JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 9: 1152~1159, Sep. 2019

향상된 보안의 닌텐도 스위치 행렬 형태 보안 키패드 제안

권혁동[1] · 권용빈[1] · 최승주[1] · 서화정[2*]

A Proposal for Matrix Shape Security Keypad for the Nintendo Switch

Hyeok-dong Kwon[1] · Yong-bin Kwon[1] · Seung-ju Choi[1] · Hwa-jeong 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

8세대 게임기로 등장한 닌텐도 스위치는 하이브리드 형 콘솔 게임기로 세계적인 판매 성과를 달성했다. 닌텐도 스위치는 자체적으로 온라인 숍을 내장하고 있으며 사용자는 자신의 계정으로 로그인하여 게임을 구매할 수 있다. 이 때 사용하는 닌텐도 스위치에 내장된 키패드는 쿼티 자판과 유사하게 생겼다. 패스워드 입력 창에는 입력 정보가 가려지지만 훔쳐보기 공격을 통해 키패드 상에서 어떤 값이 입력되는지 확인이 가능하다. 파티 형 또는 가족 형 게임이 많은 닌텐도 스위치의 특성상 근처에 화면을 보는 다른 사람이 있을 가능성이 높으며 이는 계정 보안에 큰 취약점으로 작용한다. 따라서 이를 개선한 새로운 키패드를 설계하였다. 본 논문에서는 닌텐도 스위치의 보안 키패드가 어떤 문제점을 지녔는지 확인하고 새롭게 제안한 키패드의 구현 및 불특정 다수의 사용 테스트 결과를 제시한다.

ABSTRACT

The Nintendo Switch(NSW), which appeared as an 8th generation console, has succeeded worldwide as a hybrid gaming console. The NSW has E-shop itself, users can sign in to their account and purchase games. The keypad built in the NSW is similar to QWERTY keyboard. In the password input field the input information is hidden, but it's possible to get the value entered from the keypad with shoulder surfing attack. Because of the NSW with many party or family games, there is a high probability that someone else is watching the screen nearby, which acts as a vulnerability in account security. Thus we designed the new keypad which improve from this issue. In this paper, we check the problem about the keypad which built in the NSW, we present the proposed keypad and the compared to the built in keypad by showing the test result of unspecified individuals use.

키워드 : 계정 보안, 닌텐도 스위치, 보안 키패드, 훔쳐보기 공격

Keywords : Account Security, Security Keypad, Shoulder Surfing Attack, The Nintendo Switch

Received 6 June 2019, **Revised** 10 June 2019, **Accepted** 25 June 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.2019.23.9.1152 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

게임을 즐기는 유저들은 여러 가지 플랫폼을 선택할 수 있으나 그 중에서 게임만을 위한 플랫폼인 게임기는 게임에 가장 최적화된 플랫폼으로, 오랜 세월에 거쳐 발전하며 사용자들의 사랑을 받아왔다. 게임기를 세대별로 분류하자면 현재는 8세대에 이르렀고 그 중에서 닌텐도 스위치는(이하 '스위치') 거치형과 휴대형을 오갈 수 있는 하이브리드 게임기이다.

현시대 게임기는 온라인 접속을 기본적으로 지원하고 있다. 컴퓨터에서 개인화 서비스를 제공받거나 온라인 쇼핑을 위해서 로그인을 하듯이 게임기 상에서도 로그인 과정을 거친다. 이때 사용자는 자신의 계정과 패스워드를 입력하여 로그인을 하는데, 일반적으로 게임기의 입력장치 중에는 키보드나 마우스를 기본으로 제공하지는 않는다. 따라서 게임기의 독자적인 컨트롤러를 사용하여 패스워드를 입력하는 경우가 잦다.

8세대 게임기 중 일본의 닌텐도사에서 개발한 스위치 역시 온라인 서비스를 지원한다. 사용자는 필요에 따라 네트워크에 접속하여 다양한 서비스를 이용할 수 있다. 하지만 스위치의 패스워드 입력 패드는 화면상에 노출되어 있으며 화면을 보는 것만으로도 패스워드 입력을 모두 확인할 수 있다. 다수가 모여서 즐기는 게임이 많은 스위치의 특성상 주변에 다른 사람이 있을 확률이 높으며 이는 계정 보안에 큰 취약점으로 작용한다.

따라서 우리는 스위치의 패스워드 입력 문제를 개선한 새로운 패스워드 입력 패드를 제안하며 본 패드를 사용한 다수의 불특정 사용자들의 설문 결과를 통해 제안한 패드의 장점과 효용성을 입증하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 스위치에 대한 내용과 보안 패드에 관한 관련 연구를 소개할 것이며 3장에서 스위치 키패드가 지닌 문제점과 이를 개선한 신규 보안 키패드를 소개한다. 4장에서는 기존 스위치 키패드와 제안한 키패드의 성능비교를 할 것이며 5장에서 결론을 맺는다.

Ⅱ. 관련 연구 동향

본 장에서는 주제가 되는 기기인 스위치에 대한 설명과 기존에 제안되었던 특이한 형태의 보안 키패드에 관한 동향을 살펴본다.

2.1. 닌텐도 스위치

스위치는 닌텐도사에서 2017년 3월 3일에 출시한 기기로 기존에 출시했던 Wii U의 부진한 성적을 만회하기 위해 출시되었다. 스위치는 게임기 분류상 8세대 게임기로 분류되며[1] 기기의 상세 스펙은 표 1과 같다.

Table. 1 Specification of Nintendo Switch[2]

Display	6.2“ with 1280 x 720 resolution
CPU/GPU	NVIDIA customized Tegra processor
Storage	3GB Expandable via microSD/SDHC/SDXC memory cards
Wireless Connectivity	802.11 a/b/g/n/ac Wi-Fi Bluetooth 4.1
Ports	USB Type-C 3.5mm audio jack
Maximum Resolution in TV	1920 x 1080 at 60FPS
Media	Proprietary Switch solid-state game cards
Sensors	Accelerometer Gyroscope Ambient light sensor
Battery	4310 mAh lithium-ion rechargeable

스위치는 자체적인 컨트롤러인 '조이콘'을 사용하는 것으로 조작이 가능하다. 조이콘은 블루투스 3.0을[2] 사용하며 이를 통해 본체와 등록이 가능하다. 하나의 스위치 본체에는 최대 8쌍의 조이콘을 등록할 수 있다. 기본적으로 조이콘은 좌(L), 우(R) 두 대를 한 쌍으로 취급하지만 각각 따로 등록하여 서로 다른 두 쌍의 조이콘으로 사용할 수도 있다. 조이콘 상의 버튼과 조이스틱은 잡기 방법에 따라 고유한 입력신호를 발생시킨다[3].

스위치는 온라인 숍을 내장하고 있으며 사용자는 닌텐도 계정과 패스워드를 입력하는 것으로 온라인 숍에 접속하여 게임이나 추가 콘텐츠를 구매할 수 있다. 이때 아이디와 패스워드를 입력하기 위한 자체적인 입력 패드가 화면상에 표시되며 이는 그림 1과 같다.

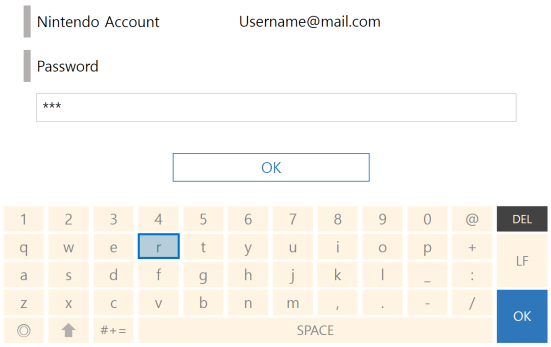


Fig. 1 Appearance of password keypad for Nintendo Switch

2.2. 보안 키패드

일반적으로 보안 키패드는 PC 또는 모바일 상에서 금융과 같은 고수준의 보안이 필요한 부분에서 사용한다. 대다수의 보안 키패드는 일반적인 키패드와 유사하게 쿼티 자판을 따르지만 레이아웃 등이 변경되어 입력 값의 유추를 방지한다. 이와 같은 보안 키패드는 다양한 형태가 제안되었다.

2.2.1. 무작위 공백 보안 키패드[4]

키패드를 호출할 때마다 공백의 위치가 매번 달라지는 형태의 키패드로 그림 2에서 확인 가능하듯이, 전체적으로 쿼티 자판은 유지한다. 하지만 공백이 키 사이에 무작위로 삽입되기 때문에 이전 입력과 동일한 좌표의 입력일지라도 실제 입력 값은 다를 가능성이 생긴다. 이는 공격자가 피해자의 입력 좌표를 획득해도 해당 좌표의 입력 값이 특정 값임을 보장하지 않는다는 보안성을 지닌다.

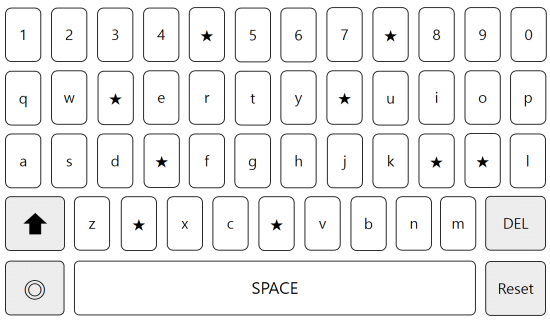


Fig. 2 Random spacing keypad

2.2.2. 테트리스 형태의 보안 키패드[5]

공백을 무작위로 배치하는 키보드는 레이아웃의 큰 틀은 유지한 채 약간의 위치만 변경된다는 특징으로 인해 훔쳐보기 공격에 취약하다. 이를 보완하기 위해 제안된 테트리스 형태의 보안 키패드는 각각의 키를 서로 다른 크기와 서로 다른 모양으로 생성하여 입력 정보 유추를 어렵게 한 키패드이다.

본 방법은 일반적인 사각형 모양의 키를 사용하지 않고 그림 3에 나오는 13개 형태의 키를 사용한다. 모든 키는 키패드 실행 시 무작위의 형태를 가지게 되며 각각의 키에 형태가 확정된다면, 이를 쿼티 레이아웃으로 배치한다. 따라서 본 키패드는 키를 다양한 형태로 제공하는 것으로 위치 정보를 획득하더라도 키패드의 형태에 따라 매번 위치 정보가 크게 변하기 때문에 정보 유추가 어렵다.

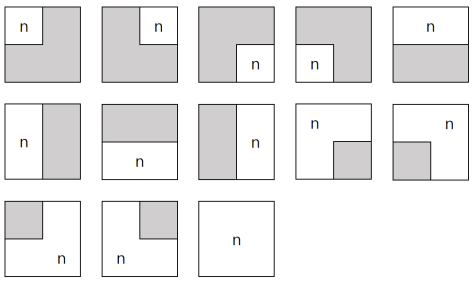


Fig. 3 Cases of keypad based on Tetris block

2.2.3. 행 단위 배치 보안 키패드[6]

쿼티 자판을 유지하는 키패드는 사용자의 편의성은 향상되나 입력 값의 유추가 쉽기 때문에 보안성은 떨어진다. 반대로 자판 배열을 무시한 무작위 키 배치의 경우 입력 값 유추가 어렵기 때문에 보안성은 향상되나 사용자도 자신이 필요한 키를 찾기 어려워서 편의성이 떨어진다. 따라서 적절한 수준의 보안성을 제공하며 사용자의 편의성을 높이기 위해서는 기존 키패드의 배치를 어느 정도 유지하는 기법이 유효하다.

제안된 키패드는 그림 4와 같이 쿼티 자판의 행 배열은 유지한 채, 시작 위치만 다르게 설정되어있다. 이때 사용자가 각각의 행을 쉽게 찾을 수 있도록 하나의 행은 서로 같은 색으로 이루어져있다. 가령 쿼티 자판에서 'z'부터 'm'은 하나의 행에 놓여있으므로 동일한 색으로 칠해져 있는 것을 확인할 수 있다. 자판의 순서는 섞여 있지만 전체적으로 쿼티 자판의 배열은 유지되어있기

때문에 사용자는 완전 무작위 배치에 비해 손쉽게 원하는 입력을 찾을 수 있고 입력 값 좌표도 크게 변하기에 높은 수준의 보안성을 제공할 수 있다.

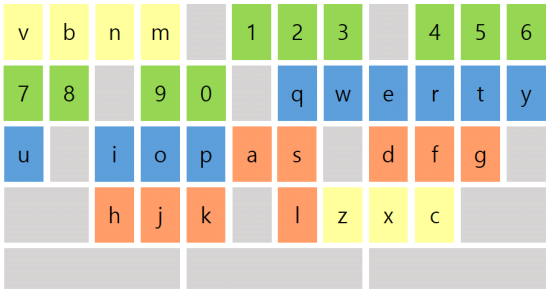


Fig. 4 Row unit randomized keypad

Ⅲ. 제안 기법

본 장에서는 현재 사용되는 스위치 키패드의 문제점을 제기하고 제안하는 기법에 대한 설명과 구현물에 대해서 서술한다. 제안 키패드 구현은 안드로이드 어플리케이션의 소켓 통신을 사용하였으며, 시연을 통해 자세한 동작 원리를 소개한다. 전체적인 시연 과정은 유튜브[7]에서 확인할 수 있으며 구현에 사용한 코드는 깃허브[8][9]를 통해 열람이 가능하다.

3.1. 기존 스위치 키패드의 문제점

스위치의 패스워드 입력은 2.1절의 그림 1처럼 쿼티 자판과 유사한 형태의 키패드를 사용한다. 키패드 상에서 커서는 조이콘을 통해 움직이며 자신이 원하는 키에 커서를 이동한 다음 조이콘의 버튼을 눌러서 입력, 띄어쓰기, 삭제 등의 행동을 취할 수 있다.

스위치의 패스워드 입력란은 문자를 '*'과 같은 특수문자로 알 수 없게 처리한다. 따라서 패스워드 란을 보더라도 입력 값이 어떤 값인지 알 수 없다. 하지만 커서의 위치는 화면에 지속적으로 노출되는 문제점이 있다.

상기 취약점을 이용하면 다음과 같은 공격 시나리오가 성립한다. 사용자가 스위치를 사용하고 공격자는 사용자의 뒤에서 화면만 지켜본다. 사용자는 스위치의 패드를 통해 자신 계정의 패스워드를 입력하기 시작한다. 이때 공격자는 사용자 커서의 이동을 보고 커서가 멈추었을 때 패스워드 란에 '*'문자가 추가되는 것을 확인한다. '*'문자가 추가된다면 커서가 위치한 곳의 문자가 입력된 것이고, 사용자가 입력 완료를 할 때까지 커서를 추적하는 것으로 패스워드를 알 수 있으며 그림 5는 이를 묘사한 구도이다.

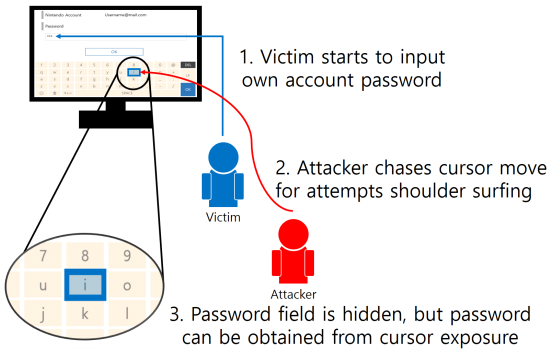


Fig. 5 Cursor exposure vulnerability to password keypad for Nintendo Switch

3.2. 행렬 형태 키패드 제안

스위치 키패드는 훔쳐보기 공격에 취약한 면모를 지니고 있다. 이를 해소하기 위해서는 커서의 노출을 제거해야 하는데 커서가 제거된 상태로는 사용자가 입력하고자 하는 값을 스스로 파악하기 어렵다. 이를 해결하기 위해서 행렬 형태의 키패드를 제안한다.

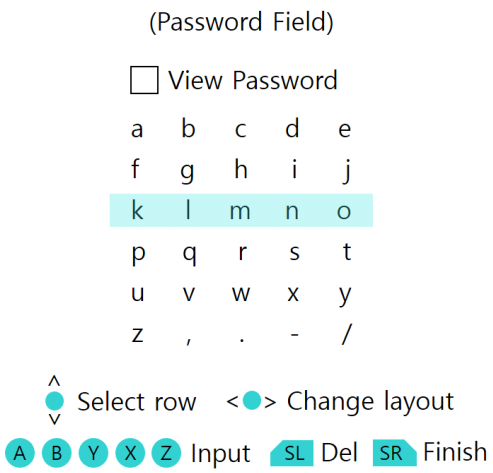


Fig. 6 Appearance of suggested security keypad

그림 6은 제안하는 키패드의 개략적인 묘사이다. 그림 6에서 음영처리 된 부분은 키패드 실행 시 무작위로 지정되는 초기 행의 위치로, 사용자가 현재 어느 행에

위치했는지 인지하도록 힌트를 준다. 음영은 약 2초간 유지된 후 사라지기 때문에 이후에는 사용자가 현재 행의 위치를 기억해야 한다. 사용자는 조이콘의 스틱을 위아래로 조작하는 것으로 행을 이동할 수 있으며, 만약 양 끝 행에 도달할 시 조이콘에 특정 패턴의 진동을 발생시켜 현재 선택이 끝단에 도달했음을 알린다.

사용자는 자신이 원하는 문자가 있는 행에 도착했을 때 A, B, Y, X, Z의 버튼을 눌러서 각각 1, 2, 3, 4, 5열에 있는 값을 입력한다. 가령 'i'문자를 입력하고자 한다면 스틱을 위아래로 조절하여 두 번째 행으로 이동하고 네 번째 열에 있는 문자이므로 X버튼을 입력하면 'i'문자가 입력된다. 만약 현재 레이아웃에 원하는 문자가 없다면 조이콘 스틱을 좌우로 움직이는 것으로 레이아웃 변경이 가능하다. 예를 들어 우측 입력을 반복한다면 영문 소문자, 영문 대문자, 특수문자1, 특수문자2의 순서로 레이아웃이 순환하며 변경된다.

상세한 동작 과정 파악을 위해 'test'라는 문구를 입력하는 상황을 가정한다. 그림 6과 동일하게 사용자는 음영을 통해 최초의 행 위치가 세 번째 행임을 확인한다.

첫 번째 문자인 't'는 네 번째 행에 있으므로 스틱을 아래로 한 번 조작하여 선택 중인 행을 하나 내린다. 이 과정은 화면상에 표시되지 않는다. 선택한 행에서 't'는 다섯 번째 열에 있으므로 Z버튼을 눌러 입력을 한다. 두 번째 문자인 'e'는 첫 번째 행에 있으므로 스틱을 위로 세 번 조작하여 첫 번째 행으로 이동한 다음 다섯 번째 열의 값을 입력하기 위해 Z버튼을 눌러 'e'를 입력한다.

세 번째 문자인 's'는 다시 네 번째 행에 있으므로 스틱을 아래로 세 번 조작하여 행을 이동한 다음 네 번째 열의 값을 선택하기 위해 X버튼을 눌러 's'를 입력한다. 마지막으로 다시 't'문자는 동일한 행의 다섯 번째 열에 있으므로 스틱 조작은 하지 않고 Z버튼을 눌러 't'를 입력한다. 그림 7은 본 전체 과정을 묘사한 그림이다.

만약 입력 값이 'test'가 아니라 'Test'와 같이 대문자가 포함되어 있다면 스틱을 우측으로 조작하여 영문 대문자 레이아웃을 호출한 다음 동일한 과정을 거쳐 입력을 할 수 있다.

스위치의 입력 패드는 항상 하단에 간편 사용자 매뉴얼을 제공한다. 마찬가지로 제안하는 행렬 형식의 보안 패드는 사용자에게 익숙하지 않은 형태이므로, 사용자가 이해하기 쉽게 그림 6의 하단과 같이 기존과 비슷한 형식으로 설명을 제공한다.

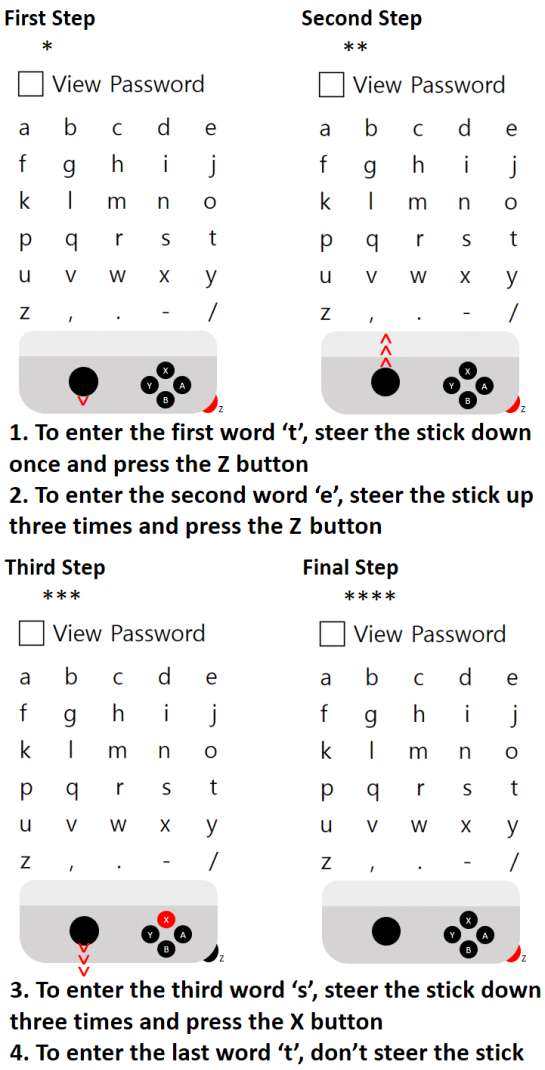


Fig. 7 The process of entering the string 'test'

이로서 제안하는 키패드의 동작 과정을 확인하였다. 그림 8은 본 키패드의 의사코드를 표현한 것으로 간략한 코드 동작을 확인 가능하며, 실제로 안드로이드 어플리케이션을 통해 시연 가능한 코드는 [8][9]에, 시연 영상은 [7]에 공개하였다.

```
Algorithm of matrix shape keypad
1. Select row = 1 to 6 randomly
2. keyLayout = 1
3. Display selected row about 2sec
4. Loop for user signal waiting
  4.1 If signal is Up or Down, row++ or row--
    4.1.1 If row <= 1, row = 1 and vibrate controller
    4.1.2 If row >= 6, row = 6 and vibrate controller
  4.2 If signal is Left or Right, keyLayout-- or keyLayout++
    4.2.1 If keyLayout < 1, keyLayout = 4 and go to 4.2.3
    4.2.2 If keyLayout > 4, keyLayout = 1 and go to 4.2.3
    4.2.3 Else change keyboard layout
  4.3 If signal is A or B or Y or X or Z, column = 1 or 2 or 3 or 4 or 5
    4.3.1 char = (row, column)
    4.3.2 add masked char '*' to password field
  4.4 If signal is SL, remove last char from password field
  4.5 If signal is SR, escape from loop
5. Password input step finished
```

Fig. 8 Pseudocode of suggested security keypad

Ⅳ. 성능평가

본 장에서는 기존 스위치에 탑재된 키패드와 제안한 키패드의 편의성과 보안성 평가를 위해 실제 사용 결과물을 제시한다. 실험 전, 실험자들이 환경에 적응 할 수 있도록 스위치의 패드와 제안 패드의 조작 연습을 5분간 진행하였다. 실험은 두 세트로 진행하며 각각의 세트는 스위치 상에서 3회, 제안 패드 상에서 3회를 입력하는 것으로 설정한다. 실험의 첫 번째 세트는 연구진에서 'ITConvergence.Dept'라는 입력 값을 제시하고, 두 번째 세트는 각자의 실험자가 원하는 값을 입력하도록 한다. 단, 실험자는 실험 종료 시까지 한번 선택한 값을 계속 사용해야만 한다.

실험을 통해 편의성과 보안성 두 가지를 확인하되, 각각의 요소에 대해 실험을 따로 진행하지 않고 동시에 진행한다. 즉, 입력 시간을 측정하여 편의성을 평가하는 동시에 실험자에게는 공격 사실을 알리지 않은 채로 연구진의 공격자가 공격을 시도하여 보안성도 판단한다. 실험에 참석한 인원은 14명으로 연령은 22세에서 29세로 분포한다.

4.1. 기존 보안 키패드 적용 시 취약점

실험 결과를 확인하기에 앞서, 2장에서 확인한 다양한 보안 키패드를 적용했을 경우를 가정한다. 첫 번째로 '무작위 공백 보안 키패드'를 적용한 경우이다. 스위치 상에서 입력은 조이콘을 사용한 커서 이동으로 이루어진다. 이때 화면상에 커서 위치가 노출되기 때문에 무작위 공백이 존재하더라도 커서의 위치가 그대로 노출되며 전체적인 쿼티 레이아웃 유지로 인해 훔쳐보기 공격에 취약하다. 마찬가지로 '테트리스 형태의 보안 키패드'도 각각의 키 모양은 다르지만 여전히 커서의 위치는 노출되고 쿼티 레이아웃을 사용하기 때문에 모바일 상에서는 훔쳐보기 공격에 강할지언정 환경이 다른 스위치 상에서는 동일 공격에 취약하게 된다.

마지막으로 '행 단위 배치 보안 키패드'의 경우에는 키 배치가 크게 변화하기 때문에 공격자가 커서 위치만을 보고 값 유추가 어려울 수 있다. 하지만 커서의 자리에 입력 값이 적혀있기 때문에 다른 키패드보다 약간의 집중을 더 한다면 여전히 공격이 가능하다.

4.2. 편의성

편의성은 사용자가 입력을 완성하는데 걸리는 시간을 척도로 하며 빠를수록 편의성이 높은 것으로 판단한다. 여러 명의 실험자가 다수의 입력을 하므로 동일한 실험 환경 별로 평균 시간을 계산하여 총 4종류의 결과를 도출한다. 실험 결과는 그림 9의 그래프와 같으며, 소수점 이하는 반올림 하였다.

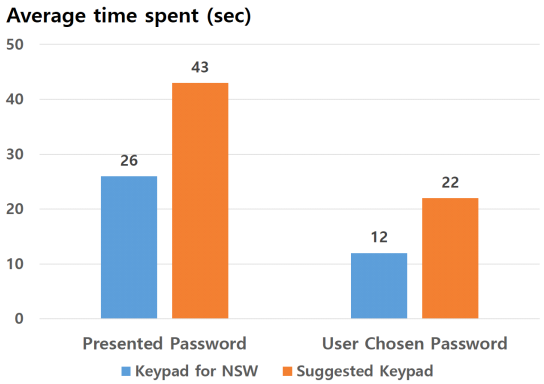


Fig. 9 The graph of time spent result

입력 값을 제시한 경우, 스위치 상에서는 평균 약 26초, 제안 패드 상에서는 평균 약 43초로 약 60%정도 느린 입력을 보였다. 마찬가지로 실험자가 원하는 값을 입력한 경우, 스위치 상에서는 평균 약 12초, 제안 패드 상에서는 평균 약 22초로 약 55% 느린 입력을 보였다. 제안 패드는 사용자에게도 현재 선택한 행을 알려주지 않는다. 따라서 사용자가 현재 행을 파악하는 시간이 추가

로 발생하는 난점이 존재한다.

다만 스위치 상의 입력은 조이콘의 스틱을 사용하여 빠른 커서 이동이 가능했지만 본 제안은 안드로이드에서 유사한 환경을 구현하였기 때문에 스틱과 버튼이 아닌 스마트폰 터치를 사용하므로 조작이 불편한 점도 있었다. 따라서 조작부가 동일한 상황이 된다면 현 상황보다 향상된 입력 속도를 보일 것으로 예상된다.

4.3. 보안성

보안성은 실험자가 입력하는 중에 공격자가 입력 값을 유추하는데 성공한 여부를 척도로 삼으며 유추에 실패할수록 보안성이 높은 것으로 판단한다. 이때 공격자는 실험자의 입력을 정확하게 유추해야 하며 단 하나의 입력이라도 틀렸을 시 실패로 간주한다.

실험자에게는 공격 상황을 알리지 않았으므로 공격자는 모든 입력 시에 공격을 시도하며 실험 종료 때 실험자에게 공격 사실을 알리고 최초로 공격이 성공한 시점을 기록한다. 공격자는 훔쳐보기 공격을 시도하며 입력 화면만이 정보로 제공된다. 단, 입력 값을 제시하는 첫 번째 세트의 경우는 이미 입력 값을 알고 있기 때문에 시행에서 제외한다. 실험 결과는 표 2와 같다.

Table. 2 The table of shoulder surfing attack result

	Keypad for NSW	Suggested Keypad
First try	7	0
Second try	2	0
Third try	3	0
Failed	2	14
Total	14	14

스위치 상에서 입력 시에는 절반의 인원이 첫 번째 입력에서 값이 유출되었고 두 명의 사용자는 두 번째 입력에서, 세 명의 사용자는 세 번째 입력에서 값이 유출되었다. 오직 두 명의 사용자만이 공격에서 벗어났다.

반면 제안 패드 상에서 입력 시에는 모든 인원이 공격에서 무사할 수 있었다. 이는 화면상에 표시되는 정보가 패스워드 입력란에 추가되는 '*' 문자와 입력 레이아웃뿐이므로 현재 사용자가 어떤 값을 선택했는지에 대한 정보는 없다. 때문에 공격자는 '*' 문자의 수로 입력의 길이는 파악 가능하나 실제 입력 값이 어떤 것인지 파악은 불가능하다.

Ⅴ. 결 론

본 논문에서는 스위치에 내장된 보안 키패드의 취약점을 이용한 공격 및 이를 해소한 새로운 유형의 보안 키패드를 제안하였다. 제안한 키패드는 기존 키패드에 비해 사용자 편의성은 조금 떨어진다고 판단되었으나 보안성 면에서는 우수한 성능을 보임을 입증하였다.

보안 분야에서 편의성과 보안성은 반비례 하는 관계를 보인다. 강한 보안성을 지니는 경우 복잡한 인증과정이나 사용자에게 익숙하지 않은 환경 등을 사용하기 때문에 어느 정도의 편의성 하락은 불가피하다[10]. 하지만 편의성을 포기하게 되면 사용자 확보가 어렵기 때문에 적절한 보안성과 편의성을 제공하기 위해서 타협안을 찾기 위한 지속적인 수정 및 검토가 필요하다.

마지막으로 제안한 키패드는 불특정 다수의 사용자가 지켜보는 경우에 매우 강력한 보안성을 제공한다. 따라서 제안사항이 스위치 상에서만 사용되지 않고 공공부문에서 사용될 수 있도록 추가적인 연구를 진행하여 개선을 진행할 예정이다.

ACKNOWLEDGEMENT

This research 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) and this research was partly supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1C1B5075742).

References

[1] Culture Of Gaming. 2019: Join the 8th Generation of Consoles. [Internet]. Available: https://cultureofgaming.com/2019-join-the-8th-generation-of-consoles/.

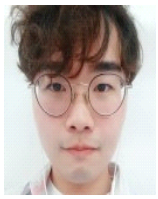
[2] iFixit. Nintendo Switch. [Internet]. Available: https://ko.ifixit.com/Device/Nintendo_Switch.

[3] Nintendo Switch Customer Support. Joy-Con usage guide.

[Internet]. Available. https://www.nintendo.co.kr/support/switch/controller/joycon/joycon_useage.php.
[4] Y. H. Lee, “An Analysis on the Vulnerability of Secure Keypads for Mobile Devices,” *Journal of Internet Computing and Services*, vol. 14, no. 3, pp. 15-21, June. 2013.
[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, June. 2017.
[6] 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, Feb. 2016.
[7] Youtube. Suggested keypad description video. [Internet]. Available. https://youtu.be/ybOgx51i1ZI.
[8] Github. PWPadForNSW. [Internet]. Available. https://github.com/korLethean/PWPadForNSW.
[9] Github. JoyconPadForNSW. [Internet]. Available. https://github.com/korLethean/JoyconPadForNSW.
[10] K. H. An, H. D. Kwon, K. H. Kim and H. J. Seo, “Implement pattern lock security enhancement using thread to measure input time,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 23, no. 4, pp. 470-476, April. 2019.

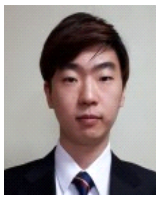
권혁동(Hyeok-dong Kwon)

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



권용빈(Yong-bin Kwon)

2018년 7월: 한성대학교 IT응용시스템공학과 공학 학사
2018년 8월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 블록체인, 머신러닝



최승주(Seung-ju Choi)

2019년 2월: 한성대학교 영어영문학과 학사
2019년 3월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 블록체인, IoT

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