教育學碩士學位論文

학내망에서 이미지를 이용한 사용자 인증에 관한 연구

2002年　8月

釜慶大學校 教育大學院

電算教育專攻

金 基 引

教育學碩士學位論文

학내망에서 이미지를 이용한 사용자 인증에 관한 연구

指導敎授　朴　志　煥

이 論文을 敎育學碩士 學位論文으로 提出함

2002年　8月

釜慶大學校 敎育大學院

電算敎育專攻

金 基 引

김기인의 교육학석사 학위논문을 인준함

2002년 6월 22일

주심 이학박사 박만곤 (인)

위원 공학박사 박승섭 (인)

위원 공학박사 박지환 (인)

<제 목 차 례>

<표 차 례>

<그림차례>

A Study of User Authentication Using An Image in School Network

Ki In Kim

Graduate School of Education
Pukyong National University

Abstract

User authentication is a central component of currently deployed security infrastructures. Most of current secure systems neglect the importance of human factors in security. The user authentication through image recognition used to solve the human limits of conventional identification system that depend on ID or password.

In this paper we propose an efficient authentication using images instead of recall-based authentication. We designed the authentication system that can overcome general password authentication system's demerits, so you could replace the existing password system to new one. Especially, we can use this system in school network. In school, the network traffic is not so high compared with the Internet. So the image based authentication system can be used efficiently for school network. And also it can be used for children who can't understanding a letter instead of password system. Comparing the existing password system with, this system has the advantage that the authentication task is more reliable, easier and fun. In addition, this system prevent users from choosing weak password and make it difficult for users to write passwords down and to communicate them down.

I. 서 론

최근 인터넷의 활용이 늘어나면서 웹을 기반으로 하는 많은 사이트들이 나날이 늘어나고 있다. 사회에서뿐만 아니라 각급 학교 내에서도 인터넷을 활용한 수업, 인터넷을 이용한 각종 학습 자료의 제공 및 학습 결과의 평가 등이 다양한 형태로 이루어지고 있다. 이러한 인터넷을 이용한 정보의 획득은 기존의 오프라인 형태의 이용에서보다 시간적, 공간적인 제약을 해소해 줄 수 있을 뿐만 아니라 다양한 정보를 보다 쉽게 획득할 수 있다는 점에서 많은 이점이 있다. 그러나 이러한 편리한 점이 있는 반면에 정보를 제공하고 이용하는 서버와 클라이언트 사이에 사용자 인증이 필수적인 요소가 되었다. 이러한 인증은 일반적으로 사용자의 아이디와 패스워드를 사용한 로그인(login)이라는 과정을 통해서 이루어지지만 이 과정에서 사용자의 패스워드가 노출되거나 도용이 되는 등 보안상의 많은 문제점이 발생하고 있다. 이러한 문제점을 해결하기 위해 여러 가지 인증 방법을 통해 사용자 인증 문제를 해결하려고 하고 있다.

인증 방식으로는 인증서를 이용하는 방법, 사용자가 패스워드를 암기해 사용하는 지식 기반 시스템(knowledge based system), 신용카드나 스마트카드 등의 하드웨어 장치 등을 이용하는 토큰 기반 시스템(token based system) 그리고 지문이나 홍채 등의 신체적 특징을 이용하는 생체 인식 기반 시스템(system based on biometrics) 등이 있다. 인증서를 사용하기 위해서는 인증기관으로부터 인증서를 발급 받고 이를 관리하기 위한 절차가 필요하며, 토큰 기반 시스템이나 생체 인식 기반 시스템의 경우에는 특별한 하드웨어적 장비들을 필요로 한다. 반면에 지식 기반 인증 시스템은

별도의 절차나 장비 없이 쉽게 사용자를 인증할 수 있어 가장 보편적으로 사용되고 있는 실정이다.

현재 가장 널리 사용되고 있는 지식 기반 인증은 패스워드 및 PIN(Personal Identification Number) 인증 방식이 사용되고 있으나, 이 역시 패스워드 관리상의 어려움이 존재한다. 즉, 단순하고 개인과 관계 있는 패스워드는 기억하기 쉬우나 공격에 취약하며, 복잡하고 의미를 지니지 않은 패스워드는 보안성은 있으나 사용자가 이를 기억하기가 쉽지 않다. 또한 사람의 기억력에는 한계가 있어 오직 제한된 수의 패스워드만을 기억할 수 있기 때문에 여러 곳에서의 사용을 위해서 그것을 기록해 두거나 또는 동일한 패스워드를 사용하는 경향이 있다.

이러한 문제점에 대한 해결 방안으로 이미지 인식 기반 인증 방식이 Perrig과 Song에 의해 제안된 바 있으며[1], 이는 사용자 인증을 개선하기 위한 접근 방법으로 패스워드나 PIN의 정확한 기억을 통한 지식 기반 인증 대신에 사용자가 이전에 보았던 이미지에 대한 인식을 바탕으로 하고 있다.

일반적으로 사람들은 다른 도움 없이 기억력에 의존하여 정보를 상기해 내는 것보다 어떤 것을 인식하는 것이 훨씬 쉬우며[8], 또한 이미지 인식 실험에 따르면 인간이 특히 그림(또는 이미지)에 대해 뛰어난 인식력을 가지고 있다는 것이 증명되었다. 그리고 또 다른 실험에서 사람들이 매우 짧은 순간에 수백에서 수천의 그림들을 기억하고 인지할 수 있다는 것이 확인되었다[9].

따라서, 패스워드에 대한 정확한 기억을 요구하기보다는 이미지에 대한 인식으로 대체함으로써 사용자 인증에서의 오류를 최소화 할 수 있다. 본 논문은 앞서 제시된 인식기반 인증 개념에 근거하여 패스워드가 드물게 가끔씩 사용되는 경우와 패스워드가 자주 바뀌어야 하는 경우 및 패스워드

의 사용이 부적절한 초등학교 저학년 아동들에게 적용 가능한 이미지 인식에 기초한 새로운 인증 시스템을 설계하고 기존의 패스워드기반 인식시스템과 비교하였다. 본 논문에서는 일반적인 상업적인 인터넷 망의 접속을 배제하고 일반적인 초, 중, 고 각급 학교 학내망에서의 학생들의 수업관련 사이트 등에의 접속을 전제로 기술하였다.

본 논문의 구성은 2장에서 기존에 널리 이용되는 패스워드 기반 인증을 위주로 사용자 인증 방식에 대하여 기술하고, 3장에서는 이미지 인식에 의한 새로운 사용자 인증 시스템을 설계하고, 4장에서 구현 및 분석을 하며 5장에서 본 논문을 요약하고 결론을 맺는다.

Ⅱ. 사용자 인증 방식

사용자 인증은 오늘날 보안 구조의 중심 구성 요소라 할 수 있다. 사용자 인증 방법은 크게 나누어 다음의 3가지로 구별할 수 있다[12].

(1) 지식 기반 시스템(Knowledge Based System)
(2) 토큰 기반 시스템(Token Based System)
(3) 생체 인식 기반 시스템(System Based on Biometrics)

지식 기반 시스템은 현재 가장 널리 사용되고 있는 패스워드 기반 인증 및 개인 식별번호(PIN; Personal Identication Number)를 이용하는 인증 시스템이다. 이 경우 본인은 자신만이 알 수 있다고 여겨지는 정보를 소유하고 있음을 보임으로써 인증시스템으로부터 신분을 확인 받게 된다. 이것은 사람의 기억력을 기초로 하고 있으며 다음과 같은 특징을 지닌다.

2.1 패스워드 인증 방식

2.1.1 일반 패스워드 방식

이것은 지식 기반 인증의 대표적인 예이다. 패스워드 인증 방식에서 사용자는 보안 시스템이 본인임을 확인하기를 요구하게 되는 경우를 위해 자신만의 고유한 ID와 일정한 패스워드를 사용하기로 하는 것이다. 패스워드는 본인과 보안시스템 서버 외에는 모르는 것이 원칙이므로 패스워드를 알

고 있다는 것은 그 사람이 이전에 보안시스템 서버에 패스워드를 등록했던 사람이라는 것을 의미한다. 패스워드 방식은 신분 확인에 있어 가장 기본적이면서도 간단한 방식이므로 현재 대부분의 회원제 웹사이트에서 채택하고 있는 방법이다. 이 때 패스워드는 개별적인 특성을 갖기 위해 일정한 길이 이상일 것, 또 흔하지 않은 것이어야 한다는 제약을 받는다.

그러나 이러한 패스워드 방식은 다음과 같은 문제점이 있다고 지적된다 [15].

① 패스워드 전송 노출 : 사용자가 전송하는 ID와 패스워드는 어떠한 안전장치 없이 전송되므로 도청과 같은 불법행위로서 패스워드를 쉽게 획득할 수 있어, 이 과정서 패스워드 노출의 위험이 있다.

② 패스워드 재전송 : 현재 사용중인 패스워드는 다음 번 인증시에도 그대로 사용되므로[1] 전송시 패스워드 정보를 복사한 경우 쉽게 신분 위장이 가능하다.

③ 서버 인증 정보 공격 : 서버가 보관하고 있는 각 사용자의 인증정보가 노출될 경우 쉽게 패스워드를 획득할 수 있고, 전송되는 사용자 인증 정보를 가로채 서버로 가장할 수 있는 문제점이 발생한다.

④ 별도의 키 분배 방식 필요 : 만약 사용자와 인증시스템 서버가 비밀 통신을 수행하려 할 경우 별도의 키를 생성해서 사전에 공유해야 하는 번거

[1] 쿠키 기능이 웹상에서 일반적으로 채택됨에 따라 이러한 위험성은 더욱 증가되고 있다. 쿠키(Cookie)란 고객이 특정 홈페이지를 접속할 때 생성되는 정보를 담은 임시 파일로 크기는 4KB 이하로 작다. 쿠키는 인터넷 사용자들의 홈페이지 접속을 돕기 위해 만들어진 것으로 특정 사이트를 처음 방문하면 아이디와 비밀번호를 기록한 쿠키가 만들어지고 다음에 접속했을 때 별도 절차 없이 사이트에 빠르게 연결할 수 있다.

로움이 발생한다.

이처럼 패스워드 방식은 전통적인 신분 확인 이론을 단순히 인터넷 사용자 인증 방식으로 적용시킨 것일 뿐, 인터넷이라는 매체가 갖고 있는 특별한 보안상 문제점을 해결하기 위한 수단을 갖고 있지 않다.

2.1.2 변형 패스워드 방식

이 방식은 위 일반 패스워드 방식의 결점을 보충하기 위하여 해시함수(Hash Function)[2]를 이용한다. 즉 사용자의 ID와 패스워드를 해시함수를 이용하여 전송함으로써 제3자에 의한 도청을 방지하고, 전송과정에서의 노출을 막고 있다. 또한 패스워드 재전송을 방지하기 위해 난수 값을 사용하고, 서버 인증 정보 공격을 막기 위해 해시함수로 생성된 정보를 그대로 사용함으로써 안전성을 확보할 수 있게 된다.

그러나 이 방식은 각 ID 소유자가 각각 하나의 패스워드를 소유하고 있고 또한 해시함수가 공개되어 있다고 가정하고 있으므로 사용자 인증 정보 전송시 및 서버 인증시에 이에 대해 공격자의 동시적인 공격이 행해질 경우 사용자 위장을 막을 수 없다는 문제점이 제기된다.

2.1.3 일회용 패스워드(One-Time Password) 방식

[2] 해시함수(Hash Function)는 어떠한 입력값에 대해 입력값보다 간결한 정해진 길이를 갖는 값을 생성해내는 함수로서, 역방향의 연산이 매우 어려운 특성을 갖고 있다. 즉 원문에 해시함수를 적용시키면 일정한 값(해시값)이 얻어지는데 반대로 해시값을 통해 원문을 알아낼 수는 없다. 이 때 확인자는 자신이 받은 메시지의 해시값을 계산하여 송신자의 해시값과 비교하여 원문이 본인에 의해 작성되었는지, 그 내용의 변경이 있었는지를 알아낼 수 있다. 현재 널리 사용되고 있는 해시함수로는 MD5, SHA 등이 있다.

이는 보안 시스템에 접근을 위한 패스워드를 예측할 수 없도록 그때그때 동적으로 산출하는 방식을 의미한다. 이 방식에서 한 번 사용된 패스워드를 다시 사용하여 접속을 하게되면 오류를 일으키고 접속요구가 거절된다. 이를 위해서는 일회용 패스워드를 생성하는 프로세서를 내장한 카드(Token Card)를 사용자가 소유하고 있을 것이 요구된다. 이는 결국 광의의 토큰기반인증에 속한다고 볼 수 있으며, 따라서 인터넷과 같은 광범위한 네트워크에 일반적으로 적용하기엔 적절치 못하다.

2.1.4 패스워드 방식의 검토

일반적으로 신분 확인이라는 것은 특징적 가치의 일치에 의해 이루어지기 때문에 그러한 특징적 가치가 타인에 의해 사용되는 한 신분 불법도용을 근원적으로 막을 수는 없다. 따라서 일반적으로 신분 확인 절차의 신뢰성을 제고시키기 위해서는 ①특징적 가치 자체를 비밀화하거나, ②타인에게 쉽게 도용당할 가능성이 없는 특징적 가치를 설정해야 한다. 그런데 패스워드 방식은 아무리 발전된 형태를 가진다 하더라도 기본적으로 지식 기반 인증(또는 이와 토큰기반인증의 결합)의 방법이기 때문에, 그 지식을 타인이 알게 된다면 타인의 신분 도용 행위를 막을 수 없다는 한계를 가진다. 즉, 패스워드 방식은 위 ②의 관점에서 볼 때 너무나 쉽게 도용당할 위험이 큰 상당히 취약한 신분 확인 방법이 아닐 수 없다. 또한 패스워드를 설정하기 전의 ID 설정단계에서 현재 대다수의 웹사이트들은 일반적으로 실명과 주민등록번호를 요구하고 있는데, 실명과 주민등록번호 역시 비밀로 하기에는 지나치게 공개적인 자료라는 점에서 타인의 신분을 도용하여 ID를 만들 수 있어 문제가 된다. 따라서 패스워드 방식은 필연적으로 그 패스워드 자체를 비밀화, 즉 암호화하는 방식과 연결되지 않을 수 없다. 이에 따라 전자서명 방식의 도입이 필요하게 된다.

2.2 PIN(Personal Identication Number; 개인식별번호) 인증 방식

PIN 인증 방식은 현금 자동 지급기나 스마트 카드 등과 같은 장치에 대한 접근 관리를 위해 개인에게 부여된 개인 식별 번호를 이용하여 인증하는 것이다.

2.3 토큰 기반 인증

토큰 기반 인증(Token Based Identification)은 오프라인에서 주민등록증, 여권 등과 같이 자신의 신원을 확인시켜줄 수 있는 증거(Token)를 소지하고 있음으로써 확인하듯이 사용자 인증시 스마트 카드가 인증된 사용자에게 제공되어지고 그것을 소유한 사람이 전자적인 인터페이스를 통하여 컴퓨터와 안전하게 통신하는 방법이 제공되는 시스템을 말한다. 인터페이스가 무엇이든 간에 인증 시스템은 컴퓨터와 교환되어지는 암호화된 메시지를 계산하고 확인하기 위해 스마트 카드를 사용하게 된다. 스마트 카드는 난수 발생과 암호화 알고리즘 그리고 독자적인 소유자 인증을 수행하는 프로세서 역할과 인증 기능 수행을 위해 개인 정보를 담는 휴대용 저장 장치 역할을 해낸다.

보통 스마트 카드를 이용한 인증의 경우에도 대부분은 보안도의 증진을 위해 PIN 또는 패스워드를 병행 사용하는 경우가 많이 있다.

스마트 카드를 비롯한 토큰 기반 인증의 경우에는 현재 누구 나 구매할 수 있을 정도로 가격을 일반화시킬 수 있느냐의 문제와 타인에의 도용 문

제가 항상 문제점이기 때문에 본인여부를 확인하기 위한 부가적인 인증(패스워드 인증 또는 생체 인식 기반 인증)이 필요하다는 것이 단점이라 할 수 있으며 또한 토큰의 제조 기술이 아직은 완전하다고 할 수 없다.

2.4. 생체 인식 기반 시스템(System Based on Biometrics)

생체인식은 살아있는 신체의 특정부위를 통해 보안 도구로 열쇠나 카드, 또는 패스워드가 아니라 자신의 지문이나 음성을 통해 신분확인을 수행하는 기법이다. 주로 이용되는 생체 척도는 인간의 눈과 지문, 얼굴, 음성, 손등, 장문 등 개인의 신체 일부분이 이용되고 있으며 최근에는 이와 관련된 신분을 확인하는 각종 생체인식시스템이 분야별로 많이 개발되어져 오고 있다

신체 정보는 사람마다 다르고 위조가 매우 어려우며 잊거나 분실할 염려가 없다는 점에서 훨씬 안전하고 정확한 신분증명 수단으로 얼굴 모양이나, 음성, 지문, 안구 등과 같은 개인의 특성은 열쇠나 비밀번호처럼 타인의 도용이나 복제에 의하여 이용될 수 없을 뿐만 아니라, 변경되거나 분실할 위험성이 없어, 보안 분야에 활용도가 뛰어나다.

특히, 생체측정학(Biometrics)은 이용자에 대한 사후 추적이 가능하여 관리적인 측면에 있어서도 안전한 시스템을 구축할 수 있다는 장점이 있으며 신체적 특징을 이용한 방법으로 물리적 특성을 이용한 것과 행동적 특성을 이용한 것으로 구분할 수 있다. 물리적 특성을 이용한 분야로 지문, 장문, 손 모양, 망막, 홍채, 얼굴, 혈관과 같은 것이 있고, 행동적 특성을 이용한 것으로는 서명, 음성, DNA, 족적, keystroke dynamics 등이 있으며 이들도 생체측정학의 분야로서 꾸준히 연구되고 있다.

생체측정학을 이용하여 개인식별 또는 인증을 자동적으로 해 주는 장치를 생체측정시스템이라 하며. 이러한 장치는 사회구조가 다양해지고 전문화됨에 따라 인력의 효율적인 관리, 보안을 위한 출입관리 및 정보관리 등에 활용되고 있으며 이에 따른 다양한 생체측정시스템이 개발되어 있다

2.5 패스워드기반 인증에서의 실제적인 문제

현재 웹사이트 인증으로 가장 널리 이용되는 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[5].

지식기반 인증 시스템의 중요한 약점은 그 비밀 정보를 사람의 정확한 기억력에만 의존한다는 것이다. 만약 사용자가 패스워드 입력시 작은 실수를 하게 되면 인증은 실패한다. 그러나 정확한 기억력은 인간의 강점이 아니며, 이전에 경험한 자극의 인식에서 부정확한 기억에 훨씬 능숙하다[9]. 정확한 기억력에 대한 인간 한계는 견고한 패스워드의 필요조건과 서로 상충된다. 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. 그리고, Klein은 패스워드 보안에 관한 광범위한 연구에서 모든 패스워드의 25%가 사전공격(dictionary attack)에 의해 깨질 수 있다는 것을 주장하였다[6]. 또한 패스워드 크래커 프로그램들의 등장으로 사용자들에 대해 패스워드를 더욱 어렵고 예측 불가능하게

만들도록 요구되며, 결과적으로 패스워드를 기록해 두거나, 작업 공간에 그것을 숨기게 된다. 또한 보안 정책에 의해 패스워드를 정기적으로 바꾸도록 요구하는 것은 결국 사용자들로 하여금 그들의 패스워드를 보다 잘 기억하기 위해 패스워드를 기록해 두는 사용자의 수만 증가시킬 뿐이다[7].

IT 기반 구조의 보안성을 제고하기 위한 시도를 하는 회사의 수와 패스워드 보호영역의 수는 계속 증가하고 있고, 동시에 사용자 ID와 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 않다는 것이다[10].

취약한 패스워드 문제를 해결하는 3가지 해결책으로는 첫째, 패스워드에 대한 사전공격에 의해 노출되기 전에 취약한 패스워드를 발견하려는 사전 노력이며[7] 둘째, 패스워드 크래킹의 계산 부하를 증가시키는 기술적인 기법을 이용하는 방법[13]과, 셋째, 사용자들의 보안 의식 향상을 위한 지속적인 보안 교육의 강화[3][4] 등이 있다. 그러나 이들 중 어느 하나라도 패스워드 인증 결점의 주 원인을 제거하지는 못한다. 그것은 패스워드기반 인증이 이상적인 인간 기억력에 의존하기 때문이며, 원인이 인간 기억력의 한계에 있기 때문이다.

Ⅲ. 사용자 인증 시스템의 설계

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

▣요구 조건

① 새로운 시스템은 인간의 기억력에만 의존해서는 안된다.

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

③ 시스템은 사용자들이 취약한 패스워드를 선택하는 것을 막아야 한다.

④ 사용자들이 패스워드를 기록하거나, 다른 사람들과 공유하는 것을 어렵게 해야 한다.

3.1 시스템 구조

본 시스템은 사람이 지닌 이미지에 대한 뛰어난 기억력에 대한 관측에 근거하고 있다[9]. 사용자는 자신이 본인임을 인증받기 위해 주어진 이미지들을 정확하게 확인해야 한다.

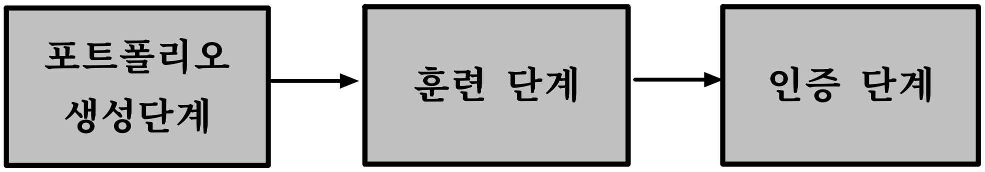
사용자는 서버에서 제공하는 견본 이미지 세트에서 N개의 이미지 부분집합을 선택하는 것으로 자신의 이미지 포트폴리오를 생성한다. 사용자를 인증하기 위하여 보안시스템은 **n**개의 이미지들로 이루어진 질문세트를 제

시한다. 이 질문세트는 사용자의 포트폴리오에서 m개의 이미지들을 포함하고 있다. 여기에서 남아 있는 n-m개의 이미지를 미끼(decoy) 이미지라고 부른다. 인증 받기 위해 사용자는 자신의 포트폴리오의 일부분인 이미지들을 정확하게 인식해야 한다.

3.2 이미지기반 인증시스템의 구성단계

이미지기반 인증시스템은 다음의 3단계로 구성된다.

(1) 포트폴리오 생성단계
(2) 훈련단계
(3) 인증단계



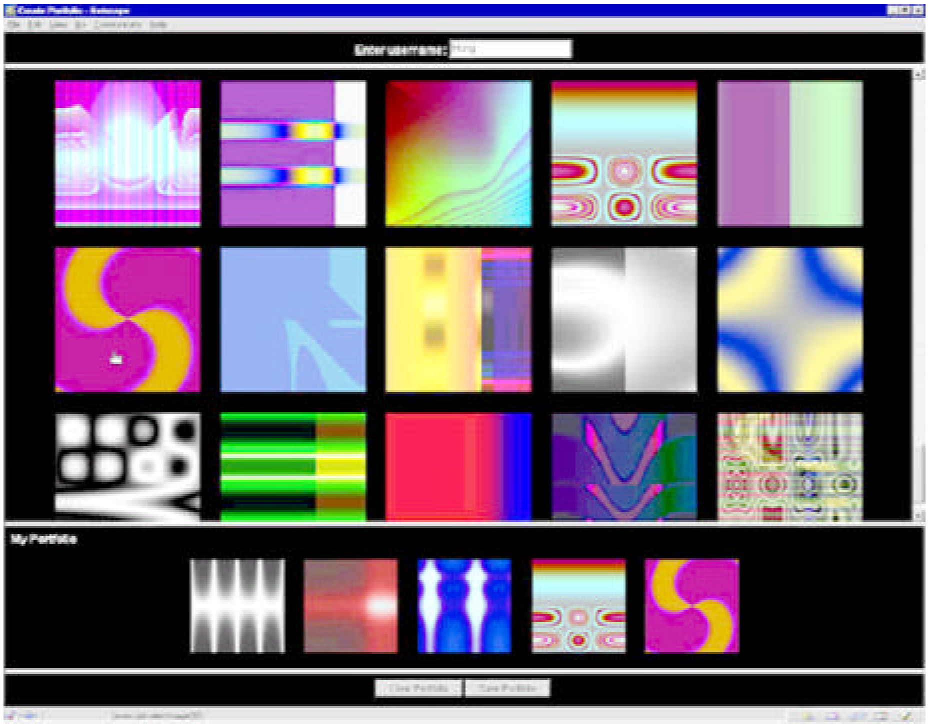
<그림 1> 이미지 인증 시스템의 구성 단계

<표 1> 이미지 인증 단계별 과정

1 단계	2 단계	3단계
포트폴리오 생성 단계	훈련 단계	인증 단계
서버에서 제공하는 견본 이미지 세트로부터 사용자 개인의 포트폴리오 이미지를 생성한다.	사용자 자신의 포트폴리오 이미지를 기억하기위한 단계이다.	보안시스템 서버에서 사용자의 포트폴리오 이미지가 포함된 질문 세트를 제시하면 사용자가 인증받기 위해 자신의 이미지를 정확하게 선택하는 단계이다.

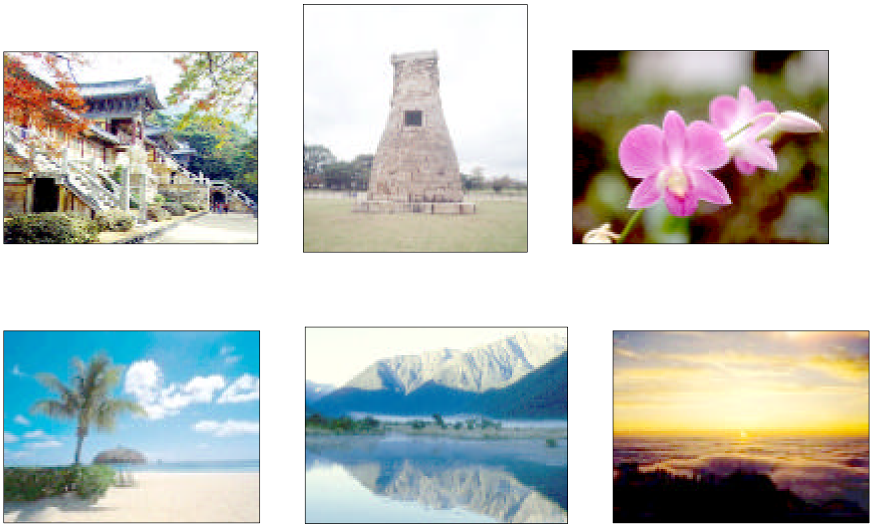
3.2.1 포트폴리오 생성단계

본 시스템의 첫 번째 단계는 사용자들이 앞으로 인증에 사용될 자신만의 이미지 세트를 구성하는 과정이다. 인증에 사용되는 사용자의 이미지 세트를 그 자신의 포트폴리오(Portfolio)라 부른다. 이미지 기반 인증시스템의 이미지 포트폴리오 구성을 위하여, 사용자는 보안시스템 서버에서 제시하는 큰 규모의 이미지 세트로부터 구체적인 수의 자신만의 이미지를 선택한다.



<그림 2> 이미지 선택화면의 예

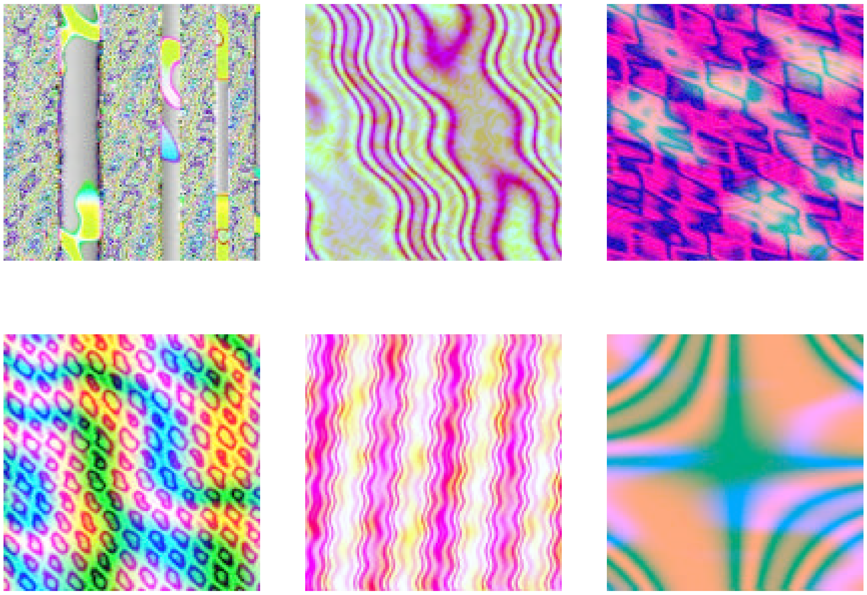
위의 <그림 2>는 이미지기반 인증시스템의 이미지 선택 화면의 예를 보여주고 있다. 본 인증시스템에 사용되는 이미지의 형태는 시스템의 보안에 매우 큰 영향을 주게 된다. 예를 들면, 실제적인 사진 이미지를 사용할 경우 사용자들이 예측할 수 있는 포트폴리오 이미지들을 선택하게 되고 또한 공격자는 사용자의 개인 성향을 예측하여 포트폴리오 이미지들을 추측할 수 있는 시도를 할 수 있게 되며, 또한 사용자가 자신의 포트폴리오 이미지에 대한 정보를 기록하기가 용이해지며, 그것을 다른 사람들과 공유하기 쉽게 되는 결점이 나타날 수 있다.



<그림 3> 일반적인 사진 이미지(1)

<그림 4> 일반적인 사진 이미지(2)

이러한 보안상의 특징에 따라서 본 시스템에서는 무작위로 추상이미지를 만들기 위하여 Andrej Bauer의 추상이미지(Random Art)를 사용한다[2].

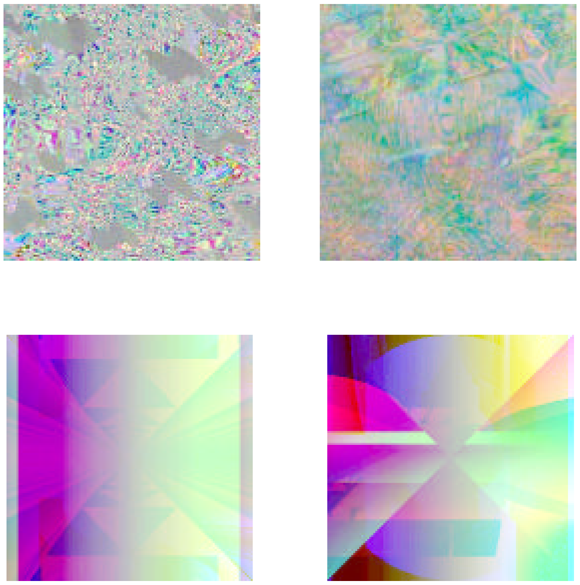


<그림 5> 추상 이미지(Random Art Image)

<표 2> 이미지의 종류에 따른 보안상의 특징

이미지의 종류	사진 이미지	추상 이미지
이미지의 예		
보안상의 특징	1) 타인에 의한 예측이 가능 2) 이미지 정보 기록이 용이 3) 타인과의 공유가 용이	1) 이미지 예측이 어려움 2) 이미지 정보 기록이 어려움 3) 타인과의 공유가 어려움

<그림 6> 너무 단순한 추상 이미지



<그림 7> 서로 유사하여 혼동될 수 있는 이미지

그리고 보안시스템에 사용되는 이미지들은 <그림 6>과 같이 너무 단순하거나 <그림 7>과 같이 시각적으로 유사한 이미지들은 사용자들에게 혼돈을 일으켜 보안에 영향을 미칠 수도 있으므로 제거되고 없는 상태이다.

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

3.2.2 훈련 단계

사용자들은 포트폴리오 생성 단계 이후에 그들의 포트폴리오 이미지에 대한 기억을 증진시키기 위하여 간단한 훈련 단계가 필요하다. 훈련단계에서 사용자는 미끼이미지들을 담고 있는 질문세트로부터 자신의 추상이미지

들을 선택하는 과정을 반복하게 된다. 이것은 뒤에 자신의 포트폴리오 이미지들을 선택하여 인증받기 위해 필요한 절차이다. 앞에서 언급했듯이 사람의 이미지 인식력은 문자나 숫자에 비해 월등히 앞서므로 일련의 훈련과정을 통해 자신의 이미지를 확고하게 인식하게 된다.

포트폴리오 생성 및 훈련 단계는 사용자 이외의 어떤 사람도 이미지 포트폴리오를 볼 수 없는 그런 안전한 환경이 요구된다.

3.2.3 인증 단계

신뢰할 수 있는 보안시스템 서버는 각 사용자를 위한 모든 포트폴리오 이미지를 저장하고 있다고 가정한다.

각각의 사용자들의 인증 시도에 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 $1/\binom{20}{5}=1/15504$ 또는 $1/\binom{25}{5}=1/53130$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.

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

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

이렇게 함으로써 초등학교 저학년 어린이들에게도 충분한 신뢰성을 가지는 인증시스템을 도입할 수 있게 된다. 이는 결함허용기법(Fault-Tolerant Scheme)을 도입하여 인증 허용의 수준을 고려한 경우와 같다[14].

3.3 공격과 대항수단

이미지 인증 시스템에서 실제 사용자를 가장하여 들어오는 공격자에 대한 대항 수단에 대하여 다음과 같이 설명할 수 있다.

3.3.1 완력공격(Brute Force Attack)

위장 공격자는 질문세트에서 추상 이미지를 고르는 것으로 실제 사용자 역을 맡는 것을 시도한다. 그 이미지들이 실제 사용자의 이미지이기를 바라면서.

위장 공격자가 성공할 확률은 $1/\binom{n}{m}$ 이것은 질문세트에서의 이미지 선택 수 n과 제시된 포트폴리오 이미지수 m에 달려 있다.

이러한 위장 공격자의 완력 공격을 예방하기 위하여 인증 시스템은 몇 차례의 시도 후에 접근을 차단할 필요가 있다. 이는 패스워드 시스템에서도 사용되는 일반적인 방법이다.

3.3.2 경험적 추측 공격(Educated Guess Attack)

만약 위장공격자가 이미지들에 대한 실제 사용자의 기호(선호)를 알고 있다면 어떤 이미지들이 실제 사용자의 포트폴리오인지를 예측할 수 있다.

이에 대한 첫 번째 대항 수단은 위장공격자로 하여금 그가 실제 사용자의 기호를 알고 있다 하더라도 실제 사용자의 포트폴리오 이미지의 추측을 어렵게 하는 추상이미지(Random Art)를 사용하는 것이다. 그렇지 않고 추상이미지 대신에 실제 사진이 사용되면 실제 사용자에 대한 약간의 지식으로 포트폴리오 이미지들을 예측하는 것이 더 쉽게 된다. 사용자들은 대부분 그들의 포트폴리오를 심미적인 그림들로 구성하려는 경향이 나타나므로 질문세트 구성 시 그러한 이미지들은 미리 삭제되어야 한다. 따라서 이미지 인증 시스템은 어떤 취약한 이미지도 사용되지 않음을 확실히 하기 위하여 이미지들을 직접 수작업으로 선택해야 한다.

3.3.3 관찰자 공격

Ross Anderson은 ATM(현금자동지급기;Automated Teller Machine)에서의 신분 위장 사용에 있어 PIN코드 관측을 보여준다[11]. 즉, 만일에 누가 다른 사람의 PIN코드를 관찰하기를 여러 번 반복한다면 그 사람의 정보는 결국 누출 될 것이다.

이미지 인증 시스템의 경우에서도 만약 위장 공격자가 여러 번의 인증과

정을 통해 실제 사용자를 관찰하면, 그는 완전하게 실제 사용자의 포트폴리오 이미지들을 알고 있을 수 있다.

이에 대한 대항 수단은 다음과 같다. 만일 실제 사용자의 포트폴리오 p의 사이즈가 질문세트의 포트폴리오 이미지수 m보다 더 크면, 관찰자가 관찰 후에 같은 포트폴리오 이미지들이라는 것을 알 수 있을 개연성은 $1/\binom{p}{m}$ 이다.

한 관찰자가 비록 포트폴리오 내의 이미지를 관찰하기를 계속한 이후에 보안성이 여전히 약화되었다 하더라도, 관찰자는 아직도 쉽게 실제 사용자를 위장할 수 없다.

이미지들이 오직 실제 사용자만이 유일하게 명백히 그것들을 볼 수 있는 방법으로 보여진다고 가정하면, 관찰자는 실제 사용자에게 주어진 질문세트의 포트폴리오 이미지들의 위치가 임의로 추출되기 때문에 선택한 그 사람을 관찰하는 것만으로는 포트폴리오에 대한 유용한 지식을 얻지 못한다.

포트폴리오 이미지들은 각각의 인증에 약간씩 바뀔 수 있다. 목표는 관찰자에게 포트폴리오에 대한 정보를 거의 누설하지 않으면서 어떤 합법적인 사용자가 그 자신만의 포트폴리오 이미지들을 여전히 확인할 수 있는 것이다.

추후 연구로 이미지 왜곡 방법을 연구하고 어떻게 이미지들의 변형이 사용자들에 의해 감지되는지를 결정하는 것이 필요하다.

3.3.4 교차점 공격(Intersection Attack)

만약 모든 포트폴리오 이미지들이 질문세트의 부분이고 모든 미끼 이미지들이 각 인증 과정 중에 바뀌게 된다면 위장 공격자는 포트폴리오를 밝혀내기 위해 각각의 질문세트들의 교차점(공통점)을 발견해 낼 수 있다. 이것은 심각한 문제가 된다. 그러나 다음의 대항 수단을 통해 이 공격에

대항할 수 있는 시스템을 설계할 수 있다.

같은 질문세트(포트폴리오 이미지들과 미끼 이미지들)는 사용자에게 항상 제시된다. 만약 동일한 것으로 남아 있으면, 교차점 공격은 어떠한 유용한 정보도 누설하지 않게 된다. 그러나 결점은 미끼 이미지들이 많은 로그인 세션을 통해 동일한 것으로 남아 있는 경우에 위장 공격자가 차후의 인증 세션에 그것을 이용할 지도 모르는 경우다. 이런 경우를 알아보기 위해 추후 연구가 필요하다.

미끼 이미지들의 소수가 여러 번의 인증 과정에 질문세트 안에 남아 있다. 이 접근에서의 문제는 사용자들은 인증 과정이 충분히 반복되고 포트폴리오 이미지에 실수를 일으키면 이미지들을 다시 학습해야 할 지도 모른다. 인증시스템은 만약 사용자가 어떠한 단계에서 실수를 하면, 그 후의 모든 단계는 어떠한 포트폴리오 이미지 없이 미끼 이미지들만 보이도록 한다. 이것은 실제 사용자 이외의 여타 사람이 포트폴리오를 발견하기 위해 되풀이된 위장공격을 방어하기 위한 것이다.

이에 따라서 이미지 인증 시스템이 기억 기반의 패스워드나 PIN 인증의 경우보다 실패율이 훨씬 낮다는 것을 알 수 있다.

Ⅳ. 구현 및 분석

기존의 패스워드에 의한 인증은 인간의 기억력에 의존하고 있으며, 이 경우 망각을 피하기 위해 기록을 해두거나 기억하기 쉬운 패스워드를 선택하여 여러 사이트에서 공동으로 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 이미지 인증시스템을 이용한 인증의 경우 이미지의 인식에 기반하기 때문에 기억에 의한 경우에서보다 인증 통과율이 훨씬 높게 나타났다. 이미지 인증 시스템을 기존의 인증방식과 비교하여 외부 공격 측면에서와 사용의 편리성 측면에서 분석하여 보았다.

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 n과 제시된 포트폴리오 중 인식해야할

이미지 수 m에 달려 있다. 이것은 각각의 이미지 수 n과 m의 수를 조절함으로써 패스워드 인증 시스템보다 강화된 보안 수준을 어렵지 않게 확보할 수 있게 된다.

다음 <표 3>은 각각의 이미지 수에 따른 인증에서의 보안도를 나타낸 것이다.

<표 3> 이미지 수에 따른 인증의 보안도

질문세트에 제시된 총 이미지 수	제시된 포트폴리오 중 인식해야 할 이미지 수	인증의 보안도
20	4	1/ 4,845
20	5	1/ 15,504
20	6	1/ 38,760
25	4	1/ 12,650
25	5	1/ 53,130
25	6	1/ 177,100
30	4	1/ 27,405
30	5	1/ 142,506
30	6	1/ 593,775

만약 위장 공격자가 사용자의 포트폴리오 이미지 사용의 선호도를 알고 있다면 불법적으로 사용자 인증이 가능하다고 생각이 되나, 이에 대항하기

위해 추상이미지를 사용하였다. 만약 사진들이 추상 이미지 대신에 사용되게 되면 사람들은 포트폴리오를 심미적인 그림들로 구성하려는 경향이 강하게 나타나므로 위장 공격자가 예측하기에 보다 더 쉽다는 것을 나타내준다[10].

어떤 취약한 이미지도 보안시스템 서버가 제공할 수 없도록 미리 잘 선별되어야 하고, 서버에서 10,000개 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.

한편 이미지 인증 시스템으로의 접속을 하여 인증 과정에서의 네트워크 전송 부하량 문제는 패스워드 인증에 비해 상당량에 이르나 질문세트를 구성하는 이미지의 개수와 크기를 조절하여 충분히 학내망에서의 사용에 지장이 없을 것으로 보인다. 물론, 질문세트의 이미지 개수가 너무 많은 경우 네트웍 부하량이 증가하여 인증에서의 시간이 문제가 될 수 있는데 이에 대해서는 추후에 상세한 연구가 필요하다 하겠다.

본 인증 시스템은 무엇보다도 패스워드 공유를 어렵게 하여 웹에 인증받으려는 사용자가 본인이외는 접속이 어렵도록 하는 데 최대의 장점이 있고, 또한 패스워드를 기록하는 것이 어려우므로 패스워드 보안도가 기존 방식에 비해 더 높아지는 것도 충분히 유효성이 있는 것이다.

<표 4>는 앞서 살펴본 패스워드 인증방식과 이미지 인증 시스템을 비교한 것이다.

<표 4> 패스워드 인증방식과 이미지 인증 시스템의 비교

	패스워드 인증방식	이미지 인증방식
위장 공격에 대한 대책	패스워드의 자리수를 늘리거나 알파벳, 숫자, 특수문자를 혼용하여 사용함	질문세트 전체의 이미지 수와 그 안에 포함되는 사용자의 포트폴리오 이미지 수를 조절
관찰에 의한 공격시	패스워드 관찰에 의해 쉽게 인증 통과 가능성	이미지를 관찰하더라도 인증시마다 이미지가 임의의 위치에 나타나므로 공격이 어려움
타인과의 공유	패스워드를 타인에게 전달가능하므로 공유가 용이	추상이미지의 전달이 어려우므로 공유가 어려움
인증시스템 구현	웹사이트 구축 및 인증 구현이 용이	이미지 인증 시스템 자체의 구축에는 별다른 어려움이 없음
사용자의 분실에 대한 대책	패스워드 복구 시스템에 의하여 처리	포트폴리오 이미지를 잊은 경우 재구성 단계가 필요함
부가적인 사항	·	추상이미지의 선별 및 이미지 크기 결정방법, 질문세트 구성 및 사용자 인터페이스 처리에 추가적인 노력이 필요함

V. 결 론

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 인증작업은 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 인증받아야 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 인증 등급의 설정 등은 남은 과제로 계속 연구되어야 한다.

참 고 문 헌

[1] 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.

[2] Andrej Bauer. Gallery of Random Art. WWW at http://andrej.com/art/ 1998.

[3] 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 ACM*, Vol. 42 No.12 pp.40-46, December 1999.

[4] W. Belgers. Unix password security, 1993.

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

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

[7] D. C. Feldmeier and P. R. Karn. UNIX password security - ten years later, 1989. Lecture Notes in Computer Science Vol. 435.

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

[9] A. Paivio and K. Csapo. Concrete image and verbal memory codes. *Journal of Experimental Psychology*, Vol.80 No.2 pp.279-285, 1969.

[10] Rachna Dahmija, and Adrian Perrig Déjà Vu: A User Study Using Images for Authentication, Oct 2000.

[11] Ross J. Anderson. Why Cryptosystems Fail. *Communications of the ACM*, Vol.37 No11 p.32 p.40, November 1994.

[12] Roger Clarke, 'Human Identification in Information System : Management Challenges and Public Policy Issues', 6 INFO. TECH. & PEOPLE, p.37, p.40 1994

[13] Udi Manber. A simple scheme to make passwords based on one-way functions much harder to crack. *Computers and Security*, pp.171-176, 1996.

[14] **공병운**, "**결함허용기법을 이용한 신분확인 방안**", **부경대학교 석사 학위 논문**, 2001.08

[15] **이임영**, '**전자상거래 보안입문**', **생능출판사**, p.264, 2001.

감사의 글

뒤돌아 보면 아쉬움도 많지만 하나의 작은 맺음이 있도록 애써주신 분들이 생각납니다. 우선 본 논문이 완성되도록 열성을 다하여 헌신적으로 지도하여 주신 이경현 교수님과 교수님 부재중에 논문을 수정해 주시고 다듬어 주신 박지환 교수님께도 진심으로 감사를 드립니다. 아울러 본 연구를 수행하는 동안 아낌없는 조언과 도움을 주신 정보보호 및 인터넷 응용 연구실의 이준석님과 조현호님께도 깊은 감사를 드립니다.

또한 바쁘신 중에도 논문 심사를 맡아 주셔서 좋은 논문이 되도록 애써주신 박만곤 교수님, 박승섭 교수님께 무한한 감사를 드립니다. 그리고 학위 과정을 통하여 열성으로 가르쳐 주시고 용기와 격려를 보내주셨던 여정모 교수님, 박흥복 교수님, 정순호 교수님과 김해자 교수님께 깊은 사의를 표합니다.

처음부터 같이 공부하면서 좋은 일이 있을 때나 어려울 때나 옆에서 조언하며 격려해주신 이규남 선생님, 황성주 선생님을 비롯한 교육 대학원의 여러 선생님들을 잊지 못할 것입니다.

이 조그만 결실이 있기까지 연구실 멤버들의 따뜻한 마음과 고마운 격려는 영원히 잊지 못할 기억으로 남을 것 같습니다. 신원 박사님, 양종필, 박영호, 신정화, 박지철, 한명진, 김희연님 산업대학원의 공병운, 박정화, 김수형, 오명동, 임범춘, 박남현, 황명국님 그리고 교육대학원 허순녕, 이재희, 김태균, 김재권, 정상영 선생님께도 마음으로 고마움을 전합니다.

그 동안 어렵고 힘들 때 항상 옆에서 격려의 말을 아끼지 않던 사랑하는 아내, 멀리서나 가까이서나 항상 마음으로 사랑과 격려를 보내주셨던 부모님께 진심으로 고마움을 전하며, 학창시절 함께하는 시간이 적어 늘 아쉬웠으나 항상 웃음으로 화답하던 우리 서영이 윤호에게도 사랑을 전하며 저의 곁에서 늘 아낌없는 성원과 격려의 말씀을 보내주신 모든 이에게 진심으로 감사드립니다.

2002년 8월　　김기인 드림