Journal of Convergence for Information Technology
Vol. 10. No. 8, pp. 144-151, 2020
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2020.10.08.144

핀테크에서 터치 위치 차단을 위한 테트리스 모양의 보안 키패드의 구현

문형진[1], 강신영[2], 신좌철[3*]
[1]성결대학교 정보통신공학부 교수, [2]호서대학교 컴퓨터소프트웨어학과 학생, [3]호서대학교 혁신융합학부 교수

Implementation of Secure Keypads based on Tetris-Form Protection for Touch Position in the Fintech

Hyung-Jin Mun[1], Sin-Young Kang[2], ChwaCheol Shin[3*]
[1]Professor, Dept. of Information & Communication Engineering, Sungkyul University
[2]Student, Dept. of Computer Software, Hoseo University
[3]Professor, Dept. of Innovation & Convergence, Hoseo University

요 약 핀테크 서비스에서 금융거래시 사용자 인증하는 절차는 필수적이다. 특히, 스마트 폰에서의 인증은 터치 스크린 상의 가상 키패드를 통해 PIN을 입력받아 수행한다. 공격자가 PIN 입력 과정을 어깨너머로 훔쳐보기로 터치한 문자와 터치위치를 활용하여 패스워드를 유추하거나 높은 해상도 카메라 등으로 녹화하여 터치한 문자를 알아내어 패스워드를 유출할 수 있다. 패스워드 유출을 차단하기 위해 다양한 기법의 가상 키패드에 대한 연구가 진행되고 있다. 한편 편리성을 높이는 동시에 변동적인 키패드로 안전성이 보장되는 보안 키패드를 설계하는 것은 쉽지 않다. 또한 사용자가 터치한 패스워드가 잘못되었는지 확인을 위해 사용자에게 입력된 정보를 보여주기 때문에 고해상도 카메라 및 구글 글래스 등으로 녹화시 패스워드가 쉽게 노출된다. 본 논문에서는 QWERTY기반 보안 키패드에 대한 장단점을 분석하였다. 이를 통해 테트리스 모양의 키패드를 생성하고, 이어 붙이는 보안 키패드를 안드로이드 환경에서 구현하고, 입력된 문자를 스마트 화면에 테트리스 모양으로 사용자에게 보여줌으로서 녹화로 인한 패스워드 노출을 차단할 수 있다.

주제어 : 보안 키패드, 어깨너머공격, 사용자 인증, 가상 키패드, 테트리스, 핀테크 보안

Abstract User-authentication process is necessary in Fintech Service. Especially, authentication on smartphones are carried out through PIN which is inputted through virtual keypads on touch screen. Attacker can analogize password by watching touched letter and position over the shoulder or using high definition cameras. To prevent password spill, various research of virtual keypad techniques are ongoing. It is hard to design secure keypad which assures safety by fluctuative keypad and enhance convenience at once. Also, to reconfirm user whether password is wrongly pressed, the inputted information is shown on screen. This makes the password easily exposed through high definition cameras or Google Class during recording. This research analyzed QWERTY based secure keypad's merits and demerits. And through these features, creating Tetris shaped keypad and piece them together on Android environment, and showing inputted words as Tetris shape to users through smart-screen is suggested for the ways to prevent password spill by recording.

Key Words : Secure Keypads, Shoulder Surfing Attack, Authentication, Virtual Keypads, Tetris, Fintech Security

*Corresponding Author : ChwaCheol Shin(ccshin@hoseo.edu)
Received July 16, 2020
Revised August 6, 2020
Accepted August 20, 2020
Published August 28, 2020

1. 서론

ICT 발달로 인해 스마트 폰을 통한 다양한 서비스가 가능하다. 스마트 폰은 항상 전원이 켜져 있고, 정보 출력의 크기가 작고 입력의 불편함으로 인해 PC보다 더 많은 위험에 노출되고 있다. 특히, 스마트폰을 이용한 금융 결제의 활성화로 PC상의 공격들이 스마트폰으로 옮겨지면서 다양한 공격이 가능해지고, 직접적인 피해가 급증하고 있다[1]. SNS 관계망을 이용한 피싱, 파밍, 스미싱, 어깨너머 공격(Shoulder surfing attack)과 같은 사회공학적 공격이 급증하고 있다[2-5].

카메라 및 GPS 등 하드웨어가 내장된 스마트폰의 사양이 높아지고, 빠른 인터넷과 휴대성이 있고, 다양한 인증 방법의 제공됨에 따라 PC환경에서 이루어지는 스파이웨어를 이용한 바이러스 감염, 불법 파일로 인한 멜웨어 설치, 키로깅(Keylogging) 공격 등 다양한 공격들이 가능하고, 확장되어 가고 있다[6]. 스마트폰을 이용한 금융거래 등에서 안전한 거래를 위해 생체인증을 활용한 FIDO(Fast Identity Online) 기술이 활용되고 있다[7-9]. FIDO 기술은 신속한 온라인 인증이라는 뜻으로 온라인 환경에서 ID 인증 없이 생체인증을 활용하여 편리하고 안전하게 사용자 인증하는 기술이다[9]. 지문, 홍채 등 신체적 특성의 생체정보뿐만 아니라 동작 등의 행동적 특성의 생체정보 인증도 가능하다. 인터넷 뱅킹 등에서 인증을 위해 PIN이나 보안카드번호의 안전한 입력을 위해 보안 키패드를 이용하고 있다. PC 뿐만 아니라 스마트폰에서도 같은 방식의 보안 키패드로 서비스를 제공하고 있다[10,11].

몰래 엿보는 어깨너머 공격이나 카메라로 사용자의 입력하는 손동작을 촬영하여 직접 엿보는 공격을 통해 사용자의 중요한 입력정보를 유추할 수 있다[5,12,13]. 문자 가독성은 거리와 글자 크기에 따라 결정되지만 고해상도 촬영이 가능한 카메라를 가진 안경이나 스마트폰 등을 이용하여 사무실이나 사람이 붐비는 커피숍, 공항 등에서 스마트 폰과 같은 단말기를 이용하여 입력하는 정보를 상당한 거리에서도 몰래 엿볼 수 있다[5]. 탈취된 공인인증서의 비밀번호나 스마트 폰을 이용한 뱅킹, 모바일 간편 결제 등 금융 거래시 패스워드를 탈취하기 위해 키로거(Keylogger)를 이용하여 사용자의 터치 위치(좌표 값)이 노출되고 보안 키패드에 입력되는 비밀정보의 탈취가 가능하다[14,15]. 터치하는 위치를 통해 입력하는 패스워드를 유추할 수 있고 특히, 키패드의 양 측면을 터치할 경우 패스워드 노출이 높아진다.

고해상도를 가진 카메라로 패스워드를 입력하거나 터치하는 것을 녹화하여 훔쳐보는 공격을 차단하는 연구가 진행되고 있다. 하지만 스마트폰의 크기가 작아 입력에 어려움이 있는 것을 고려한 보안 키패드에 대한 연구가 부족하다.

본 연구는 다음과 같이 구성한다. 2장에서는 스마트폰과 같이 터치 위치 기반 공격에 대응하는 보안 키패드에 대한 연구를 소개하고, 3장은 테트리스 모양을 가지는 보안 키패드 설계 및 구현을 제시하고, 4장에서는 의사코드를 제시하고, 제안 기법의 편리성 및 안전성에 대한 분석 및 평가를 한 뒤 5장에서 결론을 맺는다.

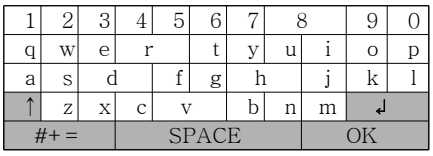
2. 관련 연구

2.1 QWERTY 가상 키패드

QWERTY 키패드는 PC 기반 키보드 자판에 익숙한 사용자에게 편리성을 주기 위해 키패드의 위치가 동일하고, 각 줄마다 한 칸이나 두 칸의 공간이 확보하여 한 칸이나 반 칸으로 임의의 위치에 배치하여 자판을 생성한다. Fig. 1은 네 줄로 구성된 가상 키패드이고, 키패드 위치가 고정을 막기 위해 한 칸 또는 반 칸의 공백을 임의의 위치에 배치한 보안 키패드의 예시이다. 첫줄에는 1부터 0까지의 10개의 숫자를 배치하고, 두 번째 줄에는 q로부터 시작하여 p까지의 10개의 로마자를 배치하고, 세 번째는 a를, 네 번째는 z를 배치하고 있다. 첫 번째와 두 번째 줄은 10개의 키패드를 사용하므로 공백 한 개를 한 곳에 배치하거나 반 칸을 두 군데에 배치한다. 왼쪽이나 오른쪽에 배치될 확률은 $\frac{1}{11}$이지만 중간에 배치될 경우 다른 키패드의 위치에 영향을 많아 미치기 때문에 대체로 왼쪽과 오른쪽에 공백이 배치될 가능성은 적다. 넷째 줄은 7개의 로마자를 배치하지만 왼쪽과 오른쪽 제어키를 배치하고, 한 칸의 공백을 사용한다. Fig. 1(b)는 (a)의 키패드에서 공백을 없애고, 옆에 있는 키패드를 합치는 형태로 생성된 보안 키패드이다.

1	2	3	4	5	6	7	8		9	0
q	w	e	r		t	y	u	i	o	p
a	s		d	f	g		h	j	k	l
↑	z	x	c		v	b	n	m	↵	
#+ =			SPACE					OK		

(a) Simple Secure Keypads



(b) Secure Keypads having no empty

Fig. 1. Example of QWERTY Secure Keypads

2.2 위치 공격을 이용한 패스워드 유추

스마트 폰의 가상 키패드가 QWERTY 자판일 경우 Fig. 2와 같이 첫 번째 줄은 "1"부터 "0"까지 10개의 숫자로 순서대로 배치한다. 맨 왼쪽에는 "1"이라는 숫자만 출력된다. 맨 오른쪽을 터치했다면 반드시 그 문자는 "0"이다. 만약 오른쪽에서 두 번째 열을 터치했다면 "9" 또는 "0"일 것이다. 숫자가 표시된 첫줄은 공백("_")이 한 개 뿐이므로 키패드의 오른쪽은 "~_90", "~9_0", "~890", "~90_"으로 4가지 경우 뿐이다. "12345678_90"의 경우는 나머지가 고정이라 1가지 경우만 존재한다. "~890"는 공백("_")의 위치가 변경되기 때문에 8가지이고, "1234567890_"의 경우는 고정되어 1가지이다. "~9_0"는 공백이므로 터치할 이유가 없다. 3번째 나올 수 있는 경우는 공백(_)이나 [2],[3] 뿐이다. QWERTY 키패드에서 맨 왼쪽과 오른쪽에 있는 키패드(1, q, a, z, 0, p, l, m) 뿐이므로 터치시 100% 확률로 유추가 가능하다[5,16,17]

location	1	2	3	4	5	6	7	8	9	10	11
number of cases	_ [1]	_ [1] [2]	_ [2] [3]	_ [3] [4]	_ [4] [5]	_ [5] [6]	_ [6] [7]	_ [7] [8]	_ [8] [9]	_ [9] [0]	_ [0]

Fig. 2. Case that is possible to be touchable in the first row

2.3 위치 노출 회피에 강한 보안 키패드

2.3.1 열기준 상하 이동 보안키패드

Fig. 3는 Lee[18]이 제안한 기법으로 각 줄마다 공백을 추가한 QWERTY 키패드를 생성한 후, 각 열마다 상단에 임의의 크기의 공백을 추가하는 키패드를 생성한다[18]. "1"의 경우 상단에 작은 폭을 가진 공백을, 숫자가 배치되지 않는 "y"열이 있다. "y"의 경우 상단에 가장 큰 폭을 가진 공백을 배치한 모습이다. 이 보안 키패드는 QWERTY 키패드와 비슷하게 배치되어 패스워드 입력시 편리성은 비슷하지만 터치한 위치를 통한 공격은 QWERTY 키패드처럼 안전성이 확보되지 않는다.

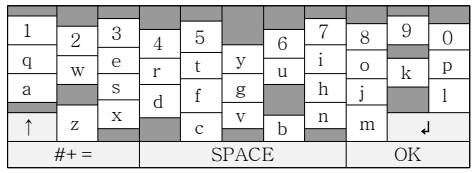


Fig. 3. Ripple type Keypads

2.3.2 열기준 상하 교환 보안키패드

Fig. 4는 Pak[19]이 제안한 기법으로 QWERTY 키패드인 Fig. 1에서 각 열의 키패드를 랜덤하게 재배치하는 키패드이다[19,20]. PC기반 키보드 자판들이 랜덤하게 배치되어 문자를 찾기도 어려워 패스워드 입력이 쉽지 않다.

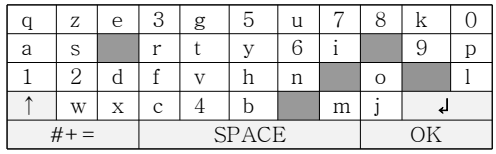


Fig. 4. Keypads exchanged based on column

2.3.3 행기준 복사 보안키패드

Fig. 5는 Lee[18]이 제안한 기법으로 QWERTY 키패드인 Fig. 1에서 네 개의 줄에서 임의의 한 개의 줄을 선택하여 상단에 복사하여 추가한 보안 키패드이다[18]. QWERTY 키패드과 비슷하여 키패드를 찾기 쉽고 중복된 줄이 있어 해당 줄의 문자일 경우 위치 공격에 상대적으로 안전하지만 하나의 행이 더 생기므로 키패드의 세로길이가 작아져서 패스워드를 터치하기 어렵다.

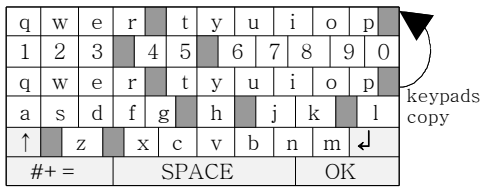


Fig. 5. Clone Keypads

2.3.4 시작위치 변경 보안키패드

Fig. 6는 Seo[13]이 제안한 기법으로 QWERTY 키패드를 기반으로 서화정이 제안한 보안 키패드이다. Fig. 6에서 보듯이 "1"의 위치를 두 번째 줄 세 번째 열에 배치할 수 있다. 즉, 시작점인 "1"의 위치를 변경한 QWERTY 키패드이다. 임의의 위치에 "1"를 배치하고,

순서대로 나열하는 보안 키패드이다. 사용자는 패스워드를 입력하기 위해서는 “1”의 위치를 찾고, “1”를 기준으로 PC 자판 전체를 암기해야 원하는 문자를 쉽게 찾을 수 있기 때문에 다른 보안 키패드보다 원하는 문자를 찾기 어렵다[13]. Fig. 6는 가독성을 위해 QWERTY 키패드의 기존 줄을 각기 다른 색으로 표시한 모습이다. 터치한 위치가 바뀌기 때문에 위치에 의한 공격에는 안전하지만 QWERTY 자판의 모든 문자의 배열에 익숙하지 않을 경우 패스워드 입력 편리성은 떨어진다.

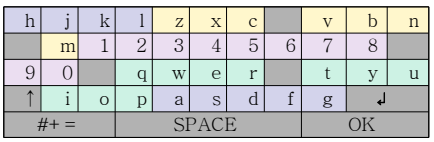


Fig. 6. Seo's Keypads

2.3.5 이중 터치기반 숫자 보안 키패드

Brute force attack, 키로킹 공격, 어깨너머 공격 등에 취약점을 해결하기 위해 키패드 마다 각각 2개의 숫자(n/M)로 이루어진 멀티 터치 키패드이다. 키패드는 2개의 숫자를 하나의 키패드에 배치하되, 왼쪽은 작은 크기로, 오른쪽은 큰 크기의 숫자가 표시된다. 키패드를 1초 이상 클릭할 경우 왼쪽 숫자가 입력되고 1초 미만 클릭할 경우 오른쪽 숫자가 입력된다. 숫자만을 입력하는 보안 키패드로 문자를 입력할 수 없다[21].

3/5	1/4	5/7
2/1	4/9	7/6
6/8	8/2	0/3
	9/0	OK

Fig. 7. Double Touch Number Keypads

2.4 어깨 너머 공격 회피 기법

스마트 폰의 디스플레이의 크기가 작아 사용자가 터치하는 과정에서 오타입력이 발생한다. 잘못 입력했는지 확인하기 위해 보안 키패드는 사용자가 입력된 마지막 문자를 보여주고, 그 다음에는 해당 문자를 *로 표시된다. 하지만 어깨너머로 훔쳐볼 경우 마지막 입력된 문자를 볼 수 있기 때문에 터치한 위치를 알 필요 없이 패스워드를 알 수 있다. 특히, 해상도가 높은 카메라 기능을 가진 스마트 폰이나 구글 글래스를 이용하여 녹화할 경우 위치공격과 상관없이 패스워드를 알아낼 수 있다.

2.4.1 Four Color Theorem를 이용한 회피기법

사용자가 로마자 “s”를 입력할 때 s 주변의 w, a, z, d 키패드를 터치할 가능성이 있다. 오타 입력 여부를 확인하기 위해 키패드마다 4개의 색으로 표시하여 터치시 터치된 키패드의 색을 출력하여 잘못 터치여부를 확인하는 기법이다. 주변의 키패드에 4개의 색을 표시하면 전체 키패드를 표현할 수 있어 색으로 터치한 문자를 색으로 대신 확인할 수 있다[22]. 입력한 문자 주변에 최대 8개의 키가 존재할 수 있다. 즉, 대각선의 키패드를 터치할 가능성이 있다.

2.4.2 저장된 정보와 비교하는 입력정보 확인기법

Seo[4]이 제안한 마지막 터치 정보 확인방법으로 사용자가 패스워드를 입력하는 과정에서는 입력된 숫자나 문자를 *로 표시되고, 보안 키패드로 패스워드를 입력을 완료한 후 패스워드를 암호화하여 데이터베이스에 저장된 정보와 비교하여 맞으면 정확하게 입력되었음을 알리는 메시지를 출력하는 방식이다[4]. 디스플레이를 통해 입력하는 과정에서의 패스워드를 노출하지 않는다는 장점을 가진다. 하지만 입력된 문자가 틀린 경우 어디에서 틀렸는지 확인이 어렵고, 전체를 다시 입력해야 하는 번거로움이 있다. 말기에 저장된 패스워드 암호문에 대한 보호 장치를 고려해야 한다. 즉, 공격자가 데이터베이스를 삭제할 경우 이 기법을 전형 사용할 수 없다.

3. 테트리스 모양의 보안 키패드

테트리스 모양으로 가상 키패드를 생성하여 QWERTY 기반의 배치한 보안 키패드이다[20]. QWERTY 자판의 키패드를 기준으로 가로 세로 이등분하여 Fig. 8와 같이 13개의 테트리스 모양의 키패드를 설계하고, 각 키패드를 1차원 배열로 표기하였다. [17,23].

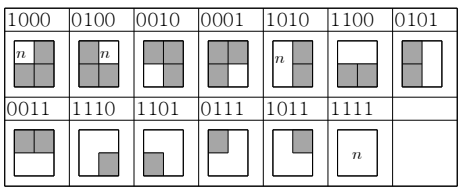


Fig. 8. Tetris Pattern

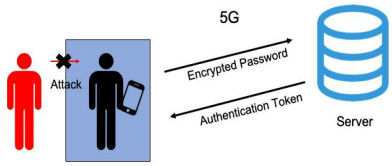


Fig. 9. System Structure Diagram

Fig. 9는 핀테크 환경에서 스마트을 통해 자신의 PIN을 안전하게 입력하는 과정을 나타낸 것이다. 제안 기법의 시스템 구조도이다. Fig. 10는 13개 테트리스 모양의 키패드를 에뮬레이터 화면와 실제를 배치한 보안키패드의 예시이다.

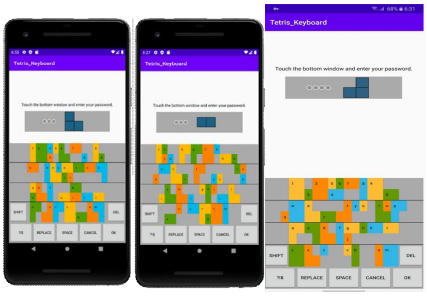
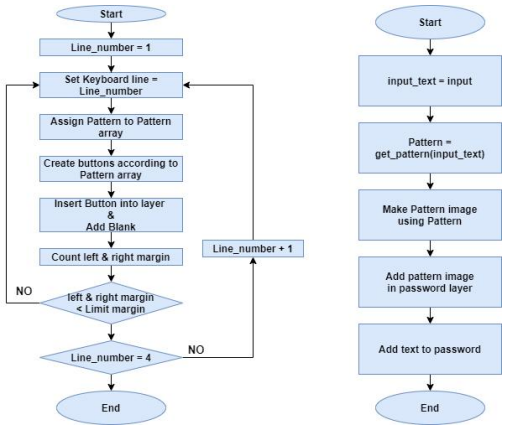


Fig. 10. Example of Secure Keypads with Tetris-Form

Fig. 11(a)는 키보드의 각 라인별로 랜덤하게 테트리스 모양의 키패드를 생성하여 키패드를 레이아웃에 배치하여 테트리스 모양의 보안키패드를 구현하는 순서도이다. Fig. 11(b) 는 구현된 보안 키패드 APP에서 사용자가 패스워드를 터치할 때 일어나는 이벤트에 대한 순서도이다.



(a) Generation of Keypads (b) User Touch Event

Fig. 11. Proposed Sequence Diagram

4. 구현 및 평가

4.1 구현 환경 및 의사코드

테트리스 모양의 보안키패드는 Android Studio 4.0(SDK 29) 환경에서 Java8을 이용하여 개발하였다. 테스트 스마트폰의 운영체제는 Android 10이 설치된 Samsung galaxy A90 5G에서 구동 및 테스트를 실시하였다. Fig. 12는 테트리스 모양의 보안 키패드를 구현한 의사코드이다.

```
Ⅰ. Set the basic settings and place the layers and buttons.
Ⅱ. for( Line = 0 ; Line < Max_Keyboard_Line ; Line++){
  for(sequence = 0 ; key_count[Line] ; sequence++){
    ①pattern_arr[Line][sequence] = make_pattern();
  }
   ② button_arr = make_button(pattern_arr);
   ③ add_buttons_in_layer(button_arr[Line], Line);
            ③-1 if(button_class[Line] == 0){
                    join_tetris_key(key);
            }
            ③-2 else if(button_class[Line] == 1){
                    stack_tetris_key(key)
            }
   ④ margin = get_margin_length(Line);
  if( margin < Limit_margin ){
    goto for
  }
}
Ⅲ. onClick_keyboard_Button(){
    passwd = passwd + bt.getText();
    pattern = get_pattern_of_keyboard(bt.getText());
    ⑤ display_tetris_form(pattern);
  }
Ⅳ. onClick_confirm{
    password_hash = to_hash_String(passwd);
    send_to_server(password_hash);
  }
```

Fig. 12. Pseudo-code for Tetris-Form Keypads

①은 pattern_arr()에 랜덤한 패턴을 할당한다. 이 패턴은 ②에서 패턴의 모양을 가진 버튼으로 만들어져 버튼리스트에 저장된다. ③에서 만들어진 버튼들을 레이어에 할당을 하며 ③-1,③-2처럼 패턴의 속성을 지정하여 만약 속성 값이 0이라면 다른 버튼과 맞물려지지 않는 버튼을 레이어에 할당하여 빈칸을 만들 수 있도록 하고 속성 값이 1이라면 다른 버튼과 맞물려지는 버튼

을 레이어에 할당하여 쌓일 수 있도록 한다. ④에서는 좌우에 생기는 빈칸의 크기가 키패드의 $\frac{1}{2}$만큼 왼쪽과 오른쪽의 여백의 합이 키패드 크기의 $\frac{3}{2}$보다 작을 경우 해당 줄을 다시 반복한다. Ⅲ과 Ⅳ는 키패드를 터치할 경우 실행되는 코드로써 Ⅲ은 문자가 있는 키패드를 터치할 경우 실행된다. Ⅳ은 패스워드의 입력이 완료되었을 때 확인키패드 터치시 실행되는 부분으로 패스워드의 해시 값이 서버로 전달된다.

4.2 터치위치공격에 대한 안전성 분석

어깨너머공격이나 카메라 녹화 등에 의한 공격을 막기 위해 QWERTY 키패드를 다양한 형태로 제시되고 있다. 하지만 터치할 패스워드를 찾는 시간이 늘어남에 따라 입력 편리성이 떨어진다는 단점이 있다. 테트리스 모양의 배치될 경우 이어붙이기가 가능하여 확보된 추가 공간을 공백으로 활용하므로 터치 위치 공격에 안전하고(Fig. 13), 터치된 마지막 문자 대신에 테트리스 모양을 화면에 보여주어 녹화를 통한 마지막 터치 문자를 확인하는 공격을 막아 패스워드를 유추가능성을 낮출 수 있다.

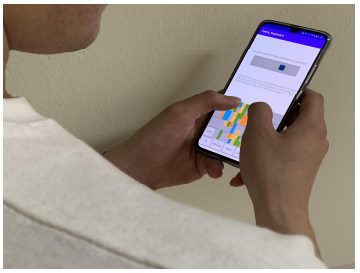


Fig. 13. Shoulder Surfing Attack

4.3 제안 기법에 대한 평가 및 분석

테트리스 모양의 키패드를 이어 붙여 공간을 확보할 수 있어 문자 간에 여백을 많이 줄 수 있기 때문에 위치에 대한 보안 안전성을 높일 수 있지만 기존 키패드보다 최대 1/4로 작아지기 때문에 문자를 터치하는데 어려움이 있다[24]. 크기가 작은 터치 스크린에서의 보안 키패드는 2가지 측면을 고려해야 한다. 패스워드 입력 시 사용자의 편리성을 높이기 위해 키패드의 위치를 쉽게 찾을 수 있어야 한다. 패스워드 입력하는 시간을 단축하면 어깨 너머 공격 등 훔쳐보기를 차단하는 효과를 가진다. 둘째로 공격자가 훔쳐보기 등으로 터치 위치를 탈취할 수 있는 환경이라면 키패드의 위치를 고정되지 않아서 패스워드 유추를 어렵게 해야 한다.

4.4 입력 편리성 및 시간 측면 비교분석

Fig. 14는 가장 많이 사용되는 패스워드(password1, iloveyou, qwerty123, abc123, 1q2w3e4r)를 가지고 10회씩 입력을 했을 때 걸리는 시간의 평균을 정리한 표이다. 제안 키패드과 기존 은행의 보안키패드를 사용하였을 때를 비교했을 때 입력 시간이 약간의 차이만 있다.

	Tetris keypads	QWERTY Keypads
A	4.718	4.643
B	4.357	4.548
C	4.251	3.636
D	4.034	3.358
E	4.664	3.426
AVG	4.40	3.92

Fig. 14. Comparison Analysis of Input Time

	Tetris keypads	QWERTY Keypads
A	1	0
B	1	0
C	0	1
D	0	0
E	2	1
AVG	0.80	0.40

Fig. 15. Comparison Analysis of Touch Error

Fig. 15는 패스워드를 10회 입력할 때 잘못 터치한 횟수를 비교한 것이다. 패스워드 1q2w3e4r를 10번 터치했을 때 제안 기법은 2회, 기존 기법은 1회 잘못 터치하였다. Fig. 15에서 보듯이 기존 기법과 비교했을때 큰 차이가 없음을 알 수 있다.

5. 결론

모바일 단말기 이용 급증으로 인해 다양한 서비스가 가능해졌다. 핀테크 환경에서는 금융거래시 인증하는 시스템이 보편화되고 있다[25].

인증과정 PC 뿐만 아니라 스마트폰에서 보안키패드를 이용하여 안전한 PIN 입력을 받아 서버에 비밀정보를 전달하고 있다. 스마트 폰을 이용한 보안키패드를 적용하면서 터치 기반의 입력과정에서 다양한 공격이 가능한 취약점이 발생하고 있다. 패스워드 입력시 근처에서 어깨너머로 훔쳐보거나 키로거 등으로 터치위치를

탈취하여 비밀정보 유추가 가능하다. 해상도 높은 카메라로 녹화하거나 구글 글래스를 이용할 경우 3m 이내의 사용자가 입력한 정보를 확인할 수 있다.

제안 기법은 테트리스 모양의 키패드로 배열하여 이어붙이기를 통해 공간을 확보되어 임의의 위치에 공백을 배치하므로 훔쳐보거나 터치위치공격에 안전성을 확보할 수 있다. 또한 마지막 터치 문자를 확인하는 것 대신에 테트리스 모양을 제시하므로써 촬영을 통해 패스워드 유출가능성을 차단할 수 있다. 테트리스 모양의 키패드가 이어 붙을 경우 원하는 문자 터치가 기존 방식보다 어려움이 존재한다. 향후 연구로는 가로형태로 좌우 회전하여 보안 키패드의 크기를 터치하기 쉽게 크기를 확대하거나 터치시 오류를 줄일 수 있는 기법 연구가 필요하다.

REFERENCES

[1] C. Nayak, M. Parhi & S. Ghosal.(2014). Robust virtual keyboard for online banking. *International Journal of Computer Applications, 107(21),* 36-38. DOI : 10.5120/19142-0530

[2] K. H. Choi, K. Y. Chung & D. K. Shin (2016). A Study of Prevention Model the Spread of Phishing Attack for Protection the Medical Information. *Journal of digital Convergence, 11(3),* 273-277. DOI : 10.14400/JDPM.2013.11.3.273

[3] B. S. Yu & S. H. Yun. (2011). The Design and Implementation of Messenger Authentication Protocol to Prevent Smartphone Phishing. *Journal of the Korea Convergence Society, 2(4),* 9-14. DOI : 10.15207/JKCS.2011.2.4.009

[4] H. J. Seo & H. W. Kim. (2014). Secure Keypad with Encrypted Input Message. *Journal of the Korea Institute of Information and Communication Engineering, 18(12),* 2899-2910. DOI : 10.6109/jkiice.2014.18.12.2899

[5] S. H. Kim, M. S. Park & S. J. Kim. (2014). Shoulder Surfing Attack Modeling and Security Analysis on Commercial Keypad Schemes. *Journal of the Korea Institute of Information Security & Cryptology, 24(6),* 1159-1174. DOI : 10.13089/JKIISC.2014.24.6.1159

[6] D. R. Kim & K. H. Han. (2013). A Study on Multi-Media Contents Security using Smart Phone. *Journal of digital Convergence, 11(11),* 675-682. DOI : 10.14400/JDPM.2013.11.11.675

[7] S. W. Choi & Y. J. Shin. (2015). Economy Effects of IT Industry on Financial and Insurance Services. *Journal of digital Convergence, 13(1),* 191-203. DOI : 10.14400/JDC.2015.13.1.191

[8] D. R. Kim. (2015). A Study on the OTP Generation Algorithm for User Authentication. *Journal of the Korea Convergence Society, 13(1),* 283-288.

[9] C. J. Chae, H. J. Cho & H.M. Jung. (2018). Authentication Method using Multiple Biometric Information in FIDO Environment. *Journal of Digital Convergence, 16(1),* 159-164. DOI : 10.14400/JDC.2018.16.1.159

[10] S. H. Lee & D. W. Lee.(2015). FinTech-Conversions of Finance Industry based on ICT. *Journal of the Korea Convergence Society, 6(3),* 97-102. DOI : 10.15207/JKCS.2015.6.3.097

[11] S. H. Hong, S. H. Park & Noe Lopez-Benitez (2017). Trends and Implications of Mobile and Online FinTech. *International Journal of Emerging Multidisciplinary Research, 1(1),* 43-47. DOI : 10.22662/IJEMR.2017.1.1.043.

[12] Q. Yue, Z. Ling, X. Fu, B. Liu, W. Yu & W. Zhao. (2014). *My google glass sees your passwords!. Proceedings of the Black Hat USA,* https://www.blackhat.com/docs/us-14/materials/us-14-Fu-My-Google-Glass-Sees-Your-Passwords.pdf

[13] H. J. Seo & H. W. Kim. (2016). Design of Security Keypad Against Key Stroke Inference Attack. *Journal of the Korea Institute of Information Security & Cryptology, 26(1),* 41-47. DOI : 10.13089/JKIISC.2016.26.1.41

[14] Y. H. Lee. (2013). An Analysis on the Vulnerability of Secure Keypads for Mobile Devices. *The Journal of Internet Computing and Services, 14(3),* 15-21. DOI : 10.7472/jksii.2013.14.3.15

[15] J. S. Song, M. W. Chung, S. H. Seo & S. H. Lee. (2015). Security vulnerability analysis of Simple Mobile Payments Services. *The Korea Information Processing Society Fall Conference, 22(2),* 817-820.

[16] Y. H. Lee. (2013). An Analysis on the Vulnerability of Secure Keypads for Mobile Devices. *Journal of Korean Society for Internet Information, 14(3),* 15-21.

[17] H. J. Mun. (2017). Virtual Keypads based on Tetris with Resistance for Attack using Location

Information. *Journal of the Korea Convergence Society, 8(6),* 37-44.
DOI : 10.15207/JKCS.2017.8.6.037

[18] D. H. Lee, D. H. Bae, S. L Yoo, J. Y. Chae, Y. Lee & H. G. Yang. (2011). Analysis of safety in secure keypads for smartphone. *REVIEW of The Korea Institute of Information Security and Cryptology, 21(7),* 30-37.
DOI : KIISC.2011.21.7.30.

[19] W.G. Pak, S. Yeo & Y.R. Cha. (2015). A Secure Virtual Keypad for Mobile devices. *Proceeding of KOREA INFORMATION SCIENCE SOCIETY,* 875-876.

[20] D. Tak & D. Choi. (2016). Password Guessing Attack Resistant Circular Keypad for Smart Devices. *Journal of Korea Multimedia Society, 19(8),* 1395-1403.
DOI : 10.9717/kmms.2016.19.8.1395

[21] J. Song, M. Jung, J. Choi & S. Seo. (2018). Proposal and Implementation of Security Keypad with Dual Touch. *KIPS Transactions on Computer and Communication Systems, 7(3),* 73-80.
DOI : 10.3745/KTCCS.2018.7.3.73

[22] H. J. Kim, H. J. Seo, Y. C. Lee, T. H. Park & H.W. Kim(2013). Implementation of virtual finace keypads with resistance for shoulder surfing attack. *REVIEW The Korea Institute of Information Security and Cryptology(KIISC), 23(6),* 21-29.
DOI : KIISC.2013.23.6.21.

[23] K. An, H. Kwon, Y. Kwon & H. Seo.(2019). Security Implementation using Flexible Keypad. *Journal of the Korea Institute of Information and Communication Engineering, 23(5),* 613-621.
DOI : 10.6109/JKIICE.2019.23.5.613

[24] H. J. Mun & K. H. Han. (2018). Tetris security keypads design with higher security using alignment and padding. *International Journal of Engineering & Technology, 7(2.33),* 11-14.
DOI : 10.14419/ijet.v7i2.33.13838

[25] Y. M. Kang, Y. G. Lee, H. J. Kwon, K. S. Han & H. S. Chung. (2016). A Study on the Information Security System of Fin-Tech Business. *Journal of IT Convergence Society for SMB, 6(2),* 19-24.

문 형 진(Hyung-Jin Mun) [종신회원]

· 1996년 2월 : 충남대학교 수학과 (이학사)
· 2008년 2월 : 충북대학교 전자계산학(이학박사)
· 2009년 3월 ~ 2012년 8월 : 중국 연변과학기술대학교 컴퓨터전자통신학부 조교수, 부교수
· 2017년 3월 ~ 현재 : 성결대학교 정보통신공학부 조교수
· 관심분야 : 정보보호, 핀테크 보안, 사용자 인증
· E-Mail : jinmun@gmail.com

강 신 영(Sin-Young Kang) [학생회원]

· 2016년 3월 ~ 2020년 2월 : 호서대학교 컴퓨터 소프트웨어 학과
· 2020년 3월 ~ 현재 : 호서대학교 유비쿼터스 연구실 연구원
· 관심분야 : 인공지능, 분산처리 시스템, 임베디드시스템
· E-Mail : kangsy0058@naver.com

신 좌 철(ChwaCheol Shin) [정회원]

· 1990년 2월 : 호서대학교 전자계산학과
· 1996년 2월 : 호서대학교 전자계산학(이학석사)
· 2007년 8월 : 호서대학교 컴퓨터공학(공학박사)
· 2019년 3월 ~ 현재 : 호서대학교 혁신융합학부 조교수
· 관심분야 : 컴퓨팅 사고력, 교양교육, 인공지능 교육, S/W 활용 교육
· E-Mail : ccshin@hoseo.edu