논문 2008-45CI-5-4

이러닝 시스템에서 사용자 인증을 위한 키스트로크의 응용 기술

(Keystroke Application Technique for User Authentication in E-Learning System)

김 천 식*, 윤 의 중**, 홍 유 식***, 문 남 미****

(Cheonshik Kim, Eun-Jun Yoon, You-Sik Hong, and Nammee Moon)

요 약

이러닝 시스템의 가장 중요한 부분 중 하나가 인증이다. 왜냐하면 적법한 학습자가 학습 시스템에 접속해서 학습하고, 평가받는 것은 매우 중요하기 때문이다. 하지만, 대부분의 시스템이 학습자의 아이디와 패스워드를 사용한 인증을 사용하고 있다. 이 경우에 해커가 어렵지 않게 아이디와 패스워드를 해킹할 수 있다. 또한, 학습자가 자신의 정보를 다른 동료에게 주어 대신 평가를 받는 수 있다. 이와 같은 문제를 해결하기 위해서는 생체 인증 방법이 보완으로 필요하다. 이와 같은 방법은 상대적으로 많은 비용이 들고 또한 거부감이 있다. 따라서, 본 논문에서는 키스트로크 방법을 이용하여 학습자가 적법한 학습자인가를 판단하는 방법을 제안하였다. 또한, 키스트로크 시스템의 성능을 위해서 통계와 신경망을 적용하였다. 그 결과, 키스트로크의 인증에서 FRR과 FAR의 성능이 개선되었다.

Abstract

It is important for users to be confirming in e-Learning system, because legitimate learner should be joined to the system for learning and testing Thus, most system for authentication was verified using id and password with learner's id and password. In this case, It can be easy for hackers to steal learner's id and password. In addition, some learner gets another to sit for the examination for one with another person id and password. For the solution like this problem, it needs a biometrics authentication for complement. This method is required so much extra cost as well as are an unwanted concern. Therefore, we proposed keystroke technique to decide which learners are righteous or unlawful in this paper. In addition, we applied statistics and neural network for the performance of keystroke system. As a result, the performance of FAR and FRR in keystroke authentication was increased by proposed method.

Keywords: e-Learning, Keystroke Dynamics, Log, FRR

I. 서 론

이러닝 환경에서의 핵심적인 것은 인증이다. 대부분의 시스템이 인증을 통해서 학생이 이러닝 환경의 자신의 공간을 로그인 하도록 허락한다. 학생의 개인 공간은 평가, 숙제, 토론 등으로 구성된다. 패스워드를 이용하는 방법이 이러닝 인증에 가장 저렴한 방법이고, 또한 보편적으로 사용되는 방법이다. 패스워드를 이용한 인증의 문제점은 패스워드 소유자가 비밀을 유지하려 하지 않는 사람에게는 보증이 되지 않는다. 만일 A학생이 자신의 패스워드를 B학생에 알려주고, B는 A의 패스워드를 이용하여 A를 대신하여 시험에 응시한다면

* 정회원, 안양대학교 교양학부
(Dept. of Liberal Arts, Anyang Univ.)
** 정회원, 대구산업정보대학
(Dept. of Computer&Information, Daegu-Polytechnic College)
*** 정회원, 상지대학교 컴퓨터공학과
(Dept. of Computer Science, Sangji Univ.)
**** 정회원, 호서대학교 벤처전문대학원
(Dept. of IT App. Tech., Hoseo Graduate School of Venture)
※ 이 논문은 2007년 정부(교육인적자원부)의 재원으로 학술 진흥재단의 지원을 받아 수행된 연구임
(KRF-2007-D0036-I00563)
접수일자: 2008년8월20일, 수정완료일: 2008년9월5일

인증은 아무 소용이 없다. 이와 같은 문제를 해결하기 위해서 생체 인증시스템이 사용되고 있다.

생체기반의 기술은 크게 두 가지로 구분된다. 하나는 신체를 활용한 방법이고 다른 하나는 개인의 행동을 이용한 방법이다. 신체를 활용한 방법은 사용자의 신체적인 특징을 의미한다. 즉, 지문, 얼굴인식, 홍채 인식 등이다. 행동을 활용한 방법은 사람들이 말하는 목소리, 서명과 같은 행동적인 특징을 말한다. 이와 같은 방법은, 이러닝을 운용하는 기관에서 생체인증 시스템을 설치해야 하는 재정적인 요구 때문에 이 방법이 보편되기 어렵다.

동적 키스트로크(Keystroke dynamic)는 행동적 범주로 분류된다. 동적 키스트로크는 사용자가 타이핑하는 습관이나 독특한 특징을 로깅하여 분석한 다음 적법인 사용자인가를 분석하는 것을 말한다. 이 방법은 이러닝 기관에서 추가 비용이 요구되지 않는 장점이 있다. 이 방법의 유래는 2차 세계 대전으로부터 기원한다. 그 당시에, 전신(telegraph)이 보편적으로 이용되고 있었고 이 방법을 이용하여 전장에서 각 부대원간에 통신을 했다. 전신은 발신자가 누구인가를 분명히 알 수 없기 때문에 본 내용을 전달하기 전에 자신이 누구인가를 나타내는 간단한 식별코드를 만들어 상대편에게 알렸다. 이때, 버튼의 짧고 긴 누름에 의해서 식별 코드를 만들었다. 오늘날 키보드를 이용하는 많은 사람들은 키보드를 사용할 때 자신만의 독특한 특징이 있다. 각 개인마다 키보드를 길게 누르는 사람도 있고 짧게 누르는 사람도 있다. 어떤 사람은 매우 빠르고 또 다른 사람은 키보드가 느리다. 키보드를 찾는대 많은 시간이 소요되는 사람도 있고 그렇지 않은 사람도 있다. 또 어떤 사람은 습관적으로 한번 씩 오류를 만드는 사람이 있다. 이와 같은 특징들은 각 개인을 식별하는 중요한 요소가 된다. 이러한 특징을 이용하여 본 논문에서는 이러닝 환경에서 허락 받지 않은 불법 사용자의 침입을 탐지하여 이러닝 인증에 도움을 주고자 한다.

Ⅱ. 관련연구

대부분의 웹을 이용한 전자상거래 시스템은 로그인을 통해서 적법한 사용자임을 인증 받고, 웹에서 물건을 고르고, 결제하는 등의 행위를 한다. 하지만, 아이디와 패스워드는 유저의 고의나 실수로 얼마든지 분실될 수 있기 때문에 100% 완전한 인증을 했다고 보기 어렵다. 이러한 이유로 키스트로크(Keystroke) 정보를 실시간으로 기록하고 분석하는 실험이 있었다[1].

이 인증 방법도 다른 생체적인 인증방법과 유사하게 키스트로크 인증은 두 가지의 에러가 있다. 하나는 FAR(False Acceptance Rate)이고, 다른 하나는 FRR (False Rejection Rate)이다. FAR은 침입자가 접속될 가능성이고, FRR은 정상 유저가 접속이 거절될 가능성이다.

1980년대 초반에 동적 키스트로크분야의 연구가 있었다[2~6]. 대부분의 연구가 컴퓨터 접속에 대한 인증이었다. 동적 키스트로크인식 시스템은 키보드액션에서 휴지 시간(休止: dwell time)과 탈출 시간(flight time)을 측정한다. 시스템은 키스트로크와 관련한 시간정보를 수집한다. 사용자의 연속적인 키스크로크에서 존속 시간(duration time)과 잠재 시간(latency time)이 계산되고, digraph, tri-graphs 혹은 n-graphs가 생성된다. 식별과정의 시간제한 때문에, 사용자의 식별을 위해서 미리 사용자의 특성을 파악하기 위해서 충분한양의 데이터를 입력하도록 해야 한다. 이러한 과정을 마치고 사용자를 등록시킨다. 그런 다음 사용자는 같은 고정된 데이터를 입력하여 인증과정을 수행한다.

[7]의 실험에서 사용자이름, 패스워드, 이름을 입력하도록 하였다. 추출된 특징을 통계를 활용하여 분석하였다. 실험의 결과 0.17%의 FAR과 13.3%의 FRR의 결과를 얻었다. [8]에서는 신경망 탐지 모델을 이용하여 사용자 패턴을 훈련하고 침입자의 탐지에 사용하였다.

[9]의 연구에서는 신경망과 K-최근접 이웃 알고리즘을 이용하여 실험하였고, 실험의 참여인원은 10명이고 10개의 서로 다른 패스워드를 사용하였고, 100명의 불법사용자를 가정하여 실험하였다. 신경망을 이용한 실험의 결과 FRR이 1이고 FAR은 29가 나왔다. K-최근접 이웃 알고리즘을 이용한 실험에서 FRR 15.4와 FAR 1.03 도출했다. 실험의 결과 신경망을 이용한 경우가 FAR이 높았다. [5]에서 동적인 인증에 관한 실험을 했다. 실험에서 800개 문자 텍스트를 이용하여 여러 번 입력하도록 하였다. 실험에서 digraph, trigraph 그리고 four-graph를 비교 알고리즘으로 사용했다. [10]의 연구에서는 거리 계산방법으로 신경망을 사용했다. 실험에서 91명의 적법한 사용자와 61명의 침입자를 가정하여 실험했다. FAR은 6.56%이고, FRR은 2.22%를 얻었다.

Ⅲ. 키스트로크 (Keystroke)

동적 키스트로크는 어떤 사람이 자판을 입력할 때 생

성되는 리듬과 타이밍의 패턴이다. 이 기술은 사람들의 키스트로크 특징을 분석하여 저장한 후, 키스트로크 하는 사람의 특징을 이용하여 적법한 사용자와 불법 사용자를 판단하여 불법 사용자의 컴퓨터 접근을 차단할 목적으로 사용하는 보안 기법이다.

1. 키스트로크 인증

사용자의 키스트로크를 식별하기 위해서는 준비 작업이 필요하다. 시스템은 사용자가 키스트로크 내용을 기록하고, 키스트로크의 특징 벡터를 추출하여 특징 벡터의 거리(Distance)를 계산하고 기록해야 한다. 특징 벡터를 추출하는 2가지 방법이 있다. 하나는 정적 인증(Static Authentication)이고 다른 하나는 동적 인증(Dynamic Authentication)이다.

정적 인증은 아이디와 패스워드를 이용하여 특징을 추출한다. 동적인증은 사용자가 컴퓨터에 접속 후에 자유롭게 문서작업을 할 때 문서의 입력 특징을 추출하여 di- 와 tri-graph 방법을 이용하여 허가 받은 사용자인가를 판정 한다[5]. 본 논문에서는 정적 인증을 사용한다.

2. 키스트로크 특징 추출

사용자가 컴퓨터를 이용하는 과정 중에서 대부분의 작업이 자판에 키를 입력하는 것이다. 이때 , 우리가 키를 입력하면 key-down 이벤트가 발생하고, 키보드에서 손을 때면 key-up 이벤트가 발생한다. 키보드를 이용하는데 있어서 빠른 속도로 입력하는 사람도 있고 그렇지 않은 사람도 있다. 이러한 차이는 키보드에 숙련된 사람과 그렇지 않은 사람에 대한 차이 일 수도 있고, 아니면 아주 생소한 키보드 자판을 이용할 경우라면 아무리 숙련된 사람도 키보드가 익숙해질 때 까지는 초보자의 키보드 입력과 비슷할 것이다. 키보드의 입력 속도는 키를 입력하는 속도와 특정한 키에서 다른 키를 찾아서 이동하는 속도로 구분할 수 있다. key- down과 key-up 시간의 차이, 하나의 키를 눌렀을 때 key-up 시간과 다음 키의 key-down 시간의 차이[5]을 이용해서 duration과 latency 시간을 알아낼 수 있고, 이를 이용해서 키보드 속도를 duration과 latency 시간을 측정할 수 있다[11].

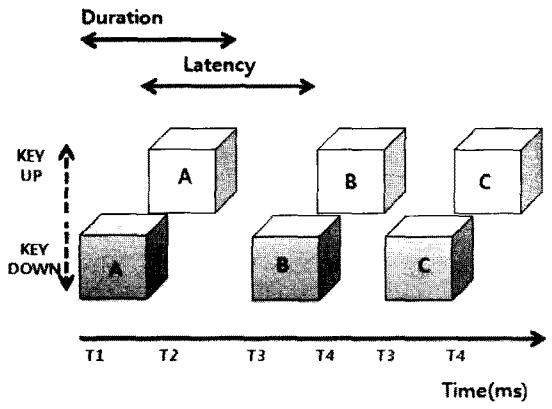

그림 1. 동적 키스트로크의 특징 추출
Fig. 1. Extract feature of dynamic keystrokes.

(그림 1)은 동적 키스트로크에서의 특징 추출과정을 나타낸 것이다. key-down과 key-up 이벤트를 이용하여 공식과 같이 Duration(1) 시간과 Latency(2) 시간을 구할 수 있다.

$$Duration = T(u)_i - T(d)_i \tag{1}$$

$$Latency = T(d)_{i+1} - T(u)_i \tag{2}$$

각 사용자를 구분하는 특징 벡터를 추출하기 위해서 공식(1), (2)을 공식(3),(4)에 적용하여 평균과 표준편차를 구한다.

$$mean(\mu) = \frac{1}{n} \cdot \sum_{i=1}^{n} x_i \tag{3}$$

$$SD(\delta) = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \mu)^2} \tag{4}$$

공식 (3),(4)에서 (x_i)는 각 문자별 duration, latency에 대한 저장된 특징 벡터이다.

3. 벡터계산 및 불법 사용자 판별

3.1 신경망 알고리즘

신경망은 예제를 통하여 학습한다. 흔히 신경망은 학습할 수 있는 여러 예제들로 이루어진 훈련 세트(training set)로 표현된다. 훈련 패턴으로 알려진 이러한 예제들은 벡터로 나타내지며 영상, 음성신호, 센서 데이터, 로봇팔의 움직임, 재정적인 데이터 등이 있다.

신경망은 병렬로 정보를 처리하는 자연적인 계산 모델이다. 기본적으로, ANN은 단순 처리 유닛(neurons)의 풀로서 정의될 수 있다. 여기서 유닛은 아날로그 신호를 전송함으로써 유닛들 간에 통신을 한다. 이들 신호는 뉴론들 간의 연결 강도를 통해 전송된다. 이들 뉴런의 각자는 수신된 입력을 누적하고 내부의 활동 함수

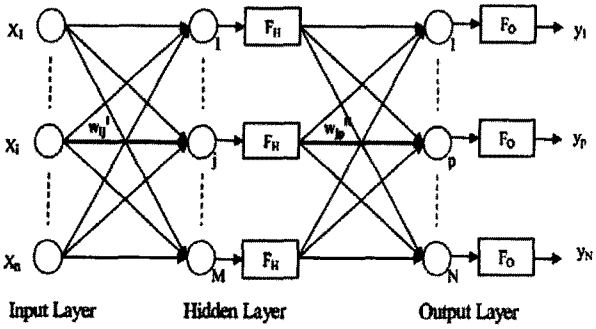

그림 2. 숨겨진 층을 갖는 전-연결 다층 퍼셉트론
Fig. 2. completes connected multi layer perceptron with hidden layers.

에 따라서 결과를 생성한다. 이 출력은 다른 뉴런을 위한 입력 값이 되거나 출력 값이 될 수 있다. (그림 2)에서 상세한 뉴런을 볼 수 있다[12].

(그림 2)는 하나의 숨겨진 층과 하나의 출력 층을 가지는 다층 퍼셉트론의 형태를 보인 것이다. 이 MLP에서 각 뉴런은 다음 층에 있는 각 뉴런에 연결되어진다. MLP의 출력은 다음의 수식으로 기술된다.

$$y_p = F_O\left(\sum_{j=0}^{N} w_{jp}^{H}\left(F_H\left(\sum_{i=0}^{N} w_{ij}^{I} x_i\right)\right)\right) \quad \text{for } p=1,2,\ldots N \tag{5}$$

에서 :

w_{jp}^{H} 는 숨겨진 층의 뉴런j로 부터 출력 뉴런 p^{th}로의 가중치를 나타낸다.

x_i는 i^{th}번째의 요소를 나타낸다.

F_H와 F_O는 숨겨진 층과 출력 층 각각에서 활동 함수를 나타낸다.

w_{ij}^{I}는 입력 층 뉴런 i에서 숨겨진 층의 뉴런 j로의 가중치이다.

학습과정은 다음에 정의한 비용 함수의 최소로 구성된다.

$$E=\frac{1}{2}\sum_{p=1}^{N}(y_p-d_p)=\frac{1}{2}\sum_{p=1}^{N}e_p^2 \tag{6}$$

여기서, y_p는 네트워크에 의해서 계산되는 p^{th}위치의 출력 값이다.

본 논문에서는 어떤 사용자가 적법한 사용자인가를 확인하기 위해서 (표 1)과 같은 키스트로크 특징을 다층 퍼셉트론의 입력에 사용한다.

본 논문에서는 실험을 위해서 사용자로부터 고정된 길이의 아이디와 패스워드를 입력받고 프로그램은 사용

표 1. 신경망을 위한 입력 변수
Table 1. Input variable for neural network.

No.	Variable in the keystroke	unit
1	max duration time	ms
2	min duration time	ms
3	mean duration time	ms
4	sd duration time	ms
5	max latency time	ms
6	min latency time	ms
7	mean latency time	ms
8	sd latency time	ms

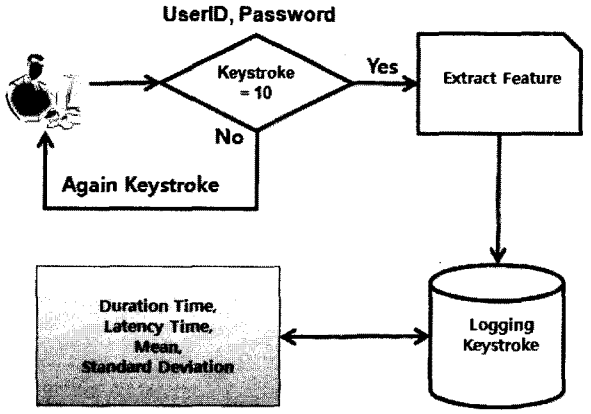

그림 3. 키스트로크 특징을 추출하기 위한 등록 과정
Fig. 3. Procedure for extracting feature of keystrokes.

의 키스트로크를 자동적으로 시간과 함께 기록하고 공식과 같이 계산한다. 또한, 이들 데이터를 데이터베이스에 자동적으로 저장하고 사용자가 로그인 할 때 거리를 계산한다.

(그림 3)은 각 사용자를 위한 키스트로크 정보의 로깅 과정과 특징을 추출하는 과정을 나타낸 그림이다. 이때, 각 사용자는 사용자 아이디와 패스워드를 10회 반복 입력한다. 입력된 로깅 정보를 공식에 적용하여 특징을 추출한다. 실험에서 백스페이스, Shift, Alt, 컨트롤키는 적용하지 않았다. 만일 사용자가 백스페이스를 키스트로크 했다면, 이 시스템은 계산을 하지 않는다.

Ⅳ. 시스템 구현

실험의 참여자는 로그인을 시도하기 전에, 여러 번 자신의 사용자 아이디와 패스워드를 입력함으로서 자신의 키스트로크 특징을 시스템에 등록한다. 이러한 과정을 통해서 피 실험자의 프로파일이 생성된다. [7]의 실험에서 6번의 키스트로크가 프로파일의 생성에 충분하

다고 주장하고 있다. 위의 주장이 타당하기 위해서는 참여자가 이미 충분히 사용하고 있는 패스워드라서 익숙하고 또한, 습관화 되어 있을 때 가능 좋은 결과를 얻을 수 있을 것이다. 본 실험에 참여한 대부분의 사람들은 타이핑능력이 우수한 사용자들이다. 단지 몇 명의 초보자가 있다. 실험에 참여할 사람들은 대부분이 학생으로 구성되어 있다. 실험에 참여한 인원은 20명이고, 대부분 20살에서 30살사이의 나이에 속한다. 고정된 패스워드를 사용하였고, 10명의 불법사용자를 가정하여 실험하였다.

(그림 4)에서 신경망 학습의 초기 값을 설정하는 것은 중요한 문제다. 초기 값을 적절하게 선택함으로써 학습오차가 작고 학습과정이 빠르게 수렴될 수 있기 때문이다. 일반적으로 신경망의 학습은 특정 초기 값에서 시작한다. 그리고 학습률은 모수 값들을 어떻게 선택하느냐에 따라서 학습오차가 작으면서 학습과정이 빠르게 수렴 할 수도 있고 조기 포화점에 빠질 수도 있다. 그렇기 때문에 분석하고자 하는 자료에 적당한 모수를 선정하여 오차가 최소값이면서 학습과정이 빠르게 수렴될

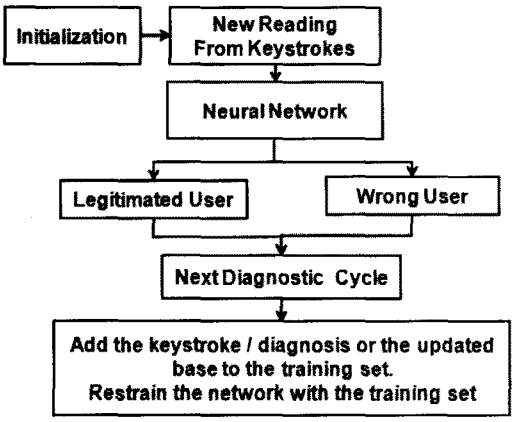

그림 4. 키스트로크를 위한 신경망 구성
Fig. 4. Organization of neural network for keystrokes.

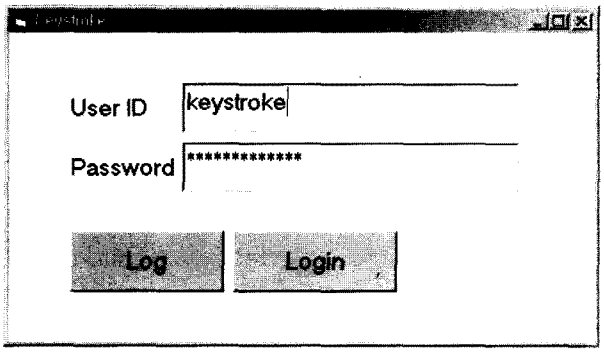

그림 5. 키스트로크 등록 화면
Fig. 5. The registration screen via keystrokes.

수 있게 학습하도록 하는 것은 매우 중요한 문제다. 그래서 제한적이지만 κ, θ, ϕ, μ (kappa, theta, phi, mu)만을 가지고 각 범위 0.1, 0.3, 0.5, 0.7, 0.9에 따라 실험을 해보았다.

패스워드의 등록 과정에서 자연스러운 키스트로크 방법과 인공적인 키스트로크 방법이 있다. 때로는 인공적인 리듬을 추가함으로써 효과적인 인증 및 인증의 성능을 향상시킬 수 있다. 그러나 인공적인 인증을 할 때 자신이 기억할 수 있는 인공적인 리듬을 기억해야만 한다. 인공적인 리듬을 사용할 때, 특정할 문자를 입력할 때 3초간 누르는 것도 리듬이 가미된 키스트로크 방법이라 할 수 있다. 본 실험에서는 인공적인 리듬을 사용하지 않았다.

(표 2)는 키스트로크의 성능을 분석하기 위해서 다른 논문제서 제안한 방법과 본 논문에서 제안한 방법의 정확도를 비교한 표이다. 본 논문에서 제안한 통계 및 신경망을 활용한 결과가 다른 방법보다 약간 개선되었음을 알 수 있다.

(그림 6)은 실험한 결과를 도표로 나타낸 것으로서, FRR과 FAR의 관계를 나타낸 것이다. 임계값이 증가함에 따라서, FRR은 높아지고 FAR은 낮아진다. 반면엣

표 2. 학습방법의 정확도 비교
Table 2. Compare correction among learning method.

학습 방법	훈련	정확도
C4.5 Decision	95.6%	93.3%
Naive Bayesian	93.3%	90.8%
Decision table	95.6%	85.6%
Neural Network & statistics	100%	95%

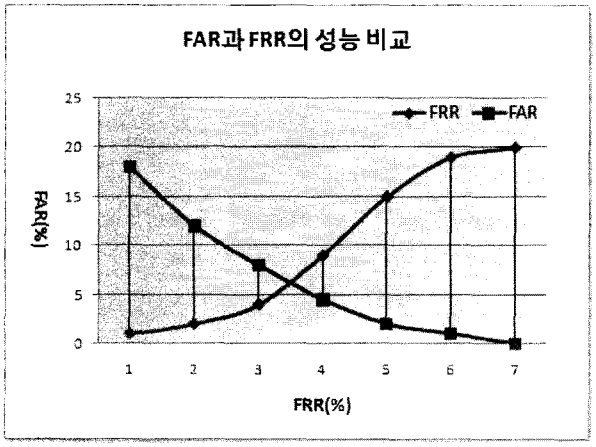

그림 6. 성능 분석 (FAR과 FRR의 비교)
Fig. 6. Analysis of performance (Compare FAR and ERR).

임계값을 낮추면 FRR은 낮아지고 FAR은 높아진다. FRR이 3%와 4% 사이가 FAR과 FRR이 같은 지점으로서 CER(Cross Error Rate)이라 부른다.

V. 결 론

개인이 기업전산망 혹은 인터넷 서비스망에 접속을 할 경우 현재는 아이디와 패스워드를 입력하여 접속자를 인증하는 방식을 사용하고 있다. 이러한 패스워드 중심의 개인인증 방식은 패스워드가 노출 될 경우 아무런 대비책이 없이 기업이나 개인에게 큰 피해를 입히게 된다. 패스워드의 경우 대부분 본인이 기억하기 쉬운 주변의 정보를 가지고 조합하여 패스워드를 만들기 때문에 패스워드는 해킹, 주변인 노출 외에 추정에 의해서도 많이 노출이 된다. 특히 이러닝 시스템에서 학생의 평가가 인터넷으로 이루어지는 점 때문에 평가의 신뢰성을 확보하기 위해서 평가의 대상인 학생이 평가를 받고 있는지에 대한 사항은 매우 중요하다. 때때로, 학생들은 자신의 아이디와 패스워드를 다른 사람에게 알려주어 대리 시험을 치루는 경우가 발생할 수 있다. 이와 같은 문제점을 개선하기 본 논문에서는 키스트로크를 이용하여 적법한 학생이 평가를 받도록 하고 그렇지 않은 대상자를 퇴실시키는 방안으로 키스트로크를 이용한 기법을 제안하였다.

본 논문에서 제안한 방법은 아이디와 패스워드를 이용한 키스트로크 방법으로서 로그인시에 사용자의 식별을 목적으로 한다. 물론, 사용자의 로그인 후에도 지속적으로 키스트로크로 감시할 수 있으나, 사용자를 다소 귀찮게 하는 측면이 있을 것으로 생각하고, 때때로 적법한 사용자에 대해서 불법사용자로 오인한 시스템의 처방이 시스템을 사용하는 사용자의 불쾌감을 유발할 수 있다. 그러므로 본 논문에서 아이디와 패스워드를 대신한 인증이라기보다는 아이디와 패스워드를 보완하는 측면에서의 활용은 매우 가치 있는 인증 법으로 판단한다. 차후에 로그인 후에도 지속적인 인증을 할 수 있는 방안에 대해서 연구하고자 한다.

참 고 문 헌

[1] Monrose, F.; Rubin, A.d., Keystroke dynamics as a biometric for authentication. *Future Generation Computer System*. Ed. Elsevior, Vol. 16, pp. 351-359, 2000.

[2] Bergadano, F., Guneti, D., Picardi, G., User Authentication through Keystroke Dynamics. *ACM Transactions on Information and System Security*, Vol. 5, No. 4, pp. 367-39, 2002.

[3] Beleha, S., Slivinsky, C., Hussein, B., Computer-access Security Systems using Keystroke Dynamics. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. PAMI-12, 12, pp.1217-1222, 1990.

[4] Brown., M., Rogers, S.J., Identification Via Keystroke characteristics of Typed Names Using Neural Networks. *International Journal on Man-Machine Studies*, Vol. 39, pp. 999-1014, 1993.

[5] Guneti D., & Picardi, C. , Keystroke Analysis of Free Text. *ACM Transactions on Information and System Security*, Vol. 8, No. 3, pp. 312-347, 2005.

[6] Leggest, J, Williams, G., Dynamic Identity Verification Via Keystroke Characteristics. *International Journal on Man-Machine Studies*. Vol. 35, 859-870, 1991.

[7] R. Joyce, G. Gupta., Identity Authentication Based on Keystroke Latencies. *Communications of the ACM*. Vol 33. Issue: 2. pp 168-175, 1990.

[8] Cho S, Han C, Han D, Kim H. Web-based keystroke dynamics identity verification using neural network. *J Organ Comput Electron Commerce*, 10(4):295-307, 2000.

[9] Wong, F., Supian, A., & Ismail, A. Enhanced user authentication through typing biometrics with artificial neural networks and k-nearest neighbor algorithm. *IEEE Conference on Signals, Systems and Computers*, 2, 911 - 915, 2001.

[10] Lin, D.-T. Computer-access authentication with neural network based keystroke identity verification. *International Conference on Neural Networks*, 1, 174 - 178, 1997.

[11] Cardot, H., Hocquet, S., & Ramel, J.-Y. Fusion of methods for keystroke dynamic authentication. *Fourth IEEE Workshop on Automatic Identification Advanced Technologies*, Oct. 2005 Page(s): 224 - 229, 2005.

[12] Zakaria Nouir, Berna Sayrac and Benoˆıt Fouresti´e, Walid Tabbara and Franc¸oise Brouaye, Comparison of Neural Network Learning Algorithms for Prediction Enhancement of a Planning Tool, *13th European Wireless Conference*, 2007.

저 자 소 개

김 천 식(정회원)
1997년 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학석사)
2003년 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학박사)
2000년~2003년 경동대학교 정보통신공학부 교수
2004년~현재 안양대학교 교수
2007년~현재 대한전자공학회 컴퓨터소사이어티 분과위원장
2008년~현재 인터넷 방송통신 TV학회 상임이사
2006년~현재 인터넷 정보학회 학회편집위원
2006년~현재 대한교통학회 정회원
2005년~현재 한국데이터베이스학회 정회원
<주관심분야: 데이터베이스, 데이터마이닝, 이미지처리, e-Learning, Agent system>

홍 유 식(정회원)
1984년 경희대학교 전자공학과 (학사)
1989년 뉴욕공과대학교 전산학과 (석사)
1997년 경희대학교 전자공학과 (박사)
1985년~1987년 대한항공(N.Y.지점 근무)
1989년~1990년 삼성전자 종합기술원 연구원
1991년~현재 상지대학교 컴퓨터공학부 교수
2000년~현재 한국 퍼지 및 지능시스템학회 이사
2004년~현재 대한 전자 공학회 ITS 분과위원장
2001년~2003년 한국 정보과학회 편집위원
2001년~2003년 한국 컴퓨터 교육산업학회 이사, 편집위원
2004년~현재 건설교통부 ITS 전문심사위원
2004년~현재 원주 시 인공지능신호등 심사위원
2005년~현재 정보처리학회 이사
2005년~현재 인터넷 정보학회 이사
2005년~현재 정보처리학회 강원지부 부회장
2008년~현재 인터넷 방송통신 TV학회 부회장
<주관심분야: 퍼지 시스템, 전문가시스템, 신경망, 교통제어>

윤 은 준(정회원)
2003년 경일대학교 컴퓨터공학과 (공학석사)
2007년 경북대학교 컴퓨터공학과 (공학박사)
2007년~현재 대구산업정보대학 컴퓨터정보계열 전임강사
2007년~현재 보안공학연구지원센터 보안공학논문지 편집위원
<주관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜>

문 남 미(정회원)
1985년 이화여자대학교대학교 전자계산학과(이학사)
1987년 이화여자대학교대학원 전자계산학과(이학석사)
1998년 이화여자대학교대학원 컴퓨터학과(이학박사)
1998년 아주대학교 미디어학과 조교수대우
1999년~2002년 이화여자대학교 정보통신연구소 연구교수, 인터넷멀티미어연구센터장, 정보통신교육원 부원장
2003년~2007년 서울벤처정보대학원대학교 디지털미디어학과 교수
2008년~현재 호서대학교 벤처전문대학원 IT응용기술학과 교수
<주관심분야 : 디지털양방향 방송, HCI, 이러닝, 양방향서비스 등>