JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 5: 613~621, May 2019

Flexible Keypad를 활용한 보안 구현

안규황[1] · 권혁동[1] · 권용빈[1] · 서화정[2*]

Security Implementation using Flexible Keypad

Kyuhwang An[1] · Hyeokdong Kwon[1] · Yongbin Kwon[1] · Hwajeong Seo[2*]

[1]Graduate Student, Department of IT Engineering, Hansung University, Seoul 02876, Korea
[2*]Assistant Professor, Department of IT Engineering, Hansung University, Seoul 02876, Korea

요 약

시중에 가장 많이 보급 된 도어락의 경우 1차원적 문제로 가장 많이 사용하는 영역이 닳아 특별한 공격방법을 사용하는 것이 아닌 닳은 영역으로 하여금 비밀번호 유추를 가능하게 한다. 이를 해결하고자 번호를 섞어 무작위로 표출하는 키패드 등 다양한 방법들이 소개되고 있지만 이 역시 완벽하게 안전하지 못 하다. 여태까지 나온 모든 해결법의 공통점은 키패드를 누르는 영역이 고정되어 있다는 점이다. 본 논문에서는 그 점을 역으로 생각하여 키패드 전체 영역 안에 전체 영역보다 작은 새로운 영역을 만들어 새로운 영역의 키패드를 무작위하게 움직이게 하여 비밀번호를 유추하지 못 하게 한다. 본 기법을 사용할 경우 키패드의 번호는 그대로 둠에도 불구하고 shoulder surfing attack 등이 불가능하여 새로운 유형의 키패드를 최초로 제안한다.

ABSTRACT

In the case of door locks most widely used in the market, the most used area as a one-dimensional problem is worn out, and a worn area which does not use a special attack method enables password guessing. To solve this problem, various methods such as a keypad for randomly displaying numbers are introduced, but this is also not completely safe. The common feature of all the solutions so far is that the keypad area is fixed. In this paper, we consider that point in reverse and create a new area smaller than the entire area in the entire area of the keypad, making the keypad of the new area move randomly, thereby preventing the password from being deduced. When using this technique, a new type of keypad is proposed for the first time because of the impossibility of a shoulder surfing attack even though the number of keypad is left as it is.

키워드 : 어깨너머 공격, 중간 탈취 공격, 추정 공격, 키패드, PIN

Key word : Keypad, Key logging attack, PIN, Shoulder surfing attack, Smudge attack

Received 26 January 2019, **Revised** 6 February 2019, **Accepted** 8 March 2019

*** Corresponding Author** Hwajeong Seo(E-mail:hwajeong84@gmail.com, Tel:+82-2-760-8033)
Assistant Professor, Department of IT Engineering, Hansung University, Seoul 02876, Korea

Open Access http://doi.org/10.6109/jkiice.2019.23.5.613 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

2000년대가 넘어서부터 집집마다 열쇠로 집 대문을 여는 형식이 아닌 터치 키패드를 사용하는 도어락 형식으로 대다수의 세대들이 교체되었다. 뿐만 아니라 스마트폰이 거의 모든 사람들에게 보급됨에 따라 터치 키패드에 비밀번호를 입력하는 행위는 사람들에게 더 이상 새로운 기술이 아닌 주변 일상에 항시 있는 기술로 받아들여지고 있다.

터치 키패드는 많은 사람들에게 편리성을 주지만 똑같은 비밀번호로 오래 사용했을 경우 그림 1과 같이 비밀번호가 눌린 자리의 터치 패드만 닳는 현상이 발생해 외부 사람들로 하여금 쉽게 비밀번호를 유추할 수 있게 만들고, 심지어는 닳는 현상이 발생하지 않더라도 지문 흔적으로 숫자를 조합하여 도어락을 풀고 침입하는 경우[1]도 발생하였다.

[1]과 같은 악의적 행위가 발생할 수 있는 이유는 터치 패드에 비밀번호 값이 고정되어 있어, 그 고정 된 값으로 하여금 유추를 할 수 있기 때문이다. 이러한 문제점을 해결하기 위해 다양한 방법들이 제시되었다. 첫 번째로 많은 시중 은행에서 공인 인증서 로그인을 할 때 사용하는 방법인 숫자들 사이에 공백을 넣는 기법과 두 번째로 숫자의 위치를 무작위로 퍼뜨리는 방법이다. 그러나 첫 번째의 경우 기존의 연구 논문에서 Brute force attack[2]과 key logging attack[3]을 이용하여 키 유추가 가능함을 증명하였고, 두 번째의 경우 Brute force attack과 Shoulder surfing attack[4]이 가능함을 선보였다.

기존의 제시 된 위에서 소개한 방법들의 공통점은 바로 터치하는 위치는 고정된 채 숫자만 바뀐다는 것이다. 해커들은 이 점을 놓치지 않고 바뀌지 않는 터치 위치 값을 활용하여 암호 키를 획득하는데 활용하고 있다. 따라서 본 논문에서는 기존의 제안 된 기법들의 공통점인 터치하는 키의 위치가 고정된 점을 역으로 활용하여 최초에 비밀번호를 누를 때 마다 새로운 위치에 비밀번호 입력 키보드가 활성화 되는 기법을 최초로 제안하여 위에서 언급 한 공격들에 대하여 완벽히 방어하는 더욱 안전한 보안 키패드를 제안하고자 한다.

Fig. 1 Keypad had some damaged from long time usage

본 논문의 구성은 다음과 같다. 2장에서는 보안 키패드 제안을 위한 어떠한 종류의 보안 키패드가 제안되었었는지 관련 연구에 대해 살펴 볼 것이며, 3장 제안 기법에서는 본 논문에서 제안하는 기법에 대한 설명과 어떻게 구현하였는지 설명할 것이다. 4장에서는 본 논문에서 제안한 기법과 여태 제안 된 보안 키패드들에 대한 성능평가가 이루어질 것이며 이와 함께 본 논문 제안 기법에 대한 일반 시민들의 평가를 알아볼 것이다. 마지막으로 5장에서 결론을 맺도록 하겠다.

Ⅱ. 관련 연구 동향

2장에서는 1장에서 언급한 보안 키패드를 위한 가장 기초적인 2가지 기법 외에 보다 심화된 연구는 무엇이 있는지 알아보도록 한다.

2.1. 테트리스 형태 보안 키패드[5]

해당 논문에서는 기존 키패드의 문제점인 같은 크기와 같은 모양으로 배치하여 공백을 통한 위치 변경을 사용한다는 점에 따라 터치 위치 정보를 가져오기 때문에 어깨너머 공격에 취약한 점을 보완하기 위해 키패드를 각기 다른 크기와 다른 모양으로 생성 후 배치함으로써 터치한 위치 정보를 통해 정보를 유추하기 어렵게 하고자 한다.

기존 키패드를 기준으로 가로, 세로 2등분하여 13개의 형태로 변경하고 이를 테트리스 형태로 연결하는 보안 키패드를 제안하며 13개의 키패드는 그림 2와 같다.

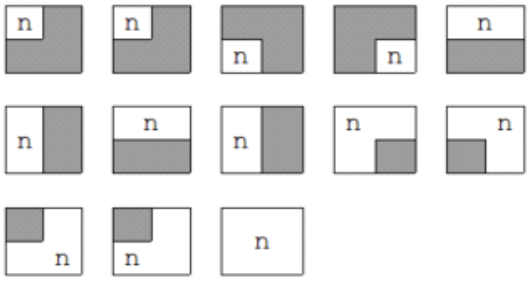

Fig. 2 The Number of cases

현 키패드는 터치 위치 정보를 알아도 유추하기 어려우며 마찬가지로 어깨 너머 훔쳐보는 공격도 가능하지만 기존의 정렬 된 키패드에 비해 기존보다 어려운 면모를 보여준다. 그림 3은 영문자 입력에 적용한 사례이다. 마찬가지로 공백을 통해 키패드의 위치를 변경하는 것은 공백을 기준으로 좌우의 키패드 배열순서는 바뀌지 않기 때문에 위치 정보가 탈취될 경우엔 사용자의 입력 일부를 획득할 수 있다. 테트리스 형태의 배치는 위치 정보를 획득 하더라도 해당 위치의 문자가 기존 키패드의 문자와 동일한지 알 수 없기 때문에 입력을 유추하기 어렵다.

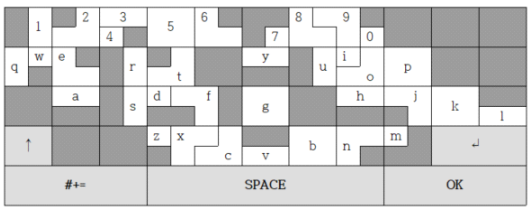

Fig. 3 Example of secure keypad with tetris type

2.2. 이중 터치를 활용한 보안 키패드 제안 및 구현[6]

해당 논문에서 제안하는 키패드는 기존의 키패드와 생김새가 다르다. 기본적으로 일반적으로 사용하는 키패드의 경우 하나의 버튼에 하나의 숫자를 입력하게 만들었으나, 이중 터치를 이용한 보안 키패드의 경우 하나의 버튼 자리에 2개의 숫자가 그림 2와 같이 들어있다.

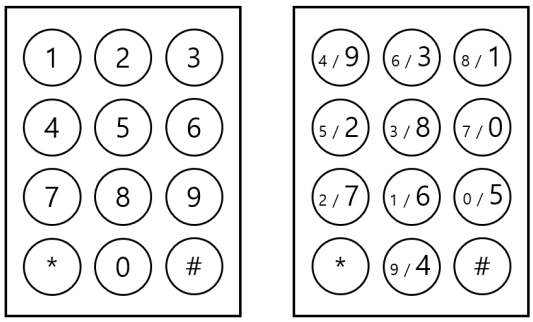

Fig. 4 Left) Current default keypad
Right) using double touch security keypad

그림 4에서와 같이 기존의 키패드 같은 경우에는 키패드를 누를 때 걸리는 시간에 구애 받지 않고 짧게 누르든 길게 누르든 상관없이 한 개의 숫자만 눌리게 된다. 그러나 본 논문에서 제안하는 기법의 경우 short touch와 long touch로 터치하는 방식을 두 가지로 나눴으며 그에 따라 하나의 키 당 두 가지의 종류로 입력할 수 있게 만들었다. 이 경우 하나의 위치에 하나의 숫자 값만 존재하는 것이 아니기 때문에 어깨너머 공격으로부터 안전함을 보이고 있다.

2.3. 스마트 디바이스 상의 안전한 개인식별번호 입력 연구 동향[7]

개인 식별 번호(Personal Identification Number, PIN)는 숫자로 이루어진 짧은 번호를 말하는 것으로, 은행 ATM, 디지털 도어락, 스마트 디바이스 등에서 사용자 인증을 위해 널리 쓰이고 있다. 이 PIN을 입력하기 위한 전통적인 키패드 방식은 엿보기나 녹화 등의 공격에 약하고 이를 방지하기 위한 설계 방식들도 Brute force attack 등에 취약할 수 있다. 어깨너머 공격 방식의 방지를 위하여 제안된 Challenge-response 방식의 경우 사용자에게 Challenge를 주고, 사용자는 이 Challenge 정보와 자신이 알고 있는 정보(PIN)를 조합하여 응답을 도출하는 방식이다. 이러한 방식은 같은 PIN일 지라도 입력하는 방식이 매 번 다르기 때문에 어깨너머 공격이나, 손자국(smudge)공격에 대응 할 수 있는 장점이 있다. 하지만 최근 카메라의 소형화와 초소형 카메라에 쉽게 접근할 수 있는 환경을 고려한다면 위험하다. 이에 대한 대응으로서 사용자의 응답이 유일한 PIN에 대응하지 않도록 하는 방법이 있다. 예를 들어 BW PIN 방식에서

한 숫자당 Challenge-response 쌍을 두 번만 진행하는 방법이 있다. 이는 응답 시간도 줄일 수 있다는 장점이 있으나, Brute force attack 대입 공격의 성공 확률을 높인다는 문제점을 가진다. 이렇듯 녹화되고 있다는 전제의 어떠한 상황에서도 Brute force attack 대입 공격 방식과 녹화 공격에 대한 안전성은 서로 반비례함이 증명된 바가 있다. 이를 극복하기 위해선 공격자로 하여금 챌린지 또는 응답을 관찰하지 못하게 하는 방법을 고려할 수 있다. 공격자가 관찰 가능한 시각 정보 채널 이외에 다른 안전한 채널을 활용하는 방법인데, 대표적으로 진동정보, 소리 채널들이 있다. 그렇지만 이러한 부가 채널을 이용하는 방식이 항상 안전한 것은 아니다. 입력시간을 조사하거나, 여러 세션을 녹화하여 조사하는 방식을 통해 PIN이 복원될 수 있다. 따라서 챌린지가 PIN에 무관하게 선택되고 시간 또한 독립적으로 분포되도록 하는 것이 중요하다. 이외에도 brain-computer interface, eye-tracker, sweet spot등의 방법들도 존재하나 전용 디바이스의 사용이 필요하기에 범용으로 이용되기엔 어려운 단점이 있다. 따라서 이러한 PIN들의 보안에는 중간점이 필요하며, PIN의 분포가 고르지 않다는 점 또 한 고려해야 할 대상이다. 기존의 시스템을 수정하는 비용과 사용자의 편의성 또한 고려 대상이다. 이러한 문제점들을 최소화하기 위해서 PIN의 공간은 유지한 채 입력 방식만을 다양화하는 것이 바람직할 것이다.

Ⅲ. 제안 기법

본 논문에서 제안하는 기법에 대하여 실제 구현과 테스트를 완료하였으며, 구현 환경은 표 1과 같다. 또한 제안 기법에 대한 구현영상[8]을 youtube에 올려놨으며[1], 해당 코드를 github[9]에 올려 open source화 하였다[2].

Table. 1 The information of experiment environment

Device	Nexus 5X
OS	Android
Version	API 28
Display	420dpi

1) https://github.com/kyu-h/CyberSecurity_Flexible_PIN
2) https://youtu.be/wCfYr9s0lDM

터치패드를 활용한 PIN 입력 방식은 편리성을 제공하지만 비밀번호가 눌린 자리의 터치 패드만 닳는 현상이 발생해 외부 사람들로 하여금 쉽게 비밀번호를 유추할 수 있게 만들고, 심지어는 닳는 현상이 발생하지 않더라도 지문으로 숫자를 조합하여 도어락을 풀고 침입하는 경우도 발생한다. 이러한 악의적 행위가 발생할 수 있는 이유는 터치 패드에 비밀번호 값이 고정되고 그 고정 된 값으로 하여금 유추가 가능하기 때문이다.

해당 문제점을 해결하기 위해 다양한 방법들이 제시되었다. 첫 번째로 숫자들 사이에 공백을 넣는 방법, 두 번째로 숫자를 랜덤 값으로 퍼뜨리는 방법 이외에도 많은 방법들이 제시되었지만 첫 번째 같은 경우 Brute force attack과 key logging attack이 가능하며, 두 번째 경우는 Brute force attack과 Shoulder surfing Attack이 가능하다. 따라서 본 논문에서는 이러한 공격들이 가능하지 않은 새로운 기법을 제안한다.

현재 키패드를 보면 숫자를 입력하는 영역이 고정되어 있다. 이 고정 된 영역으로 인해 그림 1과 같이 1차원적으로는 많이 사용하는 부분이 닳게 된다. 또한 현재 시중에서 가장 많이 사용하는 키패드의 경우 그림 5의 왼쪽과 같이 손의 움직임에 따라 어떠한 번호가 눌리고 있는지 유추가 가능하여 전체 숫자의 조합을 해보지 않더라도 비밀번호를 획득할 확률을 현저하게 줄일 수 있다.

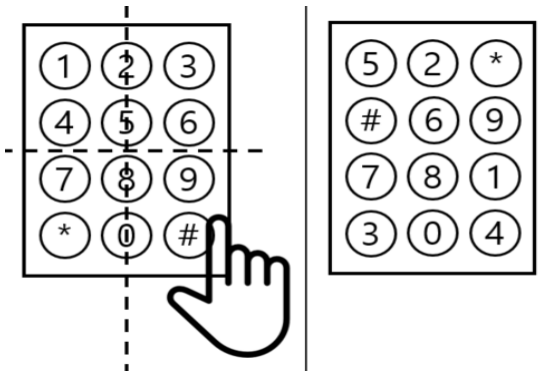

Fig. 5 Left) example of shoulder surfing attack,
Right) example of prevent shoulder surfing attack

이를 해결하고자 그림 5의 오른쪽과 같이 숫자를 랜덤하게 섞어서 보여 지는 키패드도 제안이 되었지만 숫자 값을 무작위로 섞는 경우에는 사용자가 한눈에 번호를 파악하기 힘들고 비밀번호를 입력하는데 시간이 걸

린다. 이를 방지하고자 숫자 값은 섞지 않으면서 보안에 뛰어난 새로운 키패드를 제안한다.

여태까지 나왔던 제품들의 공통점은 숫자 입력 영역이 고정되어 있다는 점이다. 이를 역으로 생각하여 숫자 입력 영역을 구동 시킬 때마다 변화를 주도록 한다. 제안하는 기법에는 그림 6과 같이 빨간색 영역인 전체 영역이 존재하고 그 안에 새로운 부분인 파란색 영역이 존재한다. 파란색부분 영역 안에서는 숫자를 입력하는 키패드가 존재하고 해당 영역은 빨간색 영역 안에서 유동적으로 이동한다. 또한 파란색 키패드를 기준으로 좌우 모서리 상 하단에 부분적인 키패드가 추가 생성되며 해당 영역에 보이는 숫자를 눌렀을 경우에도 해당 번호가 입력이 된다. 현재 그림 8에는 숫자가 눌린 모습을 보여진다.

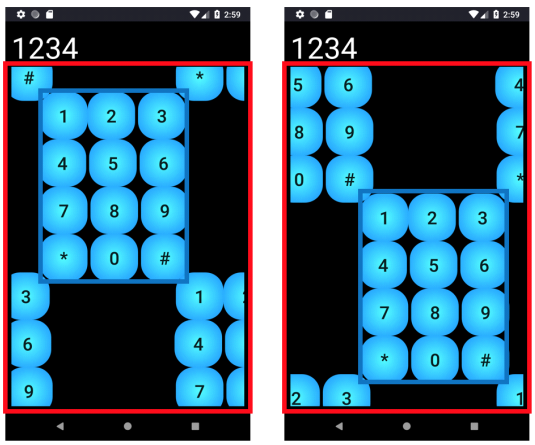

Fig. 6 Blue box can located every section in red box and the number of blue box changed every position

구체적인 구조는 그림 7과 같다. 사용자의 손의 움직임에 따라 번호를 유추하는 공격인 shoulder surfing attack에 안전하다. 앞에서 언급했던 그림 5의 random하게 숫자를 섞는 행위는 shoulder surfing attack을 막을 수 있는 방법은 확실하지만 사용자가 사용할 때 마다 매번 다른 영역에 다른 숫자 값을 주기 때문에 사용하는데 큰 불편함이 따른다. 그러나 본 제안 기법을 활용하면 키패드를 섞지 않더라도 키패드의 위치가 계속 변경되고, 추가적인 4개의 부분적 키패드로 인하여 공격자의 Shoulder surfing Attack에 강하다.

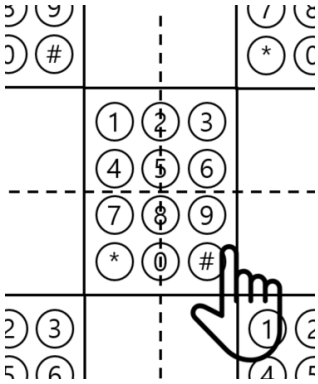

Fig. 7 Suggest technique

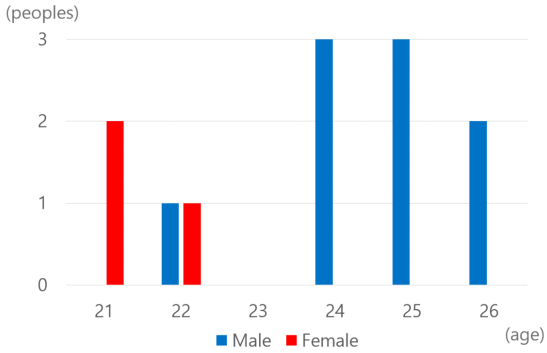

Fig. 8 The information of survey experimenter

또한 기존에 사용되고 있는 키패드를 누를 때 발생하는 소리를 들어보면 특정 숫자에 고유한 소리가 발생함을 알 수 있으며 이는 sound shoulder surfing attack의 가능성을 지닌다. 해당 공격에 대해 안전하기 위해 특정 영역의 숫자를 눌렀을 경우 모두 동일한 소리가 발생하게 만들었다.

본 제안 기법에 대한 보안 성능 테스트를 위하여 기존에 사용 된 키패드에 다양한 공격을 통해 키를 유추한 방법을 본 제안 기법에 동일하게 적용해 보았으며, 해당 논문을 작성한 연구원들 간의 테스트가 아닌 본교 12명의 학생들에게 본 제안 기법을 사용한 보안 키패드는 실제로 구현 및 테스트를 통해 기존의 보안 키패드보다 뛰어난 보안성을 입증하였으며 본교 학생들의 정보는 그림 8과 같으며, 그 결과는 4장에서 확인해보겠다.

Ⅳ. 성능 평가

본 장에서는 앞에서 언급한 공격들에 대한 기존 키패드의 보안성 테스트와 본 논문에서 제안하는 기법은 해당 공격들에 대해 기존 키패드들 보다 얼마나 뛰어난 보안성을 가지고 있는지 알아보겠다.

4.1. Smudge attack

일반적인 키패드의 경우 4자리 비밀번호를 입력하게 되면 4곳에 지문이 남겨지게 되므로 이 경우에 비밀번호는 4! = 24가지의 조합을 생각할 수 있으며 중복되는 번호가 있을 경우에는 지문이 남는 위치가 줄어들기 때문에 조합의 수는 더욱 적어지게 되어 공격자가 더 빠르게 비밀번호를 유추할 가능성이 생긴다.

하지만 제안한 기법의 키패드는 입력 시도마다 키패드의 위치가 변경되기 때문에 4자리의 같은 비밀번호를 입력해서 4곳에 지문이 남더라도 다음 입력 시도에는 키패드의 위치가 변경되기 때문에 지문이 남겨진 위치의 숫자가 이전 숫자와 동일함을 보장할 수 없다. 또한 동일 비밀번호를 계속해서 입력하더라도 계속해서 키패드의 위치가 바뀌기 때문에 지문이 남는 위치가 일정하지 않기 때문에 공격자가 지문을 획득해도 균일한 위치에 반복적으로 찍힌 지문이 아닌 여러 장소에 산발적으로 찍힌 지문을 얻기 때문에 비밀번호를 유추하는데 사용하기 어렵게 된다.

4.2. Key logging attack

4.2장에서는 제안된 키패드의 key logging attack에 대한 안전성을 이전의 평범한 키패드(그림 5 left)와 랜덤셔플 키패드(그림 5 right)와 비교 해 봄으로써 검증해 볼 것이다. 기존의 평범한 키패드와 랜덤셔플 키패드의 경우 키로깅 공격에 취약하다. 평범한 키패드의 경우에는 눌려질 수 있는 좌표가 3x4 패드의 경우 12개 구역으로 한정적이다. 따라서 공격자 입장에서는 사용자가 누를 좌표를 알고 있다면, 그 좌표에 해당하는 구역을 확인하고 있다가 그 좌표의 데이터를 갈취해 오는 것이 가능하다. 그리고 이것은 랜덤셔플 키패드의 경우에도 동일하다. 하지만 제안된 키패드의 경우에는 숫자가 올 수 있는 구역이 더욱 넓어지는 것과 동시에 패드자체의 위치가 매번 랜덤하게 이동하기 때문에 공격자가 얻어낸 좌표와 사용자가 입력할 좌표는 연관이 없게 된다. 예를들면 사용자의 비밀번호가 '1780'라고 한다면, 제안된 키패드로의 처음 시행 시 해당하는 좌표는 <2,3>, <5,1>, <3,5>, <3,6> (그림 9 left)이었고 이를 탈취 당했다고 하자. 하지만 다음 입력 시 공격자가 <2,3>, <5,1>, <3,5>, <3,6> 을 탈취하고 확인한다 하더라도 사용자의 키에 해당하는 숫자들의 좌표 즉 입력할 숫자들의 다음 좌표는 <3,2>, <3,4>, <4,4>, <1,1> (그림 9 right)으로 바뀌게 된다. 그리고 이 좌표들은 매 시도 때마다 랜덤하게 설정 될 것이다. 따라서 공격자는 키로깅을 통해 사용자의 비밀번호를 얻어내는 것이 불가능하게 된다. 이는 제안된 키패드가 기존의 평범한 키패드와 랜덤 셔플 키패드보다 높은 안정성을 가짐을 알 수 있다.

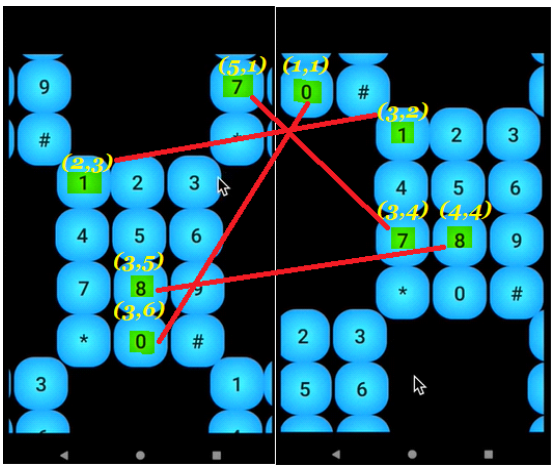

Fig. 9 How to protect key logging attack

4.3. Shoulder surfing attack & Sound shoulder surfing attack

4.3장에서는 shoulder surfing attack에 대한 안전성 실험을 위하여 두 가지로 나누어서 진행할 예정이다. 첫 번째로 shoulder surfing attack이 가능한 키패드 모델인 가장 기초적인 키패드와 본 논문에서 제안하는 기법과 비교 분석을 진행할 것이며, 두 번째로 random number keypad의 경우 본 논문에서 제안하는 기법과 마찬가지로 shoulder surfing attack이 동일하게 불가능하다. 따라서 어느 기법이 사용자 측면에서 효율적으로 편리하게 사용할 수 있는지 비교 분석할 것이며, 마지막으로 Sound shoulder surfing attack은 3가지 기법에 대하여 동일하게 비교 분석한다.

첫 번째로 기본 키패드와 본 논문에서 제안하는 flexible 키패드를 비교 분석하면, 키패드를 손의 입력 위치에 따라 그림 10의 왼쪽과 같이 4가지 영역으로 나눌 수 있다. 이를 표로 나타내면 표 2와 같다.

Shoulder surfing attack은 손의 움직임에 따라 비밀번호를 유추하는 공격 방법으로 비밀번호가 만약 '1379'와 같이 멀리 떨어진 영역의 비밀번호일 경우 더욱 더 shoulder surfing attack에 취약하다. '1'을 입력하는 손의 위치와 '9'를 입력하는 손의 위치는 확연하게 다르기 때문이다. 입력 비밀번호는 0~9까지 10개의 숫자로 구성되어 있어 brute force attack을 할 경우 최악의 경우 한 글자당 $\frac{1}{10}$의 확률로 $(\frac{1}{10})^4$만큼 진행해야한다. 그러나 shoulder surfing attack은 그림 9의 왼쪽과 같이 4개로 나누어진 영역을 토대로 번호를 어느 정도 유추가 가능하다. 예를 들면 손이 2번째 영역으로 움직였을 경우엔 '1, 4, 7, 8, 9, 0'과 같은 번호는 눌릴 확률에서 제외하고 나머지 값들만 생각하면 된다. 따라서 '1379'일 경우에는 $\frac{1}{4}*\frac{1}{4}*\frac{1}{3}*\frac{1}{3}$의 확률을 갖게 되고 기존의 전수조사 확률인 $(\frac{1}{10})^4$보다 엄청나게 낮은 확률로 비밀번호 유추가 가능하다.

본 제안 기법의 키패드의 경우 그림 9의 오른쪽과 같이 대표적인 모습을 보여주기 위해 main keypad를 중앙에 두고 진행하였지만 키패드를 구동시킬 때 마다 main keypad의 위치가 달라져 1, 2, 3, 4 영역에 추가적으로 생기는 부분적인 키패드의 모습이 항상 바뀌게 된다. 따라서 '1379'로 동일하게 진행을 하여도 각 번호를 누를 수 있는 키가 4개 중 최소한 2개의 영역에 존재하여 어떤 번호를 눌렀는지 유추가 불가능하게 되며 심지어 5, 8과 같은 경우에는 3가지 영역에 존재하게 되어, shoulder surfing attack으로는 절대적으로 유추가 불가능하다.

Table. 2 The information of shoulder surfing attack area

	Default Keypad	Flexible Keypad
First part	1, 2, 4, 5	1, 2, 4, 5, 8, 9, 0
Second part	2, 3, 5, 6	2, 3, 5, 6, 7, 8, 0
Third part	8, 9, 0	1, 2, 4, 5, 8, 9, 0
Fourth part	7, 8, 0	2, 3, 5, 6, 7, 8, 0

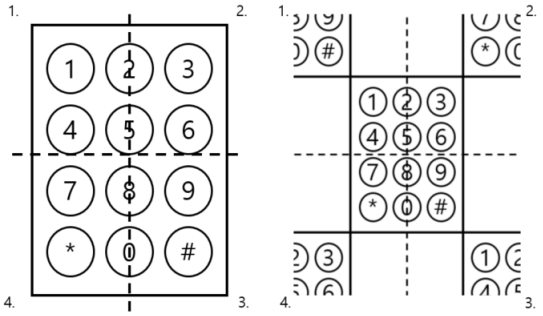

Fig. 10 How to do shoulder surfing attack

Random number keypad 같은 경우 keypad를 작동시킬 때마다 항시 다른 번호가 나오기 때문에 shoulder surfing attack이 flexible keypad와 마찬가지로 불가능하다. 두 가지 기법 모두 shoulder surfing attack에 불가능하여 안전한 방법이라고 한다면 사용자는 보다 편리한 것을 선택하여 사용하기 마련이다. 따라서 실제 실험자를 통해 어떠한 기법이 단시간 내로 비밀번호를 입력할 수 있으며 편리한 기법인지 알아보기 위해 10명의 실험자를 대상으로 '1379'를 눌렀을 때 걸리는 시간을 표 3과 같이 조사해 보았으며 해당 시간은 12명의 평균 시간을 적어두었다.

Table. 3 The time it takes to enter the password is in seconds.

	Required time to input random number keypad	Required time to input Flexible keypad
First attempt	3.690818	3.024818
Second attempt	3.135182	2.999
Third attempt	3.367091	2.701182

본 실험에서도 볼 수 있듯 random number keypad의 경우 키패드를 동작시킬 때마다 비밀번호에 입력 될 번호가 어디에 들어있는지 파악을 해야 하고, 그에 따라 사용자의 불편함이 동반되어 비밀번호를 입력하는데 걸리는 시간이 상당하다. 그러나 flexible keypad의 경우 메인 키패드는 동일하게 존재하나 키패드의 위치 값만 랜덤하게 바뀌는 역할을 주어 사용자 입장에서도 단번에 번호 위치를 파악할 수 있어 일반 키패드와 비슷한 시간 내에 입력이 가능하다.

표 3을 보면 random number keypad는 걸리는 시간이 3초 중반대로 비슷한 시간이 걸림을 보여주었다. 그러나 본 논문에서 제안하는 flexible keypad의 경우 사용자가 사용법을 익힘에 따라 최초의 시도에서는 3.02초에서 단 3번만의 시도 만에 2.7초대로 떨어졌다. Random number keypad의 최대 걸린 시간보다 약 1.37배 빠르고 간편하게 입력할 수 있음을 알 수 있었으며, 본 실험은 단 3번만의 실험 데이터를 기반으로 했지만 더 많은 사용으로 키패드가 익숙해진다면 2배 이상 편리하고 빠른 입력 속도를 낼 것이라 예상한다.

Ⅴ. 결 론

여러 연구원들이 제안한 기존의 키패드는 입력되는 영역에 변화를 주어 그 이전에 제안 된 키패드보다 나은 보안 방법을 제안했지만 본 논문에서 제안하는 기법은 국내에 한 번도 제안된 적 없는 키패드의 위치를 움직이는 방식의 새로운 기법을 제안한다.

키패드의 움직이는 영역으로 인해 번호를 섞지 않더라도 shoulder surfing attack으로부터 완벽하게 보호가 되며, 사용자 입장에서는 한눈에 들어오는 손쉬운 키패드를 사용할 수 있다. 또한 키패드 영역이 고정되어 있지 않기 때문에 key logging attack으로부터 역시 완벽하게 보호가 가능하다.

본 논문에서 제안하는 기법은 앞에서 언급한 4가지 공격들에 대해 모두 안전하며 여태까지 제안되었던 기법 중 가장 안전하다고 할 수 있는 random number keypad보다 약 1.37배 빠르게 비밀번호를 입력할 수 있다. 즉 보안에도 최고 안전하며 사용자 측면에서 빠르고 간편하게 입력이 가능하다. 따라서 본 논문에서는 국내 최초로 제안하는 키패드인 움직이는 키패드 보안 방식을 통해 PIN 보안 분야에 새로운 바람을 불러일으킬 것을 기대한다.

ACKNOWLEDGEMENT

This work was partly supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017 R1C1B5075742) and was partly supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2019-2014-1-00743) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation). This research of Hwajeong Seo was financially supported by Hansung University.

References

[1] OBS News M. “Using the fingerprint trail to unlock the door,” Available : https://www.youtube.com/watch?v=CwA9lSU9ng8

[2] K. Apostol, “Brute-force attack,” Available: https://dl.acm.org/citation.cfm?id=2378515

[3] T. Holz, M. Engelberth, F. Freiling, Learning more about the underground economy: A case-study of keyloggers and dropzones. In *European Symposium on Research in Computer Security*, pages. 1-18. Springer, Berlin, Heidelberg. 2009.

[4] A. H. Lashkari, S. Farmand, D. Zakaria, O. Bin, D. Saleh, “Shoulder surfing attack in graphical password authentication.” Available: https://arxiv.org/ftp/arxiv/papers/0912/0912.0951.pdf

[5] H. J. Mun, Virtual Keypads based on Tetris with Resistance for Attack using Location Information. *Journal of the Korea Convergence Society*. vol. 8, no. 6, pp. 37-44, 2017.

[6] J. S. Song, M. W. Jung, J. I. Choi, S. H. Seo, Proposal and Implementation of Security Keypad with Dual Touch. *KIPS Tr. Comp. and Comm. Sys*. vol.7, no.3 pp. 73-80, pISSN: 2287-5891, 2018.

[7] M. K. Lee, Research Trend of Entering Personal Identification Number on Smart Device. *Korea Institute Of Information Security And Cryptology*. pp. 16-21, 2018.

[8] Flexible Keypad youtube. “Flexible Keypad implementation video” Available: https://youtu.be/wCfYr9s0lDM.

[9] Flexible Keypad github. “Flexible Keypad opensource”
Available: https://github.com/kyu-h/CyberSecurity_Flexible_PIN.

안규황(Kyu-hwang An)

2018년 2월: 한성대학교 IT응용시스템공학과 공학 학사
2018년 3월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 암호구현, IoT 보안, 블록체인

권혁동(Hyeok-dong Kwon)

2018년 2월: 한성대학교 정보시스템공학과 공학 학사
2018년 3월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 블록체인, 암호구현

권용빈(Yong-bin Kwon)

2018년 8월: 한성대학교 IT응용시스템공학과 공학 학사
2018년 9월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 부채널 분석, TEE 프로그래밍

서화정(Hwa-jeong Seo)

2010년 2월 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업
2016년 1월~2017년 3월: 싱가포르 과학기술청
2017년 4월~현재: 한성대학교 IT 융합공학부 조교수
※관심분야 : 정보보호, 암호화 구현, IoT