KIPS Tr. Comp. and Comm. Sys.
Vol.2, No.12 pp.525~532 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2013.2.12.525

A Study on the SmartPhone GPS based Graphical Password Approach

Tae Eun Kim† · Hyeon Hong Kim† · Moon Seog Jun††

ABSTRACT

Recently smartphones, tablet, etc. Various types of smart terminal is due to the increased security in mobile devices are becoming an issue. How to enter the password in this environment is a very important issue. Difficult to have a secure password input device on various types of mobile devices. In addition you enter on the touch screen the password of character, uncomfortable and it is vulnerable to SSA attack. Therefore, in this paper provide for defense the SSA(Shoulder Surfing Attacks) and useful password input mechanism is proposed with Smartphone GPS uses a value generated via a graphical password techniques.

Keywords : Mobile, Security, Graphical Password, Shoulder Surfing Attack, Authentication

스마트폰 GPS 기반 그래피컬 패스워드 기법에 관한 연구

김 태 은† · 김 현 홍† · 전 문 석††

요 약

스마트폰, 태블릿 PC 등 다양한 형태의 모바일 스마트 단말이 증가함에 따라 이러한 모바일 단말 환경에서의 정보보호가 큰 이슈가 되고 있으며 많은 연구가 이루어지고 있다. 이런 정보보호의 한 연구 방안 중 안전하게 패스워드를 입력하는 방법은 매우 중요한 요소이며, 다양한 형태의 모바일 단말에서는 자체적인 하드웨어 제약 사항에 따라 높은 보안 등급의 패스워드 입력 장치를 구비하기 힘든 어려움을 가진다. 또한 터치스크린을 통해 단순한 문자들을 패스워드로 입력하게 되면 입력의 불편함이 따를 수 있으며, 엿보기 공격에 취약한 특성을 가지게 된다. 따라서 본 논문에서는 엿보기 공격을 방어하고 사용자 입력 편의를 제공하기 위해서 스마트폰에서 생성할 수 있는 GPS 위치 정보를 이용하여 새로운 그래피컬 패스워드 기법을 제안하고 구현하였다.

키워드 : 모바일, 보안, 그래피컬 패스워드, 엿보기(어깨넘어 훔쳐보기) 공격, 인증

1. 서 론

오늘날 기술의 발달로 컴퓨팅 환경의 패러다임의 많은 변화가 일어나고 있다. 여러 가지 변화 중 가장 중요한 변화로 모바일 환경으로의 변화가 있다. 기존의 이동성이 없는 데스크탑 환경에서 이동성이 고려되는 모바일 컴퓨팅 환경으로 변화 되면서 활용할 수 있는 기기 및 서비스 부분에서도 많은 변화 및 발전이 가속화 되고 있다.

이러한 모바일 컴퓨팅 환경으로 인해 어디서든지 정보를 얻을 수 있고 제공할 수 있다는 장점으로 많은 사람들이 자신의 모바일 기기를 이용하여 뱅킹, 주식 거래와 같은 금융서비스를 이용하고 , SNS(Social Network Service), 온라인 게임과 같은 소셜 서비스 활동 등의 여러 서비스를 장소를 가리지 않고 활용하고 있다.

모바일 기기의 활용에 따라 온라인 연결을 통해 사용하는 서비스가 증가하면서 사용자 인증을 요구하는 시스템이 더욱 많아지고 있다. 따라서 모바일 기기에서 사용자를 인증하는 것은 매우 중요한 부분이 되고 있다. 하지만 이런 모바일 기기는 몇 가지 제약사항을 가지고 있다. 첫 번째는 입력방식이 제한적이라는 점에 있다. 이동성이 없는 기존의 컴퓨팅 환경에서는 키보드, 마우스와 같은 편리한 입력 장치가 존재 했었는데, 모바일 기기를 사용할 시에는 이런 입력 장치를 항상 구비하여 사용하기 힘들다. 두 번째로 어디서든 사용자 인증이 필요한 서비스를 사용하기 때문에 개인정보가 쉽게 노출될 수 있다는 취약점이 나타난다. 이것은 보안위협 중 사회공학 기법인 어깨너머 훔쳐보기(Shoulder surfing) 공격과 연결되어 사용자 인증 과정을 위협한다. 사용자가 자신의 비밀 정보를 입력할 때 그 장면을 공격자가 엿보는 방법으로 개인정보를 노출하게 된다. 이처럼 모바일

※ 본 연구는 미래창조과학부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)의 일환으로 수행하였음[10045109, BYOD, 스마트워크 환경에서 상황정보 기반 동적 접근통제 기술 개발].
† 준 회 원 : 숭실대학교 컴퓨터학과 박사과정
†† 종신회원 : 숭실대학교 컴퓨터학과 교수
논문접수 : 2013년 10월 7일
심사완료 : 2013년 11월 20일
* Corresponding Author : Moon Seog Jun(mjun@ssu.ac.kr)

컴퓨팅 환경의 발달은 언제, 어디서나 서비스를 제공 받을 수 있다는 장점을 갖고 있는 반면에 자신의 정보 또한 노출 되기 쉽기 때문에 모바일 기기에서 개인정보를 입력하는 것은 중요한 보안 사항 중 하나로 여겨진다.

이러한 요인들로 모바일 기기에서 기존의 사용자의 비밀번호를 문자 형식으로 입력하는 패스워드 방식은 제한된 입력 장치로 인해서 정확한 패스워드의 입력이 어렵고, 어깨너머 훔쳐보기 공격에 쉽게 노출 되어있기 때문에 안전한 인증방법으로 사용하기 힘들다. 모바일 기기에서 사용해야 하기 때문에 터치스크린을 활용하여 입력하기 쉬워야 하고, 훔쳐보는 공격자에 의해 쉽게 읽혀지지 않아야 하며 기억하기 쉬워야 할 것이다. 때문에 이러한 요건들을 충족시키기 위해서 문자기반의 패스워드에 비해서 사용하기 쉽고 훔쳐보기 공격에 강한 특성을 갖는 그래피컬 패스워드(Graphical password)의 사용이 증가하고 있다[1-4].

본 논문에서는 이러한 단점들을 보완하는 그래피컬 패스워드 기법을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 기존에 연구되었던 그래피컬 패스워드 기법을 분석한다. 3장에서는 제안하는 방법에 대하여 설명하고, 4장에서는 제안하는 기법을 안드로이드 환경에서 구현하여 성능을 검증한다. 5장에서는 본 논문의 연구 결과를 설명 한다.

2. 관련 연구

그래피컬 패스워드는 단순 기억력에 의존하는 텍스트, 숫자 패스워드와는 달리 인간의 기억력과 경험(회상)이 어우러져 기억되기 때문에 더 정확하고 오랫동안 기억 할 수 있다. 또한 그래피컬 패스워드는 기존의 텍스트 기반의 패스워드 보다 월등히 큰 패스워드 영역을 가지고 있다. 예로 텍스트 패스워드가 알파벳 A to Z까지 26개 숫자 0 to 9 10개라고 가정한다면 36개, 알파벳 대소문자를 구분한다면 62개 안에서만 조합하여 이루어지지만, 그래피컬 패스워드는 그 환경이나 기법에 따라 무한하게 달라진다. 하지만 그래피컬 패스워드를 사용하기 위해서 고려해야 하는 사항이 있다. 텍스트가 아닌 그림을 기억해야하기 때문에 사용자가 상세한 비밀 이미지의 위치까지 기억하기 쉽지 않다. 또한 스마트폰을 통해 인증을 하게 되면 SSA(Shoulder Surfing Attack)에 대응해야 한다. 본 장에서는 그래피컬 패스워드를 사용자가 미리 설정해둔 패스워드를 인증 시 그대로 입력하는 상기(Recall)기반 방식, 사용자는 하나 또는 여러 개의 그림을 패스워드로 등록하고 지식 기반 인증을 통해 본질적으로 알고 있는 것에 대한 질문에 대답하여 인증하는 인지(Recognition)기반 방식으로 나누어 설명한다.

2.1 Recall-Based Graphic Password

그래피컬 패스워드가 가져야 하는 특징 중 하나는 사용자가 입력하기 쉬운 방법이어야 한다. Recall-Based 그래피컬 패스워드는 패스워드 설정 시에 했던 행동을 그대로 재연하는 방법이므로 사용자 입력이 쉽다. 이 방식은 처음 서버에서 주어지는 그림에 대해서 사용자가 원하는 포인트를 찾아서 위치를 지정한 후, 인증 요청 시 자신이 지정한 포인트를 다시 클릭하여 인증을 시도한다. 혹은 자신이 원하는 형식의 문자, 도형 등을 그려서 인증하는 방법도 있다.

1) DAS(Drow-a-Secret)

DAS(Drow-a-Secret)[5]는 사용자가 자신의 패스워드를 입력 공간 위에 그리도록 하는 기법이다. 이 기법에서 사용자의 패스워드를 입력 받기 위해서 화면을 N * N 크기의 그리드로 나누어 사용자가 그리는 패스워드를 각 그리드 좌표에 할당하는 기법이다. 이 기법은 입력하기에는 쉽지만 SSA에 있어서 취약성을 보인다.

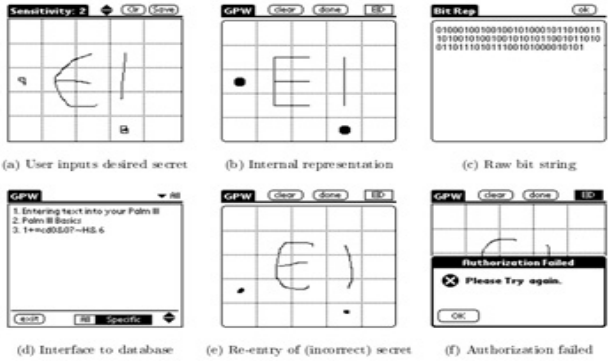

Fig. 1. Draw-a-Secret

2) I-Horng Jeng's Graphical Password

I-Horng Jeng[6] 등에 의해서 발표된 그래피컬 패스워드 기법이다. 이 기법은 DAS와 다르게 PIN 기법의 패스워드를 입력하기 위하여 전화기 숫자버튼을 그대로 이용한다. 그리고 패스워드의 한 글자를 입력하기 위한 터치는 단 한 번의 터치를 한붓그리기를 이용해서 입력한다. a부터 z까지 각 알파벳은 각각의 한붓그리기로 할당 되어져 있다. Fig. 2는 알파벳 'p'를 입력하는 화면을 보여 준다. 이 기법을 이용하게 되면 패스워드 입력하는 환경은 기존의 키패드 환경과 동일하여 사용자에게 친밀감을 주는 장점을 가지고 있다.

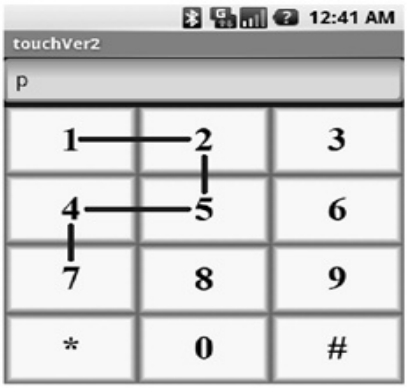

Fig. 2. I-Horng Jeng's Graphical Password

3) Grid-Selection

Grid-Selection[7]은 DAS의 확장된 형태로 DAS의 grid공간이 작은 것을 감안하여 좀 더 크게 넓혀 확장성 있게 제공하게 된다. Grid-Selection은 먼저 10cm × 10cm 공간 즉 10pt포인트라고 했을 때 30 × 30 칸의 grid를 제공한다. 여기서 자신이 원하는 시작점 ps = (x, y) 와 끝점 Pe = (x, y)를 입력하게 되면, 5×5 공간의 grid를 제공하게 되고, 제공되는 공간에서 자신이 원하는 패스워드를 만들어 인증하게 된다.

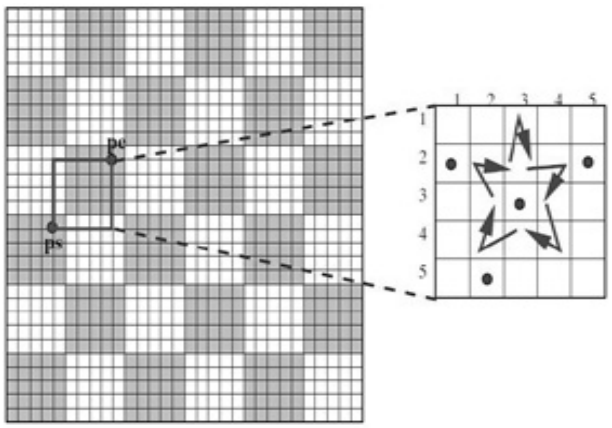

Fig. 3. Grid-Selection

4) Story-DAS

Story-DAS[8] 인증은 최근에 연구된 기술로서 SSA에 강하게 설계된 기술이며 Story를 기반으로 하여 사용자가 편리하게 사용할 수 있고, 더욱더 강한 보안성을 제공한다. 4 x 6 공간에 그림들이 랜덤으로 배치되며, 사용자가 원하는 그림을 선택하여 자신이 기억 할 수 있는 스토리를 만들어 그들을 연결하여 인증을 한다.

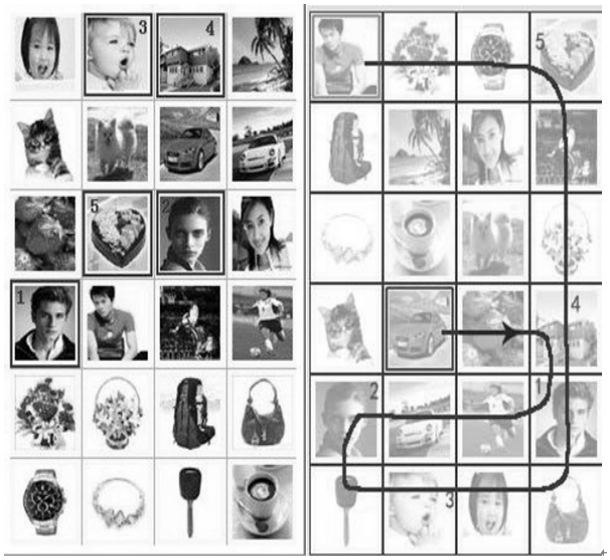

Fig. 4. Story-DAS

2.2 Recognition-Based Graphic Password

Recognition 방식은 사용자가 이미지를 등록하여 자신만의 패스워드로 생성하고 인증 단계에서 다른 여러 이미지들과 함께 사용자에게 비밀번호를 요구하게 되면 자신이 등록했던 이미지를 차례로 선택하여 인증하는 방식과, 사용자가 자신의 신원을 확인하기 위해 잊혀지지 않는 기억의 질문을 설정하게 한 후 사용자에게 해당하는 질문을 통해 인증하는 방식이 있다.

1) PassFaces

PassFaces[9]는 Realuser.com사가 개발한 인식기반의 이미지 인증 시스템으로 사람 의 얼굴 이미지를 패스워드로 사용하는 인증 방식이다. 사용자는 제시된 3×3 격자 안에 순차적으로 3명의 얼굴을 선택하여 패스워드로 등록하여, 다음 인증 시 랜덤으로 섞여 있는 3×3공간에서 자신이 선택한 사람의 얼굴을 3단계에 걸쳐서 선택하게 되면 인증이 끝나는 방식이다. PassFaces 기법은 사람의 얼굴을 통해서 인증하는 방식으로 연상이 용의하고 오래도록 기억하기 좋다.

Fig. 5. PassFaces

2) Deja Vu

Deja Vu[10]는 프랑스어로 '다시 본 것 같은' 이라는 뜻이다. 이는 이미지에 대한 사람들의 기억력이 매우 뛰어나다는 사실에 기초하고 있는 기법이다.

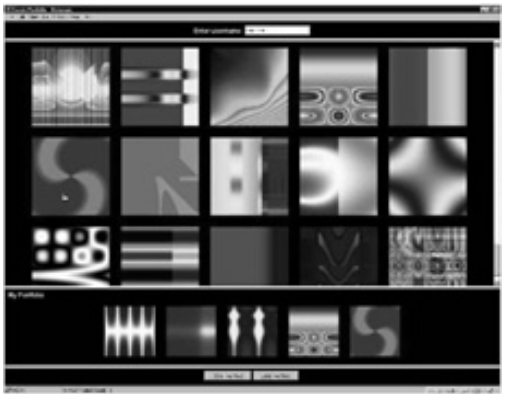

Fig. 6. Deja Vu

Deja Vu는 포트폴리오 생성, 트레이닝, 인증 단계로 이루어진다. 포트폴리오 단계에서는 사용자가 샘플 이미지 집합에서 이미지 p를 선택한다. 다음 트레이닝 과정은 사용자의 기억력을 향상시키기 위한 과정으로 자신이 선택한 이미지와 흡사한 미끼(decoy) 이미지들을 이용하여 트레이닝을 하게 된다. 그리고 마지막으로 인증과정에서는 샘플 이미지 집합에서 포트폴리오 단계에서 선택한 이미지를 찾아 인증한다.

3. 제안 기법

3.1 제안 시스템의 구성

2장의 관련연구를 통하여 지금까지 연구된 그래피컬 패스워드에 살펴보았다. 특히 이미지를 사용하여 인증하는 방법이 텍스트 기반의 기존 암호보다 뛰어난 안전성을 제공 하는걸 볼 수 있었다. 하지만 이러한 방법도 보안성을 높이면 사용자가 사용하는 방법이나 기억하기가 어려워지고, 사용성을 높이면 보안성이 저하되는 현상이 발생된다.

본 제안에서는 그래피컬 패스워드의 간편한 사용을 위하여 모바일 기기의 위치정보를 이용한 그래피컬 패스워드 인증과정을 수행한다. 또한 보안성의 강화를 위해 인증 시스템 관리자에 의해 추가적으로 사용될 수 있는 Recognition 사용자 확인 질문 인증기법을 추가 제안하여 보안성을 향상 시킨다. 제안 기법의 모든 과정은 스마트폰의 터치스크린에서 손쉽게 사용할 수 있는 지도를 이용하여 편의성을 증가한다.

사용자는 모바일 기기를 활용하여 인터넷 서비스를 이용할 때 패스워드와 같은 인증 값을 전송하게 된다. 이때 기존의 문자형식의 패스워드 대신 두 가지의 인증 값을 사용한다. 하나의 인증 값은 휴대폰의 위치가 바뀔 때마다 변경되는 위치정보 값이고, 또 하나는 기존의 패스워드를 대신

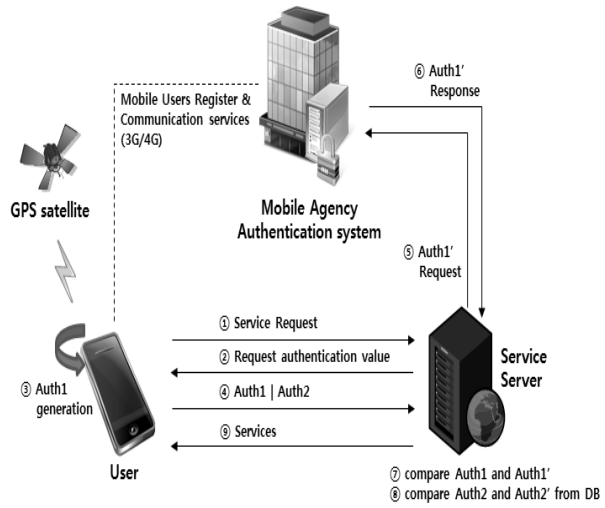

Fig. 7. The proposed system configuration

하여 등록한 지도의 특정 위치 좌표 값을 인증 값으로 사용한다.

휴대폰의 위치정보 값을 인증 값으로 전송받은 서비스 서버는 통신사 기지국을 기반으로 한 사용자의 위치정보 값을 수신하여 사용자가 자신의 모바일 기기를 이용하여 서비스를 이용하기 위한 접속 시도라는 것을 인증 하게 된다.

3.2 인증 값 등록

모바일 기기를 이용하여 서비스 서버에 회원등록을 할 때 그래피컬 패스워드를 등록하게 된다. 사용자는 인증 값의 하나로 사용 될 그래피컬 패스워드를 화면에 보여지는 지도에서 자신만의 특정 위치를 선택한다. 이때 등록한 인증 값은 위 그림의 AUTH2 값으로 사용된다.

Fig. 8. Password registration process

3.3 인증 과정

사용자가 서비스를 사용하기 위해 인증 시도 요청을 하게 되면, 패스워드를 텍스트로 입력하는 대신 패스워드 선택 버튼을 눌러 지도 화면에서 패스워드를 선택한다. 사용자 인증은 2가지의 인증 값을 조합하여 패스워드를 생성하는데 첫 번째 인증 값은 자신의 모바일 기기가 위치한 위치좌표를 통해 생성하고(AUTH1) 두 번째 인증 값은 지도 화면에서 자신이 선택한 위치의 좌표(AUTH2)를 통해 생성한다.

- Step 1~2: 사용자가 모바일 기기에서 서비스를 이용하기 위해 서버에게 요청하고 서버는 인증 과정을 요구

- Step 3: 사용자는 인증 값으로 사용할 AUTH2를 지도에서 선택하여 생성하고 모바일 기기의 Agent에서 AUTH1 값을 현재 기기의 위치를 통해 생성

· Step 4~5: 생성된 AUTH1, AUTH2를 이용하여 패스워드를 생성하여 서비스 서버에 전송

· Step 6~7: 패스워드를 검증하기 위하여 통신사에서 기지국에 접속되어있는 사용자의 위치 값 AUTH1' 수신

· Step 8: 통신사에서 수신한 AUTH1'과 사용자가 등록한 AUTH2' 값을 통해 PW'를 구해내고 사용자가 인증을 위해 전송한 값을 복호화 하여 PW를 얻는다. 이렇게 얻어진 PW와 PW'를 비교하여 사용자 인증 과정을 수행한다.

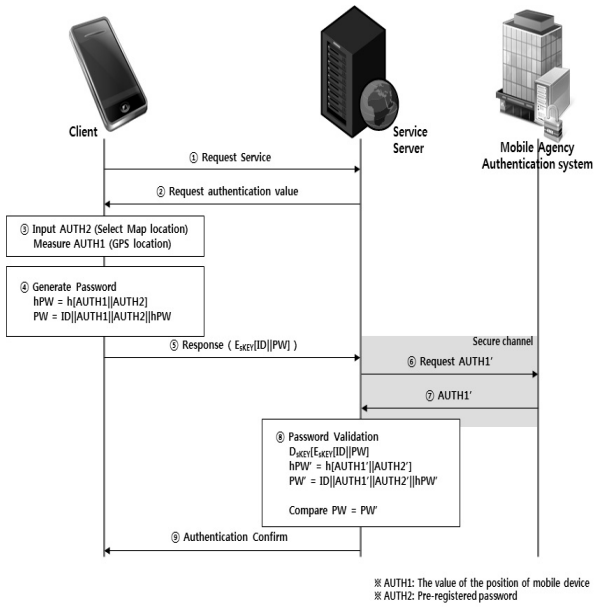

Fig. 9. Authentication Protocol

인증과정에서 사용하는 위치정보 값은 위도, 경도로 된 값을 사용한다. 하지만 AUTH1을 계산하기 위한 휴대폰이 위치한 위치정보와 기지국의 위치정보 값은 정확하게 일치하지 않고, 사용자가 인증을 위해 지도에서 선택하여 입력하는 AUTH2 값 역시 매번 같은 곳을 선택할 수 없어 정확한 값의 비교가 어렵다. 따라서 오차 범위를 조정하기 위하여 위도, 경도 값을 구성하는 도,분,초 단위의 값에서 '초' 단위의 일정 값을 뺀 나머지 값을 인증 값으로 사용한다.

3.4 추가 인증 기법

강력한 보안성을 위하여 추가적인 인증 또는 비밀번호 분실 시 사용할 수 있는 사용자 인증 방법을 사용할 수 있다. 기존의 인터넷 서비스를 이용할 때 사용자 비밀번호 분실 시 미리 설정해둔 질문의 답변을 하여 사용자를 인증하는 Recognition 방식의 인증 방법을 이용한다.

사용자가 기존의 비밀번호로 사용할 위치좌표 값 등록 시 추가적인 인증 값을 등록하게 할 수 있다. 기존의 사용자 확인을 위해 사용되는 질문과 답을 입력하는 방식과는 다르게 지도의 특정 위치를 선택하고 특정 위치를 기억하는 자신만의 정답을 등록한다. 이 추가적인 인증 값을 등록하는 과정은 여러 값을 등록 할 수 있게 하여 추후 인증과정에서 등록한 여러 값들 중 임의의 하나를 선택하여 사용자에게 질문 한다.

Fig. 10. Additional security questions

추가 인증을 위해 등록되는 특정 위치와 답(Answer)은 사용자가 자신의 지식을 통해 알고 있는 위치를 선택하고 그 위치를 설명하는 답에 해당하는 문구를 남기는 것으로, 이 값을 사용하면 사용자의 추가적인 인증과정으로 활용할 수 있다. 또한 피싱, 악성앱 등을 통해 사용자가 당할 수 있는 피해를 방지하고 서버를 인증하는 역할로도 활용할 수 있다.

이와 같은 추가 인증 방법이 기존 텍스트 형식의 'Q&A' 기법보다 SSA에 대한 안전성을 제공한다. 사용자가 선택한 기존의 텍스트 문장을 반복하여 보여주는 것이 SSA에 취약함을 보이지만, 그래픽 형태의 지도의 화면을 보여주는 과정에서 동일한 이미지를 반복적으로 보여주는 것이 아닌 지도 배율 및 위치의 변화를 주어 사용자에게 보여주기 때문에 SSA에 강력하다고 할 수 있다. 또한 사용자가 설정한 임의의 여러 위치를 항상 다른 배율로 사용자에게 보여주기 때문에 지식을 기반으로 하는 사용자 이외의 공격자에겐 복잡성을 증가시킬 수 있게 된다.

4. 성능 평가

4.1 구현 환경

본 구현은 서비스 서버에 접속하여 인증을 받기 위한 스마트폰 환경을 대상으로 하고 있기 때문에 가장 널리 사용

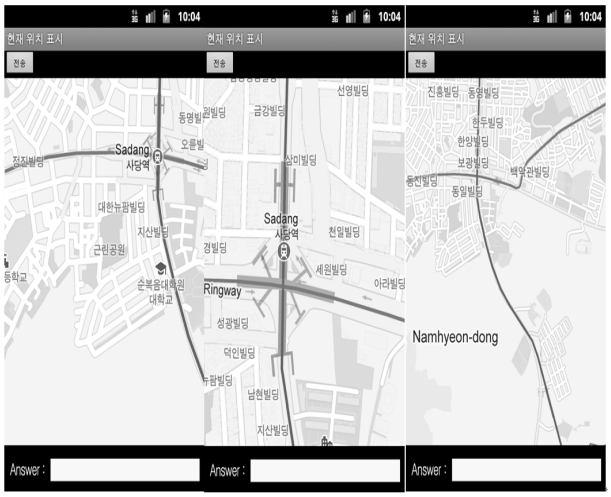

Fig. 11. Change the authentication screen for the defense of Shoulder Surfing Attack(SSA)

되고 있는 Android OS 상에서 구현하였다. Table 1은 구현된 어플리케이션을 실행하는 구현환경을 나타낸다. 또한 안드로이드 어플리케이션으로 스마트폰에 구현된 모습을 볼 수 있다. 논문에서 구현된 어플리케이션은 지도의 특정 부분을 터치 할 때 해당 위치의 좌표 값 x, y를 보여주지만 실제 사용 시에는 해당 정보를 보여주지 않는다.

4.2 구현 결과 검증

기존의 그래피컬 패스워드를 살펴보면 패스워드의 기억성을 증가시키기 위한 여러 가지 방법을 사용하였다. 직접 자신이 해당 그림을 그리는 방법, 기억하기 쉬운 이미지를 사용하는 방법, 이미지 조합을 이야기로 만드는 방법, 사용자

Table 1. Implementation environment of the proposed system

Division		Contents
Server	OS	Microsoft Window 7 Enterprise K 32bit
	H/W	CPU: Intel(R) Core(TM)2 Quad CPU @ 2.66GHz RAM : 3.00GB
	Development Tools	jdk-7u9-windows-x64 eclipse-java-juno-win32-x86_64
	Encryption Algorithm	SEED
Client	OS	Android 2.3.3 Gingerbread(API Level 10)
	H/W	Galaxy U (SHW-M130L)
	Development Tools	jdk-7u9-windows-x64 eclipse-java-juno-win32-x86_64
	Encryption Algorithm	SEED
	Application screens	

Table 2. Comparison with existing methods

password methods	Shoulder Surfing Attack	Brute Force Attack
Text 기반 패스워드	패스워드 입력 시 확연히 보임	스마트폰 입력 환경의 한정된 경우의 수를 통해 공격 가능성 존재
DAS	패스워드의 모양이 확연히 보임	입력 가능한 모양이 다수이므로 공격이 어려움
I-Horng Jeng	입력하려는 문자의 모양이 드러남	알파벳 총 개수*2개만큼의 시도로 공격 가능
Grid Selection	DAS와 마찬가지로 패스워드의 모양이 드러남	입력 가능한 모양 및 공간이 DAS보다는 월등히 많아 공격이 어려움
Story DAS	패스 이미지의 예측 이미지가 보임	중복을 허용하는 입력으로 공격이 어려움
PassFaces	선택 가능한 사람의 얼굴은 임의로 출력되지만 선택 할 사람의 얼굴은 보임	여러 라운드 형식으로 얼굴을 선택하고 매 라운드 마다 다른 선택 값이 발생하므로 공격이 어려움. 하지만 때때로 특정한 성(gender)나 종족(race)에 대한 우선선택을 하는 문제점이 발생할 수 있음
Deja Vu	선택하는 포트폴리오를 공격자가 볼 수 있음	인증시도마다 보여지는 이미지의 수가 적은 경우 공격 가능성 존재 Guessing , Dictionary Attack 가능
제안 시스템	지도 내 특정 위치를 선택함에 있어서 고정된 이미지를 선택하는 다른 기법들과 다르게 확대, 축소가 가능하므로 사용자의 선택위치를 확실히 알 수 없음	좁은 범위의 이미지 위를 선택하는 방법과 다르게 이동이 가능한 넓은 세계 지도를 사용하므로 공격 불가능하고 사용자 기기의 현재위치 인증 값으로 사용하기 때문에 다른 단말에서는 사용할 수 없음 또한 추가 인증방법의 지도 내 특정 위치의 답을 요청할 때 사용자의 기억으로 설정되어 있는 정답을 유추하기 어려움

가 직접 이미지를 등록하는 방법 등이 있다. 하지만 제안한 기법에서는 단순하게 자신의 지식과 관련된 위치 정보를 기억하고 해당하는 사용자만의 대답을 기억하면 된다. 사용자와 관련이 없는 질문과 답을 기억해야 하는 기존의 그래피컬 패스워드보다 쉽다는 장점이 있다.

4.3 구현 결과의 보안성 검증

본 절에서는 제안 시스템의 안전성을 Shoulder Surfing Attack, Brute Force Attack 등의 항목으로 구분하여 제안 시스템의 안전성을 분석하였다. 다음 Table 2는 기존 텍스트 기반의 패스워드 방식, 그래피컬 패스워드 방식과 제안 시스템의 안전성에 관한 비교분석을 기술 하였다.

5. 결론 및 추후 연구

본 논문에서는 스마트폰 환경에서 패스워드를 입력하는 사용자의 편의성 개선과 Shoulder Surfing Attack, Brute Force Attack을 막기 위해 지도의 위치정보 및 사용자 기기의 위치정보 추가적인 사용자 기억을 통한 'Q&A' 방식의 그래픽 패스워드 방식을 제안하였다. 기존 그래픽 패스워드는 텍스트 기반의 패스워드 방식보다는 사용자가 입력하기 편하고 기억에도 용이하였지만 사용자의 직접적인 기억과는 거리가 멀어 기억의 용이성이 좋지 않았다. 하지만 제안 방식은 기존의 방법들의 단점인 이미지의 고정적인 출력으로 인하여 발생하는 Shoulder Surfing Attack 공격에 안전하고, 서버에서 제공하는 이미지를 억지로 기억해야 하는 경우와 다르게 연상기억으로 인하여 패스워드의 기억성이 높다. 또한 추가적인 인증 과정을 사용하므로 안전성을 높일 수 있었다. 하지만 기존의 방법들 보다 입력할 수 있는 경우의 수가 많아 공격에는 강하지만 입력시간이 오래 걸릴 수 있다는 단점을 내포하고 있다. 따라서 추후에 사용자 인터페이스의 개선을 통하여 입력의 편의성을 증대시면 스마트폰 환경에서 사용자들이 안전하게 서비스를 사용 할 수 있을 것이다.

참 고 문 헌

[1] Sang-Jo Youk, Seung-Sun Yoo, Gil-cheol Park, and Tai-hoon Kim, "Design of Internet Phone (VoIP) for Voice Security using the VPN", International Journal of Multimedia and Ubiquitous Engineering, Vol.2, No.4, pp.55-66, 2007.

[2] Seung Wook Jung, "CAPTCHA-based DDoS Defense System of Call Centers against Zombie Smart-Phone", International Journal of Security and Its Applications, Vol.6, No.3, pp.29-36, 2012.

[3] Ali Fahmi Perwira Negara, Elyor Kodirov, Mohd Fikri Azli Abdullah, Deok-Jai Choi, Guee-Sang Lee and Shohel Sayeed, "Arm's Flex when Responding Call for Implicit User Authentication in Smartphone", International Journal of Security and Its Applications, Vol.6, No.3, pp.55-64, 2012.

[4] Jin Baek Kim and Sungmin Kang, "A Study on the Factors Affecting the Intention to Use Smartphone Banking: The Differences between the Transactions of Account Check and Account Transfer", International Journal of Multimedia and Ubiquitous Engineering, Vol.7, No.3, pp.87-96, 2012.

[5] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter and A.D. Rubin, "The design and analysis of graphical passwords," Proceedings of the 8th USENIX Security Symposium, pp.1-14, 1999.

[6] I.H. Jeng, D.R. Tsai, H.A. Chen, Y.C. Yen, and C.K. Cheng, "Touch sensitive alphanumeric encrypting PIN pad design based on hamilton connected subgraph recognition," Processing of International Conference on Intelligent Information Hiding and Multimedia Signal, pp.258-261, 2009.

[7] J.Thorpe, P.C. van Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords", 2004.

[8] H.Gao, Z.Ren, X.Chang, X.Liu, U.Aickelin Story-DAS, "A New Graphical Password Scheme Resistant to Shoulder-Surfing", International Conference on Cyberworlds, 2010.

[9] PassFacesTM, "http://www.realuser.com", last accessed on Dec., 2011.

[10] Rachna Dhamija, "Dejavu A User Study Using Images for Authentication", 2007.

김 태 은

e-mail : eunii31@ssu.ac.kr

2005년 백석대학교 정보통신학부(학사)

2007년 숭실대학교 컴퓨터학과(석사)

2007년~현 재 숭실대학교 컴퓨터학과 박사과정

2013년~현 재 한국인터넷진흥원 인터넷침해대응본부 선임연구원

관심분야 : 네트워크 보안, 모바일 보안, 정보보호

김 현 홍

e-mail : rlagusghd83@ssu.ac.kr

2009년 서일대학 인터넷정보(전문학사)

평생교육진흥원(공학사)

2013년 숭실대학교 컴퓨터학과(석사)

2013년~현 재 숭실대학교 컴퓨터학과 박사과정

관심분야 : 모바일 보안, 전자인증, 정보 보안

전 문 석

e-mail : mjun@ssu.ac.kr

1981년 숭실대학교 컴퓨터학과(학사)

1986년 University of Maryland 전산과 (석사)

1989년 University of Maryland 전산과 (박사)

1989년 Morgan State University(전산수학과 조교수)

1991년~현 재 숭실대학교 컴퓨터학부 정교수

관심분야 : 정보보호, 전자여권, 전자상거래, 암호학