석사학위논문

향상된 보안성을 지닌 새로운 유형의 보안 키패드 제안

2020년

한 성 대 학 교 대 학 원

I T 융 합 공 학 과

I T 융 합 공 학 전 공

권 혁 동

석 사 학 위 논 문
지도교수 서화정

향상된 보안성을 지닌 새로운 유형의 보안 키패드 제안

닌텐도 스위치의 신규 보안 키패드 제안

A suggest for new shape of security keypad with improved security

2019년 12월 일

한 성 대 학 교 대 학 원

I T 융 합 공 학 과

I T 융 합 공 학 전 공

권 혁 동

석 사 학 위 논 문
지도교수 서화정

향상된 보안성을 지닌 새로운 유형의 보안 키패드 제안

닌텐도 스위치의 신규 보안 키패드 제안

A suggest for new shape of security keypad with improved security

위 논문을 공학 석사학위 논문으로 제출함

2019년 12월 일

한 성 대 학 교 대 학 원

I T 융 합 공 학 과

I T 융 합 공 학 전 공

권 혁 동

권혁동의 공학 석사학위 논문을 인준함

2019년 12월 일

심사위원장 _____(인)

심 사 위 원 _____(인)

심 사 위 원 _____(인)

국 문 초 록

향상된 보안성을 지닌 새로운 유형의 보안 키패드 제안

한 성 대 학 교 대 학 원
I T 융 합 공 학 과
I T 융 합 공 학 전 공
권 혁 동

닌텐도 스위치(Nintendo Switch, NSW)는 가정용 게임기로 시대 분류상 8세대 게임기에 속한다. 닌텐도 스위치는 하이브리드 형태로 TV와 연결하는 거치 형태로 사용하거나 가볍게 들고 다니는 휴대 형태로 사용할 수 있다. 닌텐도 스위치는 동세대의 다른 게임기들과 마찬가지로 온라인 접속 기능을 내장하고 있으며, 사용자는 자신의 계정과 패스워드를 사용한 인증을 통해서 각종 서비스를 제공받을 수 있다. 사용자는 자신의 패스워드를 입력하기 위해 닌텐도 스위치에 내장된 보안 키패드를 사용하게 된다. 닌텐도 스위치의 보안 키패드는 닌텐도 스위치의 컨트롤러를 사용해서 입력하기 편리하고 직관적이나, 화면을 보는 것만으로도 입력이 전부 노출된다는 단점이 있다. 따라서 해당 문제를 개선하여 익명의 공격자가 화면을 지켜보더라도 패스워드가 노출되지 않는 새로운 키패드를 제안한다. 본 논문에서는 기존 닌텐도 스위치의 보안 키패드가 지닌 문제점을 지적하며, 본 문제점을 개선한 새로운 키패드를 설계 및 구현한 결과물을

제시한다. 또한 기존 키패드와 제안하는 키패드의 성능 비교를 위해 다수의 실험자를 동원하여 키패드를 사용한 결과를 정리한다. 실험 결과를 통해 제안하는 키패드가 기존 키패드보다 더 뛰어난 보안성을 지닌 것을 확인한다. 추가로 단일 인증만 제공하는 닌텐도 스위치에 NFC 기능을 사용한 이중 인증을 도입하여 더 강한 보안성을 제공할 수 있는 인증 체계를 제안한다.

【주요어】 근거리 무선 통신, 닌텐도 스위치, 보안 키패드, 훔쳐보기 공격

목 차

표 목 차

그 림 목 차

제 1 장 서론

제 1 절 닌텐도 스위치

닌텐도 스위치는 닌텐도 Wii U의 부진을 타개하기 위해 출시한 게임기로, 17년 3월 3일에 첫 기기가 출시되었고 19년 7월 17일에 새로운 공정을 적용한 신형 기기가 출시되었다. 게임기는 시대에 따라 지속적으로 발전하여 세대별로 구분하게 되었고, 닌텐도 스위치는 8세대 게임기로 분류된다. 닌텐도 스위치의 자세한 스펙은 [표 1-1]과 같다. [표 1-1]의 기기 스펙은 구형 닌텐도 스위치의 스펙이며, 신형 닌텐도 스위치와는 기기 스펙이 다르다. [표 1-1]의 내용에는 닌텐도 스위치 본체뿐만 아니라 독 및 전용 컨트롤러인 조이콘의 스펙까지 기재한다.

[표 1-1] 닌텐도 스위치와 주변 기기의 스펙

Switch Console	
Display	6.2“ with 1280x720 resolution
CPU/GPU	NVIDIA customized Tegra processor
Storage	32GB Expandable via microSD/microSDHC/microSDXC memory cards
Wireless Connectivity	802.11a/b/g/n/ac Wi-Fi Bluetooth 4.1
Ports	USB Type-C

	3.5mm audio jack
Maximum Resolution in TV Mode	1920x1080 at 60FPS
Media	Proprietary Switch solid-state game cards
Sensors	Accelerometer Gyroscope Ambient light sensor
Battery	4310mAh lithium-ion rechargeable
Switch Dock	
Ports	2x USB 2.0 ports HDMI port System connector AC power adapter port
Joy-Con	
Sensors	Accelerometer Gyroscope IR motion camera(Joy-Con R only)
Connectivity	Bluetooth 3.0 NFC
Battery	525mAh lithium-ion rechargeable

닌텐도 스위치는 들고 다닐 수 있는 휴대용 게임기지만, 전용 독에 거치하는 것으로 TV와 연결해서 마치 가정용 게임기처럼 사용할 수도 있다. 이를 독 모드라 칭한다.

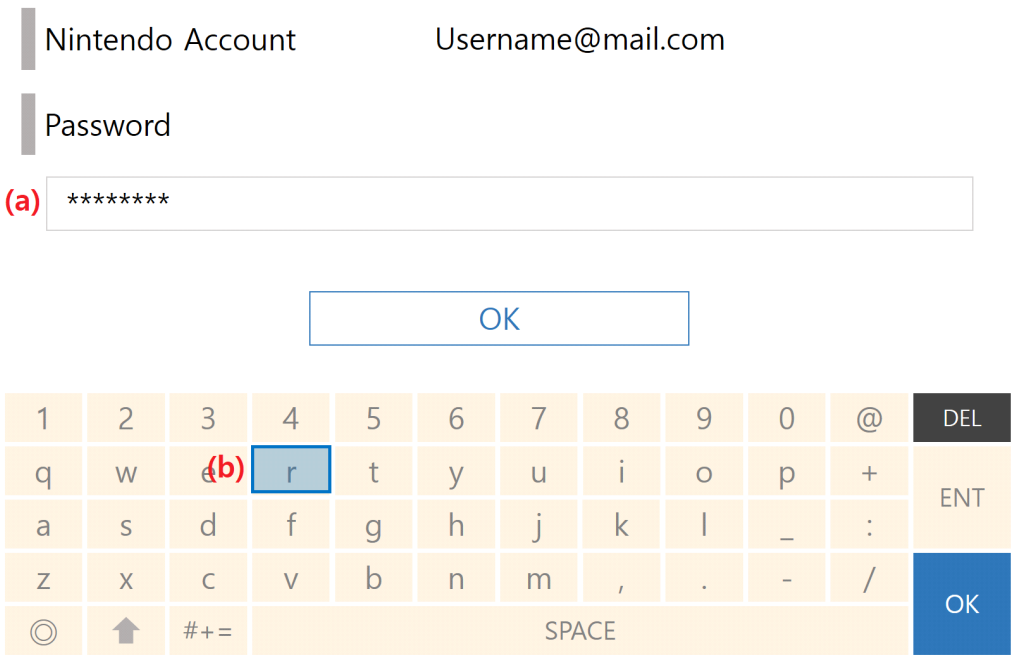
또한 닌텐도 스위치는 자체적인 컨트롤러인 조이콘과 별매인 프로콘을 지원한다. 본 논문에서는 조이콘에 관해서만 서술하도록 한다. 조이콘은 블루투스 3.0을 사용하여 본체와 연결할 수 있고, 최대 여덟 쌍의 조이콘을 등록할 수 있으며 내장된 NFC 기능을 통해 NFC 스캔도 가능하다. 조이콘의 외형은 [그림 1-1]과 동일하다.

마지막으로 닌텐도 스위치는 무선 인터넷 기능을 사용하여 온라인에 접속할 수 있다. 이때 사용자 인증으로 계정과 패스워드를 통한 인증을 거치며, 패스워드 입력 시에는 닌텐도 스위치의 액정 화면을 터치하는 것으로 입력할 수 있으나, 독 모드에서는 조이콘을 통해서만 입력할 수 있다.

[그림 1-1] 닌텐도 스위치의 조이콘 실물

제 2 절 문제 제기 및 해결 방안 제안

닌텐도 스위치는 온라인 접속을 위해서 패스워드를 입력할 필요가 있다. 만약 본체가 독 모드라면 패스워드 입력 수단은 전용 컨트롤러인 조이콘으로 한정된다. 닌텐도 스위치에서 패스워드를 입력할 때는 [그림 1-2]와 같은 보안 키패드를 사용한다.



[그림 1-2] 닌텐도 스위치의 보안 키패드

[그림 1-2]에서 (a) 부분에 사용자가 입력한 패스워드가 표시된다. 실제로는 패스워드의 유출을 막기 위해서 '*' 문자로 비식별 조치가 취해진다. (b) 부분은 사용자가 현재 선택중인 커서의 위치이다. 터치를 통해서 패스워드를 입력할 때는 커서가 필요 없지만, 독 모드라면 조이콘의 방향키 입력과 확인 버튼을 통해 패스워드를 입력해야 하므로 커서를 표시해줘야 한다.

이때 독 모드로 인하여 큰 화면으로 커서의 움직임을 확인할 수 있기에 훔쳐보기 공격을 시도할 수 있다. 즉, 독 모드 상태에서 근처에 누군가가 있다면 화면을 보는 것으로 훔쳐보기 공격을 하여 패스워드를 알아낼 수 있다. 여러 사람들과 모여서 즐기는 게임이 많은 닌텐도 스위치의 특성상, 훔쳐보기 공격 환경이 갖춰질 기회가 매우 잦으며, 그에 따라 패스워드 노출 가능성도 급증한다.

본 논문에서는 닌텐도 스위치의 보안 키패드가 지닌 보안 취약점을 개선한 새로운 보안 키패드를 제안한다. 제안하는 키패드는 커서 노출 취약점을 제거하여 훔쳐보기 공격에 내성을 지니게 된다. 제안 방법의 우수성을 확인하기 위해서 기존 보안 키패드와 제안하는 보안 키패드를 사용할 때 훔쳐보기 공격을 시도하여 공격 성공 횟수를 비교한다. 이를 통해 근처에 다수의 다른 사람이 있더라도 안전한 패스워드 입력을 시도할 수 있는 환경을 구축한다. 또한 조이콘의 NFC 스캔 기능을 이용하여 이중 인증을 할 것을 제안한다. 이는 패스워드가 노출되더라도, NFC 인증에 필요한 사물을 가지고 있지 않다면 최종적으로 인증에 실패하도록 한다. 이것으로 인해 공격자가 계정을 탈취할 가능성을 매우 낮추어서 안전한 계정 보안을 확보할 수 있게 해준다.

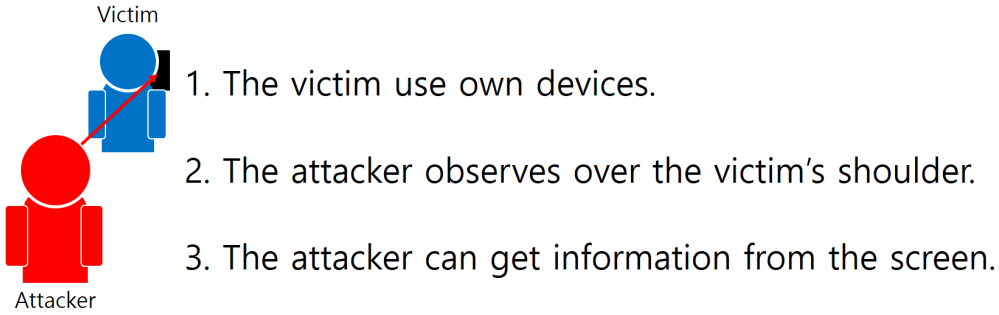
제 3 절 논문 구성

본 논문의 구성은 다음과 같다. 2장에서 훔쳐보기 공격에 대한 기법과 기존에 제안되었던 보안 키패드를 소개한다. 3장에서는 공격 시나리오에 대해서 확인한다. 이어서 4장에서는 제안하는 보안 키패드와 이중 인증 방법에 대해 설명한다. 5장에서는 기존 보안 키패드와 제안하는 보안 키패드의 성능 비교를 통해 제안 기법의 우수성을 확인하며 이중 인증을 통한 보안성 향상에 대해 검토한다. 마지막으로 6장에서 본 논문의 결론을 내리고 향후 과제를 제시한다.

제 2 장 관련 연구

제 1 절 훔쳐보기 공격

훔쳐보기 공격(Shoulder Surfing Attack)은 단순한 형태의 공격으로, 공격자가 피해자의 근처에 서서 피해자가 조작하는 기기를 관찰하여 기기의 화면에서 각종 정보를 획득하는 공격이다. 구체적인 공격 형태는 [그림 2-1]에서 확인할 수 있다.



[그림 2-1] 훔쳐보기 공격 과정

우선 공격자가 피해자의 뒤에 위치한다. 피해자는 자신의 장비를 평범하게 사용한다. 이때 공격자는 피해자의 어깨 너머로 피해자의 장비 화면을 관찰할 수 있다. 만일 피해자가 뒤에 있는 공격자를 인지하지 못하고 일반적으로 기기를 사용한다면, 화면이 노출되기 때문에 공격자는 어깨 너머로 피해자가 보고 있는 정보를 입수할 수 있다. 만일 피해자가 기기를 통해 패스워드 같은 특정 입력을 진행한다면, 입력 값에 비식별 조치가 취해지더라도 어깨 너머에서 입력 값의 좌표를 확인할 수 있기 때문에 공격자가 입력 값 전체를 획득할 가능성이 생긴다.

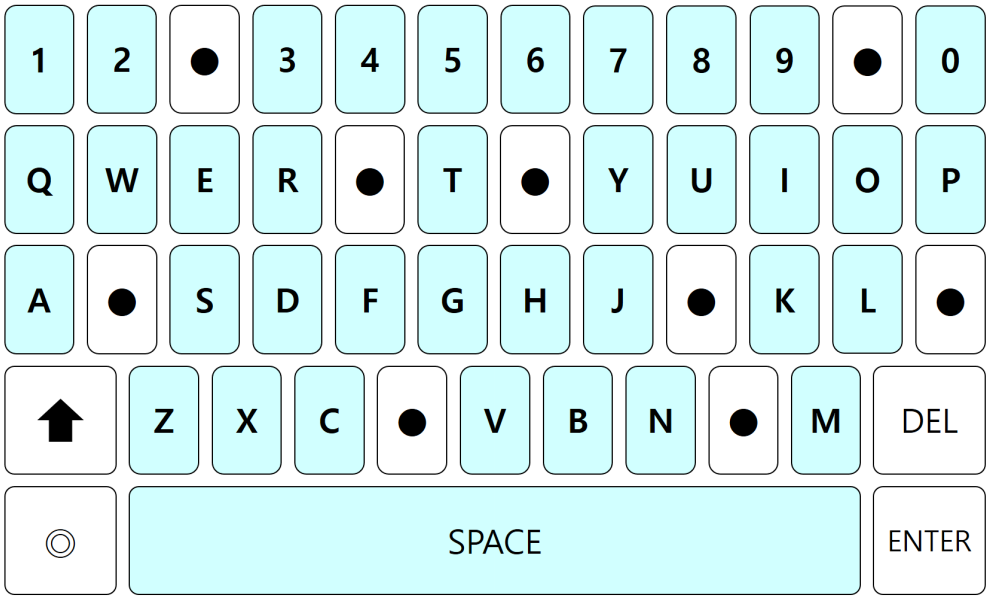
제 2 절 보안 키패드

보안 키패드는 입력 값에 대해 강력한 보안이 필요할 때, 각종 보안 위협에서 입력 값을 보호할 수 있는 특별한 키패드를 의미한다. 보안 키패드는 사용자의 편의성 증대를 위해서 일반적인 키패드와 유사한 쿼티 키보드 레이아웃을 사용한다. 하지만 레이아웃을 그대로 사용하게 되면 입력 좌표 유출로 인해 입력 값을 유추할 수 있는 문제가 발생한다. 따라서 보안 키패드는 입력 값을 암호화하는 것 외에도 입력 좌표를 획득하기 어렵게 하거나, 각 입력 시도마다 동일 입력 좌표 상에서 서로 다른 입력 값이 입력되도록 하는 기법을 사용한다.

1) 공백 삽입 보안 키패드

공백 삽입 보안 키패드는 [그림 2-2]와 같이 키 사이사이에 무작위로 공백을 삽입하는 보안 키패드이다. 공백은 키패드가 실행될 때마다 위치가 변경되기 때문에 입력 좌표가 같더라도 입력 값 자체는 다를 가능성이 생긴다.

공백 위치가 변화하는 경우는 크게 두 가지로 나눌 수 있다. 하나는 키패드가 실행될 때이다. 사용자가 패스워드 입력 등을 위해 키패드를 호출할 경우, 호출하는 순간 공백의 위치가 정해지며 이는 입력 완료와 같은 사유로 키패드가 종료될 때까지 동일한 위치를 유지한다. 또 다른 유형은 키패드 상에서 입력을 할 때마다 공백 위치가 약간씩 변화하는 것이다. 이 유형은 사용자가 조금 불편할 수 있지만, 키패드가 종료되지 않더라도 좌표가 미세하게 지속적으로 변화하기 때문에 더 높은 보안성을 제공할 수 있다.

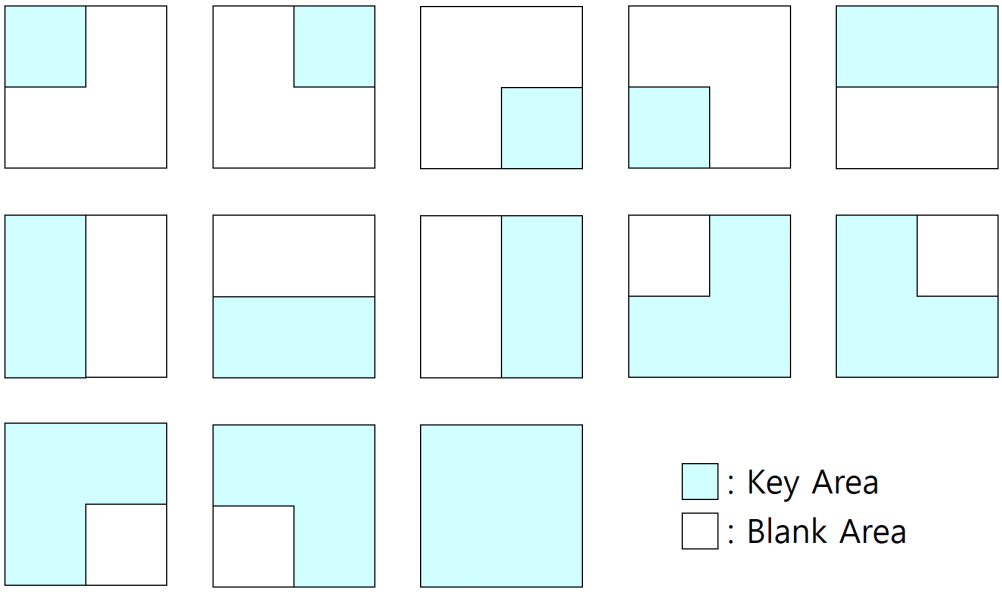


[그림 2-2] 공백 삽입 보안 키패드의 구성

2) 테트리스 블록 보안 키패드

일반적으로 키패드의 키 모양은 사각형을 유지한다. 따라서 키의 위치가 변화하더라도 키의 모양은 계속해서 사각형을 유지하기 때문에 입력 좌표 자체는 균일하게 유지될 가능성이 생기며, 이에 따라 특정 좌표상에서 입력 가능한 값을 예상할 수 있다는 문제점이 있다.

테트리스 블록 보안 키패드는 키 모양이 유지되는 문제점을 개선한 보안 키패드이다. 본 보안 키패드는 키 모양을 단순 사각형이 아닌, [그림 2-3]의 13가지 형태로 사용한다. 동작 과정은 다음과 같다. 우선 키패드가 실행될 때 모든 키는 무작위로 키 형태를 할당 받는다. 모든 키의 형태가 정해졌으면 형태에 맞춰서 키를 배치하되, 편의성을 위해 쿼티 키보드 레이아웃을 따라간다. 이는 모든 키의 형태가 매번 다르게 정해지기 때문에 배치되는 형태도 매번 달라지며, 키패드의 모양이 크게 바뀌게 된다. 따라서 입력 좌표를 획득하더라도 해당 좌표의 값이 이전과는 다를 가능성이 매우 높아지게 된다. 또한 키패드의 모양도 크게 변화하기 때문에 통상적인 보안 키패드와 동일한 공격을 시도하기도 어렵다.



[그림 2-3] 테트리스 블록 보안 키패드의 13가지 키 형태

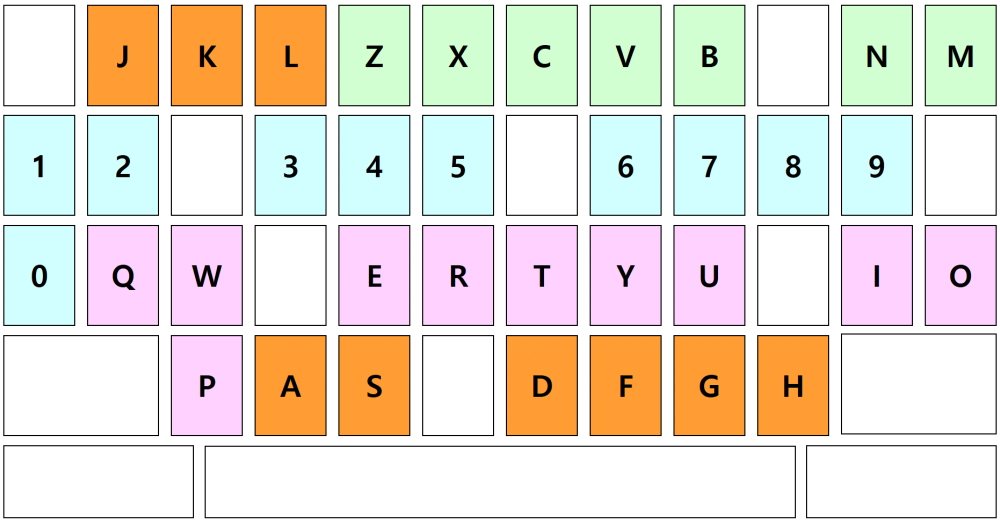
3) 유동적 행 배치 보안 키패드

일반적으로 보안성을 향상하기 위해서는 편의성이 희생되고는 한다. 하지만 너무 편의성이 떨어지면 사용자를 확보하기 어렵기 때문에 일정 수준의 편의성을 유지하고자 한다. 이에 따라 보안 키패드는 사용자 편의성을 제공하기 위해서 가장 많은 사용자를 보유한 쿼티 레이아웃을 사용한다. 하지만 쿼티 레이아웃을 그대로 사용하게 되면 입력 좌표를 크게 바꾸기 어렵기 때문에 일정 수준 이상의 공격은 제대로 방어하기 어렵다.

때문에 새로운 형태의 보안 키패드가 제안되었으며, 본 키패드는 쿼티 레이아웃을 일정 수준을 유지하지만 키의 시작 위치가 다르게 되어있다. [그림 2-4]에서 제안된 보안 키패드의 구조를 확인할 수 있다. [그림 2-4]의 같은 색으로 칠해진 키는 실제 쿼티 레이아웃에서 하나의 행에 놓여있는 부분이다. 정확히는, 1부터 0까지 있는 첫 행이 배치된다면 그 이후에는 Q부터 P까지 있는 행이, 그 다음에는 A부터 L까지 있는 행이 배치되며 마지막에는 Z부터 M까지 키가 배치된다. 전체적으로 키가 무작위로 배치된 것처럼 보이지만, 실제로는 1의 위치를 기준으로 쿼티 레이아웃이 유지됨을 확인할 수 있다. 이는 키 위치가 크게 이동하기 때문에

높은 보안성을 확보할 수 있으며 일정 수준의 쿼티 레이아웃을 유지하고 있기 때문에 보안 키패드를 처음 사용하는 사용자라도 손쉽게 키를 찾을 수 있다.

추가로 키패드 중간에 무작위로 공백 키를 삽입하는 것으로 키패드의 전체적인 모양을 유지할 수 있으며 공백으로 인해 무작위성을 더욱 높일 수 있기 때문에 더 높은 보안성을 확보할 수 있다.



[그림 2-4] 유동적 행 배치 보안 키패드의 구성

제 3 절 NFC(Near Field Communication)

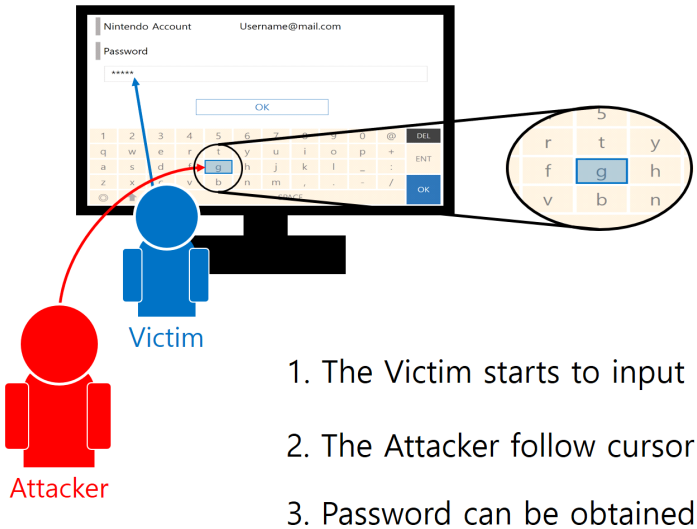
NFC는 RFID(Radio-Frequency Identification) 기술을 응용한 것으로, NFC 기능이 탑재된 기기 간에는 무선통신이 가능하다. NFC는 13.56MHz의 대역폭을 지니며 424kbit/s의 속도를 보인다. RFID와 차이점은, RFID는 단방향 통신이지만 NFC는 양방향 통신을 제공하는 대신 수신 범위가 약 10cm 정도로 매우 짧다. NFC 기술은 교통카드, 파일전송, 도어락 등의 다양한 분야에서 활용할 수 있다. 추가로 최근에는 인증 분야에도 사용되는 추세이다. 가령 NFC 기능을 내장한 스마트폰을 IoT 장치에 인접시켜 사용자 인증 절차를 거치는 방식이 있다. NFC를 인증한 방식은 NFC를 제공하는 기기가 필요하므로 소유인증 방식에 해당한다.

제 3 장 공격 시나리오

제 1 절 훔쳐보기 공격 시나리오

닌텐도 스위치는 전용 독에 장착하여 TV 출력을 하는 독 모드와 들고 다니면서 게임을 즐기는 휴대 모드가 존재한다. 이때 휴대 모드의 훔쳐보기 공격은 스마트폰 같은 휴대기기에 대한 훔쳐보기 공격과 유사하다. 또한 본 논문에서 제안하는 방안은 조이콘을 사용하여 패스워드 입력 시, 커서 노출을 개선하는 부분이기에, 본 절에서 서술하는 훔쳐보기 공격은 닌텐도 스위치가 독 모드로 동작한다는 전제조건이 필요하다.

닌텐도 스위치가 독 모드로 동작하는 중에 훔쳐보기 공격을 시도한다면 [그림 3-1]과 같은 상황이 발생한다.



[그림 3-1] 닌텐도 스위치 보안 키패드에 대한 훔쳐보기 공격 시나리오

우선 사용자가 자신의 패스워드를 입력하기 위해 보안 키패드를 호출하여 패스워드를 입력하기 시작한다. 독 모드 중에는 닌텐도 스위치의 터

치스크린이 동작하지 않기 때문에 조이콘을 사용하여 입력하여야 한다. 조이콘을 사용할 때는 사용자가 자신이 어떤 키를 선택 중인지 알 수 없기 때문에 커서가 화면에 표시된다. 사용자는 조이콘의 스틱을 사용해서 커서를 이동하고 원하는 키에 커서가 올라가면 입력 버튼을 통해 패스워드를 입력할 수 있고, 이 과정을 반복하여 패스워드 전체를 입력할 수 있다.

패스워드를 입력하는 중에는 근처에 누군가가 있을 수 있다. 편의상 이를 공격자라 칭한다. 훔쳐보기 공격은 일반적으로 공격자의 어깨 너머, 즉 뒤에서 이루어지나 현재 주어진 상황은 TV 화면이기 때문에 휴대용 기기에 비해 화면이 크다. 따라서 사용자와의 위치와는 상관없이 TV 화면이 보이는 곳이면 공격자가 어느 곳에 위치해도 상관없다.

패스워드 입력란은 입력 값이 '*'와 같은 문자로 비식별 조치가 취해진다. 따라서 입력란에서는 패스워드 유출이 발생하지 않는다. 하지만 사용자에게 제공되는 커서 위치는 노출된다. 공격자는 노출된 커서를 추적하며 커서가 멈추고 패스워드 입력란에 문자가 추가되는 것을 확인한다. 만약 패스워드 입력란에 문자가 추가된다면 현재 커서가 위치한 자리의 문자가 입력된 것이다. 가령 [그림 3-1]과 같이 커서가 'g'에 멈춘 상태로 '*' 문자가 입력된 것을 확인한다면, 사용자가 'g' 문자를 입력한 사실을 알 수 있다. 이 과정을 반복하는 것으로 사용자의 전체 패스워드를 알아낼 수 있다.

닌텐도 스위치는 사용자 경험을 향상시키기 위해 각종 효과음이나 진동을 효과적으로 사용한다. 만약 사용자가 패스워드를 입력하고 있을 때, 스피커가 켜져 있다면 값을 입력할 때 효과음이 발생하기 때문에 공격이 더욱 쉬워진다.

제 2 절 패스워드가 확보 된 시나리오

3장 1절에서 닌텐도 스위치 보안 키패드의 커서 노출 보안 취약점을 사용하여 패스워드 노출 가능성을 확인하였다. 실제로 닌텐도 스위치에서

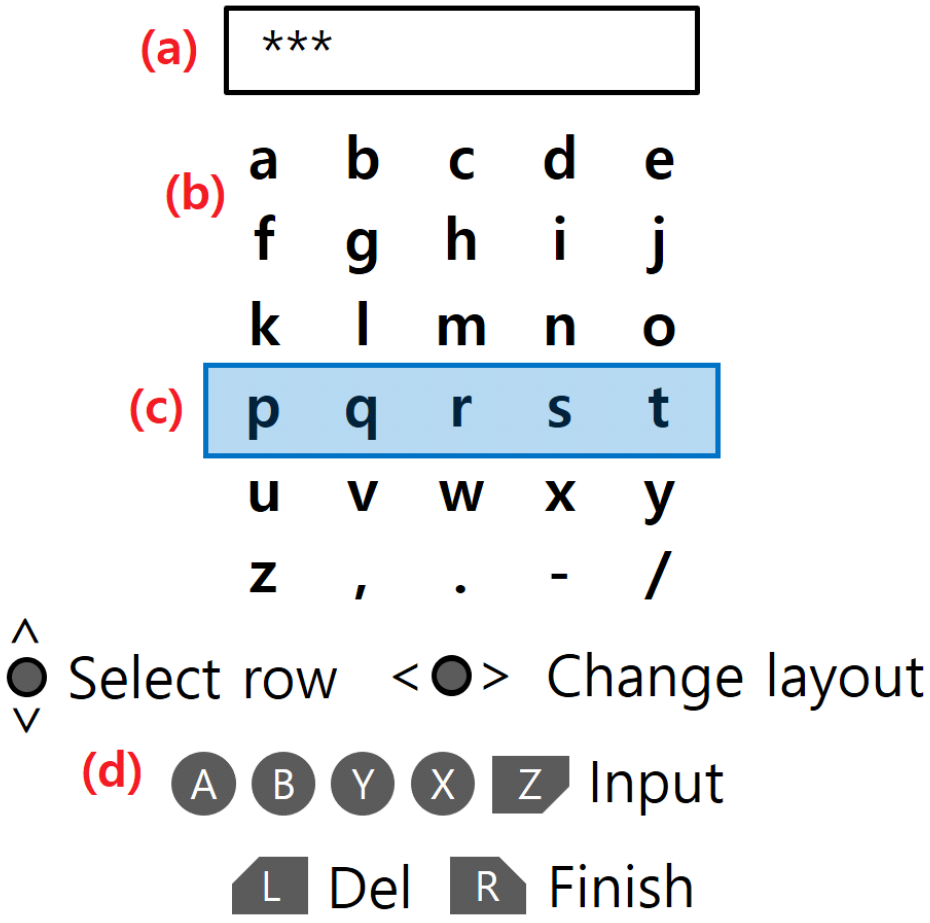
패스워드의 입력은 온라인 숍에 접속하는 등, 닌텐도 계정에 접속할 때만 사용된다. 즉 닌텐도 스위치 자체의 잠금 해제 시에는 패스워드가 필요하지 않다. 때문에 패스워드를 확보한 공격자가 닌텐도 스위치의 잠금을 풀고 온라인 기능에 접근하는 것을 방지할 수가 없다.

이는 닌텐도 스위치에 잠금 기능이 존재하지 않기 때문이다. 닌텐도 스위치는 'Parental controls'라는 보호자 관리 기능을 제공한다. 하지만 보호자 관리 기능은 아이의 기기 누적 이용 시간, 플레이한 소프트웨어 등의 확인이 가능할 뿐, 기기 자체를 잠그는 기능은 존재하지 않는다. 따라서 공격자가 3장 1절의 방법대로 패스워드를 탈취하는데 성공한다면 언제든지 닌텐도 스위치의 잠금을 해제하여 계정을 사용할 수 있다.

제 4 장 제안 기법

제 1 절 행렬 형태 보안 키패드

닌텐도 스위치 보안 키패드의 취약점은 커서가 노출된다는 점이다. 그러므로 본 취약점을 제거하는 것으로, 훔쳐보기 공격에 내성을 가질 수 있는 새로운 보안 키패드를 제안하는 바이다. 제안하는 키패드의 구성은 [그림 4-1]과 같다.



[그림 4-1] 행렬 형태 보안 키패드의 구성

[그림 4-1]은 크게 네 부분으로 나눌 수 있다. [그림 4-1]의 (a) 부분은 패스워드 입력란이다. 사용자가 입력한 값이 패스워드 입력란에 표시되며, 기본적으로 '*' 문자로 비식별 조치가 적용된다. (b) 부분은 키가 위치한 부분이다. (c) 부분은 초기 행의 위치를 표시해주는 표식으로, 키패드가 실행된 직후 잠깐 표시되고 사라진다. 마지막으로 (d)는 간단 조작 방법을 알려주는 부분이다. 닌텐도 스위치는 메뉴를 호출할 때 사용자가 조작법을 모를 수 있다는 전제를 가정하고 항시 조작법을 알려준다. 이에 착안하여, 제안하는 보안 키패드는 사용자에게 익숙한 형태가 아니므로 조작법을 표시해줘서 사용자가 조작에 어려움을 겪지 않도록 한다.

구체적인 사용 방법은 다음과 같다. 사용자는 보안 키패드 실행 직후 초기 선택 행을 확인한다. 이는 화면에 표시되는 표식을 통해 확인할 수 있다. 표식은 보안 키패드가 실행 된 후 2초 내로 화면에서 사라진다. 사용자는 스틱을 상하로 조작하는 것으로 선택 중인 행을 옮길 수 있다. 즉, 선택 중인 행에 원하는 키가 없다면 필요한 키가 있는 행으로 이동해야 한다. 버튼 A, B, Y, X, Z는 각각 1열, 2열, 3열, 4열, 5열을 선택하는 것으로, 현재 선택 중인 행과 버튼 입력을 통해 선택한 열상의 교차 값을 입력 값이 된다. 가령 첫 번째 행을 선택 중에 A버튼을 입력한다면 'a'가 입력 값이 된다. 현재 레이아웃에 대문자, 특수문자 등의 사유로 원하는 키가 존재하지 않는다면 스틱을 좌우로 조작하는 것으로 레이아웃을 변경할 수 있다. 마지막으로 L버튼을 통해 잘못 입력한 값을 제거할 수 있으며, R버튼을 통해 입력을 완료할 수 있다. 행을 이동하다가 가장 위나 아래에 위치하게 된다면 위치한 곳에 따라 조이콘에 특별한 패턴의 진동이 발생한다. 이를 통해 사용자에게 가장 바깥쪽 행에 도달했음을 알릴 수 있으며, 만약 사용자가 자신이 선택한 행을 잊었다면, 스틱을 여러 번 기울여서 커서를 양 끝 행에 위치시켜서 선택한 행을 다시 인지할 수 있다. [표 4-1]은 제안하는 보안 키패드의 의사코드로 전체적인 동작 원리를 코드로 이해할 수 있다.

[표 4-1] 행렬 형태 보안 키패드의 의사코드

Pseudocode for matrix shape security keypad

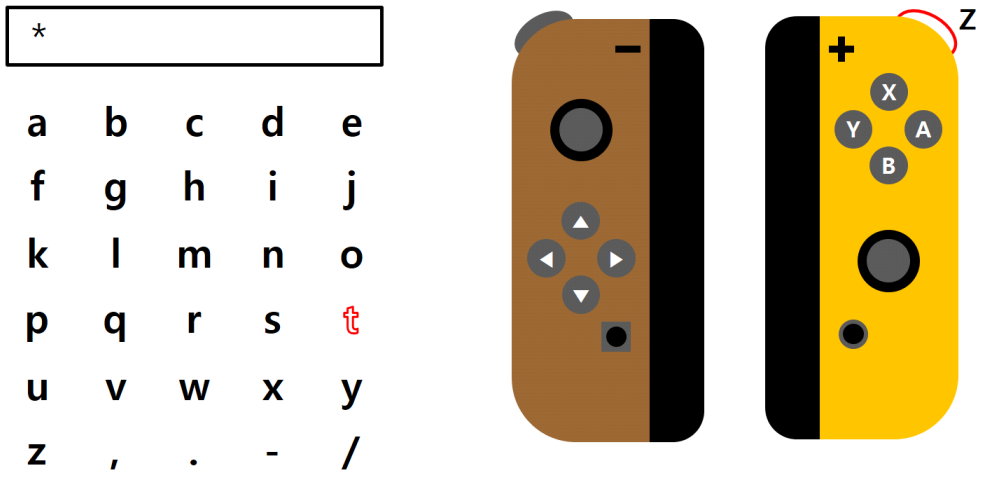
```
1:  The security keypad called
2:  Initialize row = 1 to 6 randomly
3:  Initialize keyLayout = 1
4:  Display initialized row about 2 second
5:  Loop 6-28 line, until user press right button
6:    if(signal = stickUp or stickDown)
7:      row = row + 1 or row - 1
8:        if(row <= 1)
9:          row = 1, Vibrating Joy-con
10:       else if(row >= 6)
11:         row = 6, Vibrating Joy-con
12:   else if(signal = stickLeft or stickRight)
13:     keyLayout = keyLayout + 1 or keyLayout - 1
14:     if(keyLayout < 1)
15:       keyLayout = 4
16:     else if(keyLayout > 4)
17:       keyLayout = 1
18:     change keyboard layout
19:   else if(signal = A or B or Y or X or Z)
20:     column = 1 or 2 or 3 or 4 or 5
21:     inputValue = (row, column)
22:     add inputValue to password input value
23:     add '*' character to password field
24:   else if(signal = leftButton)
25:     remove last input value from password input value
26:     remove last '*' character from password field
27:   else if(signal = rightButton)
28:     escape loop
29: Terminate the security keypad
```

위치가 따로 떨어져있는 Z버튼을 제외하고, 일반적으로 버튼의 순서는 A, B, X, Y버튼 순서로 구성되어 있다. 하지만 제안하는 보안 키패드는 A, B, Y, X버튼 순서로 열을 할당하고 있다. 만약에 A, B, X, Y버튼 순서로 키를 배치한다고 가정한다. 1열, 2열을 담당하는 A, B버튼은 시계 방

향으로 배치가 이루어지기에, 사용자는 3열 버튼도 시계 방향에 놓여있을 것이라 추측하기 쉽다. 하지만 [그림 1-1]에서 조이콘의 실물을 확인해 보면, X버튼은 시계 방향 규칙을 따르지 않고 다른 자리에 놓여있으며 시계 방향 자리에는 Y버튼이 놓여있다. 따라서 사용자의 직관성을 높이기 위해서 A, B, Y, X버튼 순서로 열을 할당하게 되었다. 물론 사용자에 따라서 이러한 배치가 불편할 수 있으므로 A, B, X, Y버튼 순서로 배치하는 설정을 제공하는 것으로 각자가 편리한 환경을 구축할 수 있다.

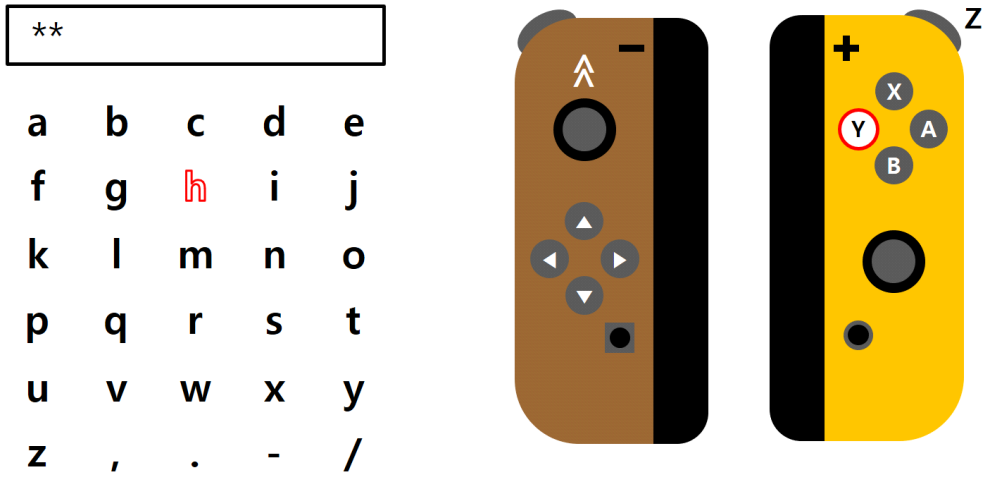
제 2 절 보안 키패드 동작 과정

본 논문의 4장 1절에서 행렬 형태 보안 키패드에 대해서 알아보았다. 이어서 본 절에서는 제안하는 보안 키패드의 구체적인 동작 과정에 대해서 확인한다.



[그림 4-2] 첫 번째 문자 't' 입력 과정

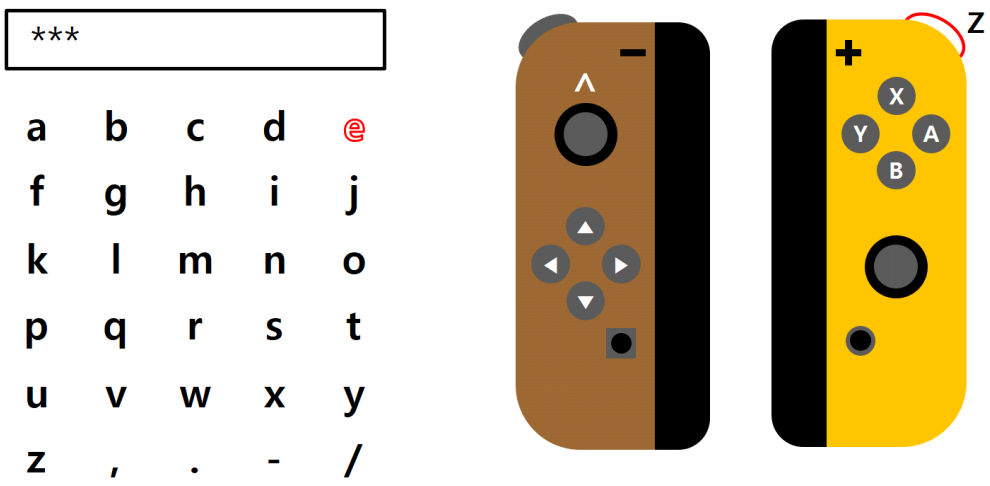
사용자의 패스워드는 'thesis'이며 4장 1절의 [그림 4-1]과 같이 최초의 행 위치는 네 번째 행에 있음을 가정한다. 사용자는 음영을 통해 초기 행 위치를 확인한다. 처음 입력하고자 하는 문자는 't'이다. 't'는 초기 선택된 행의 5열에 위치하므로 스틱은 조작하지 않고 [그림 4-2]와 같이 Z 버튼을 눌러 't' 문자를 입력한다.



Second Step: Input 'h'
-> Steer up the stick twice
-> Press the 'Y' button

[그림 4-3] 두 번째 문자 'h' 입력 과정

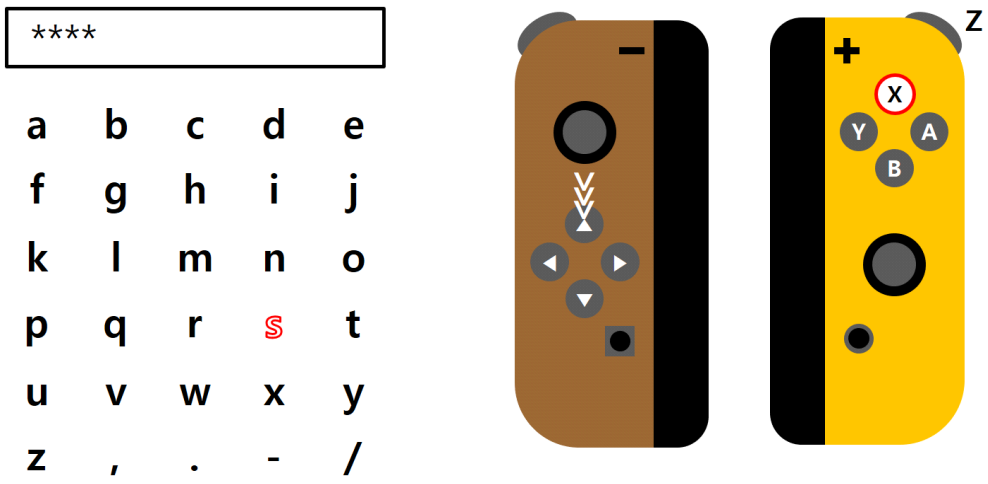
다음 문자인 'h'는 두 번째 행의 세 번째 열에 위치하며, 이는 현재 선택된 행보다 두 행 위에 있다. 따라서 사용자는 스틱을 위로 두 번 기울여서 'h'가 위치한 행으로 이동한다. 초기 표식을 제외하고 행을 표시하는 기능이 없기 때문에 이 과정은 화면에 표시되지 않는다. 사용자는 두 번째 행에 커서를 위치시켰다면 세 번째 열을 선택하기 위해 Y버튼을 입력한다. 본 과정은 [그림 4-3]에서 명확하게 확인할 수 있다.



Third Step: Input 'e'
-> Steer up the stick once
-> Press the 'Z' button

[그림 4-4] 세 번째 문자 'e' 입력 과정

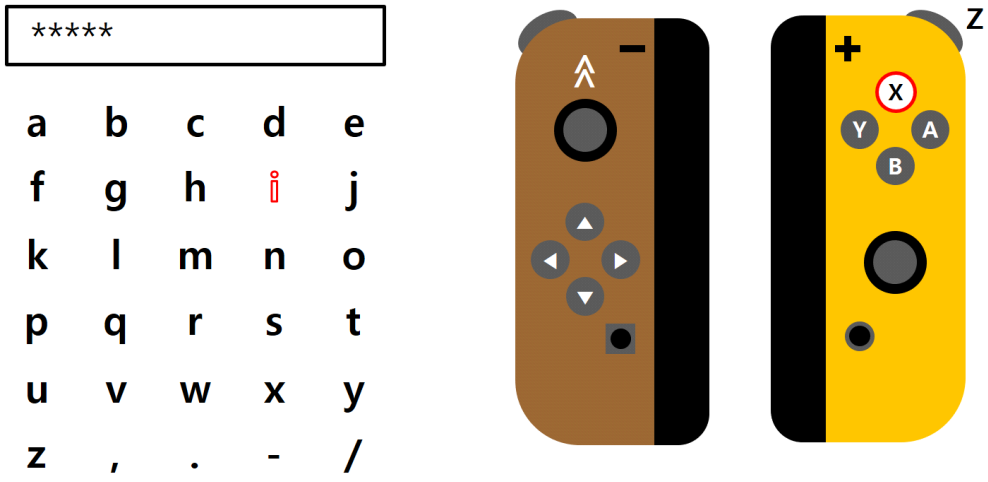
다음 문자인 'e'는 첫 번째 행의 다섯 번째 열에 위치한다. 이는 현재 선택 중인 행보다 하나 위이므로, 사용자는 스틱을 한 번 위쪽으로 기울여서 첫 번째 행으로 커서를 이동한다. 행이 선택되었으므로 Z버튼을 눌러 다섯 번째 열을 선택하여 'e'를 입력한다. 이는 [그림 4-4]의 과정과 동일하다.



Fourth Step: Input ‘s’
-> Steer down the stick three times
-> Press the ‘X’ button

[그림 4-5] 네 번째 문자 ‘s’ 입력 과정

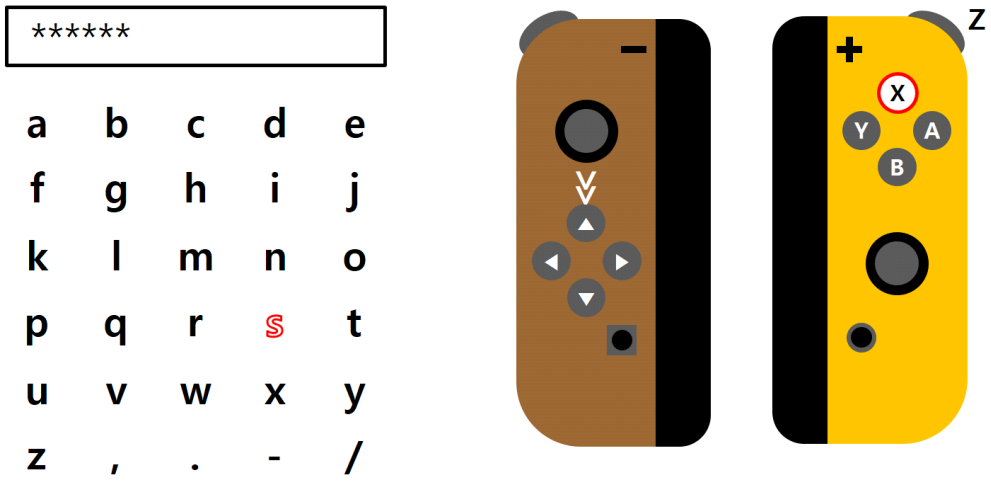
그 다음 입력 값인 ‘s’는 네 번째 행의 네 번째 열에 위치한다. 현재 선택 중인 행은 첫 번째 행이므로 사용자는 스틱을 아래로 세 번 기울여서 네 번째 행으로 커서를 이동한다. 그 후 X버튼을 입력하여 네 번째 열을 선택하는 것으로 ‘s’를 입력한다. [그림 4-5]에서 가시화 된 과정을 확인할 수 있다.



Fifth Step: Input 'i'
-> Steer up the stick twice
-> Press the 'X' button

[그림 4-6] 다섯 번째 문자 'i' 입력 과정

다섯 번째 입력 값인 'i'는 두 번째 행의 네 번째 열에 위치해있다. 현재 선택 중인 행은 네 번째 행이므로 스틱을 위쪽으로 두 번 기울여서 두 번째 행을 선택한 다음, X버튼을 눌러 네 번째 열을 선택한다. 'i'를 입력하는 본 과정은 [그림 4-6]에서 확인할 수 있다.



Final Step: Input ‘s’
-> Steer down the stick twice
-> Press the ‘X’ button

[그림 4-7] 마지막 문자 ‘s’ 입력 과정

마지막으로 다시 ‘s’ 문자를 입력해야 한다. ‘s’ 문자는 네 번째 행의 네 번째 열에 위치해있다. 따라서 현재 두 번째 행을 선택 중이므로, 스틱을 두 번 아래로 기울인 다음 네 번째 열을 선택하기 위해 X버튼을 누른다. 이로서 ‘s’를 입력할 수 있고 [그림 4-7]은 본 과정을 묘사한 그림이다.

이와 같은 단계를 거쳐 ‘thesis’라는 패스워드를 입력할 수 있었다. 만약 입력 값에 대문자나 특수문자 등의 값이 있다면 스틱을 좌우로 기울이는 것으로 대문자 레이아웃 또는 특수문자 레이아웃을 호출하여 입력할 수 있다. 특히 대문자의 경우에는 쿼티 레이아웃과 마찬가지로 대소문자만 다르고 키의 위치는 동일하기 때문에 사용자가 문자의 위치를 파악하는데 어려움을 겪지 않게 하였다.

제 3 절 조이콘을 사용한 NFC 이중 인증

본 논문에서는 닌텐도 스위치의 보안 키패드가 훔쳐보기 공격에 취약

점을 지니고 있었음을 확인하였고, 이를 개선한 행렬 형태 보안 키패드를 제안하였다. 하지만 이미 패스워드가 노출된 상황이라면 인증 과정을 손쉽게 통과할 수 있기 때문에 추가적인 인증 수단을 제안한다.

닌텐도 스위치의 컨트롤러인 조이콘 중 우측 조이콘에는 NFC 스캔 기능이 있다. 본디 이 NFC의 용도는 닌텐도 스위치와 호환이 되는 아미보(Amiibo)라는 제품을 스캔하여 게임에서 활용하는 것이다. 닌텐도 스위치가 발매된 이후 다양한 사용자들의 연구를 통해, NFC 기능이 포함된 스마트폰은 아미보 NFC 신호를 발생시킬 수 있게 되었다. 즉 스마트폰에서 만든 NFC 신호를 닌텐도 스위치의 조이콘으로 스캔할 수 있다. 이를 활용하여 다음과 같은 NFC 인증을 제안한다.

사용을 위해서 최초 등록 과정이 필요하다. 닌텐도 스위치 스마트폰 인증을 활성화 한 다음, 스마트폰에 NFC 신호를 발생시키고 우측 조이콘을 통해 신호를 스캔한다. 이후 [그림 4-8]과 같이 인증이 필요할 때 사용자 인증을 요청한다. 인증 시에는 등록과 비슷하게 스마트폰의 NFC 기능을 활성화 한 다음, 우측 조이콘에 스캔하는 것으로 인증이 완료된다.

1. Notify to user that NFC authentication is required.
2. Scan NFC signal of smartphone to Joy-con(right).
3. Authentication completed.

[그림 4-8] NFC 인증 과정

닌텐도 스위치에 NFC 인증이 도입된다면 패스워드 인증과 NFC 인증으로 이중 인증을 거치게 된다. 이는 공격자가 패스워드를 확보하더라도 NFC 인증에 필요한 기기 없이는 최종적으로 인증 완료가 되지 않으므로 기존보다 더 뛰어난 보안성을 제공할 수 있다.

제 5 장 성능 평가

제 1 절 실험 환경

4장에서 기존 닌텐도 스위치의 보안 키패드를 개선한 행렬 형태 보안 키패드와 NFC를 사용한 이중 인증 방식을 제안하였다. 각각의 보안 키패드의 성능을 비교하기 위해서 실험 환경을 다음과 같이 설정하였다.

실험을 위해서 실험 인원 14인을 모집하였고 각각의 키패드 환경에 적응할 수 있도록 연습을 진행하였다. 실험자는 연구진이 제시한 패스워드와 자신이 입력하고 싶은 패스워드를 각각 3회씩 입력한다. 단, 실험자는 자신이 고른 패스워드는 중간에 변경할 수 없다. 연구진은 패스워드의 입력 시간을 측정하는 것으로 편의성을 평가한다. 동시에 실험자에게는 알리지 않고 실험자의 뒤에서 훔쳐보기 공격을 시도하여 보안성도 평가한다. 이때 연구진이 제안한 패스워드 입력 시에는 연구진이 이미 패스워드를 알고 있으므로 시도에서 제외한다.

실험에 사용한 장비는 독 모드의 닌텐도 스위치와 조이콘 한 쌍, 그리고 Galaxy Tab A 8.0과 Galaxy Note5로 안드로이드 기기 두 대 이다. 제안하는 행렬 형태 보안 키패드는 닌텐도 스위치 상에서 구현을 할 수 없으므로 안드로이드 어플리케이션을 통해 간접적으로 구현하기 위해서 안드로이드 기기를 사용하였다. 이때 Galaxy Tab은 독 모드의 스위치 화면을 대체하고 Galaxy Note는 조이콘을 대체한다.

제 2 절 기존 보안 키패드 적용 평가

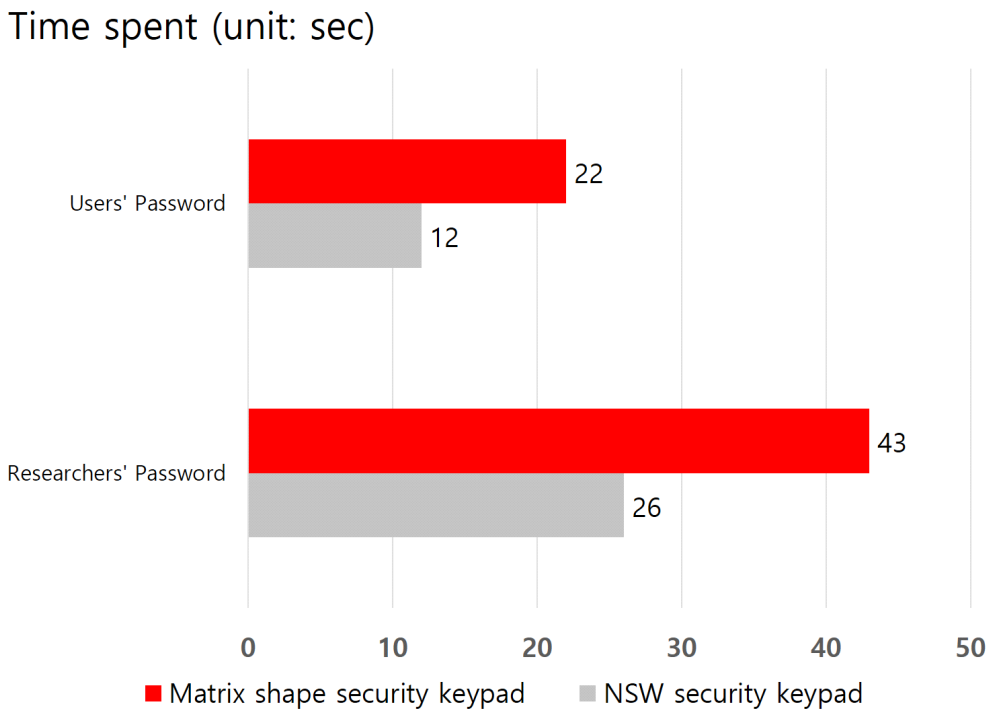
닌텐도 스위치의 보안 키패드와 제안하는 행렬 형태 보안 키패드를 비교하기에 앞서 2장 2절에서 확인한 기존 보안 키패드를 적용했을 때를 가정해본다. 가장 먼저 공백 삽입 보안 키패드이다. 공백 삽입 보안 키패드는 무작위로 공백을 삽입하기 때문에 좌표 탈취로는 정확한 입력 값을 유

추하기가 어렵다. 하지만 닌텐도 스위치는 조이콘을 사용하여 입력해야하기 때문에 사용자에게 커서 표시를 해주지 않는다면 사용자가 보안 키패드를 사용하는 것이 굉장히 어려워진다. 따라서 이를 해결하기 위해 공백 삽입 보안 키패드 상에 커서를 표시한다면, 기존 닌텐도 스위치의 보안 키패드와 마찬가지로 커서 노출로 인한 패스워드 유출 가능성이 발생한다. 테트리스 블록 보안 키패드의 경우에는 각각의 키 모양이 다르므로 키패드 모양이 크게 변할 수 있다. 하지만 공백 삽입 보안 키패드의 경우와 마찬가지로 커서가 노출되게 된다면 패스워드 유출이 일어난다. 유동적 행 배치 보안 키패드는 키 배치가 크게 바뀌는 장점이 있으나 커서 노출은 방지할 수 없다. 레이아웃이 완전히 달라지기에 공격자가 입력 값을 추적하기에 조금 어려울 수 있으나 공격이 가능하다는 점에서 커서 노출 취약점의 방어가 불가능하다.

2장 2절에서 확인한 다양한 형태의 보안 키패드는 키 레이아웃을 변경하여 동일 좌표에서 다른 입력 값이 나오는 것에 집중한다. 닌텐도 스위치 보안 키패드의 문제점은 커서 노출로 인한 훔쳐보기 공격에 취약하다는 것이다. 따라서 기존에 제안된 보안 키패드는 본 사안에 대한 방비책이 없으므로 커서 노출 취약점을 개선할 수 없다.

제 3 절 제안 키패드 편의성 평가

기존 닌텐도 스위치의 보안 키패드와 제안하는 행렬 형태 보안 키패드의 편의성을 평가한다. 편의성의 평가 기준은 입력 시간을 기준으로 하며 입력 시간이 짧을수록 사용자가 문자를 입력하는데 훨씬 편리한 것으로 간주한다. 실험에서는 다수의 실험자가 다회의 입력을 하므로 입력 시간의 평균을 계산한다. 이때 동일 종류 입력에 대해서만 평균으로 계산한다. 입력하는 키패드의 종류가 두 가지이고, 입력하는 패스워드도 두 가지 이므로 총 네 종류의 측정 시간을 기록하며 소수점 이하는 반올림한 값을 사용한다. 결과는 [그림 5-1]의 그래프와 같다.



[그림 5-1] 평균 시간 측정 그래프

먼저 실험자가 원하는 패스워드를 사용한 경우를 비교한다. 닌텐도 스위치의 보안 키패드를 사용했을 때는 약 12초가 소요되었으며, 제안하는 행렬 형태 보안 키패드를 사용했을 땐 약 22초가 소요되었다. 또한 연구진이 제시한 패스워드를 사용했을 경우는, 닌텐도 스위치의 보안 키패드 상에서 약 26초가 소요되었으며 제안하는 행렬 형태 보안 키패드 상에서 약 43초가 소요되었다.

전체적으로 제안하는 행렬 형태 보안 키패드 상에서의 입력이 최대 60%까지 느린 입력 속도를 보여줬다. 이는 제안하는 보안 키패드가 기존 닌텐도 스위치의 보안 키패드의 편의성보다 떨어진다고 판단할 수 있다. 하지만 제안하는 보안 키패드는 지금까지 제안되었던 보안 키패드들과 완전히 다른 형태를 취하고 있기 때문에 익숙하지 않다는 점을 고려할 수 있다. 기존 보안 키패드들은 쿼티 레이아웃에 기반하고 있기 때문에 다른 형태의 보안 키패드를 사용하더라도 손쉽게 적응할 수 있다. 제안하는 행

렬 형태 보안 키패드는 쿼티 레이아웃을 완전히 무너뜨린 새로운 형태이기 때문에 이와 유사한 사용 경험도 존재하지 않으므로 사용에 어려움이 존재한다. 이는 적응의 문제이므로 사용자가 오래 사용한다면 차차 개선될 수 있을 것으로 예상된다. 또한 제안하는 보안 키패드는 닌텐도 스위치 상에서의 구현이 아닌 안드로이드 어플리케이션을 통한 간접적인 구현 방식을 취했다. 스틱과 버튼을 조작하는 조이콘과는 달리 스마트폰의 터치를 통해 스틱과 버튼 조작을 구현했기 때문에 조작 환경이 다르다는 점도 감안한다면 실제 입력 속도의 차이는 더 줄어들 수 있을 것으로 결론지을 수 있다.

제 4 절 제안 키패드 보안성 평가

보안성을 평가하기 위해서는 실험자가 패스워드를 입력하고 있을 때 훔쳐보기 공격을 시도하여 패스워드를 획득 유무를 기준으로 한다. 3회에 걸쳐 입력을 하므로 공격을 성공한 시점을 기록하며 공격에 실패한 횟수가 많을수록 보안성이 높다고 판단한다. 공격 결과는 [표 5-1]에서 확인할 수 있다.

[표 5-1] 훔쳐보기 공격 결과 표

(단위: 명)

	행렬 형태 보안 키패드	기존 보안 키패드
1회차	0	7
2회차	0	2
3회차	0	3
공격실패	14	2
합계	14	14

우선 기존 닌텐도 스위치의 보안 키패드의 경우, 전체 14명 중에서 12명이 공격을 당했다. 하지만 제안하는 행렬 형태 보안 키패드 상에서는 14명 모두 공격을 방어할 수 있었다.

제안하는 보안 키패드에서 주어지는 정보는 초기 선택 행과 패스워드 입력란에 추가되는 '*' 문자의 수 및 키 레이아웃이 주어진다. 초기 선택 행은 보안 키패드 호출 후 약 2초간만 보이고 이후에는 선택 중인 행은 표시되지 않는다. 그러므로 초기 선택 행은 공격자에게 의미가 없는 정보이다. 또한 '*' 문자의 수를 세는 것으로 사용자의 패스워드 길이를 유추할 수 있다. 하지만 패스워드 길이로는 정확한 패스워드를 알아낼 수는 없다. 마지막으로 키 레이아웃 정보이다. 레이아웃 정보가 제공되므로 어떤 값이 입력된다면 그 값은 반드시 레이아웃 상의 문자 중 하나라는 것을 알 수 있다. 제안하는 보안 키패드는 하나의 레이아웃에 30종류의 문자가 표현되므로, 약 3%의 확률로 입력 값을 정확히 예상할 수 있다. 만약 패스워드가 8자리라면 약 0.00000000007% 확률로 정확한 패스워드를 유추할 수 있다. 이는 훔쳐보기 공격으로는 불가능한 수치라고 판단할 수 있다.

따라서 제안하는 보안 키패드는 기존 닌텐도 스위치에 비해 매우 뛰어난 보안성을 지닌다고 평가할 수 있다.

제 5 절 이중 인증 안전성 검토

이중 인증을 평가하기에 앞서 닌텐도 스위치의 보안 기법 별 취약점과 단점을 [표 5-2]에 정리하였다. [표 5-2]의 항목 중, '취약점 및 단점'은 보안 기법 적용 시 발생하는 취약점 또는 단점에 관한 것이다. '계'는 취약점 또는 단점 항목의 수이며 괄호 안의 숫자는 기존 보안 키패드를 기준으로 한 차이 값이다.

[표 5-2] 보안 요소별 취약점 및 단점 일람

보안 요소	취약점 및 단점	계
닌텐도 스위치 보안 키패드	패스워드 일부 또는 전체 획득 가능 패스워드 확보 시 인증 가능 키패드가 좌우로 넓어서 느린 커서 이동 키 레이아웃 변경의 번거로움	4개 (0)
행렬 형태 보안 키패드	패스워드 확보 시 인증 가능	1개 (-3)
NFC 인증	기기 탈취 시 비인가자 접근 가능 NFC 스캔이 없는 PC 상에서 인증 불가능	2개 (-2)
닌텐도 스위치 보안 키패드 + NFC 인증	패스워드 일부 또는 전체 획득 가능 키패드가 좌우로 넓어서 느린 커서 이동 키 레이아웃 변경의 번거로움	3개 (-1)
행렬 형태 보안 키패드 + NFC 인증	없음	0개 (-4)

닌텐도 스위치의 보안 키패드를 그대로 적용했을 경우에는 크게 네 가지의 보안 취약점과 단점이 발생한다. 우선 가장 주된 취약점으로 제시된 커서 노출로 인한 패스워드 획득 가능성이 존재하며, 단일 인증이므로 패스워드가 확보된다면 바로 인증을 통과하게 된다. 또한 키패드가 좌우로 넓어서 커서 이동이 불편하며 한 글자가 아닌 다수의 대문자를 입력할 경우 키 레이아웃 변경이 번거로운 단점이 있다.

행렬 형태 보안 키패드만을 적용했을 경우에는 닌텐도 스위치의 보안 키패드의 단점을 극복할 수 있으나, 다른 경로를 통해 패스워드가 확보되었다면 인증을 통과할 수 있다는 단점이 존재한다.

반면 NFC 인증을 단독으로 사용한다면 패스워드 유출은 발생하지 않으며 키패드 조작과 관련된 단점이 제거된다. 하지만 NFC 기기가 탈취된다면 인증을 진행할 수 있으며 NFC 스캔이 불가능한 환경에서 닌텐도 계정을 사용하고자 할 경우에는 인증 자체를 진행할 수 없다.

이와 같이 단일 인증은 여러 가지 취약점과 단점이 발생하기 때문에 효과적인 보안 시스템을 구축하기가 어렵다. 하지만 이중 인증을 사용할 경우 이를 상쇄할 수 있다.

닌텐도 스위치의 보안 키패드와 NFC 인증을 조합할 경우, 패스워드 유출 취약점과 키패드 조작과 관련된 단점이 남으나, 패스워드를 확보하더라도 NFC 인증이 필요하기 때문에 취약점이 하나 제거된다.

제안하는 보안 키패드와 NFC 인증을 조합한다면, 패스워드 확보 상황에서 인증이 진행되는 것을 NFC 인증으로 보호할 수 있기 때문에 모든 단점이 상쇄된다. 결론적으로 제안하는 보안 키패드도 단일 인증 시스템에서는 다른 경로를 통해 획득한 패스워드 사용을 방지할 수 없으나, NFC 복합 인증을 사용하게 된다면 해당 취약점을 제거할 수 있기 때문에 더욱 높은 보안성을 제공할 수 있다.

제 6 절 정량 평가

지금까지 제안하는 보안 키패드와 NFC 인증을 사용하여 이중 인증 시스템에 대해서 확인하였다. 실험 결과와 취약점 분석 내역을 확인한 결과, 제안하는 보안 키패드와 NFC 인증을 사용한 이중 인증 시스템은 상당히 안정적인 시스템으로 판단할 수 있다. 이를 조금 더 구체적으로 확인하기 위해 정량적인 수치로 평가하고자 한다.

1) 행렬 형태 보안 키패드 정량 평가

키패드는 패스워드를 사용하므로 안전성은 패스워드의 보안성에 의존한다. 패스워드는 개인정보의 기술적, 관리적 보호조치 기준 제 4조 8항에 따르면 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상으로 작성할 것을 권고된다. 사용 가능한 문자를 소문자 26개, 숫자 10개, 특수문자 10개라 가정하고 3종류 조합의 8자리 패스워드를 생성할 경우, 약 5.355×10^{11}개의 가짓수가 있다. 이때 조합 수가 많을수록 보안수준이 높다고 할 수 있다.

하지만 가짓수가 많은 패스워드라도 공격자가 패스워드의 일부를 획득하는 순간 조합의 수는 큰 폭으로 떨어진다. 8자리 패스워드의 예시에서 절반인 4자리의 패스워드를 획득한다면 패스워드 가짓수는 최선의 경우 4,477,456개, 최악의 경우 119,600개로 감소한다. 어느 상황이든 약 99%의 손실이 발생한다. 다양한 상황에 따라 조합의 수 변화는 [표 5-3]에서 확인할 수 있다. 표 내부의 값 중 상단의 값은 최선의 상황, 하단의 값은 최악의 상황에서 조합의 수다.

[표 5-3] 조건에 따른 패스워드 조합 수

(단위: 개)

	8자	10자	12자
노출 없음	5.355×10^{11}	1.133×10^{15}	2.398×10^{18}
2자 노출	5.355×10^{9} 2.530×10^{8}	1.133×10^{13} 5.355×10^{11}	2.398×10^{16} 1.133×10^{15}
4자 노출	4,477,456 119,600	9.474×10^{9} 2.530×10^{8}	2.005×10^{13} 5.355×10^{11}
6자 노출	2,116 260	4,477,456 119,600	9.474×10^{9} 2.530×10^{8}
8자 노출	1 1	2,116 100	4,477,456 119,600

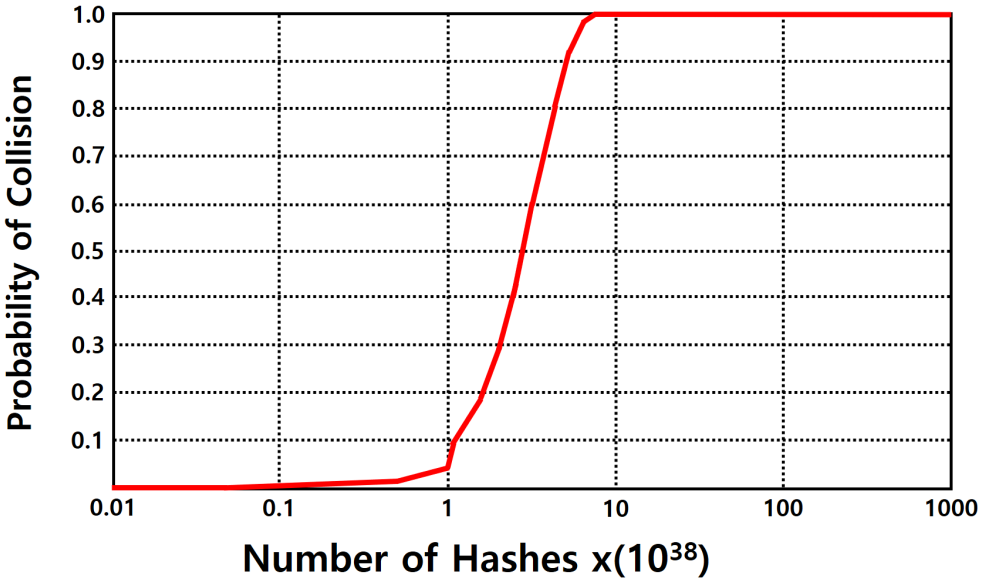
기존 닌텐도 스위치의 보안 키패드는 패스워드 노출이 일어나기 매우 쉬운 환경이며, 이는 3장 1절에서 가능성을 제시하였고 5장 4절에서 실제로 확인하였다. [표 5-3]에 따르면 패스워드의 일부만 노출되어도 보안 강도가 급격히 떨어진다. 따라서 기존 닌텐도 스위치의 보안 키패드는 사용자 패스워드의 보안강도를 대폭 떨어뜨릴 가능성이 매우 크다.

제안하는 보안 키패드는 육안으로 어떤 값이 입력되는지 전혀 확인할

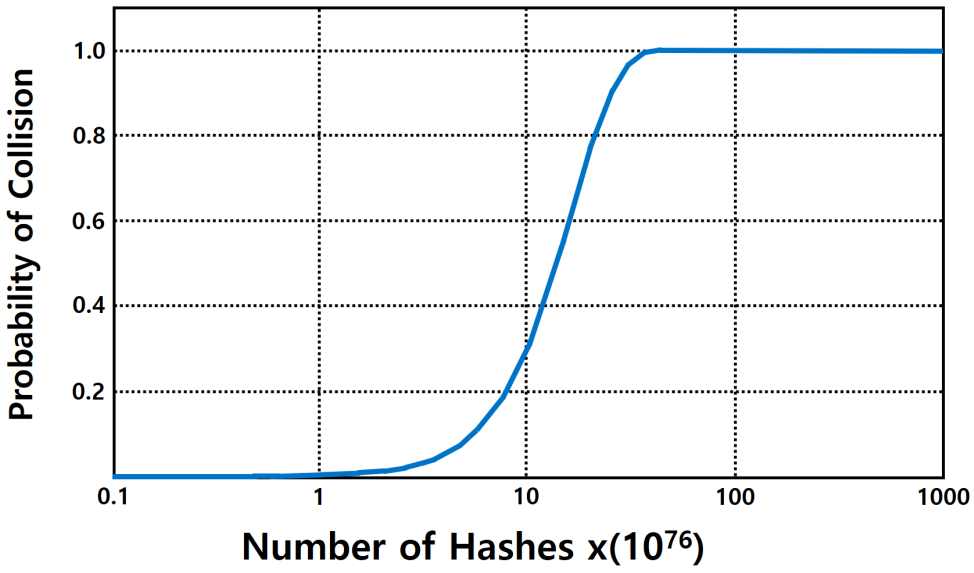
수 없다. 따라서 최소 권고 기준으로 제시한 패스워드 가짓수인 5.355×10^{11}을 그대로 유지할 수 있기에 강력한 보안수준을 제공한다. 이는 제안하는 보안 키패드의 보안성능이 뛰어남을 수치적으로 증명한다.

2) NFC 인증 정량 평가

NFC의 인증 과정에는 해시함수가 활용되므로, NFC인증의 보안성은 인증 과정의 해시함수에 의존한다. 해시함수는 여러 종류가 있지만 널리 사용 중인 SHA-2와 신규 표준으로 지정된 SHA-3를 기준으로 한다. 256비트 출력 규격을 가지는 SHA-2, SHA-3 해시함수가 50% 확률로 충돌이 발생하기 위해서는 5×10^{38}개의 해시 값이 필요하다. 또한 512비트 출력 규격의 경우, 각각의 해시함수가 50% 확률로 충돌이 일어나기 위해서 256비트 출력 규격에 비해 훨씬 더 많은 수가 필요하다. 이를 가시화하여 그래프 형태로 표현하면 [그림 5-2]와 [그림 5-3]과 같다. 여기서 [그림 5-2]는 256비트 출력 규격 기준이고 [그림 5-3]은 512비트 출력 규격 기준이다. 결론적으로 SHA-2, SHA-3를 사용하는 NFC 인증의 경우, 해시 충돌 가능성이 매우 낮기 때문에 상당히 안전하다고 평가할 수 있다.



[그림 5-2] SHA-2, SHA-3 256의 해시 충돌 가능성 그래프



[그림 5-3] SHA-2, SHA-3 512의 해시 충돌 가능성 그래프

제 6 장 결론 및 향후 연구 방안

본 논문에서는 닌텐도 스위치의 보안 키패드가 가지는 보안 취약점에 대해서 분석하였고, 이를 개선할 수 있는 행렬 형태 보안 키패드를 제안하였다. 또한 이에 그치지 않고 단일 인증이 아닌 NFC 이중 인증 도입을 제안하여 더 높은 보안성을 확보할 수 있는 방안을 제시하였다.

제안하는 보안 키패드는 기존 닌텐도 스위치의 보안 키패드에 비해 편의성은 떨어진다고 할 수 있지만, 반면에 뛰어난 보안성을 보여주었다. 일반적으로 보안성은 편의성과 반비례하는 경향을 보인다. 보안성을 높이기 위해서는 자주 사용되지 않는 환경 적용, 복잡한 인증 절차 등이 사용되기에 사용자 입장에서는 체감 편의성이 하락하게 된다. 하지만 편의성이 너무 떨어지게 된다면 사용자의 외면을 받으므로, 편의성을 유지하는 선에서 적합한 보안성을 제공할 수 있도록 균형을 맞추어야 뛰어난 보안 환경을 제공할 수 있음을 확인하였다.

마지막으로 제안하는 보안 키패드는 다수와 화면을 공유하는 환경에서 매우 뛰어난 보안성을 가진다. 그러므로 본 제안하는 보안 키패드가 닌텐도 스위치 환경뿐만 아니라 다른 분야, 특히 공공분야에서 사용될 수 있도록 향후 개선 및 연구를 진행한다면 더 많은 분야에서 강력한 보안성을 제공할 수 있을 것으로 예상된다.

참 고 문 헌

1. 국외문헌

F. Fortat, M. Laurent, M. Simatic, (2015). *Games based on active NFC objects: model and security requirements*. Proceedings of the 2015 International Workshop on Network and Systems Support for Games, 12, 1-3.

H. J. Jeong, N. H. Kim, (2013). *How Do they Manage Personal Information in Hospital? -A Survey Study for IT Governance in Hospitals-*. Korean review of crisis and emergency management, 9(8), 47-65.

H. J. Mun, (2017). *Virtual Keypads based on Tetris with Resistance for Attack using Location Information.* Journal of the Korea Convergence Society, 8(6), 37-44.

H. J. Seo, H. W. Kim, (2016). *Design of Security Keypad Against Key Stroke Inference Attack*. Journal of The Korea Institute of Information Security & Cryptology, 26(1), 41-47.

J. N. Soliman, T. A. Mageed, H. M. El-Hennawy, (2017). *Digital Signature and Authentication Mechanisms Using New Customized Hash Function For Cognitive Radio Networks*. IEEE International Conference on Computer Engineering and Systems, 12, 175-181.

K. H. An, H. D. Kwon, K. H. Kim, H. J. Seo, (2019). *Implement pattern lock security enhancement using thread to measure input time*. Journal of the Korea Institute of Information and Communication Engineering, 23(4), 470-476.

M. Flamberg, (2017). *Games 360 U.S. Report*. Nielsen Games, 1-28.

M. M. Singh, K. A. A. K. Adzman, R. Hassan, (2018). *Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures*. International Journal of Engineering & Technology, 7, 298-305.

S. J. Kim, (2018). *Computer User Authentication and Power Management System using Internet of Things based on NFC*. Proceedings of

Symposium of the Korean Institute of communications and Information Science, 1120-1121.

S. Nashwan, (2017). *Secure Authentication Protocol for NFC Mobile Payment Systems*. International Journal of Computer Science and Network Security, 17(8), 256-263.

S. Vaidya, S. Kadam, V. Bhosale, (2017). *Preventing shoulder surfing attack using touch screen based PIN authentication method in invisible form*. 2017 International Conference on Trends in Electronics and Informatics (ICEI), 444-449.

Y. H. Lee, (2013). *An Analysis on the Vulnerability of Secure Keypads for Mobile Devices*. Journal of Internet Computing and Services, 14(3), 15-21.

ABSTRACT

A suggest for new shape of security keypad with improved security

Kwon, Hyeok-Dong

Major in IT Convergence Engineering

Dept. of IT Convergence Engineering

The Graduate School

Hansung University

The Nintendo Switch(NSW) is a home gaming console which belongs to the 8th generation of gaming consoles. The Nintendo Switch can be used as hybrids. So it can be connects to TV or it can also be used as light carry-on portable form. Like other gaming consoles of the same generation, The Nintendo Switch have built-in online connectivity and users can receive services through their accounts and passwords. The users will use the built-in security keypad of the Nintendo Switch to enter their own passwords. A security keypad for the Nintendo Switch is convenient and intuitive, because it using the controller of the Nintendo Switch. However it has vulnerability which is that all the input is exposed just by looking at the screen. Thus we propose a new keypad what improved the problem, so that even if an attacker watches the screen, the

passwords are not exposed. In this paper, we point out the problems of the existing keypad for Nintendo Switch, and propose the result of designing and implementing a new keypad that improves the issue. In addition, to compare the performance of the existing keypad with the proposed keypad, a number of experimenters are mobilized to summarize the results of using the proposed keypad. And we check out the proposed keypad has stronger security than the existing keypad through the experimental results. Also, the Nintendo Switch which provides only a single authentication. So we proposed that two-factor authentication scheme which using the NFC scan, it can be serve powerful security.

KEYWORD: Near Field Communication, Security Keypad, Shoulder Surfing Attack, The Nintendo Switch