향상된 보안성을 지닌 새로운 유형의 보안 키패드 제안

한성대학교 IT융합공학부 권혁동

19.12.09.

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.

Contents

닌텐도 스위치

보안 키패드

제안 키패드

성능평가

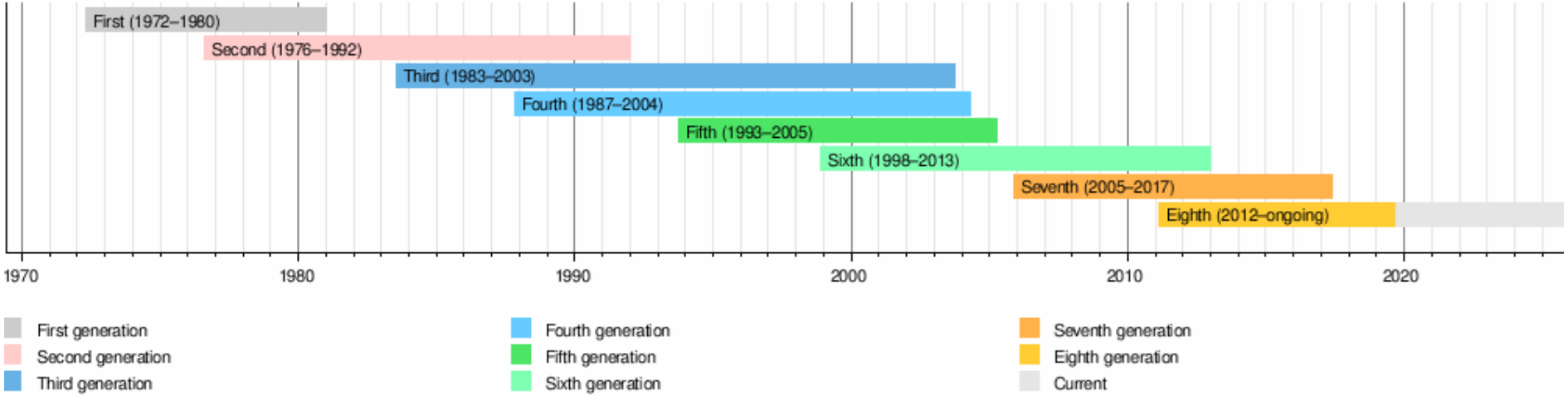
결론

CryptoCraft LAB

닌텐도 스위치: 개요

- 게임기란?
  - 게임, 특히 **비디오 게임을 즐기기 위한** 전용 기기
- 최근에는 컴퓨터, 모바일 기기의 발전으로 지분을 나눠 가졌지만 **전문성은 최상위**
- 사용 위치에 따른 분류
  - 가정에서만 사용 가능한 가정용 게임기
  - 이동하면서 사용 가능한 휴대용 게임기
- 흔히 **콘솔**이라는 명칭을 사용

닌텐도 스위치: 개요



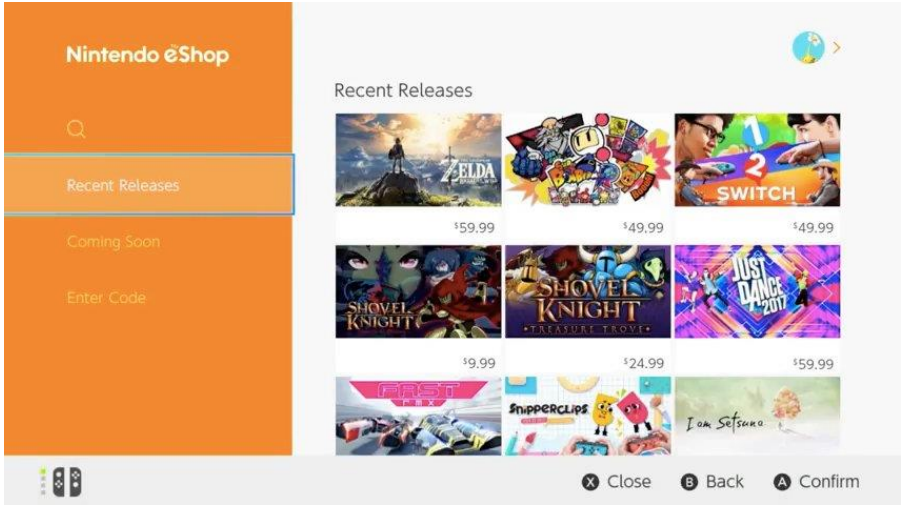
- 시대별로 발전하며 8세대로 분류
- 다수의 세대가 공존하고 있는 시점도 존재
- 주제인 **닌텐도 스위치는 8세대 게임기**로 분류

닌텐도 스위치: 개요

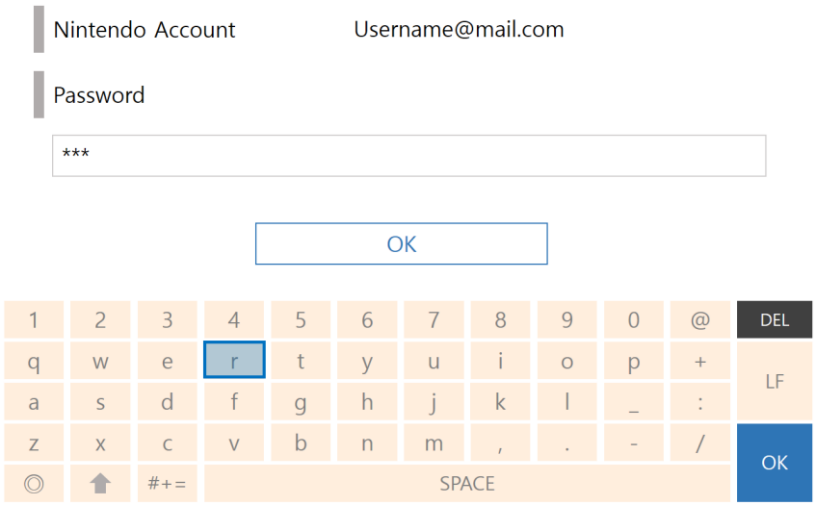
- 2017년 3월 3일 출시
  - 한국 출시일은 동년 12월 1일
  - 19년 8월 1일(한국) 신규 모델 출시
  - 19년 9월 20일(전세계) 휴대 전용 기기 출시
- **최초의 가정용, 휴대용 하이브리드 콘솔**
  - **본 제안은 가정용 상황을 가정**
- 콘솔 게임을 집 밖에서도 즐길 수 있는 장점
- 전용 컨트롤러 **조이콘**을 통해 조작
  - **진동**, **NFC**, IR센서 등이 내장

닌텐도 스위치: 문제 확인

- 닌텐도 스위치는 **e-shop을 내장**하고 있음
- 계정 로그인을 통해 게임 구매가 가능

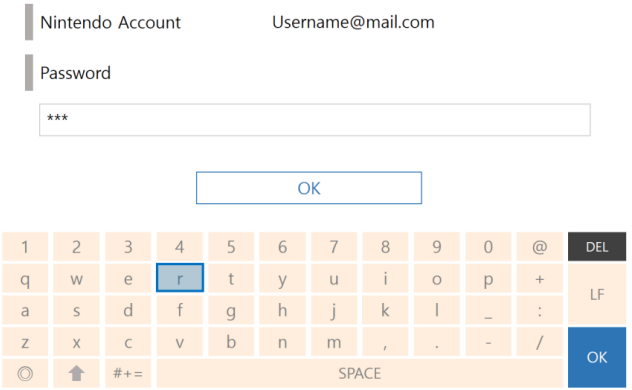


- 조이콘을 사용하여 패스워드 입력
- **보안 키패드가 제공**됨



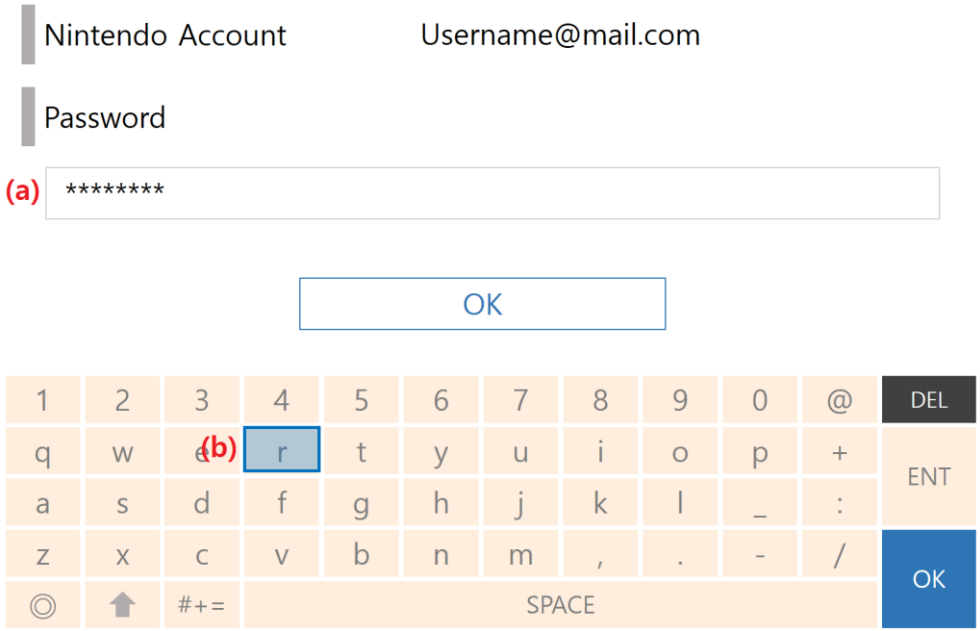
닌텐도 스위치: 문제 확인

- 가정용(독 모드)에서는 **조이콘을 통한 패스워드 입력**만 가능
- 조이콘 사용시에는 커서가 노출되는 문제
- 커서 노출로 인해 패스워드 노출 가능성 존재



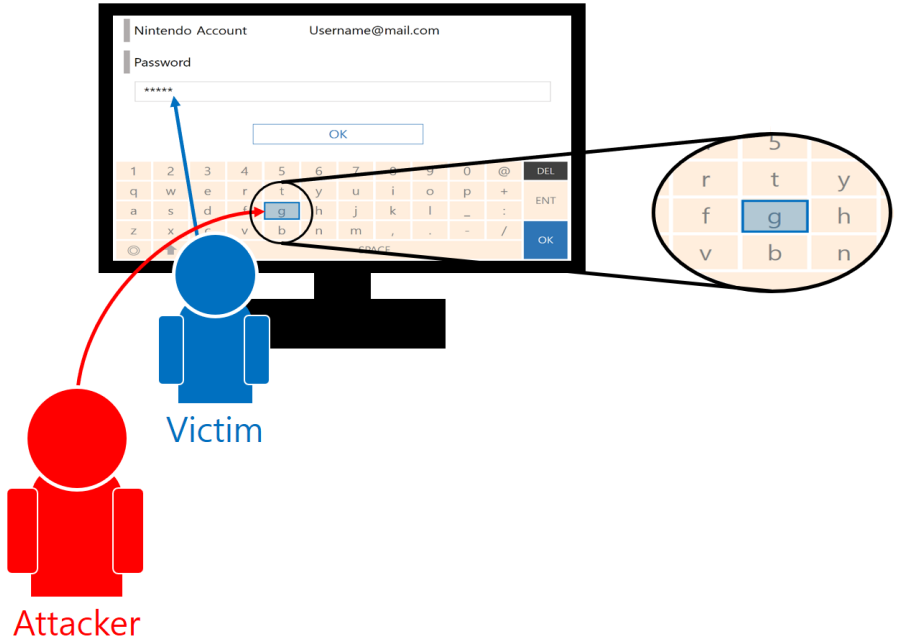
닌텐도 스위치: 문제 확인

- (a): 패스워드 입력란
  - 입력 값은 '*'로 **식별 불가**
- (b): 보안 키패드
  - 조이콘 사용시 커서 노출
- 입력 값을 <u>직접 확인은 불가능</u>
- **커서를 추적**하는 것으로 **확인 가능**



닌텐도 스위치: 문제 확인

- 패스워드 입력 창은 모든 입력 값이 가려짐
  - 입력 창에서 값을 알 수 없음
- 키패드 상에는 **커서가 노출**
  - 입력하는 사용자가 커서 위치를 알아야 함
  - **화면을 보는 것만으로 패스워드 노출**
- 훔쳐보기 공격(Shoulder Surfing Attack)
- 스위치는 다수가 즐기는 게임이 많음
  - **취약점이 지닌 조건 형성이 쉬움**

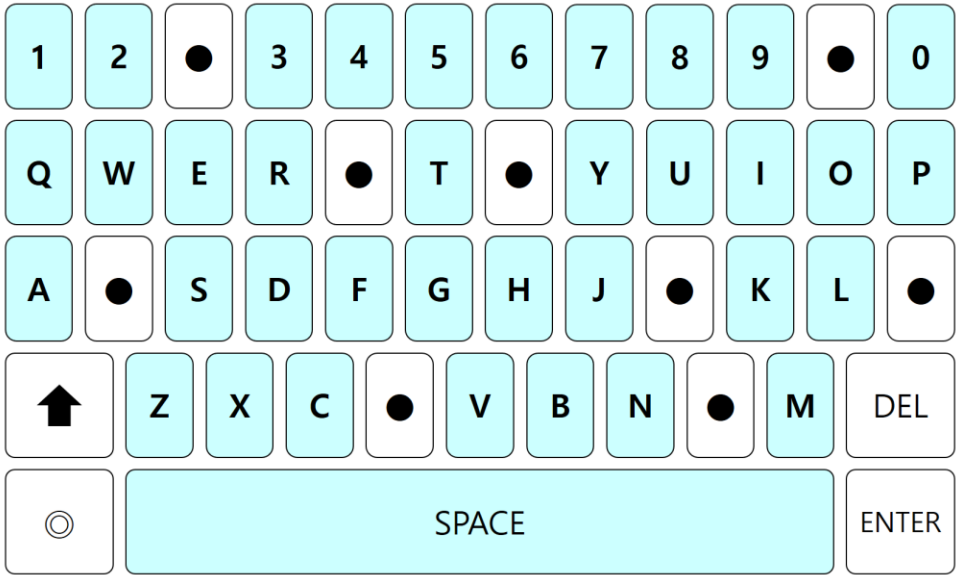


닌텐도 스위치: 제안 목록

- **키패드 제안 내용**
  - **훔쳐보기 공격에 내성**을 지니는 보안 키패드 제안
  - 커서 노출 취약점 제거
- **보안 강화 내용**
  - NFC를 활용한 **이중 인증** 제안

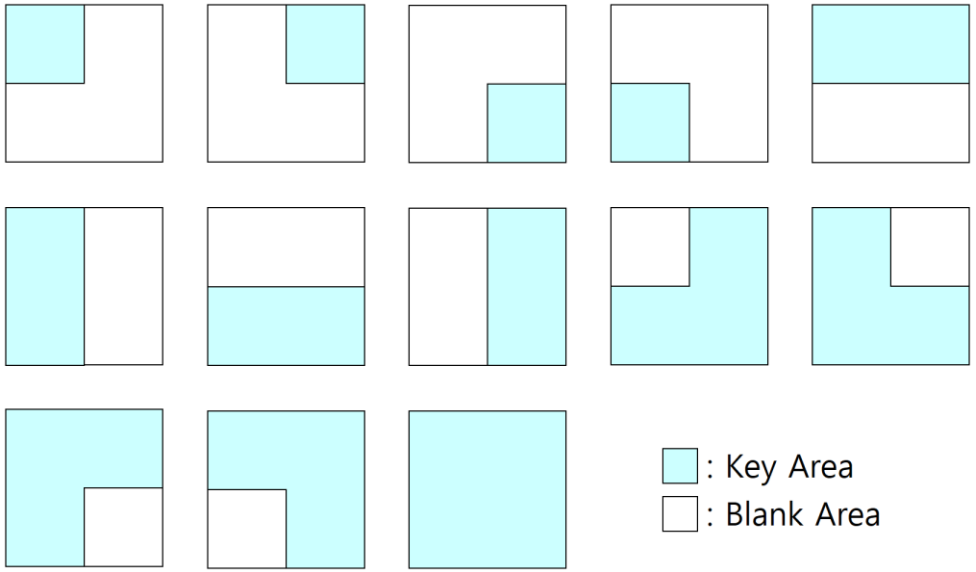
보안 키패드

- 공백 삽입 보안 키패드
- 키 레이아웃은 동일
- 키 중간 중간에 **공백이 삽입**
  - 공백의 **위치는 무작위**
- **동일 좌표**임에도 **입력 값이 다를 수 있음**
  - 첫 줄 네번째 칸의 값이 ‘4’일지 아닐지 모름
- **커서 노출 문제를 해결할 수 없음**



보안 키패드

- 테트리스 블록 보안 키패드
- 키를 사각형이 아닌 다양한 형태로 제공
- 각각의 **형태를 짜맞추는 것으로 키패드 완성**
- 입력 좌표는 같아도 값은 다를 수 있음
- **커서 노출 문제를 해결할 수 없음**



보안 키패드

- 유동적 행 단위 배치 보안 키패드
- 쿼티 자판의 **행은 유지한 채 시작점을 바꿈**
- 동시에 다수의 무작위 공백을 포함
- 같은 좌표 입력이지만 서로 다른 값일 확률이 매우 높음
- **커서 노출 문제를 해결할 수 없음**

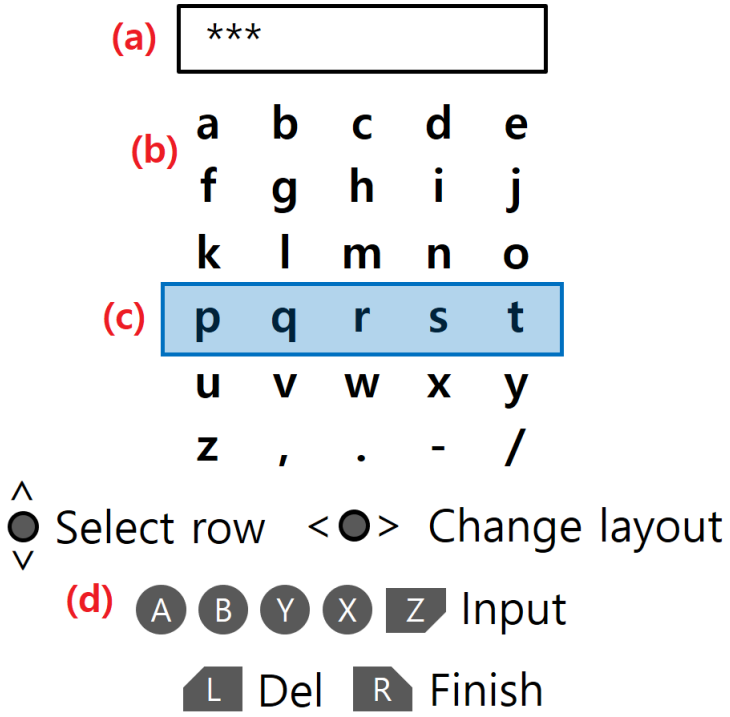
보안 키패드

- 닌텐도 스위치 보안 키패드의 특징과 문제점
  - 조이콘 입력에 최적화 됨
  - 사용자의 입력 편의성을 위해 키패드 상에 현재 **커서가 노출**
  - 상기의 특성으로 입력 창의 내용은 가려지나 화면을 보는 것으로 패스워드 노출

- 기존 보안 키패드의 특징
  - 입력 **좌표가 같더라도** 입력 **값이 다르다**는 공통점
  - 주로 금융앱 등의 **모바일 디바이스**에 활용하기 위해 개발
  - 공격자가 화면을 볼 수 없지만 입력 좌표를 획득할 수 있을 때 매우 강력
  - **화면을 직접 보는 것에 대한 방어 미비**

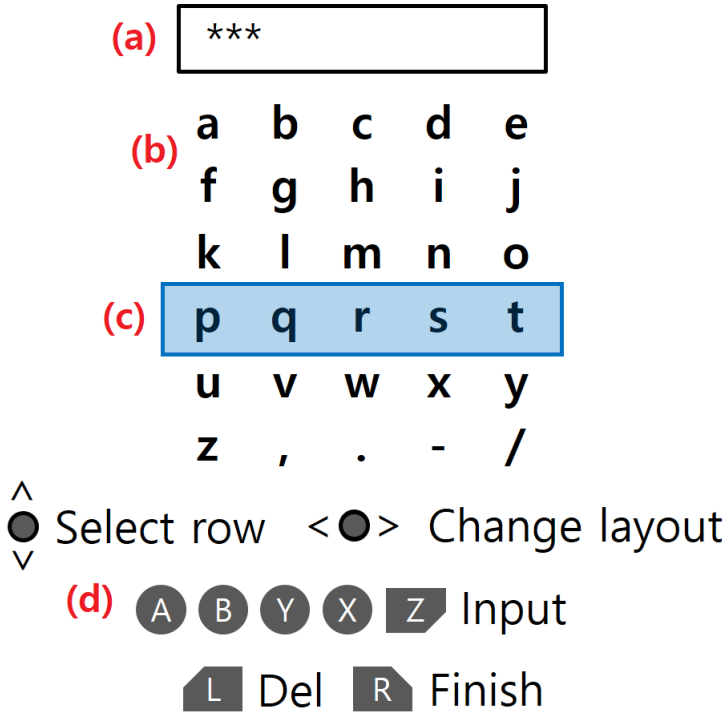
제안 키패드

- **행렬 형태 보안 키패드**를 제안
- (a): 패스워드 입력란
- (b): 키패드
- (c): 선택 중인 행 표식
- (d): 조작 가이드



제안 키패드

- 사용자는 조이콘을 통해 패스워드 입력을 진행
  - 상하: 선택 행 변경
  - 좌우: 입력 레이아웃 변경
  - A,B,Y,X,Z: 열 선택
- 현재 **선택 중인 행과 선택한 열의 값**을 입력
  - 1행 Y(3)열: c 입력
  - 3행 Z(5)열: o 입력
- **양 끝 행**에 도달시 사용자에게 조이콘 **진동 피드백**

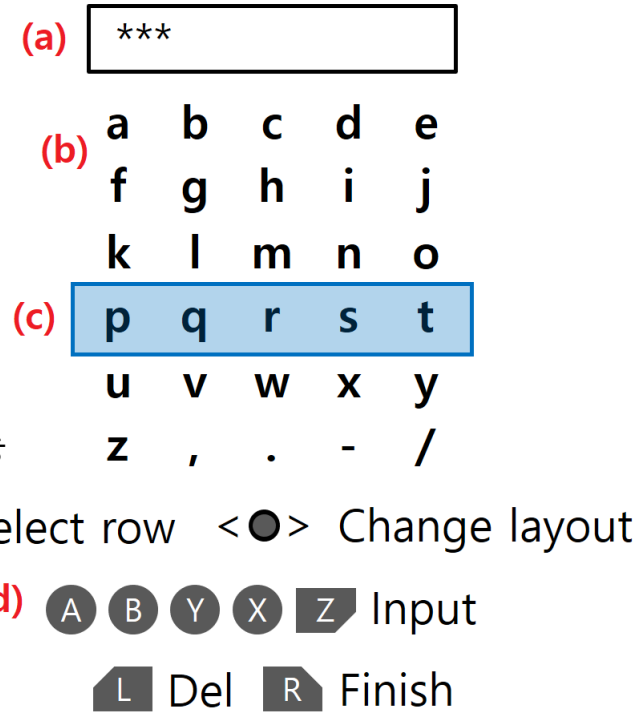


제안 키패드

- 동작 과정

1. 사용자에게 **초기 행의 위치**를 알려줌
   - 음영을 통해 알려주며, 짧은 시간이 지난 후 소멸
   - 초기 위치는 무작위로 지정
2. 스틱 조절로 **입력 값이 위치한 행**으로 이동
   - 원하는 값이 없다면 스틱 조절로 레이아웃 변경 가능
3. 입력 값이 위치한 열을 **버튼으로 입력**

- 현 조건에서 'thesis' 입력 예시를 시행



제안 키패드

*

a	b	c	d	e
f	g	h	i	j
k	l	m	n	o
p	q	r	s	t
u	v	w	x	y
z	,	.	-	/

제안 키패드

**

a	b	c	d	e
f	g	h	i	j
k	l	m	n	o
p	q	r	s	t
u	v	w	x	y
z	,	.	-	/

제안 키패드

***

a	b	c	d	e
f	g	h	i	j
k	l	m	n	o
p	q	r	s	t
u	v	w	x	y
z	,	.	-	/

제안 키패드

****

a	b	c	d	e
f	g	h	i	j
k	l	m	n	o
p	q	r	s	t
u	v	w	x	y
z	,	.	-	/

제안 키패드

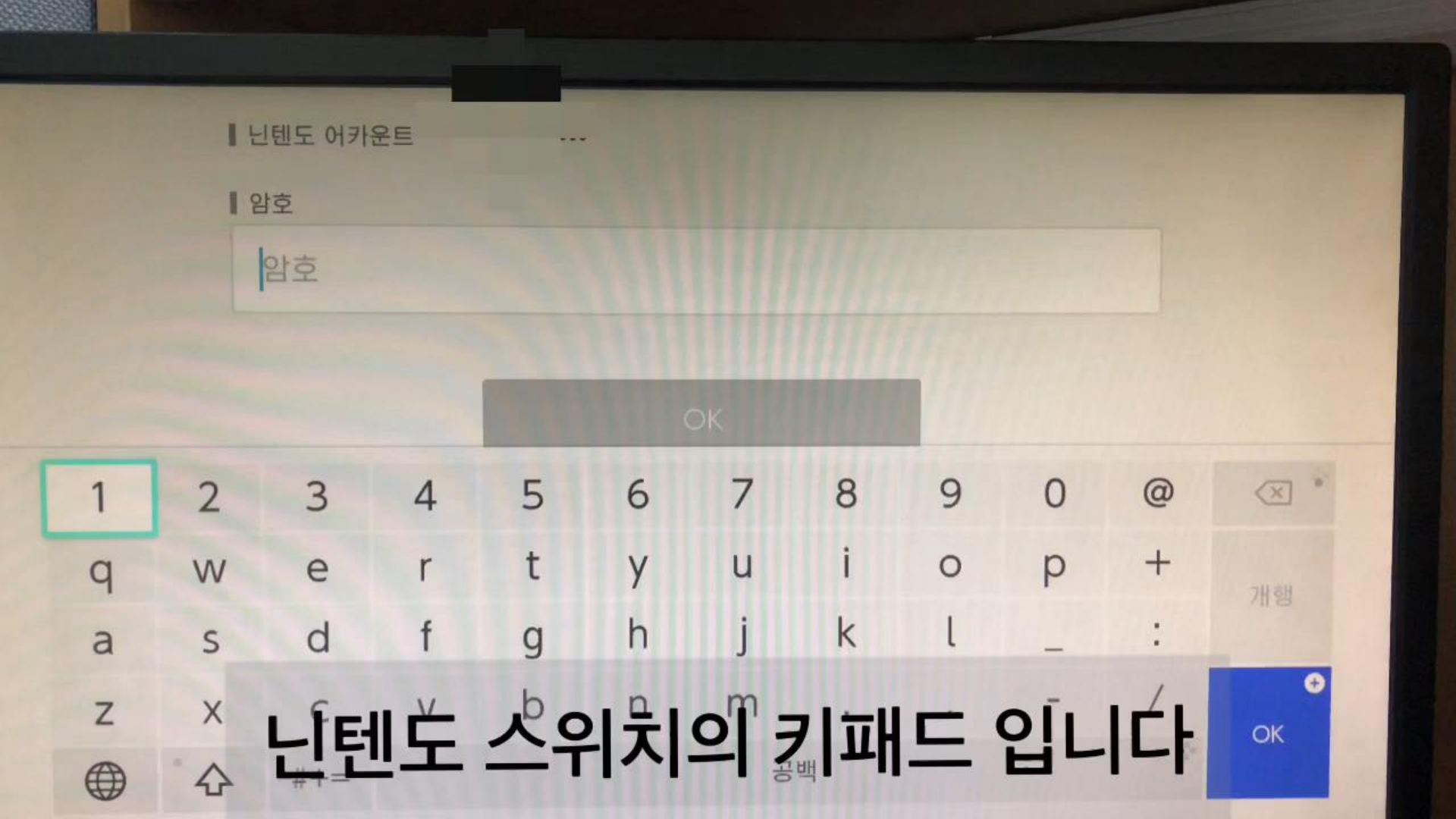
*****

a	b	c	d	e
f	g	h	i	j
k	l	m	n	o
p	q	r	s	t
u	v	w	x	y
z	,	.	-	/

제안 키패드

******

a	b	c	d	e
f	g	h	i	j
k	l	m	n	o
p	q	r	s	t
u	v	w	x	y
z	,	.	-	/


닌텐도 어카운트
암호
암호
OK
1 2 3 4 5 6 7 8 9 0 @
q w e r t y u i o p +
a s d f g h j k l _ :
z x c v b n m
개행
OK
닌텐도 스위치의 키패드 입니다

이중 인증

- 닌텐도 스위치는 패스워드를 통한 **단일 인증** 사용
  - 보안 키패드의 자체적인 취약점으로 **쉽게 무력화 가능**
- 조이콘의 **NFC 기능을 활용**한 추가적인 인증 제안
  - 이중 인증을 통한 **더 강한 보안성** 확보 가능

이중 인증

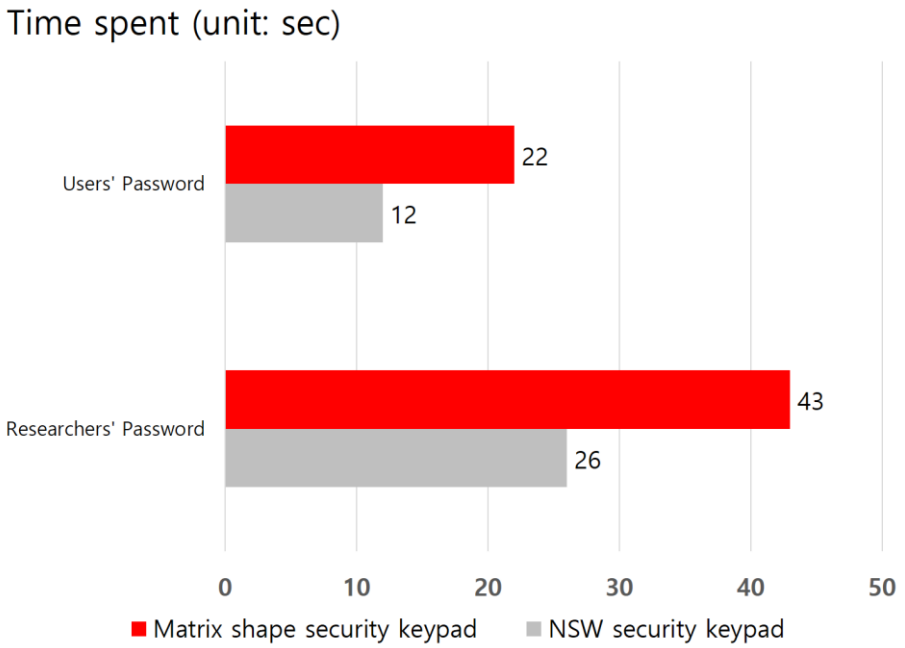
1. 인증 상황 발생시 사용자에게 인증이 필요함을 고지
2. 스마트폰의 NFC 기능 활성화 후 우측 조이콘에 스캔
3. 인가된 NFC 신호일 경우, 인증 성공

성능평가

- **기존 닌텐도 스위치 보안 키패드와 제안 키패드의 성능 비교**
- 비디오 게임을 즐기는 14인, 22 ~ 29세 연령 분포
- 편의성
  - 사용자가 패스워드를 **입력하는 시간**을 측정
  - **입력시간이 빠를 수록** 편의성이 높은 것으로 판단
  - 사용자 지정 패스워드, 연구진 지정 패스워드 두 종류를 입력
- 보안성
  - 사용자가 패스워드 입력 중에 연구진이 공격
  - 공격은 **화면을 보는 것**만으로 이루어짐
  - **패스워드 노출 수가 적을 수록** 보안성이 높은 것으로 판단

성능평가: 편의성

- (지정 패스워드) 기존: 평균 26초
- (지정 패스워드) **제안: 평균 43초**
- (사용자 패스워드) 기존: 평균 12초
- (사용자 패스워드) **제안: 평균 22초**
- 기존 키패드가 대체로 55~60% 빠름
  - 제안 키패드는 안드로이드 어플로 개발
  - 환경의 차이를 감안할 필요 존재
- **사용자 숙련도에 따라 큰 차이 발생 가능**



성능평가: 보안성

- 기존: 공격 성공 12회
- **제안: 공격 성공 0회**
- 기존 키패드와는 달리 **확실하게 방어**
- **보안성 부분에서 압도적인 성능 차이 확인**

	기존 키패드	제안 키패드
1차	7(50.0%)	0(0.0%)
2차	2(14.3%)	0(0.0%)
3차	3(21.4%)	0(0.0%)
실패	2(14.3%)	14(100.0%)

성능평가: 이중 인증

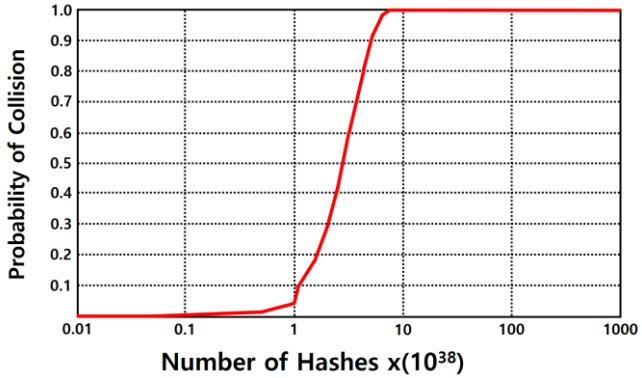
보안 요소	취약점 및 단점	계
닌텐도 스위치 보안 키패드	패스워드 일부 또는 전체 획득 가능 패스워드 기 확보 시 인증 가능 키패드가 좌우로 넓어서 느린 커서 이동 키 레이아웃 변경의 번거로움	4개 (0)
행렬 형태 보안 키패드	패스워드 기 확보 시 인증 가능	1개 (-3)
NFC 인증	기기 탈취 시 비인가자 접근 가능 NFC 스캔이 없는 PC 상에서 인증 불가능	2개 (-2)
닌텐도 스위치 보안 키패드 + NFC 인증	패스워드 일부 또는 전체 획득 가능 키패드가 좌우로 넓어서 느린 커서 이동 키 레이아웃 변경의 번거로움	3개 (-1)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

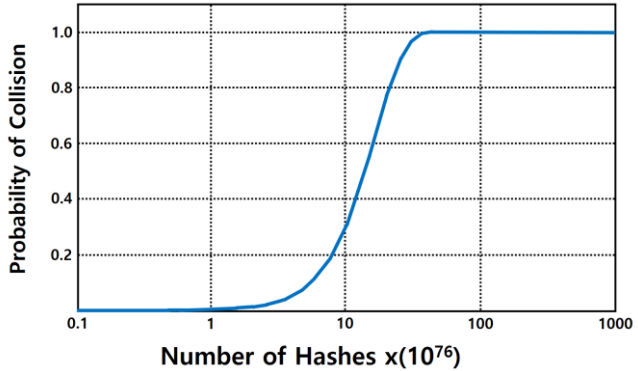
성능평가: 정량적

- 개인정보의 기술적, 관리적 보호조치 제 4조 8항
  - 영문, 숫자, 특수문자 중 **2종류** 이상 최소 **10자**
  - 영문, 숫자, 특수문자 중 **3종류** 이상 최소 **8자**
- 닌텐도 스위치의 보안 키패드는 패스워드의 일부 획득 가능성 존재
- 패스워드 **일부 획득 시 안전성이 급락**
  - 3종류 8자리 패스워드 조합의 수: $5.355 * 10^{11}$
  - 2글자 패스워드 노출 시 조합의 수: $5.355 * 10^{9}$ or $2.530 * 10^{8}$
- **따라서 패스워드의 노출이 발생하지 않는 제안 키패드의 정량적 평가는 우수함**

성능평가: 정량적

- NFC 인증 과정에는 해시 함수가 사용
  - NFC의 안전성은 해시 함수에 의존
- 사용중인 해시 함수: SHA-2, SHA-3
  - 출력 규격 256, 512를 기준
  - 256규격 50% 충돌 발생 해시 수: **$5 * 10^{38}$**
  - 512규격 50% 충돌 발생 해시 수: **$3 * 10^{76}$**
- 해시 충돌 발생 가능성은 매우 낮음
- **따라서 해시 충돌에서 안전하므로 NFC의 안전성 확보**





결론

- 기존 닌텐도 스위치의 보안 키패드는 **커서가 노출되는 문제** 존재
  - 사용자 편의성을 위해 커서를 제거할 수 없음
  - **여러 형태의 보안 키패드 역시 스위치 상에서는 커서가 노출되는 문제**가 발생
- 커서 노출을 최소화한 채로 사용
  - **시작 위치만 잠깐 표시**한 후 이후 커서 위치를 표시하지 않음
  - 사용자가 커서 위치를 잊을 수 있으므로 **양 끝 도달시에는 진동 피드백**
  - 입력 값 선택은 각 열에 배정된 버튼을 사용하므로 **커서가 필요 없음**
- 제안한 키패드는 편의성은 조금 떨어지나 **강력한 보안성을 제공하는 것으로 평가**
- **이중 인증 도입 시 훨씬 안전한 계정 보호가 가능**

Q & A