Journal of The Korea Society of Computer and Information
Vol. 17 No. 9, September 2012
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2012.17.9.065

숫자기반의 패턴 형식 패스워드 사용자인증 기술

주 승 환*, 서 희 석*

A study on User Authentication Technology of Numeric based Pattern Password

Seung-Hwan Ju*, Hee-Suk Seo*

요 약

기존의 텍스트 기반 패스워드들은 추측, 사전 공격, 키로거, 사회공학, 훔쳐 보기, 스파이웨어 등의 공격에 취약하고, 이는 모바일 환경에서 더욱 심각한 문제이다. 훔쳐보기 공격은 패스워드에 대한 대표적인 공격방법 중 하나로, 공격자는 로그인 과정을 직접 관찰하거나 사용자의 인증 과정을 녹화하는 방식으로 패스워드에 대한 정보를 얻을 수 있다. 이러한 취약점을 보완하기 위한 연구를 진행하였다.

본 논문에서 제안하는 패턴 기반의 숫자 패스워드 인증 기술에서는 길이가 긴 패턴 시퀀스로 사용자 인증함으로써 기존 패스워드의 보안성을 강화시키려 하였으며, 높은 보안성을 제공하면서 사용자로 하여금 4개의 숫자만을 기억하도록 하여 사용의 편의성은 침해하지 않으려 하였다. 그 결과로, 사용하기 편리하고 훔쳐보기 공격과 전사적 대입 공격을 방지하기 위한 새로운 패스워드 시스템을 제안하고 이에 대한 보안성과 유용성을 검토하고자 한다.

▸ Keywords : 패턴 기반 패스워드, 숫자 패스워드, 패스워드 보안성

Abstract

The traditional text-based password is vulnerable guessing, dictionary attacks, keyloggers, social engineering, stole view, etc. these vulnerability effect more serious problem in a mobile environment. In this study, By using the pattern number to enter the password of an existing four-digit numeric password, User easily use to new password system.

The technology on pattern based numerical password authorization proposed in this paper would intensify the security of password which holds existing 10 numbers of cases by authorizing a user

• 제1저자 : 주승환 • 교신저자 : 서희석
• 투고일 : 2012. 04. 26, 심사일 : 2012. 07. 04, 게재확정일 : 2012. 08. 02.
* 한국기술교육대학교 컴퓨터공학과(Dept. of Computer Science Engineering, Korea University of Technology and Education)

and would not invade convenience of use by providing high security and making users memorize only four numbers like old method. Making users not have inconvenience and raising complexity, it would have a strength to an shoulder surfing attack of an attacker. So I study password system that represents the shape-based of number. I propose the new password system to prevent peeking attacks and Brute-force attack, and this proposal is to review the security and usability.

▸ Keywords : Pattern-based password, Numeric password, Password Security

I. 서 론

인터넷 사용자의 증가와 컴퓨터 보급의 확대는 정보보호의 중요성을 증대시키고 있다. 정보보호는 가로채기 및 파괴, 수정 등의 공격에 대응하는 것으로 가용성 및 무결성, 기밀성, 인증, 부인봉쇄 등의 보안목적에 의해 이루어진다. 가용성과 같은 보안 목적은 주로 백신 프로그램과 침입탐지시스템과 같이 시스템 구현에 의해 이루어지며, 무결성과 가용성 등의 보안목적을 이루기 위해 암호 기술이 이용된다. 사용자 인증은 시스템 접근자나 서비스 요구자가 정당한 사용자인가를 판단하는 것으로, IT와 관련한 거의 모든 분야에서 요구되는 정보보호 목적으로 암호알고리즘과 프로토콜 기술, 생체 인식 기술들이 이용되고 있다.[1]

사용자 인증이란 사용자가 제시한 신분의 타당성을 확인하는 절차로 이는 사용자가 특정 시스템이나 자원에 접근하는 것을 허용할지 여부를 결정하는 문제이다. 사용자 인증은 보통 3가지 유형으로 이루어진다.

표 1. 사용자 인증 방법
Table 1. User Authentication Method

지식기반 사용자인증	알고 있는 어떤 것
소유기반 사용자인증	가지고 있는 어떤 것
신체기반 사용자인증	본인 자체의 어떤 것

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 장비의 구입비용이 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 기존의 알파벳과 숫자로 이루어진 문자를 이용한 문자 입력 방식(alphanumeric)이나 4자릿수 숫자 기반의 개인 식별 번호(Personal Identification Number: PIN)가 모바일 기기에서 사용될 경우 훔쳐보기 공격이나 불법 카메라 등을 이용한 공격, 스머지 공격 등에 취약하다는 단점이 있기 때문이다.[2-3] 패턴 방식의 숫자 패스워드 입력 방법을 제시함으로써 패스워드의 보안 강도를 강화하고자 한다.

II. 관련 연구

1. 시선 추적을 이용한 패스워드 시스템

Screen oriented technique for reducing the incidence of shoulder surfing[4] 논문에서는 사용자의 시선 추적을 이용하여 패스워드 패턴을 입력할 수 있도록 설계하였다.

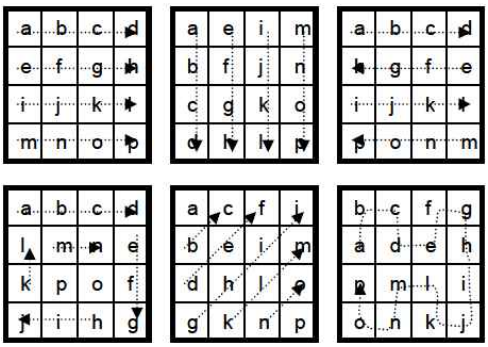

그림 1. 시선 추적을 이용한 패스워드 패턴입력 시스템
Fig. 1. Input pattern system using tracking sight

2. PassFaces 패스워드 시스템

그림 2. PassFace 시스템
Fig. 2. PassFace System

PassFaces[5]은 Real User Corporation 에서 개발된 서비스이다. 사람들은 사람의 얼굴을 잘 기억할 수 있는 장점을 이용하여 구현하였다.

Passface 시스템은 사람의 얼굴을 이용하여 암호를 입력하도록 하였다. 사용자가 선호하는 얼굴들을 사전에 저장한 뒤, 사진 선택을 통한 사용자 인증 시스템이다. 또한 보안성을 높이기 위해서 PassFace시스템과 함께 다른 인증 시스템을 결합한 two factor인증을 수행할 것을 권장하고 있다. 하지만, 얼굴 사진에 대한 생성 및 수집이 어렵다는 문제점이 있다.

3. 이미지 클릭을 통한 사용자 인증 시스템

Authentication using graphical passwords[6]은 일반적인 이미지를 이용하여 사용자를 인증하는 시스템을 제안하였다.

이미지 클릭을 이용한 사용자 인증은 이미지의 특정한 곳을 클릭하게 만들어서 사용자 인증을 수행한다. 또한 단순히 이미지의 위치를 클릭하여 인증하는 것이 아닌 클릭하는 순서를 기억하여 올바르게 클릭하여야 사용자 인증이 제공된다.

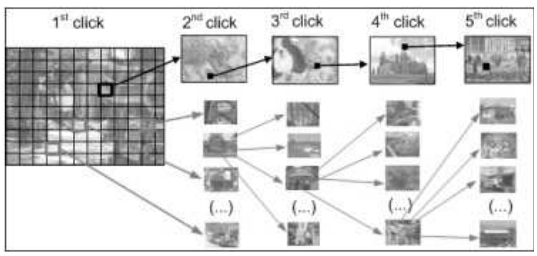

그림 3. 이미지 기반 패스워드 시스템
Fig. 3. Image Based Password System

사용자에게 제공되는 이미지는 일반적인 이미지로 제안했다. 일반적인 이미지로 제안한 이유는 그림으로 하는 것보다 일반적인 이미지에는 사용자가 특별하게 생각하거나, 특정한 부분이 더 많은 것으로 나타나기 때문이다.

또한 클릭을 할 때마다 다른 이미지를 보여주어 이미지의 복잡성을 높였다.

4. Graphical Password System

Image Based Registration and Authentication System[7] 에서는 그래피컬 패스워드 시스템을 제안하고 있다.

Akula와 Devisetty's 알고리즘[7]은 Dejavu[8]비슷한 방법으로 Graphical Password를 제공한다. 하지만 다른 점은 SHA-1 을 활용하여 메모리와 사용자 인증을 더 강화하였다. Akula 시스템은 PDA 나 모바일 환경에서도 동작하는 것으로 알려졌다.

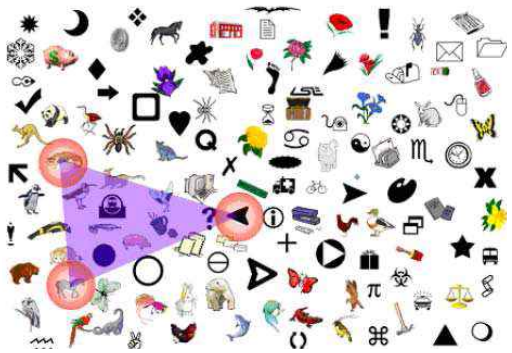

그림 4. 이미지 기반 패스워드 시스템
Fig. 4. Graphical Password Authentication

Pass-object를 적용하여, 사용자가 지정한 Pass-object를 convex hull로 구성하여, 구성된 convex hull 안의 개체를 클릭하여 사용자 인증을 제공, 하지만 너무 많은 개체와 까다로운 방법으로 식별이 힘들다.

5. 이미지 경로 기반 패스워드 시스템

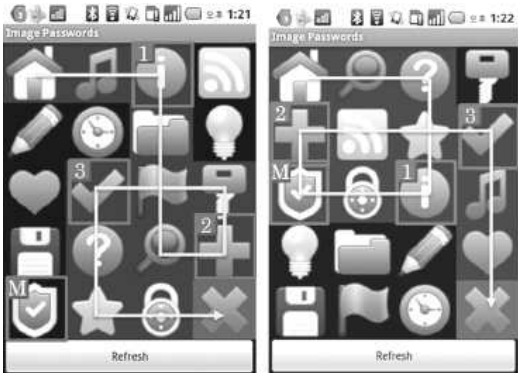

그림 5. 이미지 경로를 이용한 패스워드 시스템
Fig. 5. Password System Using Image Trace

모바일 환경에서 훔쳐보기 공격에 강한 그래픽 패스워드 인증 기법[9]에서는 훔쳐보기 공격을 막기 위해 한붓그리기 방식을 이용한 그래픽 패스워드 방식을 제안하였다.

기존 그래픽 패스워드 방식에 한붓그리기 개념을 도입하여 패스 이미지간의 순서를 맞춰 경로에 포함하고 마인 이미지를 포함하지 않는 방식을 사용하였다. 기존의 4자리의 PIN방식의 암호보다 스머지 공격이나 훔쳐보기 공격 등에는 강한 방식이지만 무작위 대입 공격에는 약한 것을 확인할 수 있다.

6. 다중 입력을 이용한 패스워드 시스템

멀티터치 환경에서의 다중 입력을 통한 패스워드 기반의 사용자 인증 기법[10] 에서는 현재 터치패널은 하나의 접점만 인식하는 것이 아닌 현재 기술로 여러 개 접점을 인식하는 멀티터치 방식을 채택하고 있다는 점을 이용하였다.

멀티터치 환경에서 다중 입력을 통해 동시에 여러 숫자 패스워드를 입력하는 방식을 설계함으로써 사용자 패스워드의 보안 강도를 높이고 사용자로 하여금 패스워드 입력의 복잡성을 높여 패스워드의 물리적 노출 위험을 줄이려 하였다.

멀티 터치 환경을 지원하는 터치 패널이 필요하기 때문에 고가의 부가적인 장비가 필요하다는 단점이 있다.

그림 6. 멀티터치를 이용한 패스워드 시스템
Fig. 6. Password System for Multi-touch Environment

III. 패턴 형식의 숫자 패스워드 기술

1. 패턴기반 패스워드 기술

패스워드 시스템과 관련된 기타 다른 연구들은 입력 방식의 패스워드 시스템을 개선하려 하였다. 패스워드를 입력하는 방법을 바꾸어 접근하기에 실제로 적용하기에 어려움이 많았다.

사실 은행, 핸드폰, 신용카드, 도어락 등의 삶의 중요한 영향을 미치는 패스워드가 대부분 한 자리의 숫자를 4회 연속

입력하는 것으로 구성되어 10,000개 만의 경우의 수를 갖는 패스워드로 보안에 취약한 실정이다.

실제로 어린이부터 노인까지 다양한 연령대의 사용자가 패스워드를 사용 중이나 이 중 대부분의 사용자가 어렵고 복잡한 것보다 사용하기 간편하고 쉬운 것을 선호하여 패스워드 입력이 복잡하고 어려울 경우 경제적으로 영향을 미칠 것을 우려하여 대부분 현 체계 사용하고 있다.

많은 수의 사용자가 개인정보와 관련되거나 같은 패스워드를 통합하여 사용하는 경우가 많으나 개인정보 유출로 인해 경제적 피해가 우려되는 만큼 현 패스워드 시스템보다 개선된 시스템 도입이 필요하다.

패턴 방식을 사용할 경우 하나의 숫자로 인증하는 것이 아닌 숫자의 만들어진 모양에 의미를 둘 수 있어 사용자는 더욱 기억하기 쉽지만 기존보다 훨씬 복잡한 패스워드 생성 가능하다.

패턴 기반의 숫자 패스워드 인증 기술에서는 길이가 긴 패턴 시퀀스로 사용자 인증함으로써 기존의 0~9까지의 10가지 경우의 수를 갖는 패스워드의 보안성을 강화시키려 하였으며, 패턴으로 숫자 패스워드를 입력하게 하여 패스워드 보안성을 강화하고자 한다. 본 패스워드 기술은 보안성뿐만 아니라 사용자로 하여금 기존의 방식대로 4개의 숫자만을 기억하도록 하여 사용의 편의성까지 제공하려 한다. 사용자로 하여금 불편함이 없으면서도 입력의 복잡성을 높여 공격자의 훔쳐보기 공격에도 강성을 가지고자 한다.

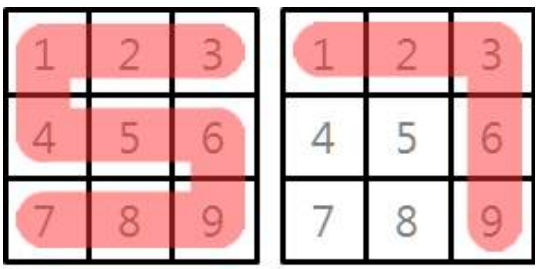

그림 7. 패턴입력을 통한 숫자 패스워드 시스템
Fig. 7. Numeric Password System through Pattern

2. 패스워드 패턴 시퀀스

패턴 기반의 숫자 패스워드는 패턴으로 숫자 패스워드를 입력하게 하여 패스워드 보안성을 강화한 기술이다. 숫자에 대한 패턴은 사용자 임의대로 지정 할 수 있기 때문에 각각의 숫자가 갖는 경우의 수가 증가하여 패스워드 보안성을 강화하고자 한다. 기존의 숫자 패스워드에서 패스워드 '1' 이 갖는 경우의 수는 단순히 숫자 '1'을 입력하는 하나의 행동이었다. 하지만 패턴 기반의 숫자 패스워드에서는 패스워드 '1'의 입력이 갖는 경우의 수가 많기 때문에 전사 공격에 강성을 갖는다.

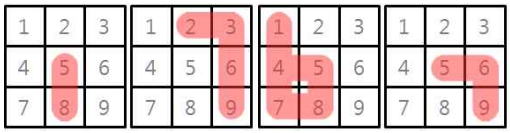

그림 8. 사용자A의 패턴 패스워드 예 : 1-7-6-7
Fig. 8. Password Example of User A : 1-7-6-7

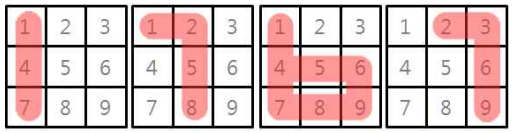

그림 9. 사용자B의 패턴 패스워드 예 : 1-7-6-7
Fig. 9. Password Example of User B : 1-7-6-7

그림 8과 그림 9에서는 두 사용자의 패스워드가 "1-7-6-7"로 같다. 하지만 같은 숫자 패스워드라도 다른 패턴으로 입력하기 때문에 두 패스워드는 상이하다. 그렇게 같은 숫자라도 다른 패턴으로 패스워드를 지정할 수 있도록 하여 공격자가 쉽게 유추하지 못하게 하였다.

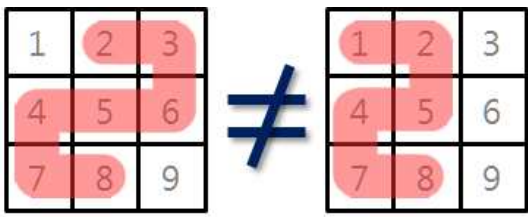

그림 10. 숫자 패스워드 시퀀스의 예
Fig. 10. Example of Numeric Password Sequence

그림 10은 사용자A와 사용자B의 패스워드에서 사용된 숫자 '2' 이다. 하지만 각각의 사용자가 갖는 패스워드 시퀀스는 확연히 다르다. 사용자 A의 숫자 '2' 패스워드 시퀀스는 "2-3-6-5-4-7-8", 이며, 사용자 B의 숫자 '2' 패스워드 시퀀스는 "1-2-5-4-7-8" 이다. 이렇게 같은 숫자 '2'라도 패턴에 따라 다른 패스워드로 인식하고, 이는 패턴기반 패스워드이기 때문에 패턴이 가지는 경로로 패스워드를 구성할 수 있는 것이다. 이렇게 숫자의 조합을 패턴으로 입력함으로써 유추하기가 어려워 보안성이 크게 향상된다.

3. 패스워드 패턴이 갖는 경우의 수

본 논문에서는 패턴 패스워드의 경우의 수를 계산하기 위해 대각선 패턴을 배제하였다. 패턴 "1" 이후에는 "5"로 패턴을 형성할 수 없으며, "2"나 "3"으로 패턴을 형성하여야 한다. 또한 "1-3" 과 같이 떨어져 있는 숫자를 이용하여 패턴을 형성할 수 없다는 규칙을 가지고 패턴기반 숫자 패스워드의 경우의 수를 계산하였다.

그리고 패턴 입력은 위에서 아래로 진행하는 것을 가정하였다. 패턴을 거꾸로 입력하는 것도 패스워드로 설정할 경우 그 경우의 수는 2배가 된다.

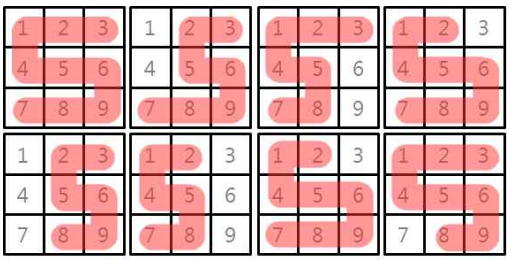

그림 11. 패턴 기반 패스워드의 예 : '5'의 패턴
Fig. 11. Example of Pattern based Password : Pattern '5'

그림 11에서는 숫자 '5'를 표현할 수 있는 8개의 패턴을 나타내고 있다. 이렇게 숫자 '5'가 여러 패턴 시퀀스를 갖는 것을 알 수 있다.

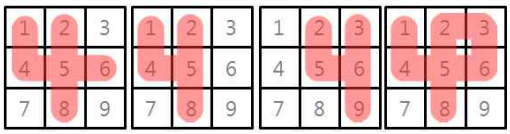

그림 12. 패턴 기반 패스워드의 예 : '4'의 패턴
Fig. 12. Example of Pattern based Password : Pattern '4'

그림 12에서는 숫자 '4'를 표현할 수 있는 4개의 패턴을 나타내고 있다. 같은 패턴 형태라도 시퀀스의 순서에 따라 다른 패스워드로 판단할 수 있지만 본 논문에서는 숫자 4를 표현하는 패턴은 4개로 설정하였다.

숫자 1을 표현하는 패턴은 9가지, 숫자 2는 8가지 등 패턴기반 숫자 패스워드가 가질 수 있는 경우의 수는 54개이다.

54개 경우의 수를 갖는 패턴기반 숫자 패스워드가 4회에 걸쳐 입력되면 패스워드는 544=8,503,056 개의 경우의 수를 갖는다.

쉬운 경우의 수 측정을 위해 패턴 시퀀스의 순서를 가정하였기 때문에 54개의 경우의 수를 갖고, 패턴 시퀀스의 순서를 고려한다면 100개 이상의 경우의 수를 갖는다.

표 1. 패스워드 숫자 별 패턴의 수
Table 1. The number of password patterns by numbers

패스워드 숫자	패턴의 수
1	9
2	8
3	11
4	4
5	8
6	5
7	10
8	3
9	6

그림 13에서 첫 번째 패턴이 갖는 패턴 시퀀스가 "6-5-4-1-2-3-6-9" 이거나 "3-2-1-4-5-6-3-6-9" 일 수 있기 때문이다. 하나의 형태가 패턴 시퀀스에 따라 더 많은 경우의 수를 가질 수 있다.

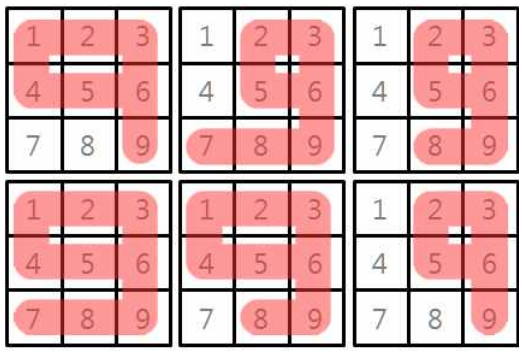

그림 13. 패턴 기반 패스워드의 예 : '9'의 패턴
Fig. 13. Example of Pattern based password : pattern '9'

IV. 패턴기반 패스워드 기술의 보안성

1. 무작위 대입 공격

패턴 기반의 숫자를 이용한 패스워드는 조합 가능한 패턴의 수가 54개이다. 이는 일반적으로 사용되는 PIN방식의 패스워드 시스템이 가지는 경우의 수가 9가지인거에 비해 훨씬 높은 수치이다. 그러므로 일반적인 4자리 패스워드보다 전사 공격에 대해 높은 보안성을 갖는다.

공격자가 사용자 인증에 사용되는 패턴의 정보를 알고 있는 경우에도 패턴의 복잡성으로 인해 실제 암호를 알아내기 위해서 많은 시간이 걸린다. 사용자가 패턴의 수가 가장 적은 "4444"로 설정한 경우에도 공격자는 사용자가 설정한 패턴을 찾는데 최악의 경우 44=256만큼의 시도를 해야 한다. 반대로 패스워드를 패턴의 수가 가장 많은 "3333"을 설정한 경우 공격자는 최악의 경우 114=14,641번의 시도를 수행해야 패스워드를 알아낼 수 있다.

표는 일반적인 숫자 패스워드에서는 패스워드 크랙 실험 결과의 예이다. 임의로 발생시킨 4자리 패스워드와 해제하는 소요된 시간을 15개 실험을 예로 들었다.

표 3. 4자리 숫자 패스워드 크랙 실험
Table 3. 4-digit password-cracking experiment

4자리 숫자 패스워드 크랙 실험 예 (시간:ms)					
설정 패스워드	0416	6745	4135	7011	6125
유추 소요 시간	7	22	16	22	21
설정 패스워드	0638	1862	5682	2983	2746
유추 소요 시간	8	12	19	14	15
설정 패스워드	5452	8366	9425	5715	7326
유추 소요 시간	18	22	26	19	22

그림 14는 100회에 걸친 4자리 패스워드 크랙 실험의 결과이다. 10000개의 경우의 수를 갖는 패스워드를 크랙하는데 걸린 시간은 평균 17.4ms 였으며, 최소 7ms, 최대 27ms의 시간 만에 패스워드 시스템을 무력화 시킬 수 있었다.

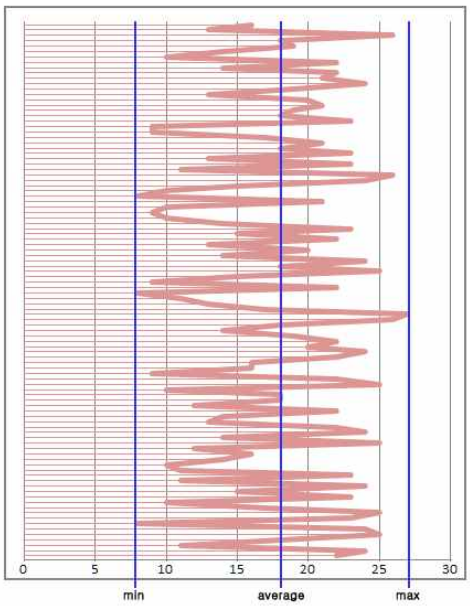

그림 14. 4자리 숫자 패스워드 크랙 실험 결과
Fig. 14. 4-digit password-cracking results

패턴기반 숫자 패스워드 시스템의 보안성을 같은 방법으로 실험하였다. 아래 표 패턴기반 숫자 패스워드에서는 패스워드 크랙 시간을 나타내고 있다. 위 실험과 같은 방법으로 총 100회에 걸쳐 패스워드 해제 실험을 하였다.

그림 15는 100회에 걸친 패턴기반 숫자 패스워드 시스템의 크랙 실험 결과이다. 544=8,503,056개의 경우의 수를 갖는 패스워드를 크랙하는데 걸린 시간은 평균 120.7ms 였으며, 최소 13ms, 최대 142ms의 시간이 소요되었다.

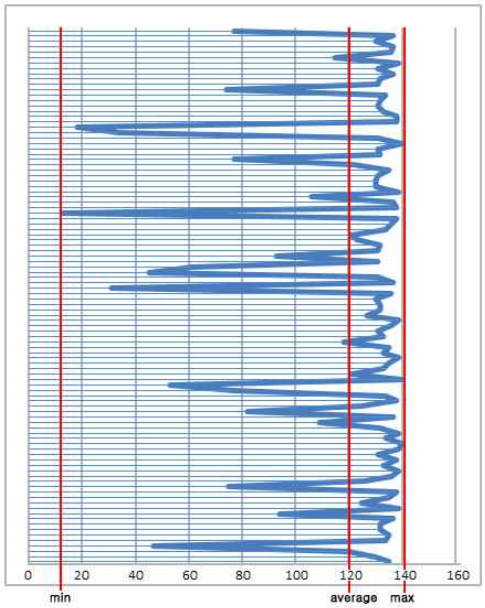

그림 15. 패턴기반 숫자 패스워드 크랙 실험 결과
Fig. 15. Pattern-based numeric password-cracking results

2. 스머지 공격

스머지 공격이란 터치 인식을 지원하는 모바일 기기에서 가능한 공격 방식 중 하나로써 스크린을 터치 할 때 스크린 상에 남아있는 얼룩을 이용한 공격 방식 이다. 사용자의 모바일 기기 스크린을 사진 등을 통하여 저장한 후에 스크린 위에 남아있는 얼룩을 판별하여 비밀번호를 유추하여 공격한다. 이러한 공격 방식은 기존 PIN 방식, 알파벳과 숫자의 혼합 방식의 패스워드 시스템에서는 치명적이다.

하지만 본 논문에서 제안하는 방식의 경우 패턴방식의 패스워드가 단일 입력이 아닌 여러 번에 걸쳐 입력되기 때문에 공격자가 공격 패턴 군을 형성하기가 어렵다. 따라서 해당 패스워드 시스템은 스머지 공격으로부터 안전하다고 볼 수 있다.

3. 훔쳐보기 공격

제안 하는 패턴기반 숫자 패스워드 방식의 경우 패턴의 시작 지점으로부터 숫자를 자신이 지정해 놓은 패턴을 이용하여 패스워드를 입력하게 된다. 패턴을 만들어 나가게 될 경우 주변에 패스워드에 사용되지 않는 숫자들이 공격자를 혼란스럽게 할 수 있다. 그렇기 때문에 공격자가 훔쳐보기 공격을 통해 패스워드 패턴을 파악하기는 매우 어렵다.

V. 결 론

오늘날 세계 각국에서 해커들의 의해 자신들도 모르게 개인정보 유출 및 금전적인 피해 등의 의하여 현재 IT업계 시장들은 패스워드 보안에 대한 관심이 기울어지고 있다. 이에 따라 패스워드 보안의 초점이나 규모 등 다양한 측면에 관한 지식 습득의 필요성 및 중요성이 점차 높아지고 있는 실정이다.

본 논문에서 제안하는 패턴 기반의 숫자 패스워드 인증 기술에서는 길이가 긴 패턴 시퀀스로 사용자 인증함으로써 기존의 0~9까지의 10가지 경우의 수를 갖는 패스워드의 보안성을 강화시키려 하였으며, 높은 보안성을 제공하면서 사용자로 하여금 기존의 방식대로 4개의 숫자만을 기억하도록 하여 사용의 편의성은 침해하지 않으려 한다. 사용자로 하여금 불편함이 없으면서도 입력의 복잡성을 높여 공격자의 훔쳐보기 공격에도 강성을 가지고자 한다.

본 연구의 성과로 은행, 신용카드, 핸드폰, 도어락 등 기존 패스워드 방식 대신에 응용할 수 있으며 사용자는 패스워드 입력 시 패스워드 노출로부터의 걱정 등으로부터 해방될 수 있다. 또한 본 연구로 인하여 새로운 방식의 패스워드 기기를 관련 업계에서 새로이 개발하여 유통함으로써 보안 시장의 활성화를 불러올 수 있으며 새로운 방식의 패스워드를 제안함으로 인해 이를 착안하여 정체된 패스워드 방식에 새롭고 창의적인 아이디어를 기대할 수 있을 것이다.

감사의 글

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2010- 0021951).

참고문헌

[1] W. Jansen, "Authenticating mobile device users through image selection," The Internet Society: Advances in Learning, Commerce and Security, vol.1, pp.183-194, 2004.

[2] A. H. Lashkari, O. B. Zakaria, S. Farmand, and R. Saleh, "Shoulder surfing attack in graphical password authentication," International Journal of Computer Science and Information Security, vol.6, no.2, pp.145-154, 2009.

[3] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," Proc. of the 21st Annual Computer Security Applications Conference, pp.463-472, 2005.

[4] Hoanca, B. and K. Mock. Screen Oriented Technique for Reducing the Incidence of Shoulder Surfing. In Proceedings of International Conference on Security and Management (SAM). Las Vegas, Nevada, USA, 2005.

[5] RealUser, "www.realuser.com," last accessed in 2012.

[6] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005.

[7] S. Akula, V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.

[8] R. Dhamija and A. Perrig, "D´ej`a vu: a user study using images for authentication," in Proc. of the 9th conference on USENIX Security Symposium. Berkeley, CA, USA: USENIX Association, 2000.

[9] Gunyoung Moon, Jonguk Kim, Manpyo Hong, "A Graphical Password Scheme Resistant to Shoulder Surfing Attack in Mobile Environments", Korea Information Science Society, Journal of KISS: Computing Practices and Letters, No. 18 No. 1 page (s): 90-94, 2012.

[10] Seung-hwan Ju, Hee-suk Seo, "Password Based User Authentication Methodology Using Multi-Input on Multi-Touch Environment," Journal of the Korea Society for Simulation, Vol 20, No 1, 2011.

저 자 소 개

주 승 환

2009 : 한국기술교육대학교 인터넷미디어공학부 정보보호공학과 공학사

2011 : 한국기술교육대학교대학원 컴퓨터공학과 석사

현 재 : 한국기술교육대학교대학원 컴퓨터공학과 박사 과정

관심분야 : 모바일 보안, 모바일 악성코드, 사용자 인증, 네트워크 보안

Email : judeng@koreatech.ac.kr

서 희 석

2000 : 성균관대학교 산업공학과 공학사

2002 : 성균관대학교대학원 전기전자 및 컴퓨터공학과 석사

2005 : 성균관대학교대학원 전기전자 및 컴퓨터공학과 박사

현 재 : 한국기술교육대학교 컴퓨터공학부 부교수

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

Email : histone@koreatech.ac.kr