Journal of the Korea Convergence Society
Vol. 8. No. 6, pp. 37-44, 2017
https://doi.org/10.15207/JKCS.2017.8.6.037

# 위치정보로 비밀정보를 유추할 수 있는 공격에 내성이 있는 테트리스 형태 기반의 보안 키패드

문형진[1*]
[1]성결대학교 정보통신공학부

# Virtual Keypads based on Tetris with Resistance for Attack using Location Information

Hyung-Jin Mun[1*]
[1]Dept. of Information & Communication Engineering, Sungkyul University

**요 약** 모바일 단말기는 터치 스크린 상의 가상 키패드로 비밀번호와 같은 중요 정보를 입력하여 결제 및 인증을 통해 다양한 서비스를 제공한다. 사용자가 모바일 단말기로 입력한 비밀번호를 유추하기 위해 공격자는 사용자의 터치 위치정보를 탈취한다. 구글 글래스를 이용한 훔쳐보기나 어깨너머 공격으로부터 터치된 비밀번호 정보를 알아내거나 탈취된 위치정보를 이용하여 터치한 비밀번호를 유추할 수 있다. 이는 기존 보안 키패드는 손쉬운 입력을 위해 일부 키를 제외하고 거의 정해진 순서대로 같은 크기의 키패드로 같은 문자를 배치하기 때문에 구글 글래스나 어깨너머 공격 등에 취약하다. 보안 키패드를 다양한 모양과 위치를 재배치하므로 보안성을 높일 수 있다.
본 논문은 13가지의 테트리스의 다양한 형태와 크기를 생성하고, 키패드를 이어 붙여서 배치하는 보안 키패드를 제안한다. 보안 키패드는 다양한 모양과 크기를 테트리스 게임처럼 배열하므로 가상 키패드를 다양하게 만들어 공격자가 터치한 위치정보가 알더라도 키패드의 크기를 달라 입력된 비밀정보를 유추하기가 어렵다.

• 주제어 : 보안 키패드, 키패드, 어깨너머공격, 인증, 가상 키패드, 비밀번호

**Abstract** Mobile devices provide various services through payment and authentication by inputting important information such as passwords on the screen with the virtual keypads. In order to infer the password inputted by the user, the attacker captures the user's touch location information. The attacker is able to infer the password by using the location information or to obtain password information by peeping with Google Glass or Shoulder Surfing Attack. As existing secure keypads place the same letters in a set order except for few keys, considering handy input, they are vulnerable to attacks from Google Glass and Shoulder Surfing Attack. Secure keypads are able to improve security by rearranging various shapes and locations.
In this paper, we propose secure keypads that generates 13 different shapes and sizes of Tetris and arranges keypads to be attached one another. Since the keypad arranges different shapes and sizes like the game, Tetris, for the virtual keypad to be different, it is difficult to infer the inputted password because of changes in size even though the attacker knows the touch location information.

• Key Words : Secure Keypads, Keypads, Shoulder Surfing Attack, Authentication, Virtual Keypads, Password

# 1. 서론

ICT 발달이 4차산업을 견인하는 시대가 도래하면서 IT 기반 서비스가 다양해지고 있다. 특히, PC 기반 서비스에서 스마트폰 기반의 서비스로 서비스 형태가 변화하고 있다. PC상에서 발생가능한 공격들이 스마트폰으로 옮겨지면서 공격들이 다양해지고, 직접적인 피해가 양상되고 있다[1,2]. 특히, SNS 등을 통해 관계망을 통한 공격이나 피싱, 파밍, 스미싱과 같은 사회공적인 공격이 급속하게 확장되고 있다[3,4,5,6,7,8,9]. 이는 스마트폰 단말기가 듀얼 코어 이상이 탑재되어 빠른 처리가 되고, 인터넷 역시 3G에서 LTE 사용으로 인해 빠른 접속이 이루어짐에 따라 PC상에서 없던 공격들도 계속적으로 생성되고 있다[10]. 스마트폰과 같은 모바일 단말기에서 이루어지는 공격을 막기 위한 연구들이 꾸준히 진행되고 있다[11,12].

모바일 단말기 사용이 급증하면서 많은 금융서비스에서는 스마트폰을 이용한 금융거래 등에서 안전한 거래를 위해 다양한 방법으로 사용자인증을 하고 있다[13,14,15,16]. PC를 이용한 인터넷뱅킹 등에서 보안 키패드를 제공하여 PIN이나 보안카드번호 입력를 보호하고 있다. 이를 스마트폰에서도 같은 방식의 보안 키패드로 서비스를 제공하고 있다[17,18,19,20,21].

구글 글래스(Google Glass)를 이용하여 3m 떨어진 거리에서 비밀정보를 입력하는 과정을 촬영한 사용자의 손동작을 분석하여 90%의 정확도로 비밀번호를 유추하는 어깨 너머 공격이 가능하다[22,23,24].

또한 스마트 폰이 오픈 플랫폼 기반으로 개발되어 PC보다 해킹에 취약하다. 사용자가 등이 스마트 폰의 Root 권한을 갖고자 루팅이나 탈옥을 하므로 더 쉽게 공격자로서 공격이 가능하고 악성코드로 피해가 급격하게 발생한다.

금융거래 등을 위한 스마트폰의 애플리케이션에서 제공하는 보안 키패드는 PC기반과 같은 QWERTY 키패드와 알파벳순으로 나열된 ABC 키패드를 제공한다. 랜덤하게 영문자를 배열하는 방식을 사용하지 않는 이유는 사용자로 하여금 원하는 문자를 찾는데 시간을 단축하고 쉽게 입력하기 위해 키보드 배열인 QWERTY 키패드나 알파벳순으로 나열된 ABC 키패드를 주로 사용하고 있지만 대체로 QWERTY 키패드를 사용하고 있다. 키 사이에 공백을 통해 약간의 배치를 조정하지만 터치한 위치정보를 알게 되면 왼쪽과 오른쪽에 가까이 있는 키패드를 확실하게 구별되고, 가운데에 있는 키패드의 경우는 확률적으로 판단하여 유추할 수 있다. 이는 같은 행에 사용되는 문자가 결정되고, 1~4개의 공백으로 위치를 변경하기 때문이다. 즉, 같은 크기의 모양으로 다양한 배치로 보안성을 높이고자 하였지만 이는 터치 위치정보를 이용한 입력한 정보를 유추하는 공격을 완벽하게 해결하기 어렵다.

제안 기법은 키패드를 같은 크기의 직사각형이 아니라 다양한 크기와 모양으로 키패드를 생성하고, 이를 테트리스 게임처럼 배치하여 터치 위치정보가 같아도 다른 문자가 입력되도록 하여 이를 통해 위치정보를 알아내도 입력한 정보를 알아내기 어렵다.

본 연구는 다음과 같이 구성한다. 2장에서는 위치정보로 인한 공격을 보호하기 위한 기존의 보안 키패드에 대한 관련연구를 소개하고, 3장은 테트리스 형태의 키패드로 공격에 내성을 갖는 제안기법을 제안하고, 4장에서는 위치정보 공격 기법을 분석한 뒤 5장에서 결론을 맺는다.

# 2. 관련 연구

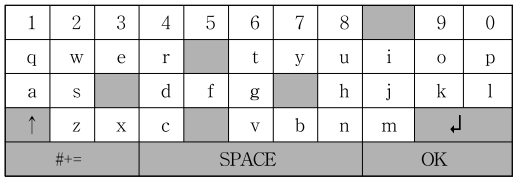
## 2.1 보안 키패드

모바일 단말기내의 금융 관련된 앱에서 비밀정보 입력시 단말기내의 키패드가 아닌 보안 키패드를 사용하고 있다. 공백이나 마크를 이용한 QWERTY 키패드와 알파벳 순서로 배열된 ABC 키패드로 구분하고 있다.

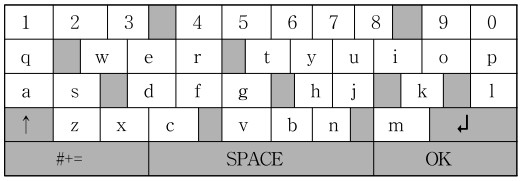
### 2.1.1 QWERTY 키패드

QWERTY 키패드의 배열이 PC자판과 동일하며 4개의 행으로 구성되고, 각 행마다 임의의 위치에 1~4개의 공백을 두어 생성한다.

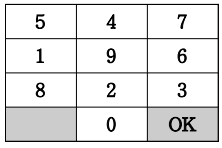
[Fig. 1] (a)은 4개의 행으로 구성된 보안 키패드이다. 1행은 10개의 숫자, 2행은 10개의 영문자, 3행은 9개의 영문자, 4행은 7개의 영문자로 구성되어 있다. 1행, 2행과 4행은 한 칸의 공백이 3행은 두 칸의 공백이 있다. 하나의 공백을 (a)에서는 한 번에 사용하고, (b)처럼 반으로 나누어 2배 사용할 수도 있다[25,26]. (c)는 수 키패드로 램덤하게 배치된다.




(a) Method with spacing as the size of keypad




(b) Method with spacing in half of the size of keypad



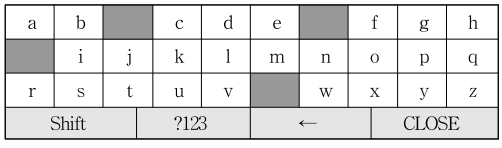

(c) Number keypad arranged randomly

[Fig. 1] QWERTY Keypads

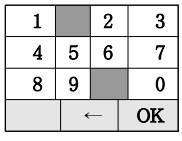
2.1.2 ABC 키패드

ABC 키패드는 알파벳 순서대로 키패드를 배열하되, 임의의 위치에 공백이나 마크를 추가한 키패드이다.

[Fig. 2](a)처럼 보통 3개의 행으로 구성되어 26개의 영문자와 4개의 공백으로 구성된다. 수 키패드(b)는 3개의 행으로 구성하고, 숫자 10개와 공백 2칸으로 키패드를 생성한다[26].




(a) Alphabetical keypads



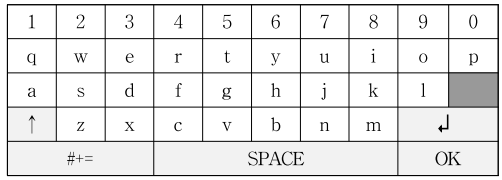

(b) Number keypads

[Fig. 2] ABC Keypads

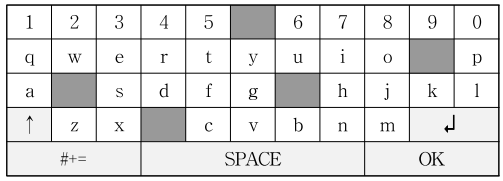
## 2.2 개선된 보안 키패드

2.2.1 물결형 키패드

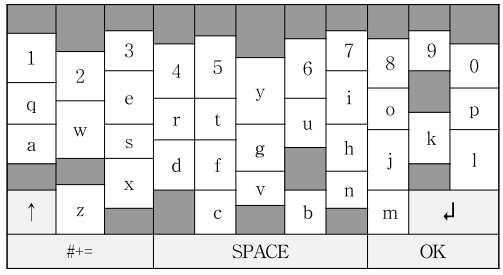
[Fig. 3]는 PC 키보드(a)에서 각 행마다 한 칸의 공백을 삽입하여(b) 보안의 강도를 높인 QWERTY 키패드에서 각 열마다 반 칸의 공백을 추가하는(c) 키패드를 생성한다[26].




(a) Traditional PC keypads



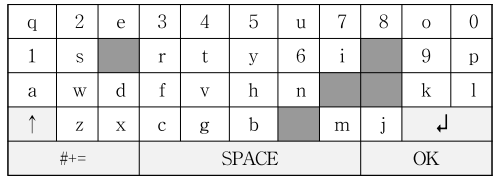

(b) Keypads inserted with horizontal space




(c) Keypads with vertical spacing

[Fig. 3] Keypads technique by Lee – ripple type keypad

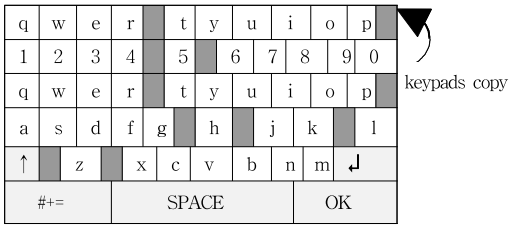
[Fig. 4]는 [Fig. 3](b)에서 각 열마다 k행, 여백, k-1행, k+1행의 키패드를 교환하여 배치된 키패드이다[27].




[Fig. 4] Keypads technique by Pak - keypads exchanged based on column

2.2.2 클론 키패드

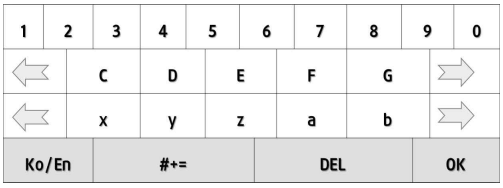
[Fig. 5]는 QWERTY 키패드의 4개 행중 하나를 임의로 선택하고 복사하여 위에 추가하는 키패드를 생성한다[26].




[Fig. 5] Keypads technique by Lee – clone keypad

2.2.3 터치&슬라이드 키패드

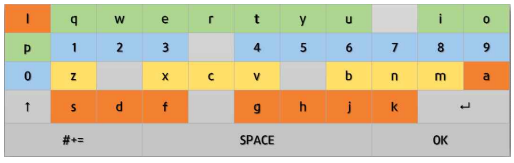
[Fig. 6]는 키패드의 화살표를 터치하여 좌우로 문자를 이동하거나 슬라이드를 통해 원하는 문자를 선택할 수 있는 키패드를 생성한다[26].




[Fig. 6] Keypads technique by Lee – touch & slide keypads

2.2.4 서화정 키패드

[Fig. 7]는 서화정이 제안한 키패드이다. 기존 QWERTY 키패드는 1부터 시작되는 키패드이지만 서화정 키패드는 임의의 위치부터 1을 시작하고, 나머지를 배치하고, 사용자로 하여금 원하는 문자를 쉽게 찾기 위해 기존 키패드의 각 행을 다른 색으로 표시하여 출력된 키패드를 생성한다[23].




[Fig. 7] Keypads technique by Seo

## 2.3 어깨 너머 공격을 회피 개선기법

사용자가 입력된 정보는 *로 표시되지만 터치 키패드의 높은 오타율로 인해 올바르게 입력되었는지 확인을 위해 마지막 문자를 보여주고 있다. 이로 인해 구글 글래스나 어깨너머공격에 대한 취약점이 발생한다.

입력된 키패드의 색깔을 출력하거나 입력된 정보가 맞는지를 확인하여 오류 없음을 메시지형태로 출력하는 방법 등이 제기되고 있다.

2.3.1 Four Color Theorem

사용자가 s를 터치할 경우 s 주변의 w, a, z, d 로 키가 터치될 경우가 높다. 이를 해결하기 위해 키패드에 색을 표시하여 입력된 키와 같은 색을 출력하여 오타 여부를 확인해 주는 기법이다. 4개의 색을 이용하면 대부분의 키를 표현할 수 있는 이론을 활용한 기법이다. 즉, 색으로 입력된 정보를 확인하는 방식이다[28].

2.3.2 서화정 마지막 입력확인

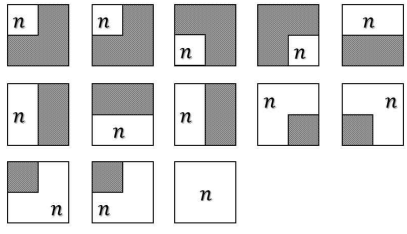
사용자가 입력한 비밀번호가 서버로부터 받은 비밀번호 정보와 비교하여 동일여부를 판단하는 기법으로 동일할 경우 메시지를 출력하는 방식이다. 즉, 입력한 정보를 알려주지 않고, 입력된 전체 정보가 맞는지 확인하는 방식이다[9].

# 3. 제안기법

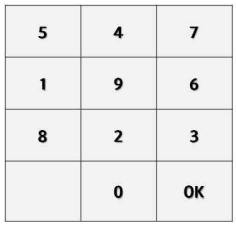
## 3.1 보안 키패드

기존 키패드는 같은 크기와 같은 모양으로 배치하고, 단지 공백을 통해 약간의 위치변경으로 생성되어 터치한 위치 정보를 알거나 구글 글래스 등을 통해 어깨너머로 훔쳐보기를 통해 입력된 정보를 유추할 수 있는 취약점이 존재한다. 이를 보완하기 위해 키패드를 다른 크기와 다른 모양으로 생성하여 배치하므로서 터치한 위치 정보를 이용하고 입력된 정보를 유추를 어려운 테트리스 형태의 보안키패드를 제안한다.

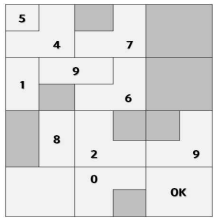
기존 키패드를 기준으로 가로 세로 2등분하여 [Fig. 4]와 같이 13개의 형태로 변경하여 테트리스 형태로 연결하는 보안 키패드를 제안한다. 13개의 모양의 키패드를 수 보안키패드로 변환하는 제안 기법의 예는 [Fig. 8]과 같다.



[Fig. 8] Number of cases arranged in quadrisection




(a) Example of secure keypad with tradition number




(b) Secure keypads with Tetris type

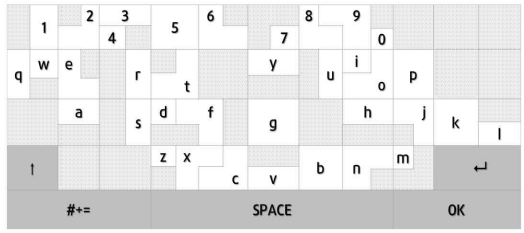
[Fig. 9] Application case of number secure keypad

[Fig. 9] (a)를 테트리스 형태로 적용사례는 (b)와 같다. 수 키패드는 임의의 위치에 배치되기 때문에 위치정보를 알아도 입력된 정보를 유추하기 어렵지만 같은 크기로 일정한 위치에 배치된다면 어깨너머 훔쳐보기는 여전히 가능하다. (b)는 제안기법이 적용된 사례로 사용자가 입력하기는 번거롭지만 어깨너머로 훔쳐보기는 기존보다 어렵다.

13개의 모양의 키패드를 영문자 입력에서 적용된 사례는 [Fig. 10] (b)와 같다. [Fig. 10] (a)처럼 총 4개의 공백만으로 키패드가 배열되어 있어 왼쪽과 오른쪽의 키패드를 변동이 없다. 그래서 왼쪽이나 오른쪽의 위치정보를 탈취할 경우 사용자의 입력한 비밀번호의 일부를 알게 된다.

(b)처럼 다양한 크기의 키패드로 테트리스 형태로 배치하므로서 위치정보를 알아내도 왼쪽의 몇 개의 키패드를 제외하고는 문자의 키패드의 위치정보가 바뀌기 때문에 거의 알아내기 어렵다.


(a) example of traditional secure keypad




(b) Example of secure kepad with tetris type

[Fig. 10] Application case of alphabetical secure keypad

# 4. 분석 및 토의

## 4.1 보안 키패드

보안 키패드 기법들은 2가지 측면을 고려해야 한다. 사용자의 편리한 입력을 위해 키패드의 위치를 사용자가 쉽게 찾아야 한다. 이를 통해 입력하는 시간 간격을 짧게 할 수 있고, 어깨 너머 공격 등을 차단하는 효과를 가질 수 있다. 둘째로는 공격자가 터치 위치를 탈취할 경우에도 위치에 고정되지 않는 키패드의 배열을 통해 입력된 문자가 무엇인지 추측이 어려워야 한다.

## 4.2 터치 위치정보 기반의 정보 유추 방법

QWERTY 키보드에서 1행이 1부터 0까지 10개의 숫자로 맨 왼쪽 즉, 첫 번째 키가 나올 수 있는 숫자는 1밖에 없다. 즉, 100%이다. 두 번째 키에는 1또는 2가 나올 수 있다. X12, 1X2, 123, 12X 으로 4가지 경우가 있다. X12는 1가지 경우, 123나 12X의 경우 9가지 경우가 나올 수 있다.

[Fig. 11]에서 보듯이 6번째 나올 수 있는 경우는 공백(*)이나 5나 6이다.

| | 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. 11] key types that is possible to be inserted in the first row

공백이 2개가 포함된 3행 세 번째 키는 [a],[s],[d]영문자과 공백(X)이다. [a]는 XXa 으로 경우의 수는 1이고, [s]는 Xas, aXs 으로 경우의 수는 8, 8 이고, [d]는 asd 으

로 ${}_8C_2 = 28$이다. 전체의 경우의 수는 ${}_{11}C_2 = 55$이지만 공백(X)를 클릭하지 않는 다는 전제에서 경우의 수는 45이다. [a]의 확률 $1/45 = 0.022$, [s]의 확률 $16/45 = 0.356$, [d]의 확률 $28/45 = 0.622$이다. <Table 1>는 키보드 형식의 QWERTY 키패드에서의 위치별로 키의 확률을 나타낸 것이다[24,25]

<Table 1> key probability of secure keypad for each location

| location / row | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 row | 1 100% | 1 10%<br>2 90% | 2 20%<br>3 80% | 3 30%<br>4 70% | 4 40%<br>5 60% | 5 50%<br>6 50% | 6 60%<br>7 40% | 7 70%<br>8 30% | 8 80%<br>9 20% | 9 90%<br>0 10% | 0 100% |
| 2 row | q 100% | q 10%<br>w 90% | w 20%<br>e 80% | e 30%<br>r 70% | r 40%<br>t 60% | t 50%<br>y 50% | y 60%<br>u 40% | u 70%<br>i 30% | i 80%<br>o 20% | o 90%<br>p 10% | p 100% |
| 3 row | a 100% | a 20%<br>s 80% | a 2%<br>s 36%<br>d 62% | s 7%<br>d 47%<br>f 47% | d 13%<br>f 53%<br>g 33% | f 22%<br>g 56%<br>h 22% | g 33%<br>h 53%<br>j 13% | h 47%<br>j 47%<br>k 7% | j 62%<br>k 36%<br>l 2% | k 80%<br>l 20% | l 100% |
| 4 row | z 100% | z 14%<br>x 86% | x 29%<br>c 71% | c 43%<br>v 57% | v 43%<br>b 57% | b 29%<br>n 71% | n 14%<br>m 86% | m 100% | | | |

### 4.3 비교분석

어깨너머 공격을 막기 위해 QWERTY 키패드를 다양한 방법으로 재배열하여 기존 방식보다 안전성을 높였지만 복잡하게 재배치할 경우 사용자가 비밀번호를 입력시 키패드를 찾는 시간이 늘어나서 공격자의 공격시간을 늘어나 공격 가능성이 높아진다. 입력시간을 줄이기 위해 키패드를  단순하게 배치할 경우 보안 키패드의 방식을 아는 공격자는 사용자가 터치한 위치정보로 입력한 정보를 유추할 수 있는 확률이 기존 보안 키패드보다 낮아지지만 공격 가능성은 여전히 존재한다.  제안 기법은 기존의 QWERTY 키패드와 같은 방식으로 배열되어 사용자가 비밀정보를 입력하기 쉽고, 다양한 크기로 재배치되어 위치정보를 이용한 입력정보 유추가능성이 낮아진다.

## 5. 결론

모바일 단말기의 급격한 이용으로 인해  금융거래 등에서 비밀정보를 입력하여 인증하는 시스템이 보편화되고 있다.

PC에서 인터넷뱅킹에서도 보안키패드를 통해 마우스로 클릭하는 방식으로 비밀정보를 전달하고 있다. 이 방식을 스마트 폰에서 적용하기 시작하였다. 하지만 단말기의 이동성과 터치를 통해 정보를 입력하다보니 다양한 공격이 가능한 취약점이 발생하고 있다. 어깨너머로 훔쳐보기나 터치위치정보를 탈취하여 비밀정보를 유추하는 공격이 가능하다. 구글 글래스로 3m 이내의 사용자가 입력한 정보를 알아내는 공격이 가능하게 되었다.

제안기법은 테트리스 형태의 보안 키패드를 통해 훔쳐보기나 터치위치정보를 이용한 유추 공격을 막을 수 있다. 테트리스 형태 중 넓이가 작은 것을 터치하기 어려운 단점이 있다. 향후 연구로는  비슷한 크기의 모양과 색깔 기반의 보안 키패드에 대한 연구가 필요하다.

## REFERENCES


[1]E. J. Choi, W. C. Jung, S. Y. Kim,“Attacks and Defenses for Vulnerability of Cross Site Scripting,” Journal of digital Convergence, Vol. 13, No. 2, pp. 177-183, 2015.

[2]H. J. Mun, G.H, Choi, Y.C. Hwang, "Countermeasure to Underlying Security Threats in IoT communication," Journal of IT Convergence Society for SMB, Vol. 6, No. 2, pp. 37-44, 2016.

[3] S. H. Hong, “XSS Attack and Countermeasure: Survey,” Journal of digital Convergence, Vol. 11, No. 7, pp. 327-332, 2013.

[4]K. H. Choi, K. Y. Chung, D. K. Shin, “A Study of Prevention Model the Spread of Phishing Attack for Protection the Medical Information”, Journal of digital Convergence, Vol. 11, No. 3, pp. 273-277, 2016.

[5] B. S. Yu, S. H. Yun, “The Design and Implementation of Messenger Authentication Protocol to Prevent Smartphone Phishing,” Journal of the Korea Convergence Society, Vol. 2, No. 4, pp. 9-14, 2011.

[6]S. H. Hong,“Cognitive Approach to Anti-Phishing and Anti-Pharming : Survey”, Journal of IT Convergence Society for SMB, Vol. 3, No. 2, pp. 33-39, 2013.

[7]S. D. Yoo, J.G. Kim, “How to improve carrier (telecommunications) billing services to prevent damage”, Journal of digital Convergence, Vol. 11, No. 10, pp. 217-224, 2013.

[8]J. H. Kim, J. Y. Go, K. H. Lee, “A Scheme of Social Engineering Attacks and Countermeasures Using Big Data based Conversion Voice Phishing,” Journal of the Korea Convergence Society, Vol. 6. No. 1, pp.

85-91, 2015.

[9]H. J. Seo, H. W. Kim, “Secure Keypad with Encrypted Input Message,” Journal of the Korea Institute of Information and Communication Engineering, Vol. 18, No. 12, pp. 2899-2910, 2014.

[10]S. Y. Jun, I. J Jeong, “LTE Spectrum Policy: Focused on the OECD 12 Countries,” Journal of digital Convergence, Vol. 12, No. 8, pp. 1-18, 2014.

[11]J. S. Han, “Security Threats in the Mobile Cloud Service Environment,” Journal of digital Convergence, Vol. 12, No. 5, pp. 263-269, 2014.

[12]D. R. Kim, K. H. Han, “A Study on Multi-Media Contents Security using Smart Phone,” Journal of digital Convergence, Vol. 11, No. 11, pp. 675-682, 2013.

[13]S. W. Choi, Y. J. Shin, “Economy Effects of IT Industry on Financial and Insurance Services”, Journal of digital Convergence, Vol. 13, No. 1, pp. 191-203, 2015.

[14]D. R. Kim, “A Study on the OTP Generation Algorithm for User Authentication,” Journal of the Korea Convergence Society, Vol. 13, No. 1, pp. 283-288, 2015.

[15] S. H. Hong, "New Authentication Methods based on Users Behavior Big Data Analysis on Cloud," Journal of IT Convergence Society for SMB, Vol. 6, No. 4, pp. 31-36, 2016.

[16] H. J. Moon, M. H. Lee, K. H. Jeong, “Authentication Performance Optimization for Smart-phone based Multimodal Biometrics,” Journal of digital Convergence, Vol. 13, No. 6, pp. 151-156, 2015.

[17]C. Shuang, S. J. Lee, K. R. Lee, “A Study on Chinese User Resistance of Mobile Banking,” Journal of digital Convergence, Vol. 12, No. 1, pp. 105-111, 2014.

[18]D. R. Kim, “Secure One-Time Password Authentication in Mobile Environments,” Journal of digital Convergence, Vol. 11, No. 12, pp. 423-430, 2013.

[19] S. H. Lee, D. W. Lee, “FinTech - Conversions of Finance Industry based on ICT,” Journal of the Korea Convergence Society, Vol. 6, No. 3, pp. 97-102, 2015.

[20] J. M. Ryu, Y. M. Seo, H. J. Cho, “A Study on Business Model of Fintech - Focus on the Business model canvas-,” Journal of digital Convergence, Vol. 14, No. 3, pp. 171-179, 2016.

[21]Y. M. Kang, Y. G. Lee, H. J. Kwon, K. S. Han, H. S. Chung, “A Study on the Information Security System of Fin-Tech Business,” Journal of IT Convergence Society for SMB, Vol. 6, No. 2, pp. 19-24, 2016.

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

[23]H.J. Seo, 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.

[24]S. H. Kim, M. S. Park, S. J. Kim, “Shoulder Surfing Attack Modeling and Security Analysis on Commercial Keypad Schemes,” Journal of the Korea Institute of Information Security & Cryptology, Vol. 24, No. 6, pp. 1159-1174, 2014.

[25]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.

[26]D.H. Lee, D.H. Bae, S.L. Yoo, J. Y. Chae, Y.H. Lee, H.G. Yang, “Analysis of safety in secure keypads for smartphone,” REVIEW OF KIISC, Vol. 21, No. 7, pp. 30-37, 2011.

[27]W.G. Pak, S.K Yeo, Y.R. Cha, “A Secure Virtual Keypad for Mobile devices,” Proceeding of KOREA INFORMATION SCIENCE SOCIETY, pp. 875-876, 2015.

[28] H. J. Kim, H. J. Seo, Y. C. Lee, T. H. Park, H.W. Kim, “Implementation of virtual finace keypads with resistance for shoulder surfing attack,” REVIEW OF KIISC, Vol. 23, No. 6, pp. 21-29, 2013.

## 저자소개

문 형 진(Hyung-Jin Mun) [종신회원]

- 1996년 2월 : 충남대학교 수학과
- 2008년 2월 : 충남대학교 전자계산학(이학박사)
- 2009년 3월 ~ 2012년 8월 : 중국 연변과학기술대학교 컴퓨터전자통신학부 조교수, 부교수
- 2017년 3월 ~ 현재 : 성결대학교 정보통신공학부 조교수

<관심분야> : 정보보호, 네트워크 보안, 프라이버시보호, 사용자인증