지뢰찾기 게임을 응용한 어깨너머 훔쳐보기 공격에 안전한 패스워드 인증 기법

김태진*, 김시완*, 박은애*, 이정현*
*숭실대학교 컴퓨터학과
{tjkim, kimsiwan, eunsang5, jhyi}@ssu.ac.kr

Minesweeper Game Based Password Authentication Scheme Resistant to Shoulder-Surfing Attack

Taejin Kim*, Siwan Kim*, Eunae Park*, Jeong Hyun Yi*
*Department of Computer Science and Engineering
Soongsil University, Seoul, Korea

요 약

스마트폰이 널리 보급되면서 사진, 금융정보 같은 중요한 정보를 저장하고 이를 활용한 다양한 서비스가 제공되고 있으며, 이러한 중요정보를 보호하기 위해 사용자인증의 중요성이 증대되고 있다. 하지만 일반적으로 많이 사용하는 4자리 PIN(Personal Identification Number)은 무작위 대입 공격 및 어깨너머 훔쳐보기 공격에 취약하다. 이러한 문제점을 해결하기 위해 다양한 인증 기술들이 개발되고 있다. 본 논문은 지뢰찾기 게임을 이용하여 어깨너머 훔쳐보기 공격에 안전한 새로운 패스워드 기반 사용자 인증방식을 제안한다. 제안기술은 사용자가 쉽게 패스워드를 기억할 수 있으며 실제 패스워드를 직접 입력하는 것이 아닌 패스워드를 이용한 계산된 값을 입력하는 방식을 통해 어깨너머 훔쳐보기 공격에 안전성을 보장한다.

1. 서론

최근 스마트폰이 빠르게 보급되면서 스마트폰을 이용한 다양한 서비스들을 이용하게 되었고, 이러한 서비스들의 활용도가 높아짐에 따라 PC를 이용한 업무를 대체하는 것이 가능해졌다. 이처럼 스마트폰의 발전은 사용자에게 편리함을 제공하지만, 개인정보 노출, 바이러스, 악성코드와 같은 다양한 위협에 노출될 수 있다. 따라서 스마트폰에 저장된 중요한 정보를 안전하게 관리하기 위한 사용자 인증의 중요성은 점점 증대 되고 있다.

기존 모바일 기기에서 패스워드 기반 사용자 인증은 사용하기 편리하지만 어깨너머 훔쳐보기 공격(Shoulder-Surfing Attack)[1], 무작위 대입 공격(Brute Force Attack)[2]에 매우 취약하다. 이를 해결하기 연구들이 활발하게 진행되고 있다. 하지만 기존 기술들은 모바일 환경을 고려하지 않거나, 보안 취약점을 해결하는 대신 사용성이 지나치게 떨어지거나, 반대로 사용성은 높으나 어깨너머 훔쳐보기 공격에는 여전히 취약한 문제점을 앉고 있다. 따라서 본 논문에서는 모바일 환경 하에서 어깨너머 훔쳐보기 공격을 방지하면서도 적절한 사용성을 보장하는 패스워드 기술을 제안한다. 본 논문에서는 제안 기술과 기존 기술의 안전성 분석을 통해, 제안 기술이 무작위 대입, 어깨너머 훔쳐보기 공격에 안전함을 증명한다.

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(20100011057).

본 논문에 구성은 다음과 같다. 2장에서는 기존 패스워드 인증 기법들을 살펴보고, 3장에서는 제안 패스워드 인증 기법에 대해 기술한다. 4장에서는 제안기법의 안전성에 대하여 분석하며, 5장에서는 사용자 테스트를 통한 제안기법의 사용성을 평가한다. 6장에서는 결론을 맺는다.

2. 관련연구

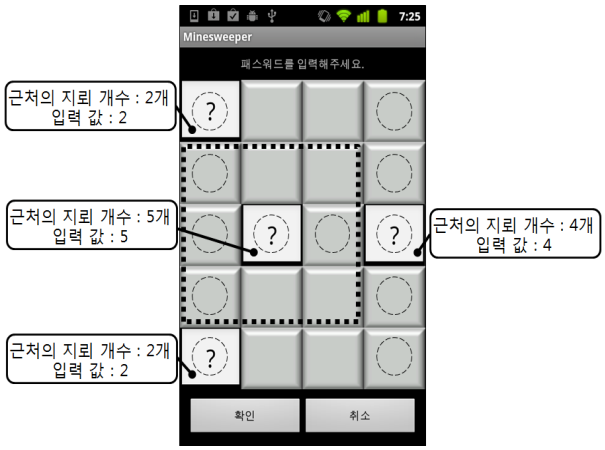
PIN-Entry[3]기술은 V. Roth, et al.이 제안한 기술로 일반적인 PIN을 패스워드로 사용한다. 인증기법은 PIN자리마다 해당되는 배경색을 입력 값으로 사용하며, 각 자리마다 4번씩 입력한다. 인증 방식은 크게 즉시 선택과 지연 선택으로 나눌 수 있으며, 즉시 선택 방식은 정확도가 높지만 인증하는 시간이 오래 걸리는 단점이 있고, 지연 선택 방식은 인증 속도는 빠르지만 오류율이 높아 사용성이 떨어지는 단점이 있다.

㈜신비테크에서 개발한 DAS(Dynamic Authentication System)[4]는 어깨너머 훔쳐보기 공격을 방지하는 PIN 기반 가상 키패드 기술이다. 이 기술은 무작위로 배치된 키패드의 위치를 기억하고, 키패드의 숫자가 사라지면 기억한 숫자의 위치를 선택한다. 키패드의 숫자가 사라진 상태에서 입력하기 때문에 일시적인 어깨너머 훔쳐보기 공격에는 안전하지만 지속적인 어깨너머 훔쳐보기 공격과 레코딩 공격에 취약하다.

㈜민인포에서 개발한 Dementor-SGP[5]기술은 이미지

간의 상대경로를 패스워드로 사용하는 기술이다. 패스워드는 사용자 이미지 3개와 홀 이미지 1로 구성되며, 사용자 이미지와 홀 이미지 간에 상대경로를 통해 인증한다. 보안 단계를 구성하여 사용자가 선택적으로 이용할 수 있도록 제공되며 단계가 올라 갈수록 입력방법은 어려워지지만 안전성은 높아진다. 어깨너머 훔쳐보기, 무작위 대입, 사전 공격에 강인하지만 사용성이 떨어지는 단점이 있다.

Passfaces Corporation에서 개발한 Passfaces[6]는 사람의 얼굴 이미지를 패스워드로 사용하는 기술이다. 인증 기법은 자신이 선택한 얼굴이미지를 찾아 순서대로 입력한다. 이 기술은 얼굴 이미지가 다른 이미지보다 더 기억하기 쉽다는 것을 이용하였다. 하지만 지속적인 어깨너머 훔쳐보기 공격과 레코딩 공격에 취약하다.



(그림 2) 사용자 인증화면 예

3. 제안 패스워드 인증 기법

기존 패스워드 인증 기술들은 안전성과 사용성을 동시에 만족시키지 못하고 있다. 예로 PIN-Entry, DAS, Passfaces 기술들은 어깨너머 훔쳐보기 공격에는 안전하지만 여전히 레코딩 공격에는 취약하며 Dementor-SGP 기술은 안전성은 높지만 사용성이 낮다. 따라서 본 논문에서는 안전성과 사용성을 동시에 만족시키기 위해 지뢰찾기 게임을 응용하는 패스워드 인증기법을 제안한다. 많은 사용자들에 친근한 지뢰찾기 게임을 응용하여 사용자들의 흥미를 유발하고 익숙한 인터페이스로써 높은 사용성을 가질 수 있으며 레코딩 공격을 포함하는 어깨너머 공격에도 안전하다. 안정성에 대한 분석은 4장에서 자세히 다루도록 한다.

제안 기법의 패스워드는 지뢰의 위치와 개수로 구성된다. 먼저 패스워드 설정 화면에서 자신이 원하는 위치에 지뢰를 선택한다. 지뢰 선택 완료 후 확인 버튼을 입력하여 자신의 패스워드 설정을 완료한다. 사용자 인증 방법은 무작위로 생성되는 입력 인터페이스의 위치를 확인하고, 확인한 입력 인터페이스를 중심으로 한 셀 거리 이내의 가운데, 상, 하, 좌, 우, 대각선에 존재하는 지뢰의 개수를 입력한다.

(그림 1) 패스워드 설정 화면 예

생성된 모든 입력 인터페이스에 지뢰의 개수를 입력 후 확인 버튼을 입력하여 인증한다. 모든 입력 값과 지뢰의 개수가 옳으면 인증에 성공한다.

예를 들어, 제안기술이 4×5 그리드를 사용하고, 인증 시도의 입력 값 개수가 4개일 때, 패스워드를 [그림 1]과 같이 H모양으로 지뢰를 배치한다고 가정하자. 본 논문에서 제안 기술의 인증과정을 설명하기위해 그리드가 1에서 y까지의 행과 1에서 x까지의 열로 구성된다고 했을 때 그리드의 좌표를 (x,y)로 기술한다. 먼저, 사용자 인증단계에서는 [그림 2]와 같이 무작위로 위치한 입력 인터페이스를 통해 패스워드를 입력한다. 사용자는 (1,1)에 위치한 입력 인터페이스의 입력 값으로 (1,1), (1,2)에 존재하는 지뢰의 개수인 “2”를 입력한다. 이와 같이 (2,3)에 위치한 입력 인터페이스는 (1,2), (1,3), (1,4), (2,3), (3,3)에 존재하는 지뢰의 개수인 “5”를 입력하고 (4,3)에 위치한 입력 인터페이스는 (3,3), (4,2), (4,3), (4,4)에 존재하는 지뢰의 개수인 “4”을 입력하며 (1,5)에 위치한 입력 인터페이스는 (1,4), (1,5)에 존재하는 지뢰의 개수인 “2”를 입력한다. 모든 입력 인터페이스에 지뢰의 개수를 입력한 후 “확인”버튼을 눌러 인증한다. 입력한 지뢰의 개수가 모두 옳으면 인증에 성공한다.

4. 안전성 분석

본 장에서는 제안하는 패스워드 인증 기법에 대한 안전성을 분석한다. 안전성 분석 설명에 사용되는 기호 및 설명은 <표 1>과 같다.

<표 1> 기호 정의

기호	설명
T	패스워드를 구성하는 원소 개수
N	패스워드의 길이
X	그리드의 가로 개수
Y	그리드의 세로 개수
M	입력을 요구하는 위치의 개수
S	공격자가 획득한 입력 값 개수

4.1 패스워드 공간 크기

패스워드 공간 크기는 주어진 패스워드 공간에서 조합 가능한 모든 패스워드의 경우의 수를 말한다. 기존 기술과 제안기술의 패스워드 구성과 패스워드 공간크기는 <표 2>와 같다.

<표 2> 기술별 패스워드 구성과 공간

	패스워드 구성	패스워드 공간
PIN	숫자 N자리	10^N
DAS	숫자 N자리	10^N
Dementor-SGP	사용자 이미지 N개 (홀 이미지 포함)	${}_TP_N$
Passfaces	얼굴 이미지 N개	${}_TP_N$
PIN-Entry	숫자 N자리	10^N
제안 기법	지뢰의 설치 위치 N개	2^{XY}

제안 기술의 패스워드 공간은 2^{XY} 로 기존 PIN 기반 패스워드에 비해 높은 공간 크기를 가진다. 또한 DEmentor-SGP, Passfaces와 같이 X와 Y의 크기를 일정 수준 증가 시킬 수 있기 때문에 무작위 대입 공격에 더욱 안전할 수 있다.

4.2 무작위 대입 공격

무작위 대입 공격이란 공격자가 패스워드를 구성하는 전체 요소의 집합에서 가능한 모든 조합의 경우의 수를 추측해 봄으로써 패스워드를 알아내는 공격이다. <표 3>는 기존에 존재하는 기술과 제안기술의 무작위 대입 공격 성공 확률을 나타낸다.

<표 3> 기술 별 무작위 대입 공격 시 성공 확률

	무작위 대입 공격 성공 확률
PIN	10^{-N}
DAS	10^{-N}
Dementor-SGP	$1/({}_TP_N)$
Passfaces	9^{-N}
PIN-Entry	10^{-N}
제안 기술	$1/2^{XY}$

무작위 대입 공격의 성공 확률은 패스워드 공간 크기에 영향을 받으며 제안기술이 X = 4, Y = 5 일 경우 $1/2^{20}$의 무작위 대입 공격 성공 확률을 가진다. 이것은 Dementor-SGP가 M = 30, N = 4 일 경우 보다 약 1.59배, PIN, DAS, Dementor- SGP가 N = 4 일 경우 보다 약 104배, Passfaces가 N = 4 일 경우 보다 약 159배 안전하다. 이는 기존 4자리 PIN 기반 패스워드보다 안전하며 상용 인증 기술은 Dementor-SGP보다 무작위 대입 공격에 더 안전하다.

4.3 어깨너머 훔쳐보기 공격

어깨너머 훔쳐보기는 사용자가 인증 시 어깨 너머로 인증과정을 지켜보고 패스워드를 획득하는 공격이다. PIN, DAS, Passfaces, PIN-Entry 기술은 사용자 인증 시 패스워드 입력 과정이 그대로 노출되기 때문에 어깨너머 훔쳐보기 공격에 매우 취약하다. 본 논문에서 제안하는 사용자 인증방식은 사용자 인증 시 입력하는 값은 실제 패스워드가 아닌 근처의 지뢰 개수를 입력함으로써 실제 지뢰의 위치를 숨길 수 있다. 또한 공격자가 입력 값을 획득하더라도 시도 입력 인터페이스의 위치는 매번 무작위로 바뀌기 때문에 공격자의 성공 확률은 매우 낮다. 이 확률을 구하기 위해서 공격자가 획득한 입력 값의 개수가 S라고 하고, M개의 입력 인터페이스 중 미획득한 입력 값의 개수가 n이라고 가정한다. 이때 미획득한 입력 값의 조합의 개수가 ${}_{(XY-S)}C_n$가지, 획득한 입력 값의 조합의 개수가 ${}_SC_{(M-n)}$ 가지이기 때문에 n개의 미획득한 입력 값이 포함된 입력 인터페이스가 선택될 확률은 ${}_{XY-S}C_{(M-n)}({}_{XY-S}C_n / {}_{XY}C_M$이다. 또한, n만큼 무작위로 선택된 입력 인터페이스에 올바른 입력이 요구된다. 마지막으로 모든 n의 경우를 합하여 확률을 구한다. 다음 수식 (1)은 공격자의 인증 성공을 나타낸다.

$$\sum_{n=0}^{M}\left\{\frac{{}_SC_{(M-n)}({}_{XY-S}C_n}{{}_{XY}C_M}\left(\frac{4}{5XY}+\frac{2(X+Y)-8}{7XY}+\frac{XY-2(X+Y)+4}{10XY}\right)^n\right\} \quad (1)$$

본 논문에서 구현 실험한 것과 같이 제안기술에서 X = 4, Y = 5, M = 4 의 값을 갖고, 한 번의 어깨너머 훔쳐보기 공격으로 획득할 수 있는 정보 S = 4 라 가정하면, 어깨너머 훔쳐보기 공격 후 인증 성공 확률은 약 6.51×10^{-3}이다. 따라서 제안 기술은 어깨너머 훔쳐보기 공격에 안전하다.

4.4 레코딩 공격

레코딩 공격은 어깨너머 훔쳐보기 공격의 일부분으로 카메라와 같은 장비를 통해 인증과정을 모두 녹화하는 방법이다. 제안 기술의 경우 한 번의 레코딩 공격으로 획득할 수 있는 인증 값의 개수는 M개 이다. 하지만 시도 입력 인터페이스의 위치는 매번 무작위로 바뀌기 때문에 공격자가 레코딩 공격에 성공하기 위해서는 정확한 사용자 패스워드 지뢰의 위치를 획득하거나 또는 모든 위치의 입력 값을 획득해야 한다. 하지만 공격자입장에서 전자 보다는 후자의 경우가 더 용이하다. 그 이유는 모든 입력 값 중 한 자리의 숫자만 바뀌어도 패스워드 지뢰의 위치는 변경되며, 모든 입력 값이 같은 서로 다른 지뢰배치가 존재하기 때문이다.

공격자가 모든 위치의 인증 값을 알기 위해서는 최소한 XY/M회 이상의 레코딩 공격이 필요하다. 그러나 레코딩 공격을 2회 이상 할 경우 이전에 얻었던 정보와 중복되는 경우가 발생한다. 따라서 XY/M회 공격으로만 모

든 인증 값을 얻을 확률은 극히 낮다. 다음 수식 (2)는 공격자가 레코딩 공격으로 획득한 인증 입력 값의 개수가 S라고 가정 시 새로 얻을 수 있는 인증 값 개수의 평균을 나타낸다.

$$\begin{cases} f_{(0)} = M \\ f_{(S)} = \sum_{N=0}^{M} N \frac{(XY-S)C_N \; {}_S C_{(M-N)}}{{}_{XY}C_M} \end{cases} \quad (2)$$

다음 수식 (3)은 수식 (2)를 이용하여 n회 레코딩 공격 시 얻을 수 있는 입력 값의 개수를 나타낸다.

$$\begin{cases} g_{(0)} = f_{(0)} \\ g_{(n)} = g_{(n-1)} + f_{(g_{(n-1)})} \end{cases} \quad (3)$$

따라서 $g_{(n)} > XY$가 성립하는 최소 n의 크기만큼 레코딩 공격을 시도해야 모든 위치의 입력 값을 획득이 가능하다. 따라서 제안기술에서 X = 4, Y = 5, M = 4 일 때 평균 17회 정도 레코딩 공격을 시도해야 모든 위치의 입력 값이 획득가능하다. 따라서 실제 세계에서 한 사용자에 대한 10여회 이상 반복되는 레코딩 공격은 어려우므로 제안 기술은 레코딩 공격에 안전하다.

5. 사용성 평가

객관적인 사용성 평가를 위해 본 논문에서는 실제 안드로이드폰에 제안 기술을 구현하여 사용자 실험을 실시하였다. 구현에 사용된 개발도구로 Eclipse Helios, Android SDK 2.3, JAVA 1.6.0을 사용하였다.

사용자 실험을 위해 남자 21명 여자 9명 총 30명을 모집하였다. 연령대는 10대 10명, 20대 10명, 30대 5명, 40대 이상 5명으로 구성하였다. 사용자 실험 방법은 패스워드 설정시간, 인증시간을 미리 정해놓은 방법에 따라 각각 5회씩 실행한 후 시간과 인증 에러율을 측정하였다.

<표 4>은 기술별 설정시간 및 인증시간 그리고 에러율을 나타낸다. 실험 결과 평균 패스워드 설정 시간은 기존 기술들에 비해 빠르게 측정 되었다. 사용자 인증의 경우 제안 기술은 평균 19.36초로 PIN-Entry 기술의 즉시 입력 방법에 비해 1.82초 빠르게 측정 되었지만 다른 기술들에 비해서 다소 느리게 측정 되었다. 이는 지뢰의 위치를 찾는 시간이 비교적 많이 소요된 것으로 판단된다. 에러율에서는 평균 8.94%로 비교적 낮은 에러율을 보인다. 실험 결과를 종합해 보면 제안 기술의 패스워드 설정 시간은 기존 기술에 비해 빠르게 측정되었고 사용자 인증 시간은 기존 기술 보다 약간 느리게 측정되었다. 하지만 상대적으로 낮은 에러율을 보여, 실제 사용자들이 제안 기술에 보다 익숙해 졌을 때 보다 높은 사용성을 가질 것을 기대할 수 있다. 또한 텍스트 보다 그림을 더 기억하기 쉬운 점을 이용하여 지뢰의 위치를 특정 도형이나 글자 등의 모양으로 만들어 사용함으로써 기억용이성을 높일 수 있다.

<표 4> 사용성 테스트 결과

		설정 시간(s)	인증 시간(s)	에러율(%)
DAS		14.67	11.56	8.70
PIN-Entry	즉시 입력	18.80	21.18	23.30
	지연 입력		8.35	42.00
Dementor-SGP	1단계	33.33	9.02	5.30
	2단계		19.60	8.70
	3단계		14.69	19.30
Passfaces		111.17	14.55	15.50
제안 기술		12.78	19.36	8.94

6. 결론

본 논문에서는 안전성과 사용성을 모두 만족시킬 수 있는 패스워드 기법으로써 지뢰찾기 게임을 이용한 새로운 패스워드인증 기법을 제안하였다. 제안 기법의 안정성 및 사용성을 실험해 보기위해 실제 안드로이드 폰에 구현 실험을 수행하였으며, 특히 사용성 평가를 위해 사용자 평가를 추가적으로 실시하였다. 실험 결과 제안 기술은 어깨너머 훔쳐보기, 무작위 대입 공격에 안전하며 특히, 레코딩 공격에 또한 안전하다. 사용자 실험 결과 기존 기술들에 비해 높지는 않지만 어느 정도 수긍 가능한 사용성을 보였으며, 대중성 있는 게임을 활용한 측면에서 사용성은 좀 더 높게 평가될 수 있는 여지가 있다. 따라서 제안 기술은 모바일 환경에서 높은 안전성과 동시에 적절한 사용성을 동시에 만족시킬 수 있는 패스워드 기법이라 사료된다.

참고문헌

[1] Oxford University Press, “Shorter Oxford English Dictionary” 6th Ed. Oxford Univ Pr 2007.

[2] C. Paar, J. Pelzl, and B. Preneel, “Understanding Cryptography: A Textbook for Students and Practitioners”, Springer, pp.7, 2010.

[3] V. Roth, K. Richter, and R. Freidinger, “A PIN-Entry Method Resilient against Shoulder Surfing”, ACM Conference on Computer and Communications Security, 2004.

[4] 박승배, “관찰자에게 입력정보가 노출되는 것을 방지할 수 있는 정보입력방법”, 국내특허, 등록번호: 100743854, 2005.

[5] (주)민인포, “그래픽 오티피를 이용한 사용자 인증 방법”, 국내특허, 등록번호: 100844195 , 2008.

[6] Passfaces, http://www.passfaces.com.