Journal of Knowledge Information Technology and Systems(JKITS), Vol. 15, No. 5, pp. 591-598, October 2020
https://doi.org/10.34163/jkits.2020.15.5.001

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700 (Print), ISSN 2734-0570 (Online)

http://www.kkits.or.kr

Secure Numeric Keypad against Attacks Guessing Passwords from Key Touching

Iksu Kim*

School of Computer Science and Engineering, Soongsil University

ABSTRACT

Currently, smartphones are used in various online services such as electronic payments, stocks, and mobile banking. So far, there have been many studies to counter attacks that can occur when entering a password on a smartphone. Secure numeric keypads, which are currently popularly used, add spaces between keys or shuffle the order of keys to improve the security of existing keypads. Keypads with spaces have a problem that the location of the touched key is easily exposed to the attacker, and the method of shuffling the order of the keys can easily be exposed to the attacker when the password consists of the same number. In this paper, we propose a secure numeric keypad against password guessing attacks that can occur when entering a password on a smartphone. The proposed keypad shuffles the order of the keys and moves the touched keys to a random location so that the password composed of the same numbers is not easily exposed to the attacker. As a result, it is possible to avoid touching the same location when entering the same numbers. Therefore, the proposed keypad is strong against the password guessing attack that can occur when entering a password on a smartphone.

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

ARTICLE INFO: Received 6 August 2020, Revised 21 September 2020, Accepted 13 October 2020.

*Corresponding author is with the School of Computer Science and Engineering, Soongsil University, 369, Sangdo-ro, Dongjak-gu, Seoul, 06978, KOREA.

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

1. 서 론

최근 많은 사람들이 전자결제, 주식, 모바일 뱅킹과 같은 다양한 온라인 서비스에 스마트폰을 이용하고 있다. 휴대성이 중요한 스마트폰은 PC와 달리 데이터 입력을 위한 키보드가 단말기에 탑재된다. 스마트폰 상에서 넓은 디스플레이 영역을 확보하기 위해 최근 출시되는 대부분의 스마트폰은 물리적 키패드 대신 손가락으로 화면을 터치하여 입력할 수 있는 가상 키패드를 탑재하고 있다. 기존의 물리적 키패드와 비교할 때 가상 키패드의 장점은 랜덤한 위치에 키들을 배치할 수 있어 악의적인 키로거 프로그램에 안전하다는 점이다. 물리적 키패드는 항상 고정된 위치에 키가 배치되기 때문에 키로거 프로그램을 통한 키 입력 정보를 수집하여 정확한 패스워드를 알 수 있다. 반면, 가상 키패드로 구현되는 랜덤 키패드들은 키의 위치가 매번 변하기 때문에 터치된 위치 정보의 수집으로 정확한 패스워드를 알아내기가 어렵다.

지금까지 스마트폰의 패스워드 입력 시 발생할 수 있는 공격에 대응하기 위해 많은 연구가 진행되어왔다. 현재 대중적으로 사용되고 있는 보안 숫자 키패드는 기존 키패드의 보안성을 개선하기 위해 키 사이사이에 공백을 추가하거나 키의 순서를 뒤섞어 배치한다. 공백을 추가하는 방법은 터치된 키의 유추가 가능하며, 키의 순서를 뒤섞어 배치하는 방법은 패스워드가 같은 숫자로 구성되었을 때 공격자에게 쉽게 노출될 수 있다는 문제가 있다.

본 논문에서는 스마트폰에서 가능한 패스워드 추측 공격에 안전한 숫자 키패드를 제안한다. 제안하는 키패드는 보안성 개선을 위해 키의 순서를 뒤섞어 배치하고, 같은 숫자로 구성된 패스워드가 공격자에게 쉽게 노출되지 않도록 터치된 키를 랜덤한 위치로 이동시킨다. 따라서 같은 숫자를 연속으로 입력하는 경우, 같은 위치를 터치하는 것을 피할 수 있어 공격자의 패스워드 추측 공격에 강인하다.

본 논문의 2장에서는 스마트폰의 패스워드 추측 공격 방법과 이에 대응하기 위해 개발된 보안 키패드들을 소개한다. 3장에서는 제안하는 키패드에 대해 기술하고 그 사용성을 분석한다. 그리고 마지막으로 4장에서 결론을 맺는다.

2. 관련 연구

2.1 스마트폰 패스워드 추측 공격

가장 단순한 스마트폰 패스워드 공격은 디스플레이에 남겨진 지문의 흔적을 확인하고 패스워드를 추측하는 스머지 공격이다[1]. 패턴으로 설정된 패스워드는 스머지 공격에 매우 취약하다. 패턴 입력을 통한 인증은 <그림 1>의 좌측과 같이 디스플레이에 점들이 배치되면 사용자는 손가락으로 점들을 연결하여 패턴을 입력한다. 이 경우 <그림 1>의 우측과 같이 액정에 지문이 남아 쉽게 패스워드가 노출되는 문제가 있다.

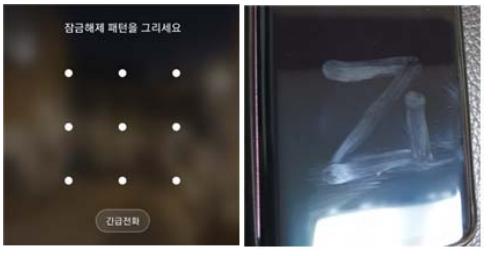

그림 1. 스머지 공격
Figure 1. Smudge attack

패턴은 물론, 숫자로 구성된 패스워드를 추측하기 위한 공격 방법에서 방향 센서와 가속도 센서와 같은 모션 센서들을 사용할 수 있다. 사용자가 비밀번호를 입력하기 위해 키보드의 키를 누를 때,

각 키의 위치에 따라 사용자가 들고 있는 스마트폰의 방향 및 기울기 등이 달라진다. 이에 착안하여 모션 센서가 생성하는 데이터들을 이용해 패스워드를 알아내는 방법들과 구글 글래스를 이용하여 단거리의 다른 사용자가 입력하는 패스워드를 유추하는 방법이 소개되었다[2-7].

2.2 보안 키패드

스마트폰의 qwerty 키패드에서 발생 가능한 패스워드 추측 공격에 대응하기 위해 다양한 연구들이 진행되어왔다[8, 9]. <그림 2>와 같이 여러 개의 키들을 버튼 하나에 그룹화하는 방법은 초기에 좌측과 같이 표시되며, 사용자가 만일 q를 입력할 경우 qwert 버튼을 먼저 터치한다[8]. 그러면 <그림 2>의 우측과 같이 중앙에 5개의 키가 랜덤한 위치에 배치되며, 사용자는 q 버튼을 찾아 터치를 하여 패스워드를 입력한다. 항상 키의 위치가 변하기 때문에 패스워드를 알아내는 것이 어렵지만 하나의 문자를 입력할 때마다 2회의 버튼 터치가 필요한 단점이 있다.

그림 2. 그룹화된 키를 갖는 키패드
Figure 2. Keypad with grouped keys

qwerty 키패드와 마찬가지로 숫자 키패드에서의 패스워드 추측 공격에 대응하기 위한 연구들도 활발히 진행되어오고 있다[10, 11]. 국내에서 현재 대표적으로 사용되고 있는 보안 숫자 키패드로는 <그림 3>과 같이 키 사이에 공백을 갖는 숫자 키패드이다.

그림 3. 공백을 갖는 숫자 키패드
Figure 3. Numeric keypad with spaces

공백을 갖는 숫자 키패드는 매번 실행될 때마다 공백이 임의의 위치에 배치되어 각각의 키들이 배치되는 위치가 변경되도록 한다. 하지만 공백을 임의의 위치에 배치하는 보안 키패드는 특정키가 특정 위치에 배치될 확률들이 서로 다르기 때문에 사용자의 패스워드 입력을 지속적으로 감시하는 경우에 패스워드의 유추가 가능하다는 문제가 있다[12, 13]. 특히 <그림 3>에서 사용자가 패스워드를 입력할 때 1행 1열을 터치하는 경우에는 패스워드에 '1' 이 포함되어 있다는 사실이 노출되기 때문에 보안상 매우 취약하다고 할 수 있다. 또한, <그림 3>에서와 같이 숫자키가 배치될 때, 사용자가 기존에 패스워드를 '1234'로 설정하였다고 가정해보자. 이 경우, 패스워드 '1234'를 입력할 때 단 한 번의 패스워드 입력으로 공격자에게 패스워드가 노출되는 문제가 있다.

공백을 갖는 숫자 키패드와 함께 널리 사용되고 있는 랜덤 키패드는 <그림 4>와 같이 모든 숫자키를 랜덤한 위치에 배치하여 공격자에게 패스워드가 노출되는 것을 막는다. <그림 5>는 공백을 랜덤 키패드에 추가한 형태이다.

랜덤한 위치에 숫자키가 배치될 경우에는 공백만 추가된 키패드들과 달리 모든 숫자키가 배치되는 위치의 확률이 같고, '1234'와 같이 패스워드를 연속적인 숫자로 설정하더라도 공격자는 패스워드를 추측할 수 없다. 하지만, 이 키패드는 사용자가 '1111'과 같이 동일한 숫자로 패스워드를

설정하는 경우 보안상 매우 취약하다. 만일, 사용자가 패스워드를 '8888'로 설정하였다고 가정할 때, <그림 4>의 경우 사용자는 1행 1열을 4번 터치하게 되며, 공격자는 같은 키를 4번 터치했다는 사실을 통해, '0000'부터 '9999'까지 최대 10회의 입력으로 인증을 통과할 수 있다는 문제가 있다.

그림 4. 랜덤 키패드
Figure 4. Randomized keypad

그림 5. 공백을 갖는 랜덤 키패드
Figure 5. Randomized keypad with spaces

이외에도 패스워드 추측 공격에 대응하기 위해 스마트 워치를 이용하거나 키패드의 누름 시간에 따라 입력되는 키 값을 상이하게 하는 등의 다양한 방법으로 연구가 진행되고 있다[14-18].

3. 보안 숫자 키패드

본 장에서는 앞서 살펴본 키패드들의 보안 취약성을 개선한 키패드를 구현하고 이를 평가한다.

3.1 키패드 구현

<그림 5>의 랜덤 키패드에서 동일한 번호로 구성된 패스워드는 공격자에게 쉽게 노출될 수 있다. 이러한 취약점을 보완하기 위해 키를 터치할 때마다 전체 키들의 위치를 뒤섞는 방법을 선택할 수 있다. 하지만 키를 터치할 때마다 전체 키들의 위치가 뒤섞여 배치될 경우, 패스워드에 해당하는 키를 매번 찾아서 터치해야 하기 때문에 많은 시간이 소요될 수 있다.

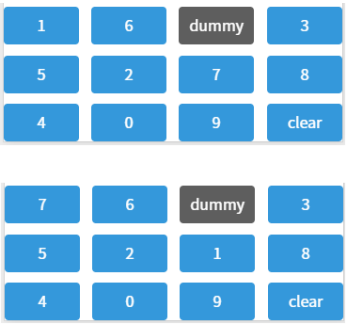

그림 6. 제안된 키패드
Figure 6. Proposed keypad

<그림 6>의 상단 이미지는 본 논문에서 제안하는 키패드를 처음 실행했을 때를 나타낸다. <그림 5>와 비슷하지만 제안된 키패드는 공백 대신 더미 키를 하나 보유하고 있다. 또한, 특정 키를 터치하면 해당 키는 임의의 다른 키와 위치가 교환된다. 예를 들어, <그림 6>의 상단 이미지와 같이 키패드가 생성되었을 때, 사용자가 '1'을 입력하기 위해 '1'을 터치하게 되면, clear 키를 제외한 나머지 키들 중의 하나와 위치가 교환된다. <그림 6>의 하단 이미지는 상단 이미지에서 사용자가 '1'을 터치하였을 때 '7'과 위치가 서로 교환된 것을 나타낸다. 따라서 '1111'과 같이 같은 숫자로 구성된 패스워드를 입력할 경우 기존 키패드들과 달리 터치해야 할 키의 위치가 달라지게 된다. 따라서 공격자는 같은 숫자로 구성된 패스워드임을 알 수 없다.

현재 스마트폰에서 사용되는 숫자 패스워드는 4자리 혹은 6자리이다. 하지만 6자리 패스워드는 4자리 패스워드와 비교하면 기억하기 어려운 문제로 사용자가 '111111'과 같이 기억하기 쉽지만 취약한 패스워드를 만들게 한다. 이에 제안된 키패드는 사용자가 패스워드를 4자리로 설정하되 터치는 총 6번을 수행하도록 하여 공격자가 4자리 패스워드임을 인지하지 못하도록 한다. 사용자가 6자리 패스워드를 등록하는 방법은 랜덤하게 배치된 키패드를 통해 6자리의 패스워드를 입력한다. 패스워드 등록 시 공격자가 '112288'과 같이 같은 수가 연속으로 나오는 패스워드임을 알아차리지 못하도록 키를 터치할 때마다 다른 키와 위치가 교환된다. 반면, 4자리 패스워드를 등록하기 위해서는 4자리 패스워드를 입력한 후, 나머지 2회에 걸쳐 더미 키를 찾아 터치하여 패스워드를 등록한다. 사용자가 입력한 패스워드가 서버로 전달될 때에는 해시함수에 의한 고정된 길이의 해시값으로 전달되기 때문에 패스워드가 몇 자리로 설정되었는지 유추할 수 없다.

패스워드의 인증 방법은 6자리 패스워드의 경우 6개의 해당 키를 터치하여 인증하며, 4자리 패스워드의 경우에는 4개의 해당 키를 터치한 후 2회에 걸쳐 더미 키를 찾아 터치하여 인증한다. 등록 과정과 마찬가지로 인증 과정에서도 매 키의 터치는 해당키의 위치를 변동시켜 같은 키를 연속으로 입력한다는 사실을 외부로 노출시키지 않는다. 따라서 제안된 키패드는 2.2절에서 기술한 공백이 포함된 키패드와 랜덤 키패드가 갖는 보안상 문제점을 해결할 수 있다.

3.2 제안 키패드 평가

공백을 갖는 숫자 키패드의 경우 <그림 3>에서와 같이 배치된 상황에서 1234와 같은 4자리의 연속된 패스워드를 입력할 때 4개의 키를 터치하게 된다. 이때 다양한 순서로 4개의 키를 터치할 수 있는 경우의 수는 24가지이므로 공격자가 한 번의 시도로 패스워드 인증에 통과할 수 있는 확률은 식 1과 같다. 하지만 최악의 경우 <그림 3>의 상황에서 패스워드가 1111이라고 가정하면, 동일한 키를 4번 터치하기 때문에 터치된 좌표 정보를 통해 한 번의 시도로 패스워드 인증에 통과할 수 있다.

$$P = \frac{1}{4} \times \frac{1}{3} \times \frac{1}{2} \times \frac{1}{1} = 0.041666. \quad (1)$$

기존의 랜덤 키패드의 경우에는 4개의 지문이 인접하여 남는 경우, 4개의 서로 다른 숫자로 구성된 패스워드라는 사실을 알 수 있다. 따라서 공격자가 한 번의 시도로 패스워드 인증에 통과할 수 있는 확률은 식 2와 같다.

$$P = \frac{1}{10} \times \frac{1}{9} \times \frac{1}{8} \times \frac{1}{7} = 0.000198. \quad (2)$$

반면, 최악의 경우와 같이 패스워드가 동일한 숫자로 구성된 경우라면 동일한 키를 4번 터치하기 때문에 위치 정보를 통해 한 번의 시도로 패스워드 인증에 통과할 수 있는 확률은 식 3과 같다.

$$P = \frac{1}{10} = 0.1 \quad (3)$$

하지만 제안 키패드는 임의의 위치에 키를 배치하고 매번 터치된 키의 위치를 다른 임의의 키와 바꾸기 때문에 4개의 지문이 인접하여 남더라도 모든 경우의 수로 공격을 시도해야 한다. 그러므로 공격자가 한 번의 시도로 패스워드 인증에 통과할 수 있는 확률은 식 4와 같다. 또한, 1111과 같이 동일한 숫자로 구성된 패스워드이거나, 서로 다른

숫자로 구성된 패스워드이지만 패스워드 입력 시 하나의 키만 터치하는 상황이 발생하더라도 패스워드 유추가 불가능하기 때문에 모든 경우의 수로 공격을 시도해야 한다.

$$P = \frac{1}{10} \times \frac{1}{10} \times \frac{1}{10} \times \frac{1}{10} = 0.000100. \quad (4)$$

<표 1>은 키패드 별 패스워드 입력 시간을 비교한 것이다. 패스워드 입력 시간은 총 100회의 6자리 패스워드 입력에 대한 평균값을 산출하였다.

표 1. 키패드 별 6자리 패스워드 입력 시간
Table 1. Time required to enter 6-digit password for each keypad

키패드	6자리 패스워드를 입력하는데 걸린 시간
공백을 갖는 숫자 키패드	2.42초
공백을 갖는 고정 랜덤 키패드	2.96초
제안 키패드	4.26초

공백을 갖는 숫자 키패드는 키의 위치가 순차적으로 배치되어 있으며 매 입력 시 키의 위치가 변하지 않기 때문에 패스워드를 입력하는데 걸리는 시간이 가장 적게 걸렸다. 공백을 갖는 고정 랜덤 키패드의 경우에는 키가 랜덤한 위치에 배치되기 때문에 순차 키패드와 비교하여 약 0.54초가 더 걸렸다. 마지막으로 제안 키패드는 매 터시 시 터치된 키와 다른 키의 위치가 교환되기 때문에 입력 키의 식별 시간이 더 걸리는 문제로 고정 랜덤 키패드와 비교하여 약 1.3초가 더 걸렸다.

제안 키패드는 입력 시간이 기존 보안 키패드와 비교하여 1.3초에서 1.84초까지 더 걸리는 단점을 가지고 있다. 하지만 기존 키패드들은 특정 상황에서 패스워드 추측 공격에 매우 취약한 문제점이 있다. 제안 키패드는 기존 키패드들의 보안상 문제점을 개선하였기 때문에 입력 시간이 더 걸리는 문제는 안전성 강화로 상쇄될 수 있다.

4. 결 론

스마트폰은 전자결제, 주식, 모바일 뱅킹에 이르기까지 현대 시대에 없어서는 안 될 휴대용 필수품이 되었다. 하지만 언제 어디서든 사용할 수 있는 스마트폰은 구글 글래스를 악용하는 공격자의 표적이 될 수 있으며, 모션 센서를 악용하는 악성 앱에 의해 패스워드가 유출될 수 있는 문제가 있다. 이에 대응하기 위해 많은 연구가 진행되어 왔으며, 국내에서는 랜덤 숫자 키패드와 공백이 포함된 숫자 키패드가 가장 많이 사용되고 있다. 하지만 이러한 숫자 키패드들은 같은 숫자로 구성된 패스워드 입력 시 쉽게 노출될 수 있다는 문제점을 가지고 있다.

본 논문에서 제안한 키패드는 같은 숫자로 구성된 패스워드가 공격자에게 쉽게 노출되지 않도록 터치된 키를 랜덤한 위치로 이동시킨다. 따라서 같은 숫자를 연속으로 입력하는 경우, 같은 위치를 터치하는 것을 피할 수 있어 악성 프로그램이나 구글 글래스를 사용하는 공격자의 패스워드 추측 공격에 안전하다. 또한, 6자리 패스워드를 기억하기 부담스러운 사용자는 단지 4자리 패스워드만을 기억하면서 6자리 패스워드처럼 사용하는 것이 가능하므로 편이성 제공은 물론 안전성을 유지할 수 있다.

References

[1] 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.

[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] A. J. Aviv, B. Sapp, M. Blaze, and M. M. Smith, *Practicality of accelerometer side channels on smartphones*, Proceedings of the 28th Annual Computer Security Applications Conference, pp. 41-50, 2012

[4] 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.

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

[8] I. S. Kim, and J. M. 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] I. S. Kim, and J. M. Choi, *Secure keypad against password guessing attacks with accelerometer and gyroscope sensors*, Journal of Knowledge Information Technology and Systems, Vol. 9, No. 4, pp. 483-491, 2014.

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

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

[12] Y. H. 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.

[13] D. H. Lee, D. H. Bae, S. R. Yoo, J. Y. Chae, Y. H. Lee, and H. G. Yang, *Security analysis on the keypad for smartphones*, Review of KIISC, Vol. 21, No. 7, pp. 30-37, 2011.

[14] P. S. Teh, N. Zhang, A. B. J. Teoh, and K. Chen, *A survey on touch dynamics authentication in mobile devices*, Computer & Security, Vol. 59, pp. 210-235, 2016.

[15] T. Y. Nguyen, N. Sae-Bae, and N. Memon, *DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices*, Computer & Security, Vol. 66, pp. 115-128, 2017.

[16] H. J. Seo, and H. W. Kim, *Design of security keypad against key stroke inference attack*, Journal of the Korea Institute of Information Security & Cryptology, Vol. 26, No. 1, pp. 41-47, 2016.

[17] Y. J. Choi, A. H. Cho, and S. H. Lee, *A numeric security keypad using two fundamental arithmetic operations and connection between smart watch and smart phone*, Proceedings of the Korean Institute of

Information Scientists and Engineers, pp. 1926-1928, 2017.

[18] J. S. Song, M. W. Jung, J. I. Choi, and S. H. Seo, *Proposal and implementation of security keypad with dual touch*, KIPS Transactions on Computer and Communication Systems, Vol. 7, No. 3, pp. 73-80, 2018.

키 터치로부터 패스워드를 추측하는 공격에 안전한 숫자 키패드

김익수

숭실대학교 컴퓨터학부 부교수

요 약

현재 스마트폰은 전자결제, 주식, 모바일 뱅킹과 같은 다양한 온라인 서비스에 이용되고 있다. 지금까지 스마트폰의 패스워드 입력 시 발생할 수 있는 공격에 대응하기 위해 많은 연구가 진행되어왔다. 현재 대중적으로 사용되고 있는 보안 숫자 키패드는 기존 키패드의 보안성을 개선하기 위해 키 사이사이에 공백을 추가하거나 키의 순서를 뒤섞어 배치한다. 공백을 추가하는 방법은 터치된 키의 위치가 쉽게 노출되며, 키의 순서를 뒤섞는 방법은 패스워드가 같은 숫자로 구성되었을 때 공격자에게 쉽게 노출될 수 있다는 문제가 있다. 본 논문에서는 스마트폰에서 패스워드를 입력할 때 발생 가능한 패스워드 추측 공격에 대응하는 안전한 숫자 키패드를 제안한다. 제안하는 키패드는 키의 순서를 뒤섞어 배치하고, 같은 숫자로 구성된 패스워드가 공격자에게 쉽게 노출되지 않도록 터치된 키를 랜덤한 위치로 이동시킨다. 그 결과 사용자가 같은 숫자를 입력할 때 같은 위치를 터치하는 것을 피할 수 있다. 따라서 제안된 키패드는 패스워드를 입력할 때 발생하는 패스워드 추측 공격에 강인하다.

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 associate professor in the School of Computer Science and Engineering at Soongsil University since September 2009. His research interests include system security, network security, and blockchain.

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