한국시뮬레이션학회 논문지
Vol. 20, No. 1, pp. 39-49 (2011. 3)

멀티터치 환경에서의 다중 입력을 통한 패스워드 기반의 사용자 인증 기법

주승환[1] · 서희석[1†]

Password Based User Authentication Methodology Using Multi-Input on Multi-Touch Environment

Seung-hwan Ju · Hee-suk Seo

ABSTRACT

Nowaday, Many equipments like TabletPC, Digital kiosk, ATM using touch-panel service instead of keyboard or button, to support intuitively input for user. Furthermore these days touch-panels recognize up to 5 contact points using recent technology. On this study, I Introduce password input/store methodology on multi-touch environment. On past, User must input password 1 character by 1 character, like [1, 2, 3, 4]. but, on multi-touch environment user can input more than one character at the same time, like [(1,3), 2, (3,4), (1,2,3)]. In result, users can use password more intensely. This study is utilized post security technology study on multi-touch environment.

Key words : Multi-touch, Password, User authentication

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 개 접점을 인식하는 멀티터치 방식을 채택하고 있다. 본 연구에서는 이러한 멀티터치 환경에서의 비밀번호 입력 및 저장방식에 관한 아이디어를 소개하고 시뮬레이션 해보았다. 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 같이 동시에 여러 숫자를 입력하는 방식으로 설정함으로써 사용자 패스워드의 보안 강도를 높였다. 또한 사용자로 하여금 패스워드 입력의 복잡성을 높여 패스워드의 물리적 노출 위험을 줄이려 하였다. 본 연구는 나아가 멀티터치 기반에서 사용자 인증을 위한 보안 기술 연구의 초석으로 활용 될 것이다.

주요어 : 멀티터치, 패스워드, 사용자 인증

1. 서 론

1.1 사용자 인증 및 인증 방식

사용자 인증이란 사용자가 제시한 신분의 타당성을 확인하는 절차이다. 기계가 사람을 인증하는 문제이다. 이러한 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 패스워드는 “the knowledge factors”인 제 1유형의 예가 된다. 제 1유형인 패스워드와 같이 지식기반의 인증이 가장 많이 활용되고 있다. 위 세 가지 방식 중 “the knowledge factors”의 지식기반의 인증보다 “the

*이 논문은 2010년도 정보(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2010-0021951).
접수일(2011년 1월 5일), 심사일(1차 : 2011년 3월 12일), 게재 확정일(2011년 3월 28일)
[1] 한국기술교육대학교 컴퓨터공학과
주 저 자 : 주승환
교신저자 : 서희석
E-mail; histone@kut.ac.kr

표 1. 사용자 인증 방법

the knowledge factors	Something the user **knows**
the ownership factors	Something the user **has**
the inherence factors	Something the user **is** or **does**

ownership factors"과 "the inherence factors"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 오늘날 정보보안 시스템에 있어 상당히 취약한 연결고리가 되고 있다는 것이 일반적인 인식이다. 이상적인 패스워드는 사용자가 그것을 알고 있어야 하는데 사용자가 알고 있다는 것을 컴퓨터가 검증 할 수 있어야 함을 의미 한다. 그리고 공격자는 컴퓨터의 자원을 무제한 사용하더라도 그것을 알아 낼 수 없어야 한다. 하지만 현실적으로는 이러한 이상적인 상황에 근접하는 것조차 어렵다.

사용자가 그것을 알고 있어야 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.

1.2 패스워드 시스템의 보안적 위협

패스워드 시스템의 보안적 위협이란 사용자의 패스워드가 불법적으로 노출되는 것을 말한다. 시스템에 침입하려는 공격자는 아래의 세 가지 방법으로 사용자의 패스워드를 알아 낼 수 있다[1].

첫째, 시스템의 패스워드 파일을 읽어내는 방법이 있다. 패스워드 파일은 사용자들의 패스워드와 식별자를 저장한 파일로써 만약 노출되면 시스템과 모든 사용자들의 자료는 위험에 빠지게 된다. 따라서 패스워드 파일은 일반 사용자에게 접근을 제한하며 오직 보안 관리자만이 권리를 갖게 한다. 그러나 시스템의 고장이나 보안관리자가 악의적으로 패스워드 파일을 노출시킨 경우에 이러한 패스워드 시스템은 전혀 안전하지 못하다. 보다 확실한 방법은 패스워드를 일방함수를 통해 그 결과를 식별자와 함께 파일을 저장하여 패스워드 파일이 노출되더라도 사용자 패스워드를 안전하게 유지하는 것이다. 이 방법은 입력된 패스워드에 일방함수를 적용하여 그 결과를 저장된 것과 비교함으로써 사용자 인증을 한다.

둘째, 사용자와 시스템 간에 패스워드를 주고 받는 통신을 도청 할 수 있다. 만약 보안 관리자가 패스워드 시스템의 도청 위험이 크다고 판정하면 통신되는 패스워드는 입력 장소에서 암호화되어 비교 장소까지 전달되는 방법을 취해야 한다.

셋째, 패스워드가 부주의하게 만들어져 쉽게 추측할 수 있는 경우이다. 실제로 사용자들은 자신들과 연관되거나 흔히 사용하는 단어를 패스워드로 선택하는 경우가 많으므로 패스워드의 추측이 용이한 경우가 많다. 패스워드의 추측을 어렵게 하려면 사용자가 보다 무작위하게 선택하거나 자동으로 시스템에서 패스워드를 무작위하게 만들어주는 방법이 있다[2].

본 논문에서는 패스워드가 단순하여 쉽게 추측할 수 있거나 물리적으로 패스워드를 쉽게 얻을 수 있는 보안 위협에 대해 보안성을 강화하고자 하였다.

2. 멀티-터치 터치스크린 기술 동향

사용자 인터페이스(UI) 분야의 성배는 장치를 다루는 데 있어서 중요한 감각인 시각과 촉각을 가장 효과적이고 직관적으로 이용하여 최적의 사용자 경험을 창출해내는 UI를 개발하는 것이라고 할 수 있다.

효과적인 상용 장치들의 대다수는 이 두 감각을 본질적으로 별개의 것으로 다루는 경우가 많다. 터치스크린이 하는 일은 바로 매우 기초적인 수준에서 시각과 촉각을 같은 목적으로 다루는 것이다[3].

이것은 기초적인 개념처럼 보이지만 사실은 사용자들과 전자장치 간의 상호작용 방법에 혁명을 가져오고 있는 커다란 혁신으로서, 때로는 UI 혁명이라고도 불리고 있다.

터치스크린의 투명성은 새로운 사용자 인터페이스 디자인을 가능케 해준다. 사용자는 디스플레이 내의 다양한 콘텐츠를 직접 "만질 수" 있기 때문이다. 전자 장치 주변부에 이런 저런 버튼을 두는 대신에 이제는 장치의 어떠한 어플리케이션과 직접 상호작용할 수 있다[4].

물론 전에도 컴퓨터 마우스와 트랙패드로 화면상의 어플리케이션들 사이를 돌아다닐 수는 있었지만, 디스플레

이를 실제로 만짐으로써 화면 및 그 안의 어플리케이션들과 하나가 되었던 것은 아니었다.

모든 종류의 행동이나 제스처들을 단지 디스플레이를 만지는 것만으로 실현할 수 있도록 해줌으로써 터치스크린은 근본적으로 디스플레이에 생명을 부여한다[5].

2.1 싱글-터치 터치스크린

터치스크린의 위력이 제일 먼저 발휘된 것은 그 가장 간단한 형태, 즉 화면상의 한 지점을 손가락 하나로 터치하는 것이었다. 이제 싱글터치 터치스크린에서는 사용자 제어 인터페이스를 화면 자체에 직접 통합시킴으로써 기존의 사용자 제어용 기계식 버튼을 필요 없게 만들었다.

이는 사용자 인터페이스에 두 가지 주요 이점을 가져다준다. 첫째는 특히 작은 장치들에 있어서 설계 공간이 최적화되어 화면과 버튼을 동일한 공간에 집어넣을 수 있다는 점이다. 둘째는 장치가 "버튼들"을 얼마든지 가질 수 있다는 것이다. 버튼을 장치의 운영체제 내에 있는 어떠한 어플리케이션과도 연계되도록 할 수 있기 때문이다.

주로 터치스크린 기술을 토대로 하는 이러한 기능은 가전 장치, 공항의 키오스크, 잡화점의 POS 단말기, 자동차용 GPS 시스템 등에서 매우 널리 사용되게 되었다.

2.2 멀티-터치 터치스크린

싱글터치 터치스크린과 여기에 사용된 터치스크린 기술은 분명 놀랍고 혁신적이긴 하지만 두 가지 중요한 단점이 있었다.

첫째, 싱글터치 터치스크린 기술은 터치스크린의 작지만 물리적인 움직임에 의존했다는 점이다. 이는 사용에 따른 정상적인 마모로 인해 성능 저하를 야기하는 것으로 밝혀졌다.

둘째, 싱글터치만이 가능했다. 즉, 특정 화면상에서 한 번에 단지 하나의 손가락으로 한 가지 일만을 할 수 있었던 것이다. 장치의 사용자 상호작용을 손가락 하나로만 제한할 이유가 없다. Apple社가 투영 정전용량(Projected Capacitive) 기술 기반의 터치스크린 아이폰으로 사용자 인터페이스의 혁명에 기념비적인 기여를 한 것이 바로 이 부분이다. 스마트폰처럼 작은 장치에서도 어플리케이션과 운영체제에 담긴 기능들에 최적의 사용성을 부여하기 위해서는 여러 손가락의 사용이 요구된다. 이제는 Apple사 덕분에 한 손가락 및 두 손가락 제스처로 그림 크기나 사진 앨범, 웹페이지 등의 방향을 마음대로 바꿀 수 있게 되었다.

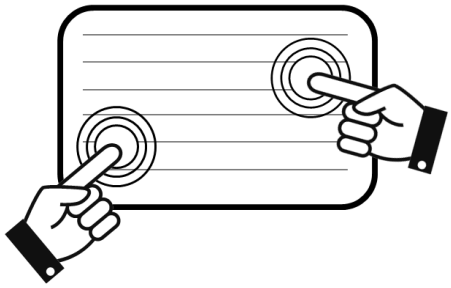


그림 1. 멀티-터치 터치스크린

2.3 터치 기반 UI의 시장성

유명한 미래학자인 Ray Kurzweil은 10년 전에 2009년이 되면 대부분의 포터블 컴퓨터에서 키보드가 없어질 것이라고 예언을 한 바 있다. 결과적으로 그의 예언은 틀렸다. 아직도 노트북 컴퓨터의 키보드는 기본이니 때문이다. 그렇지만 완전히 틀렸다고 할 수 없는 것이 각종 모바일 기기의 등장과 함께 나타난 터치기반 스마트 폰의 약진은 실제로 주된 입력의 기반이 키보드에서 동작이나 터치 등과 같은 것으로 주도권이 넘어갈 수 있음을 충분히 보여주고 있기 때문이다.

이미 터치기반 입력 기술은 우리 생활에 너무 익숙해지고 있다. 대부분의 ATM 기기나 많이 사용되는 네비게이션 기기 등은 터치스크린을 이용해서 내용을 입력하는 것이 기본으로 되었다. 이러한 인터페이스들이 기본적으로 단일 터치를 바탕으로 진행이 되었다면, 지난 수년 간 돌풍을 일으킨 애플社의 모바일 기기들은 향후 나타나게 될 멀티터치 인터페이스의 세상을 일찌감치 예고하고 있다.

3. 모바일 기기의 사용자 인증 기법

3.1 구글 안드로이드의 사용자 인증

구글社의 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 방식과 거의 같은 방식이며, 오히려 기존의 패스워드 입력 방식의 보안 메커니즘보다 보안성이 떨어진다.

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 가

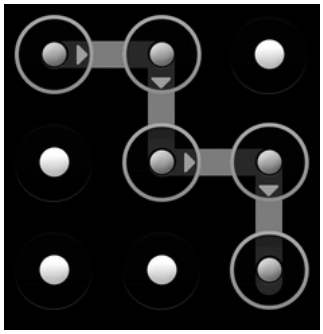


그림 2. 안드로이드 패턴 인식 예

그림 3. iPhone 사용자 인증

야한다는 점에서 안드로이드 패턴인식 보안 메커니즘은 기존의 패스워드 방식보다 보안성이 더 떨어진다는 것을 알 수 있다.

3.2 애플 iPhone의 사용자 인증

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

하지만 안드로이드와 iPhone의 이러한 보안 메커니즘은 1차원적인 패스워드로써 기본 4자리 패스워드보다는 보안성이 강화되었더라도 여전히 패스워드의 문제점을 갖고 있다.

iPhone의 사용자 인증 패스워드는 최소 1자리와 최대 9자리라는 범위가 있기 때문이다. 공격자는 이 패스워드 범위를 통해 전사공격을 시도 할 수 있고, 혹 공격자가 패스워드의 정확한 길이를 알면 더욱 쉽게 패스워드를 유추할 수 있게 된다.

4. 멀티-터치 기반의 패스워드

4.1 멀티 터치 기술

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.

최근 인터페이스의 흐름은 멀티터치가 대세를 이루어 가고 있다. 손을 이용한 멀티터치는 자연스러운 사용자 참여를 유도할 수 있어, 컴퓨팅 환경을 처음 접하는 사용자들의 참여를 유도하는데 아주 좋은 인터페이스이다. 애플(Apple Inc.)의 아이폰, 아이팟 터치, 맥북(iPhone, iPod Touch, MacBook Air)등으로 대중에게 선보인 멀티터치 기술은 2006년 TED(Technology Entertainment Design) 컨퍼런스에서 컴퓨터 공학자 재미교포 2세 제프 한(Jefferson Y. Han)에 의해서 선보였다. 제프 한이 보여준 전반사 장애(FTIR:Frustrated Total Internal Reflection)현상을 이용한 기술은 상당한 반응을 일으켰고 많은 연구자들에게 영향을 끼쳤다.

이렇게 한 번에 여러 터치 포인트를 인식할 수 있는 멀티 터치 환경에 패스워드를 적용함으로써 그 강도를 높이고자 한다.

4.2 제안하는 멀티터치 기반 패스워드

현재 많이 사용되고 있는 숫자 4자리 패스워드 입력은 아래 그림 4. 숫자 패스워드 입력 예와 같다.

그림 4에 [6. 2, 8, 3]으로 설정된 이러한 패스워드는 0000부터 9999까지의 10000개의 패스워드 범위를 가지기 때문에 공격자가 모든 경우의 수를 대입하는 전사 공격을 통해 패스워드를 크래킹 할 수 있으며, 4자리 숫자

그림 4. 숫자 패스워드 입력 예

그림 5. 멀티 터치의 예

임을 고려해 사용자 정보로부터 공격자가 쉽게 유추하고 공격할 수 있다.

요즘 터치스크린 패스워드와 관련 된 보안 문제점에 대해 발표되고 있다. 입력한 패스워드가 전송되는 네트워크 상의 프로토콜이나 기기 자체의 애플리케이션 취약점이 아닌 물리적인 취약점도 발표되고 있다. 패스워드 입력 시 터치스크린에 지문 자국이 남아 공격자가 쉽게 유추할 수 있다고 경고하고 있는 상황이다. 다시 말하면 공격자가 터치스크린에 남은 지문 자국을 이용해 패스워드에 사용된 숫자 4개가 어떤 건지 알게 된다면 그 4가지 숫자 배열순서만 바꿔 시도함으로써 최대 4 ! = 24번 안에 매우 쉽게 공격할 수 있다.

또한 일반적인 경우에도 정상 사용자가 패스워드를 입력하는 것을 공격자가 엿볼 수 있다면 입력이 단순한 일반 패스워드는 쉽게 유추 될 수 있다.

이토록 숫자로 이루어진 4자리 패스워드는 프로토콜과 애플리케이션의 보안성 외에도 많은 문제점이 지적되고 있다. 이처럼 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.

기존에는 1자리에 10가지 경우로 유추 가능하던 싱글 터치 패스워드를 그림 5. 멀티 터치의 예와 같이 한 번에 여러 숫자를 터치하여 패스워드를 구성하려 한다. 그림 5. 멀티터치의 예는 동시에 여러 개의 입력을 받는 것을 표현한 그림이다. 그림에서는 2와 4가 동시에 터치되었음을 나타내고 있다. 이렇게 멀티터치를 이용한 패스워드는 1

표 2. 2단계 멀티터치 1자리 패스워드의 조합

(0, 1)	(0, 2)	(0, 3)	(0, 4)	(0, 5)	9개
(0, 6)	(0, 7)	(0, 8)	(0, 9)		
(1, 2)	(1, 3)	(1, 4)	(1, 5)	(1, 6)	8개
(1, 7)	(1, 8)	(1, 9)			
(2, 3)	(2, 4)	(2, 5)	(2, 6)	(2, 7)	7개
(2, 8)	(2, 9)				
(3, 4)	(3, 5)	(3, 6)	(3, 7)	(3, 8)	6개
(3, 9)					
(4, 5)	(4, 6)	(4, 7)	(4, 8)	(4, 9)	5개
(5, 6)	(5, 7)	(5, 8)	(5, 9)		4개
(6, 7)	(6, 8)	(6, 9)			3개
(7, 8)	(7, 9)				2개
(8, 9)					1개
총 경우의 수 : $_{10}C_2 = 45$					

자리 멀티터치 패스워드라도 45개의 경우의 수를 갖는다.

표 2. 2단계 멀티터치 1자리 패스워드의 조합에서는 동시에 두 개를 터치하는 2단계 멀티터치의 1자리 패스워드의 모든 경우를 나타내고 있다. 동시에 두 개를 터치하기 때문에 같은 숫자로 이루어진 숫자 쌍을 이룰 수 없으며, 순서가 다른 같은 순서쌍은 같은 것으로 판단하였다. 예를 들어 (1, 3)과 (3, 1) 모두 1과 3을 동시에 터치한 것이다.

4.2.1 은행 ATM 기기 패스워드에 멀티터치 적용

터치스크린을 이용하여 패스워드를 입력하는 것은 은행 ATM 기기가 대표적이다. 은행 ATM 기기에 적용한 멀티터치 패스워드에 대해 알아보고자 한다.

현재 은행 ATM 기기에서의 사용자 인증은 카드와 기본 숫자 4자리 패스워드로 두 가지 보안 방법을 활용하고 있다. 이 두 가지는 사용자가 가지고 있는 카드를 이용한 “갖고 있는 어떤 것”의 사용자 소유 기반의 인증과 패스워드를 이용한 “알고 있는 어떤 것”의 사용자 지식 기반의 2-factor 인증으로 이루어진다.

이 패스워드는 0000부터 9999까지의 10000개의 패스워드 범위를 가지기 때문에 공격자는 패스워드가 4자리 숫자임을 고려해 사용자 생일이나 휴대 전화번호 등의 정보로부터 공격자가 쉽게 추측하고 공격할 수 있다. 또한 모든 경우의 수를 대입해보는 전사공격에도 취약점을 가진다.

그림 6. 멀티 터치를 통한 4자리 패스워드 입력 예

기존의 10000가지 경우로 유추 가능하던 싱글터치의 4자리 패스워드를 그림 6. 멀티 터치를 통한 4자리 패스워드 입력 예와 같이 한 번에 여러 숫자를 터치하여 패스워드를 구성하려 한다.

기존의 10000가지 경우로 유추 가능하던 싱글터치의 4자리 패스워드를 그림 6. 멀티 터치를 통한 4자리 패스워드 입력 예와 같이 한 번에 여러 숫자를 터치하여 패스워드를 구성하려 한다.

위 그림 6. 멀티 터치를 통한 4자리 패스워드 입력 예와 같이 패스워드 정책을 적용한다면 그 경우의 수는 매우 많아 질 것이다.

그림 6. 멀티 터치를 통한 4자리 패스워드 입력 예에서는 멀티 터치를 통한 사용자 패스워드 입력에서 음영 처리된 부분이 동시에 터치되는 접점이다. 그림 6. 멀티 터치를 통한 4자리 패스워드 입력 예는 멀티터치 4자리 패스워드이다. 1자리는 1과 0이 동시에 터치 된 것이고, 2자리는 5, 3째 자리는 7, 8, 9가 동시에 터치 된 것이고, 또 4째 자리는 2만 터치 된 것이다. 이렇게 한 번에 여러 개 터치 된 것은 [(0, 1), (5), (7, 8, 9), (2)]로 나타낸다. 이 예에서는 한번에 3개 터치까지 표현하였지만 멀티 터치 기반의 패스워드 입력은 최대 10개까지 멀티터치로 패스워드 입력이 가능하다.

입력의 복잡성을 높여 사용자가 패스워드 입력하는 모습을 공격자가 보더라도 쉽게 알 수 없다. 또한 한 번에 여러 개의 터치가 이루어지기 때문에 패스워드를 추측/유추하기에도 어렵다.

4.3 멀티터치 기반 패스워드의 보안성

4.3.1 다중 입력을 통한 패스워드 경우의 수

표 3. 멀티터치 기반의 1자리 숫자 패스워드 경우의 수에서와 같이 멀티 터치 기반의 1자리 숫자로 이루어진 패스워드는 식 (1)과 같으며, 총 $1023 = 2^{10} - 1$개의 경우를 갖는다. 본 논문에서는 동시에 눌리는 접점의 개수, 즉 동시에 r개를 터치하는 것을 'r단계 멀티 터치'라 한다.

표 3. 멀티터치 기반의 1자리 패스워드 경우의 수

멀티터치 기반의 1자리 숫자 패스워드가 갖는 경우의 수		
1단계 멀티 터치	$\frac{10!}{(10-1)!\,1!} = {}_{10}C_1$	10
2단계 멀티 터치	$\frac{10!}{(10-2)!\,2!} = {}_{10}C_2$	45
3단계 멀티 터치	$\frac{10!}{(10-3)!\,3!} = {}_{10}C_3$	120
4단계 멀티 터치	$\frac{10!}{(10-4)!\,4!} = {}_{10}C_4$	210
5단계 멀티 터치	$\frac{10!}{(10-5)!\,5!} = {}_{10}C_5$	252
6단계 멀티 터치	$\frac{10!}{(10-6)!\,6!} = {}_{10}C_6$	210
7단계 멀티 터치	$\frac{10!}{(10-7)!\,7!} = {}_{10}C_7$	120
8단계 멀티 터치	$\frac{10!}{(10-8)!\,8!} = {}_{10}C_8$	45
9단계 멀티 터치	$\frac{10!}{(10-9)!\,9!} = {}_{10}C_9$	10
10단계 멀티 터치	$\frac{10!}{(10-10)!\,10!} = {}_{10}C_{10}$	1
총	$\sum_{i=1}^{10} {}_{10}C_i$	1023

$$\sum_{i=1}^{10} {}_{10}C_i \tag{1}$$

멀티터치 기반의 패스워드로 4자리 숫자 패스워드는 $(2^{10})^4 - 4\times(2^{10})^3 + 6\times(2^{10})^2 - 4\times(2^{10}) + 1 = (2^{10}-1)^4$개의 경우의 수를 갖게 되므로 C언어에서 int(integer) 자료형의 범위보다 많아진다.

이처럼 1자리 멀티터치 숫자 패스워드에서 1023개의 경우의 수를 갖는다. 현재 애플 iPhone의 보안 매커니즘과 마찬가지로 영문 대/소문자와 숫자를 모두 지원하는 경우에는 패스워드의 경우의 수가 더욱 많아져 보안을 강화 할 수 있다. 영문대/소문자와 숫자를 모두 지원하는 경우의 조합의 개수는 더욱 많아진다.

4.3.2 멀티터치 패스워드의 전사공격 보안성

멀티 터치를 이용한 패스워드는 조합 가능한 경우의 수가 많다. 그러므로 전사공격에 대해 높은 보안성을 갖는다.

멀티터치 패스워드를 전사공격 프로그램을 통해 실험하였다. 실험한 전사공격 프로그램은 암호가 걸린 ZIP 파

표 4. 일반적인 숫자 패스워드

일반적인 숫자 패스워드 크랙에 걸린 시간(ms)					
	1차 실험	2차 실험	3차 실험	4차 실험	평균
1자리	7	7	8	8	7.5
2자리	11	11	10	14	11.5
3자리	11	11	15	15	13
4자리	20	17	16	15	17
5자리	20	16	17	17	17.5
6자리	26	25	28	25	26
7자리	119	121	126	117	120.7
8자리	2054	2055	2442	2364	2228

표 5. 일반적인 영문+숫자 조합 패스워드

영문+숫자 패스워드 크랙에 걸린 시간(ms)				
	1자리	2자리	3자리	4자리
1차 실험	10	15	17	92
2차 실험	14	15	15	82
3차 실험	16	13	16	43
4차 실험	14	16	18	78
평균	13.5	14.75	16.5	73.75

일을 전사 공격, 사전 입력 공격으로 암호를 푸는 프로그램으로 주로 암호를 잊어버린 ZIP 확장자의 압축 파일의 패스워드를 해제하는데 사용한다.

전사 공격은 대문자, 소문자, 숫자, 키보드로 입력 가능한 특수문자, 공백을 선택하여 공격이 가능하며 문장의 길이를 알고 있다면 문장의 길이 역시 선택 가능하다.

해당 프로그램으로 전사 공격을 수행 할 경우 초당 2천만 개의 패스워드를 순차적으로 입력하여 암호를 풀어낸다. 예로 4자리 영문/숫자 패스워드를 크랙 한 결과 9,466,719 개의 패스워드를 대입하여 445ms 만에 패스워드 “nstl”을 알아냈다.

이 프로그램을 통하여 일반적인 숫자 패스워드, 영문+숫자 조합 패스워드, 멀티터치 숫자 패스워드의 분석 시간에 대해 실험하였다.

표 4 일반적인 숫자 패스워드에서는 패스워드 길이 별 패스워드 크랙 시간을 나타내고 있다. 각 패스워드 길이마다 총 4번의 실험을 하였고, 패스워드가 가질 수 있는 전체 범위를 4등분 하여 패스워드를 설정하였다.

4자리 숫자 패스워드는 17ms 만에 크랙되는 것을 확인 할 수 있었으며, 7자리부터 100ms 이상 걸리는 것을 실험으로 알 수 있었다.

표 6. 멀티터치 숫자 패스워드

멀티터치 숫자 패스워드 크랙에 걸린 시간(ms)				
	1자리	2자리	3자리	4자리
1차 실험	11	109	95955	4870234
2차 실험	11	112	87354	4794842
3차 실험	15	114	90542	4804562
4차 실험	15	109	94236	4902646
평균	13	111	92021	4843071

표 5. 일반적인 영문+숫자 패스워드에서는 패스워드 길이 별 영문+숫자 조합 패스워드의 크랙 시간을 나타내고 있다. 영문 대소문자와 숫자의 62개 조합이 되는 이 패스워드 방식은 3자리까지는 일반적인 숫자 패스워드와 크랙에 걸리는 시간이 비슷하다가 5자리부터 급격히 시간이 많이 걸리는 것을 알 수 있었다.

표 6 멀티터치 숫자 패스워드에서는 패스워드 길이 별 멀티터치 숫자 패스워드의 크랙 시간을 나타내고 있다. 한 자리 당 1023개의 조합을 갖는 이 패스워드 방식은 2자리 패스워드 크랙에 0.1초를 소요하였고, 3자리는 92초 약 1분 30초, 4자리 패스워드는 4843초로 약 1시간 20분을 소요하였다.

5. 시뮬레이션 및 구현

5.1 DEVS 방법론

B.P. Zeigler가 제안한 이산 사건 시스템 명세(discrete event system specifications; 이하 DEVS)는 계층적이고 모듈화 된 이산 사건 시스템을 표현하기 위한 방법론으로서, 집합이론을 기반으로 체계적으로 정립된 형식론이다. DEVS에서 대상 시스템은 시간을 기반으로 하는 입력, 상태, 출력, 상태 변환 함수들로 표현되며, 함수들은 현재 상태와 입력을 근거로 하여 다음 상태와 출력을 결정하게 된다. DEVS 형식론에서 시스템을 기술하기 위한 두 가지 모델 유형, 기본(basic)모델과 결합(coupled) 모델이 있다. 기본 모델(M)은 시스템의 동작(behavior)의 단위가 되는 시스템의 구성 요소들을 표현하기 위한 것이고, 결합 모델(DN)은 시스템의 구성 요소 간의 상호작용을 의미하는 구조(structure)를 표현하기 위한 것이다.

5.2 멀티 터치 패스워드 시스템 모델링

멀티터치 시스템(Multi-touch System)은 터치스크린, 터치 패드를 활용하여 동시에 여러 개의 터치를 인식하고,

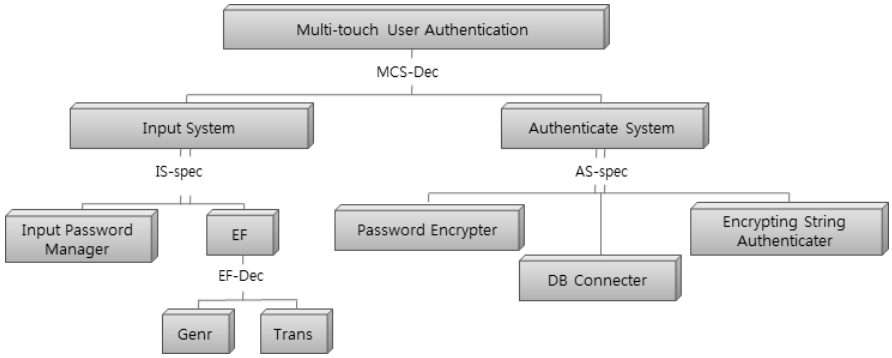


그림 7. 멀티 터치 패스워드 시스템 모델링 구조

인식한 정보를 바탕으로 사용자의 요구사항을 분석, 해당하는 요구사항을 실행 후 그 결과를 사용자에게 보여주는 일련의 행동이라고 할 수 있다.

그림 7은 멀티 터치 패스워드 시스템 모델링의 구조이다.

멀티터치 패스워드 시스템은 크게 Input System과 Authenticate System으로 구성된다.

Input System은 사용자가 터치 패드를 이용해서 입력하는 패스워드를 관리하기 위한 시스템 모듈로서 내부적으로 Input Password Manager과 EF 모델을 포함하고 있다. EF는 모델은 사용자가 패스워드를 입력할 때, Input Password Manager의 내부 상태를 바꿔 사용자가 입력한 패스워드를 관리할 수 있도록 해 준다.

Authenticate System은 사용자가 입력한 패스워드에 대한 인증 작업을 수행하는 모델이다. 하위에 Password Encrpter, DB Connecter와 Encrypting String Authenticater로 구성이 된다.

사용자가 입력한 값이 네트워크를 통해 전송되어 비교를 수행하게 된다면 네트워크 전송 과정에서 스니핑을 통해 사용자가 입력한 패스워드를 도청 당할 경우를 대비하여 Password Encrypter을 통해 네트워크를 통한 전송과정 이전에 사용자가 입력한 패스워드를 암호화 한다. 또한, 리눅스 시스템에서 사용자 계정의 패스워드는 일방향성 함수를 통해서 암호화 되어서 저장된다. 멀티 터치 패스워드 시스템에서도 이러한 부분을 지원하기 위해서 일방향성 암호화를 진행한다.

DB Connecter에서는 원격지에 떨어져있는 패스워드 저장소에 접속하기 위해 사용되는 모델이다. 사용자가 처음 패스워드를 설정할 때 저장된 패스워드 값을 획득하기 위해여 사용되는 모듈이다.

Encrypting String Authenticater은 사용자가 입력한 패스워드와 이전에 설정해 놓은 패스워드를 비교하기 위해 사용되는 모델이다. 사용자가 입력한 패스워드를 Password Encrypter로 암호화한 결과 값과 DB Connecter을 통해 가지고온 사용자가 이전에 설정한 패스워드를 서로 비교하게 된다.

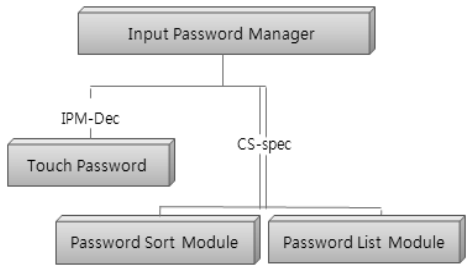


그림 8. Input Password Manager 모듈 구조

Input System 하위에 존재하는 Input Password Manager는 사용자가 입력하는 패스워드를 관리 하게 사용되는 모듈로 하위에는 Touch Password와 Password Sort Module 그리고 Password List Module 가 존재한다.

Password Sort Module은 사용자가 입력한 패스워드를 오름차순으로 정렬을 실행 한다. 예를 들어 사용자가 멀티 터치를 이용하여 입력한 값이 (5, 2)인 경우 (2, 5)으로 정렬을 수행한다. 즉 Input Password Manager은 (2, 5)와 (5, 2)를 같은 값으로 처리하게 된다.

Password List Module은 멀티 터치로 사용자가 입력한 패스워드를 하나의 리스트로 만들어 준다. 예를 들어 사용자가 처음 터치로 1-6-2, 그리고 다음 터치로 4-1를 입력한 경우 Password Sort Module에서 오름차순으로 정렬이 되고 Password List Module에서 (1, 2, 6), (1, 4)로 리스트화 된다.

Password Encrypter 하위에는 일방향성 함수를 적용할 Password와 일방향성 함수에서 Key로 사용된 값을 생성해 주는 Key generator 그리고 key generator에서 생성된 값으로 password을 암호화시킬 one-way Function Module가 존재 한다.

Password는 사용자가 입력하는 패스워드로 그 길이는 사용자가 몇 자리의 패스워드를 입력했는지에 따라 달라진다.

Key generator에서는 이 password을 각각의 값을 모두 반영한 키를 생성해 내게 된다.

one-way Function Module에서는 Key generator에서 생성된 key값을 이용하여 사용자에게 입력받은 전체 패스워드에 대하여 일방향성 함수를 적용시켜 암호화 하는 기능을 담당하게 된다.

Encrypting String Authenticater은 사용자에게 입력받아 암호화가 된 b패스워드와 사용자가 이전에 설정해 놓은 패스워드를 비교하여 인증 작업을 수행한다. 내부에는 Encrypt Password, Set password, 와 Password compare Module과 Authentication Module이 존재 한다.

Encrypt Password는 Password Encrypter에서 생성된 패스워드로 사용자가 입력한 패스워드를 암호화 시킨 패스워드이다.

Set Password는 사용자가 이전에 설정해 놓은 패스워드로서 DB connecter를 이용하여 값을 가지고 온다.

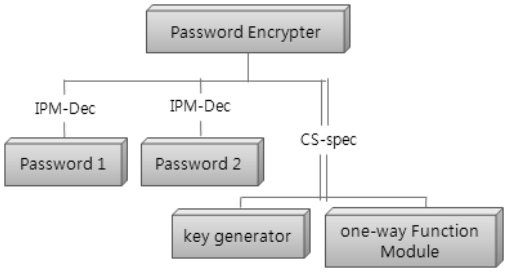


그림 9. Password Encrypter

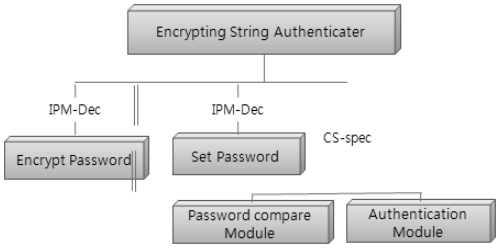


그림 10. Encrypting String Authenticater

Password compare Module에서는 사용자가 입력한 패스워드의 최종 결과 값인 Encrypt Password와 사용자가 이전에 설정해 놓았던 Set Password의 값을 비교하는 모듈이다.

Authentication Module는 Password compare Module에서 비교한 결과를 활용하여 사용자인증을 수행하는 모듈로 최종 결과물을 생성해 낸다.

5.3 멀티 터치 패스워드 시스템 구현

기존의 싱글 터치 기반의 4자리 패스워드에서는 정수형이나 문자열로 입력받아 암호화 후 그 결과를 비교하는 방식이었다.

멀티 터치 기반의 다중 입력 패스워드의 경우 동시에 눌리는 값들에 대해 처리하는 방법이 필요하다.

입력받은 패스워드를 인증 서버가 갖고 있는 패스워드와 같은지 비교 후에 그 결과를 가지고 접근제어를 하게 된다.

제안하는 다중 입력 패스워드 인증 방식도 패스워드 인증 프로세스는 동일하다. 하지만 패스워드 저장 방식에 대해 언급할 필요가 있다. 앞에서의 그림 4. 숫자 패스워드 입력 예에서 입력된 패스워드는 [6 2 8 3]이다. 이를 암호화 한 후 인증 서버의 그것과 비교하기는 쉽다.

하지만 멀티 터치를 통한 패스워드 입력 예로 입력된 패스워드를 [0 1 5 7 8 9 2]와 같이 1차원적으로 저장한다면 인증 서버 입장에서는 싱글터치로 입력된 결과 값인지 어떤 조합으로 멀티터치 된 입력 값인지 판단 할 수 없고 결국 기존의 패스워드 방식에 입력만 복잡하게 한 결과가 된다. 그렇기 때문에 다중 입력된 패스워드는 구분

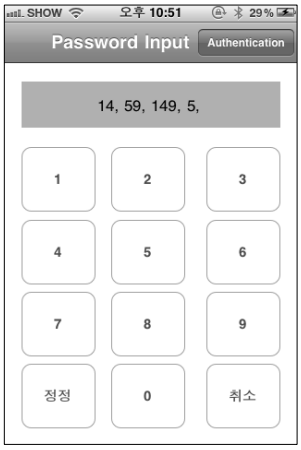


그림 11. 멀티터치 패스워드 구현 예

표 7. 멀티터치 패스워드 리스트 예

List Password[0]	(1)→(4)
List Password[1]	(9)→(5)
List Password[2]	(1)→(4)→(9)
List Password[3]	(5)

자를 통해 구별할 필요가 있다. 본 논문에서는 그러한 구분자로 소괄호를 사용하고 있다. [(0, 1), (5), (7, 8, 9), (2)]와 같이 멀티 터치를 통한 패스워드 입력 예를 표현하고 있다. 멀티 터치를 통한 패스워드 인증 구현을 위해서 리스트를 사용한다.

멀티 터치 환경에서 패스워드가 1단계부터 9단계까지 동시에 터치 되는 것이 고정적이지 않기 때문에 리스트를 이용하여 구현하는 것이 효과적이다. 기존에 문자(C언어에서는 char) 데이터 타입을 사용하던 것을 LIST 의 데이터 타입으로 변경하기만 하면 기존의 방식에서 크게 변하지 않고 멀티터치 패스워드를 적용 시킬 수 있다. 기존의 char password[0]의 값을 인증 서버의 그것과 비교한 것과 똑같이 LIST password[0]의 값을 비교하면 멀티 터치에서 입력 된 패스워드를 인증할 수 있다.

그림 11 멀티터치 패스워드 구현 예에서는 동시에 터치된 숫자를 표 7 멀티터치 패스워드 리스트 예와 같이 리스트로 입력받아 그것을 오름차순으로 정렬하고 콤마(,)로 입력을 구분하여 멀티터치 패스워드 인증 시스템을 구현하였다.

6. 결론 및 고찰

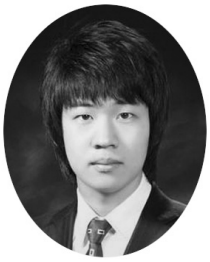
터치패널은 하나의 접점만 인식하는 것이 아닌 여러 개의 접점을 인식하는 멀티터치 방식이 대두되고 있다. 본 논문에서는 이러한 멀티터치 환경에서의 다중 입력을 통한 사용자 인증 방식에 대한 아이디어를 소개하였다. 멀티터치 환경에서의 비밀 번호 입력으로 이전의 싱글터치 기반에서 1글자씩 입력되던 비밀번호가 멀티터치 기반에서는 2개 이상의 그룹으로 입력될 수 있다. 멀티터치 기반의 패스워드 입력은 단순히 [1, 2, 3, 4]로 입력되던 패스워드를 [(1,3), (2), (3,4), (1,2,3)]와 같은 방식으로 설정함으로써 사용자 패스워드의 암호화 강도를 높이고 입력의 복잡성을 향상시킴으로써 패스워드 노출 위험을 줄이려 하였다. 멀티터치 패스워드의 도입으로 조합할 수 있는 경우의 수가 많아지고, 그에 따라 전사 공격에 대해 더 나은 보안성을 갖도록 하였다. 전사 공격에 대한 보안성은 전사 공격 프로그램을 통한 실험으로 증명하였다.

이 멀티 터치 기반의 패스워드는 ATM기기, 개인용 모바일 기기, 물리적 접근통제 시스템에서 기존 패스워드를 대체할 기술로 활용 될 수 있다.

또한 제안하고자 하는 멀티 터치 기반의 패스워드 방식의 인증 방식은 기존의 패스워드 인증 방식과 크게 다르지 않기 때문에 현재 상용되고 있는 One-Time Password (OTP) 등의 패스워드 보안성 강화 기술들과 함께 사용되어 더 좋은 보안 성능을 나타낼 수 있을 것이다. 본 연구는 나아가 멀티터치 기반에서 사용자 패스워드를 넘어 개인 인증 방법을 위한 보안 기술 연구의 초석으로 활용 될 것이다.

참 고 문 헌

1. Robert Morris, Ken Thompson, “Password security: a case history”, Communications of the ACM, Volume 22 Issue 11, Nov. 1979.
2. 윤병남, 반형식, “공공분야의 정보보호 - 공공분야의 공인인증 서비스 -” 한국통신학회, 한국통신학회지 (정보통신) 제19권 8호, 20~29쪽(총10쪽), 2002.08.
3. Chitiz Mathema, “멀티-터치 올-포인트(Multi-Touch All-Point) 터치 스크린:유저 인터페이스 디자인의 미래”, Cypress Semiconductor Corp, July 2009.
4. Bill Buxton, “Multi-Touch Systems that I Have Known and Loved”, Microsoft Research, October 2009.
5. Wikipedia : Multi-touch, http://en.wikipedia.org/wiki/Multi-touch
6. Roger S. Pressman “Software Engineering A Practltiners' Approach” 3rd Ed. McGraw Hill.
7. Jefferson Y. Han, “Low-cost multi-touch sensing through frustrated total internal reflection”, UIST '05 Proceedings of the 18th annual ACM symposium on User interface software and technology, 2005.
8. Jefferson Y. Han, “Multi-touch interaction research”, SIGGRAPH '06 ACM SIGGRAPH 2006 Computer animation festival, 2006.
9. http://code.google.com/android/
10. http://www.apple.com



주 승 환 (judeng@kut.ac.kr)

2009 한국기술교육대학교 인터넷미디어공학부 정보보호공학과 학사
2011 한국기술교육대학교대학원 컴퓨터공학과 석사
2011～현재 한국기술교육대학교대학원 컴퓨터공학과 박사 과정

관심분야 : 모바일 보안, 모바일 악성코드, 센서네트워크 보안, 디지털 포렌식

서 희 석 (histone@kut.ac.kr)

2000 성균관대학교 산업공학과 학사
2002 성균관대학교대학원 전기전자 및 컴퓨터공학과 석사
2005 성균관대학교대학원 전기전자 및 컴퓨터공학과 박사
2005～현재 한국기술교육대학교 컴퓨터공학부 조교수

관심분야 : 모델링&시뮬레이션, 네트워크보안, 보안 시뮬레이션, USN