Journal of the Korea Academia-Industrial cooperation Society
Vol. 14, No. 3 pp. 1409-1415, 2013

http://dx.doi.org/10.5762/KAIS.2013.14.3.1409

변동형 비밀번호 생성방법 및 이를 이용한 인터넷 인증 시스템에 관한 연구

강정하[1], 김재영[2*], 김은기[1]
[1]한밭대학교 정보통신학과, [2]한국전자통신원구원 융합기술연구부문

A Study on the Variable Password Generation Method in Internet Authentication System

Jung-Ha Kang[1], Jae Young Kim[2*] and Eun-Gi Kim[1]
[1]**Dept. of Information and Communication Engineering, Hanbat National University**
[2]**IT Convergence Technology Research Lab., Electronics and Telecommunications Research Institute**

요 약 인터넷 통신의 발전과 함께 다양한 온라인 서비스의 이용이 크게 확대되었고, 이에 따라 사용자를 확인하기 위한 인증 기술의 중요성이 증가되고 있다. 사용자 인증기술로 가장 일반적으로 사용되고 있는 방식은 사전에 약속된 비밀번호를 활용하는 기법이다. 그러나 기존의 비밀번호 인증 방식은 인증 마다 매번 동일한 비밀번호가 사용되기 때문에 공격자에 의하여 비밀번호가 노출되면 악의적으로 이용될 수 있다. 본 논문에서는 사용자가 접속한 날짜, 시간 및 IP 주소와 같은 정보를 이용하여 접속 시 마다 새로운 비밀번호를 생성하는 변동형 비밀번호 생성 방법 및 이를 이용한 인터넷 인증 시스템을 제안하였다. 본 논문에서 제안된 방식은 비밀번호 노출에 따른 개인정보의 유출을 미연에 방지하여 인터넷 인증분야 및 보안시스템 분야에서 신뢰성 및 경쟁력을 향상시킬 수 있고, 전자문서의 확인이나 다양한 분야의 보안 시스템에도 적용할 수 있어, 사용상의 범용성을 향상 시킬 수 있다.

Abstract With the development of Internet communication and the use of a variety of online services has been greatly expanded. Therefore, the importance of authentication techniques for users of online services has increased. The most commonly used methods for user authentication is a technique that utilizes a prearranged password. However, the existing password scheme for authentication must use the same password every time. Therefore, the password being leaked by attackers, it can be used maliciously. In this paper, we proposed the Variable Password Generation Method in Internet Authentication System that generates a new password using information such as the access date, time, and IP address when user logs in. The method proposed in this paper prevents disclosure of personal information due to password exposure and improves the reliability and competitiveness in the field of security systems

Key Words : Authentication, Password, Security, Password Generation, Password Policy

1. 서론

인터넷 통신의 발전과 함께 사용자들의 휴대용 단말기 또는 개인용 컴퓨터를 통한 다양한 온라인 서비스의 이용이 가속화되고 있다. 따라서 다수의 이용자가 온라인 서비스를 이용하는 환경에서 불법적 사용을 통제하기 위하여 사용자를 확인하는 사용자 인증 기술이 발달하고, 이에 대한 중요성도 증가되고 있다. 일반적으로 사용자 인증 기술은 인증이 기반이 되는 요소에 따라서 지식을 통한 인증, 소유한 물건을 이용한 인증, 신체적 특징을 이

본 연구는 건설기술혁신사업의 연구비지원(12기술혁신C01)에 의해 수행되었음.
*Corresponding Author : Jae Young Kim(ETRI)
Tel: +82-10-3411-0513 email: jyk@etri.re.kr
Received February 18, 2013 Revised(1st February 28, 2013 2nd March 6, 2013) Accepted March 7, 2013

용한 인증 등으로 구분된다.

온라인 서비스에서 사용되는 가장 일반적인 사용자 인증 기술은 비밀번호 인증 방식이다. 인터넷 사이트를 통하여 온라인 서비스를 이용할 때, 사용자는 자신이 설정하여 서버에 저장된 ID(Identifier)와 비밀번호(Password)을 이용하여 해당 인터넷 사이트에 로그인을 수행한다[1]. 인터넷 사이트의 인증시스템은 입력된 ID와 비밀번호를 이용하여, 접속하고자하는 사용자의 정당성을 확인하게 된다. 이러한 비밀번호를 이용한 인증 방식은 온라인 서비스를 제공하는 서버에 접근하기 위한 필수요소이고, 인증 방식과 비밀번호형식이 단순하여 여러 목적으로 매우 넓게 활용 되고 있다. 그러나 이러한 단순한 인증 방식은 사용자의 관리 소홀이나, 네트워크상의 공격 기법에 의하여 타인에게 노출되기 쉽다는 문제점이 있다. 특히, 인터넷 상에서 이루어지는 패스워드 인증 과정에서 트로이 목마와 같은 악성코드에 의하여 비교적 쉽게 패스워드가 유출될 수 있을 뿐만 아니라, 패스워드의 유출 사실을 사용자기 인지할 수 없다는 문제점이 있다. 또한 많은 사용자들은 기억의 편의성을 위하여 동일한 ID와 비밀번호를 이용하여 다수의 사이트에 등록하고 있고, 이로 인하여 사용자가 등록한 다수의 사이트 중에서 한곳이라도 해킹이 되거나 개인 정보가 누출되면, 사용자가 등록한 다수의 사이트가 모두 해킹 될 수 있다는 문제점이 있다.

따라서 본 연구는 시간 및 IP 주소와 같은 정보를 이용하여 접속 시 마다 새로운 비밀번호를 생성함으로써, 비밀번호의 노출에 따른 개인정보의 유출을 방지할 수 있는 변동형 비밀번호 생성방법 및 이를 이용한 인터넷 인증 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 사용자 인증 방식에 대하여 기술하고, 3장에서는 변동형 비밀번호 생성 방법에 대하여 기술한다. 4장에서는 변동형 비밀번호 생성 방식을 이용한 인터넷 인증 시스템에 관하여 기술하고, 5장에서는 결론을 맺는다.

2. 사용자 인증 방식

가트너의 인증 분류(a Taxonomy of Authentication)에서 전자인증은 실시간 처리 시스템에서 전자적인 정보를 이용해 올바른 사용자를 확인하고, 사용자에 해당하는 올바른 신뢰 수준을 확인하는 과정이라고 정의하고 있다[2]. 온라인과 같은 비대면 환경에서 사용자를 식별하기 위하여 사용자의 여러 정보를 고유한 인증정보로 매칭시키고, 사용자의 인증 수단을 생성한다. 사용자가 인증을 요청하면서 자신을 증명하는 정보를 제출하고, 인증시스템은 이 정보를 통하여 올바른 사용자임을 확인한다[3,4].

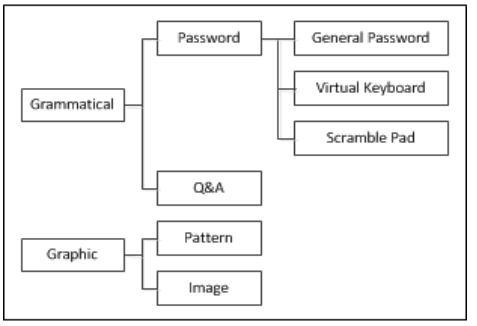
이러한 전자인증방법은 대표적으로 사용자가 가진 지식에 기반을 하는 지식기반, 사용자가 소유한 형체화된 인증 수단을 이용하는 토큰기반, 사용자의 생체적인 정보를 인증수단으로 사용하는 생체기반의 세 분류로 나누어진다.

2.1 지식기반 인증 방식

지식기반 인증방법들은 사용자가 가진 지식이나 사용자가 알고 있는 정보를 확인해 사용자를 인증하는 방식으로 휴대해야하는 장치가 없고, 편의성이 높아 사용자가 이용하기 간단하다는 정점을 가진다. 또한 인증 시스템을 간단하게 구축 할 수 있어 보편적으로 가장 많이 사용되는 인증 방식이다.

그러나 편의성의 높은 반면, 보안이 취약하여 쉽게 유출될 수 있기 때문에, 금융서비스와 같이 중요한 서비스에서는 타인증 방법들과 함께 복합적으로 사용되는 경우가 많다[5].

Fig. 1은 국내외에서 사용되고 있는 지식기반 인증 수단들의 종류이다.



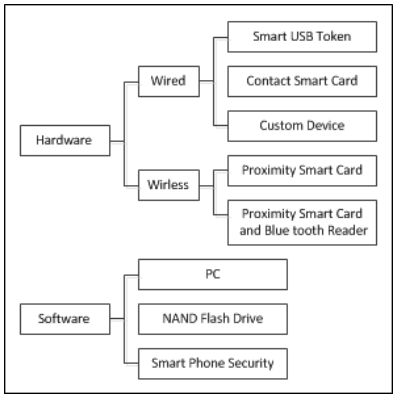
[Fig. 1] Knowledge-based Authentication Method

2.2 토큰기반 인증 방식

토큰기반 인증방법들은 사용자가 소지하고 있는 인증토큰을 이용해 사용자를 인증하는 방식이다. 즉, 사용자가 가진 인증토큰이 정당한 인증 토큰인지 확인하거나, 사용자가 가진 인증토큰이 생성성하는 정보를 확인해 올바른 사용자의 여부를 확인하는 방식이다. 이러한 토큰기반 인증수단들은 소프트웨어 토큰과 하드웨어 토큰으로 나눌 수 있다. 소프트웨어 토큰은 소프트웨어 형태로 구성된 토큰을 의미하며, 대표적인 인증수단으로 공인인증서를 들 수 있다. 하드웨어 토큰에 비하여 편의성은 높지

만, 인증수단의 유출 가능성이 높아 보안성은 낮은 편에 속한다. 하드웨어 토큰은 인증정보를 생성하는 기기(Device) 형태로 제공되는 방식으로 대표적인 예로 OTP 생성기를 들 수 있다[6]. 소프트웨어 토큰에 비해 유출 가능성은 적지만, 늘 휴대해야하기 때문에 편의성은 낮은 편에 속한다. 토큰기반 인증 수단들은 지식 기반 인증 수단에 비해 높은 보안성을 가지지만, 인증시스템 구축이 어렵고 인증수단의 발급을 위하여 적어도 한번의 오프라인 인증 환경을 거쳐야 하며, 소유한 인증 수단을 안전하게 보관해야 하므로 지식기반 인증 수단에 비해 편의성은 낮은 편에 속한다.

Fig. 2는 대표적인 토근기반 인증방법을 보여준다.



[Fig. 2] Token-based Authentication Method

2.3 생체기반 인증 방식

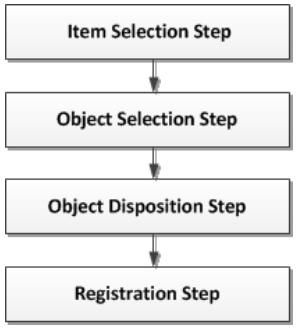
생체기반 인증방법은 사용자가 가지는 고유한 지문이나 홍채, 얼굴구조등과 같은 생체적 특징 등을 이용해 인증하는 방식으로 높은 보안성을 지닌다. 하지만 시스템 구축 및 관리 등에 많은 투자가 필요하고, 사용자가 가진 변하지 않은 특징이므로, 유출시 많은 문제가 발생 가능하기 때문에, 높은 보안성이 요구되는 대규모 금융거래나 출입통제등과 같은 제안한 시스템에 많이 적용되어 사용되고 있다.

3. 변동형 비밀번호 생성

지식기반 인증 방법들 중 ID와 비밀번호 인증 방식은 사용자 측면에서는 편의성이 높고, 인증시스템 측면에서는 구축이 단순하여 일반적으로 많이 사용되고 있다. 그러나 ID와 비밀번호가 유출되기 쉬운 문제점이 있고, 이 문제점을 해결하기 위하여 주기적인 패스워드 변경과 같은 요구사항들이 증가하고 있다. 그러나 이러한 요구사항의 증가로 사용자의 편의성이 감소되지만, 그에 따른 보안성의 증가는 미비한 수준이다. 본 논문에서는 사용자에게 편의성을 제공하면서 보안성이 강화되는 변동형 비밀번호 생성과 이를 이용한 인터넷인증 시스템을 제안한다.

3.1 변동형 비밀번호 생성 과정

변동형 비밀번호를 생성하기 위한 인증항목으로 날짜, 시간, IP주소, 문자, 숫자, 연산자와 같은 항목을 정의한다. 정의된 항목을 이용하여 변동형 비밀번호를 생성하는 과정은 Fig. 3과 같다.



[Fig. 3] The procedure of Variable Password Generation Method

항목 선택 단계에서는 정의된 인증 항목들 중 사용자의 인증 확인을 위한 항목을 하나 이상 선택한다. 사용자가 선택한 인증항목들은 변동 항목과 고정항목, 조합항목 중 하나의 항목으로 구분 된다.

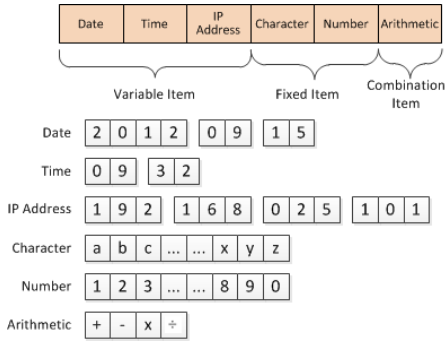
객체선택 단계에서는 선택된 각 개별항목에 포함된 복수개의 객체들에서 특정 객체를 선택하도록 한다.

객체 배치 단계에서는 사용자에 의하여 선택되거나 이미 설정된 객체 배치 방법에 따라 선택된 객체들의 위치를 재배치하게 된다. 이러한 과정이 완료되면 사용자는 선택한 비밀번호 생성 방법을 해당 온라인 사이트에 등록하게 된다.

3.2 항목 선택 단계

사용자는 등록하고자하는 사이트로부터 인증항목들을 제공받고, 이들 중 변동타입 또는 고정타입을 포함하여 개별항목들을 선택한다. 예를 들면, 사용자가 PC나 스마트폰 등의 단말기를 이용하여 특정 사이트에 접속하여 비밀번호 생성방법 등록을 신청하면, 해당 사이트는 인증항목들이 표시되는 화면을 사용자 단말기에게 제공하여 사용자가 개별적 인증항목을 선택할 수 있도록 한다.

Fig. 4는 본 논문에서 제안한 변동형 비밀번호 생성방법에서 사용될 수 있는 인증 항목들이다. 인증항목들은 변동항목, 고정 항목, 조합항목으로 구분될 수 있다. 변동항목에는 날짜 항목, 시간항목 및 IP주소와 같은 시간이나 장소에 따라 변동되는 정보를 개별항목으로 포함 할 수 있다. 고정항목은 문자나 숫자와 같이 일정하게 정해진 정보를 개별항목으로 포함 할 수 있다.



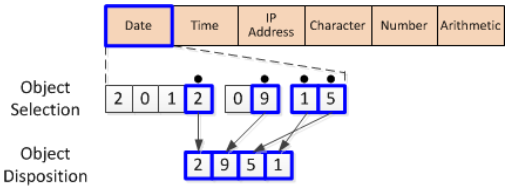
[Fig. 4] The Authentication Items

조합 항목은 사칙연산과 같은 연산항목이 포함 될 수 있고, 사칙연산 이외에도 변동항목과 고정항목의 객체를 조합 할 수 있는 다양한 방법들을 추가로 포함 할 수 있다.

Fig. 4에서 나타낸 것과 같이, 날짜 항목은 연월일의 8개의 객체로 구성될 수 있고, 시간항목은 시간 및 분의 4개 객체로 구성될 수 있다. IP 주소항목은 12개의 객체로 구성되고, 문자항목은 영문자, 숫자항목은 한 자리 숫자의 객체로 구성될 수 있다.

3.3 객체선택 및 객체배치 단계

항목선택단계에서 인증항목이 선택되면, 각 개별항목이 포함하는 복수의 객체들 중에서 사용자가 인증에 사용할 객체들을 선택한다. Fig. 5는 사용자가 항목선택단계에서 날짜항목을 선택한 경우의 객체선택단계와 객체배치단계를 설명한다.

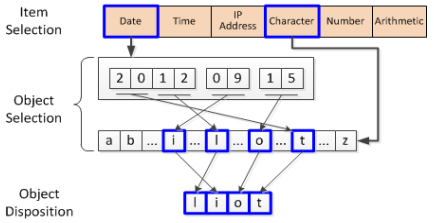


[Fig. 5] The Object Selection and Disposition using Date Objects

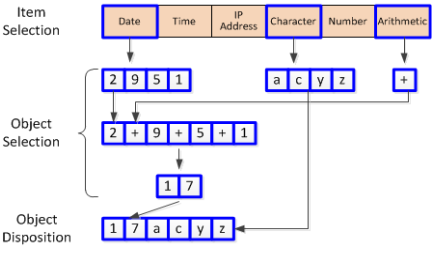
Fig. 5에서 사용자가 날짜항목을 선택하면, 오늘의 연월일의 화면에 표시되고, 사용자는 연월일이 포함하는 8개의 객체들 중에서 원하는 객체로 연도의 마지막자리 숫자, 월의 마지막자리 숫자, 일의 2개의 숫자를 선택한다. 선택된 객체들은 객체배치과정에서 순서를 변경하여 재배치 할 수 있다. 객체의 선택 및 재배치는 사용자의 편의를 위하여 마우스 등을 이용하여 해당객체를 드래그 방식으로 수행할 수 있다. 따라서 사용자는 날짜의 연월일 중 자신의 선택한 위치와 재배치 방법만 기억하고 있으면, 이후 인증을 요청하는 날짜에 따라 쉽게 변동된 비밀번호를 입력하고 인증시스템으로부터 인증을 받을 수 있다.

사용자는 항목선택, 객체선택, 객체 배치의 설정과정을 통하여 비밀번호 생성방법을 해당 사이트에 등록하게 된다. 등록 된 이후, 사용자가 해당 사이트에 접속하여 인증을 요청하는 경우, 사용자는 자신이 설정하여 암기하고 있는 비밀번호 생성방법에 따라 해당 사이트에 비밀번호를 입력한다. 해당 사이트는 인증을 요청하는 사용자의 비밀번호 생성방법에 따라 비밀번호를 생성하고, 사용자가 입력한 비밀번호와 일치하는지 확인하여 인증여부를 결정한다.

Fig. 6에서는 날짜항목, 문자항목, 연산항목 등을 조합한 비교적 복잡한 비밀번호 생성방법을 설명한다.



(a) The Password Generation Method(1)



(b) The Password Generation Method(2)

[Fig. 6] The Complex Password Generation Method

본 논문에서 제안된 비밀번호 생성방식은 Fig. 5와 Fig. 6에 설명된 예시이외에도 사용자에 따라 다양한 비밀번호 생성방식을 설정할 수 있다.

3.4 응용프로그램을 이용한 설정 및 등록

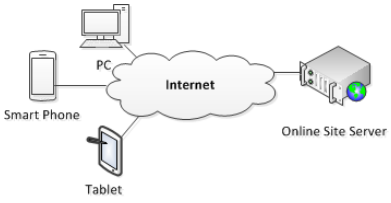
Fig. 5와 같이 비교적 단순한 비밀번호 생성방법은 사용자가 암기하기 용이하지만, Fig. 6과 같이 복잡한 비밀번호 생성방법은 암기가 어려울 뿐만 아니라 생성방법을 이용하여 비밀번호를 생성하기도 복잡하다. 따라서 본 논문에서 제안된 변동형 비밀번호 생성방법이 적용된 응용프로그램 실행하여 비밀번호 생성방법의 설정하고 등록할 수 있다. 이러한 응용프로그램은 사용자단말기, 해당 온라인 서비스 서버, 인증 서버 등에서 저장 및 실행 될 수 있다.

사용자는 자신이 휴대한 사용자단말기에서 비밀번호 생성을 위한 응용프로그램을 실행시키고, 비밀번호 생성 방법을 설정하여 자신의 사용자단말기에 등록할 수 있으며, 이후 사용자단말기에서 응용프로그램을 실행하여 등록된 방법에 따라 비밀번호를 생성할 수 있다. 또한, 사용자단말기에 등록된 비밀번호 생성방법은 해당 사이트의 서버 및 인증서버 등에도 동일하게 등록되어, 인증 요청 시 등록된 방법에 따라 응용프로그램을 실행하여 인증확인을 위한 비밀번호를 생성할 수 있다.

4. 변동형 비밀번호를 이용한 인증시스템

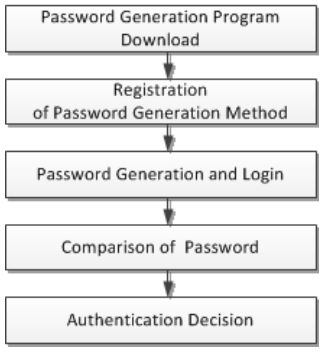
본 논문에서 제안된 변동형 비밀번호 생성방법은 다양하게 구성된 인터넷 기반의 인증 시스템에서 이용될 수 있고, 이러한 인터넷 기반의 인증 시스템은 다음과 같은 방식으로 운영될 수 있다.

Fig. 7과 Fig. 8은 별도의 인증업체를 이용하지 않고, 인터넷 사이트를 운영하는 업체나 기관에서 사용자에 대한 인증을 관리하는 운영 방식을 설명하고 있다.



[Fig. 7] The Case of None Authentication System

사용자가 사용자단말기를 이용하여 인터넷에 연결된 해당 사이트의 서버에 접속하면, 업체 서버는 최초접속자에게 본 논문에서 제안한 변동형 비밀번호 생성방법이 적용된 비밀번호 생성프로그램을 사용자 단말기로 전송한다.

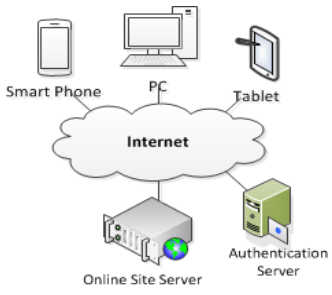


[Fig. 8] Authentication Flow in case of None Authentication System

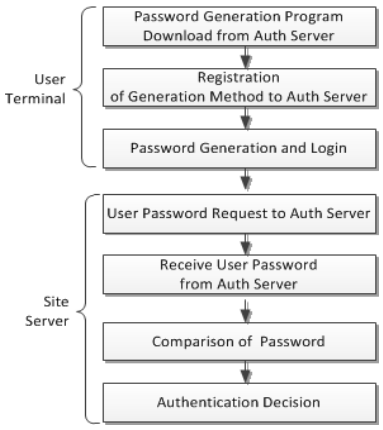
사용자는 다운받은 비밀번호 생성 프로그램을 이용하여 Fig. 3에 따라 사용자 단말기에 비밀번호 생성방법을 등록한다. 또한 등록된 비밀번호 생성 방법을 업체서버로 전송하여 해당 사이트에 등록할 수 있다. 이때, 업체서버는 비밀번호 생성방법과 함께 사용자 단말기의 고유번호(MAC 주소) 등을 매핑하여 등록하여 등록된 사용자단말기 이외의 단말기로는 해당 사용자와 매핑되는 비밀번호를 생성하거나 인증할 수 없도록 할 수 있다.

등록과정이 완료된 이후, 사용자가 해당 사이트에 로그인 할 경우, 사용자단말기에 다운로드된 비밀번호 생성 프로그램을 실행하여 인증용 비밀번호를 생성하고, 생성된 비밀번호를 이용하여 업체서버에 인증을 요청한다. 업체서버는 이미 등록된 사용자의 비밀번호 생성방법을 이용하여 확인용 비밀번호를 생성하고, 전송된 인증용 비밀번호와 비교하여 사용자의 인증여부를 결정한다.

Fig. 9과 같이 인증업체를 이용할 경우 인증서버의 역할에 따라 Fig. 10과 Fig. 11과 같이 인증 수행이 될 수 있다. Fig. 10에서 사용자 단말기는 인증서버로부터 비밀번호 생성 프로그램을 다운로드하여 생성방법을 인증 서버에 등록한다. 업체서버는 사용자의 로그인 시, 인증서버로부터 수신된 확인용 비밀번호를 이용하여 인증 여부를 결정한다.

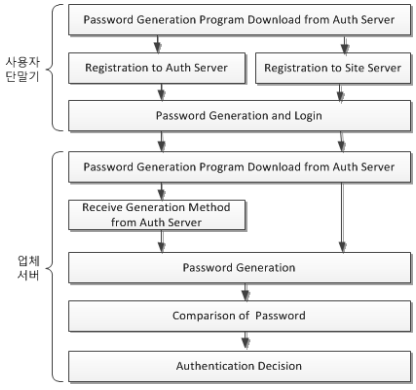


[Fig. 9] The case of using Authentication System



[Fig. 10] Password Generation in Authentication Server

Fig. 11에서 인증서버는 비밀번호 생성프로그램을 사용자단발기와 업체서버에 제공하고, 사용자 로그인시 확인용 비밀번호는 업체서버에서 생성하도록 하는 방식이다.



[Fig. 11] Password Generation in Site Server

5. 결론

IT 기술의 발달로 다양한 온라인 서비스들이 등장하게 되었고, 이에 따라서 온라인 서비스를 이용하는 사용자를 인증하기 위한 다양한 인증기술이 등장하게 되었다. 대표적으로 비밀번호 인증 방식은 단순하고 암기가 쉽기 때문에 많이 활용되고 있지만, 이러한 이유 때문에 타인에게 노출되기 쉽다는 문제점이 있다.

본 연구에서는 접속 시 마다 새로운 패스워드를 생성하여 패스워드의 노출에 따른 개인정보 유출을 방지할 수 있는 변동형 비밀번호 생성방법을 제안하였다. 본 연구에서 제안한 방식은 사용자 마다 비밀번호 생성방식을 서로 다르게 적용하여 비밀번호의 생성 방법 유추 및 이를 통한 비밀번호의 역추출을 미연에 방지할 수 있도록 하였다. 사용자가 강한 비밀번호를 부여하기 위하여, 복잡한 패스워드 생성방법을 설정해야할 경우, 이를 프로그램화하여 제공함으로서 사용상의 편의성을 향상시킬 수 있도록 하였다. 본 논문에서 제안된 변동형 비밀번호 생성방법은 인터넷 상에서 제공되는 다양한 시스템에게 쉽게 적용할 수 있으며, 전자문서의 확인이나 다양한 분야의 보안 시스템에도 적용할 수 있어 범용적으로 사용할 수 있는 장점이 있다. 따라서, 본 논문에서 제안된 방식은 인터넷 인증 분야 및 보안 시스템 분야는 물론, 사용자 인증을 요구하는 다양한 분야에 적용될 수 있을 것이라고 사료된다. 향후에는 본 논문에서 제안한 알고리즘을 구현하여 보안성과 편의성에 대한 실험 결과를 제시하고, 실험결과를 기존의 사용자 인증 방식과 비교하여 본 논문에서 제안된 알고리즘의 객관적인 성능을 제시하기 위한 연구를 진행할 예정이다.

References

[1] Karen Scarfone, Murugiah Souppaya,“Guide to Enterprise Password Management(Draft)”, p.11-13, NIST, 2009.
[2] Ant Allan, “A Taxonomy of Authentication Methods”, p.10-30, Gertneer, 2011.
[3] William E, Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W, "e-authentication guideline", p.19-38, NIST, 2011.
[4] ITU-T, “Entity authentication assurance”, p.9-15, ITU-T, 2011.
[5] FFIEC "Supplement to Authentication in an Internet Banking Environment", p.1-7, FFIEC, 2011.
[6] Neil M. Haller, "The S/Key One-Time Password System", p.1-5, RFC 1760, 1995.

강 정 하(Jung-Ha Kang) **[정회원]**

- 2001년 8월 : 한밭대학교 정보통신공학과 (정보통신공학석사)
- 2002년 1월 ~ 2012년 4월 : 휴메이트 책임연구원
- 2005년 8월 ~ 현재 : 한밭대학교 정보통신공학과 (정보통신공학박사 과정)

<관심분야>
컴퓨터 네트워크, 무선통신, 암호화, 네트워크 보안

김 재 영(Jae Young Kim) **[정회원]**

- 1992년 2월 : 연세대학교 대학원 전자공학과 (전자공학 석사)
- 1996년 8월 : 연세대학교 대학원 전자공학과 (전자공학 박사)
- 1996년 9월 ~ 1999년 2월 : ㈜ 대우전자
- 1999년 3월 ~ 현재 : 한국전자통신연구원 책임연구원

<관심분야>
에너지IT, 암호화, 센서무선통신

김 은 기(Eun-Gi Kim) **[정회원]**

- 1989년 2월 : 고려대학교 대학원 전자공학과 (전자공학 석사)
- 1994년 2월 : 고려대학교 대학원 전자공학과 (전자공학 박사)
- 1995년 2월 ~ 현재 : 한밭대학교 정보통신공학과 교수

<관심분야>
컴퓨터 네트워크, 임베디드 S/W, 암호화, 네트워크 보안