스마트폰 동적 가상키보드의 취약점 분석

방민제*, 최숙희**, 조태남***
*우석대학교 정보보안학과
**우석대학교 심리학과
***우석대학교 IT전자융합공학과
e-mail: bmj8777@naver.com*, shchoi@ws.ac.kr**, tncho@ws.ac.kr***

Analysis on Vulnerabilities of Dynamic Virtual Keyboard for Smartphone

Min-Je Bang*, SookHee Choi**, Taenam Cho***
*Dept. of Information Security, Woosuk University
**Dept. of Psychology, Woosuk University
***Dept. of IT&Electronics Engineering, Woosuk University

요 약

스마트폰의 높은 보급률과 다양한 앱의 개발로, 최근에는 PC의 많은 작업을 스마트폰의 앱을 통하여 손쉽게 수행할 수 있게 되었다. 그러나 스마트폰은 PC에 비하여 화면의 크기 등 여러 가지 물리적 제약점을 가지기 때문에 PC와 다른 취약점을 가진다. 본 논문에서는 패스워드 입력에 사용되는 스마트폰의 동적 가상키보드의 취약점에 대하여 분석하였다.

1. 서론

대부분의 웹사이트나 스마트폰 앱은 회원가입 후 아이디와 신용정보를 이용하여 로그인해야만 사용할 수 있다. 특히 금융과 관련된 경우에는 2개 이상의 인증 단계를 거치기도 하지만 패스워드는 사용자를 인증하는 가장 기본적이고 널리 사용되는 인증 방법이다. 이러한 이유로 패스워드를 알아내기 위한 키보드 로깅을 방지하도록 키보드 대신 마우스를 이용하는 가상키보드를 이용한다. 그러나 가상키보드를 이용하더라도 마우스의 입력 위치의 노출로 패스워드가 분석될 수 있으므로 가상키보드의 키의 위치가 변하는 동적 가상키보드를 많이 이용한다.

PC의 많은 작업을 대신할 수 있는 스마트폰은 PC에 비하여 휴대성이라는 편리함을 제공하는 대신 성능이나 작은 화면과 같은 하드웨어적인 제한점을 가진다. 동적 가상키보드의 경우에도 스마트폰은 물리적 제약으로 인하여 PC보다 많은 취약점을 가진다.

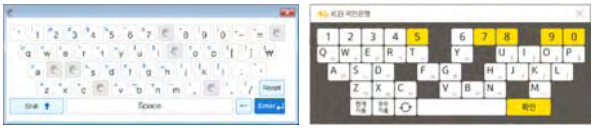
본 연구에서는 스마트폰의 앱에서 사용하는 동적 가상키보드에 대하여 물리적 제약으로 인한 취약점을 분석하여 향후 대응책 마련의 기초를 제공하였다.

2. 동적 가상 키보드 현황

2.1 PC 환경

일반적으로 공인인증서를 이용한 로그인, 아이디/패스워드를 이용한 로그인과 추가적으로 스마트폰을 연계한 간편 로그인 등을 제공한다. 공인인증서나 아이디를 이용한 로그인에는 대부분 가상키보드를 제공한다. 예로서 (그림 1)은 전북은행의 아이디를 이용한 로그인에 사용되는 동적 가상키보드와 계좌의 비밀번호 입력에 사용되는 가상키보드이며, (그림 2)는 국민은행에서 공인인증서와 아이디를 이용한 로그인에 사용되는 동적 가상키보드를 보여준다.

(그림 1) 전북은행 가상키보드

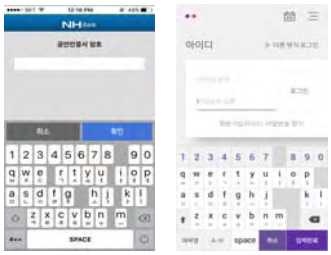


(그림 2) 국민은행 가상키보드

은행마다 제공되는 가상키보드의 성격이 다르며, 동일한 은행인 경우에도 로그인 방법에 따라 다르다. 즉, 재배열되는 키의 범위(숫자에만 한정), 키의 재배열 방법(상대적 위치 유지) 패스워드 입력 도중 키보드 재배열 가능 여부, 키의 재배열 단위(1칸 혹은 1/2칸), 빈 키의 삽입 여부, 가상키보드의 이동 허용 여부, 멀티마우스 기능 제공 여부 등에 따라 다양해진다.

2.2 스마트폰 환경

스마트폰 앱들도 패스워드 입력을 위하여 대부분 PC와 유사한 동적 가상키보드를 제공하고 있다. 본 논문에서는 4개의 은행 앱과 2개의 신용카드 앱을 대상으로 조사하였으며, (그림 3)과 같이 모두 랜덤한 위치에 빈칸의 키를 삽입함으로써 키의 위치를 동적으로 배치하고 있다.



(그림 3) 농협은행과 롯데카드 앱의 가상키보드

PC환경에서와 마찬가지로 각 앱의 동적 가상키보드는 각기 다른 보안적 특성을 가진다. 각 요소에 따라 앱들의 특징을 분석하면 <표 1>과 같다.

<표 1> 은행 및 신용카드 앱별 동적 가상키보드 특징

대상	앱이름	재배열 버튼	자동 재배열	빈칸 크기	화면 캡처	기타
IBK 기업은행	i-ONE뱅크	○	×	1	×	
CITI은행	씨티모바일	○	×	1	×	
하나은행	하나카드	○	×	0.5	×	
농협	NH Bank	○	×	0.5	○	
롯데카드	Lotte Card LIFE	○	×	1	○	
현대카드	현대카드	×	○	1	○	숫자만 입력

3. 스마트폰 동적 가상키보드 입력 분석

PC는 모니터의 크기, 해상도 및 다중모니터 등 사용자의 환경이 매우 다양할 뿐만 아니라, 제공되는 로그인 방법도 다양하다. 또한 PC에서는 사용 중인 작업창의 위치를 옮기거나 화면의 확대 및 축소로 상황에 따라 가상키보드의 위치 및 크기도 달라질 수 있기 때문에 마우스 클릭 위치를 추적하여 패스워드를 알아내는 것이 상대적으로 어렵다.

스마트폰도 기기의 종류와 해상도가 매우 다양하지만, 작업창의 이동이 불가능하고 확대/축소가 제한적이며 패스워드 입력화면은 회전이 불가능하여 고정되므로, 스크린 터치로부터 입력되는 패스워드의 추측이 상대적으로 용이하다.

스마트폰의 경우에는 사용자의 편의를 위하여 키의 재배열 방법을 제한적으로 적용하고 있다. 즉, 키의 위치를 재배열한다기 보다는 각 줄별로 1-2개의 빈칸을 삽입함으로써 동일한 키도 매번 다른 곳에 위치하도록 제공한다. 따라서 각 키가 속한 줄은 고정되며, 각 줄에서 키들의 상대적 위치는 변경되지 않는다. 예를 들면, q는 항상 2번째 줄에 있으며 w보다 오른쪽에 위치하지 않는다. 또한 화면 회전이 허용되지 않기 때문에 키의 크기는 고정된다.

본 논문에서는 삽입되는 빈칸의 크기가 1인 경우를 분석하였으며, 빈칸이 삽입되는 위치의 확률은 균일하다고 가정하였다. 1개의 빈칸이 추가되는 경우(1, 2, 4번 줄)와 2개의 빈칸이 추가되는 경우(3번 줄)로 구분되므로, 2번 줄과 3번 줄을 분석하여 <표 2>와 <표 3>에 표시하였다. 2번 줄의 경우를 예를 들면, 1개의 빈칸이 추가되어 키의 개수는 11개(#0~#10)가 된다. 만약 0번 키(#0)가 터치되었다면 입력값은 확실하게 'q'이다. 만약 1번 키(#1)가 터치되었다면 'q'일 확률과 'w'일 확률이 각각 0.1과 0.9이다. 반면에 5번 키(#5)가 터치되었다면 't'와 'y'일 확률이 각각 0.5로서 동일하다. 따라서 가운데 키에 비하여 양쪽에 있는 키는 공격자에 의해 분석될 확률이 높아진다. 또한 패스워드 입력을 마칠 때까지 키를 재배열하지 않으면 'pass'와 같이 패스워드에 동일한 키가 중복되는 경우는 동일한 위치를 터치하게 되므로 중복성이 노출된다. 따라서 하나의 키 입력마다 자동적인 재배열이 권고된다.

4. 결론 및 향후 연구

본 논문에서는 제한적 환경을 가지는 스마트폰의 동적 가상키보드의 취약점을 분석하였다. 향후에는 많은 앱을 조사 분석하고, 빈칸의 크기가 1/2인 경우와 키의 위치에 따라 다른 분석 확률을 보완한 빈칸의 삽입위치에 관한 연구를 수행할 것이다.

ACKNOWLEDGMENT

본 연구는 한국연구재단의 연구 지원(NRF-2017R1D1A3B03032637)에 의한 것임

<표 2> 빈칸이 1개일 경우의 확률 분석

위치	#0	#1		#2		#3		#4		#5		#6		#7		#8		#9		#10
키	q	q	w	w	e	e	r	r	t	t	y	y	u	u	i	i	o	o	p	p
확률	1	0.1	0.9	0.2	0.8	0.3	0.7	0.4	0.6	0.5	0.5	0.6	0.4	0.7	0.3	0.8	0.2	0.9	0.1	1

<표 3> 빈칸이 2개일 경우의 확률 분석

위치	#0	#1		#2			#3			#4			#5			#6			#7			#8			#9		#10
키	a	a	s	a	s	d	s	d	f	d	f	g	f	g	h	g	h	j	h	j	k	j	k	l	k	l	l
확률	1	0.2	0.8	0.022	0.356	0.622	0.067	0.467	0.467	0.133	0.533	0.333	0.222	0.556	0.222	0.333	0.533	0.133	0.467	0.467	0.067	0.622	0.356	0.022	0.8	0.2	1