情 報 保 護 學 會 誌
第21卷 第7號, 2011. 10

스마트폰을 위한 보안 키패드의 안전성 분석

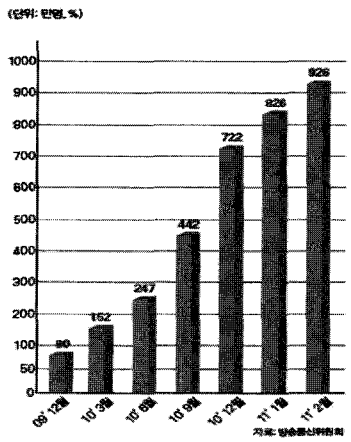
이 동 현*, 배 동 환*, 유 승 록*, 채 진 영*, 이 윤 호**, 양 형 규***

요 약

보안 키패드는 사용자가 스마트폰을 이용하여 금융 거래를 할 때 사용자가 입력한 패스워드의 터치 좌표가 노출되더라도 키 값을 유추할 수 없도록 한 보안 애플리케이션이다. 하지만, 현재 상용화된 보안 키패드는 좌표값 노출에 따른 키값 노출을 막기 어려우며, 특히 휴리스틱 분석이나 사전 공격(dictionary attack)등에 취약한 문제가 있다. 본 논문에서는 현재 사용되는 보안 키패드의 취약점을 분석하고, 이러한 취약점을 해결하기 위한 몇 가지 개선 방안을 제안한다.

Ⅰ. 서 론

최근 국내 휴대전화 단말기 5대 가운데 1대가 스마트폰일 정도로 스마트폰 사용자가 급증하고 있다 ([그림 1] 참조). 또한 스마트폰뿐만 아니라 태블릿 PC와 같은 스마트기기 이용자도 꾸준한 추세로 늘어가고 있으며, 듀얼코어를 탑재한 신형 스마트기기의 등장과 최근 선보인 LTE 기반 후속 스마트폰 모델들을 생각하면 스마트폰 및 기기 이용자는 계속 증가추세를 보일 것으로 예상되는 가운데 전문가들은 올 연말까지 스마트폰 가입자 수가 이천만명을 돌파할 것으로 내다보고 있다 [1].



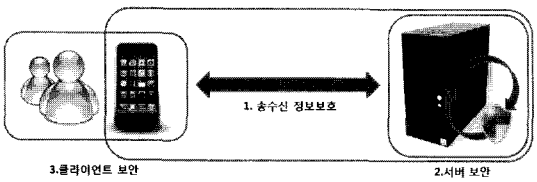
[그림 1] 스마트폰 사용자 증가 추이

스마트폰은 와이파이나 3G 이동통신망을 이용해 언제 어디서든 인터넷에 접속할 수 있는 특징이 있으며, 사용자가 원하는 다양한 애플리케이션을 앱스토어나 마켓에서 다운받아 사용할 수 있다는 특징을 가지고 있다. 이러한 애플리케이션으로 인하여 현재 내가 있는 위치 주변에 어떠한 건물이 있는지 검색할 수 있게 되었고, 버스나 지하철 같은 대중교통의 도착시간을 실시간으로 확인하거나 인터넷 뱅킹 및 주식거래, 음악 감상, 게임 등을 장소와 시간에 구애받지 않고 이용할 수 있는 환경을 구축하였다 [2].

이런 편리한 애플리케이션들 중에 주식, 증권, 뱅킹 같은 금융 애플리케이션들은 개인정보 및 인증서, 패스워드 등 중요 정보를 다루고 있고 이러한 정보가 노출될 시 큰 피해를 입을 수 있기 때문에 은행이나, 증권 등의 금융사들은 여러 가지 방법으로 보안에 중점을 두고 애플리케이션을 개발하였다 [3] [4].

금융이나 뱅킹 애플리케이션들은 크게 세 가지 방법으로 중요한 정보를 보호하는데 서버와 클라이언트 사이의 송수신 정보 보호를 위한 데이터 암호화, 서버나 데이터베이스 보안을 위한 시스템 보안, 그리고 보안 키패드를 중심으로 한 클라이언트 보안이 그것이다 ([그림 2] 참조).

* 강남대학교 컴퓨터미디어정보공학부 정보보호동아리 (abinknight@naver.com, shadowbug@naver.com, yabi01@naver.com, leopard524@naver.com)
** 광주대학교 사이버보안경찰학과 교수 (leeyh@gwangju.ac.kr)
*** 강남대학교 컴퓨터미디어정보공학부 교수 (hkyang@kangnam.ac.kr)



〔그림 2〕 스마트폰 보안 통신 환경

서버와 클라이언트 사이의 송수신 정보를 암호화하는 것과, 서버 내부 시스템 보안은 높은 강도의 보안 알고리즘 및 보안정책이 적용되어 설계되어있기 때문에 외부의 접근으로 인하여 정보가 노출되거나 변조될 확률은 낮다. 하지만, 클라이언트 보안의 경우 사용자의 중요 정보 입력 방법 등 편의성을 고려하여야 하고, OS 환경 등의 제약 조건으로 인해 앞의 두 가지 경우처럼 높은 보안정책을 적용하기 어려우며, 이로 인해 해커들도 비교적 접근하기 쉽고 보안이 취약한 이 부분을 주요 공격 대상으로 삼고 있다[5] [6].

이러한 문제를 해결하기 위해 PC에서 처럼 스마트폰용 각종 백신 애플리케이션이 존재하는데 국내 프로그램으로는 V3모바일, 알약 안드로이드가 존재하고, 외국 프로그램으로는 안티 바이러스 프리(Anti Virus Free), 룩아웃 모바일 시큐리티(Lookout Mobile Security)같은 무료 백신 소프트웨어가 존재하며, 삼성의 스마트 기기 같은 경우 V3모바일을 출시할 때부터 탑재하고 하고 있다. 하지만 타사의 스마트기기 같은 경우 사용자가 직접 설치를 해야 하는 번거로움과, 아직 스마트폰용 백신이 나온 지 오래되지 않아 안정성이 충분히 검증되지 않은 백신들도 존재하며, 사용 시 잦은 팝업으로 인해 삭제하거나 실시간 감시를 꺼두는 사용자들도 존재한다[7] [8] [9] [10].

특히, 애플리케이션 자체의 보안이 아무리 충실하다고 해도 요즘 나오는 스마트폰의 경우에는 멀티태스킹을 지원하고 있는데, 해커가 해킹용 애플리케이션을 백그라운드로 동작시키거나, 해킹 툴을 이용해 애플리케이션을 해킹하여 보안 키패드에서 입력된 터치 좌표 값을 가로챈다면 클라이언트와 서버와의 암호화 송수신을 통한 보안을 무시한 채 사용자가 입력한 패스워드 값을 알 수 있게 된다. 이러한 이유로 패스워드 등의 주요 정보를 입력할 때 보안 키패드를 적용하고 있는데, 보안 키패드란 각 키의 위치를 무작위로 변경하여 터치 좌표가 노출되더라도 실제 입력된 키 값을 알 수 없도록 하는 키패드를 말한다. 하지만 사용상 각 키의 변경 위치에 제한이 있을 수밖에 없기 때문에 키 값을 안전하게 보호하기에는 한계가 있을 수밖에 없다.

본 논문에서는 스마트폰에서 사용자가 입력한 터치 좌표값이 해커에 의해 노출 되었을 때 현재 사용 중인 보안 키패드 애플리케이션이 실제로 안전한지에 대해 검증을 해보고 현재 취약점을 극복할 수 있는 방안을 제시한다.

Ⅱ. 보안 키패드의 종류

금융관련 애플리케이션의 경우 보안을 위해 OS에서 제공하는 일반 키패드가 아닌 자체 보안 키패드를 사용하고 있으며, 현재 사용되고 있는 보안 키패드는 비슷한 방식을 사용하는데, 공백이나 마크를 이용하고, 사용자의 편의성에 중점을 둔 QWERTY 보안 키패드와 보안에 중점을 둔 ABC 키패드 등 크게 2가지로 구분할 수 있다.

2.1 QWERTY 키패드

QWERTY 키패드는 키의 배열이 기존 자판과 동일하며 공백의 넓이에 따라서 크게 2가지로 구분 된다. 우선 입력 키 넓이의 반 정도 되는 공백을 이용한 보안 키패드들의 특징은 10개의 공백(첫줄 2개, 둘째 줄 2개, 셋째 줄 4개, 넷째 줄 2개)을 무작위로 배치하여 터치 좌표를 무작위로 변화시키며([그림 3] 참조) 기존 QWERTY 키보드와 전체적인 형태가 크게 다르지 않다.

배열된 키의 넓이와 동일한 공백 또는 마크를 이용한 보안 키패드는 5개(첫줄 1개, 둘째 줄 1개, 셋째 줄 2개, 넷째 줄 1개)의 키 넓이와 동일한 공백 또는 마크를 사

(a)국민은행 (b)외환은행 (c)하나은행

〔그림 3〕 키의 절반 크기의 공백을 이용한 QWERTY 방식의 보안 키패드

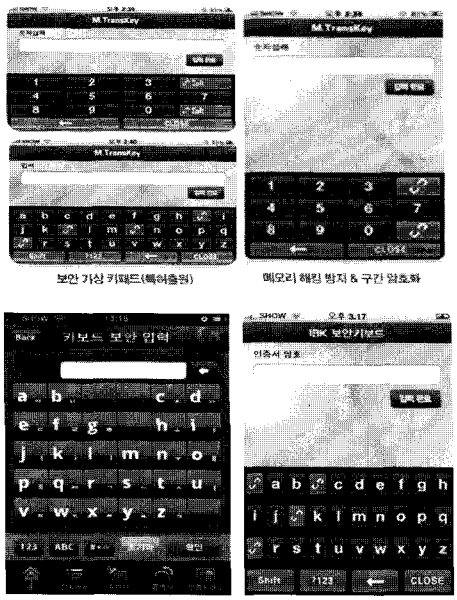
(a) 우리은행 (b) 미래에셋증권

〔그림 4〕 키의 한칸 크기의 스마트뱅킹 보안 키패드

용한다 ([그림 4] 참조).

2.2 ABC 키패드

ABC 키패드의 특징으로는 위에서 분석한 QWERTY 방식의 키패드와는 다르게 ABC 순서로 키를 배열하며 역시 공백 또는 마크를 추가한다([그림 5) 참조) [11] . 키패드의 각 줄 마다 고정적인 키가 들어가는 QWERTY 키패드와는 달리 ABC 키패드는 사용시점에 따라 무작위로 삽입되는 공백에 따라 각 줄마다 들어가는 키의 개수가 다르기 때문에 QWERTY 키패드에 비하여 좌표



보안 가상 키패드(특허출원) 메모리 해킹 방지 & 구간 암호화

(위) 소프트시큐리티 'mTransKey'
(아래) (좌)신한은행 (우)IBK 기업은행

〔그림 5〕 ABC형식의 스마트뱅킹 보안 키패드

값이 노출되더라도 실제 키의 값을 유추하기가 어렵다.

Ⅲ. 보안 키패드에 대한 안전성 분석

앞에서 언급한 키패드들 중에 안드로이드 환경의 국민은행 보안 키패드에 대한 이론적 안전성 분석을 통해, 터치 좌표가 노출 된 경우에도 키패드 값을 보호할 수 있는지 살펴보고 실제로 비슷한 키패드 환경을 구현하여 실제적인 안전성을 분석하도록 한다. 보안 키패드의 핵심은 패스워드와 같은 중요 정보를 입력할 때 키 배열을 매번 다르게 함으로써 좌표값이 노출되더라도 입력 키 값을 알 수 없도록 하는데 있다. 이 때 특정키가 위치할 수 있는 곳이 모두 n 개라고 가정했을 때 각각에 위치할 확률은 $1/n$로 균등해야 불확실성을 극대화할 수 있으며 안전성을 보장할 수 있게 된다. 만약 특정 위치에 있을 확률이 매우 높거나 매우 낮다면 키의 위치를 바꾸는 것이 의미없게 되며 좌표값으로부터 키 값을 유추할 가능성이 높아진다.

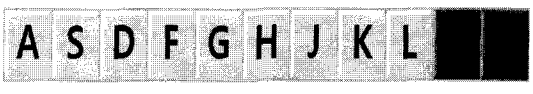
3.1 QWERTY 보안 키패드의 안전성 분석

편의상 공백과 키의 길이가 같다고 가정했을 때, 세 번째 키패드 열의 가장자리에 위치한 "A" 키와 가운데에 위치한 "G" 키를 이용하여 무작위 위치에 따른 안전성을 분석하면 다음과 같다. A, S, D, F, G, H, J, K, L 키로 구성된 세 번째 키패드 열의 경우 공백을 포함하여 모두 11개의 자리로 구성되어 있으며 공백의 위치를 무작위로 정할 경우 가능한 키패드 열은 $C_2^{11} = 55$ 개이다 ([그림 6] 참조).

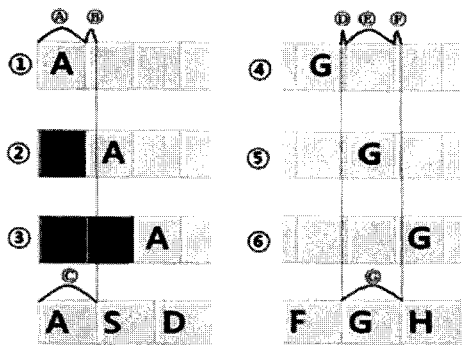
3.1.1 확률적 분석

공백이 적용 된 키패드의 경우 각각의 키는 공백의 위치에 따라 움직일 수 있는 범위를 가지게 된다.

예를 들어 "A" 키의 경우 공백에 따라 ①, ② 또는 ③ 번과 같은 형태를 갖게 되는데, ① 번과 같은 형태일 확률은



〔그림 6〕 문자 키패드의 구성 예



(좌) 공백에 따른 "A" 키의 위치변화
(우) 공백에 따른 "G" 키의 위치변화

〔그림 7〕 공백 위치에 따른 각 키의 위치 변화

$$\frac{45}{55}\times 100 = 81.81\%$$

이며, ② 번과 같은 형태일 확률은

$$\frac{9}{55}\times 100 = 16.36\%$$

이고, ③ 번과 같은 형태일 확률은

$$\frac{1}{55}\times 100 = 1.81\%$$

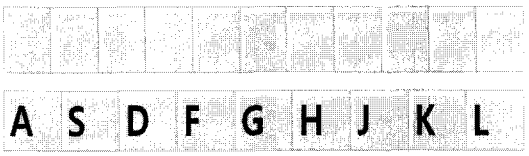
이다.

"G" 키의 경우 공백에 따라 ④, ⑤ 또는 ⑥ 번과 같은 형태를 갖게 되는데, ④ 번과 같은 형태일 확률은 27.27%, ⑤ 번과 같은 형태일 확률은 45.45%, 그리고 ⑥ 번과 같은 형태일 확률은 27.27%이다. 이상의 결과를 분석해 보았을 때, 각 형태에 대한 확률은 균등하지 않으며 특히 가장자리인 경우 확률이 극단적으로 차이가 남을 알 수 있다.

3.1.2 좌표값을 이용한 키 검출

III.I.I의 결과에 따라 공백이 적용되었음에도 불구하고 중간에 위치한 키는 어느 정도의 보안강도를 가지나 가장자리 부분의 키들은 굉장히 낮은 취약점을 가지고 있음을 알 수 있다. 공백을 고려하지 않고 전체 키 열을 균등 분할하여 키 값을 추출할 경우의 안전성을 분석해 보면 다음과 같다 ([그림 8] 참조).

예를 들어 "A" 키의 균등 분할한 넓이 Ⓒ = Ⓐ + Ⓑ 이므로 "A" 키를 누르기 위해 Ⓒ 영역을 터치할 확률은 85.08%이며 ([그림 7-(좌)]), "G" 키의 균등 분할한 넓이 Ⓖ = Ⓓ + Ⓔ + Ⓕ 이므로 "G" 키를 누르기 위해



〔그림 8〕 공백을 고려하지 않는 키패드 열의 균등 분할

Ⓖ 영역을 터치할 확률은 50.85% 이다([그림 7-(우)]). 즉, 키패드 열을 균등분할한 후 터치 좌표값으로부터 키 값을 유추할 경우의 정확도가 가장자리의 키는 무려 85% 이상이며, 중간에 위치한 키의 경우도 1/2 이상이라는 의미이다.

3.1.3 3회 적용 후의 안전성

균등분할 방법을 이용하여 좌표값으로부터 키 값을 추측할 수 있지만, 단 한번만에 정확한 키 값을 찾을 수는 없기 때문에 사용자가 같은 패스워드를 3회 입력한 각각의 좌표값을 공격자가 입수했다는 가정 하에 안전성을 분석하면 다음과 같다.

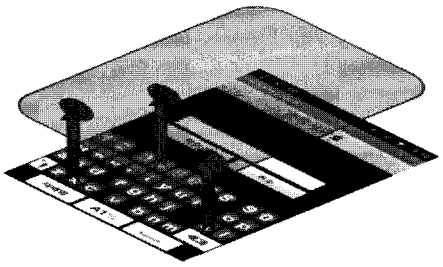
먼저 "A" 키를 입력하기 위해 Ⓒ를 터치할 확률을 p 라고 하면 3번 중 2번 이상 Ⓒ를 터치할 확률 P를 $P = p^3 + 3p^2(1-p)$와 같이 계산할 수 있는데, $p = 85.08\%$ 이므로 P는 93.08%가 된다. 마찬가지로 "G" 키에 대한 확률을 계산해 보면 51.27%로 상당히 높은 확률을 갖게 된다.

3.2 QWERTY 보안키패드 해킹SW 구현

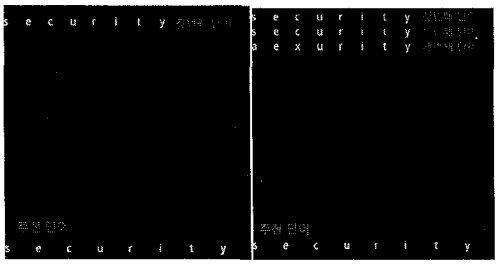
본 절에서는 위에서 분석한 이론적 안전성을 바탕으로 실제 보안 키패드 환경을 안드로이드 환경 하에 구축한 후 임의로 패스워드를 선정하여 3회 입력하였고, 각각의 입력 좌표값을 공격자가 가로챘을 때, 정확하게 패스워드를 유추할 수 있는지 검증해 보도록 한다.

3.2.1 안드로이드 키패드 메시지 후킹

안드로이드 UI는 터치 메시지가 전달 될 때, 상위 프레임에서 하위 프레임으로 터치 메시지를 전달하는 구조로 이루어져 있어서, 비슷한 환경의 보안 키패드 위에 3.1.2에서 사용된 터치인식방법을 적용한 해킹 프레임을 놓아 터치 좌표를 중간에 후킹 하는 구조로 해킹 툴



〔그림 9〕 터치 메시지 후킹 구조



〔그림 10〕 표본의 개수에 따른 추천 단어

을 구현하였다 ([그림 9) 참조).

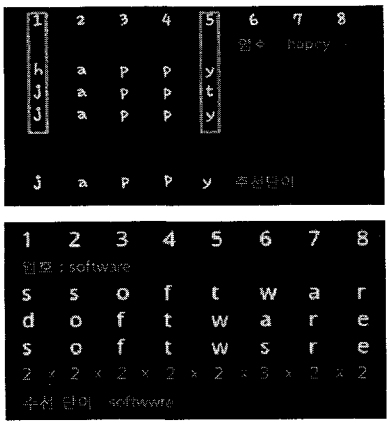
3.2.2 패스워드 추측 알고리즘

[그림 10]은 위에서 설명한 방법에 따라 터치 좌표로부터 키 값을 추출한 예이다.

예를 들어 사용자가 패스워드 "security"를 입력했을 때, 첫 번째 단어와 두 번째 단어에서는 "security"로 정확하게 유추했지만 세 번째 단어에서는 "aexurity"로 잘못 유추하였다. 하지만 각 문자에 대한 다수결 원칙을 적용하였을 때 "security"가 패스워드 인 것으로 추측할 수 있다.

다수결의 원칙에 의하여 추천 단어가 인증에 성공하면 사용자가 입력한 패스워드를 정확하게 유추한 경우이며, 그렇지 않은 경우라도 3회 유추한 패스워드의 각 문자를 조합하거나 휴리스틱 분석을 통하여 정확한 패스워드를 유추 할 수 있다.

예를 들어 [그림 11-(위)]와 같이 패스워드가 "happy"였을 때, 첫 번째 추출 값이 "happy", 두 번째 추출 값이 "jappt", 그리고 세 번째 추출 값이 "jappy"이기 때문에 추천 단어는 "jappy"가 되지만 이는 잘못된 패스워드이므로 인증에 실패하게 된다. 하지만 첫 번째 자리와 다섯 번째 자리가 추출 값마다 다르므로 나머지



(위) 경우의 수가 적은 경우
(아래) 경우의 수가 많은 경우

〔그림 11〕 추천 단어로 인증에 실패한 경우

단어("happy", "jappt", "happt")를 대입할 경우 정확한 패스워드를 유추할 수 있다.

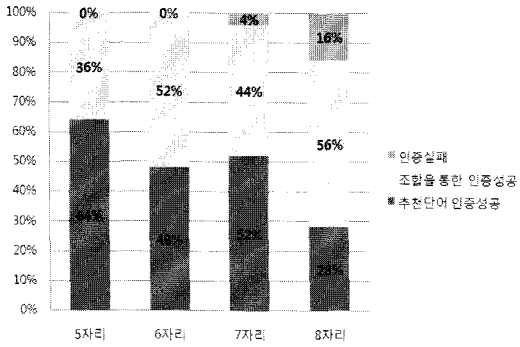
하지만 모든 경우가 이렇게 해결되지는 않는데, [그림 11-(아래)]도 추천 단어를 이용하여 패스워드 인증에 실패한 경우이지만 유추할 수 있는 모든 경우의 수를 계산해보면 $2^7 \times 3 = 384$ 로 매우 많다. 단, 이러한 경우 휴리스틱 분석을 이용한다면 추천 단어인 "softwwre"로부터 "software"가 패스워드일 것으로 추측할 수 있다.

3.3 구현 결과

[그림 12]와 같이 실제 사용자들이 가장 많이 사용하는 패스워드의 길이는 5자리~8자리이기 때문에, 테스트에 사용한 패스워드 역시 5자리~8자리로 정했으며 의미가 있는 영어단어와 영어자판으로 한글을 입력한 단어와 숫자의 조합으로 각각 25개씩, 모두 100개의 패스워드를 무작위로 선택하였고, 각각의 패스워드에 대해

Pass Length	Amount	Frequency
6	31516	26.99%
8	28105	24.07%
7	24790	21.23%
9	8782	7.52%
5	8026	6.87%
4	6225	5.33%
10	5913	5.06%
3	1194	1.02%
11	1112	0.95%
12	374	0.32%

〔그림 12〕 사용자들이 사용하는 패스워드 길이



〔그림 13〕 자릿수 별 성공률

3번씩 입력된 좌표값으로부터 키 값을 유추하였다.

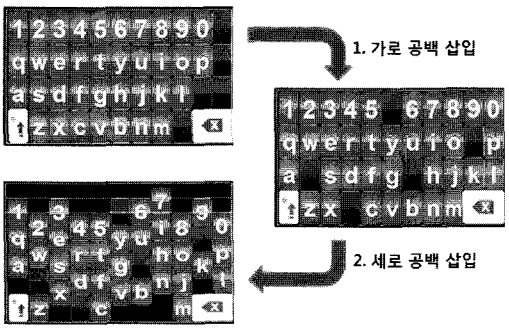
분석 결과, [그림 13]과 같이 각 자릿수별로 추천단어로 인증에 성공한 횟수는 최소 7번(28%, 8자리의 경우)에서 최대 16번(64%, 5자리의 경우)이며, 경우의 수를 대입하여 인증에 성공한 횟수는 최소 9번(36%, 5자리의 경우)에서 최대 14번(56%, 8자리의 경우)으로 인증에 성공할 확률은 전체 평균 95%로 나왔다. 자릿수를 무시하고 전체의 경우로 봤을 때, 추천단어를 받아 인증에 성공한 경우는 48개(48%)이고, 표본들의 각 경우의 수를 대입하여 인증에 성공한 경우는 47개(47%)이다. 두 방법이 모두 실패할 경우는 5개(5%)로 나왔다. 이와 같이 터치 좌표 3회 노출에 따른 패스워드 유출 확률이 95%라는 것은 이미 각종 금융거래에 사용중인 보안 키패드가 안전하지 않다는 것을 뜻하며, 보다 안전한 키패드 설계가 시급함을 의미한다.

IV. 개선방안

현재 상용화된 QWERTY 보안 키패드의 문제점은 키 배열의 확률 분포가 균등하지 않기 때문이다. 따라서, 각 키의 위치 변화를 극대화하면서 사용성을 크게 훼손하지 않는다면 보다 안전한 키패드를 만들 수 있다. 본 장에서는 앞의 분석결과에서 나타난 사용자가 터치한 좌표값이 노출되었을 때 공격자가 패스워드 값을 알아낼 수 있는 현 보안 키패드의 취약점을 보완할 수 있는 새로운 형태의 몇 가지 보안 키패드를 제시하고자 한다.

4.1 물결형 키패드

물결형 키패드는 현재 사용하는 QWERTY 기반 보안 키패드 중 한 칸짜리 공백을 추가한 키패드를 기반으로 세로줄에 공백을 추가하여 보안의 강도를 올린 키패드이다. 한 칸 공백의 키패드를 생성할 때처럼 먼저 각 가로줄에 공백을 생성하여 키 사이에 무작위로 끼워 넣고 이렇게 생성된 키패드의 세로줄에 키의 반 칸짜리 공백을 추가하여 키패드를 생성한다 ([그림 14] 참조). 이와 같은 순서로 생성된 물결형 키패드는 위의 취약점 분석 방법과 같은 방법으로 좌표값과 알파벳을 매칭 하면 세로까지 공백이 추가되었기 때문에 스캔해야 할 범위가 세로까지 확장되어 취약점을 보완할 수 있게 된다.



〔그림 14〕 물결형 키패드 생성 알고리즘

4.2 클론 키패드

클론 키패드는 공백 또는 마크를 이용한 기존의 QWERTY 키패드에서 4 개의 키패드 열 가운데 한 열을 무작위로 복사한 후 추가로 생성하는 방식이다 ([그림 15] 참조). 예를 들어 [그림 15]의 경우 두 번째 키패

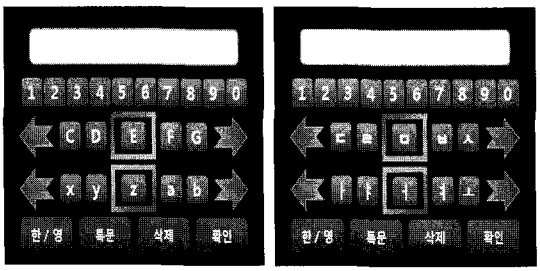
〔그림 15〕 클론 키패드

드 열을 복사하여 추가하였으며 복사된 키패드 열이나 원본 키패드 열 모두 터치할 수 있는 키로 동작한다. 이 때 사용자에게 같은 키패드 열임을 알리기 위해 같은 배경을 이용할 수도 있다.

이러한 방식은 같은 키를 입력하더라도 다른 좌표값으로 구성되기 때문에 패스워드 추측을 어렵게 할 수 있다.

4.3 터치&슬라이드 키패드

터치&슬라이드 키패드는 기존의 QWERTY 키패드가 아닌 새로운 형태의 키패드이다 ([그림 16] 참조). 키패드에 있는 화살표 부분을 터치하여 좌우로 하나의 문자씩 넘어가거나 화면을 슬라이드하여 원하는 문자를 찾아 이동한 후 가운데 사각형 부분을 클릭하면 사각형 안에 있는 문자가 입력된다. 한글과 영문 키패드를 모두 지원하며 두 줄의 입력창을 통해 영문은 [그림 16]의 왼쪽과 같이 대문자와 소문자를 따로 표시하고, 한글은 [그림 16]의 오른쪽과 같이 자음과 모음을 따로 표시하여 입력의 편의성을 높일 수 있다.



〔그림 16〕 터치 & 슬라이드 키패드

V. 결 론

스마트폰과 스마트기기를 이용한 금융거래가 급증함에 따라 스마트폰 보안이 사회적 이슈가 되고 있다. 특히 사용자의 입력정보를 보호하기 위해 각 금융사는 보안 키패드를 도입하였으나, 안전성 분석 결과 터치좌표가 노출될 경우 매우 높은 확률 즉, 5~6자릿수는 100% 노출되었으며, 7자릿수는 96%의 성공률을 보였으며, 8자릿수는 84%의 높은 성공률로 중요정보가 노출되는 것으로 나타났다. 본 논문에서 이러한 취약점을 보완하기 위해 물결형 키패드, 클론 키패드, 그리고 터치&슬라이드 키패드 등 세 가지의 방식 새로운 키패드를 제안하였다. 앞으로도 꾸준히 스마트폰을 이용한 금융거래 사용자는 증가할 것으로 예상되기 때문에 각 금융사들은 취약점이 발견된 기존의 키패드가 아닌 위에서 제안한 세 가지 방식과 같은 취약점을 개선한 보안 키패드의 도입을 시급히 추진해야 할 것이다.

참고문헌

[1] 서울경제, "스마트폰 이용자 1,000만명 시대", Mar 2011

[2] 방송통신위원회,"방통위, 2011년 상반기,'제3차'스마트폰이용실태조사결과발표,Jul 2011.

[3] 한국일보, "스마트뱅킹 500만 스마트금융 시대'활짝'", Jun 2011.

[4] 한국경제TV, "스마트폰 금융거래 안전한가?", Apr 2011.

[5] 보안뉴스, "스마트폰 백신도 무용지물인 악성코드 존재는 과연 무엇", Jul 2011.

[6] SBS CNBC,"'모바일 뱅킹'도 해커 먹잇감… "와이파이·탈옥 조심하세요"" Jun 2011.

[7] ITDAILY, "스마트폰 보안 간과 시 '해커들 먹잇감 된다'", Jul 2011.

[8] mk 뉴스, "스마트폰 이용자 51% '보안교육 받은적 없어, Jul 2011.

[9] ZDNET KOREA, "스마트폰 백신, '앱 보안 검증' 유명무실", Jun 2011

[10] Newstomato, "보안위한 백신 어플이 오히려 스마트폰 보안 위협?", Jul 2011.

[11] 소프트시큐리티, "모바일보안 제품소개", 특허 4020110041630, Jun 2011.

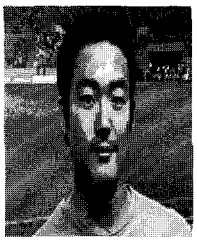
〈著者紹介〉

이 동 현 (DongHyun Lee)

2004년 3월~현재 : 강남대학교 컴퓨터미디어정보공학과 재학중
전공 : 컴퓨터공학
복수전공 : 미디어정보공학
관심분야 : 정보보호, 역공학, 안드로이드, 데이터베이스

배 동 환 (DongHwan Bae)

2007년 3월~현재 : 강남대학교 컴퓨터미디어정보공학과 재학중
전공 : 컴퓨터공학
관심분야 : 정보보호, 데이터베이스, 안드로이드



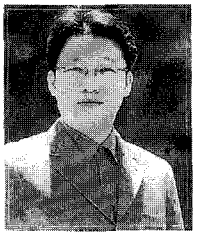
유 승 록 (SeungLok Yoo)

2005년 3월~현재 : 강남대학교 컴퓨터미디어정보공학과 재학중
전공 : 컴퓨터공학
복수전공 : 미디어정보공학
관심분야 : 정보보호, 안드로이드

채 진 영 (JinYoung Chae)

2007년 3월~현재 : 강남대학교 컴퓨터미디어정보공학과 재학중
전공 : 컴퓨터공학
관심분야 : 정보보호, 안드로이드

이 윤 호 (Yunho Lee)
정회원
1987년 3월~2008년 2월 : 성균관대학교 정보공학과(학사, 석사, 박사)
1993년 3월~2000년 4월 : 한국통신(KT)연구개발본부전임연구원
2000년 5월~2005년 1월 : KBS인터넷(주) 기술지원팀장
2008년 3월~2011년 8월 : 성균관대학교 박사 후 연구원, 연구교수
2011년 9월~현재 : 광주대학교 사이버보안경찰학과 교수



양 형 규 (HyungGyu Yang)

1995년 2월 : 성균관대학교 정보공학과 공학박사
1995년 5월~현재 : 강남대학교 컴퓨터미디어공학부 교수
관심분야 : 암호이론, 디지털 워터마킹, 정보이론, 정보보호