIN을 입력하기 위하여 사용자가 스마트폰의 스크린을 터치하는 동작은 필요하지 않다.

우리가 제안하는 기법의 이해를 돕기 위해 하나의 예시를 들어보자면 다음과 같다. 사용자는 현재 상태 값의 초기 값을 0으로 설정하였고, 7593이라는 PIN을 입력하려고 한다. 먼저 사용자는 스마트폰을 왼쪽으로 기울여서 진동이 3번 울리면 스마트폰을 정면으로 되돌린다. 이 행동의 시간은 1.8초에서 3.3초 사이가 될 것이며, 이렇게 되면 7이 입력될 것이다. 다음으로는 다시 스마트폰을 왼쪽으로 기울여서 진동이 5번 울리면 스마트폰을 정면으로 되돌린다. 이 행동의 시간은 3초에서 5.5초 사이가 될 것이며, 이렇게 되면 5가 입력될 것이다. 다음으로는 다시 스마트폰을 왼쪽으로 기울여서 진동이 1번 울리면 스마트폰을 정면으로 되돌린다. 이

행동의 시간은 1.2초에서 2.2초 사이가 될 것이며, 이렇게 되면 9가 입력될 것이다. 마지막으로는 스마트폰을 오른쪽으로 기울여서 진동이 3번 울리면 스마트폰을 정면으로 되돌린다. 이 행동의 시간은 1.8초에서 3.3초 사이가 될 것이며, 이렇게 되면 3이 입력될 것이다. 결과적으로 약 7.8초에서 14.3초 사이의 시간이 걸릴 것이고, 7593이 입력되게 된다. 그리고 이러한 입력 과정을 슈도코드로 나타내면 (알고리즘 1)과 같다.

Algorithm 1. Pseudo code for use example

```
1 : Tilt Left
2 :   Vibration occurrence
3 :   if a number of Vibration == 3
4 :     Revert to the front
5 : Tilt Left
6 :   Vibration occurrence
7 :   if a number of Vibration == 5
8 :     Revert to the front
9 : Tilt Left
10 :  Vibration occurrence
11 :  if a number of Vibration == 1
12 :    Revert to the front
13 : Tilt Right
14 :  Vibration occurrence
15 :  if a number of Vibration == 3
16 :    Revert to the front
```

3.2 보안성 분석

보안성 분석에서는 현재 상태 값의 초기 값을 0으로, 사용자의 PIN을 7593이라고 기준을 정하고 진행한다. 또한 현재 상태 값의 초기 값이 0인 상황이므로, 사용자가 최대한 빠르게 PIN을 입력하기 위해 1, 2, 3, 4는 스마트폰을 오른쪽으로 기울여서 선택한다고 하고, 5, 6, 7, 8, 9, 0은 왼쪽으로 스마트폰을 기울여서 선택한다고 기준을 정한다.

1) 스머지 공격 및 키로깅 공격

사용자는 7593을 입력하기 위하여, 스마트폰을 왼쪽 또는 오른쪽으로 기울이거나 스마트폰의 스크린을 사용자의 정면으로 되돌리기만 하면 된다. 그러므로 스마트폰의 스크린을 터치하지 않아도 되기 때문에 스마트폰 스크린의 지문을 이용한 스머지 공격이나 터치하는 키가 무엇인지를 탈취하는 키로깅 공격에 안전하다고 말할 수 있다.

2) 숄더 서핑 및 촬영 공격

공격자는 스머지 공격, 키로깅 공격이 아닌 숄더 서핑 및 촬영 공격으로도 사용자를 공격할 수 있다. 그런데 공격자는 숄더 서핑 및 촬영 공격으로 사용자를 공격한다고 하더라도, 사용자가 스마트폰을 기울이고 있었던 시간을 분석해야 하기 때문에 사용자의 PIN을 바로 알아 낼 수 없다.

예를 들면 사용자가 6을 입력하려고 하고, 현재 상태 값의 초기 값, 진동 시간, 진동 이전의 랜덤한 공백 시간을 고려하면, 6을 입력하는 시간은 2.4초에서 4.4초 사이가 될 수 있다. 그리고 2.4초에서 4.4초 사이의 시간은 6뿐만 아니라 3, 4, 5, 7을 선택하는 시간이 될 수도 있기 때문에 공격자는 사용자가 어떤 숫자를 입력했는지 바로 알 수 없을 것이다. 이에 대하여 숫자 하나하나에 대하여 숄더 서핑 및 촬영 공격으로 공격당할 확률을 계산하면 Table 1과 같다.

Table 1. Probability that Numbers can be Attacked

#	Time		Possible candidates	Probability (about)
	Min	Max		
1	0.6 s	1.1 s	1	100%
2	1.2 s	2.2 s	1, 2	50%
3	1.8 s	3.3 s	2, 3, 4, 5	25%
4	2.4 s	4.4 s	3, 4, 5, 6, 7	20%
5	3.0 s	5.5 s	1, 2, 3, 4, 5, 6, 7	14%
6	2.4 s	4.4 s	3, 4, 5, 6, 7	20%
7	1.8 s	3.3 s	5, 6, 7, 8	25%
8	1.2 s	2.2 s	7, 8	50%
9	0.6 s	1.1 s	9, 0	50%
0	0.1 s	0.7 s	9, 0	50%

Table 1을 기반으로 사용자가 네 자리의 PIN 7593을 입력한다고 가정하고, 이것에 대하여 공격당할 확률을 계산하면 0.25 × 0.14 × 0.5 × 0.25 × 100이므로 약 0.437%이다. 그런데 사용자의 PIN은 7593이 아닐 수도 있기 때문에, 우리는 한 자리에 대하여 숫자들이 공격당할 확률들을 평준화하였고, 평준화를 하면 (1 × 0.5 × 0.25 × 0.2 × 0.14 × 0.2 × 0.25 × 0.5 × 0.5 × 0.5) × 100이므로 평준화된 확률은 약 40.428%이었다. 그리고 PIN은 보통 네 자리이기 때문에 네 자리에 대한 평준화된 확률을 계산하면 $((0.40428)^4) \times 100$이므로 약 2.671%가 된다. 그런데 여기서 현재 상태 값의 초기 값은 사용자 의존성을 가지기 때문에, 공격자는 사용자의 현재 상태 값이 초기 값이 0부터 9 사이 중 어떤 값인지 알 수 없으므로, 최종적으로 평준화된 확률은 2.671 × 0.1 × 100 = 0.267%가 된다. 그리고 이것을 수식으로 나타내면 아래의 Equation (1)과 같으며, M은 평균을 의미한다.

$$(M(probability\ of\ numbers))^4 \times 0.1 \quad (1)$$

이렇게 했을 때 기존의 PIN 입력 기법들과 비교 분석한 결과는 Table 2와 같다. 현재 상태 값의 초기 값과 사용자의 PIN은 사용자 의존성을 가지기 때문에, 결과적으로 이 기법을 사용하는 사용자가 숄더 서핑 및 촬영 공격으로 공격당할 확률은 사용자에 따라 달라질 수 있다. 그렇지만 Table 2에 나와 있듯이 공격당할 확률을 평준화하였을 때 약 0.267%였기 때문에 기존에 기법들에 비해서 이 논문에서 제안하는 기법은 보다 안전할 것으로 보인다.

Table 2. The Comparison of Technique for PIN Entry Against Shoulder Surfing Attack and Recording Attack

Technique for PIN entry	Probability against SSA and RA (about)
Using the normal numeric keypad	100%
Using the numeric and blank keypad	100%
Using the randomly placed numeric keypad	100%
Using randomly changing numeric keypad	100%
Using black and white keypad	100%
Using the Phone Lock	10%
Without touch on smartphone	0.267%

4. 사용성 실험

4.1 사용성 실험 방법

우리는 사용자들이 우리가 제안하는 기법을 얼마나 쉽게 사용할 수 있는지를 검토하기 위하여, 사용 정확도와 사용자 편의성 실험을 진행하였다. 사용 정확도 실험은 사용자가 얼마나 정확하게 사용할 수 있는지를 알아보기 위하여 진행하였고, 사용 편의성 실험은 사용자가 얼마나 빠르게 사용할 수 있는지를 알아보기 위하여 진행하였다.

실험을 위해 8명의 피험자를 모집하였으며, 피험자 1과 2는 30대 남성, 피험자 3과 4는 20대 남성, 피험자 5와 6은 30대 여성, 피험자 7과 8은 20대 여성이었다. 그리고 피험자 1, 2, 3, 4, 8은 대학 연구실에서, 피험자 5, 6, 7은 카페에서 실험을 진행하기로 정하였고, 실험에 사용할 스마트폰은 Nexus 6P로 정하였다. 다음으로는 우리가 제안한 PIN 입력 방법을 모든 피험자들에게 자세하게 설명하였고 PIN을 입력하는 과정을 직접 2번씩 보여주었다. 그리고 이 실험은 보안성 분석과 마찬가지로 현재 상태 값의 초기 값을 0으로, 사용자의 PIN을 7593이라고 기준을 정하고 진행하였다. 또한 현재 상태 값의 초기 값이 0인 상황이므로, 사용자가 최대한 빠르게 PIN을 입력하기 위해 1, 2, 3, 4는 스마트폰을 오른쪽으로 기울여서 선택한다고 하고, 5, 6, 7, 8, 9, 0은 왼쪽으로 스마트폰을 기울여서 선택한다고 하는 규칙을 정하고 진행하였다.

우리는 먼저 이전의 사용되고 있는 기법과 비교해보기 위하여 5명의 피험자들에게 2.3 입력할 때마다 숫자 키패드의 배치가 랜덤으로 변경되는 PIN 입력 기법을 이용하여 5번의 성공이 이루어질 때까지 PIN 입력을 시도하게 하였고, 각 시도에 대하여 성공·실패 여부와 시간을 기록하였다. 그 다음에는 우리가 제안한 기법을 이용하여 5번의 성공이 이루어질 때까지 PIN 입력을 시도하게 하였고, 각 시도에 대하여 성공·실패 여부와 시간을 기록하였다.

그리고 피험자들이 우리가 제안한 기법에 익숙해짐에 따라 사용성이 올라가는지를 알아보기 위하여 일주일 후에 다시 우리가 제안한 기법을 이용하여 3번의 성공이 이루어질 때까지 PIN 입력을 시도하게 하였고, 각 시도에 대하여 성공·실패 여부와 시간을 기록하였다.

4.2 사용성 실험 결과

Table 3은 입력할 때마다 숫자 키패드의 배치가 랜덤으로 변경되는 PIN 입력 기법을 이용한 실험 결과이다. 피험자들은 5번의 PIN 입력이 성공할 때까지 실험을 진행하였다. 피험자들은 PIN 입력을 할 때에 실패한 적이 없었으며, 그에 따라 평균 PIN 입력 성공률은 100%였다. 그리고 입력할 때의 평균적으로 걸린 시간은 약 5.0초였다.

Table 3. Results of Usability Experiment Using Randomly Changing Numeric Keypad

	1st	2nd	3rd	4th	5th
Subject 1	8.1 s	5.8 s	5.1 s	5.5 s	5.7 s
Subject 2	5.6 s	4.8 s	5.1 s	6.0 s	5.1 s
Subject 3	5.2 s	4.1 s	4.2 s	3.5 s	3.5 s
Subject 4	5.1 s	5.1 s	3.9 s	4.4 s	4.7 s
Subject 5	5.1 s	5.5 s	4.9 s	6.2 s	5.2 s
Subject 6	6.1 s	4.8 s	5.7 s	5.2 s	5.4 s
Subject 7	5.3 s	5.5 s	4.2 s	4.8 s	4.5 s
Subject 8	4.2 s	3.9 s	4.0 s	4.6 s	3.5 s
Average	Success rate : 100% / Elapsed time : 5.0 s				

Table 4. Results of Usability Experiment Using Proposed Method (Time unit: second)

	1st	2nd	3rd	4th	5th	6th	7th	8th
Sub. 1	19.7	X	14.0	14.9	12.0	11.8		
Sub. 2	16.2	17.2	14.6	13.5	14.1			
Sub. 3	17.2	13.9	13.5	X	12.4	11.6		
Sub. 4	X	X	18.8	X	14.2	15.9	11.8	14.0
Sub. 5	X	18.1	16.4	16.1	16.7	15.8		
Sub. 6	17.9	17.8	X	16.3	15.9	16.3		
Sub. 7	16.3	15.9	17.5	17.1	X	16.5		
Sub. 8	17.8	17.0	17.3	15.1	16.0			
Aver.	Success rate : 83% / Elapsed time : 15.6 s							

Table 4는 스마트폰에서 가속도 센서와 진동 센서를 이용한 PIN 입력 기법을 이용한 실험 결과이다. 피험자들은 5번의 PIN 입력이 성공할 때까지 실험을 진행하였다. 첫 번째 피험자는 1번, 세 번째 피험자는 1번, 네 번째 피험자는 3번, 다섯 번째 피험자는 1번, 여섯 번째 피험자는 1번, 일곱 번째 피험자는 1번의 PIN 입력 실패가 있었으며, 두 번째와 여덟 번째 피험자는 실패 없이 연속으로 5번을 성공하였다. 그에 따라 평균 PIN 입력 성공률은 83%였다. 그리고 입력할 때의 평균적으로 걸린 시간은 15.6초였다.

Table 5는 피험자들이 우리가 제안한 기법에 익숙해짐에 따라 사용성이 올라가는지를 알아보기 위하여 일주일 후에 다시 우리가 제안한 기법을 이용하여 3번의 성공이 이루어질 때까지 PIN 입력을 시도하게 한 실험의 결과이다. 8명의 피험자 모두 PIN 입력에 대하여 실패는 없었으며, 평균적으로 걸린 시간은 약 13초였다.

Table 5. Results of Usability Experiment Using Proposed Method After One Week

	1st	2nd	3rd
Subject 1	11.3	10.4	10.5
Subject 2	12.3	12.2	12.3
Subject 3	12.0	11.6	12.0
Subject 4	14.4	13.3	12.4
Subject 5	14.3	12.9	13.2
Subject 6	13.1	13.8	12.1
Subject 7	13.5	12.7	12.5
Subject 8	16.6	16.3	15.8
Average	Succeess rate : 100% / Elapsed time : 13 s		

우리가 제안한 PIN 입력 기법은 이전에 사용되고 있던 기법보다 높은 보안성을 가지고 있지만, 사용자 실험 결과인 Table 3과 Table 4를 비교해보면 우리가 제안한 기법이 이전의 사용되고 있던 기법보다 사용성이 낮다는 것을 알 수 있었다. 왜냐하면 이전에 사용되고 있던 기법의 PIN 입력 성공률은 100%이고 걸린 시간은 약 5.0초였지만, 우리가 제안한 기법의 PIN 입력 성공률은 83%이고 걸린 시간은 약 15.6초였기 때문이다.

그러나 우리가 제안한 기법을 이용하여 일주일 간격을 두고 실험한 결과인 Table 4와 Table 5를 비교해보면 PIN 입력 성공률은 83%에서 100%로 증가하였고, 걸린 시간은 약 15.6초에서 13초로 감소하였으며, 이에 따라 우리가 제안한 PIN 입력 기법은 사용자가 이 기법에 익숙해짐에 따라 사용성이 올라간다는 것을 알 수 있었다. 여기서 걸린 시간에 대한 결과를 그래프로 내타내었더니 Fig. 8과 같았으며, 결과적으로 사용성은 사용자가 이 기법을 많이 사용하면 할수록 그에 따라 점점 높아질 것으로 보인다.

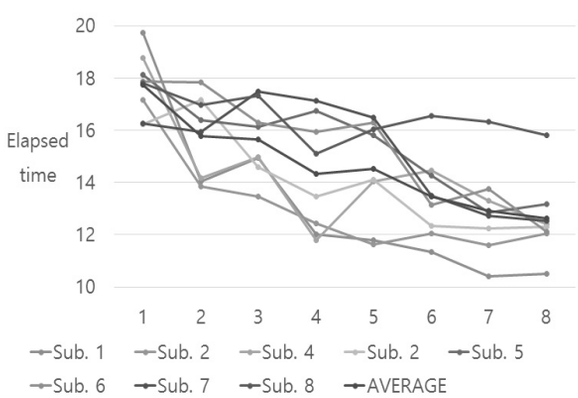


Fig. 8. An Overall Results of Usability Experiment Using Proposed Method

그리고 또한 Table 5의 사용성 실험 결과를 피험자의 연령별, 성별, 장소별로 구분하면 다음 Table 6과 같았으며, 이러한 특성들로 구분한 결과의 차이는 두드러지게 보이지 않았다.

Table 6. Results of security experiment

	Success rate on Aver.	Elapsed time on Aver.
Thirty	100%	12.4 s
Twenty	100%	13.6 S
Male	100%	12.1 s
Female	100%	13.9 s
in Lab	100%	12.9 s
in Cafe	100%	13.1 s

4.3 보안성 실험 방법

사용성 실험 이후에 우리는 촬영 공격에 대하여 우리가 제안한 기법이 얼마나 안전한지를 검토하기 위하여 보안성 실험을 진행하였다. 피험자의 수, 사용한 스마트폰, 현재 상태 값의 초기 값, 사용자의 PIN, PIN을 입력할 때의 기울이는 방향은 모두 사용성 실험과 동일하게 진행하였다.

먼저 이전의 사용되고 있는 기법과 비교해보기 위하여 8명의 피험자들에게 2.3 입력할 때마다 숫자 키패드의 배치가 랜덤으로 변경되는 PIN 입력 기법을 이용하여 PIN을 입력하는 장면을 녹화해서 3번을 보여준 다음 PIN 입력을 시도하게 하였고, 각 시도에 대하여 성공·실패 여부를 기록하였다. 그 다음으로는 우리가 제안한 기법을 이용하여 PIN을 입력하는 장면을 녹화해서 3번을 보여주었다. 녹화 장면을 보여줄 때에는 스마트폰을 기울이는 시간을 기억하라고 한 다음에, 최대한 비슷하게 PIN 입력을 시도하라고 요청하였으며, 우리는 각 시도에 대하여 성공·실패 여부를 기록하였다.

4.4 보안성 실험 결과

Table 7은 보안성 실험의 결과이다. 피험자들이 2.3 입력할 때마다 숫자 키패드의 배치가 랜덤으로 변경되는 PIN 입력 기법으로 PIN을 입력하는 녹화 장면을 시청한 후 공격을 시도했을 때에는 공격 성공률이 100%였으며, 우리가 제안한 기법으로 PIN을 입력하는 녹화 장면을 시청한 후 공격을 시도했을 때에는 공격 성공률이 0%였다. 제안한 기법의 성공·실패 여부 옆의 나와 있는 숫자는 피험자가 공격할 때 입력한 PIN을 의미한다.

피험자들이 2.3 입력할 때마다 숫자 키패드의 배치가 랜덤으로 변경되는 PIN 입력 기법으로 PIN을 입력하는 촬영 장면을 3번 시청하였을 때는 모두 정확하게 어떤 PIN이 입력이 되었는지 알 수 있었다. 촬영 장면에서 어떤 숫자 버튼이 터치 되는지 바로 보였기 때문이다. 그러나 우리가 제안한 기법으로 PIN을 입력하는 촬영 장면을 3번 시청한 후 공격을 시도했을 때에는 피험자들이 스마트폰을 기울이는 시간을 100% 완벽하게 따라할 수 없었기 때문에 공격에 성공한 피험자는 없었다. 우리가 제안한 기법은 랜덤한 공백 시간이라는 특징을 갖고 있기 때문에, 비슷한 시간이어도 발생하는 진동의 수가 다를 수 있고, 그에 따라 다른 숫자가 입력될 수 있기 때문이다. 결과적으로 촬영 장면을 통해서 올바른 사용자가 정확하게 어떤 PIN을 입력하였는지 피험자들은 알 수 없었다. 5번 피험자 같은 경우는 7693을 입력하였으며, 올바른 사용자의 PIN인 7593하고 비교해보았을 때 약 3/4이 맞았지만, 공격자 입장에서는 공격할 때의 자기가 입력한 PIN이 올바른 사용자의 PIN과 어떻게 다르기 때문에 공격에 실패했는지 모르기 때문에, 즉, 공격자가 입력한 7693 중 어떤 자리의 숫자가 맞았는지 또는 틀렸는지 정확하게 알 수 없기 때문에 정확하게 사용자의 PIN이 무엇인지 알아내기 힘들 것이다. 이를 통해 우리는 이전에 사용되고 있던 PIN 입력 기법보다 촬영 공격에 대하여 안전하다는 것을 알 수 있었다.

Table 7. Results of Security Experiment

	Random key	Proposed Tech.
Subject 1	Success	Fail (7692)
Subject 2	Success	Fail (7584)
Subject 3	Success	Fail (8764)
Subject 4	Success	Fail (5683)
Subject 5	Success	Fail (7693)
Subject 6	Success	Fail (7692)
Subject 7	Success	Fail (7694)
Subject 8	Success	Fail (6693)
Average Suc. rate	100%	0%

5. 결 론

이 논문에서 제안하는 기법은 PIN을 입력하기 위하여 스마트폰의 스크린을 직접 터치하는 것이 아니라, 진동 센서와 가속도 센서를 이용하는 기법이다. 우리는 이 기법을 구현하였으며, 보안성 분석, 사용성 실험, 보안성 실험을 진행하였다. 그리하여 기존의 기법들 보다 이 논문에서 제안하는 기법이 더 안전하지만, 사용자에게 더 부담이 될 수 있다는 것도 확인하였다. 그러나 사용자가 우리가 제안한 기법을 사용하면 할수록 그 부담은 점점 줄어든다는 것도 확인하였으며 지하철, 버스, 강의실 등의 공공장소에서는 공개된 장소이기 때문에 부담이 있더라도 보안성을 높여서 사용

해야 하므로, 우리가 제안하는 기법이 충분히 쓰일 수 있을 것으로 예상된다. 보안 분야에서 사용성과 보안성은 항상 트레이닝 오프 관계를 가지며, 사용성과 보안성을 동시에 높이는 연구는 추후 연구로 남긴다. 또한 가속도 센서 뿐만이 아닌 다른 센서들도 함께 이용하여 인증을 진행하는 연구도 추후 연구로 남긴다. 이 기법은 사용자 인증, 모바일 간편 결제 시스템 그리고 모바일 뱅킹 등에 적용되어 사용될 수 있을 것으로 기대된다.

References

[1] C. Adams, "Personal Identification Number (PIN)," *Encyclopedia of Cryptography and Security*, pp.927, 2011.

[2] S. B. Lee, "Simple Payment Market, still in Warring States period," Industry Report on Kyobo Securities Co., Ltd. Research Center, 2016.

[3] 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*, Washington, 2010.

[4] F. Mohsen and M. Shehab, "Android Keylogging Threat," *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Texas, 2013.

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

[6] Q. Yue, Z. Ling, X. Fu, B. Liu, W. Yu, and W. Zhao, "My google glass sees your passwords!," in *Proceedings of the Black Hat USA 2014*, Las Vegas, 2014.

[7] D. Gafurov, E. Snekkenes, and P. Bours, "Gait Authentication and Identification Using Wearable Accelerometer Sensor," *2007 IEEE Workshop on Automatic Identification Advanced Technologies*, Alghero, 2007.

[8] J. S. Seo and J. S. Moon, "A Study on User Authentication with Smartphone Accelerometer Sensor," *Journal of the Korea Institute of Information Security & Cryptology*, Vol.25, No.6, pp.1477-1484, 2015.

[9] Y. K. Kim and J. S. Moon, "User Authentication Using Accelerometer Sensor in Wrist-Type Wearable Device," *KIPS Transactions on Computer and Communication Systems*, Vol.6, No.2, pp.67-74, 2017.

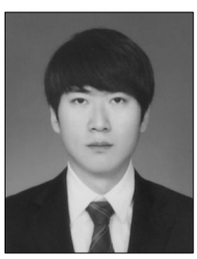
[10] B. Shakirov, H. J. Kim, K. H. Lee, and D. H. Nyang, "Analysis on Vulnerability of Password Entry Using Virtual Onscreen Keyboard," *Journal of the Korea Institute of Information Security & Cryptology*, Vol.26, No.4, pp.857-869, 2016.

[11] V. Roth, K. Richter, and R. Freidinger, "A PIN-Entry Method Resilient Against Shoulder Surfing," *CCS '04 Proceedings of the 11th ACM conference on Computer and Communications Security*, Washington, pp.236-245, 2004.

[12] A. Bianchi, I. Oakley, V. Kostakos, and D. Kwon, "The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices," *TEI '11 Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction*, Funchal, pp.197-200, 2011.

정 창 훈

http://orcid.org/0000-0001-6299-1207
e-mail : jcptk677@gmail.com
2014년 인하대학교 컴퓨터정보공학과 (석사)
2014년~현 재 인하대학교 컴퓨터공학과 박사과정
관심분야 : 인증 프로토콜, 네트워크 보안, 정보보호



장 룡 호

http://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

http://orcid.org/0000-0001-5183-891X
e-mail : nyang@inha.ac.kr
1994년 한국과학기술원 과학기술대학 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

http://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