Journal of The Korea Society of Computer and Information
Vol. 20, No. 1, January 2015
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2015.20.1.119

이중 표시 방법을 이용한 패스워드 기반 사용자 인증 기법

용 승 림*

Password-based user authentication scheme using a dual-display method

Seung-lim Yong*

요 약

본 논문에서는 모바일 환경에서 훔쳐보기 공격에 안전하면서도 사용자 편의성이 뛰어난 패스워드 입력 방식을 제안한다. 제안 기법은 기존의 PIN방식과 같은 숫자 패스워드 입력 방식이다. 하나의 버튼은 숫자와 색, 두가지의 정보를 이중으로 표시하도록 한다. 사용자는 한 버튼 내에 있는 색이나 숫자 정보 중 하나를 선택하여 패스워드로 입력하도록 한다. 제안한 기법에서 공격자는 사용자가 색과 숫자 어느 것을 입력한 것인지 모르기 때문에, 훔쳐보기 공격으로부터 안전할 수 있다. 또한 숫자와 색 정보의 무작위 변경을 통하여 스머지(Smudge) 공격과 패스워드 추측 공격에도 강인하도록 한다.

▸ Keywords : 패스워드, 이중표시, 사용자 인증

Abstract

In this paper, we propose a user friendly password input method for mobile devices which is secure against SSA. The proposed method is a numeric password input method such as a conventional PIN method. One of the buttons, numbers and colors, so as to display the two pieces of information to double. The user can select one of the colors or numbers within one button to type in the password. Because an attacker does not know whether the user has entered any color and number, the proposed technique is safe from the SSA. Also to be secure for smudge attacks and password guessing attacks through random changes in the number and color information.

▸ Keywords : Password, Double display, User authentication

•제1저자 : 용승림
•투고일 : 2015. 1. 3, 심사일 : 2015. 1. 15, 게재확정일 : 2015. 1. 17.
* 인하공업전문대학 컴퓨터시스템과(Dept. of Computer systems and engineering, Inha technical college)
※ 이 논문은 2013학년도 인하공업전문대학 교내연구비지원에 의하여 연구되었음.

I. 서 론

모바일 기기의 사용이 증가하고 사용자의 신상정보, 금융정보, 사진 등 중요 정보가 저장되고 있다. 이에 따라 모바일 기기에 저장된 개인정보를 안전하게 보호하기 위한 방법에 대한 요구가 증가하고 있다. 모바일 기기의 사용자 개인정보를 보호할 수 있는 방법 중 하나로 모바일 기기에 대한 사용자 인증 방법이 중요한 기술로 부각되고 있다. 이에 따라 모바일 기기의 분실 및 도난에 대비한 개인정보 보호를 위한 사용자 인증 기법에 대한 많은 연구는 진행 중에 있다.

모바일 기기에서 사용자를 인증하기 위해서는 기존의 컴퓨팅 방식과 비교할 때 제약조건이 따른다. 첫 번째는 입력방식의 제한이다. 기존 컴퓨터 환경에서는 키보드와 마우스의 입력장치가 존재하지만 대부분의 모바일 기기에서는 터치가 가능한 화면 내에 사용자의 입력이 이루어져야 한다. 또한 사용자가 패스워드로 설정할 수 있는 내용도 터치스크린 화면 크기에 종속되기 때문에 입력 내용에 대한 제한이 존재한다.

두 번째, 모바일 기기는 이동성으로 인해 기존 컴퓨팅 환경에서의 사용자 인증에서 발생되는 보안상의 문제점과 더불어 스머지 공격이나 훔쳐보기 공격과 같은 공격이 발생될 수 있다. 스머지 공격이란 터치기기 위에 남아있는 지문 자국으로 사용자의 패스워드를 유추하는 공격이다. 자주 터치되는 영역이나 패턴 형태의 그림은 흔적이 남기 때문에 패스워드를 유출할 수 있는 빌미가 된다. 따라서 고정된 자리를 누르는 패스워드 방식 또는 패턴락 방식의 사용자 인증 방식들은 스머지 공격에 매우 취약할 수 있다. 훔쳐보기 공격이란 패스워드를 통한 사용자 인증 기법에 대한 대표적인 공격 방법 중 하나이다. 공격자는 사용자의 로그인 과정을 직접 관찰하거나 카메라로 녹화하는 방식을 통하여 패스워드에 대한 정보를 얻을 수 있다[1][2]. 훔쳐보기 공격을 방지하기 위한 방법으로 관찰자가 사용자의 입력을 정확히 알기 힘들도록 방해 요소를 첨가하는 연구 등이 진행되어 왔다.

모바일 기기에서의 사용자 인증에 널리 사용되는 방법으로는 텍스트 기반의 패스워드 방식, 그래피컬 방식, 텍스트와 그래픽을 혼용한 방법, 지문인식 방법 등이 있다. 텍스트 기반의 방식인 숫자 기반의 사용자 식별 번호 방식과 그래피컬 방식은 사용자의 편의성을 고려하여 많은 연구가 진행되었으나[3],훔쳐보기 공격(Shoulder Surfing Attack (SSA))이라 하는 공격에 취약하다고 알려져 있다[4][5]. 지문인식 방법은 사용자 인증을 위해 추가적인 고가의 장비나 별도의 장치가 필요하거나 바이오정보가 노출되어도 정보를 수정하지 못하는 단점이 있다.

본 논문에서는 기존의 사용자 식별 번호 입력 방식의 사용자 인증 기법을 보완한 사용자 인증 기법에 대하여 제안한다. 제안하는 기법은 기존의 숫자 기반 식별 번호 방식에 훔쳐보기 공격으로부터 안전할 수 있도록 방해 요소를 첨가한다. 숫자 버튼에 색 정보를 추가하고 매 인증시 숫자와 색의 위치를 무작위로 재배열함으로써 기존의 사용자 식별 번호 입력 방식의 편리성은 취하나 약점은 보완하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 사용자 인증 기법에 대해 알아보고 장단점을 분석한다. 3장에서는 본 논문에서 제안하는 시스템에 대한 상세 내용을 제시하고 제안 기법의 안전성과 편리성에 대한 분석을 제시한다. 마지막으로 4장에서 결론을 도출한다.

II. 관련 연구

1. 사용자 인증 기법

모바일 기기에서의 사용자 인증에 사용되는 방법으로는 텍스트시반의 패스워드 방식, 그래픽을 활용한 그래피컬 방식과 이 둘의 조합인 텍스트와 그래피컬 방식, 그리고 사용자의 지문이나 얼굴 등을 이용하는 방식이 연구되어 왔다. 본 절에서는 별도의 장비를 필요로하는 생체정보 방식을 제외한 연구에 대하여 알아본다.

1) 텍스트 기반 패스워드

텍스트 기반 패스워드 인증은 숫자 또는 숫자와 문자의 조합을 이용하여 패스워드를 입력하는 방식이다. 텍스트 기반 인증 방식 중 사용자 식별 번호(Personal Identification Number: PIN)[PIN]은 은행 계좌나 신용카드 비밀번호, 스마트폰 해제용 번호 등 다양한 용도로 친숙하게 이용되는 사용자 인증수단이다. 기존의 단순 4자리 숫자 입력 방식은 항상 같은 입력 방법으로 인증을 수행하기 때문에 엿보기 또는 촬영 공격에 취약한 것으로 알려져 있으며 따라서 이를 보완하는 다양한 연구가 진행되어왔다.

Binary 방법[6]은 1부터 0까지 10개의 숫자들을 일반 PIN 패스와 같은 순서로 배열하되, 다섯 개는 흰색으로, 나머지는 검은 색으로 배경을 색칠하여 보여준다. 매 인증시마다 검은색과 흰색의 숫자는 무작위로 결정된다. 사용자는 현재 단계에서 입력해야 하는 번호를 직접 누르는 것이 아니라 숫자의 배경색을 아래쪽의 black 혹은 white 버튼 중 선택하

여 입력한다. 하나의 PIN 숫자를 입력하기 위해서는 네 번의 색 선택 단계가 필요하며 일반적으로 많이 쓰이는 네 자리 PIN 숫자를 입력하기 위해서는 16회 black 혹은 white 버튼을 반복 입력하여야 한다.

그림 1. Binary 방법
Fig. 1. Binary scheme

LIN 방법은 10개의 숫자들 아래에 익숙한 기호들을 무작위 배치시키고 기호에 PIN번호를 맞추는 방식으로 인증을 수행한다[7]. 즉, 사용자는 먼저 1~0의 10개 숫자들 아래에 있는 기호 들 중 PIN 번호 첫 번째 숫자(그림의 경우에는 '2') 아래에 있는 기호를 세션키로 기억한 후 'OK' 버튼을 누른다. 2단계부터 4단계는 PIN의 두 번째부터 네 번째 자리 수를 이 세션키에 맞추어 입력하게 된다. 입력시에는 'Left' 또는 'Right' 버튼을 적절히 눌러 세션키가 해당 단계의 PIN 숫자와 맞도록 이동시킨 후 'OK'를 눌러 입력하게 된다.

그림 2. LIN 방법
Fig. 2. LIN scheme

ColorPIN은 PIN의 각 자리가 1~9 중 하나의 숫자와 검정, 빨강, 흰색 중 하나의 색깔의 순서쌍으로 구성되도록 PIN을 새로 정의하였다[8]. 예를 들어 PIN이 '1(검정), 2(빨강), 3(흰색), 4(검정)'와 같을 경우, 사용자는 자신의 첫 번째 PIN 숫자인 1의 아래쪽에 무작위로 주어진 세 글자들 중 자신의 첫 번째 PIN 색깔인 검정으로 칠해진 'Q'를 확인하여 이를 키패드 상에 입력하면 된다. PIN 패드 상의 글자는 9개의 서로 다른 글자가 3군데의 숫자 패드 밑에 나오도록 설계되었다.

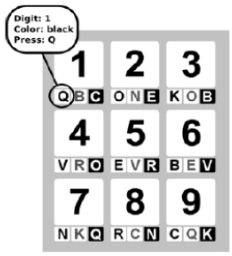

그림 3. ColorPIN 방법
Fig. 3. ColorPIN scheme

2) 그래피컬 패스워드

그래피컬 패스워드는 사용자가 시스템에서 제공하는 이미지나 그래픽을 이용하여 패스워드를 생성하고 인증하는 기법이다[9]. 그래피컬 패스워드 기법은 텍스트 기반 인증에서의 단점을 보완하며 텍스트 기반 기법을 대체할 수 있는 인증 기법으로 빠른 발전을 보여 왔다.

passfaces[10]은 숫자나 문자가 아닌 사람의 얼굴 이미지를 이용하여 패스워드를 입력하는 방법이다. 이 기법에서는 사용자 인증에 필요한 사람 얼굴을 데이터베이스에 저장하고 저장된 사람 얼굴 이미지 중에서 4개의 사람 얼굴을 이용하여 패스워드를 설정한다.

그림 4. passfaces 방법
Fig. 4. passfaces scheme

DAS(Draw-A-Secret) 시스템은 그림 5와 같으며 사용자는 구역이 나눠진 화면에 패턴을 그린다. 패턴이 그려지면서 지나가는 구역의 순서가 기억되고, 사용자는 패스워드를 만들 때 그렸던 패턴과 어느 구역에 어떤 순서로 패턴을 그려야 하는지를 기억하였다가 재현함으로써 인증을 수행한다[11].

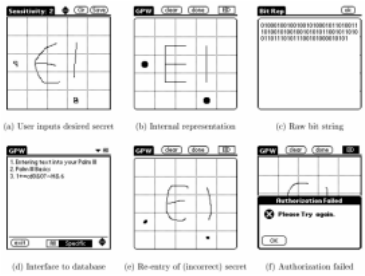

그림 5. Draw-A-Secret 방법
Fig. 5. Draw-A-Secret scheme

3) 그래픽과 텍스트 혼용 패스워드

그래픽 방식과 텍스트 방식을 혼합하여 사용하는 하이브리드 방식으로는 S3PAS(Scalable Shoulder-surfing Resistant Textual Graphical Password Authentication System)이 있다[12].

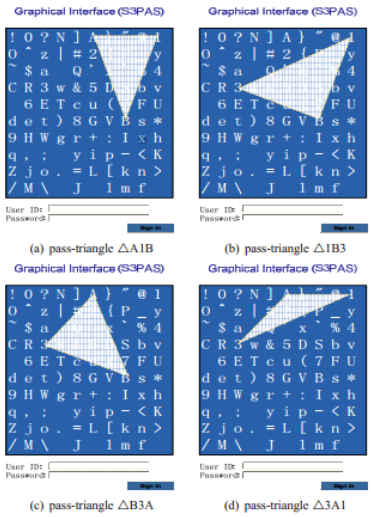

그림 6. S3PAS 방식
Fig. 6. S3PAS scheme

로그인을 위해 사용자는 로그인 이미지에 보이는 자신의 오리지널 패스-문자들을 찾아 "패스-삼각형(pass-triangles)"이라 불리는 보이지 않는 삼각형의 내부를 클릭한다. 이S3PAS에서 사용자는 오리지널 패스워드와 세션 패스워드, 총 두 개의 패스워드를 가지며, 사용자는 계정 생성 시에는 오리지널 패스워드를 선택하고 모든 로그인 과정에서 사용자는 서로 다른 세션 패스워드를 입력한다. 따라서 사용자의 오리지널 패스워드가 노출되는 것을 막을 수 있다.

III. 본 론

1. 이중표시방법을 이용한 패스워드인증 기법

제안하는 인증방법은 숫자 입력을 위한 숫자 버튼에 숫자 정보와 색 정보가 동시에 표시되도록 하는 이중 표시 방법을 이용한다. 사용자는 패스워드 입력을 위하여 버튼에서 제공하는 숫자와 색 정보 중 숫자 또는 색을 선택하여 입력할 수 있으나 입력 행위는 하나의 버튼을 누르는 것으로 동일하다.

사용자가 입력하는 버튼에 두 가지의 정보가 동시에 표시되며 번호와 색 정보 중 어떤 정보에 초점을 맞추어 입력하는지는 사용자만 알 수 있다. 제안하는 기법은 사용자가 패스워드를 설정하는 단계와 인증을 위하여 패스워드를 입력하고 인증받는 단계로 구분할 수 있다.

1) 설정 단계

설정단계에서 사용자는 입력할 패스워드를 설정하게 된다. 사용자는 패스워드의 자릿수와 함께 숫자, 색 또는 숫자와 색의 조합으로 패스워드를 설정할 수 있다. 패스워드의 길이는 안전성의 확보를 위하여 4자리 이상으로 입력하도록 한다.

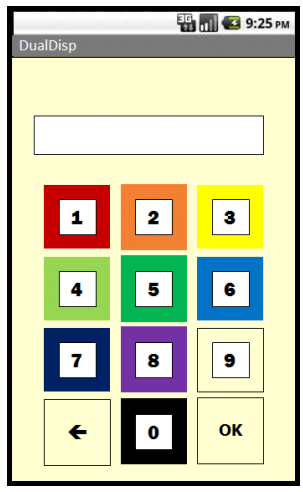

그림 7. 제안 기법의 화면
Fig. 7. Screen of Proposed scheme

사용자가 패스워드를 설정하는 방법은 다음과 같다. 예를 들어 [그림 3]과 같은 화면에서 사용자는 네 자리 패스워드를 [1,2,3,5]와 같이 숫자만 선택하거나 [빨강, 주황, 노랑, 초

록]과 같이 색만, 또는 [1, 주황, 3, 초록]과 같이 숫자와 색을 조합하여 설정할 수 있다. 버튼을 선택할 때 중복은 허용하며 설정시 버튼을 누르는 순서대로 인증시에도 순서를 지켜 입력해야 한다.

숫자와 색이 하나의 버튼에 표시되기 때문에 숫자를 선택한 것인지, 색을 선택하여 입력하는 것인지의 구분 방법이 필요하게 된다. 사용자는 버튼을 누르는 시간을 달리하여 두 정보를 구분할 수 있다. 제안하는 기법에서는 한번 짧게 터치할 때는 숫자로 인식하고 길게 터치할 때는 색으로 인식하도록 설계한다.

사용자는 그림 3과 같은 설정화면에서 다음과 같은 단계로 패스워드를 설정하게 된다.

단계 1. 사용자는 설정하고자 하는 패스워드를 정한다. 패스워드는 숫자, 색 또는 숫자와 색의 조합으로 구성할 수 있다.

단계 2. 사용자가 정한 패스워드를 터치하여 패스워드를 설정한다. 숫자를 선택했을 경우에는 버튼을 짧게 터치하고, 색을 선택했을 경우에는 버튼을 길게 터치한다.

단계 3. 4자리 이상의 패스워드 정보를 입력하고 나면 "OK" 버튼을 눌러 설정을 종료한다.

[그림 8]은 설정 단계에서의 흐름도를 나타낸다.

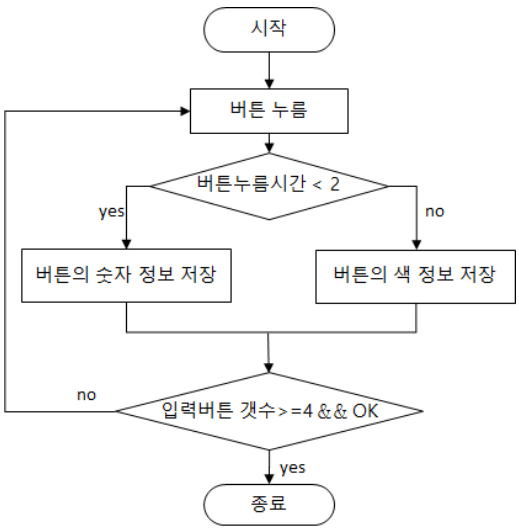

그림 8. 설정 단계 흐름도
Fig. 8. Flow Chart of password setting

2) 인증 단계

인증 단계에서는 설정 단계에서 저장한 대로 패스워드를 입력하여 인증하는 단계이다. 사용자의 저장된 패스워드 정보와 입력된 값을 비교하여 정확한 암호를 입력하면 잠금이 해제된다. 인증단계에서는 설정단계와는 달리 패스워드 입력을 위하여 숫자를 선택하던 색을 선택하던 버튼을 터치할 때 그 시간은 동일하다. 즉, 버튼이 눌렸을 때 그 버튼의 색 또는 숫자 정보 중 설정되어 저장된 패스워드와 맞는지 비교하는 것은 시스템에서 수행하게 된다. 사용자가 입력한 패스워드가 틀리게 되면 숫자와 색상은 무작위로 재배열되어 표시되며 인증의 첫 단계부터 다시 수행하도록 한다.

예를 들어 사용자가 설정한 패스워드가 [5, 주황, 3, 파랑]이면 [그림 8]과 같이 인증 화면이 제공되었을 때 

의 네 개의 버튼을 누르면 된다. 첫 번째 버튼은 숫자정보, 두 번째 정보는 색 정보, 세 번째 버튼은 숫자정보, 네 번째 정보는 색 정보를 기준으로 선택되었다. 사용자는 숫자와 색을 조합하여 선택하게 되지만 엿보기를 수행하는 공격자는 숫자와 색 정보 중 어느 단계에서 어떤 정보를 선택하여 버튼을 눌렀는지 알아내기 어렵다. 정확한 암호를 입력하지 못한 경우에는 실패했다는 메시지를 보이며 번호와 색이 무작위로 재배열되어 나타난다.

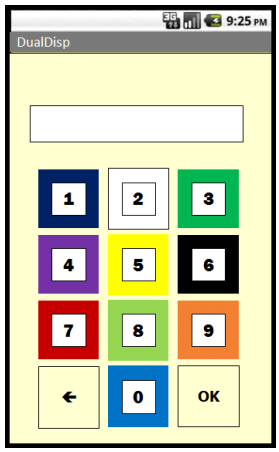

그림 9. 변경된 인증 화면
Fig. 9. Screen of authentication phase

인증 시 제공되는 화면은 매 인증마다, 그리고 인증이 실패했을 경우에는 인증 실패 메시지와 함께 숫자와 색이 무작위로 재배열되어 보여진다.

2. 제안 기법의 보안성 분석

1) 패스워드 추측 공격(random guessing attack)

패스워드 추측 공격(random guessing attack,RGA)이란 공격자가 추측을 통하여 임의로 비밀번호를 알아내어 입력하는 공격이다. 편의상 사용자의 패스워드 선택이 랜덤하다고 가정할 때 유효한 패스워드 공간의 크기가 클수록 안전성이 높을 것이다. 패스워드 공간은 조합 가능한 모든 패스워드의 경우의 수로 정의한다. 사용자 또는 공격자가 입력 가능한 조합의 수를 RGA의 안전성으로 정의할 수 있다.

[7]에 따르면 패스워드 추측 공격에 대한 안전성과 훔쳐보기 공격에 대한 안전성은 반비례 관계에 있다. 즉, 훔쳐보기 공격에 대한 안전성이 높도록 패스워드 입력 방법을 설계하였다면 추측 공격의 성공률은 더 높아지게 된다. 이에 대한 해결책으로 패스워드 공간의 크기를 크게 하거나[Yan] 패스워드 입력시에 공격자가 관찰 불가능한 채널을 이용하는 방법 등이 제안되고 있다.

제안한 기법에서는 패스워드 공간의 크기를 늘리는 방법을 적용하여 패스워드 추측 공격으로부터 안전하도록 설계하였다.무작위 공격에 대한 안전성을 암호 공간의 크기로 살펴보면 패스워드를 구성하는 자릿수를 N이라 가정할 때 기존 방식의 패스워드 공간과 제안한 기법의 패스워드 공간은 [표 1]과 같다. 비교하는 기존의 방식들은 제안 기법과 유사한 숫자를 입력하는 방식을 선정하여 비교분석하였다.

제안한 기법의 패스워드 공간의 크기가 기존의 기법들보다 큰 것을 볼 수 있다.

2) 훔쳐보기 공격(Shoulder Surfing attack)

어깨너머 훔쳐보기 공격은 사용자가 버튼을 눌렀을 경우에 어깨너머 공격을 수행한다고 해도 번호를 누른 것인지 색을 누른 것인지 구분할 수 없기 때문에 훔쳐보기를 통하여 획득한 정보를 동일하게 입력하여도 인증에 성공할 수 없다. 일반적인 PIN 입력 방식의 경우 공격자가 인증 과정을 훔쳐보기 하였을 때 그 정보를 활용하여 인증에 성공할 수 있는 확률은 1이 된다. 즉, 사용자의 패스워드가 {1,2,3,4}라고 가정하였을 때 공격자가 획득한 정보는 매번 인증 시에 같은 내용의 입력을 요구하기 때문에 획득한 정보를 통하여 공격에 성공할 확률은 1이 된다. 제안한 기법의 경우 훔쳐보기를 통하여 획득한 정보는 각 자리마다 2가지의 정보를 포함하고 있기 때문에 네 개의 입력하는 정보를 획득하였다 하더라도 그 정보를 다음번 인증에 이용하여 성공할 확률은 1/16이 된다. 따라서 훔쳐보기 공격의 안정성도 어느 정도 보장된다고 할 수 있다.

표 1. 패스워드 입력 방법 비교
table 1. Comparison of Password input method

방법	패스워드 공간 크기	패스워드 추측 성공률	훔쳐보기 성공률
PIN 입력	10^N	$1/10^N$	1
Binary[6]	10^N	$1/10^N$	1
LIN[7]	10^{N-1}	$1/10^{N-1}$	1/10
ColorPIN[8]	9^N	$1/9^N$	1/81
제안 기법	20^N	$1/20^N$	1/16

3) 스머지 공격

터치기반 모바일 기기의 경우, 사용자가 인증을 위해 터치스크린 위의 일정한 자리를 반복하여 입력하는 경우 스머지 공격에 노출되기 쉽다. 제안 기법은 매 인증시마다 숫자와 색깔 디스플레이를 무작위로 재배열하므로 자리가 매번 변경되기 때문에 인증시마다 서로 다른 위치를 터치하여야 한다. 따라서 제안 기법은 스머지 공격으로부터 안전할 수 있다.

IV. 결 론

본 논문에서는 기존에 사용자에게 익숙하게 이용되고 있는 숫자 입력 방식의 버튼에 색 정보를 추가한 패스워드 기반의 사용자 인증 기법을 제안하였다. 제안 기법은 하나의 버튼에 번호와 색의 두 개의 정보를 표현하고 사용자는 두 가지의 정보 중 하나의 정보를 선택하여 입력한다. 공격자는 사용자가 선택한 정보가 숫자정보인지 색 정보인지 알지 못하게 함으로써 훔쳐보기 공격에 대한 안전성을 확보한다. 또한 매 인증시마다 버튼을 무작위로 재배치하여 디스플레이함으로써 사용자가 계속 같은 자리를 터치하지 않도록 함으로써 스머지(Smudge) 공격도 방어할 수 있도록 설계하였다. 하나의 버튼에 두 가지의 정보를 표한하도록 함으로써 패스워드 공간의 크기는 기존의 PIN 입력 방식에 비하여 크게 할 수 있어 패스워드 추측 공격에도 강인하게 설계하였다. 제안 방식을 통해 스마트폰 보안 기법의 편의성과 안전성의 증대를 얻을 수 있다.

참고문헌

[1] Y. Berger, A. Wool, and A. Yeredor, "Dictionary

attacks using keyboard acoustic emanations," Proceeding of the 13th ACM Conf. on Computer and Communications Security, pp.245-254, 2006.
[2] M. G. Kuhn, "Electromagnetic evesdropping risks of flat-panel displays," Proceeding of the 4th Workshop on Privacy Enhancing Technologies, pp.23-25, 2004.
[3] S. Wiedenbeck, J.Water, L.Sobrado, and J. Birget, " Design and evaluation of a shoulder-surfing resistant graphical password scheme," Proceeding of the Advanced Visual Interfaces, pp. 177-184, 2006.
[4] A. J. Aviv, et al., "Smudge Attacks on Smartphone Touch Screens," Proceedings of the 4th USENIX conference on Offensive technologies, 2010.
[5] F.Tari, A. Ozol and S.H.Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," Proceeding of the second symposium on usable privacy and security, 2006.
[6] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," Proceedings of ACM Conf. Computer Communication and Security, pp. 236-245, 2004.
[7] M-K. Lee, "Security notions and advanced method for human shoulder-surfing resistant PIN-entry," IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp.695-708, Apr. 2014.
[8] A. D. Luca, K. Hertzshuch, and H. Hussmann, "ColorPin-securing PIN Entry through indirect input", International Conference on Human Factors in Computing Systems, pp. 1103-1106, 2010.
[9] G. E. Blonder, "Graphical passwords", United States Patent 5559961, 1996.
[10] Paul Dunphy, James Nicholson and Patrick Olivier, Securing passfaces for description, Proceedings of the 4th symposium on Usable privacy and security, 2008.
[11] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin, "The design and analysis of graphical passwords", Proceedings of USENIX Security Symposium, 1999.
[12] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," Proceedings. of 21st international Conference on Advanced Information Networking and Applications Workshops, 2007.

저 자 소 개

용 승 림

1998: 이화여자대학교 전자계산학과 공학사.
2000: 이화여자대학교 컴퓨터공학과 공학석사.
2006: 이화여자대학교 컴퓨터공학과 공학박사
현 재: 인하공업전문대학 컴퓨터시스템과 교수
관심분야: 컴퓨터공학, 알고리즘, 정보보안
Email : slyong@inhatc.ac.kr