멀티터치 환경에서 다중 입력을 통한 패스워드 기반의 사용자 인증

주승환*, 서희석*
*한국기술교육대학교 컴퓨터공학부
e-mail:judeng@kut.ac.kr

A study on password-based user authentication methodology on multi-touch environment

Seung-Hwan Ju*, Hee-Suk Seo*
*School of Computer Science, Korea University of Technology and Education

요 약

현재 타블렛PC, 전자칠판, 디지털 키오스크 단말, 은행 ATM기기 등에서 키보드 및 버튼이 아닌 터치패널을 이용해 사용자가 더욱 직관적인 입력을 할 수 있도록 지원하고 있다. 나아가 이러한 터치패널은 하나의 접점만 인식하는 것이 아닌 현재 기술로 여러 개의 접점을 인식하는 멀티터치 방식을 채택하고 있다. 본 논문에서는 이러한 멀티터치 환경에서의 다중 입력을 통한 사용자 인증 방식에 대한 아이디어를 소개하고자 한다. 멀티터치 환경에서의 비밀 번호 입력으로 이전의 싱글터치 기반에서 1글자씩 입력되던 비밀번호가 멀티터치 기반에서는 2개 이상의 글자로 입력될 수 있다. 멀티터치 기반의 패스워드 입력은 단순히 [1, 2, 3, 4] 로 입력되던 패스워드를 [(1,3), 2, (3,4), (1,2,3)] 와 같은 방식으로 설정함으로써 사용자 패스워드의 암호화 강도를 높이고 패스워드 노출 위험을 줄이려 하였다. 본 연구는 나아가 멀티터치 기반에서 사용자 패스워드를 넘어 개인 인증을 위한 보안 기술 연구의 초석으로 활용 될 것이다.

1. 서론

사용자 인증이란 사용자가 제시한 신분의 타당성을 확인하는 절차이다. 사용자 인증은 보통 3가지 유형으로 이루어진다. 제 1유형 인증 방법은 사용자 지식 기반 인증 방법으로 패스워드와 같이 사용자가 기억하고 있는 정보로 인증하는 방식으로 구현하기 쉬워 가장 널리 사용되고 있다. 제 2유형 인증 방법은 사용자 소유 기반의 인증으로써 스마트카드나 출입카드 등이 속한다. 제 3유형 인증방법으로는 사용자 신체 특징을 이용한 인증으로써 지문과 목소리 인식 등이 그 예이다.

위 방식 중 제 1유형인 패스워드와 같이 지식기반의 인증이 가장 많이 활용되고 있다. 위 세 가지 방식 중 “알고 있는 어떤 것”의 지식기반의 인증보다 “가지고 있는 어떤 것”과 “본인 자체의 어떤 것”의 방식이 보안적인 측면에서 훨씬 더 우수한데도 불구하고 “알고 있는 어떤 것”의 지식기반 인증이 보편화 되어있다. 그 첫 번째 이유는 비용이고, 두 번째 이유는 편리성이다. 스마트카드나 생체인식 장비는 비용이 드는데 비해 패스워드 방식은 비용이 들지 않는다. 또한 과중한 업무에 시달리고 있는 시스템 관리자 입장에서는 새로운 스마트카드를 발급하는 것보다 패스워드를 생성하는 것이 간편하기 때문이다.

이처럼 패스워드를 이용한 사용자 인증 방법이 사용자에게 편리하고 또한 구현이 쉽고 간단하여 많이 활용되고 있다.

하지만 사람은 패스워드를 선정할 때 취약한 패스워드를 선택하는 경향이 있으며 그러한 패스워드는 쉽게 노출된다. 실제로 패스워드를 통해 충분한 보안성을 확보한다는 것이 근본적으로 어렵다는 것은 수학적 논거만으로도 확인할 수 있다.

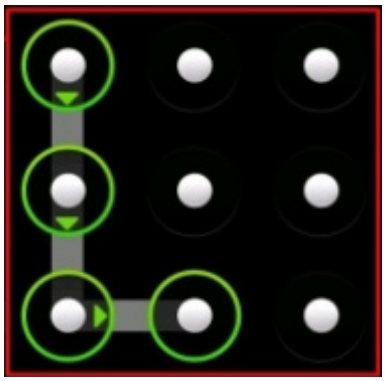
현재 타블렛PC, 은행 ATM기기 등에서 키보드 및 버튼이 아닌 터치패널을 이용해 사용자가 더욱 직관적인 입력을 할 수 있도록 지원하고 있다. 멀티터치 기반에서의 패스워드 입력 방법을 제시함으로써 패스워드의 보안 강도를 강화하고자 한다.

2. 관련 연구 및 기술 동향

모바일 기기 스마트폰을 예로 간단한 소형 기기에서의 사용자 인증 방식에 대해 논하려한다.

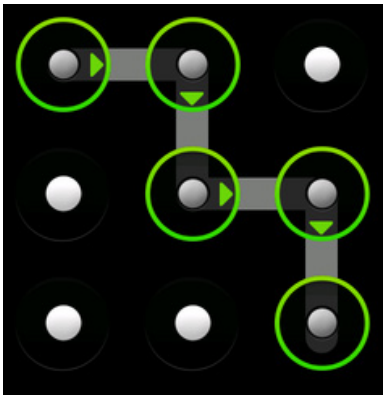
구글의 안드로이드는 패턴 인식을 통해 기존의 암호 대신 일련의 동작을 입력하여 모바일 기기에 비 인가된 사용자의 접근을 방지하고 있다.

이 안드로이드의 패턴인식 방식은 기존의 패스워드 입력 방식의 보안 메커니즘보다 보안성이 떨어진 다는 것을 알 수 있다.



(그림 1) 안드로이드의 패턴 인식

(그림 2) 안드로이드 패턴인식의 예에 나타나 있는 패턴은 기존 패스워드 입력 방식의 [1, 2, 5, 6, 9] 라는 패스워드를 손가락의 패턴으로 입력하도록 하였다. 또한 안드로이드 패턴인식 보안 메커니즘은 [1, 9, 5] 와 같이 멀리 떨어져 있는 번호를 입력할 수 없고 근접한 번호를 거쳐 가야한다는 점에서 안드로이드 패턴인식 보안 메커니즘은 단순히 4글자 패스워드보다는 보안 강도가 높아 보이지만, 최소 1글자부터 최대 9글자를 가질 수 있는 기존의 패스워드 방식과 비교하였을 때 기존의 패스워드 방식보다 보안성이 더 떨어진다는 것을 알 수 있다.



(그림 2) 안드로이드 패턴인식 예

애플 아이폰의 경우 기본 숫자 4자리 패스워드를 요구하지만 사용자의 설정에 따라 영문 대소문자, 숫자 조합으로 패스워드를 입력할 수 있도록 하여 보안 강도를 높이고자 하였다.

하지만 안드로이드와 아이폰의 이러한 보안 메커니즘은 1차원적인 패스워드로써 기본 4자리 패스워드보다는 보안성이 강화되었더라도 여전히 패스워드의 문제점을 갖고 있다. 공격자는 최소 1자리와 최대 9자리라는 것을 알기 때문에 범위가 지정되기 때문이다. 혹 공격자가 패스워드의 길이를 알면 더욱 쉽게 패스워드를 유추할 수 있게 된다.

(그림 3) 애플 아이폰의 인증 메커니즘

3. 멀티 터치 기반의 사용자 인증

멀티터치(Multi-touch)는 터치스크린, 터치패드가 동시에 여러 개의 터치 포인트를 인식하는 기술로, 일반적인 하나의 터치 포인트만 인식을 하는 것보다 더 다양한 조작을 할 수 있다. 현재 정전식 터치 기술이 사용된 터치패드, 터치스크린에서만 적용되는 기술이며, 애플컴퓨터사의 제품들인 아이폰, 아이팟 터치, 맥북, 마이크로소프트의 윈도우즈 7 등 에서 주로 사용되고 있다.

싱글 터치를 통해서 위치 변화만 입력할 수 있었기 때문에 다양한 조작을 위하여 보조 단추 같은 별도의 조작이 필요했던 기존의 터치방식과는 달리, 멀티 터치는 감지되는 터치 포인트의 개수에 따라 터치에 대한 장치의 반응을 지정할 수도 있고 터치 포인트 간격 변화를 통한 조작도 가능하기 때문에 더 직관적이고 쉽고 편하게 조작할 수 있게 되었다. 이렇게 한 번에 여러 터치 포인트를 인식할 수 있는 멀티 터치 환경에 패스워드를 적용함으로써 그 강도를 높이고자 한다.

은행 ATM 기기에서의 사용자 인증은 카드와 기본 숫자 4자리 패스워드로 2단계 보안이었다. 사용자가 가지고 있는 “갖고 있는 어떤 것”의 사용자 소유 기반의 인증과 “알고 있는 어떤 것”의 사용자 지식 기반의 인증으로 이루어진다.

현재 은행 ATM기기에서의 숫자 4자리 패스워드 입력은 아래 (그림 4) 은행 ATM 기기 패스워드 입력 예와 같다.

예제에서는 [1. 9, 3, 0]으로 설정된 이러한 패스워드는 0000부터 9999까지의 패스워드 범위를 가지기 때문에 공격자가 쉽게 유추하고 공격할 수 있다.

또한 요즘 패스워드 입력 시 터치 패널에 지문이 남아 공격자가 쉽게 유추될 수 있다고 경고하고 있는 상황에서 공격자가 패스워드에 사용된 숫자 4개를 알게 된다면 매우 쉽게 공격할 수 있다.

(그림 4) 은행 ATM 기기 패스워드 입력 예

(그림 5) 멀티터치의 예

이렇게 보안 강도가 약한 기존의 숫자 4자리 패스워드를 대신하여 한 번에 여러 숫자를 터치할 수 있는 멀티 터치를 이용하여 이러한 단순 숫자 패스워드의 보안 강도를 높이고자 한다.

기존의 10000가지 경우로 유추 가능하던 싱글터치의 4자리 패스워드를 (그림 5) 멀티 터치의 예와 같이 한 번에 여러 숫자를 터치하여 패스워드를 구성하려 한다.

아래 (그림 6) 멀티 터치를 통한 패스워드 입력 예와 같이 적용한다면 그 경우의 수는 매우 많아 질 것이다.

(그림 6) 멀티 터치를 통한 패스워드 입력 예

(그림 6)에서는 멀티 터치를 통한 사용자 패스워드로 [(0, 1), (5), (7, 8, 9), (2)] 와 같이 패스워드가 구성되어 있다. 이 예에서는 한번에 3개 터치까지 표현하였지만 멀티 터치 기반의 패스워드 입력은 최대 10개까지 멀티터치로 패스워드 입력이 가능하다.

입력의 복잡성을 높여 공격자가 패스워드 입력 광경을 보더라도 쉽게 알 수 없다. 또한 한 번에 여러 개의 터치가 이루어지기 때문에 패스워드를 유추하기에도 어렵다.

4. 멀티 터치 패스워드의 보안 강도

아래 <표 1> 멀티터치 기반의 1자리 숫자 패스워드 경우의 수 에서 보는 것과 같이 멀티 터치 기반의 1자리 숫자로 이루어진 패스워드는 $\sum_{i=1}^{10} {}_{10}C_i$ 로, $1024 = 2^{10}$ 개의 경우를 갖는다.

<표 1> 멀티터치 기반의 1자리 패스워드 경우의 수

멀티터치 기반의 1자리 숫자 패스워드가 갖는 경우의 수		
1-터치	${}_{10}C_1$	1
2-터치	${}_{10}C_2$	10
3-터치	${}_{10}C_3$	45
4-터치	${}_{10}C_4$	120
5-터치	${}_{10}C_5$	210
6-터치	${}_{10}C_6$	252
7-터치	${}_{10}C_7$	210
8-터치	${}_{10}C_8$	45
9-터치	${}_{10}C_9$	10
10-터치	${}_{10}C_{10}$	1
총	$\sum_{i=1}^{10} {}_{10}C_i$	1024

만약 멀티터치 기반의 패스워드로 4자리 숫자 패스워드를 구성한다면 $(2^{10})^4 = 2^{40}$ 개의 경우의 수를 갖게 되므로 C프로그래밍에서 int(integer) 자료형의 범위보다 많아진다. <표 2> 패스워드 별 경우의 수 비교에서 멀티 터치 도입으로 인한 보안성 강화에 대해 설명하고 있다.

<표 2> 패스워드 별 경우의 수 비교

1자리 숫자 패스워드가 갖는 경우의 수		
일반적인 숫자 패스워드		10
멀티 터치	공격자가 r단계 멀티터치인지 아는 경우	${}_{10}C_r$
	공격자가 아무런 정보를 갖지 못하는 경우	1024

5. 결론 및 기대효과

터치패널은 하나의 접점만 인식하는 것이 아닌 현재 기술로 여러 개의 접점을 인식하는 멀티터치 방식이 대두되고 있다. 본 논문에서는 이러한 멀티터치 환경에서의 다중 입력을 통한 사용자 인증 방식에 대한 아이디어를 소개하였다. 멀티터치 환경에서의 비밀 번호 입력으로 이전의 싱글터치 기반에서 1글자씩 입력되던 비밀번호가 멀티터치 기반에서는 2개 이상의 그룹으로 입력될 수 있다. 멀티터치 기반의 패스워드 입력은 단순히 [1, 2, 3, 4] 로 입력되던 패스워드를 [(1,3), 2, (3,4), (1,2,3)] 와 같은 방식으로 설정함으로써 사용자 패스워드의 암호화 강도를 높이고 입력의 복잡성를 향상 시킴으로써 패스워드 노출 위험을 줄이려 하였다. 제안하고자 하는 멀티 터치 기반의 패스워드 방식의 인증은 현재 상용되고 있는 One-Time Password(OTP) 등과 함께 사용되어 더 좋은 보안 성능을 나타낼 수 있을 것이다. 본 연구는 나아가 멀티터치 기반에서 사용자 패스워드를 넘어 개인 인증을 위한 보안 기술 연구의 초석으로 활용 될 것이다.

참고문헌

[1] Roger S. Pressman "Software Engineering A Practltiners' Approach" 3rd Ed. McGraw Hill

[1] Wikipedia : Multi-touch, http://en.wikipedia.org/wiki/Multi-touch

[2] Bill Buxton, "Multi-Touch Systems that I Have Known and Loved", Microsoft Research, October 2009

[3] Chitiz Mathema, "멀티-터치 올-포인트 (Multi-Touch All-Point) 터치 스크린:유저 인터페이스 디자인의 미래", Cypress Semiconductor Corp, July 2009

[4] http://code.google.com/android/

[5] http://www.apple.com