Journal of Knowledge Information Technology and Systems(JKITS), Vol. 9, No. 4, pp. 483~491, August 2014

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Secure Keypad against Password Guessing Attacks with Accelerometer and Gyroscope 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

According to recent studies, data generated from smartphone's built-in accelerometer and gyroscope sensors can be used to infer users' passwords. Currently, the secure keypad which is being used in smartphone apps is vulnerable to password attacks using sensor data. In this paper, we propose a secure keypad against password guessing attacks with accelerometer and gyroscope sensors. In the keypad, the rows of keys on the proposed keypad is randomly changed whenever a user inputs a letter of the password. Accordingly, it is very difficult to find out the user' password using accelerometer and gyroscope sensor data. Moreover, the proposed keypad uses fake key buttons to further reduce the success rate of the attack. Users do not have to memorize fake keys. Users only need to touch the fake keys on the proposed keypad when they input their passwords. Because attackers cannot distinguish fake keys from touched keys, they cannot find out users' passwords with accelerometer and gyroscope sensors. Therefore users can safely use a variety of internet services.

KEYWORDS: Secure keypads, Password guessing attacks, Randomized keypads, Smartphones, Accelerometer sensors, Gyroscope sensors

ARTICLE INFO: Received 28 July 2014, Revised 14 August 2014, Accepted 14 August 2014.

1. 서 론

최근 태블릿, 스마트폰과 같은 다양한 모바일 기기가 광범위하게 보급됨에 따라 언제 어디서나 모바일 뱅킹, 전자상거래, 다양한 콘텐츠 제공 사이트 이용이 가능하게 되었다[1]. 모바일 기기는 언제

[*]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

어디서든지 사용할 수 있어야하기 때문에 휴대성이 좋아야 한다. 이에 대부분의 태블릿과 스마트폰들은 물리적인 키보드 대신 디스플레이의 터치를 통해 입력할 수 있는 가상 키패드를 제공한다. 하지만 최근 연구에 따르면 태블릿과 스마트폰에 내장된 가속도 센서나 방향 센서를 악용하면, 가상 키패드를 통해 입력되는 패스워드를 쉽게 알아낼 수 있음이 증명되었다[2-6].

현재 국내에서는 모바일 뱅킹 앱을 통해 금융사이트에 접속 시 공인인증서의 패스워드를 입력하도록 되어있으며, 이용자에게 배포되는 모바일 뱅킹 앱에는 임의의 위치에 공백을 삽입하여 키의 위치를 임의적으로 변경하는 보안 키패드가 탑재되어 있다. 하지만 현재 모바일 뱅킹 앱에 탑재된 보안 키패드는 단순히 키패드의 임의의 위치에 공백을 추가하기 때문에 각 키들이 배치되는 위치가 제한적이다. 따라서 여러 번의 패스워드 입력에 따른 터치 위치 정보가 수집될 경우에 사용자가 입력한 패스워드가 노출될 수 있는 문제가 있다. 이러한 문제를 해결하고자 [7]과 같은 보안 키패드 연구가 진행되어 왔다. 하지만 가속도 및 방향 센서를 통해 여러 번의 패스워드 입력 정보가 수집될 경우, [7]에서 제안한 키패드들은 여전히 패스워드 공격에 취약하다. 이에 [8]에서는 여러 번의 패스워드 입력에도 패스워드가 노출되지 않는 랜덤 키패드를 제안하였다. 하지만 이 키패드를 사용할 경우, 사용자의 패스워드 자리 수가 n개일 때 최악의 경우 2n번을 터치해야 하는 단점을 가진다.

이에 본 논문에서는 [8]이 가지는 단점, 즉 패스워드 입력 시 필요한 과도한 터치 횟수를 줄일 수 있으며, 가속도 및 방향 센서를 통한 공격으로부터 패스워드 노출을 막을 수 있는 보안 키패드를 제안한다. 제안된 키패드는 사용자가 패스워드를 입력할 때마다 각 행들의 위치는 일정한 규칙에 의해 변경된다. 변경된 위치를 통해 패스워드를 입력할 경우 터치되는 위치는 기존의 고정된 QWERTY 키패드 상에서 터치되는 위치와 서로 다르기 때문에 가속도 및 방향 센서를 이용한 패스워드 공격을 통해 정확한 패스워드를 알 수 없다. 또한 제안된 키패드는 사용자의 선택에 따라 해커의 패스워드 공격 성공률을 더 낮추기 위해 속임수 키를 추가하여 보안성을 강화할 수 있다. 속임수 키는 사용자가 외울 필요가 없기 때문에 추가적인 부담이 없으며, 해커에게는 터치되는 위치 정보를 통한 패스워드 추측 공격을 더욱 어렵게 한다.

본 논문의 2장에서는 스마트폰에서의 패스워드 공격 방법과 현재 모바일 뱅킹 앱에서 사용되고 있는 보안 키패드를 소개한다. 3장에서는 2장에서 소개한 보안 키패드의 안전성을 분석하고 제안하는 키패드를 설명한다. 4장에서는 제안된 키패드의 안전성을 분석한 후, 마지막으로 5장에서 결론을 내린다.

2. 관련 연구

2.1 스마트폰 패스워드 공격 방법

최근 들어서 스마트폰 사용자 수는 크게 증가하였으며, 스마트폰을 이용한 금융 거래가 활성화되었다. 최신 스마트폰들은 기계식 키보드 대신에 디스플레이를 통해 입력할 수 있는 가상 키패드를 제공한다. 하지만 가상 키패드를 통해 입력되는 패스워드는 디스플레이에 남겨진 지문을 통해 패스워드를 획득하는 스머지(Smudge) 공격에 취약하며 [9], 스마트폰에 내장된 가속도 및 방향 센서를 통한 패스워드 공격이 가능하다[2-6].

<그림 1>은 안드로이드 스마트폰에서 제공하는 패턴 기반의 패스워드 입력 방식에서 패스워드 공격이 가능한 지문 흔적을 보여준다. 사용자가 자신의 패스워드를 입력하기 위해 디스플레이 상에서

손가락으로 패턴을 그리면 지문에 의한 흔적이 남게 되기 때문에 사용자의 패스워드가 쉽게 노출될 수 있다. 패턴 기반의 패스워드는 사용자에게 편의성을 제공하지만 스머지 공격에 매우 취약하기 때문에 스마트폰 관리에 세심한 주의가 필요하다.

그림 1. 스마트폰에 남겨진 지문
Figure 1. Fingerprint on the smartphone

최근 출시되는 대부분의 스마트폰에는 방향 센서와 가속도 센서가 탑재되어 있으며, 이들 센서는 현재 많은 모바일 앱과 게임에 사용되고 있다. 방향 센서를 통해서는 스마트폰이 어느 방향을 바라보고 있으며 어느 정도 기울어졌는지를 측정할 수 있으며, 가속도 센서를 통해서는 스마트폰이 어느 방향으로 얼마나 빠르게 움직였는지를 측정할 수 있다. [3]에서는 스마트폰 방향 센서가 감지하는 3차원 방향 데이터를 통해 사용자가 디스플레이상에서 터치한 키를 식별함으로써 패스워드를 유추하는 Touchlogger를 구현하였다. 가상 키패드에 존재하는 키들을 터치할 때에 방향 센서가 생성하는 데이터들은 서로 다른 값을 갖기 때문에 이 값을 통한 패스워드 획득이 가능해진다. 특히, 안드로이드 스마트폰의 경우 백그라운드로 프로세스가 실행될 수 있기 때문에 Touchlogger와 같은 앱이 사용자의 스마트폰에 설치될 경우 사용자가 입력하는 패스워드를 몰래 획득할 수 있다. [3]에서 구현된 Touchlogger는 3행 4열의 숫자 키패드를 통해 사용자가 입력하는 0부터 9까지의 키를 식별하는데 약 70% 이상의 정확성을 보였다.

[5]에서는 방향 센서와 함께 사용자의 터치 위치를 더욱 정확하게 추적하기 위해 가속도 센서를 통해 가속도 데이터를 수집한 후, 기계 학습 분석을 통해 태블릿과 스마트폰의 터치 위치를 추적하는 TapPrints를 구현하였다. TapPrints를 통한 실험 결과 태블릿과 스마트폰에서의 QWERTY 방식의 키패드에서 각각 90%와 80%의 정확성으로 터치된 문자를 알아낼 수 있음을 보였다. 그리고 [6]에서는 패턴 기반의 패스워드 입력 시 사용자가 디스플레이를 스와이프(swipe)하는 경우에도 스마트폰에 내장된 센서를 통해 패스워드를 알아낼 수 있음을 보였다.

2.2 스마트폰용 보안 키패드

현재 모바일 뱅킹 앱에서 공인인증서 패스워드를 입력받기 위해 가장 많이 사용되고 있는 보안 키패드는 <그림 2>와 같다.

그림 2. 공백이 추가된 보안 키패드
Figure 2. Secure keypad with blanks

인증 시 마다 키패드 임의의 위치에 공백을 삽입하여 사용자가 패스워드 입력 시 터치하는 위치가 매번 달라지게 한다. 예를 들어 패스워드가 “dragon37”이고 사용자가 공인인증서의 패스워드를 입력하고자 할 때 <그림 2>의 좌측과 같이 키패드가 생성되었다고 하자. 사용자는 패스워드의 첫 번째 자리인 ‘d’를 입력할 때 3행 3열의 키를 터치하게 된다. 사용자가 차후에 모바일 뱅킹 서비스를 이용하기 위해 공인인증서의 패스워드를 입력

하려 할 때 <그림 2>의 우측과 같이 이전의 키 배열과는 다른 키패드가 생성된다. 이 때 사용자가 패스워드의 첫 번째 자리인 'd'를 입력할 때에는 3행 4열을 터치하게 된다. 이와 같이 매 인증 시 마다 키들의 위치가 임의로 바뀌기 때문에 기존의 고정된 키패드에 비해 안전하다 할 수 있다. 하지만 단순히 공백이 추가되는 보안 키패드는 키들이 배치되는 위치가 제한적이기 때문에 패스워드 입력 시 터치되는 위치 정보를 여러 번 수집할 경우 해커에게 패스워드가 쉽게 노출될 수 있다.

[10-11]에서는 숫자 키들로 구성된 랜덤 키패드를 제안하였다. 이 키패드들은 임의의 위치에 숫자 키들을 생성하기 때문에 가속도 및 방향 센서를 이용한 패스워드 추측 공격에 안전하다. 하지만 숫자 키들로만 구성되어 있기 때문에 숫자를 제외한 다른 문자들을 패스워드로 사용할 수 없다. [8]에서는 앞서 기술한 보안 키패드들을 개선한 랜덤 키패드를 제안하였다. 이 키패드는 숫자는 물론 문자로 구성된 패스워드 입력이 가능하며 키 배치가 기존의 ABC 혹은 QWERTY 키패드와 거의 유사하기 때문에 사용자는 입력하고자 하는 키를 쉽게 찾을 수 있는 장점을 가지고 있다. 하지만 전체 길이가 n인 패스워드를 입력할 때에, 최악의 경우 2n번을 터치해야 하는 단점을 가진다. <표 1>은 앞서 기술한 키패드들의 장단점을 요약한 것이다.

표 1. 기존의 보안 키패드 비교
Table 1. Comparison of existing secure keypads

키패드	장점	단점
공백이 추가된 키패드	패스워드 입력이 용이	패스워드 노출 가능성이 매우 높음
[10-11]	센서 데이터를 이용한 공격에 안전	숫자 패스워드만 사용 가능
[8]	센서 데이터를 이용한 공격에 안전	패스워드 입력 시 과도한 키 버튼 터치 발생

3. 제안하는 랜덤 키패드

3.1 공백이 포함된 보안 키패드 안전성

표 2. 각 키들의 배치 가능한 위치
Table 2. arrangement position of each key

키	출현 위치 열
'1', 'q'	1, 2
'2', 'w', 'z'	2, 3
'3', 'e', 'x'	3, 4
'4', 'r', 'c'	4, 5
'5', 't', 'v'	5, 6
'6', 'y', 'b'	6, 7
'7', 'u', 'n'	7, 8
'8', 'i', 'm'	8, 9
'9', 'o'	9, 10
'0', 'p'	10, 11
'a'	1, 2, 3
's'	2, 3, 4
'd'	3, 4, 5
'f'	4, 5, 6
'g'	5, 6, 7
'h'	6, 7, 8
'j'	7, 8, 9
'k'	8, 9, 10
'l'	9, 10, 11

<표 2>는 임의의 위치에 공백이 포함된 보안 키패드에서 각 키들이 배치될 수 있는 위치를 보여준다. <표 2>에서도 알 수 있듯이 보안 키패드의 1행, 2행, 4행에 존재하는 키들은 두 개의 열에서만 배치될 수 있으며, 3행에 존재하는 키들은 세 개의 열에서만 배치될 수 있다. 또한, 각 키들이 배치될 수 있는 열의 위치도 다르기 때문에 사용자가 여러 번의 패스워드 입력 시 생성되는 터치 위치 정보가 수집된다면 패스워드는 쉽게 노출될 수 있다. 예를 들어, 패스워드가 "passwd12" 라고 가정하자. 사용자가 패스워드의 첫 번째 자리인 'p'를 입력한다면, 'p'가 배치될 수 있는 위치인 2행 10열 혹은 2행 11열을 터치하게 된다. 만일 2행 11

열을 터치하였다면 터치된 위치 정보와 <표 2>를 통해 'p'를 입력했다는 것을 바로 알 수 있다. 이는 2행 11열에 배치될 수 있는 키가 오직 'p' 뿐이기 때문이다. 반면, 2행 10열을 터치하였다면 'p'나 'o'를 입력했다는 것을 알 수 있다. 이 경우에는 한 번의 패스워드 입력을 통해서 'p'를 입력했는지 'o'를 입력했는지 판단할 수 없다. 하지만 사용자가 차후에 패스워드를 입력할 때 'p'가 2행 10열이 아닌 2행 11열에 배치되고 사용자가 2행 11열을 터치하게 되면 패스워드가 'p'라는 것을 알 수 있다. 또 다른 예로 사용자가 's' 키를 입력한다고 가정하자. 이 때 's' 키가 배치될 수 있는 위치는 2, 3, 4열 위치 중 하나가 된다. 따라서 사용자는 's' 키를 입력하기 위해 2, 3, 혹은 4열 중 한 위치를 터치하게 된다. 여러 번의 패스워드 입력 시 생성되는 터치 위치 정보를 수집하게 되면 's' 키를 터치할 때 2, 3, 4 열의 위치 정보가 모두 수집될 수 있기 때문에 's' 키의 입력을 확인할 수 있다. 이와 같이 임의의 위치에 공백을 배치하는 보안 키패드에서 여러 번의 패스워드 입력 시 발생하는 터치 위치 정보가 수집될 경우, 사용자 패스워드가 쉽게 노출될 수 있는 문제가 있다. 이에 대한 대안으로 [8]에서 제안한 랜덤 키패드를 사용할 경우 패스워드 노출을 막을 수 있지만, 앞서 기술했듯이 패스워드 입력 시 과도한 키 버튼 터치가 요구된다.

3.2 제안 키패드의 키 배열

터치된 위치 정보를 통한 패스워드 공격에 안전한 키패드는 여러 번의 패스워드 입력 시 생성되는 위치 정보를 통해 패스워드가 직접적으로 노출되어서는 안 된다. <그림 3>은 제안하는 키패드가 생성할 수 있는 4가지 형태의 키 배열을 나타낸다. QWERTY 키패드에 익숙한 사용자를 고려하여 키패드의 키들은 일반 키패드와 마찬가지로 각 열의 위치는 고정된다.

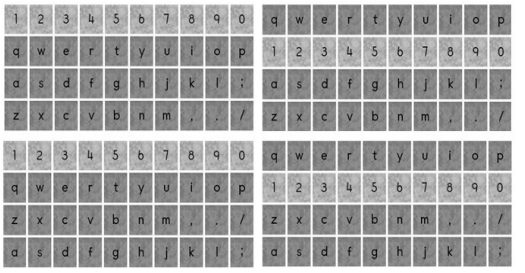

그림 3. 제안 키패드
Figure 3. The proposed keypad

반면, 여러 번의 패스워드 입력 시 수집된 위치 정보를 통해 패스워드가 노출되는 것을 방지하기 위해 키패드의 행들은 임의의 위치로 변경될 수 있다. 행들의 위치가 변경될 때에는 1행과 2행의 위치가 서로 바뀌며, 3행과 4행의 위치가 서로 바뀐다. 그리고 랜덤 키패드를 통해 사용자가 전체 패스워드를 입력할 때까지 키패드가 4가지 형태의 키 배열 중 하나로 고정되지 않으며 패스워드의 각 자리를 입력할 때마다 4가지 형태의 키 배열이 랜덤하게 나타난다. 만일 패스워드 전체를 입력하는 동안 한 가지 형태의 키 배열로 고정될 경우, 해커는 터치된 위치 정보를 통해 평균 2회의 패스워드 입력으로 인증에 성공할 수 있게 된다.

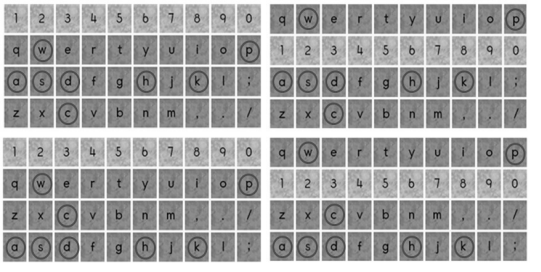

그림 4. "pswdhack"을 입력할 때의 터치 위치
Figure 4. touch position when entering "pswdhack"

예를 들어 패스워드가 pswdhack이라 가정하면, 사용자가 4가지 형태의 키패드에서 패스워드를 입력할 때 터치하는 위치는 <그림 4>와 같다. 해커는 터치된 위치 정보를 통해 최대 4번의 패스워드 입력을 시도하여 인증에 성공할 수 있으며, 평균적으로 2번의 패스워드 입력 시도를 통해 인증에 성공할 수 있다. 하지만 사용자가 패스워드의 각 자리를 입력할 때마다 키패드의 행 위치가 변경될 경우에는 패스워드의 길이에 따라 공격 성공률은 낮아진다. <표 3>은 제안된 키패드에서 각 키 들이 배치될 수 있는 위치를 나타낸 것이다.

표 3. 각 키들의 배치 가능한 위치
Table 3. arrangement position of each key

키	출현 위치 행
'1', '2', '3', '4', '5', '6', '7', '8', '9', '0'	1, 2
'q', 'w', 'e', 'r', 't', 'y', 'u', 'i', 'o', 'p'	1, 2
'a', 's', 'd', 'f', 'g', 'h', 'j', 'k', 'l', ';'	3, 4
'z', 'x', 'c', 'v', 'b', 'n', 'm', ',', '.', '/'	3, 4

<표 3>에 따르면 기존의 고정 키패드에서 1행과 2행에 존재하는 키들은 제안된 키패드에서 1행 혹은 2행에 배치된다. 그리고 기존의 고정 키패드에서 3행과 4행에 존재하는 키들은 제안된 키패드에서 3행 혹은 4행에 배치된다. 따라서 1행이나 2행에 배치된 키를 누를 때 해커는 숫자키를 눌렀는지 문자키를 눌렀는지 알 수 없다. 또한 3행이나 4행에 배치된 키를 눌렀을 때에도 마찬가지이다. 예를 들어 패스워드가 "wakeup36" 이라고 가정할 때 패스워드 첫 번째 자리인 'w'는 2행 2열 혹은 1행 2열에 배치될 수 있기 때문에 사용자가 'w' 키를 누른다고 하더라도 'w' 키를 눌렀는지 '2' 키를 눌렀는지 알 수 없다. 단지 문자키 'w' 혹은 숫자키 '2' 중 하나를 눌렀다는 사실만 알 수 있다.

3.3 속임수 키 생성

제안된 키패드는 해커의 패스워드 공격 성공률을 더 낮추기 위해 속임수 키를 제공하여 보안성을 강화한다. 사용자는 자신이 생성한 패스워드의 임의의 자리에 속임수 키를 추가할 수 있다. 그리고 속임수 키의 개수와 속임수 키가 추가될 위치는 사용자가 임의로 설정할 수 있다. 사용자가 패스워드를 "cage1024"로 설정하였고 속임수 키의 개수가 1개이며, 패스워드에 추가될 속임수 키의 자리가 네 번째라고 하자. 이 경우 사용자가 설정한 속임수 키 1개는 cag 와 e1024 사이에 추가되며, 이후의 모든 패스워드 인증 과정에서 사용자는 'c', 'a', 'g', '속임수 키', 'e', '1', '0', '2', '4' 키를 순차적으로 누르면 된다.

예를 들어 속임수 키를 'n'으로 결정하였다면 네 번째 패스워드를 입력할 때 키패드는 <그림 5>와 같이 4행 6열 혹은 3행 6열에 색깔이 다른 버튼이 배치되는 형태로 나타난다.

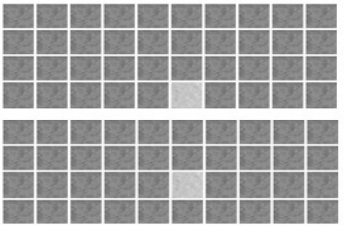

그림 5. 제안 키패드에서의 속임수 키
Figure 5. fake key on the proposed keypad

4행 6열과 3행 6열은 문자키 n이 배치될 수 있는 위치에 해당한다. 사용자는 패스워드를 입력하는 과정에서 속임수 키가 출현하면 다른 키들과 색깔이 확연히 구분되는 속임수 키를 누르고 계속해서 이후의 패스워드 자리 수들을 입력하면 된다. 사용자는 속임수 키를 기억할 필요가 없으며 단지

색깔이 다른 버튼을 누르기만 하면 된다. 해커는 입력된 값이 n 혹은 h라고 추측할 수 있지만 정확한 값을 알 수 없다.

공백을 임의의 위치에 삽입하는 기존의 보안 키패드는 사용자의 패스워드 입력 정보를 여러 번 수집할 경우 패스워드를 알아낼 수 있다. 하지만 제안된 키패드는 사용자가 패스워드 각 자리를 입력할 때마다 키들의 행 위치가 임의로 바뀌며, 속임수 키가 추가되기 때문에 정확히 사용자의 패스워드를 알아내는 것이 불가능하다. 특히, 속임수 키는 사용자가 외울 필요가 없기 때문에 기억해야 할 추가적인 부담이 없으며, 해커에게는 터치되는 위치 정보를 통한 패스워드 추측 공격을 더욱 어렵게 한다.

4. 안전성 분석 및 평가

제안된 키패드에서는 패스워드의 각 자리를 입력할 때마다 1, 2행과 3, 4행간의 위치가 임의로 바뀌기 때문에 가속도 및 방향 센서를 통해 해커가 패스워드 공격에 성공할 확률 P는 다음과 같다.

$$P = \frac{1}{2^{n+k}} \quad (1)$$

수식 (1)에서 n은 패스워드의 길이이며, k는 속임수 키의 개수이다. 해커는 n자리의 패스워드를 추측하여 인증에 성공하기 위해서는 최악의 경우 2n+k 번을 입력해야 하며, 평균적으로 2n+k-1번을 입력해야 인증에 성공할 수 있다.

현재 보안상의 이유로 패스워드를 생성할 때에는 패스워드의 길이를 최소 8자리 이상으로 설정하도록 권고하고 있으며, 현재 공인인증서의 패스워드 역시 8자리 이상으로 설정해야 한다. 만일 해커가 8자리로 설정된 패스워드에 추측 공격을 시도한다면 평균적으로 27번의 로그인 시도를 해야 공격에 성공할 수 있다. 즉, 해커가 인증에 성공할 평균 확률은 약 0.0078125에 해당한다. 만일 패스워드 길이가 8자리이며 속임수 키를 두 개로 설정한 경우의 평균 확률은 수식 (2)와 같다. 속임수 키가 하나씩 증가할 때마다 해커에 의한 추측 공격 성공률은 반씩 감소하게 된다.

$$P = \frac{1}{2^{8+2-1}} = 0.001953 \quad (2)$$

표 4. 제안하는 키패드와 [8]에서 제안된 키패드 비교
Table 4. Comparison between our keypad and the keypad proposed in [8]

키패드	8자리 패스워드 공격 성공률	8자리 패스워드 평균 터치 횟수	8자리 패스워드 전체 입력 시간
[8]	0.000304	12	19.03초
제안 키패드	0.0078125	8	8.97초

<표 4>는 본 논문에서 제안한 키패드와 [8]에서 제안된 키패드 간의 비교 결과이다. 제안 키패드는 [8]과 비교할 때 패스워드 공격에 대한 해커의 성공 확률이 상대적으로 높지만, 여전히 성공 확률이 매우 낮기 때문에 해커로부터 안전하다. 그리고 8자리 패스워드를 입력할 때 [8]은 평균적으로 12번의 터치가 필요하지만, 제안 키패드의 경우에는 8번의 터치만 요구되므로 신속하게 전체 패스워드를 입력할 수 있는 장점을 가진다. 실제로 [8]에서 제안된 키패드와 본 키패드의 패스워드 입력 시간을 측정한 결과 [8]의 경우 평균적으로 한 번의 터치에 1.58초가 소요된 반면, 본 키패드에서는 1.12초 밖에 소요되지 않았다. 이는 [8]에서 제안된 키패드보다 본 키패드에서 입력하고자 하는 키를 더 쉽게 찾을 수 있다는 것을 입증한다.

5. 결 론

최근 스마트폰 사용자가 3천만 명을 초과하였으며, 모바일 뱅킹 이용자 수가 2천만 명을 넘을 정도로 스마트폰을 이용한 모바일 뱅킹 서비스는 매우 활성화 되어 있다. 하지만 패스워드 입력 시 터치하는 위치 정보를 이용한 패스워드 공격 방법에 관한 연구가 보고되었다. 국내에서는 키패드에 공백을 추가하는 방법으로 패스워드 공격에 대응하는 보안 키패드가 사용되고 있지만, 여러 번의 패스워드 인증 과정을 통해 수집된 키 터치 위치 정보를 통해 사용자의 패스워드가 쉽게 노출될 수 있다는 문제점을 가지고 있다.

본 논문에서 제안한 키패드는 여러 번의 인증 과정에서 수집된 정보를 분석하더라도 정확한 패스워드를 알아내는 것이 불가능하다. 또한 [8]에서 제안한 키패드와 비교할 때 본 키패드는 패스워드 입력 시 키 입력 시간을 현저히 줄일 수 있다. 게다가 사용자의 선택에 따라 속임수 키를 추가함으로써 해커의 패스워드 추측 공격 성공률을 더욱 낮출 수 있는 장점을 가지고 있다. 결론적으로 본 논문에서 제안한 키패드가 스마트폰 앱에 탑재된다면 사용자는 더욱 안심하고 안전하게 모바일 뱅킹 서비스를 이용할 수 있을 것으로 판단된다.

References

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

[2] 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.

[3] 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.

[4] 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.

[5] E. Miluzzo, A. Varshavsky, S. Balakrishnan, and R.R. Choudhury, *TapPrints: Your finger taps have fingerprints*, Proceedings of the 10th international conference on Mobile systems, applications, and services, pp. 323-336, 2012.

[6] A.J. Aviv, B. Sapp, M. Blaze, and J.M. Smith, *Practicality of accelerometer side channels on smartphones*, Proceedings of the 28th Annual Computer Security Applications Conference, pp. 41-50, 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] I. Kim, and J. Choi, *Randomized keypad against password guessing attacks with motion sensors*, Journal of Knowledge Information Technology and Systems, Vol. 9, No. 1, pp. 75-83, 2014.

[9] A.J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J.M. Smith, *Smudge attacks on smartphone touch screens*, Proceedings of the USENIX 4th Workshop on Offensive Technologies, 2010.

[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.

가속도 센서와 방향 센서를 이용한 패스워드 추측 공격에 대응하는 보안 키패드

김익수[1], 최종명[2]

[1] *숭실대학교 컴퓨터학부*

[2] *목포대학교 컴퓨터공학과*

요 약

최근 연구들에 따르면 스마트폰에 내장된 가속도 센서와 방향 센서로부터 생성되는 데이터는 사용자의 패스워드를 유추하기 위해 사용될 수 있다. 현재 스마트폰 앱에서 사용되고 있는 보안 키패드는 센서 데이터를 이용한 패스워드 공격에 취약하다. 이에 본 논문에서는 가속도 센서와 방향 센서를 이용한 패스워드 추측공격에 대응하는 안전한 키패드를 제안한다. 제안 키패드 상의 행들은 사용자가 패스워드의 한문자를 입력할 때마다 임의로 위치가 변경된다. 따라서 해커는 가속도 센서와 방향 센서로부터 생성되는 데이터를 이용하여 사용자의 패스워드를 알아내는 것이 매우 어렵다. 또한, 속임수 키 버튼을 사용하여 공격 성공률을 더욱 낮출 수 있다. 사용자는 속임수 키를 기억할 필요가 없으며, 패스워드 입력 시 단지 속임수 키를 터치하기만 하면 된다. 해커는 사용자가 터치하는 속임수 키를 보통의 키와 구분할 수 없기 때문에 가속도 센서와 방향 센서를 이용한 패스워드 추측 공격이 불가능하다. 따라서 사용자는 다양한 서비스들을 안전하고 편리하게 이용할 수 있다.

Iksu Kim received the B.S., M.S., and Ph.D. in 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 currently an assistant professor in the School of Computer Science and Engineering at Soongsil University since September 2009. His research interests include system security, network security, and mobile 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 computer interaction, context-aware systems, social computing, and healthcare.

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