ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

모바일 기기를 위한 보안 키패드의 취약점 분석☆

An Analysis on the Vulnerability of Secure Keypads for Mobile Devices

이 윤 호1*
Yunho Lee

요 약

스마트폰과 태블릿 PC 등의 모바일 플랫폼이 급격히 보급됨에 따라 이를 이용한 금융 거래나 전자상거래도 급증하고 있다. 모바일 환경에서는 데스크탑 PC 환경과는 달리 키보드나 마우스 대신 터치 스크린 상의 가상 키패드를 이용하여 패스워드 등의 중요 개인 정보를 입력하게 되는데, 이 때 터치 좌표가 노출될 경우 키 값이 쉽게 노출될 수 있다. 이러한 문제를 해결하기 위해 금융 거래와 관련된 대부분의 모바일 프로그램은 가상 키패드에서 키의 위치를 무작위로 바꾸는 보안 키패드를 채택하고 있다. 하지만, 각 키의 가변 위치가 2~3개에 불과하고 확률도 균등하지 않기 때문에 사용자의 중요 정보를 보호하는데는 한계가 있다. 본 논문에서는 대부분의 금융 관련 모바일 프로그램에 사용되는 보안 키패드에 대해 설명한 후, 기존 안전성 분석의 한계를 지적하고 터치 위치를 기반으로 키 값을 유추하는 새로운 공격 방법을 제시하고자 한다.

주제어 : 모바일 보안, 보안 키패드, 개인 정보, 키 로거

ABSTRACT

Due to the widespread propagation of mobile platforms such as smartphones and tablets, financial and e-commercial transactions based on these mobile platforms are growing rapidly. Unlike PCs, almost all mobile platforms do not provide physical keyboards or mice but provide virtual keypads using touchscreens. For this reason, an attacker attempts to obtain the coordinates of touches on the virtual keypad in order to get actual key values. To tackle this vulnerability, financial applications for mobile platforms use secure keypads, which change position of each key displayed on the virtual keypad. However, these secure keypads cannot protect users' private information more securely than the virtual keypads because each key has only 2 or 3 positions and moreover its probability distribution is not uniform. In this paper, we analyze secure keypads used by the most financial mobile applications, point out the limitation of the previous research, and then propose a more general and accurate attack method on the secure keypads.

☞ keyword : Mobile Security, Secure Keypads, Personal Information, Keylogger

1. 서 론

2009년 말부터 국내에서 시작된 스마트폰 열풍은 불과 2년 남짓 지난 지금 가입자가 3,000 만명에 이를 정도로 빠르게 확대되고 있다[2]. 세계적으로도 우리나라와 다르지 않은데, 미국의 경우 올해 2월 기준으로 보급된 전체 휴대폰의 50%가 스마트폰일 정도로 폭발적인 성장을 거듭하고 있으며 모바일 광고 등을 포함한 관련 시장 역시 급격히 확대되고 있다. 이의 가장 큰 원인으로는 풍부한 애플리케이션을 들 수 있는데, 누구나 공개된 SDK(Software Development Kit)를 이용하여 자유롭게 애플리케이션을 개발/배포할 수 있기 때문이다. 이렇게 스마트폰이 보급되면서 은행이나 증권사 등의 금융사도 스마트폰 금융 애플리케이션을 제작・배포하고 있는데, 2009년 말 13,000명에 불과하던 스마트폰 기반의 모바일뱅킹 가입자는 2012년 8월 현재 1,679 만명에 달하며, 일일 이용 실적도 9,000억원을 넘을 정도로 급성장하고 있다[3].

하지만, 기존 휴대폰과는 달리 스마트폰은 누구나 애플리케이션을 개발할 수 있다는 특성 때문에 일반 PC와 마찬가지로 해킹에 취약할 수 밖에 없다. 특히 스마트폰 운영체제를 변경하여 애플리케이션에게 root 사용자 권한을 부여하는 이른바 '루팅'이나 '탈옥'이 확산되면서 스마트폰 악성코드로 인한 피해가 우려되는 상황이다[4-9, 11-13]. 사용자의 부주의로 스마트폰에 악성코드가 설치되고 root 사용자 권한을 부여받아 실행될 경우 스마트폰에 저장된 각종 개인정보는 물론이고 유료 통화 유발 등으로 금전적

1 Dept. of Cyber Security & Police, Gwangju University, 277 Hyodeok-ro, Nam-gu, Gwangju, 503-703 KOREA.
* Corresponding author (leeyh@gwangju.ac.kr)
[Received 8 September 2012, Reviewed 9 October 2012(R2 13 February 2013), Accepted 23 April 2013]
☆ 이 연구는 2013년도 광주대학교 대학 연구비의 지원을 받아 수행되었음.

http://dx.doi.org/10.7472/jksii.2013.14.3.15

피해가 생길 수도 있는데 스마트폰 기반 악성코드는 갈수록 증가하는 추세에 있으며 APT 공격을 위한 악성코드가 발견되기도 하는 등 갈수록 진화하고 있는 추세이다[10]. 특히 가상 키패드를 통해 패스워드와 같은 중요 정보가 입력될 때, 사용자의 터치 좌표가 노출될 경우 패스워드가 그대로 유출될 수 있기 때문에 주의가 필요하다. 일반 PC에서는 사용자의 키보드 입력을 가로채 중요 정보를 유출하는 키로거(Keylogger) 위협을 막기 위해 금융 거래시 키보드 보안 프로그램을 추가로 설치하도록 하고 있지만 이를 스마트폰 환경에 그대로 적용하기는 현실적으로 쉽지 않다. 왜냐하면, 현재 대부분의 스마트폰은 사용자로부터 정보를 입력받을 때 별도의 하드웨어 키패드 대신 PC의 키보드와 유사한 소프트웨어 가상 키패드를 이용하고 있기 때문에 PC의 경우처럼 표준화된 드라이버 모델이 존재할 수 없고, 키패드 구현 방법에 따라 통신 방법도 다양하기 때문이다.

이러한 스마트폰 환경을 고려하여 거의 모든 스마트폰 금융 애플리케이션은 패스워드와 같은 중요 정보 입력시 독자적인 보안 키패드를 제공하여 터치 좌표가 노출되더라도 입력값을 알 수 없도록 하고 있다. 스마트폰 금융 애플리케이션에서 제공하는 보안 키패드는 크게 QWERTY 키패드와 ABC 키패드로 구분할 수 있으며, ABC 키패드보다는 기존 PC 자판과 배열이 동일한 QWERTY 키패드가 많이 사용되고 있다. 타입과 무관하게 거의 모든 보안 키패드의 기본 원리는 각 키의 배열을 매번 바꿈으로써 터치 좌표가 노출되더라도 입력된 키의 값을 알 수 없도록 하는데 있다. 하지만, 키의 위치 변화가 제한적이고, 가장자리에 위치한 키의 경우는 위치가 바뀌더라도 쉽게 노출되기 때문에 안전성을 높이는데 한계가 있다.

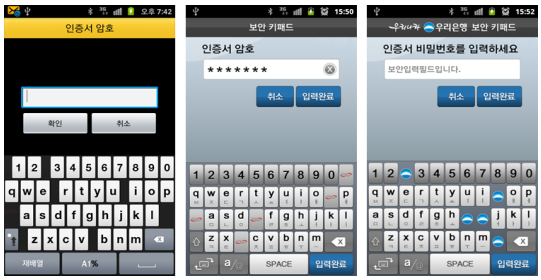
이러한 보안 키패드 안전성 분석 방법으로 균등 분할 방법이 제안되어 있지만, QWERTY 타입 보안 키패드 분석에만 적용될 수 있다는 한계가 있다. 본 논문에서는 타입과 무관하게 안전성을 분석할 수 있으며, 분석 결과의 정확도를 획기적으로 높인 새로운 안전성 분석 방법을 제안하고자 한다.

2. 기존 연구

스마트폰의 급격한 확산은 모바일 금융 거래의 급증을 가져왔으며 이로 인해 현재는 거의 대부분의 은행이나 증권사에서 전용 애플리케이션을 제공하고 있고, 사용자의 중요한 개인 정보를 보호하기 위해 보안 키패드를 채택하고 있다. 본 장에서는 모바일 보안 키패드의 동작 원리에 대해 살펴보고, 이에 대한 기존 공격 방법을 설명한다.

2.1 모바일 보안 키패드의 동작 원리

현재 국내에서 사용되고 있는 보안 키패드의 동작 원리는 각 키의 위치를 바꾼다는 점에서 기본적으로 같은데, 은행에서 사용하는 QWERTY 타입의 보안 키패드의 모습은 (그림 1)과 같다.



(그림 1) 은행의 보안 키패드 (국민은행, 우체국, 우리은행)
(Figure 1) Banks' Secure Keypads(KB, ePost, Wooribank)

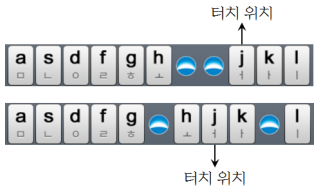
보안 키패드가 실행될 때마다 각 키의 위치가 무작위로 바뀌게 되며, 실행중인 상태일 때도 화면 아래쪽의 재배열 버튼을 눌러 키의 배치를 바꿀 수 있다(그림 2 참조). 일반적으로 각 키는 고정된 세로 위치를 갖지만 가로 방향의 위치를 바꿈으로써 터치 위치를 바꾸도록 하고 있으며, 단위 공백의 넓이는 키의 넓이와 동일하다.

(그림 2) 보안 키패드의 무작위 배열
(Figure 2) Random Layout of a Secure Keypad

국민은행의 경우 다른 보안 키패드와는 다르게 단위 공백의 넓이가 키 넓이의 1/2이기 때문에 키 배열에 대한 경우의 수가 훨씬 많다(그림 3 참조).

보안 키패드의 경우 실행할 때마다 키의 배열을 무작위로 바꾸기 때문에 같은 패스워드를 입력하더라도 터치 좌표는 매번 달라지게 된다. (그림 3)은 (그림 2)와 같은 자판

(그림 3) 국민은행 보안 키패드의 무작위 배열
(Figure 3) Random Layout of the KB's Secure Keypad



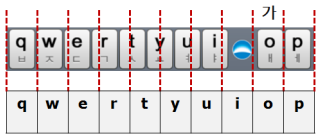
(그림 4) 터치 좌표의 변화
(Figure 4) Change of Touch Coordinates

배열일 경우, 패스워드 중 'j'를 입력한다고 했을 때의 좌표 변화를 나타낸다.

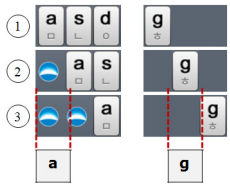
2.2 기존 공격 방법

2.1 절에서 설명한 바와 같이 같은 패스워드를 입력하더라도 터치 위치는 매번 바뀌기 때문에 공격자가 터치 좌표를 획득했다고 하더라도 이를 통해 실제 입력된 정확한 키 값을 알아낼 수는 없다. 하지만, 키패드의 위치 변화가 제한적이기 때문에 몇차례 터치 좌표를 획득했다면 통계적인 방법을 이용하여 패스워드의 근사값을 알아낼 수는 있으며, 최종적으로 사전 공격 등을 이용하면 거의 대부분 패스워드를 유추할 수 있게 된다. 이동현 등은 단위 공백의 넓이가 키의 넓이와 같은 경우에 한해 균등 분할 방식을 적용하여 안전성을 분석하였다[1].

균등 분할 방식이란 (그림 5)와 같이 공백을 고려하지 않고 키패드를 구성한 후 터치 좌표를 적용하는 방식인데, 예를 들어 터치 좌표가 그림의 '가' 위치일 경우 키 'o'라고 판단하게 된다. 이 방식은 왼쪽이나 오른쪽 등 가장자리에 위치한 키(예를 들면 q나 a 등)와 가운데에 위치한 키(예를 들면 y나 g 등)의 위치 변화를 확률적으로 분석한 결과를 기반으로 하고 있다. 가장자리에 해당하는 'a' 키의 경우 모두 그림 6의 ①, ②, ③ 세가지 위치에 나타날 수 있는데, ①과 같을 확률은 81.8%로 매우 높지만 ②와 같을 확률은 16.4%, 그리고 ③과 같을 확률은 1.8%에 불과해 전체적으



(그림 5) 균등 분할 방식
(Figure 5) A Method of Uniform Partition



(그림 6) 가장자리와 가운데 자리 키의 확률 차이
(Figure 6) Probability Difference between the Border and the Center Key

로 균등 분할한 'a' 위치에 터치할 확률이 85.1%로 매우 높음을 알 수 있다.

하지만, 상대적으로 가운데 위치한 키의 경우는 확률이 그렇게 높지 않게 되는데, 예를 들어 'g' 키를 고려해 보면 50.9%에 불과하여 정확도가 많이 떨어짐을 알 수 있다(그림 6 참조). 즉, 패스워드를 구성하는 각 키가 가장자리의 키인 경우에는 정확하게 유추할 수 있지만, 가운데에 위치한 키는 그렇지 못한 단점이 있다.

[1]에 따르면 공격자가 터치 좌표를 3회 획득했을 경우 실제 패스워드를 유추할 수 있는 확률이 95%에 이르는 것으로 나타났는데, 이 가운데 모든 키를 정확하게 유추한 경우는 48%이기 때문에 정확도 측면에서 보면 개선할 여지가 있다고 볼 수 있다.

2.3 기존 공격 방법의 한계

기존 공격 방법은 키패드의 각 행에 위치한 키가 일정해야 하는 제약이 있다. 즉, QWERTY 타입 키패드인 경우에만 적용되며 키가 정렬되어 있는 ABC 타입 키패드에는 적용되지 않는다(그림 7 참조). 예를 들어, 그림 7의 키패드에서 i 키의 위치를 보면, 왼쪽 그림의 경우 두 번째 행에 있지만, 오른쪽 그림에서는 공백의 위치에 의해 세 번째 행에 표시되기 때문에 균등 분할 방식으로 입력 키를 유추하는데 한계가 있다. 왜냐하면 균등 분할 방식은 행마다 표시되는 키가 일정해야 하기 때문이다.

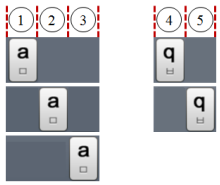
(그림 7) ABC 타입 보안 키패드
(Figure 7) ABC Type Secure Keypad

3. 제안한 공격 방법

2 장에서 살펴본 바와 같이 모바일 보안 키패드의 안전성은 터치 좌표의 무작위성에 기반하고 있다. 하지만, 터치 좌표의 변화가 제한적이고 가로 방향의 변화만 있을 뿐 세로 방향의 변화가 없다는 점에서 높은 안전성을 기대하기 어렵다는 점은 기존 안전성 분석 연구 결과로 발표된 바 있다[1]. 본 장에서는 기존 공격 방법 및 결과를 요약하여 살펴보고 보다 향상된 공격 방법에 대해 설명하도록 한다.

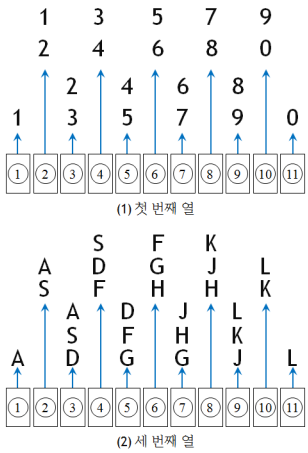
3.1 보안 키패드 분석

현재 상용화된 보안 키패드를 보면 각 키의 위치가 2~3 개로 고정되어 있다. 예를 들어, a 키의 경우 ①, ② 또는 ③의 위치에만 표시되며, q 키는 ④ 또는 ⑤ 위치에만 표시된다(그림 8 참조). 또한 각 위치에 표시될 확률이 균일하지 않기 때문에 사용자가 특정 위치에 터치한 경우 어떤 키인지 높은 확률로 유추할 수 있게 된다.



(그림 8) 각 키의 표시 위치
(Figure 8) Display Position of Each Key

예를 들어, 세 번째 열은 a, s, d, f, g, h, j, k, l 등 9개의 키와 함께 공백 두 개를 포함하여 11개의 키로 구성되기 때문에 전체 배열의 수는 $_{11}C_9 = {}_{11}C_2 = \frac{11!}{(11-2)!\times 2!} = \frac{11\times 10}{2} = 55$개다. 가장 왼쪽에 해당되는 ① 위치에 a 키가 위치하는 경우의 수는 $_{10}C_8 = 45(81.8\%)$이며, ② 위치에 a 키가 위치하는 경우의 수는 $_9C_1 = 9(16.4\%)$이고, ③ 위치에 a 키가 위치하는 경우의 수는 1(1.8%)임을 알 수 있다. 이를 토대로 각각의 터치 위치별로 키의 확률도 계산할 수 있는데, 첫 번째 열과 세 번째 열을 분석한 결과는 (그림 9)와 같다.



(그림 9) 첫 번째와 세 번째 열의 배열
(Figure 9) Layout of the First and the Third Row of Keypad

첫 번째, 두 번째 및 네 번째 키열의 경우 공백을 하나 포함하게 되고, 세 번째 키열은 두 개의 공백을 포함하기 때문에 여기서는 첫 번째와 세 번째 키열을 분석하도록 한다. 두 번째 및 네 번째 키열은 첫 번째 키열과 유사하게 분석할 수 있다. 그림 9-(1)을 보면 숫자가 표시되는 첫 번째 키 열의 경우 ① 위치에 표시될 수 있는 키는 1 키와 공백이지만 일반적으로 공백을 터치하지는 않기 때문에 사용자가 ① 위치를 터치하였다면 100% 확률로 1 키임을 알 수 있게 된다. ③ 위치의 경우 2 키와 3 키가 위치할 수 있지만 2 키인 경우의 수가 $_2C_1 \times 1 = 2\times 1 = 2$이고, 3 키인 경우의 수가 $1\times {}_8C_1 = 1\times 8 = 8$이기 때문에 80% 확률로 3 키임을 유추할 수 있다.

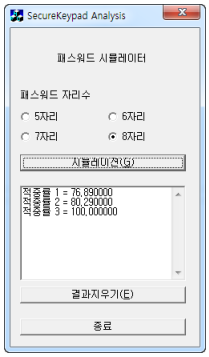
공백이 두 개 포함된 세 번째 키열의 경우 ② 위치와 ⑤ 위치를 분석해 보면, ② 위치에 올 수 있는 키는 공백을 제외하고 a, s 두 개이며, ⑤ 위치에는 공백을 제외하고 d, f, g키 뿐이다. ② 위치의 키가 a인 경우의 수는 $_1C_1 \times {}_9C_1 = 1\times 9 = 9$이며, s 인 경우의 수는 $_9C_2 = \frac{9\times 8}{2} = 36$이기 때문에 a 키일 확률은 20%, s 키일 확률은 80%가

(표 1) 보안 키패드에 대한 위치별 키 확률
(Table 1) Probability of Each Key of Keypad

키열 \ 위치	①		②		③		④		⑤		⑥		⑦		⑧		⑨		⑩		⑪	
첫 번째	1	100%	1	10%	2	20%	3	30%	4	40%	5	50%	6	60%	7	70%	8	80%	9	90%	0	100%
			2	90%	3	80%	4	70%	5	60%	6	50%	7	40%	8	30%	9	20%	0	10%		
두 번째	q	100%	q	10%	w	20%	e	30%	r	40%	t	50%	y	60%	u	70%	i	80%	o	90%	p	100%
			w	90%	e	80%	r	70%	t	60%	y	50%	u	40%	i	30%	o	20%	p	10%		
세 번째	a	100%	a	20.0%	a	2.2%	s	6.6%	d	13.3%	f	22.2%	j	13.3%	k	6.6%	l	2.2%	l	20.0%	l	100%
			s	80.0%	s	35.6%	d	46.7%	f	53.4%	g	55.6%	h	53.4%	j	46.7%	k	35.6%	k	80.0%		
					d	62.2%	f	46.7%	g	33.3%	h	22.2%	g	33.3%	h	46.7%	j	62.2%				
네 번째	z	100%	z	14.3%	x	28.6%	c	42.9%	b	42.9%	n	28.6%	m	14.3%	m	100%						
			x	85.7%	c	71.4%	v	57.1%	v	57.1%	b	71.4%	n	85.7%								

된다. 마찬가지로 ⑤ 위치의 키가 d 인 경우의 수는 ${}_4C_2 = 6$이고, f 인 경우의 수는 ${}_4C_1 \times {}_6C_1 = 4 \times 6 = 24$이며, g 인 경우의 수는 ${}_6C_2 = 15$이기 때문에 d 키일 확률은 13.3%, f 키일 확률은 53.4%, 그리고 g 키일 확률은 33.3% 이다. 전체 위치에 따른 키 확률을 분석한 결과는 다음 (표 1)과 같다.

예를 들어 네 번째 키 열의 ⑤ 위치에 터치되었다면 b 키(42.9%)와 v 키(57.1%)로 유추할 수 있다. 만약 해커가 이러한 터치 좌표를 두 번 이상 획득했다면 키 유추 확률을 보다 높일 수 있다. 예들 들어 첫 번째 획득에서 ⑤ 위치, 두 번째 획득에서 ⑥ 위치, 그리고 세 번째 획득에서 ④ 위치로 확인되었다면 해당 키는 f 임을 쉽게 알 수 있다.



(그림 10) 시뮬레이터
(Figure 10) Simulator

3.2 안전성 분석 결과

본 논문에서는 기존 연구와 마찬가지로 해커가 3회 터치 좌표를 획득한 경우를 가정하였으며, 5 - 8 자리 패스워드에 대해 시뮬레이션을 진행하여 안전성을 분석하였다 (그림 10 참조). 구현과 관련한 세부 내용은 다음 (표 2)와 같다.

(표 2) 시뮬레이션 환경
(Figure 2) Simulation Environment

구현 환경	Windows 7 + Visual Studio 6.0
패스워드 자리 수	5 - 8 자리
패스워드 수	10,000 개
해커가 획득한 터치 좌표의 수/패스워드	3 회

기존 연구에서는 추천 패스워드가 일치한 경우와 각 터치 좌표를 모두 조합하여 일치한 경우 등 두가지를 측정하였지만, 본 논문에서는 이를 보다 세분화하여 추천 패스워드가 일치한 경우, 세 개의 추천 패스워드가 일치한 경우, 그리고 모든 조합에 대해 일치한 경우 등 세가지로 측정하였다. 제안한 패스워드 추측 방법을 이용할 경우 모든 조합에 대해 일치하는 패스워드가 반드시 존재하기 때문에 세 번째 측정은 모두 100%를 보였다. 기존 연구 결과와 제안한 안전성 분석 결과를 비교하면 다음 그림과 같다.

비교 결과를 보면 추천 패스워드가 일치한 경우가 적게는 18.6%에서 많게는 47.9%까지 제안한 방식이 높게 나왔다. 또한, 모든 조합에서 패스워드가 일치하는 경우가 자리수와 무관하게 모두 100%로 나오는 등 현재 상용화된 보안 키패드의 안전성에 심각한 문제가 있음을 알 수 있다.

(표 3) 시뮬레이션 결과
(Table 3) Simulation Results

	추천 패스워드 일치		세 개의 추천 패스워드 일치		모든 조합에서 일치	
	기존연구	제안방식	기존연구	제안방식	기존연구	제안방식
5자리	64%	83.9%	-	99.6%	100%	100%
6자리	48%	81.3%	-	96.6%	100%	100%
7자리	52%	79.8%	-	89.0%	96%	100%
8자리	28%	76.9%	-	80.3%	84%	100%

4. 결 론

본 논문에서는 기존 모바일 금융 거래의 안전성을 높이기 위해 사용되는 보안 키패드의 안전성을 분석해 보았다. 현재 상용화된 보안 키패드의 경우 무작위로 키의 배열을 바꿈으로써 좌표값으로부터 키 값을 유추하지 못하도록 하고 있지만, 바뀌는 키의 위치가 매우 제한적이기 때문에 안전성을 높이는데 한계가 있다. 즉, 해커가 두 번 이상 동일한 패스워드에 대한 터치 좌표를 획득했다면 매우 높은 확률로 키를 유추할 수 있게 된다. 하지만, 기존 연구에서는 자주 사용되는 8 자리 패스워드의 경우 추천 패스워드가 일치할 확률이 28%에 불과하였지만, 본 논문에서 제안한 방법에 따라 패스워드를 추측할 경우 일치할 확률이 75.9%에 이르는 것으로 나왔다. 이는 해커에게 3 회 터치 좌표가 노출된다면 매우 높은 확률로 패스워드가 유출됨을 의미하기 때문에 기존 보안 키패드에 심각한 안전성 문제가 있음을 알 수 있으며 보다 안전성을 높인 보안 키패드의 개발이 시급함을 의미한다. 또한 제안한 안전성 분석 방법은 QWERTY 타입 보안 키패드 뿐만 아니라 ABC 타입 보안 키패드에도 적용할 수 있다는 장점이 있다.

참 고 문 헌(Reference)

[1] 이동현, 배동환, 유승록, 채진영, 이윤호, 양형규, “Security Analysis on the Keypad for Smartphones”, Review of KIISC, Vol. 21, No. 7, KIISC, 2011, pp. 30-37.

[2] MK News, “국내 스마트폰 가입자 3000만명 돌파 전망”, http://news.mk.co.kr/newsRead.php?year=2012&no=469973.

[3] MoneyToday, “모바일뱅킹 고객 3천만. ‘스마트폰’ 열풍 덕”, http://news.mt.co.kr/mtview.php?no=2012081609493763978&type=1.

[4] Roland M., Langer J. and Scharinger J., “Practical Attack Scenarios on Secure Element-Enabled Mobile Devices,” 2012 4th International Workshop on Near Field Communication, 2012, pp. 19-24.

[5] Porras P., Saidi H. and Yegneswaran V., “An Analysis of the iKee.B iPhone Botnet,” MobiSec 2010, 2010, pp. 141-152.

[6] Vidasa T., Zhangb C. and Christin N., “Toward a general collection methodology for Android devices,” 11th Annual Digital Forensics Research Conference, 2011, pp. S14-S24.

[7] Schmidt, A. D., Schmidt, H. G., Batyuk, L., Clausen, J. H., Camtepe, S. A., Albayrak, S. and Yildizli, C., “Smartphone malware evolution revisited: Android next target?,” 4th International Conference on Malicious and Unwanted Software, 2009, pp. 1-7.

[8] Sanders, B. M., “Privacy and Security Enhancements for Android Applications,” Thesis of Master of Science in Computer Science, University of California, 2008.

[9] La Polla, M., Martinelli, F. and Sgandurra, D., “A Survey on Security for Mobile Devices,” IEEE Communications Surveys & Tutorials, 2012, pp. 1-26.

[10] AhnLab, “An Android Malwares for the APT attacks”, Ahnlab ASEC Report Vol. 31, 2012.

[11] Guo, C, Wang, H. J. and Zhu, W., “Smart-phone attacks and defenses,” Proceedings of the 3rd Workshop on Hot Topics in Networks, 2004.

[12] Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y. and Dolev, S., “Google Android: A State-of-the-Art Review of Security Mechanisms,” CoRR abs/0912.5101, 2009.

[13] Chin, E., Felt, A. P., Sekar, V. and Wagner, D., “Measuring user confidence in smartphone security and privacy,” Proceedings of the Eighth Symposium on Usable Privacy and Security, 2012.

◐ 저 자 소 개 ◑

이 윤 호

1991년 성균관대학교 정보공학과 졸업(학사)
1993년 성균관대학교 정보공학과 졸업(석사)
2008년 성균관대학교 컴퓨터공학과 졸업(박사)
1993년~2000년 한국통신(KT) 연구개발본부 전임연구원
2000년~2005년 KBS인터넷(주) 기술지원팀장
2004년~2005년 ㈜뱅크타운 책임연구원
2008년~2011년 성균관대학교 컴퓨터공학과 연구교수
2011년~현재 광주대학교 사이버보안경찰학과 교수
관심분야 : 전자투표, 컨텐츠보안, 응용보안 등
E-mail : leeyh@gwangju.ac.kr