어깨 넘어 훔쳐보기에 저항성을 가진 가상금융키패드의 구현

저자
(Authors)
김현진, 서화정, 이연철, 박태환, 김호원
Hyun-Jin Kim, Hwa-jeong Seo, Yeon-Chul Lee, Tae-Hwan Park, Ho-won Kim

출처
(Source)
정보보호학회지 23(6), 2013.12, 21-29 (9 pages)
REVIEW OF KIISC 23(6), 2013.12, 21-29 (9 pages)

발행처
(Publisher)
한국정보보호학회
Korea Institute Of Information Security And Cryptology

URL
http://www.dbpia.co.kr/Article/NODE02334138

APA Style
김현진, 서화정, 이연철, 박태환, 김호원 (2013). 어깨 넘어 훔쳐보기에 저항성을 가진 가상금융키패드의 구현. 정보보호학회지, 23(6), 21-29.

정 보 보 호 학 회 지
제23권 제6호, 2013. 12

어께 넘어 훔쳐보기에 저항성을 가진 가상금융키패드의 구현

김 현 진*, 서 화 정**, 이 연 철***, 박 태 환****, 김 호 원*****

요 약

새로운 금융 서비스의 등장은 사용자의 부주의에 따라 악의적인 공격자에게 소중한 개인정보가 노출 될 수 있는 위험성을 가지고 있다. 현재의 금융어플리케이션의 보안은 눈에 보이지 않는 여러 암호 기술을 통해 통신상의 안전한 보안 매커니즘을 구축하였으나 사회공학적인 공격기법에 취약한 면을 가지고 있다. 특히 현재 금융어플리케이션의 키패드는 오타방지를 위해서 입력하는 끝 글자를 보여주고 있으나 이 점은 공공장소에서 사용 시 외부자의 훔쳐보기로 인해 노출 될 수 있다. 본 논문에서 제안하는 기법은 기존의 가상 키패드 입력 방법에서 마지막 글자를 보여주는 대신 각 키가 색을 가지고 끝 글자는 키의 색 정보로 대치하였다. 이로써 공격자가 입력란만을 보면 끝 글자를 통해 전체적인 비밀번호를 유출할 수 있는 수단이 사라져 기존의 훔쳐보는 공격으로부터 안전하다. 해당 기법을 실제 안드로이드로 구현 했을 시 기존의 기법에 비해 68% 향상된 보안성을 제공하면서도 기존의 기법과 유사한 정확도와 신속성을 지닌다. 이는 기존의 스마트폰 상에서의 보안 키패드를 안전하게 대체할 수 있는 기술로서 그 효용성이 높다고 할 수 있다.

Ⅰ. 서 론

무선 인터넷이 가능한 스마트폰과 스마트폰에 설치되는 금융어플리케이션으로 스마트폰에 공인인증서를 저장하고 보안카드만 휴대하면 사용자는 언제 어느 장소에서나 온라인 금융서비스에 접속하여 간단한 은행업무를 보는 것이 가능해졌다. 2013년 1/4분기 기준으로 모바일 뱅킹 서비스의 하루 평균 이용률은 5,285 만건으로써 전 분기 대비 10.8%의 성장률을 보이고 있다. 또한 사용 연령대는 20~30대 비중에 75.2%에서 64.7%로 낮아짐에 따라 점차 전 연령대가 자유롭게 모바일 뱅킹을 사용하고 있음을 알 수 있다 [1].

현재 모바일 뱅킹 어플리케이션에서는 다양한 솔루션을 통해서 사용자의 안전한 금융거래를 지원하고 있는데 크게 보안카드, 공인증서 그리고 스마트폰용 가상키패드 솔루션으로 나누어 볼 수 있다. 보안카드는 은행에서 발급해주는 비밀 정보들을 적어놓은 카드로서 불규칙적인 난수 규칙에 의해 생성되었기 때문에 공격자가 해당 적보를 유추하는 것은 불가능 하다. 공인인증서의 경우에는 사용자가 신분을 법적으로 증명하여 공인된 기관으로부터 발급받은 인증서를 파일형태로 저장한 것으로 온라인에서도 신분을 증명하는 용도로 쓰인다. 키패드 보안 솔루션의 경우는 가상 키패드를 이용해 중요 입력정보를 암호화 하여 정보가 유출 또는 변조되지 않도록 지원하는 역할을 한다.

여러 번의 난수화 된 암호화 자신만의 암호 그리고 키패드 보안 솔루션으로 인해 소프트웨어적인 안전망을 갖추었으나 모든 금융회사가 사용 중인 가상키패드의 경우 화면상에 입력된 비밀번호의 마지막 글자를 보여주는 방법을 통해 입력 값에 대한 피드백을 줌으로서 어께 넘어 훔쳐보기 공격에 취약하다. 이렇게 위험한 방법으로 피드백을 주는 이유는 터치 키패드의 입력 오타율이 물리 키패드에 비해 높아 사용자에게 피드백을 주어야 하기 때문이다. 현재 스마트폰 모바일 뱅킹은 사용

* 부산대학교 전자전기컴퓨터공학과 정보보호 및 IoT 연구소 (moonshinek@naver.com)
** 부산대학교 전자전기컴퓨터공학과 정보보호 및 IoT 연구소 (hwajeong84@gmail.com)
*** 부산대학교 전자전기컴퓨터공학과 정보보호 및 IoT 연구소 (lycshotgunl@gmail.com)
**** 부산대학교 전자전기컴퓨터공학과 정보보호 및 IoT 연구소 (pth5804@gmail.com)
***** 부산대학교 전자전기컴퓨터공학과 정보보호 및 IoT 연구소 (howonkim@gmail.com)

이 간단하고 이용자의 위치에 제약을 받지 않기 때문에 공공장소에서도 많은 이용이 되고 있는데 이점 때문에 주위의 사람이 우연히 사용자의 스마트폰을 어깨 넘어 보게 된다면 비밀번호가 유출 될 수 있고 유출된 정보로 인해 피해를 입을 수 있다.

본 논문에서는 주위의 사람에 의해 입력과정이 보여지더라도 노출될 위험이 없는 어께 넘어 훔쳐보기에 강인한 보안 키패드를 제안한다. 해당 제안 기법은 암호입력의 정확성을 위해 입력에 대한 피드백을 사용자에게 보여주면서도 입력한 글자를 공격자에게 노출시키지 않는 기술이다. 따라서 해당 기법을 통해 기존의 보안 키패드의 기능을 모두 만족하면서 어깨 넘어 훔쳐보기 공격에 보다 안전한 키패드를 사용하는 것이 가능하다.

Ⅱ. 관련 연구

여기서는 금융 모바일 어플리케이션에 관련된 보안 및 취약점에 관련된 사항들을 살펴보고자 한다.

2.1. 스마트폰의 금융 정보 보안

금융 보안 연구원의 스마트폰 보안 가이드에 따르면 금융 정보를 보호하기 위해서 중요 입력정보와 입력정보의 전달 구간 내 저장 및 노출 금지와 중요 입력 지점에 대한 보호기술이 적용되어야 한다고 명시되어 있다[2]. 이는 네트워크의 전송구간 상 메시지 탈취와 메모리 분석 그리고 키 로깅을 통한 물리적인 정보 획득 공격을 사용자가 방지 할 수 있어야 함을 의미한다. 모든 금융사에서 모바일용 어플리케이션 개발 시 위 요구조건을 만족해서 설계 하고 있다.

각 요구 조건에 대해 살펴보면 입력정보와 입력정보의 전달 구간 내 저장 및 노출금지의 경우 가상키패드를 통해 입력된 정보는 단순히 입력 그대로의 문자가 아닌 이미지화 된 값으로 표시되며 입력 값 역시 암호화 되어 있기 때문에 메모리 해킹으로부터 보호 한다. 또한 자체 구간 암호화를 통한 네트워크 위, 변조에 대한 대응을 하고 암호화된 입력 값은 서버에서만 복호화 되어 E2E를 지원한다. 중요 입력 지점에 대한 보호 기술은 키패드 값은 사용 시점에서 랜덤으로 생성되기 때문에 입력에 대한 좌표 값이 노출되더라도 실제 값이 유출되는 것은 불가능하다. 즉 같은 좌표 값이라도 매번 다른 숫자 또는 문자와 매칭 된다.

2.2. 사회 공학적 기법

사회 공학적 기법에 의한 해킹이란 소프트웨어나 하드웨어 시스템을 기반으로 공격하는 방식이 아닌 사람의 심리상태나 습관에서 발생하는 취약점을 공격하여 원하는 정보를 얻는 공격기법이다[3]. 대표적인 사회 공학적 기법은 피싱, 파싱 그리고 어깨 넘어 훔쳐보기 공격이 있다[4]. 어께 넘어 훔쳐보기 공격은 사용자 주변에서 육안이나, 카메라, 비디오카메라 등을 이용하여 사용자의 조작을 훔쳐봄으로서 중요 정보를 얻어내는 공격 기법이다.

국내에서도 ATM 기기에서 어깨 넘어 훔쳐보기 공격이 시도되어 범죄 화된 사례가 여럿 존재한다. 이것은 비밀번호 입력기반의 시스템의 사용자 인증이 취약 할 수 있음을 말해준다. 스마트폰 금융 어플리케이션은 ATM 보다 많은 단계의 비밀번호를 입력함으로서 보안성을 강화했지만 여전히 비밀번호에 의존하여 개인인증을 하는 한계를 가진다. 실제적으로 금융 모바일 어플리케이션에서 요구되는 비밀번호는 계좌 비밀번호 네 자리와 열자리 안팎의 공인인증서 비밀번호 그리고 난수가 입력된 보안카드번호 입력이 있다. 이 중에서 대체적으로 짧고 사용자의 기억력에 의존하는 계좌 비밀번호와 공인인증서 비밀번호만 어께 넘어 훔쳐보기로 공격한다면 보안카드번호는 물리적인 방법을 통해서 탈취가 가능하다.

2.3. 어께 넘어 공격에 대한 기법

어께 넘어 공격이 대응하는 다양한 방어 기법이 연구되었다. ‘Cognitive trapdoor game’기법에서는 기존의 비밀번호 입력 방식을 대체하기 위해 새로운 방식을 제안 하였는데 초기 입력 화면이 공격자에게 노출된다고 하더라도 실제 입력하는 숫자가 노출되지 않는 방식을 취하기 때문에 어깨 넘어 공격으로부터 안전하다[5]. 하지만 확률을 기반으로 동작하기 때문에 실용적인 구현은 힘들다는 단점이 존재한다.

그래픽 기반 패스워드도 어깨 넘어 공격을 방지하기 위해 제안되었다. ‘CHC(Convex Hull Click)’ 기법은 이미지 기반 입력 화면에 초기 설정된 이미지들을 사용

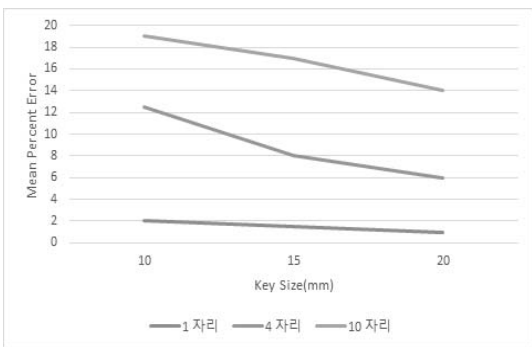
하여 Convex Hull을 만들고 이미지들이 연결된 내부 도형을 선택함으로서 Challenge를 발생시킨다. 이를 통해 안전하게 키를 선택하는 것이 가능 하지만 초기에 3개의 이미지를 선택하고 기억하고 있어야 한다[6]. 'EyePassword'에서는 시선 추적을 통해 버튼을 입력하도록 하였다[7]. 빨간 포인트를 키패드 각각에 추가하여 시선이 키패드 버튼 중심에 위치 할 수 있도록 하여 보다 정확성을 증가시켰으나 기법의 특수성으로 인한 비용증가로 인해 실제 활용에는 적합지 않다.

2.4. 가상 키패드

스마트폰에서의 풀 터치 키패드는 사이즈와 무게를 줄일 수 있다는 장점이 있지만 손가락이 키에 비해 크기 때문에 입력 속도가 느리고, 오타율이 높은 단점을 가진다[8]. 또한 물리 키보드는 키가 오목한 면으로 구분되어 촉각적인 피드백을 통해 오타를 감지 할 수 있지만 터치 키보드는 피드백이 없어 높은 오타율이 발생한다[9]. 오류율을 줄이기 위해 키에 대한 접촉 면적이 다른 키에 비해 높다는 예측 적 접근과 같은 기술 등이 사용되고 있으나 원천적 차단은 불가능 하다.

터치 키패드에서는 키가 커질수록 오류율이 감소하고 입력 길이가 길어질수록 오류율이 감소한다[10].

그래프를 참조하여 실제 금융어플리케이션의 가상키패드에서의 오류율을 추측하면 계좌비밀번호로 사용하는 4자리 비밀번호 기준으로 각 키 사이즈가 갤럭시 S2 기준 가로 30mm * 세로 20mm라고 할 때 오타 입력 확률은 2~4% 정도 이다. 그에 반해 공인인증서에 입력하는 일반적인 비밀번호 길이를 10자리라고 가정 한다면 여기서 사용하는 쿼티 키패드에서는 키패드의 크기가 20mm*10mm의 크기이므로 오타율은 14~16% 다소 높다는 것을 확인할 수 있다.



〔그림 1〕 일반적인 키패드 상에서의 오류율[6]

따라서 스마트폰의 가상 키패드에서는 사용자가 자신의 오타를 인식하고 이를 알맞게 수정하는 피드백 작업을 효율적으로 수행하기 위한 방법이 필요하다. 터치 키패드에서는 높은 오타율에 대한 피드백을 주기 위해 암호 입력 시 입력한 마지막 키값을 화면에 그대로 표시하고 이전 입력 값은 `*'를 통해서 은닉 하는 방법을 사용하고 있다.

위 입력 피드백은 터치 키패드의 높은 입력 오류율의 해결에는 효과적이지만 공공장소에서 악의적인 공격자의 어깨너머 공격에 매우 취약한 단점을 가진다. 따라서 비밀번호를 주위의 악의적인 공격자에게 숨기면서 사용자에게는 적절한 피드백을 줄 수 있는 방안에 대한 연구가 필요하다.

위 문제를 해결하려면 오타율과 그에 대한 피드백에 대한 시나리오를 쿼티 키패드를 통해 확인 할 필요가 있다. 만약 사용자가 키 `j'를 눌렀을 경우에 오타를 누를 가능성이 있는 주변의 키들은 i, h, k, n, m이다. 따라서 사용자가 누르고자 했던 j와 주변키들 간에 차별화된 피드백을 사용자에게 비밀리에 전달할 수 있다면 사용자는 오타를 인식할 수 있을 뿐 아니라 비밀번호를 주위의 공격자에게 노출하지 않게 될 것이다.

2.5. Four Color Theorem

본 논문에서 제안 할 기법은 색을 통해 키패드로 입력된 정보를 확인하는 방식이다. 따라서 해당 키패드에 적절한 색상이 무작위로 선택 되어야 정형화된 키패드로 인한 공격을 방지 할 수 있다. 그러나 너무나 많은 색을 사용하게 되면 사용자에게 혼란을 가져다 줄 수 있다. 따라서 각 키패드의 구분을 확연하게 하면서도 최소한의 색을 사용해야 한다. 이를 위해 본 논문에서는 Four Color Theorem[11] 을 통해서 결정하였다. 해당 이론은 네 가지 색 만으로도 지구상의 모든 국가를 같은 색이 연속되지 않게 칠 할 수 있다는 것으로서 최소한의 색상을 통해 분별력 있는 지도 색을 결정 할 수 있다.

Ⅲ. 제안 기법 및 알고리즘

여기서는 위에서 제기된 어께 넘어 훔쳐보기 공격에 강인한 보안 키패드를 제안한다.

3.1. 제안 기법

본 논문에서는 어깨너머 공격에 강인한 보안 키패드를 제안한다. 위에서 제시한 기법들 기존의 실제 문자를 화면에 띄워주는 방식과는 달리 색 정보를 화면에 띄워줌으로써 공격자의 어깨너머 공격을 효과적으로 방어한다. 이는 키패드의 각 글자쇠 버튼에 색을 입히고 사용자가 해당 글자쇠를 입력하는 경우 비밀번호 입력란에 '*'기호에 색상이 입혀져서 표시되도록 하는 방식이다. 예를 들어 키 s의 경우 주위에 w, e, a, d, z, x 키가 인접하여 나타날 수 있을 것이다. 그러면 위 키들과 s 키가 서로 다른 색을 가지고 있다면 사용자 입장에서는 확연한 구분 이 될 것이고 피드백의 경우 입력확인 박스 란의 '*'에 해당 글자쇠에 입혀져 있던 색이 '*'에 입혀져 있기 때문에 입력에 대한 피드백 역시 가능하다. 글자쇠와 인접한 다른 글자쇠는 Four Color Theorem을 적용하여 해당키의 색을 제외한 3가지 색으로 구분될 것이다. 이정도 색의 경우는 복잡하지 않는 범위 내에서 충분히 인지 가능한 수 이다.

공격자 입장에서는 키보드에 무작위로 입혀진 색상 정보를 알 수 없거니와 혹여 해당 정보를 얻더라도 동일한 색상을 가지는 경우의 수가 중복적으로 존재하기 때문에 다시 해당 정보를 통해 전수조사를 해야 하는 보안성을 가진다. 따라서 기존의 보안키패드에 비해 보안성이 한층 높아졌다고 할 수 있다.

3.2. 보안 숫자 키패드 생성 알고리즘

보안 숫자 키패드의 생성을 위해서는 알고리즘 1과 같은 과정을 통해 생성된다. 먼저 step 1에서는 보안 키패드의 배치를 무작위로 나타내기 위해 알고리즘 2의 난수 생성기 기반 보안 숫자 키패드를 생성한다. step 2에서는 하나의 버튼에 대해 색상을 정의하게 되고 나머지 색상들은 해당 정의에 따라 차례대로 이루어지게 된다. step 3~5에서는 각각의 버튼에 임의로 배치된 키패드 C를 인가시킴으로써 보안 숫자 키패드가 완성되게 된다.

Step 1에서는 난수 생성기의 seed값에 해당하는 nonce값을 입력받아 난수 생성기를 초기화시키는 작업을 수행한다. Step 4에서는 난수생성기로부터 난수 값을 생성하며 Step 5에서 해당 난수를 10으로 모듈러 연산하여 키패드에 적합한 난수 값을 계산한다. Step 6에서는 숫자의 배치 중 중복된 값이 없는 경우 해당 난수 값을 배열에 인가하고 반복문을 나오게 된다. 해당 과정은 키패드의 모든 배치가 완료될 때 까지 수행된다.

〔표 1〕 알고리즘 2. 난수 생성기를 이용하여 숫자 키패드에 배치의 순서 생성

입력: None 출력: 보안 숫자 키패드(K[n])	
1.	알고리즘 2를 이용하여 키패드 무작위 배치(C) 생성
2.	1행 1열의 버튼 색상을 선택하고 나머지는 규칙적으로 색상 생성
3.	For t=0 to C.size do
4.	버튼에 C[t]값 인가
5.	End For

〔표 2〕 알고리즘 2. 난수 생성기를 이용하여 숫자 키패드에 배치의 순서 생성

입력: Nonce값 출력: 숫자 키패드의 배치 정보(C[10]) 생성, 여기서 C는 배열이며 배열의 정수값 0~9은 각각 무작위 숫자 배치정보를 저장함	
1	난수 생성기에 Nonce값을 입력
2	For t=0 to 9 do
3	While(1)
4	난수 값(R) 생성
5	R = R % 10
6	If(배열 C에서 중복된 R값을 가지지 않는 경우)
7	C[t] = R
8	Break
9	End If
10	End While
11	End For
12	Return C

3.3. 보안 쿼티 키패드 생성 알고리즘

알고리즘 3-5에서는 보안 쿼티 키패드 생성 알고리즘에 대해 제시한다. Step 1에서는 알고리즘 4를 이용하여 키패드의 연결 정보를 생성하도록 한다. 이는 각각의 키들이 어떤 키와 인접하여 있는지를 확인하여 4색 이론을 보다 적합하게 적용하기 위한 하나의 방안이다. Step 3에서는 해당 키가 색상이 없는 경우 난수로 색상 정보리스트를 생성하도록 한다. 해당 색상이 주변 노드와 동일하지 않은 경우 해당 노드에 색상정보를 대입하게 된다. 해당 과정은 모든 노드를 색칠할 때까지 수행된다.

〔표 3〕 알고리즘 3. 보안 쿼티 키패드 생성, (n은 전체 키패드의 문자 개수)

입력: 키패드 배치 정보(P[n]) 출력: 보안 쿼티 키패드(K[n])	
1	알고리즘 4를 이용하여 키패드의 연결 정보(A) 생성
2	For t=0 to A.size do
3	While(A[t] has no color)
4	알고리즘 5을 통해 난수로 색상 정보(C) 생성
5	if(주변 노드와 동일한 색이 없는 경우)
6	해당 노드(K)에 색상 정보(C) 대입
7	break
8	End While
9	End For
10	Return K

알고리즘 4에서는 키패드의 배치정보를 통해 연결정보를 알아내는 과정을 수행한다. Step 3에서는 해당 노드와 인접노드가 있는 경우 해당 노드를 연결 정보 벡터에 넣어주게 된다. 이를 통해 해당 벡터는 주변 인접 노드와의 연결 정보를 저장하고 있게 된다.

〔표 4〕 알고리즘 4. 키패드 배치 정보 생성, (n은 전체 키패드의 문자 개수)

입력: 키패드 배치 정보(P[n]) 출력: 키패드 연결 정보(A[n]는 Vector class 혹은 Linked list로써 주변 키패드와의 연결정보를 저장)	
1	Initialize A
2	For t=0 to n do
3	If (P[t] has adjacent node)
4	A[t].push(adjacent node)
5	End For
6	Return A

〔표 5〕 알고리즘 5. 난수 생성기를 이용하여 키패드에 사용될 색상의 순서 생성

입력: Nonce값 출력: 색상의 순서 정보(C[4]) 생성, 여기서 C는 배열이며 배열의 정수값 0, 1, 2, 그리고 3은 빨강, 노랑, 파랑 그리고 녹색을 각각 의미함	
1	난수 생성기에 Nonce값을 입력
2	For t=0 to 3 do
3	While(1)
4	난수값(R) 생성
5	R = R % 4
6	If(배열 C에서 중복된 R값을 가지지 않는 경우)
7	C[t] = R
8	Break
9	End While
10	End For
11	Return C

알고리즘 5에서는 난수 생성기를 통해 색상을 무작위로 배열한다. 먼저 Step 1에서는 난수생성기를 초기화하기 위한 nonce값을 넣어준다. Step 4에서는 난수생성기를 통해 난수를 생성한다. Step 5에서는 난수를 4로 모듈러 연산하여 4가지의 색상을 차례로 나타낸다. Step 6에서는 해당 값이 색상 순서 정보에서 중복되지 않은 경우 배열에 넣어주게 된다.

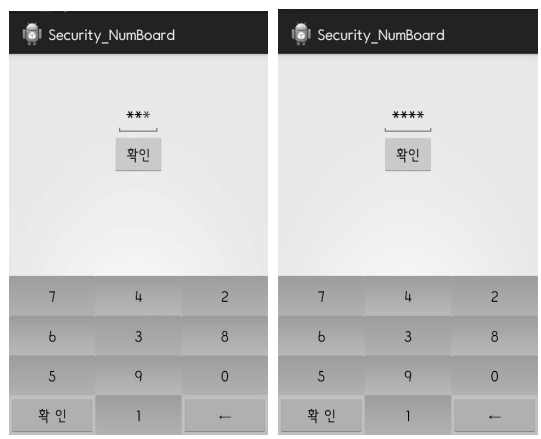
Ⅳ. 구현 및 성능 평가

이 장에서는 안드로이드 스마트폰으로 구현한 결과에 대해 설명하고 실제 실험을 통해서 성능에 대해 평가한 내용이다.

4.1. 숫자 키패드 구현 결과

숫자 키패드는 키 간 간격이 넓어서 오타의 확률이 적고, 숫자의 배열이 무작위로 되어 있기 때문에 공격자가 키패드의 배치와 색 매핑 정보를 파악하는 것이 불가능하다. 따라서 쿼티 키패드에서 가능했던 색 정보 유추 공격에도 숫자 키패드는 안전하다. 그렇기에 키패드의 키를 난수로 생성한 무작위 색 배치를 적용하지 않고 세 개의 색중 두 개의 색을 임의로 선택하여 키패드를 생성한다. 이 경우 키패드의 색을 교대로 배치하여 주위의 키패드와 중복되지 않도록 배치하였다.

[그림 2]에서는 왼쪽 화면은 빨간색 숫자 키패드를 마지막에 누른 경우이며 오른쪽 화면은 파란색 숫자 키패드를 마지막에 누른 경우이다. 공격자는 어깨 너머 공



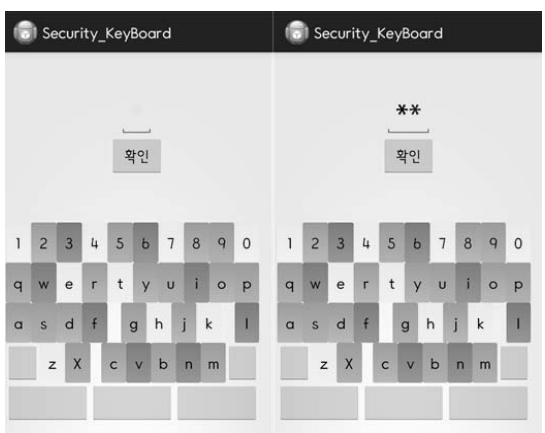
〔그림 2〕 숫자 키패드 구현 결과

격을 통해 색깔 정보를 확인할 수 있다. 하지만 색 정보와 숫자 키패드의 정보는 1대1로 매칭 되는 정보가 아니므로 공격자는 다시 해당 색 정보로 키를 확인해야 하는데 무작위로 숫자가 배열되어 있기 때문에 이러한 방법은 불가능하다.

4.2. 쿼티 키패드 구현 결과

쿼티 키패드는 각 키의 순서는 유지 한 채 위치만 좌우로 변경하는 재배열 기능을 제외하고 본래와 유사하게 키의 위치 및 크기를 구현하였다. 재배열 기능은 가상 키패드에서 입력지점에 의한 공격을 차단하기 위해 키의 배치 일부분을 좌우로 옮겨 입력지점을 파악한다고 해도 대항할 수 있게 만든 기능이다. [그림 3]은 보안 쿼티 키패드의 구현된 형태를 나타낸다. 키패드는 각각의 명확한 구별이 가능한 네 가지 색을 이용하여 상, 하, 좌, 우로 같은 색의 키가 겹치지 않게 무작위로 배치한다. 재배열로 인해 일부 키의 위치가 이중으로 겹치게 되지만 Four Colour Theorem에 따라 네 가지 이상의 색을 사용하여 겹치지 않게 키를 배치 할 수 있다. 사용한 색은 파랑, 빨강, 초록, 노랑의 네 가지 색으로 색 인지가 명확하기 때문에 혼돈을 불러올 가능성이 적다.

위의 좌측 그림은 노란색의 키인 '1' 키를 터치한 화면이다. 비밀번호 입력란이 '*'로 채워지고 '*'의 색은 노란색임을 확인 할 수 있다. 좌측에서 두 번째 그림은 파란색인 '3'키를 터치한 화면이다. 역시 화면에 '*'이 추가되어 두 개의 암호를 입력했음을 알 수 있다. 또한 두 번째 '*'키는 파란색으로 채워지지만 숫자키패드와 같이 이전의 '*'은 검은색으로 변경되기 때문에 이전의 입력한 값에 대한 정보를 드러내지 않는다.



〔그림 3〕 쿼티 키패드 구현 결과

4.3. 성능 평가

본 장에서는 보안성에 대해 테스트하기 위해 실제적 환경의 다양한 상황에서 어께 너머 공격을 실행할 경우에 비밀번호를 알아 낼 수 있는지 없는지에 대한 공격 성공률에 대해서 분석 한다. 또한 보안 키패드의 성능 분석을 위해서 키패드 상에서의 타자의 신속성 그리고 정확성을 비교 분석 한다.

4.3.1. 실험 환경

초기 사용된 타겟 보드는 네 가지 갤럭시S1,2,3,4 스마트폰 이였으나 갤럭시S1의 경우 실험결과 속도가 느리고 스크린의 크기 및 안드로이드 버전 문제로 인해서 정상적인 키 형태로 개발되지 않아 타자입력의 원활성 문제로 해당 성능 평가에서 제외되었다. 최신 스마트폰의 경우 가장 큰 화면과 해상도를 제공하는데 큰 화면크기로 인해 버튼의 크기가 커지게 되고 추후에 실험에서 나타나는 바와 같이 높은 정확도와 빠른 타자 속도를 제공하게 된다.

〔표 6〕 디바이스 상세 스팩

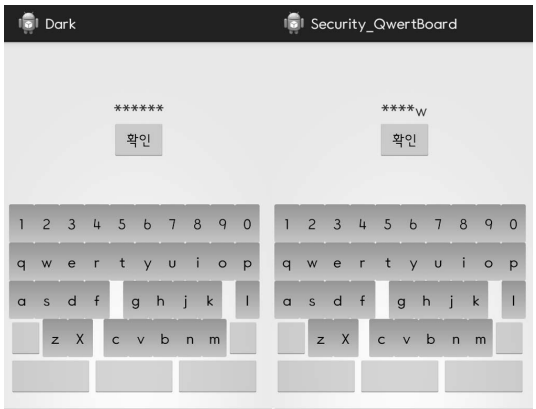
특성	갤럭시S2	갤럭시S3	갤럭시S4
해상도	480X800	720X1280	1920X1080
액정크기	4.3인치	4.8인치	5인치
버튼크기	0.5x0.8	0.6x0.75	0.6x0.85
CPU	1.2GHz 듀얼	1.4GHz쿼드	1.6GHz옥타

해당 디바이스로 4명의 참가자가 교대로 공격자와 사용자 역할을 수행하였다. 중요시 된 부분은 키와 시력 그리고 어깨 너비이다. 시력의 경우 네 명 모두 1~2m 거리에서 화면을 충분히 인식하였다.

〔표 7〕 실험자에 대한 상세 설명

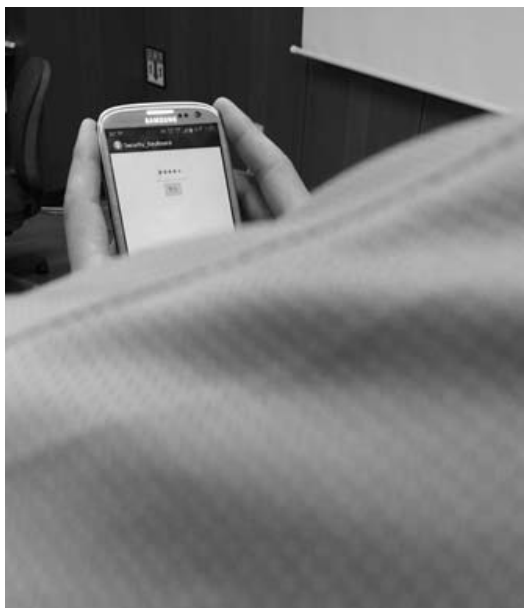
특성	실험자1	실험자2	실험자3	실험자4
시력	0.8	0.7	0.8	1.0
어깨너비	105	100	100	105
체중	74	65	66	83
키	180	175	176	177

또한 실험을 위해 2가지의 대조군으로 사용하기 위해 현재 사용 중인 끝 글자가 보이는 키패드, 일반적으로 PC환경에서 사용되는 모든 글자가 '*'로 은닉되는 키패드를 개발하였다. 세 종류의 키패드를 이용하여 정확도와 신속도 그리고 보안에 대한 실제적인 데이터를 수집 및 분석하였다.



〔그림 4〕 기존 방식의 대조 키패드

좁은 공공장소를 가정하여 사용자의 어께 바로 뒤에서 공격자는 사용자의 화면을 바라보고 입력한 문자를 외운다. 입력 문자는 사전에 약속하였고 일반적인 암호

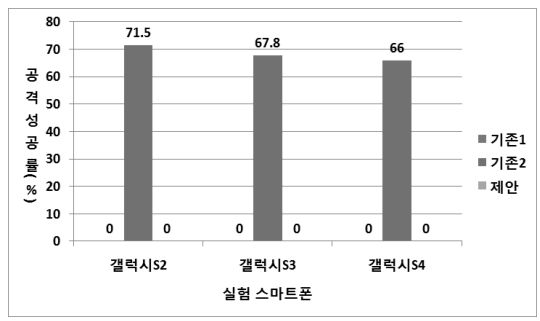


〔그림 5〕 공격자의 시선에서 바라본 사용자의 입력창

화 같이 특별한 뜻이 없는 숫자와 문자가 섞인 8~12글자 내로 선택하였다. 해당 방식으로 세 종류의 키패드에 각 각 실험하였다.

4.3.2. 결과

비밀번호를 전혀 보여 주지 않는 PC에서의 기존기법1과 제안기법은 공격자가 입력창만을 확인해서는 절대로 비밀번호를 확인할 수 없다. 그 이유는 모든 값이 '*' 형식으로 표현되어 공격자가 얻을 수 있는 정보는 오직 비밀번호의 길이밖에 없다. 그와 반대로 현재 스마트폰에서 가장 많이 사용되는 마지막 글자를 보여주는 기존기법2에 대해서는 공격 성공률의 평균을 스마트 폰에 따라 조사한 결과 갤럭시 S2에서 71.5%, 갤럭시 S3에서 67.8% 그리고 갤럭시 S4에서 66%임을 확인할 수 있었다. 여기서 흥미로운 점은 최신 장비로 갈수록 공격 성공률이 떨어진다는 점이다. 쉽게 생각해 볼 수 있는 점은 화면의 크기가 큰 최신모델이 보다 공격에 취약하다고 생각할 수 있다. 하지만 다음 장에서 설명된 바와 같이 최신 모델에서 타자 신속도가 가장 높다. 왜냐하면 스마트폰의 버튼 크기가 가장 커서 사용자가 타자입력을 원활히 할 수 있기 때문이다. 이처럼 기존기법2와 달리 제안기법은 정보 노출이 하나도 되지 않으므로 기존기법2에서 노출된 평균 공격 성공률인 68.23%의 보안 취약점이 개선되었다고 할 수 있다.



〔그림 6〕 보안 키패드에 대한 공격 성공률

Ⅴ. 결 론

기존 스마트폰에서 안전한 금융 서비스를 위해 사용되는 보안 키패드는 오탈자를 확인하기 위한 용도로 사용자에게 입력된 문자의 마지막 정보를 제공한다. 이로

인해 악의적인 공격자는 쉽게 사용자의 비밀정보를 어깨너머 공격을 통해 확인하는 것이 가능하다. 본 논문에서는 기존의 보안 키패드가 가지는 보안 취약성을 해결하기 위해 색감 정보를 통해 기존의 정보 제공 방식을 효과적으로 대체하는 새로운 개념의 보안 키패드를 제안한다. 기존의 오탈자 확인 정보가 문자 본연의 정보가 화면에 들어나는 방식이었다면 제안하는 방식은 사용자만 알 수 있는 색감정보를 통해 보안성을 제공함과 동시에 입력정확성도 확인할 수 있는 장점을 가진다. 해당 제안은 실제 구현을 통해 성능이 평가되었으며 보안성이 68.23% 향상되었으며 신속성과 정확도 또한 기존의 기법과 유사한 결과를 도출하였다.

참고문헌

[1] 한국은행, “2013년 1/4분기 국내 인터넷뱅킹서비스 이용현황”, 2013.05.15.

[2] 금융보안연구원, “금융부문 스마트폰 보안 가이드”, 2010.12

[3] 조한진. "개인정보 입력 감지를 이용한 사회 공학적 공격 대응방안." 한국콘텐츠학회논문지 12, no. 5 (2012): 32-39.

[4] 서동일. "사회 공학적 공격방법을 통한 개인정보 유출기술 및 대응방안 분석." 情報保護學會誌 16, no. 1 (2006): 40-48.

[5] Roth, Volker, Kai Richter, and Rene Freidinger. "A PIN-entry method resilient against shoulder surfing." In Proceedings of the 11th ACM conference on Computer and communications security, pp. 236-245. ACM, 2004.

[6] Wiedenbeck, Susan, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. "Design and evaluation of a shoulder-surfing resistant graphical password scheme." In Proceedings of the working conference on Advanced visual interfaces, pp. 177-184. ACM, 2006.

[7] Kumar, Manu, Tal Garfinkel, Dan Boneh, and Terry Winograd. "Reducing shoulder-surfing by using gaze-based password entry." In Proceedings of the 3rd symposium on Usable privacy and security, pp. 13-19. ACM, 2007.

[8] 양형규. "스마트폰을 위한 보안 키패드의 안전성 분석." 정보보호학회지 21, no. 7 (2011): 30-37.

[9] Kwon, Sunghyuk, Donghun Lee, and Min K. Chung. “Effect of key size and activiation area on the performance of a regional error correction method in a touch-screen QWERTY keyborad.” International Journal of Industrial Ergonomics 39.5(2009):888-893

[10] 임수민; 김형중; 김성기. Shoulder Surfing 공격을 고려한 패스워드 입력 시스템 구현 및 통계적 검증. 전자공학회논문지, 2012, 49.9: 215-224.

[11] Jungnickel, Dieter. Graphs, networks and algorithms. Vol. 5. Springer, 2008.

[12] Darer, Alexander. "A key-logger which infers keystrokes on a touch-screen keyboard from smartphone motion." (2013).

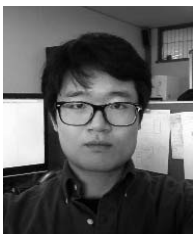
〈저 자 소 개〉

김 현 진 (Hyun-Jin Kim)
학생회원

2013년 2월 : 부산대학교 컴퓨터공학과 졸업
2013년 3월~현재 : 부산대학교 컴퓨터공학과 석사과정
<관심분야> 정보보호, 암호화 기술 구현

서 화 정 (Hwa-jeong Seo)
학생회원

2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~현재: 부산대학교 컴퓨터공학과 박사과정
<관심분야> 정보보호, 암호화 구현



이 연 철 (Yeon-Chul Lee)
학생회원

2013년 2월 : 부산대학교 컴퓨터공학과 졸업
2013년 3월~현재 : 부산대학교 컴퓨터공학과 석사과정
<관심분야> 정보보호, FPGA 암호화 구현

박 태 환 (Tae-Hwan Park)
학생회원

2013년 2월 : 부산대학교 컴퓨터공학과 졸업
2013년 3월~현재 : 부산대학교 컴퓨터공학과 석박 통합과정
<관심분야> 소리인식, 데이터마이닝, 생체정보기반보안

김 호 원 (Ho-won Kim)
종신회원

1993년 2월: 경북대학교 전자공학과 학사 졸업
1995년 2월: 포항공과대학교 전자전기공학과 석사 졸업
1999년 2월: 포항공과대학교 전자전기공학과 박사 졸업
2008년 2월: 한국전자통신연구원 정보보호연구단 선임연구원/팀장
2008년 3월~현재: 부산대학교 정보컴퓨터공학부 부교수
<관심분야> 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, embedded system 보안, IoT