논문 2012-49-9-24

Shoulder Surfing 공격을 고려한 패스워드 입력 시스템 구현 및 통계적 검증

(Designing Password Input System Resistant on Shoulder Surfing Attack with Statistical Analysis)

임 수 민*, 김 형 중*, 김 성 기**

(Soo Min Lim, Hyoung Joong Kim, and Seong Kee Kim)

요 약

사용자 인증을 위해 패스워드를 사용하는 것은 구성이 간단하고 인증 과정에서 걸리는 시간이 비교적 짧기 때문에 사용성이 높은 암호시스템이다. PC, 스마트 폰, 태블릿 PC등 다양한 입력 디바이스에서의 활용성이 높은 반면 패스워드를 입력하는 과정에서 공격자에게 패스워드가 노출될 물리적인 위험이 존재하는데 이것을 일컬어 Shoulder Surfing 공격이라 한다. 패스워드의 형태는 과거보다 조금 더 복잡해진 문자형 패스워드를 비롯해 최근에는 이미지를 이용하거나 시나리오를 활용하는 등 사용자의 의도가 반영된 패스워드가 개발되고 있다. 다양한 패스워드가 개발되면서 사용자 중심으로의 사용가능성과 보편성에 대한 평가 기준에 대한 연구가 부진 하다. 본 논문 에서는 간단한 이미지를 이용한 패스워드 시스템과 자판 변환이 가미된 입력 시스템을 구현한 후 해당 입력 시스템의 사용가능성을 통계적인 방법을 이용하여 검증해보고자 하였다.

Abstract

Using password on system is easy to build and shorten the access time to authorize user, which is high in use for vary system that requires users' authorization. Many input device are able to perform the password system easily, such as PC, smart-phone, tablet PC, etc. Beside the high usability of password, physical attack occurs when user put their password on the device, known as Shoulder Surfing attack. It used to be formed in numbers, characters or mix of different kinds, but new kind of password arose. Exploiting image or making scenarios are those kinds which are able to reflect users' intentions. Not many estimation exists for new password, so there's need to be standard for those new password for highlighting usability and accessability. In this paper, we propose password system with simple image and switching key-board to test statistical method to estimate usability on the password.

Keywords : Security, Graphical Password, Shoulder Surfing Attack, Usability.

Ⅰ. 서 론

본인 인증용으로 패스워드가 널리 사용되고 있다. 그 예로, 사용자는 스마트폰이나 PC로 인터넷 뱅킹과 자금 이체 서비스를 비롯한 다양한 금융 서비스와 네트워크를 이용한 외부에서의 홈 컨트롤 등 밖에서도 본인 인증을 통한 다양한 서비스를 제공받음으로서 활동성을 넓힐 수 있게 되었다. 사용자의 활동 범주가 넓어질 수 있도록 빠른 인증을 돕는 패스워드는 활용이 간단하고 효율적이며 해쉬 함수 등을 이용한 추가 변수로 보안성을 높일 수 있다는 장점이 존재하기 때문이다[1]. 이밖에

* 정회원, 고려대학교 정보보호대학원
(Dept. of Security Engineering, Korea University)
※ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을받아 수행된 연구임 (No.2012015587)
접수일자: 2012년7월23일, 수정완료일: 2012년9월6일

도 패스워드는 웹페이지 접속에서부터 이메일 계정, 등 사용자의 인증을 필요로 하는 다양한 분야에서 쓰이고 있으며 간단하게 문자로 구성된 패스워드로 한정되었던 예전에 비해 새로운 형태의 패스워드가 개발되고 있다.

앞서 언급했던 것처럼 문자열로 구성된 패스워드는 높은 사용성을 가지고 사용자에게 활동성을 부여하지만, 여러 서비스를 이용하기 위해서는 그에 맞는 패스워드를 기억해야한다는 단점이 존재 한다. 또한 하나의 패스워드를 일괄적으로 사용한다면 공격자에게 공격 받을 시 모든 정보가 노출될 수 있는 위험이 존재하기 때문에 기존의 문자열 패스워드를 사용할 때 사용자는 보안상의 이유로 여러 개의 패스워드를 사용하는 것이 권고되고 있다. 하지만 개인이 여러 개의 랜덤한 패스워드를 생성한다고 해도 익숙하지 않는 정보를 기억할 수 있는 기억 능력의 한계 때문에 자연스럽게 사용자의 행동양식이나 본인 정보, 예를 들면 핸드폰 번호나 생년월일, 집 주소, 차량번호 등과 관련된 숫자, 문자가 포함되는 패스워드를 만들 가능성이 높다. 이러한 가능성은 공격자들이 사용자의 정보를 얻게 되면서 패스워드의 전수 공격을 가능하게 하게 되었다. 이러한 사용자의 부담으로부터 그리고 공격으로부터 피할 수 있도록 사용자의 인식을 높이고 보안성을 보장할 수 있는 새롭고 다양한 형태의 패스워드를 설계하려는 연구가 꾸준히 진행되고 있다.

이미지와 패턴을 이용한 그래픽 패스워드(Graphic Password)는 사용성이 높고 보편적인 패스워드라고 할 수 있다. 기존의 문자열 패스워드에서 사용자가 외워야만 이용할 수 있는 부담을 덜어 단순 패턴이나 사용자가 고른 이미지 등을 이용하여 사용자가 손쉽게 외울 수 있도록 돕는다. 사용자가 여러 개의 패스워드를 외울 부담을 줄여주지만 아직 널리 쓰이지 않고 사용자와 친한 지인들에게 쉽게 공격받을 수 있는 단점이 존재하고 어떤 패턴이나 이미지를 골라야 무결성과 보안적인 측면에서 안전할 수 있는지의 인지적 관점 연구가 필요하다. 또한 범용적으로 쓰일 수 있도록 꾸준한 보완 연구가 필요하다.

홍채, 지문, 혈관 등 생체 인식을 요하는 물리적 패스워드도 새로운 패스워드의 종류 중 하나로 사용자의 물리적인 요소를 사용한다. 하지만 여러 용도에서 사용하게 되면서 한 번의 공격으로 사용자가 가입한 모든 사용처의 패스워드가 노출될 수 있는 위험이 존재 한다.

본 논문의 Ⅰ장에서는 기존의 문자열 패스워드가 갖는 단점과 새롭게 등장하는 패스워드의 종류를 알아보았고 제 Ⅱ 장에서는 사용자의 인지적인 관점에서 기억력의 부담을 줄일 수 있는 패스워드 종류에 대해 서술 하였으며 제 Ⅲ 장에서는 제안되는 패스워드의 구성에 대해서 설명하였고 제 Ⅳ장에서는 실험 과정에 대해서 편차를 줄이기 위해서 어떻게 실험을 진행 하였는지 자세히 서술 하였다. 제 Ⅴ 장에서는 실험을 통한 결과에 따른 분석을 통계적인 관점에서 어떻게 해석할 수 있는지 서술 하였다. 제 Ⅵ 장을 끝으로 제안된 패스워드가 어떤 장점을 갖는지를 설명하고 본 논문은 끝을 맺는다.

Ⅱ. 사용자 인지 관점의 패스워드 종류

사용자가 패스워드를 입력할 때 다른 사용자가 패스워드를 직접적으로 혹은 비디오 레코딩이나 스크린에 남은 패턴과 지문등을 이용하여 간접적으로 알아내는 공격 방법을 ‘shoulder surfing attack’이라고 한다. 이 공격 방법은 사용자가 키보드, 터치스크린, 마우스, 스타일러스 등으로 패스워드를 입력할 때를 노려 외부에 노출되어 있는 디바이스의 고유적인 특성을 이용해 공격자가 패스워드의 위치 및 패턴을 알아내는 방법이다. 일상에서 개인은 키보드, 스마트폰 키패드 및 은행의 현금인출기(ATM: automatic teller machine)등 패스워드를 사용할 때마다 ‘shoulder surfer’ 공격을 통해 패스워드가 공격받을 가능성이 있다는 것을 알 수 있다. 특히나 숫자로만 이루어진 패스워드를 사용하는 ATM의 경우 사용자는 공격자에게 패스워드의 노출을 스스로 예방하도록 권고한다. 그래픽 패스워드나 생체 인식 패스워드의 경우 사용자의 잔여 패스워드 패턴을 남기지 않기 때문에 이러한 공격에 안전할 것으로 생각 된다. 본 장에서는 보편화된 그래픽 패스워드에 대해 살펴보고자 한다.

이미지를 사용하여 패스워드를 구성하는 그래픽 패스워드 중 하나인 CHC(Convec Hull Click) Scheme을 다음 논문에서 제안 하였다[3].

해당 논문에서 제안한 방법은 사용자의 위치 패턴이 디바이스에 남는 패스워드의 틀을 깬 암호 시스템으로 사용자가 선택하는 위치가 패스워드의 위치로부터 비교적 자유로운 방법이다. 사용자가 임의로 선택한 키 요

소들로 구성된 심미적인 영토에 선택한 요소들을 포함시키면서 공격자에게 키 요소를 노출시키지 않고 매번 키 요소의 위치가 다르기 때문에 사용자의 패턴이 남지 않음으로서 Shoulder Surfing 공격에 안전하다고 할 수 있다. 하지만 사용자가 고를 수 있는 키 요소의 집합이 커질수록 선택해야 되는 요소 또한 늘어나기 때문에 패스워드를 입력하는데 시간이 걸리고 범주 대비 키 개수가 노출될 수 있음을 감안해야하는 단점이 존재 한다. 이런 방법 이외에 디바이스의 입력 인터페이스로부터 자유로운 패스워드 시스템 또한 존재 하는데 그것은 다음과 같다. 알파벳 혹은 숫자로 구성된 패스워드들은(textual password)은 제 삼자에게 노출되기 쉬우며 암호들이 저장된 데이터베이스 자체가 공격받는 경우도 있기 때문에 공격의 빈도도 많이 발생하는 편이고 공격 성공 가능성이 높다. 사람의 기억능력 또한 영향을 받기도 하고 사용자는 여러 암호를 외워야하는 한계성 때문에 보안성 높은 암호를 설정 하는 것과 외울 수 있는 암호를 설정하는 것 사이에는 그것을 정해야하는 사용자의 딜레마가 존재한다. 여기서 다음의 논문[4]은 텍스트로 구성된 암호에 비해 높은 엔트로피 값을 기대할 수 있는brain computer interface(BCI)를 제안하였다. 사용자의 생각을 기기로 전달하여 인식할 수 있다는 가정 아래 세워진 연구는 여전히 활발한 연구 활동이 진행되고 있는 분야 중에 하나이다. 특히나 사람의 뇌파를 읽고 해석 할 수 있는 기기의 중요성이 부각되는 연구이다. 다음의 그림 1에는 BCI의 원리가 간략하게 설명되어 있다.

간단하게 BCI는 사용자가 알고 있는 것 “What you know”과 가지고 있는 것 “What you have”을 사용자의 뇌파가 기기로 전달된 후 해석하여 패스워드처럼 사용하게 되는 것이다. 이 방법은 앞서 언급한 것처럼 텍스트로 구성되었을 때 우려되는 Shoulder Surfing 공격 및 사용자의 기억 용량의 한계 및 오류의 발생을 낮추어줌으로 써 이상적이지만 아직 까지 연구 분야가 활성되지 않았기에 사람의 생각을 해석할 수 있는 기기의 발명이 필요한 분야이기도 하다.

이처럼 기존의 텍스트 패스워드를 대체 할 수 있는 방법을 찾기 위한 다양한 연구가 진행되는 가운데 사용자가 가지고 있는 용할 수 있는 사용될 수 있는

게임을 이용해 사용자의 경험 및 사용성(Usability), 그리고 기억의 한계성(Memorability)을 극복하기 위해 가지고 있는 정보를 곧 활용하여 쓸 수 있는 그래픽 패스워드나 시나리오 패스워드 및 뇌파를 이용한 의사 결정 인식 패스워드와 같은 다양한 아이디어들이 꾸준히 등장하여 이목을 끌고 있다.

[5]에서 소개하는 방법 또한 시나리오 패스워드의 일종이다. 이 논문에서 소개하는 ‘ToonPaswords’는 사용자의 의사결정에 의해 시스템의 인증을 받을 수 있는 방법이다. 예를 들어 사용자에게 그림을 사전에 제시하고 세 개의 만화를 연속적으로 선택하게 한 다음 그 사람의 인증을 받을 때 어떠한 그림의 순서로 선택하는지 보는 방법이다. 만약 제시할 수 있는 그림의 개수가 40개라면 $40^3(64{,}000)$개의 패스워드가 만들어질 수 있다. 이 방법 또한 Shoulder Surfing공격에 강인할 수 있도록 사용자의 생각을 패스워드 대용으로 사용자의 흔적이 남지 않음을 알 수 있다. 사용자의 기억 용량에 따른 부담을 줄일 수 있지만 사용자와 친분이 있는 사람에게 공격받게 될 경우에 시스템 부분에서 인식할 수 없기 때문에 공격이 발생할 수 있다는 단점이 존재 한다.

BCI를 이용한 패스워드는 텍스트로 구성된 패스워드

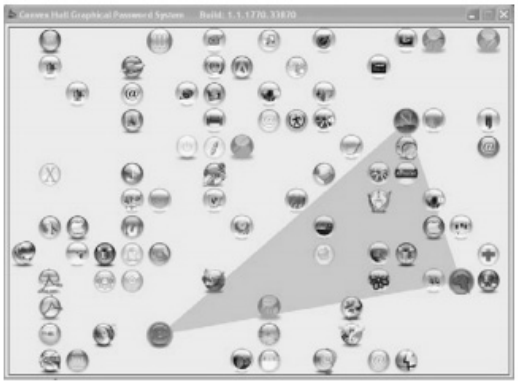


그림 1. CHC Scheme.
Fig. 1. Example of Convex Hull Click.

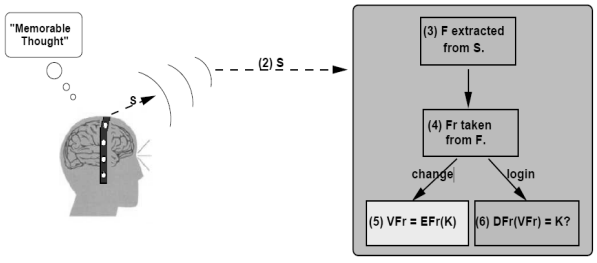


그림 2. BCI의 원리
Fig. 2. Diagram of Brain Computer Interface.

들보다는 상대적으로 높은 엔트로피 값으로 인해 안전성을 기대할 수 있지만 뇌파를 읽고 해석할 수 있는 기기의 성능 발전이 필요하고 그래픽 패스워드처럼 여러 이미지를 사용할 수 있으나 일반적으로 널리 쓰이기 위한 이미지 집합을 정하는데 발생하는 문제 해결이 우선적으로 필요하기 때문에 아직은 실생활에서 활용되기에 어려울 것이라 예측 된다.

본 장에서 소개된 패스워드들은 사람의 인지적인 관점이 기억 용량의 한계를 줄여주기 때문에 문자열로 구성된 패스워드들보다 효용적이라고 설명한다. 하지만 범용적으로 쓰이기에는 한정된 이미지 도메인과 이용하기 어렵다는 접근성 때문에 오히려 문자열로 구성된 패스워드보다 실용성이 떨어질 것이라고 생각된다. 이러한 점을 극복하기 위해서는 사람들에게 친숙한 요소를 찾는 인지적 관점의 연구가 선행적으로 진행될 필요가 있다고 생각 한다.

다음 장에서는 사용자들에게 단순한 이미지와 키열의 변환을 구현하여 사용자에게 어느 정도 인지될 수 있는지 밀러가 제안한 매직넘버의 개념[6]과 비교 실험해 보았다.

Ⅲ. 제안되는 패스워드 구성

본 논문에서는 숫자와 단순한 도형 및 색깔을 이용하여 사용자에게 어느 것의 인지도가 높은지에 대해서 실험을 해 보았다. 패스워드의 기억단위가 사용자의 숫자, 색깔, 도형간의 어떤 차이가 있는지 세 요소간의 인지의 차이가 패스워드의 기억 용량에 어떤 영향을 주는지에 대한 실험을 통해 사용성(Usability) 및 보안성(Security)을 살펴보기 위한 실험을 시도하였고 복잡한 이미지를 사용하지 않은 단순한 이미지로도 기존의 숫자 패스워드가 가지는 취약점을 개선할 수 있는 가능성을 보이고자 한다. 또한 기존의 키패드의 위치를 변화시켜 사용자가 패스워드를 입력하는데 어떤 영향을 주는지 병행하여 실험하였다. 숫자로 구성된 패스워드의 경우는 대부분의 시스템에서 이용되고 있고 사용자도 손쉽게 사용할 수 있는 장점이 있지만 그만큼 패턴을 읽힌다면 공격이 쉬운 단점도 존재한다. 이러한 단점을 극복할 수 있도록 고안된 그래픽 패스워드가 안전성을 보장할 수 있을지, 또 복잡한 이미지가 아닌 단순한 이미지와 도형을 사용한 해당 실험이 통계적으로 유효한 결과를 의미하는지 통계적인 분석방법을 통하여 다음 장에서 결론을 내릴 것이다.

심리학 및 인지공학에서 널리 사용되고 있는 'magic number plus/minus seven'[6]은 조지 밀러의 1956년 연구로 사람이 일반적으로 외울 수 있는 기억의 단위를 7±2라고 제시했다. 이 의미는 7을 중심으로 5부터 9까지 사이에 속한 정수만큼의 기억 단위를 쉽게 외울 수 있어 이런 현상을 'magic number'로 비유했다. 다양한 실험 결과를 통해 사람은 단순한 이진법적인 기억 용량의 경우 정수로 아홉 자리 정도를 쉽게 외울 수 있고 영문 단어와 같은 경우에는 다섯 개 정도라고 결론지었다. 현재 밀러의 법칙은 다양한 제품의 UI(User Interface)를 설계할 때 사용되고 있다.

패스워드의 경우 기억 용량의 한계와 보안간의 모순이 존재한다. 사람은 많은 패스워드를 외울 수 없고 단순한 패스워드는 쉽게 공격 받기 때문에 패스워드는 정신중하게 정해야 한다. 그렇기 때문에 사용자의 패턴이 남지 않고 사용자가 쉽게 외울 수 있는 그래픽 패스워드는 shoulder surfing 공격의 예방으로 최적이라고 생각 한다. 사람의 일반적인 기억의 단위를 정의한 밀러의 논문을 바탕으로 사용자에게 효과적으로 전달되는 정보의 유기적인 단위가 상황별로 7이상의 2단위의 숫자이거나 7이하의 2단위의 사이에 존재하는 것을 도형과 색깔을 이용하면 어떻게 적용될지, 아니면 키 변환을 통해서 보안을 보장받을 수 있을지를 실험을 통해 살펴보기로 하였다. 이는 친숙 하지 많은 요소로 이루어진 패스워드일수록 사용자가 외울 때 더 어려울 것이고 외울 수 있는 개수 또한 숫자와 비교했을 때 낮을 것이라 가정을 도출하였다.

편의상 숫자는 N, 그림 또는 도형은 F, 색깔은 C라고 줄여 부르기로 한다. 이들 요소들이 shoulder-surfing을 줄이는데 어느 정도 기여할 수 있는지 알아보고, shoulder-surfing을 줄이는 대신 지불해야 할 대가에 대해서도 사용성 관점에서 살펴보기로 한다.

사용자의 인지적인 관점에서 사용성(usability) 및 노출의 안전성(security)을 제공할 수 있는지 알아보기 위한 실험을 진행 하기 위해서는 사람들에게 좀 더 친근한 색깔이나 도형으로 구성된 실험을 선행적으로 진행하여 색깔과 도형에 대한 변별력을 높여야 하지만 해당 실험에서는 도형과 색깔로 구성된 패스워드로 사용성 및 안정성을 살펴보기 위한 실험이었기 때문에 간단한

이미지와 도형을 사용하여 실험을 진행 하였고 변별력을 구분 하기위한 이미지와 도형은 후속 연구에서 다루기로 하였다.

Ⅳ. 제안된 패스워드 인지 실험

4.1 실험계획

사용자가 숫자 N, 도형 F 및 색깔 C에 대한 기억능력에 대해 알아보기 위해 2×5행렬로 C, N, F를 화면에 디스플레이 한다.

보통 숫자는 4×3행렬을 사용하는 게 일반적이나 2×5 행렬 또한 쓰이는 키 배열이고 0에서 9까지의 열 가지의 숫자를 실험용 모니터에 고르게 디스플레이 시켰다. 4×3행렬에서는 열 개의 숫자 외에도 '*'와 '#'등 추가 변수를 더 표현할 수 있다. 같은 모양의 네모 열 개를 만들기 위해 9mm×9mm의 동일한 사이즈로 각각 설계했다. 일반적으로 대부분의 시스템이 숫자만을 이용한 패스워드 체계를 기본적으로 사용하고 있다. 현실적으로 키를 열 개 내외로만 배열시켜야 하는 응용분야가 아니라면 보안성을 고려해 좀 더 복잡한 패스워드를 요구할 경우 알파벳 문자열과 조합한 패스워드 체계를 사용하기도 한다.

그에 비해 C와 F는 친숙하면서도 널리 쓰이지 않는 요소이므로 패스워드로 쓰일 때 많은 오류가 발생할 수 있다. 실험에서 쓰인 색깔의 종류와 도형의 형태는 임의로 정하되 단순한 이미지를 사용하기 위해 사용자의 성향을 고려하지 않음으로 인해 나타날 수 있는 영향을 고려하지 않았다. 예를 들어 색맹에 대한 영향, 특정 색깔을 선호하는 경향 등이 그 예이다.

또한 해당 실험을 통해 개인이 범할 수 있는 오류도 고려하지 않았다. 숫자의 순서를 정확히 알고서도 실수로 입력 값을 더 넣었을 경우가 바로 그러한 오류이다. 숫자가 아닌 다른 요소로 구성된 패스워드 입력 시스템을 설계했을 때 사용자들이 새롭게 구성된 패턴을 어느 정도 맞출 수 있지 가늠해 보고자 했고 실험의 유의성을 알아보기 위해 통계적인 분석을 시도했다. 다음 장에서는 해당 분석방법을 통해 기존의 숫자로 구성된 암호 체계와는 다른 요소를 사용함으로써 얻어지는 결과로 사용성을 측정할 수 있다.

4.2 실험구성

실험에 참여한 인원은 총 92명의 스마트폰 사용자 이다. 숫자, 도형, 색깔로 사용된 패스워드의 인지성이 어느 정도 되는지를 실험하기 위해 어플리케이션을 개발했으며, 개발 환경은 표 1과 같다.

실험을 위해 삼성의 Galaxy 2 LTE와 Galaxy Note 10.1를 사용하기 위한 기기별 어플리캐이션을 개발했으며, 실험을 위한 어플리케이션은 표 1을 참조한 Eclipse Indigo, JAVA JDK 6.0을 Window 7 (32bit) 환경에서 활용했다.

Galaxy 2 LTE의 디스플레이 크기는 기기 전체 크기의 125.3mm×66.1mm(4.3 인치) 중 99mm×60mm부분을 차지하며 그 중 입력 값 키패드의 크기는 9mm×9mm로 2×5 키 배열로 구성 되었다. 한편 두 번째 실험에 사용한 기기는 Samsung Galaxy Note로 디스플레이 크기는 1280mm ×800mm 중 키패드 각각의 크기는 $20mm \times 20mm$로 4×3 키 배열로 구성했으며 어플리

표 1. 어플리케이션 개발 환경
Table 1. Application Development Tool.

구분	특징
운영체제	Microsoft Window 7 (32bit)
개발언어	Java SE Development Kit (JDK) 6.0
통합개발환경	Eclipse Indigo 3.7.1 Service Release 2 Android SDK Ver. 3.0
기타	개발툴과 관련된 많은 문서들 무상제공 삼성, LG등이 안드로이드를 기본 OS로 채택

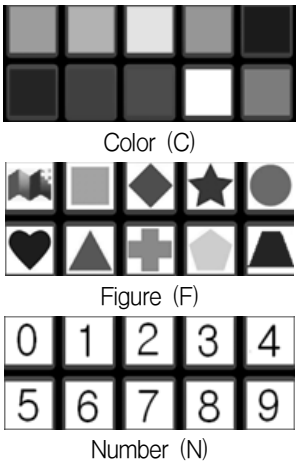
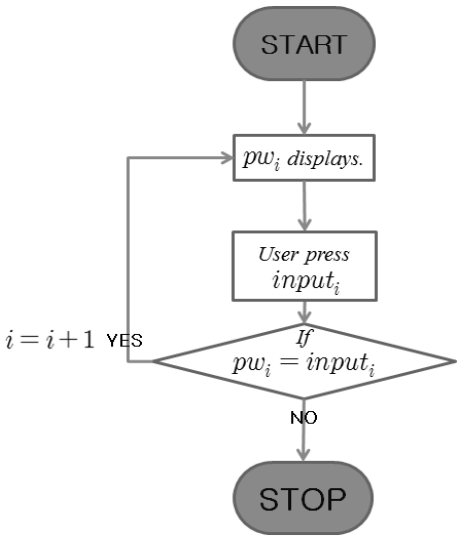


그림 3. 실험에 사용된 색깔(C), 도형(F), 숫자 요소
Fig. 3. Element of Experiment Color(C), Figure(F) and Number(N).

케이션 개발 환경은 앞의 환경과 동일하다. 그림 2와 그림 3에서 색깔을 실험하기 위한 갤럭시 폰과 탭을 각각 보여주고 있다.

4.3 실험 절차

실험은 다음 그림 4의 플로우 차트를 따라 기본적으로 구성된다. 패스워드의 구성이 첫 번째 실험에서는 숫자, 색깔, 도형인 점과 두 번째 실험에서는 키 변환으로 i의 값이 $i=4$로 고정된다.



$where,$

pw_i = *패스워드*

$input_i$= *사용자 입력값*

i = *패스워드 개수*

- *첫 번째 실험 :* $3 \leq i \leq 10$
- *두 번째 실험 :* $i = 4$

4.3.1 요소간 관계성 실험

1. 사용자는 상단의 숫자(N), 도형(F), 색깔(C) 순서로 각각 실험을 진행한다. 이하 대상은 숫자, 도형, 색깔 중 하나를 나타낸다.

A. 랜덤하게 뽑힌 대상이 화면의 상단 좌측에서부터 3초간 디스플레이 된 후 사라진다.
B. 사용자는 디스플레이 되는 3초 동안 대상을 볼 수 있다.

디스플레이 크기
99mm×60mm
키패드 크기
9mm×9mm

그림 4. 실험용 Galaxy 2 LTE 프로토 타입
Fig. 4. Proto-type of Galaxy 2 for Experiment.

C. 사라진 대상을 디스플레이된 모양과 순서대로 아래 2×5 행렬의 보드에서 고른 후 사용자가 입력한다.
D. 사용자가 입력한 값이 맞으면 (모양과 순서가 일치하면) 맞춘 개수보다 하나 더 대상의 수를 증가시켜 상단에 디스플레이하고 실험을 계속하며, 맞추지 못할 경우 (즉, 입력을 마친 후 확인버튼을 눌렀을 때 하나라도 틀린 것이 있으면) 실험이 실패한 것으로 간주하고 현재 디스플레이된 대상의 개수보다 하나 적은 상태에서 멈춘 것으로 간주한다.

2. 해당 실험을 통해 알아내고자 하는 변수

A. 사용자가 많이 맞춘 개수: 각 카테고리 별(도형, 숫자, 색깔) 사용자가 맞춘 개수

4.3.2 키 배열 실험

1. 사용자에게는 4×3 행렬의 숫자 키패드가 주어진다.

A. 랜덤하게 네 자리로 이루어진 숫자 배열이 키패드 상에 음영이 바뀌며 차례대로 디스플레이된다.
B. 사용자는 디스플레이된 네 자리의 숫자를 기억한다.
C. 네 자리수의 디스플레이가 끝난 순간으로부터 사용자가 네 자리의 입력을 완료하기까지의 시간이 초단위로 측정된다.
D. 사용자가 디스플레이되었던 네 자리의 패스워드를 기억한 후 키패드의 위치가 변형되지 않은 경우 1회, 키패드의 위치가 매번 변형되는 경우 1회를 각각 실험한다.

2. 해당 실험을 통해 원하는 값

A. 사용자가 패스워드를 기억 한 후 완료까지의 시간: 네 자리 수의 패스워드를 외운 후 두 가지 다

른 경우에서의 완료 시간 (키패드의 위치가 변했을 때와 키패드의 위치가 변하지 않았을 때)

V. 실험 결과 분석

5.1 요소간 관계성 실험

실험에 참여한 92명은 남자 76명 여자 16명으로 구성되어 있다. 숫자는 인간에게 매우 친숙한 기호이므로 세 개도 맞추지 못하는 경우가 없었다. 또한 심볼 간 인식의 차이가 있는지 확인하는 게 실험의 목표였으므로 숫자의 경우 열 개까지만 보여주기로 했다. 상대적으로 색상이나 도형인 경우 열 개까지 맞춘 사례가 없어 이 가정이 유효하다고 판단할 수 있다.

숫자는 그림 4를 볼 때 4부터 10까지 대체로 정규분포와 유사한 분포를 보인다. 샘플의 수가 적고 모집단에 대한 정보가 없지만 그럼에도 불구하고 숫자(N)를 사용하는 경우에는 비모수검정인 Smirnov-Komogorov 테스트를 통해 정규성을 지닌다는 점을 보였다. 테스트 결과는 정규성을 지니는 것으로 판명되었다.

한편, 도형과 색깔의 경우에는 7 이상을 맞춘 사례가 없고, 3과 4를 중심으로 한쪽으로 치우치는 분포를 이룬다는 점이 특이하다.

색상, 도형을 포함한 숫자들의 경우 20대 이상의 학생을 대상으로 실험을 진행하였기 때문에 맞출 수 없다는 예측 없이 3개를 맞추는 것부터 진행했다. 하지만 정확한 측정을 위해서는 1개와 2개의 경우가 포함되어야 하고 해당 과정이 들어간 실험은 향후 연구에 포함되어 진행 될 것이다.

또 일부 피실험자는 색맹이어서 색상의 경우 흑백으로만 보인다고 말해 해당 실험에서 제외시켰다.

도형의 경우 또한 마찬가지이다. 결론적으로 실험에는 참여했지만 92명에는 포함시키지 않았다. 피실험자가 충분히 이해하고 숙지할 수 있도록 사전에 실험 과정을 이해시키는 것도 잊지 않았다.

기초 통계량 값은 다음과 같다. 색깔, 도형, 숫자의 순으로 평균 4.16, 4.09 7.23개를 맞췄으며 표준편차는 각각 0.94, 0.94, 1.73으로 나타났다. 이를 통해 숫자는 평균 7개 정도의 수를 맞출 수 있음을 증명하여 밀러의 실험이 유효함을 할 수 있었다. 하지만 색깔과 도형으의 경우에는 그 격차가 존재 하는데 각각 맞출 수 있는 개수의 평균이 최소는 4개 이상의 수를 갖게 되었다.

표 2. 각 원소의 기초 통계량 값 (단위:초)
Table 2. Elementary Statistic Analysis.

	Color	Figure	Number
평균	4.161290	4.086022	7.225806
표준편차	0.935883	0.940119	1.726576

표 3. 'Kolmogorov - Smirnov Test' 검정
Table 3. Kolmogorov-Smirnov Test.

	Figure-Number	Color-Number
D_{mn}	5.22	4.94
$D_v^{0.05}$	0.13965	
Result	$5.22 > 0.13965$	$4.94 > 0.13965$

이러한 경우 사용자의 숫자에 대한 인식과 이미지와 도형에 대한 인식이 다른 반면에 도형과 이미지에 관련된 사용자의 인식이 비슷하다고 말 할 수 있으며, 이미지와 도형의 경우 최소한 4개의 구성으로 된 패스워드를 구축한다고 하면 다른 사람에게 노출되더라도 shoulder surfing에 강인할 수 있을 것 이라고 예측할 수 있다.

일반적으로 많이 쓰이는 숫자로 구성된 패스워드 시스템과 제안한 도형 및 색깔의 패스워드 시스템과의 요소의 차이가 존재하는지 여부를 증명하기 위한 비모수적 증명방법으로 분포의 차이를 통계적으로 검정할 수 있는 'Kolmogorov-Smirnov Test'를 실시했다. C나 F의 경우 7 이상에서는 빈도가 0이므로 카이스퀘어 검정을 통한 분포 분석을 시도할 경우 예측빈도가 5 이상되어야 하는 등 검증요구조건을 만족하지 못하는 상황이 발생한다. 따라서 카이스퀘어 분석은 적용하기 어렵다. 또한 C나 F 샘플의 분포는 정규성을 지니지 않는다는 약점도 지니고 있다. 그래서 누적분포함수인 CDF, 즉 cumulative distribution function을 이용해 비모수검정인 Kolmogorov-Smirnov 테스트를 적용하기로 했다. 통계분석을 위해 귀무가설은 두 그룹의 분포가 동일하다고 설정하였고 대립가설로는 두 그렇지 않다고 설정했다. 표 3은 검정통계량을 보여주는데 F-N의 경우 5.22, C-N의 경우 4.95로 통계적 유의수준 0.05에 해당하는 통계량 0.14보다 커서 두 경우 모두 귀무가설을 기각하게 된다.

즉, N의 분포와 C또는 F의 분포는 다르고, 따라서 차이가 있음을 알 수 있다.

5.2 키 배열 변환

일반적인 키패드의 숫자는 입력할 때마다 키보드 배

열이 변하지 않는다는 약점에서 비롯되기도 한다. 이럴 경우 키보드 위치와 패스워드가 연계되어 위치만 기억해도 패스워드가 공격자에게 노출될 수 있는 위험성이 있다. 키 배열이 바뀌지 않는 이상 위치는 곧 패스워드를 의미하기 때문이다. 이것은 숫자뿐만이 아니라 색깔이나 도형 등 키 배열을 이용하여 패스워드를 입력해야 하는 다른 요소에서도 마찬 가지다.

위치의 순서에 따른 패턴의 노출을 고려하여 공격자가 비밀번호를 외우기 어렵게 하기 위해 키보드 배열을 바꾸면 사용자의 입력시간도 길어지고 실수가 늘어날 것이라고 예상할 수 있다. 입력시간을 측정하는 것은 사용자가 패스워드를 입력 하는데 어려움이 존재하는지 혹은 입력 시간의 증감으로 키 배열이 시스템에 미치는 영향을 살펴보기 위해 실험을 진행했다.

그림 5는 해당 어플리케이션을 이용하여 실험할 키보드 배열을 보여준다. 왼편은 기존의 키보드 배열로 키가 고정되어 변화하지 않는다. 이에 반해 오른편은 키가 매번 바뀌는 상황 중 하나를 보여주고 있다. 피실험자는 키보드 배열이 변하지 않는 상황과 변하는 상황에서 각각 한 번씩 네자리 숫자를 입력하게 된다. 실험 과정에서 두 경우 모두 입력오류를 범한 경우가 없었다. 이는 키보드 배열 변화가 실수를 유발하는 요인을 제공한다고 보기 어렵다는 것을 의미 한다.

총 24명의 인원을 이용하여 실험을 진행하였고, 모두 스마트폰 또는 태블릿 PC를 사용한 경험이 있는 사용자였다. 두 종류의 키 배열을 사용했을 때 걸리는 시간이 통계적으로 유의한 차이를 가지는지 비교하기 위하여 'T-Test'검정을 사용하였다. 두 조건간의 평균을 비교하여 통계적으로 유의한 값의 차이가 있는지 알기 위하여 귀무가설을 두 종류간의 시간 차이가 없다고 설정하였고, 대립 가설은 두 가지 조건의 차이가 있다고 설정하였다. 검정 통계량 값은 표 4와 같다.

수식을 통해 구한 값인 T-Value는 5.50이고 T-Table에서 샘플 수가 24개에 자유도를 23을 갖는 검정통계량 값은 2.07이기 때문에 검정통계량 5.50은 기각역에 속한다. 따라서 배열이 변하는 키보드 입력시간이 그렇지 않은 입력시간과 다르다는 것을 알 수 있다.

귀무가설인 두 조건에 대한 통계적으로 유의미한 차

디스플레이 크기
1280mm × 800mm
키패드 크기
$20mm \times 20mm$

그림 5. 실험용 Galaxy Note 10.1 프로토타입
Fig. 5. Proto-type Galaxy Note 10.1 for Experiment.

표 4. T-Test 검정
Table 4. T-Test.

	Static	Dynamic
Mean	1.928	3.509
SD	1.157	0.803
Number	24	24
T-Value	5.500	
$\alpha_{0.05}$	2.07	
자유도	23	

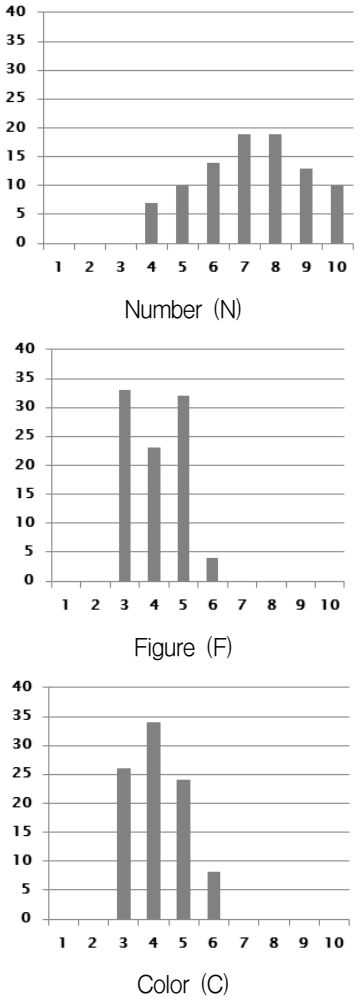


그림 6. 각 요소별 맞춘 개수의 분포
Fig 6. Distribution of Experiment.

그림 7. 일반적인 키 배열(좌측)과 위치가 변하는 키 배열 (우측)
Fig. 7. General Key location(left), Lotating Key location(Right).

이를 가지므로 귀무가설을 기각하고 평균적으로 키 배열이 변화할 때 걸리는 평균시간이 3.5초로 변화하지 않았을 때 걸리는 평균시간 1.9초와 비교해서 약 2배의 입력 시간의 차이를 갖는 것을 알 수 있다.

입력 시간의 차이는 키 배열이 변하지 않았을 때와 변했을 때 사용자가 느끼는 어려움의 정도를 반영한다고 할 수 있다. 즉, 키 배열이 변하는 경우에는 사용자가 패스워드를 입력할 때 약 2배정도의 심리적 어려움을 수반한다고 하는 것을 보여준다. 앞서 실험에서 입력오류가 발생하지 않았음을 보였다. 결국 입력오류가 발생하지 않는 대신 입력시간 증가로 이어진다.

Ⅳ. 결 론

두 실험을 통하여 전체적인 패스워드 입력 시스템에 변화 없이 패스워드를 입력받을 때 숫자와 도형, 이미지간의 사용자의 인식이 어떻게 다른지 알 수 있었다. 또한 키패드의 위치만 변환시킴으로서 얻어지는 유의미한 결과들을 살펴보았다. 키패드에 관련된 실험은 ATM을 기본적인 모델로 삼고 진행하였지만, ATM을 비롯한 안드로이드 핸드폰, 태블릿 PC등에도 사용될 수 있기 때문에 보안성을 고려한 키패드의 사용성을 기대해도 좋을 것이다.

본 논문에서 이뤄진 실험의 결과가 주목이 되는 것은 다음의 이유에서 비롯된다.

- 첫 번째로, 단순한 이미지를 사용하여도 사용자들은 최소 4개의 개수를 맞출 수 있는 반면에 숫자는 최소 7개의 개수를 평균적으로 맞추는 점으로 이미지와 도형을 이용하면 작은 개수로도 패스워드를 구성할 가능한 점
- 두 번째로, 키 배열을 기존의 패스워드 시스템을 크게 변화 시키지 않고 단순히 위치만을 변화 시켰을 때 유의미한 시간 차가 발생한 점

첫 번째 실험으로부터 숫자가 아닌 색깔과 도형으로 키패드를 사용한 실험에서는 다음과 같은 결론을 도출하였다. 실험에 참여했던 사용자가 외울 수 있는 개수가 숫자는 평균 7.23개이나 색깔이나 도형을 이용할 때 그 개수가 평균 4.16과 4.09로 줄어드는 것을 알 수 있었다. 이것은 밀러가 주장한 기억 단위의 기준인 7에 가까운 숫자이며 7을 기준으로 사용자들에게 7자리 패스워드가 주어지더라도 shoulder surfing할 수 있는 기억 단위임을 의미한다. 반대로 숫자가 아닌 도형과 색깔을 이용하면 사용자가 패스워드를 외울 수 있는 수가 평균 4.16개, 4.09개로 줄어드는 것을 알 수 있었다. 이는 숫자가 아닌 다른 요소를 사용하여 패스워드 시스템을 설계하였을 때 필요한 패스워드의 기억단위가 줄어들면서 적은 패스워드의 개수로 공격을 피할 수 있음을 의미한다. 이것은 나아가 도형과 색깔을 이용하면 공격자가 패스워드를 쉽게 알아내지 못하는 것을 의미하고 숫자보다는 작은 단위의 정보로도 쉽게 공격받을 수 없다는 것을 의미한다. 이것은 또한 다양한 이미지와 도형의 조합으로 새로운 패스워드의 구성을 인지적인 관점으로 접근할 수 있음을 의미 한다.

두 번째 실험으로부터 일반적인 네 자리의 패스워드를 사용하면서 키 배열의 위치만 변화시켰을 때 그것을 외우고 올바르게 입력하는 시간이 증가함에 따라 공격자로부터 위치가 노출되는 위험을 피할 수 있음을 알 수 있었다. 24명을 대상으로 실험하였을 때 평균적으로 네 자리수의 패스워드를 입력하는 평균 시간은 1.9초 정도로 짧았으나 키 배열이 바뀌면 평균 3.5초로 시간의 증가하는 것을 알 수 있었다. 이것은 사용자가 기존의 키패드로 패스워드를 입력했을 때 사용된 암호가 평균적으로 1.9초 정도의 사이에서 노출될 수 있고 공격자 또한 1.9초 만에 네 자릿수의 숫자 패스워드를 외울 수 있다는 점을 알 수 있다. 또한 네 자릿수의 숫자를 사용했을 때 발생하는 에러율 및 실수가 거의 없었다는 것은 네 자릿수의 숫자는 사용자가 쉽게 외울 수 있다는 것을 의미한다. 이것은 키 배열이 바뀌는 경우에도 마찬 가지다.

참 고 문 헌

[1] Eun-Jun Yoon, You-Sik Hong, Cheon-Shik Kim and Kee-Young Yoo, “Strong password mutual authentication protocol”, Second Symposium on Usable Privacy and Security, Journal of the Institute of Electronics Engineers of Korea, vol.46, no.1, 2009.

[2] F. Tari, A. A. Ozok, and S. H. Holden, “A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords,” in Proc. of the Second Symposium on Usable Privacy and Security, pp. 56 - 66, 2006.

[3] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, “Design and evaluation of a shoulder-surfing resistant graphical password scheme,” in Proc. of the Working Conference on Advanced Visual Interfaces, pp. 177-184, 2006.

[4] J. Thorpe, P. C. van Oorschot, and A. Somayaji, “Pass-thoughts: authenticating with our minds.” in Proc. of New Security Paradigms Workshop, Sept. pp. 45-56, 2005.

[5] C. Hinds and C. Ekwueme, “Increasing security and usability of computer systems with graphical passwords,” in Proc. of the 45th Annual Southeast Regional Conference, pp. 529-530, 2009.

[6] G. A. Miller, “The magical number seven, plus or minus two: Some limits on our capacity for processing information,” Psychological Review, vol. 63, pp. 92-97, Mar. 1956.

저 자 소 개

임 수 민(정회원)

2006년 고려대학교 산업공학과 학사

2012년 고려대학교 정보보호학과 석사 과정

<주관심분야 : Image Forensic, Image Hashing, Data Compession, Stereography >

김 형 중(정회원)

1978년 서울대학교 전기공학과 학사

1986년 서울대학교 제어계측 공학과 석사

1989년 서울대학교 제어계측 공학과 박사

1990년～2006년 강원대학교 교수

1992년～1993년 USC Univ. 방문교수

2007년～현재 고려대학교 정보호호대학원

<주관심분야 : Watermarking, Parallel Computing, Image Hashing, Data Compression, Stereography>

김 성 기(정회원)

2008년 한양대학교 경영학 학사

2012년 고려대학교 정보보호학과 석사 과정

<주관심분야 : Digital Forensic, Network Security>