Journal of The Korea Knowledge Information Technology Society

ISSN 1975-7700

http://www.kkits.or.kr

Randomized Keypad against Password Guessing Attacks with Motion Sensors

Iksu Kim[1], **Jongmyung Choi**[*2]

[1]*School of Computer Science and Engineering, SoongSil University*
[2]*Department of Computer Engineering, MokPo National University*

ABSTRACT

With the increase of smartphone users, smartphone users using the mobile banking services has increased significantly. For using the mobile banking services, users have to input their passwords in mobile banking App. According to recent studies, passwords inputted on a keypad could be inferred by using smartphone's built-in motion sensors. In this paper, we propose a randomized keypad against password guessing attacks with motion sensors. When users try to input their passwords, the proposed keypad displays the area of random arrangement on which users can input their passwords. Accordingly, the location information of touched keys is different whenever users input their passwords. Users can safely use the mobile banking service because it is impossible to infer the inputted passwords with motion sensors.

KEYWORDS: Secure keypads, Password guessing attack, Randomized keypads, Mobile, Motion sensors

ARTICLE INFO: Received 9 December 2013, Revised 17 January 2014, Accepted 14 February 2014.

1. 서 론

최근 스마트폰 사용자가 급증함에 따라 스마트폰을 이용한 모바일 뱅킹 서비스 이용자도 크게 증가하였다. 2013년 6월 현재 스마트폰을 통한 모바일 뱅킹 서비스 이용자수는 3131만 명에 이르렀으며, 일평균 이용금액도 1조 3934억 원에 달하고 있다[1]. 현재 스마트폰을 사용하여 모바일 뱅킹 서비스를 이용하기 위해서는 보안성 강화를 위한 공

[*]Corresponding author is with the Department of Computer Engineering, MokPo National University, 1666 Youngsan-ro Cheonggye-myeon Muan-gun Jeonnam, 534-729, KOREA.
E-mail address: jmchoi@mokpo.ac.kr

인인증서와 보안 카드를 함께 사용해야 한다. 이용자는 모바일 뱅킹 서비스를 이용할 때 공인인증서의 패스워드를 입력함으로써 자신임을 증명한다.

과거의 휴대폰과는 달리 스마트폰은 사용자가 원하는 앱을 설치하여 사용할 수 있다는 큰 장점을 가지고 있다. 하지만 이러한 장점의 이면에는 보안상 큰 위험성이 존재하고 있다. 문자메시지 혹은 웹 페이지의 링크를 클릭하여 다운로드한 앱에 모바일 악성코드가 포함된 경우 공인인증서의 패스워드가 유출될 수 있다. 모바일 악성코드는 2004년 처음 등장하였으며, 주로 심비안 운영체제가 탑재된 스마트폰을 공격 대상으로 하였다[2]. 최근 모바일 악성코드의 수는 다양한 모바일 운영체제의 등장과 함께 기하급수적으로 증가하였는데, 안랩에 따르면 2013년 1분기에 안드로이드 기반의 악성코드 샘플이 206,628개나 수집되었다고 한다[3].

[4-6]에서는 사용자가 스마트폰 상에서 패스워드를 입력할 때 스마트폰에 내장된 방향 센서와 가속도 센서 같은 모션 센서를 이용하여 디스플레이의 터치된 위치 정보를 통해 패스워드를 획득할 수 있음을 보였다. 현재 국내에서는 이러한 방법을 통해 패스워드가 노출되는 것을 막기 위해 공백을 임의의 위치에 추가하여 패스워드 추측을 어렵게 하는 보안 키패드가 사용되고 있다. 이 키패드는 패스워드 인증 과정에서 매번 각 행에 하나 이상의 공백을 임의의 위치에 배치하기 때문에 사용자가 패스워드 입력 시 터치하는 위치가 매번 다르다. 하지만 각 키가 특정 위치에 배치될 확률이 서로 다르기 때문에 여러 번의 패스워드 입력 시 수집된 위치 정보를 분석하면 실제 패스워드를 쉽게 알아낼 수 있다[7-8].

본 논문에서는 스마트폰에 내장된 모션 센서를 이용한 패스워드 추측 공격에 안전한 랜덤 키패드를 제안한다. 제안된 키패드는 사용자가 패스워드를 입력할 때, 키패드의 중앙에 랜덤한 배열의 키를 갖는 영역을 제공함으로써 패스워드 입력 시 터치하는 위치 정보를 매번 다르게 생성한다. 제안된 키패드에서 각 키가 특정 위치에 배치될 확률은 그룹별로 서로 같기 때문에 터치 위치 정보에 대한 분석을 통해 정확한 패스워드를 알아내는 것은 불가능하다.

2. 관련 연구

2.1 모션 센서를 이용한 패스워드 추측 공격

안드로이드 플랫폼에서 각 앱은 자신만의 가상 머신에서 실행된다. 만일 특정 앱이 또 다른 앱에서 생성되는 데이터를 읽기 위해서는 데이터 읽기를 허용하는 앱의 메니페스트 파일에 다른 앱의 접근 권한을 허용해야 한다. 따라서 특정 앱이 메니페스트 파일을 통해 접근 권한을 허용하지 않을 경우에는 해커의 데이터 접근이 불가능하다. 안드로이드 플랫폼에서 동작하는 모바일 뱅킹 앱의 경우에도 계좌번호나 비밀번호를 사용자가 입력할 때, 이 앱이 다른 앱의 접근을 허용하지 않는다면 사용자가 입력을 위해 터치한 키 값이나 키의 위치를 알 수 없다. 하지만 [5-6]에서는 안드로이드 스마트폰에 내장된 모션 센서 중에서 방향 센서와 가속도 센서가 생성하는 데이터를 이용한 공격 가능성을 제시하였다.

방향 센서는 스마트폰의 현재 방향과 기울기 값을 3차원의 x, y, z 값으로 측정하며, 가속도 센서는 현재 스마트폰이 어느 방향으로 얼마나 빠르게 움직이는지를 3차원의 값으로 측정하는 센서이다. 방향 센서와 가속도 센서를 이용한 패스워드 유추 공격의 원리는 사용자가 키패드 상의 터치 위치에 따라 x, y, z 값이 다르게 생성된다는 점을 착안한 것이다. 키패드의 각 버튼을 여러 번 터치했을 때

의 x, y, z값을 수집한 후, 이 정보를 토대로 사용자가 특정 키를 터치했을 때 어떠한 값을 입력했는지를 확률적으로 알아낼 수 있다. 방향 센서나 가속도 센서가 생성하는 데이터는 현재 안드로이드 환경에서 특별한 권한 부여 없이 모든 앱들이 사용할 수 있기 때문에 이를 이용한 패스워드 추측이 가능하다.

2.2 스마트폰용 보안 키패드

mTranskey는 현재 금융관련 앱에서 대표적으로 사용되는 보안 키패드이다[9].

그림 1. mTranskey
Figure 1. mTranskey

<그림 1>은 mTranskey가 적용된 앱이며, 공인인증서의 패스워드를 입력하기 위한 키패드가 기존 키패드와는 달리 공백이 삽입되어 있는 것을 알 수 있다. 키패드의 1행부터 3행에는 1열부터 11열의 임의의 위치에 공백이 삽입된다. 4행의 경우는 2열부터 9열의 임의의 위치에 공백이 삽입된다. 또한, 1, 2, 4행에는 공백이 하나씩 삽입되며, 3행은 2개의 공백이 삽입된다. mTranskey는 매 인증 시마다 <그림 1>과 같이 공백을 임의의 위치에 삽입하여 각 키들이 다른 위치에 배치된다. 그러므로 인증 시에 사용자가 패스워드를 입력하면 터치 위치가 매번 달라진다. 따라서 모션 센서는 패스워드 인증 시 마다 다른 값들을 생성하기 때문에 해커는 쉽게 패스워드를 알 수 없다.

[7]에서는 패스워드 노출을 막기 위해 물결형 키패드, 클론 키패드, 터치 & 슬라이드 키패드를 제시하였다. 물결형 키패드는 mTranskey와 같이 임의의 열에 공백을 추가한 후, 임의의 행에도 공백을 추가하여 패스워드 추측을 더욱 어렵게 하였다. 클론 키패드는 키패드의 특정 행을 또 다른 행에 더 추가한 키패드이다. 사용자는 원하는 키 값을 입력할 때 둘 중 하나의 행에 있는 키를 선택하여 입력할 수 있다. 따라서 같은 키 값을 입력하더라도 모션 센서는 다른 값을 생성하게 된다. 터치 & 슬라이드 키패드는 일부 키만을 화면에 출력하고 좌우 화살표 버튼을 통해 나머지 키들로 이동할 수 있도록 구현된 키패드이다. 사용자는 입력하고자 하는 키를 찾을 때까지 화살표 버튼을 눌러 이동한 후, 해당 키를 터치하여 패스워드를 입력한다. [10-11]에서 기술된 랜덤 키패드는 0부터 9까지의 숫자 키를 임의의 위치에 생성하기 때문에 모션 센서를 이용한 패스워드 추측 공격에 안전하다.

앞서 기술했듯이 mTranskey는 단순히 공백만을 추가하기 때문에 각 키가 특정 위치에 배치될 확률이 서로 다르다. 따라서 여러 번의 패스워드 입력 시 수집된 위치 정보를 분석하면 실제 패스워드가 쉽게 노출될 수 있다. 또한 한 행에 10개의 버튼과 공백을 배치해야하기 때문에 액정 크기가 작은 스마트폰에서 사용자가 손가락으로 입력하고자 하는 키를 터치할 때, 인접한 다른 키를 터치할 가능성이 높다. 물결형 키패드는 각 키들이 지그재그로 배치되기 때문에 터치해야 할 키를 찾기가 어렵고, 모션 센서를 통해 수집된 터치 정보가 충분히 많을 경우 패스워드 예측이 가능해진다. 그리고 클론 키패드는 사용자가 새로 추가된 행을 사용하지 않을 경우 여전히 모션 센서를 이용한 패스워드 추측 공격에 취약하다. 터치 & 슬라이드 키패드는 키가 알파

표 1. 키가 특정 위치에 배치될 확률
Table 1. Probability of keys to be placed in specific location

키	1열	2열	3열	4열	5열	6열	7열	8열	9열	10열	11열
'1', 'q'	90.91	9.09	0	0	0	0	0	0	0	0	0
'2', 'w'	0	81.82	18.18	0	0	0	0	0	0	0	0
'3', 'e'	0	0	72.73	27.27	0	0	0	0	0	0	0
'4', 'r'	0	0	0	63.64	36.36	0	0	0	0	0	0
'5', 't'	0	0	0	0	54.55	45.45	0	0	0	0	0
'6', 'y'	0	0	0	0	0	45.45	54.55	0	0	0	0
'7', 'u'	0	0	0	0	0	0	36.36	63.64	0	0	0
'8', 'i'	0	0	0	0	0	0	0	27.27	72.73	0	0
'9', 'o'	0	0	0	0	0	0	0	0	18.18	81.82	0
'0', 'p'	0	0	0	0	0	0	0	0	0	9.09	90.91

벳 순서로 배치되어 있어 화살표 버튼의 터치 수를 추적한다면 패스워드 유추가 가능해진다. 또한, 랜덤 키패드는 숫자 키로만 구성되어 있기 때문에 패스워드 설정 시 숫자를 제외한 다른 문자들을 사용할 수 없는 단점이 있다.

3. 제안하는 랜덤 키패드

본 장에서는 현재 모바일 뱅킹 앱에서 사용되고 있는 mTranskey의 안전성을 분석하고 모션 센서를 통한 패스워드 추측 공격에 안전한 랜덤 키패드를 기술한다.

3.1 mTranskey 안전성 분석

앞서 살펴본 mTranskey에서 1행 1열에 공백이 위치하는 경우 숫자키 1은 1행 2열에 배치된다. 그리고 공백이 1행 1열이 아닌 1행의 임의의 열에 배치될 경우에는 숫자키 1은 1행 1열에 배치된다. 따라서 숫자키 1이 1행 1열에 배치될 확률은 약 90.91%이며, 1행 2열에 배치될 확률은 9.09%이다.

표 2. 패스워드를 20회 입력한 결과
Table 2. Result of inputting a password 20 times

패스워드 입력 시도	9가 배치된 열	4가 배치된 열	7이 배치된 열	6이 배치된 열
1번째	10	5	8	7
2번째	10	4	7	6
3번째	10	4	7	6
4번째	10	5	8	7
5번째	10	5	8	7
6번째	10	5	8	7
7번째	10	4	7	6
8번째	10	5	8	7
9번째	9	4	7	6
10번째	10	5	8	7
11번째	10	4	8	7
12번째	10	4	8	7
13번째	10	4	8	6
14번째	10	4	8	7
15번째	9	4	7	6
16번째	9	4	7	6
17번째	10	4	8	6
18번째	10	4	7	6
19번째	10	4	8	6
20번째	10	5	8	7

<표 1>은 1행과 2행의 각 키들이 배치되는 위치와 배치 확률을 나타낸 것이며, <표 2>는 mTranskey에서 패스워드 9476을 실제로 20번 입력해 본 결과이다. 20번의 패스워드 입력 시 버튼

9는 1행 9열에서 15%, 1행 10열에서는 85% 출현하였다. 버튼 4의 경우에는 1행 4열에서 65%, 1행 5열에서 35% 출현하였으며, 버튼 7은 1행 7열에서 35%, 1행 8열에서 65% 출현하였다. <표 1>에 명시된 각 키의 배치 확률과 패스워드 입력 시 사용자가 터치하는 위치의 빈도수를 비교하면 해커는 입력된 패스워드의 처음 세 자리가 9, 4, 7이라는 것을 추측할 수 있다. 반면 20번의 패스워드 입력 시 버튼 6은 1행 6열과 1행 7열에 동일한 횟수로 배치되었기 때문에 20번의 패스워드 입력 결과를 통해 패스워드의 네 번째 자리를 추측할 수는 없다. 하지만 더 많은 패스워드 입력을 관찰한다면 <표 1>을 통해 패스워드의 네 번째 자리를 알 수 있다.

3.2 랜덤 키패드 구현

패스워드를 생성할 때에는 보안상의 이유로 패스워드 길이를 최소 8자리 이상으로 설정하도록 권고하고 있으며, 현재 공인인증서의 패스워드 역시 8자리 이상으로 설정해야 한다. 또한, 공인인증서를 통한 인증 시 해커의 불법적인 접근 시도를 막기 위해 3회 이상 패스워드 입력에 실패하면 서비스 이용을 차단하고 있다. 그러므로 해커는 최소 길이가 8자리인 패스워드를 3번안에 올바르게 입력해야만 공격에 성공할 수 있다. mTranskey의 취약점은 패스워드 인증과정에서 각 키가 특정 위치에 서로 다른 확률로 배치된다는 데에서 기인한다. 따라서 모션 센서가 생성하는 정보를 이용하는 악성 앱은 mTranskey를 통해 입력되는 패스워드를 쉽게 알아낼 수 있다. 이러한 공격에 안전한 키패드는 패스워드 입력 시, 터치되는 키의 위치가 수시로 달라져야 한다. <그림 2>는 제안된 랜덤 키패드의 초기화면을 나타낸다.

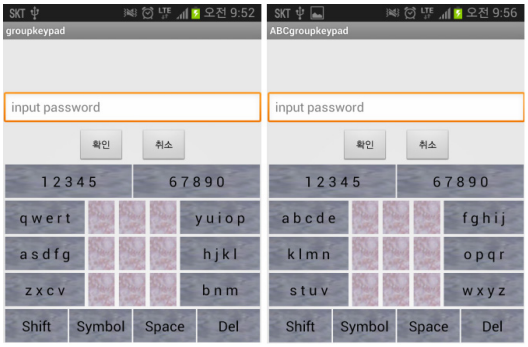

그림 2. 제안된 키패드
Figure 2. Proposed keypad

사용자의 편의를 위해 랜덤 키패드는 QWERTY 방식과 ABC 방식으로 패스워드를 입력할 수 있다. 기존 키패드와의 차이는 각 키들이 개별 버튼으로 존재하지 않고 좌측과 우측으로 그룹화 되어 있다. 즉, 기존의 QWERTY 키패드에서 2행의 'q', 'w', 'e', 'r', 't' 키들은 좌측에 하나의 그룹버튼으로 통합되어 있으며, 'y', 'u', 'i', 'o', 'p' 키들은 우측에 하나의 그룹버튼으로 통합되어 있다. 그러므로 사용자가 만일 'q', 'w', 'e', 'r', 't' 중 하나를 입력할 경우에는 2행 1열에 배치된 'qwert' 버튼을 누르며, 'y', 'u', 'i', 'o', 'p' 중 하나를 입력할 경우에는 2행 2열에 배치된 'yuiop' 버튼을 누르면 된다. 예를 들어, 사용자 패스워드가 'wow1024#'이라고 가정하자. 사용자는 패스워드의 첫 번째 문자 'w'를 입력하기 위해 'qwert' 버튼을 누르면 제안 키패드는 <그림 3>의 좌측과 같이 중앙의 랜덤 키 영역에 'q', 'w', 'e', 'r', 't' 키들을 랜덤한 위치에 보여준다. 사용자는 패스워드의 첫 번째 문자를 입력하기 위해서 랜덤 키 영역의 중앙에 위치해 있는 'w' 버튼을 눌러 패스워드를 입력한다. 이후 'o'를 입력하기 위해 'yuiop' 버튼을 누르면 중앙의 랜덤 키 영역에 'y', 'u', 'i', 'o',

‘p’ 키가 랜덤한 위치에 뜨며 사용자는 랜덤 키 영역에서 ‘o’ 버튼을 눌러 패스워드를 입력한다.

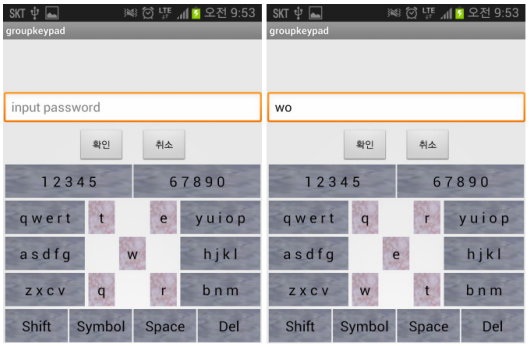

그림 3. 제안 키패드의 키 배치

Figure 3. Key arrangement of the proposed keypad

다음 ‘w’를 입력하기 위해 ‘qwert’ 버튼을 누르면 이전에 ‘qwert’ 버튼을 눌렀을 때와는 달리 <그림 3>의 우측과 같이 키들의 위치가 달라진다. 즉, 랜덤 키 영역의 각 키들은 고정된 위치가 아닌 임의의 위치에 배치되기 때문에 패스워드를 입력할 때마다 센서에 의해 수집되는 위치 정보는 달라진다. 따라서 해커는 수집된 위치 정보를 통해 사용자가 어떤 키를 입력했는지 알 수 없다. ABC 순으로 배치된 키패드 역시 여러 키들이 그룹화 되어 있으며, 특정 그룹 버튼을 선택하면 랜덤 키 영역에 해당 그룹의 키들이 임의의 위치에 배치된다.

<그림 4>는 5개의 키로 구성된 “qwert” 그룹 버튼을 눌렀을 때의 랜덤 키 영역을 보여준다. 각 그룹 버튼에는 5개의 키가 존재하기 때문에 그룹 버튼을 선택하였을 때 랜덤 키 영역에는 5개의 키가 랜덤한 위치에 배치된다. 따라서 각 키가 특정 위치에 배치될 확률은 20%로 동등하게 나타나며, 그룹 버튼 “12345”과 “67890”, “yuiop”, “asdfg”을 눌렀을 때도 동일하다.

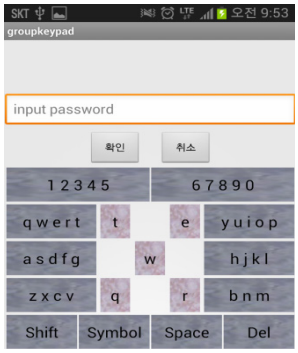

그림 4. 5개의 버튼을 갖는 랜덤 키 영역

Figure 4. 5-button random key area

그림 5. 4개의 버튼을 갖는 랜덤 키 영역

Figure 5. 4-button random key area

<그림 5>는 4개의 키로 구성된 “zxcv” 그룹 버튼을 눌렀을 때의 랜덤 키 영역을 나타낸다. 각 그룹 버튼에는 4개의 키가 존재하기 때문에 그룹 버튼을 선택하였을 때 랜덤 키 영역에는 4개의 키가 랜덤한 위치에 배치된다. 따라서 각 키가 특정 위치에 배치될 확률은 25%로 동등하게 나타나며, 그룹 버튼 “hjkl”을 눌렀을 때도 동일하다.

마지막으로 <그림 6>은 3개의 키로 구성된 “bnm” 그룹 버튼을 눌렀을 때의 랜덤 키 영역을 나타낸다. 각 그룹 버튼에는 3개의 키가 존재하기 때문에 그룹 버튼을 선택하였을 때 랜덤 키 영역에는 3개의 키가 랜덤한 위치에 배치된다. 따라서

각 키가 특정 위치에 배치될 확률은 33.3%로 동등하게 배치된다.

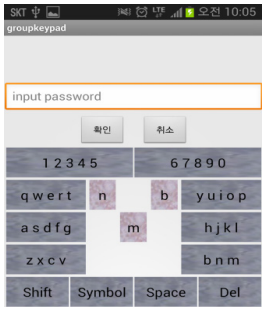

그림 6. 3개의 버튼을 갖는 랜덤 키 영역
Figure 6. 3-button random key area

3.3 안전성 분석 및 평가

랜덤 키패드의 모든 키들은 그룹으로 존재하며 그룹 키에 속하는 키들이 랜덤 키 영역에 배치될 때에는 동일한 확률로 특정 위치에 배치된다. 따라서 사용자가 특정 버튼을 눌렀을 때 센서에 의해 수집된 위치 정보를 통해서는 사용자가 터치한 키 값을 정확히 알 수 없다. 또한, mTranskey와 달리 많은 패스워드 입력을 통해 수집된 위치 정보를 통해서도 배치 확률을 통한 패스워드 추측이 불가능하다.

제안된 랜덤 키패드에서 사용자가 패스워드를 입력할 때, 모션 센서가 생성한 위치 정보를 이용하여 해커가 인증에 성공할 확률 P는 다음과 같다.

$$P = \frac{1}{3^p \times 4^q \times 5^r}, \quad n = p + q + r \qquad (1)$$

수식 (1)에서 n은 패스워드의 길이이며, p는 3개의 키로 구성된 그룹 키에서 패스워드의 일부가 나오는 회수이다. 그리고 q, r 은 각각 4개와 5개의 키로 구성된 그룹 키에서 패스워드의 일부가 나오는 회수를 나타낸다. 사용자가 최악의 패스워드를 선정한 경우를 고려해보자. 최악의 패스워드는 'b', 'n', 'm' 문자로만 구성된 패스워드이다. 8자리의 패스워드를 'b', 'n', 'm' 문자로만 생성한 경우에 해커가 패스워드를 입력하여 인증에 성공할 확률은 다음과 같다.

$$P = \frac{1}{3^8 \times 4^0 \times 5^0} = 0.000152 \qquad (2)$$

반면, ABC 방식의 키패드에서는 4개의 키로 구성된 그룹 버튼에서만 패스워드를 선정한 경우에 가장 취약한 패스워드가 생성된다. 만일, 사용자가 8자리의 패스워드를 'w', 'x', 'y', 'z' 문자로만 생성했다면 해커가 공격에 성공할 확률은 약 0.000015에 해당한다. 따라서 해커가 공인인증서 패스워드를 3번안에 올바르게 입력하여 인증에 성공하는 것은 매우 어렵다.

제안된 키패드에서 8자리 패스워드를 입력할 때에는 먼저 그룹 버튼을 선택한 후에 랜덤 키 영역에서 패스워드를 입력해야하기 때문에 최악의 경우 16번의 키 입력이 필요하다는 단점이 존재한다. 반면, 하나의 그룹 버튼 내에 패스워드의 각 자리가 모두 존재할 경우에는 9번의 키 입력이 필요하다. 즉, 사용자가 패스워드를 입력하는데 필요한 키 입력은 패스워드 각 자리에 대한 그룹 버튼 내의 위치에 따라 상이할 수 있다.

제안 키패드는 그룹 버튼 내의 키 개수에 따라 보안성과 사용 용이성이 서로 반비례한다. 즉, 그룹 버튼에 속하는 키가 많을수록 랜덤하게 배치되는 키들로부터 입력할 키를 찾는 데에 더 많은 시간이 소요되지만, 공격자가 입력한 키를 추측하는 것은 더욱 어려워진다.

<표 3>은 기존의 보안 키패드와 제안된 키패드를 비교한 것이다. mTranskey를 비롯하여 [7]에서

제안한 보안 키패드들은 2.2절에서 기술했듯이 모션 센서를 통한 패스워드 추측 공격에 취약하다. 반면, 랜덤 숫자 키패드는 숫자 키를 동일한 확률로 임의의 위치에 생성하기 때문에 모션 센서를 통한 패스워드 추측 공격에 안전하다. 하지만 숫자로만 구성된 패스워드 입력 시에만 사용 가능하다는 문제가 있다. 본 논문에서 제안한 키패드는 숫자는 물론 문자로 구성된 패스워드에도 적용 가능하며 랜덤 숫자 키패드와 같이 모션 센서를 통한 패스워드 추측 공격에 안전하다. 하지만 사용자의 패스워드 선택에 따라 최악의 경우 패스워드 길이의 두 배에 해당하는 터치가 발생한다는 단점이 있다.

표 3. 기존의 보안 키패드와 제안 키패드 비교
Table 3. Comparison between existing secure keypads and the proposed keypad

키패드	장점	단점
mTranskey	패스워드 입력이 용이	패스워드 추측 공격에 매우 취약
물결형 키패드	패스워드 추측 공격이 다소 어려움	입력할 키의 식별이 어려움
클론 키패드	패스워드 추측 공격이 다소 어려움	사용자가 복사된 행 버튼을 사용하지 않을 경우 취약
터치 & 슬라이드 키패드	패스워드 입력이 용이	화살표 버튼의 터치 수를 통해 패스워드 추측이 가능
랜덤 숫자 키패드	패스워드 추측 공격에 강인함	숫자로 구성된 패스워드에만 적용 가능
제안된 키패드	패스워드 추측 공격에 강인함	최악의 경우 패스워드 길이의 두 배에 해당하는 터치 발생

4. 결 론

본 논문에서는 스마트폰에 내장된 모션 센서를 이용한 패스워드 추측 공격에 안전한 랜덤 키패드를 제안하였다. 안전성 분석을 통해서도 알 수 있듯이 제안된 키패드는 기존의 mTranskey 보다 매우 안전하다. 또한, 랜덤 숫자 키패드와 비교할 때 제안 키패드는 문자와 숫자 조합으로 구성된 패스워드에도 적용 가능한 장점을 갖고 있다. 본 연구에서 제안한 키패드는 모바일 악성코드의 수가 급속히 증가하는 현실에서 사용자들이 안전하게 모바일 뱅킹 서비스를 이용할 수 있는 가능성을 제공한다는 점에서 가치가 있다.

References

[1] The power of smart phones, http://www.etoday.co.kr/news/section/newsview.php?idxno=777734

[2] K. Dunham, S. Abu-Nimeh, M. Becher, S. Fogie, B. Hernacki, J. Morales, and C. Wright, *Mobile malware attacks and defense*, Syngress, 2008.

[3] smartphone malware trends, http://blog.ahnlab.com/ahnlab/1754

[4] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang, *ACCessory: Password inference using accelerometers on smartphones*, Proceedings of the 12th Workshop on Mobile Computing Systems & Applications, 2012.

[5] L. Cai, and H. Chen, *TouchLogger: Inferring keystrokes on touch screen from smartphone motion*, Proceedings of the 6th USENIX conference on Hot topics in security, 2011.

[6] Z. Xu, K. Bai, and S. Zhu, *TapLogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors*, Proceedings of the 5th ACM conference on Security and Privacy in Wireless and Mobile Networks, pp.113-124, 2012.

[7] D. Lee, D. Bae, S. Yoo, J. Chae, Y. Lee, and H. Yang, *Security analysis on the keypad for smartphones*, Review of KIISC, Vol. 21,

No. 7, pp. 30-37, 2011.

[8] Y. Lee, *An analysis on the vulnerability of secure keypads for mobile devices*, Journal of Korean Society for Internet Information, Vol. 14, No. 3, pp. 15-21, 2013.

[9] mTranskey, http://www.raonsecure.com/solution/mtranskey.php

[10] Y. Ryu, D. Koh, B. Aday, X. Gutierrez, and J. Platt, *Usability evaluation of randomized keypad*, Journal of Usability Studies, Vol. 5, No. 2, pp. 65-75, 2010.

[11] I. Kim, *Keypad against brute force attacks on smartphones*, IET Information Security, Vol. 6, No. 2, pp. 71-76, 2012.

모션 센서를 이용한 패스워드 추측 공격에 안전한 랜덤 키패드

김익수[1], 최종명[2]

[1]*숭실대학교 컴퓨터학부*

[2]*목포대학교 컴퓨터공학과*

요 약

스마트폰 사용자가 급증함에 따라 스마트폰을 이용한 모바일 뱅킹 서비스 이용자도 크게 증가하였다. 스마트폰 사용자가 모바일 뱅킹 서비스를 이용하기 위해서는 모바일 뱅킹 앱에서 공인인증서의 패스워드를 입력해야 한다. 최근 연구에 따르면 키패드로 입력되는 패스워드의 추측이 스마트폰에 내장된 모션 센서를 통해 가능하다는 보고가 있었다. 본 논문에서는 스마트폰에 내장된 모션 센서를 이용한 패스워드 추측 공격에 안전한 랜덤 키패드를 제안한다. 제안된 키패드는 사용자의 키 입력을 위한 랜덤키 영역을 키패드의 중앙에 별도로 제공함으로써 패스워드 입력 시 발생하는 위치 정보를 매번 다르게 생성한다. 해커가 모션 센서를 이용하여 입력된 키에 대한 정보를 수집하더라도 패스워드 유추가 불가능하기 때문에 사용자는 안전하게 모바일 뱅킹 서비스를 이용할 수 있다.

Iksu Kim received the B.S., M.S., and Ph.D. in the Department of Computer Science from Soongsil University, South Korea, in 2000, 2002, and 2008, respectively. He worked at SKYCOM as a manager until January 2009. He is a professor of School of Computing at Soongsil University from September 2009. He achieved the CISSP(Certified Information Systems Security Professional) certification in 2008. His research interests include system and network security.

E-mail address: iksuplorer@ssu.ac.kr

Jongmyung Choi received the Bachelor's degree, Master's degree, and Ph. D. in computer science from Soongsil University, South Korea, in 1992, 1996, and 2003 respectively. He is currently an associate professor in the Department of Computer Engineering, Mokpo National University, South Korea, since 2004. He did research as a visiting scholar at Georgia Institute of Technology, USA, from 2010 to 2011. His research interests are human robot interaction (HRI), context-aware systems, social computing, and healthcare.

E-mail address: jmchoi@mokpo.ac.kr