이미지를 이용한 사용자 인증 시스템

김기인* 이경현**
*부경대학교 교육대학원
**부경대학교 전자컴퓨터정보통신공학부

A User Authentication System Using Images

Ki-In Kim*, Kyung-Hyune Rhee**
*Department of Computer Science Education, PuKyong National University
**Division of Electronic, Computer and Telecommunications Engineering, PuKyong National University

요 약

인터넷 이용자가 급증하고 있는 오늘날, 제공되는 서비스가 중요할수록 각 사용자에 대한 신분 확인이 다양한 방법에 의해 이루어지고 있다. 본 논문은 현재 가장 많이 이루어지고 있는 패스워드와 PIN 등의 기억기반 인증 방법과 신분확인에 유용하나 전문장치를 필요로 하고 사용에 약간의 불쾌감을 줄 수 있는 생체인식기법을 대체할 수 있는 인식 기반의 이미지 인증 방법을 제안하고 기존의 기억기반 인증 방법과 비교하였다.

1. 서론

사용자 인증은 오늘날 보안 구조의 중심 구성요소라 할 수 있다. 사용자 인증 방법은 크게 나누어 다음의 3가지로 구별할 수 있다.

(1) 지식기반 시스템(Knowledge Based System)
(2) 토큰기반 시스템(Token Based System)
(3) 생체인식기반 시스템(System Based on Biometrics)

이 중에서 생체인식기반 시스템은 신분확인에 유용하더라도, 한가지 문제는 많은 생체인식기반 시스템에서 고가의 전문 장치들을 필요로 하고 있으며, 또한 사용하기에 약간 불쾌감을 줄 소지가 있다. 그리고 대부분의 토큰기반 인증시스템은 토큰(예, 신용카드, 스마트카드)의 도난과 분실을 통한 도용를 방지하기 위해 지식기반 인증을 병행 사용하고 있다. 따라서, 오늘날 대부분의 사용자 인증은 지식기반 시스템으로 이루어지고 있다.

현재 가장 널리 사용되어지고 있는 지식기반 시스템에서의 인증은 패스워드 및 PIN(Personal Identification Number) 인증 방식을 사용하고 있으나, 이 역시 패스워드의 관리상의 어려움이 존재한다. 즉, 단순하거나 개인과 관계 있는 패스워드는 기억하기 쉬우나 사회공학 공격에 취약하며, 복잡하고 의미를 지니지 않은 패스워드는 보안성은 있으나 기억하기가 어렵다. 또한 사람의 기억은 오직 제한된 수의 패스워드만을 기억할 수 있기 때문에, 그것을 적어두거나 다른 목적을 위해 유사하거나, 심지어 동일한 패스워드를 사용하는 경향이 있다.

이러한 문제점에 대한 해결 방안으로 이미지 인식 기반 인증 방식이 Perrig과 Song에 의해 제안되었으며[6], 이는 사용자 인증을 개선하기 위한 접근 방법으로 패스워드나 PIN의 정확한 기억을 통한 지식기반 인증 대신에 사용자가 이전에 보았던 이미지에 대한 인식 방식을 사용하고 있다.

일반적으로 사람들은 도움 없이 기억력에 의존하여 정보를 상기해 내는 것보다 어떤 것을 인식하는 것이 훨씬 쉬우며[1], 또한 이미지 인식 실험으로 인해 인간이 특히 그림(또는 이미지)에 대해 뛰어난 인식력을 가지고 있다는 것이 증명되었다[2, 3].

또한, 실험에서 사람들이 매우 짧은 순간에 수백에서 수천의 그림들을 기억하고 인지할 수 있다는 것이 확인되었다. [4, 5]

따라서, 패스워드에 대한 정확한 기억보다는 이미지에 대한 인식으로 대체함으로써 사용자 인증에서의 오류를 최소화 할 수 있다. 본 논문에서는 앞서 제시된 인식기반 인증 개념에 근거하여 패스워드가 드물

게 가끔씩 사용되는 경우와 패스워드가 자주 바뀌어야 하는 경우 및 패스워드의 사용이 부적절한 초등학교 저학년 아동들에게 적용 가능한 이미지 인식에 기반한 새로운 인증 시스템을 제안하고 기존의 패스워드기반 인식시스템과 비교하였다.

2. 패스워드기반 인증의 결점

패스워드 및 PIN 기반 인증은 많은 결함들을 가지고 있다. 불행하게도 현재의 많은 보안시스템들은 보안이 전적으로 패스워드에 의존이 되도록 설계되어 있고, 웹 사이트의 경우도 마찬가지이다. Cheswick과 Bellovin은 빈약한 패스워드가 시스템 침입의 가장 공통 원인인 것을 지적하고 있다.[7]

지식기반 인증 시스템의 중요한 약점은 그 비밀 정보를 사람의 정확한 기억력에만 의존한다는 것이다. 만약 사용자가 패스워드 입력시 작은 실수를 하게 되면 인증은 실패한다. 그러나 불행하게도 정확한 기억력은 인간의 강점이 아니며, 이전에 경험한 자극의 인식에서 부정확한 기억에 훨씬 능숙하다.[4, 5] 정확한 기억력에 대한 인간 한계는 견고한 패스워드의 필요조건과 서로 상충되고 있다. 패스워드 보안에 관한 Morris와 Thompson의 연구에서 사용자의 15% 이상이 3문자 이하의 짧은 패스워드를 선택하는 것을 지적하고 있으며, 또한 모든 패스워드의 85%가 단순한 탐색 및 사전을 이용한 공격으로 쉽게 깨질 수 있다는 것을 밝혔다.[8] 그리고, Klein은 패스워드 보안에 관한 광범위한 연구에서 모든 패스워드의 25%가 사전공격(dictionary attack)에 의해 깨질 수 있다는 것을 주장하였다.[9]

따라서, 사용자들에 대해 패스워드를 더욱 어렵고 예측 불가능하게 만들도록 요구되며, 결과적으로 패스워드를 기록하고, 작업공간에 그것을 숨기게 된다. 또한 보안 정책에 의해 패스워드를 정기적으로 바꾸도록 요구하는 것은 결국 사용자들로 하여금 기억하기 위해 패스워드를 기록하도록 하는 비율만 증가시킬 뿐이었다.[10, 11]

IT기반 구조의 보안성을 제고하기 위한 시도를 하는 회사의 수와 패스워드 보호영역의 수는 계속 증가하고 있고, 동시에 사용자명과 패스워드의 조합을 요구하는 인터넷 사이트들의 수 또한 증가하고 있다. 이를 극복하기 위해 사용자들은 서로 다른 목적을 위해 유사하거나 또는 동일한 패스워드를 사용한다. 그것은 결국 패스워드 안전성을 감소시키고 있다.

패스워드 인증의 또 다른 문제는 그것들이 기록하기 쉽고 다른 사람들과 공유하기가 쉽다는 것이다. 일부의 사용자들은 다른 사람들에게 그들의 패스워드를 누설하는 것에 대해 별다른 걱정을 하지 않으며 그것을 위험으로서 보고 있지 않다.[16]

취약한 패스워드 문제를 해결하는 3가지 해결책으로는 첫째, 패스워드에 대한 사전공격에 의해 노출되기 전에 취약한 패스워드를 발견하려는 사전노력이며[8, 10] 둘째, 패스워드 크래킹의 계산 부하를 증가시키는 기술적인 기법을 이용하는 방법과,[12] 셋째, 사용자들의 보안 의식 향상을 위한 보안 교육의 강화 등이 있다.[13, 14] 그러나 이들 중 어느 하나라도 패스워드 인증 결점의 주원인을 제거하지는 못한다. 그것은 패스워드기반 인증들이 이상적인 인간 기억력에 의존하는 것이며, 원인이 인간 기억력의 한계에 있기 때문이다.

3. 이미지를 이용한 새로운 인증시스템

앞서 살펴본 패스워드 인증의 결점에 대한 해결책을 제시하며 다음의 요구조건의 충족을 목표로 하는 새로운 인증시스템을 제안한다.

요구 조건

① 시스템은 인간의 정확한 기억력에 의존해서는 안 된다.

② 반면에 사용자에게 더욱 신뢰성 있으며, 또한 보다 쉬운 작업에 근거한 인식에 기반해야 한다.

③ 시스템은 사용자들이 취약한 패스워드를 선택하는 것을 막아야 한다.

④ 사용자들이 암호를 기록하거나, 다른 사람과 공유하는 것을 어렵게 해야 한다.

3.1 시스템 구조

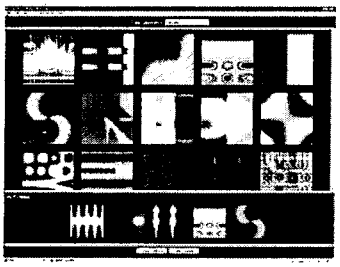
본 시스템은 사람이 지닌 이미지에 대한 뛰어난 기억력에 대한 관측에 근거하고 있다.[2, 3, 4, 5] 사용자는 사용자가 본인임을 인증 받기 위해 주어진 이미지들을 정확하게 확인해야 한다.

사용자는 견본 이미지 세트에서 N개의 이미지 부분집합을 선택하는 것으로 자신의 이미지 포트폴리오를 생성한다. 사용자를 인증하기 위하여 보안시스템은 **n**개의 이미지들로 이루어진 질문세트를 제시한다. 이 질문은 사용자의 포트폴리오에서 **m**개의 이미지들을 포함하고 있다. 여기에서 남아 있는 **n-m**개의 이미지를 미끼(decoy) 이미지라고 부른다. 인증을 위해 사용자는 자신의 포트폴리오의 부분인 이미지들을 정확하게 인식해야 한다.

3.2 이미지기반 인증시스템의 구성단계

3.2.1 포트폴리오 생성단계

이미지기반 인증시스템의 이미지 포트폴리오 구성을 위하여, 사용자는 보안시스템 서버에서 제시한 큰 규모의 이미지 세트로부터 구체적인 수의 자신만의 이미지를 선택한다.



위 그림은 이미지기반 인증시스템의 이미지 선택 화면의 예를 보여주고 있다.

이미지 인증 시스템에 사용되는 이미지의 형태는 시스템의 보안에 매우 큰 영향력을 가지고 있다. 예를 들면, 실제적인 사진 이미지를 사용할 경우 공격자는 사용자의 개인 성향을 예측하여 포트폴리오들을 고르는 시도를 할 수 있으며, 또한 사용자가 포트폴리오 이미지에 대한 정보를 기록하기 용이해지며, 그것을 다른 사람들과 공유하기 쉽게 되는 결점이 나타날 수 있다.

따라서 본 연구에서는 무작위로 만들어진 추상이미지(Random Art)를 사용한다. 그리고 사용자들의 이미지 선택화면에 보여지는 보안시스템이 제공하는 이미지들은 시각적으로 유사하거나 너무 단순한 이미지들은 제거되고 없는 상태이다.[15]

보안시스템 서버에 이용되는 추상 이미지들의 생성과 선택에 관한 것은 추후 연구과제로 남겨두고자 한다.

3.2.2 훈련 단계

사용자들은 포트폴리오 생성단계 이후에 그들의 포트폴리오 이미지에 대한 기억을 증진시키기 위하여 간단한 훈련 단계가 필요하다. 훈련단계에서 사용자는 미끼이미지를 포함하는 질문세트로부터 자신의 추상 이미지들을 선택한다. 포트폴리오 생성 및 훈련 단계는 사용자 이외의 어떤 사람도 이미지 포트폴리오를 볼 수 없는 그런 안전한 환경을 요구한다.

3.2.3 인증 단계

신뢰할 수 있는 보안시스템 서버는 각 사용자를 위한 모든 포트폴리오 이미지를 저장하고 있다고 가정한다. 각각의 사용자들의 인증시도에 대하여 보안시스템 서버는 포트폴리오와 미끼(decoy) 이미지들로 이루어져 있는 질문세트를 생성한다. 생성된 질문세트가 사용자에게 화면으로 제시되면 사용자는 자신의 이미지들을 정확하게 인식/선택하게 된다. 그러면 보안시스템 서버는 사용자를 인증하게 되는 것이다.

인증에서의 보안 수준은 보통의 경우 예를 들어 질문세트에 제시되는 전체이미지의 수가 20개내지 25개 정도이고 거기에 포함된 사용자의 포트폴리오 이미지의 수가 5개 정도라고 할 때 $1/(\frac{20}{5})=1/15504$ 또는 $1/(\frac{25}{5})=1/53130$이므로 대략 4자리 또는 5자리 패스워드의 인증 수준과 비슷하다. 보안시스템 서버가 제공하는 질문세트의 이미지 수와 포함되는 사용자 이미지의 수를 조절하여 더 높은 보안 수준을 유지할 수 있으나 사용자입장에서 자신의 포트폴리오 이미지를 오인식할 경우도 있으므로 본 인증시스템에서는 사용자의 수준별로 등급을 구분하여 임계값을 설정하여 사용자가 자신의 이미지를 모두 정확하게 선택하지 못한다하더라도 임계값 이상의 비율로 선택할 수 있으면 인증되도록 설계를 하였다. 보안 수준에 대한 임계값은 다음의 식에 의해 결정된다.

$$S = \sum_{n=m}^{N} \sum_{t=m}^{n} \binom{n}{t} (P(s))^{t} (1-P(s))^{n-t}$$

S : 시스템의 보안 수준
N : 전체 이미지의 수
$P(s)$: 사용자가 이미지를 인식할 확률
n : 사용자에게 제시되는 포트폴리오 이미지 수
m : 사용자가 인증 받기 위해 선택해야할 이미지 수

이렇게 함으로써 초등학교 저학년 어린이들에게도 충분한 신뢰성을 가지는 인증시스템을 도입할 수 있게 된다. 이는 결함허용기법(Fault-Tolerant Scheme)을 도입하여 인증허용의 수준을 고려한 경우와 같은 개념이다.[17]

4. 패스워드 인증시스템과의 비교 분석

기존의 패스워드에 의한 인증은 인간의 기억력에 의존하고 있으며, 이 경우 망각을 피하기 위해 기록을

해두거나 기억하기 쉬운 패스워드를 선택하여 여러 사이트에서 공통으로 사용하는 경우가 흔히 발생한다. 패스워드 방식에서는 가능한 공격에 대비하기 위하여 알파벳 문자에 숫자와 문자의 조합이나, 긴 패스워드의 사용, 심지어는 특수 문자의 사용도 의무화하는 경우가 있다. 즉, 복잡한 패스워드일수록 공격에 강한 반면, 인간의 두뇌는 이러한 의미 없는 숫자, 문자, 특수 문자의 조합을 오래 기억하는 것은 사실상 힘들다.

그런 반면에 이미지기반 인증시스템을 이용한 인증의 경우 이미지의 인식에 기반하기 때문에 기억에 의한 경우에서보다 인증 통과률이 훨씬 높게 나타났다.[16]

4.1 공격측면

합법적인 사용자를 가장하여 인증을 시도하는 경우의 공격과 방어수단을 고려한다. 패스워드 인증의 경우 합법 사용자를 가장한 가장공격(impersonation attack)의 경우 방어 수단으로서는 패스워드의 자릿수를 늘리거나 알파벳과 숫자의 조합으로 만든 패스워드의 사용, 그리고 특수문자의 사용 등으로 해결하고 있다. 본 시스템에서는 위장 공격자가 성공할 확률은 질문세트에서의 이미지 총 수 **n**과 제시된 포트폴리오 중 인식해야할 이미지 수 **m**에 달려 있다. 이것은 각각의 이미지 수 **n**과 **m**의 수를 조절함으로써 패스워드인증 시스템보다 강화된 보안 수준을 어렵지 않게 확보할 수 있게 된다.[16]

만약 위장 공격자가 사용자의 포트폴리오 이미지 사용의 선호도를 알고 있다면 불법적으로 사용자 인증이 가능하다고 생각이 되나, 이에 대항하기 위해 추상이미지를 사용하였다.[15] 만약 사진들이 추상 이미지 대신에 사용되게 되면 사람들은 포트폴리오를 심미적인 그림들로 구성하려는 경향이 강하게 나타나므로 위장 공격자가 예측하기에 보다 더 쉽다는 것을 나타내 준다.[16]

어떤 취약한 이미지도 보안시스템 서버가 제공할 수 없도록 미리 잘 선별되어야 하고, 서버에서 10000개 이상의 고정된 세트의 이미지들로 가능하기 때문에 결점이 되지 않는다.

또한 패스워드 인증방식의 경우 공격자가 합법 사용자의 로그인 과정에서 관찰을 통해 패스워드를 파악하기가 쉬우나 이미지기반 인증시스템의 경우 공격자가 이미지 관찰하기를 계속하여 이후에 보안 수준이 약화되었다 하더라도 질문세트의 포트폴리오 이미지들의 위치가 임의로 추출되기 때문에 관찰하는 것만으로는 합법사용자를 위장하기는 힘들게 된다.

사용자는 자신의 포트폴리오 이미지 생성단계와 훈련단계에서 보안도가 높은 환경에서 이미지를 관찰하였기 때문에 앞서 논의한 가장 공격에 대하여 충분히 대처할 수 있으며, 자신의 포트폴리오 이미지를 타인에게 공유하기 또한 매우 어렵게 된다. (이미지가 나타나는 위치가 아닌 추상이미지 자체의 인식을 기반으로 하므로) 이것은 패스워드 인증의 경우 패스워드가 타인에 노출되거나 또는 한 사용자가 다른 사용자에게 일부러 패스워드를 가르쳐 줌으로 해서 나타날 수 있는 불법 사용이 가능하게 되나 본 이미지기반 인증시스템의 경우에는 그런 것이 근본적으로 매우 어렵게 된다. 이것은 경우에 따라 매우 큰 장점으로 작용할 수 있다.

4.2 사용의 편리성 측면

현재 가장 많이 사용되고 있는 지식기반의 패스워드 인증이나 PIN인증의 경우에는 웹사이트에서의 인증 시스템의 구현이나 이용에 큰 어려움이 없다. 이미지기반 인증시스템을 이용하는 경우에 웹사이트 인증 구현에는 어려움이 없으나 인증 이미지의 선별, 질문세트 구성 방법 및 거기에 사용되는 이미지의 크기 등 사용자 인터페이스 처리에 추가적인 노력이 필요하다.

그리고 지식기반 인증시스템의 경우보다는 확률적으로 매우 낮지만 사용자가 자신의 포트폴리오 이미지를 잊은 경우 포트폴리오 재구성 단계가 보안환경에서 이루어져야 하는데 거기에 어려움이 따른다.

5. 결론 및 향후과제

앞서 지식기반 인증시스템이 이미지기반 인증시스템보다 취약함을 기술하였으며, 기존에 제안된 시스템의 취약점에 대한 해결책의 대부분은 기술적인 개선 또는 사용자 교육에 의존해 왔다. 지식 기반 인증시스템의 기본적인 문제에 대한 어떤 해결책에서도 인증 작업은 비밀의 정확한 기억력에 근거하고 있다.

따라서 본 논문은 사람들이 패스워드 구문의 정확한 숙지보다는 이전에 자신이 보았던 이미지를 알아보는 것에 훨씬 능숙하기 때문에 인증을 위해 인식기반 접근법을 사용하였다. 이 방법은 인증 작업을 더 믿을 만하고, 더 쉽고 재미있게 하며, 추가적으로 사용자들이 취약한 패스워드의 선택을 방지하고, 암호를 기록하는 것과 다른 사람들에게 전달하는 것을 어렵게 하여 확실히 본인임을 인증 받아야 하는 경우에

더 유효하게 사용될 수 있다.

또한 텍스트로 된 패스워드의 입력이 힘든 초등학교 저학년 학생의 경우나 패스워드가 가끔씩 드물게 사용되는 경우 및 패스워드가 자주 바뀌어야 하는 상황에 가능성 있는 응용이다. 한편 인증에 사용되는 추상이미지의 생성과 선택 및 사용자의 수준을 고려한 구체적인 인증등급의 설정 등은 남은 과제로 계속 연구되어야 한다.

[참고문헌]

[1] Jakob Nielsen, "*Usability Engineering*", Academic Press, 1993.

[2] Ralph Norman Haber, "How we remem-ber what we see", *Scientific Americ*an, 222(5):104-112, May 1970.

[3] L. Standing, J. Conezio, and R.N. Haber. "Perception and memory for pictures: Single-trial learning of 2500 visual stimuli", *Psychonomic Scienc*e, 19(2):73-74, 1970.

[4] Helene Intraub, "Presentation rate and the representation of briefly glimpsed pictures in memory", *Journal of Experimental Psychology: Human Learning and Memor*y, 6(1):1-12, 1980.

[5] A. Paivio and K. Csapo, "Concrete image and verbal memory codes", *Journal of Experimental Psycholog*y, 80(2):279-285, 1969.

[6] Adrian Perrig and Dawn Song, "Hash visualization: A new technique to improve real-world security", In *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce (CryTEC '99)*, 1999.

[7] B. Cheswick and S. Bellovin, "Firewalls and internet security: Repelling the wily hacker", 1994.

[8] R. Morris and K. Thompson, "Password security: A case history", *Communications of the AC*M, 22(11), Nov 1979.

[9] Daniel Klein, "A survey of, and improvements to, password security", In *Proceedings of the USENIX Second Security Workshop, Portland, Orego*n, 1990.

[10] D. C. Feldmeier and P. R. Karn, "UNIX password security - ten years later (invited)", 1989. Lecture Notes in Computer Science Volume 435.

[11] D. Muffett, "Crack: A sensible password checker for unix", 1992. A document distributed with the Crack 4.1 software package.

[12] Udi Manber, "A simple scheme to make passwords based on one-way functions much harder to crack", *Computers and Security*, 15(2):171-176, 1996.

[13] Anne Adams and Martina Angela Sasse, "Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures", *Communications of the AC*M, 42(12):40-46, December 1999.

[14] W. Belgers, "Unix password security", 1993.

[15] Andrej Bauer, "Gallery of random art. WWW" at http://andrej.com/art/, 1998.

[16] Rachna Dahmija, Adrian Perrig, "DejaàVu: A User Study Using Images for Authentication", Oct 2000.

[17] 공병운,""결합허용기법을 이용한 신분확인 방안",",석사학위논문, 부경대학교, 2001.8.