http://dx.doi.org/10.5392/JKCA.2015.15.11.501

사용자 ID만을 활용한 간편한 사용자 인증 방안

Convenient User Authentication Mechanism Using only User Identification

김선주*, 조인준**
한국정보통신기술협회*, 배재대학교 사이버보안학과**

Seon-Joo Kim(sunjoo@tta.or.kr)*, In-June Jo(injune@pcu.ac.kr)**

요약

대부분의 웹사이트나 정보시스템은 사용자를 식별하고 인증하기 위하여 ID/PW(Identification/Password) 기술을 사용하고 있다. 그러나 ID/PW 기술은 보안에 취약하다. 또한 사용자는 ID와 PW를 기억해야하고, 패스워드는 쉽게 예측하지 못하도록 영문자, 숫자, 특수문자 등을 조합하여 복잡한 패스워드를 사용해야 하고, 주기적으로 패스워드를 변경해야 한다. 이에 본 논문에서는 외장 스토리지에 사용자 인증정보를 저장하여 사용자를 인증하는 방법을 제안하였다. 이를 통해 다른 사람이 ID와 PW가 알게 되더라도 인증정보가 저장된 외장 스토리지가 없이는 사용자 인증이 되지 않는다. 사용자 인증정보는 사용자가 로그인에 성공할 때마다 새로운 인증정보가 생성되어 외장 스토리지에 저장된다. 따라서 제안한 사용자 인증 방법은 기존의 ID/PW 기술을 활용하는 웹사이트나 다양한 정보시스템 등에서 활용된다면 보안성을 크게 향상시키고, 사용자의 ID만을 사용하기 때문에 사용자의 편의성도 크게 향상될 것으로 기대한다.

■ 중심어 : | 사용자 인증 스킴 | ID/PW 기술 | 사용자 식별 | 사용자 인증 | 난수 | 해시 함수 |

Abstract

Most web sites, information systems use the ID/Password technique to identify and authenticate users. But ID/Password technique is vulnerable to security. The user must remember the ID/Password and, the password should include alphabets, numbers, and special characters, not to be predicted easily. User also needs to change your password periodically. In this paper, we propose the user authentication method that the user authentication information stored in the external storage to authenticate a user. If another person knows the ID/Password, he can't log in a system without the external storage. Whenever a user logs in a system, authentication information is generated, and is stored in the external storage. Therefore, the proposed user authentication method is the traditional ID/Password security technique, but it enhances security and, increases user convenience.

■ keyword : | User Authentication Scheme | ID/PW Technology | User Identification | User Authentication | Random Number | Hash Function |

I. 서 론

최근 인터넷 금융거래에서 크게 부각된 기술이 공인인증서를 활용하지 않는 간편 결제기술이다. 이러한 간편 결제기술의 핵심요소는 인가된 사용자인지 아니면 인가되지 못한 사용자인지를 확인하는 사용자 인증기

접수일자 : 2015년 08월 24일
수정일자 : 2015년 10월 01일
심사완료일 : 2015년 10월 01일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

술이다. 이러한 사용자 인증기술로는 공인인증서를 활용한 사용자 인증기술이 보편적이다. 하지만, 공인인증서를 사용하기 위해서는 많은 액티브X 프로그램을 설치하고, 복잡한 사용자 인증 절차에 따라야 하는 많은 불편함이 있다. 이처럼 사용하기에 불편한 공인인증서를 우리나라는 전자금융 거래에 공인인증서 등을 사용하도록 강제하고 있다[1][2]. 이로 인해 국외에서 국내 쇼핑몰 전자상거래를 제한시키는 결과를 가져와 세계화 시대에 역행한다는 점이 부각되었다.

사용자 인증기술로 공인인증서를 사용하는 것은 보안상 안전성은 매우 높지만, 이를 활용하기 위한 부대비용이 많이 들고, 사용자의 편의성은 떨어진다. 이로 인해 안전성을 높이면서 사용자의 편의성을 제공하는 공인인증서를 대체하는 새로운 사용자 인증방법이 필요하다[3].

사용자 인증 기술로는 단순한 ID/PW 방식[12], OTP 방식[4][5][9][10], 공인인증서[13], 보안카드[6], 지문인식[7][8][11] 등 다양한 기술들이 있다. 하지만, 우리나라에서 많이 사용하는 공인인증서를 제외하고는 안전한 전자상거래를 위한 사용자 인증기술은 다양하지 않다[3].

본 논문에서는 이러한 시대적인 요구에 부응할 수 있는 대안으로 새로운 사용자인증 방안을 제안하였다. 즉, 가장 기본적이면서도 사용하기에 익숙한 ID/PW 인증기술을 응용한 방안으로, 기존의 ID는 그대로 유지하고, 사용자 PW 대신에 정당한 사용자임을 나타내는 사용자 인증정보가 저장된 외장 스토리지를 제시하면 인증되는 방법이다.

이 기술을 통해서 ID/PW기술에서 발생하는 대부분의 보안 취약점을 해소하였다. 또한 응용시스템의 제약 없이 손쉽게 구현이 가능하고, 추가적인 소요 비용에 대한 부담이 적어서 범용적인 활용을 기대할 수 있을 것으로 본다.

본 논문의 구성은 2장에 본 논문과 관련된 기존의 사용자인증 인증방법을 정리하고, 3장에 제안 시스템을 설명하였다. 4장에 제안시스템의 객관적 타당성을 제시하기 위해 다른 사용자 인증방법과 비교 분석을 하였고, 5장에 결론을 맺었다.

II. 제안 동기 및 관련 기술

1. 인증의 개요

암호화는 특별한 지식을 소유한 사람들을 제외하고는 아무도 읽을 수 없도록 평문데이터를 가공하는 것이며, 이를 해독하는 과정 즉, 복호화 과정을 거쳐 암호화된 정보를 다시 읽을수 있다. 또한 해시는 임의의 길이의 데이터를 고정된 길이의 데이터로 변환시켜주는 알고리즘으로 입력값이 같으면 출력값은 항상 동일한 특징을 갖는다. 보안서비스의 4대 요소는 기밀성, 무결성, 인증, 부인봉쇄이며, 그 중에서 인증은 사용자 인증과 메시지 인증으로 분류된다. 특히, 사용자 인증은 다양한 응용시스템으로의 접근 가능 여부를 결정하는 매우 중요한 보안 요소로, 본 논문에서 제안한 방법은 기존에 PW 기반의 사용자 인증 방법을 개선하는 것이다. 기존 ID/PW 기반의 사용자 인증시스템에서 ID/PW가 해커에게 노출되면, 해커는 해당 응용 시스템에 정당한 사용자로 로그인 막대한 피해를 줄 수 있다[3].

2. 사용자 인증 기술

사용자 인증기술은 해당 사용자만이 알고 있거나 혹은 소유하고 있는 정보를 사전에 응용 시스템에 등록하고, 응용 시스템에 로그인 시 사용자의 패스워드, 사용자의 인증서, 보안카드, 전화, 전자메일, 지문, 홍채 등을 제시하고, 등록된 정보와 일치하는 사용자만 정당한 사용자로 허용하고, 그이외의 모든 사용자를 거부한다.

이러한 방식으로 가장 널리 사용되는 방식은 ID/PW 방식이다. 이는 사용자 등록 시, 사용자가 제시한 식별자(ID, Identifier)와 패스워드(PW, Password)를 응용시스템에 저장한다. 사용자 등록된 이후에는 응용 시스템이 사용자에게 ID와 PW를 요구하며, 입력된 ID와 PW가 응용 시스템에 저장된 내용과 일치하면 응용 시스템으로의 접근을 허용하는 인증 기술이다. 하지만, 응용 시스템에 저장된 ID/PW 정보가 해킹에 의해 노출되거나 시스템 관리자가 ID/PW 정보를 악의적으로 이용하는 경우 막대한 피해를 입을 수 있다. 이러한 피해를 방지하기 위해 대부분 ID/PW 파일을 암호화하여 저장하고, PW 조합규칙(예. 최소 9자이상 15자 이내, 영문

자/숫자/특수문자 조합 등)을 강제로 요구한다. 하지만, 이러한 ID/PW 보호대책에도 불구하고 ID/PW 기반의 사용자 인증 기술은 사전 공격, 스니핑 등의 해킹 공격에 취약한 약점이 있고, 복잡한 PW 조합규칙과 주기적인 갱신으로 인해 사용자의 불편함을 초래한다[12-14].

이러한 취약점을 보완하기 위해 복잡하고 추가적인 비용을 요구하는 PKI(Public Key Infrastructure) 기반의 인증서 방식을 도입하였다. 이러한 PKI 기술은 인터넷 상의 전자상거래를 안전하게 사용하고 관리하기 위한 정보보호표준 방식으로, 발급 받은 인증서를 이용하여 인터넷 상의 사용자 간의 전자서명과 암호화를 지원한다[13]. 즉, PKI 기반의 인증서를 사용자가 응용 시스템에 제시하고 이를 PKI 인증 시스템을 통해 본인임을 확인받는 방식이다. PKI 기반 인증서 방식은 ID/PW 방식보다 보안 강도가 뛰어나지만, PKI 인증 시스템을 운영해야하고 인증서를 발급하고 안전하게 유지해야하는 부담 등이 약점이다.

또 하나의 사용자 인증방식으로 널리 사용되는 방식이 보안카드와 일회용 패스워드(OTP, One Time Password), 핸드폰 및 메일 인증을 들 수 있다. 이들 인증방식은 독자적으로 사용되기 보다는 ID/PW 또는 인증서 방식과 혼합시켜 사용자 인증을 강화하는 방안으로 주로 사용한다. 하지만, 보안카드는 인쇄된 제한적인 35개의 4자리 숫자만 사용하기 때문에 해킹에 노출된 사례가 발생하였다[14][15]. 따라서 일회용 패스워드를 생성하는 생성기인 OTP로 대체하여 사용자 인증을 강화하는 방향으로 진화하고 있다. 이러한 기술들은 사용자 인증 강화에는 도움이 되지만, 보안카드나 OTP를 제작하고 사용자에게 배포하는 비용이 수반되는 단점이 있다. 다음으로 핸드폰 및 메일 인증은 각 이동 통신사 및 메일 시스템에서 사용자를 확인해주는 수단으로 개입되기 때문에 안전한 인증 수단으로 볼 수는 없다.

마지막으로 사용자의 지문이나 홍채 등의 인간의 생체 정보를 이용하는 사용자 인증 방식이 있으나, 고가의 지문이나 홍채 인식 장비 필요한 단점이 있다.

3. 제안 동기

ID/PW 방식처럼 단순하면 사용성은 우수하지만, 보안에 취약하다. 반면에, 인증서 방식 / OTP 방식 / 생체정보를 이용한 사용자 인증 방식은 안전성은 뛰어나지만 사용의 제약 및 추가적인 비용이 요구되는 단점이 존재한다.

따라서 가장 중요한 사용자 인증 강도를 높이면서도 사용의 수월성을 확보할 수 있는 새로운 방안으로 외장 스토리지를 활용한 PW기반 사용자 인증기술이 제안되었다[3]. 제안기법은 ID/PW 기술을 준용하면서 인증정보를 외장 스토리지에 저장하여 사용자 인증 강도와 사용의 수월성을 제고한 방안이다. 하지만, 이 기술은 사용자 패스워드를 항상 기억하여 입력해야 하는 번거로움이 내재되어 있다.

본 논문에서는 외장 스토리지를 활용한 PW기반 사용자 인증기술의 단점을 해결하고자 한다. 즉, 기존의 ID/PW 방식에서 사용자 인증을 위한 보안 강도를 인증서 수준으로 높이면서, 사용자는 자신의 ID만 기억하고 인증정보는 외장 스토리지에 저장함으로써 가능한 간편 사용자 인증 기술이다. 또한, 제안시스템은 응용 시스템에 제한 없이 도입이 편리하도록 설계 하였으며 사용자는 외장 스토리지만 있으면 사용자 등록과 응용 시스템에 사용이 가능하도록 하였다.

따라서 제안 시스템은 인증서 방식처럼 다양한 기반 시스템 설치 및 운영이 필요 없고, 보안카드나 OTP 기기를 추가로 제작하여 배포할 필요도 없으며, 지문이나 홍채와 같은 고가의 장비가 필요 없다. 이러한 이유로 인해 사용자 인증 시스템 구축비용이 저렴하고 응용 시스템의 제한 없이 적용 가능하여 범용성을 확보하였다.

지금까지 다양한 사용자 인증기술의 특성을 정리하고 본 논문을 제안하게 된 동기를 설명하였다. 다음 장에서는 본 논문에서 제안한 사용자 인증시스템의 설계 내용 및 동작절차를 설명하였다.

Ⅲ. 제안 방안

본 논문에서는 응용시스템에서 사용하는 ID/PW 방식의 보안 취약점 개선 및 사용자 편의성 제고에 초점을 맞추었다. 즉, ID/PW 방식의 가장 큰 취약점은 사용자의 패스워드가 해킹을 통해 제3자에게 노출되는 경

우, 응용시스템은 속수무책으로 당할 수밖에 없다. 이러한 해킹으로부터 사용자를 보호하기 위해 영문자/숫자/특수문자로 구성되는 복잡한 패스워드를 사용하도록 하며, 이러한 패스워드를 주기적으로 변경하도록 요구하고 있다.

제안 시스템은 최초 사용자가 ID/PW를 등록 시 ID만 입력하면 그에 대응되는 사용자인증정보와 응용시스템 인증정보 파일을 자동으로 생성하여 외장 스토리지에 암호화되어 저장한다. 응용시스템 사용자로 등록된 사용자가 응용 시스템에 접근 시 자신의 ID와 소지하고 있는 외장 스토리지에 저장된 인증정보를 응용시스템에서 불러와 사용자를 인증하는 시스템이다. 따라서 사용자는 복잡한 조합규칙을 갖는 패스워드를 기억하고 입력 할 필요가 없을 뿐만 아니라, 주기적으로 패스워드를 변경하지 않아도 동일한 안전성을 보장하는 새롭고 간편한 사용자인증 기술이다. 즉, 사용자의 ID가 해킹공격에 의해 노출되더라도, 외장 스토리지에 저장된 인증정보가 없으면 사용자 인증에 성공할 수 없는 안전성이 보장된 방안이다. 이를 위해서 사용자가 소지하고 있는 외장 스토리지(예. USB 메모리 등)에 사용자 인증정보를 저장하고, 필요시 이를 제시하도록 하였다.

먼저 제안시스템을 설명하기 위해 사용되는 기호에 대한 표기법은 다음과 같은 의미를 갖는다[표 1].

표 1. 표기법

부호	의미
Un_ID	사용자 Un의 식별자 ID
En(m)	n이란 키로 m을 대칭 암호화
Dn(m)	n이란 키로 m을 대칭 복호화
(I+m+n…)	I , m, n ..항목으로 구성된 레코드

1. 사용자 등록 절차

본 절에서는 제안시스템에서 사용자 Un을 등록하는 절차에 대해 설명한다.

[그림 1]에서 보는 바와 같이 사용자 등록 절차는 다음과 같다.

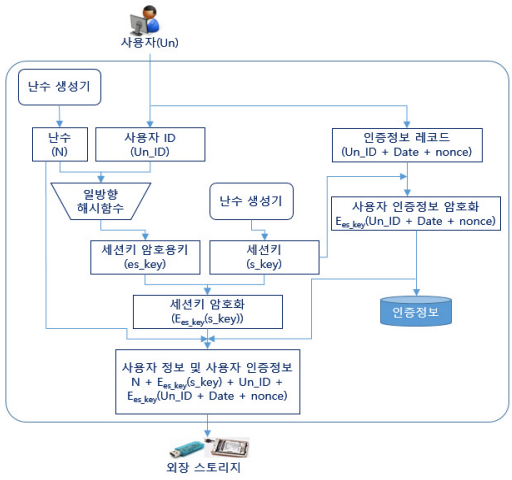

그림 1. 사용자 Un의 등록 절차

Step 1) 사용자 Un이 패스워드 입력 없이 사용자 ID인 Un_ID를 입력한다.

Step 2) 난수 생성기를 통해서 난수 N을 생성한다.

Step 3) 입력된 사용자 ID인 Un_ID와 Step 2)에서 생성한 난수 N을 조합한 문자열을 일방향 해시함수 입력 후 출력 값으로 세션키 암호용 키 es_key를 생성한다. 생성된 es_key는 사용자 인증정보를 보호하기 위해 사용하는 세션키 s_key를 보호하기 위한 대칭키이다.

Step 4) Step 2)와 같이 의사난수 생성기를 사용하여 사용자 인증정보를 보호하기 위한 세션키 s_key를 생성한다.

Step 5) Step 1)에서 입력된 사용자 ID인 Un_ID를 이용하여 사용자 Un의 인증정보 레코드를 생성한다. 즉, {Un_ID+date+nonce}이다. 먼저, Un_ID은 사용자 ID이고, date는 사용자 인증정보 등록날짜이고, nonce는 사용자 인증정보의 재사용 공격을 방어하기 위한 비표이다.

Step 6) Step 3)에서 생성된 es-key로 Step 4)에서 생성된 s_key를 암호화 한다.

⇒ Ees_key(s_key)

Step 7) Step 5)에서 사용자 Un의 인증정보 레코드를 step 4)에서 생성된 s_key로 암호화한다.

⇒ Es_key(Un_ID+date+nonce)

Step 8) Step 7)에서 사용자 Un과 인증정보 레코드를 암호화한 Es_key(Un_ID+date+ nonce))를 조합하여 제안시스템의 인증정보 파일로 저장한다.

Step 9) 외장 스토리지에 저장할 인증정보를 생성하는 단계로, Step 2)에서 생성된 난수 N과 Step 6)에서 만들어진 세션키를 암호화 결과 Ees_key(s_key), 그리고 Step 8)에서 만들어진 인증 정보 파일 저장값(즉, Un_ID + Es_key(Un_ID+date+nonce))를 조합하여 외장 스토리지에 저장한다.

⇒ N + Ees_key(s_key) + Un_ID + Es_key(Un_ID +date+nonce)

2. 사용자 인증 절차

이 절에서는 앞 절에서 등록된 사용자 Un이 제안시스템에 접근했을 때 상세한 인증절차를 설명한다. 사용자 Un이 제안시스템에서 인증 받는 절차는 [그림 2]와 같다. 사용자 Un의 단계별 인증절차는 다음과 같다.

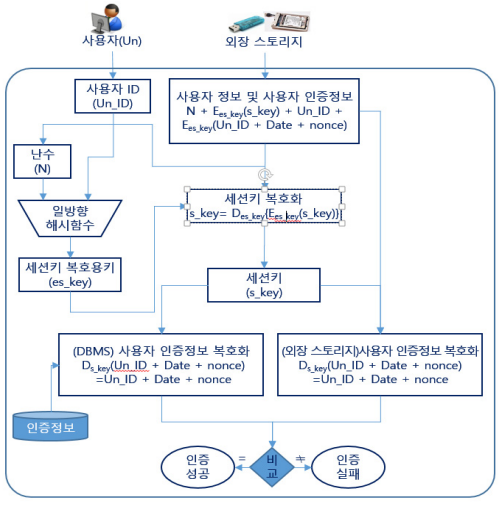

그림 2. 사용자 Un의 인증 절차

Step 1) 사용자 Un이 자신의 Un_ID를 입력한다.

Step 2) 외장 스토리지로부터 난수 N과 Step 1)에서 입력된 사용자 Un의 Un_ID를 일방향 해시함수에 입력하여 세션키 복호용 키 es_key를 생성 한다.

Step 3) 외장 스토리지로부터 불러온 데이터Ees_key (s_key)를 Step 1)에서 생성된 세션키 복호용 키 es_key로 복호화하여 세션키 s_key를 구한다.

⇒ Des_key{Ees_key(s_key)} = s_key

Step 4) 외장 스토리지로부터 암호화된 사용자 Un의 인증정보를 Step 3)에서 복호된 s_key로 복호화 한다.

⇒ Ds_key{Es_key(Un_ID+date+nonce))} = Un_ID+date+nonce

Step 5) 인증정보 파일로부터 읽어 들인 사용자 Un의 인증정보를 Step 3)에서 복호된 s_key로 복호화 한다.

⇒ Ds_key{Es_key(Un_ID+date+nonce))} = Un_ID+date+nonce

Step 6) Step 4)와 Step 5)에서 복호된 인증정보가 동일하면 사용자 인증에 성공하고, 다르면 사용자 인증에 실패한다.

3. 인증에 성공한 사용자의 인증정보 재구성 절차

본 절에서는 2절에서 인증에 성공한 사용자 (Un)의 다음 인증세션을 위해 인증정보를 재구성하는 절차를 설명한다. 사용자 인증정보 재구성 절차는 [그림 3]과 같다.

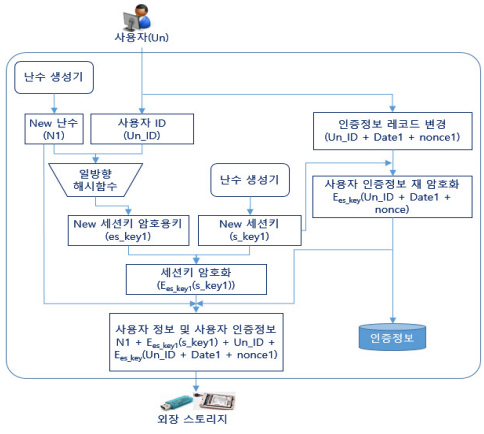

그림 3. 사용자 인증정보 재구성 절차

세부 단계별 사용자 인증정보 재구성 절차는 다음과 같다.

Step 1) 제안 시스템은 난수 생성기로 새로운 난수 N1을 생성한다.

Step 2) 입력된 사용자 ID인 Un_ID와 Step 1)에서 생성된 난수 N1을 조합한 문자열을 일방향 해시함수에 입력값으로 사용하고, 출력값으로 세션키 암호용 키 es_key1를 생성한다.

Step 3) 사용자 인증정보를 암호화하기 위한 새로운 세션키 s_key1을 난수 생성기로 생성한다.

Step 4) 변경된 날짜 date1과 변경된 nonce값 nonce1을 조합하여 사용자 Un의 인증정보를 변경한다.

⇒ Un_ID + date1 + nonce1

Step 5) Step 2)에서 생성된 es_key1과 세션키s_key1의 노출을 방지하기 위해 새로운 es_key1로 암호화 한다.

⇒ Ees_key1(s_key1)

Step 6) Step 4)에서 변경된 사용자 Un의 인증정보의 노출을 방지하기 위해 Step 3)에서 생성된 s_key1로 인증정보를 암호화한다.

⇒ Es_key1(Un_ID+date1+nonce1))

Step 7) Step 6)에서 암호화된 인증정보를 제안 시스템 인증정보 파일에 저장한다.

Step 8) Step 1)에서 생성된 난수 N, Step 5)에서 암호화된 Ees_key1(s_key1), Step 6)에서 암호화된 사용자 인증정보를 외장 스토리지에 저장한다.

지금까지 제안시스템을 사용자 등록에서부터 사용자 인증절차, 사용자 인증 후 인증정보의 재구성 절차를 설명하였다. 다음 장에서는 제안시스템의 안전성을 기존의 여러 인증방식과 비교하였다.

Ⅳ. 고찰 및 검증

본 논문에서 제안한 시스템은 참고문헌[3]을 개선한 것이다. 즉, 사용자 인증을 위해 기존의 ID/PW 방식에서 PW를 입력받지 않고, 외장스토리지에 저장된 사용자 인증정보를 활용할수 있도록 하여 보안성을 높이고, 시스템 구축비용을 낮추며 사용자의 편리성을 가질 수 있도록 고안하였다.

이를 위해, 기존의 여러 가지 사용자 인증 방법과 비교하여 제안시스템의 우수성을 객관적으로 제시하였다.

본 장에서는 기존의 ID/PW, 인증서, 지문, OTP, 참고문헌[3] 등의 사용자 인증방법과 비교하였다.

표 2. 기존 인증방법과 제안 인증방법 비교분석

종류 / 대상	ID/PW	인증서	지문	OTP	참고문헌 [3]	제안 시스템
인증정보 특성	정적	정적	정적	동적	동적	동적
PW 변경	필요	필요	없음	불필요	불필요	없음
재사용	가능	가능	가능	불가 (1회 사용)	불가 (1회 사용)	불가 (1회 사용)
인증 요소	기억정보	기억정보 + 인증서	생체정보	난수정보	기억정보 + 이동매체 정보	저장매체 비밀정보
휴대성	높음	보통	높음	낮음	보통	보통
구축 비용	하	상	상	중	하	하
위변조 가능성	높음	낮음	낮음	낮음	낮음	낮음
편리성	중	하	상	중	중	상
보안 강도	하	상	상	상	상	상

[표 2]에서 살펴본 바와 같이 제안 시스템은 패스워드를 입력받지 않아서 주기적인 패스워드의 변경이 요구되지 않고, 영문자/숫자/특수문자 등의 조합규칙을 준수하거나 기억하지 않아도 되어 사용자의 편의성을 크게 향상 시켰다. 또한 인증정보는 해당 세션에서만 사용하는 1회성이므로 재사용이 불가능하고, 암호화 되어 저장되므로 위변조 가능성이 적으면서도 보안성이 뛰어남을 알 수 있다. 마지막으로, 저렴한 외장 스토리지를 별도의 포맷이나 변경 없이 바로 활용할 수 있어 휴대가 편리하고 작은 비용으로 시스템을 구축하여 보안성을 향상시킬 수 있는 장점이 있다.

V. 결 론

본 논문에서는 ID/PW 기반의 사용자 인증 방법에서 자주 발생하는 패스워드(PW) 노출에 대한 해결 방안을 제안하였다. 즉, 제안 시스템에 사용자 등록 시 ID만을 등록하면 인증정보가 자동으로 생성되어 안전한 외장 스토리지에 저장되고, 제안 시스템에 등록된 사용자가 제안 시스템에 접근하는 경우 사용자가 자신의 ID와 외장 스토리지만을 제시하면 안전하게 사용자 인증이 된다. 또한, 인증이 완료될 때마다 새로운 인증정보를 생성하여 외장 스토리지에 저장하고 사용자가 제안 시스템에 재접속 시 새로운 인증정보를 사용한다.

제안 방안은 사용자 인증정보를 외장 스토리지에 저장하고 인증정보 활용시마다 재구성 함으로써, 기존의 ID/PW 방식의 보안 취약점인 패스워드 노출 취약성을 완전히 해결하였으며, 복잡하고 어려운 사용자 패스워드를 주기적으로 변경할 필요성이 없어졌다. 따라서 제안 방안은 ID/PW 기반의 사용자 인증 방식을 사용하는 대부분의 정보시스템에서 외장 스토리지와 조합하여 활용 가능하다.

향후 연구방향으로는 다양한 외장 스토리지(USB, 스마트폰 등)에 사용자 인증정보를 안전하게 저장하는 기술을 개발하고, 이를 다양한 정보시스템에 적용하며, 사용자 인증정보를 통합관리가 가능하도록 지속적인 연구가 필요하다.

참 고 문 헌

[1] 이정현, “스마트 환경에서의 공인인증서 활용과 문제점,” Internet & Security Focus, 2013년 3월호.

[2] 전자서명법 [법률 제10008호, 2010.02.04. 시행].

[3] 김선영, 김선주, 조인준 “이동저장매체를 활용한 패스워드기반 사용자인증 강화 방안,” 한국콘텐츠학회논문지, 제14권, 제11호, 2014(11).

[4] 송성현, 김근옥, “국내외 OTP 표준화 동향,” 정보보호학회지, 제22권, 제2호, 2012(4).

[5] 최동현, 김승주, 원동호, “일회용 패스워드 기술 분석 및 표준화 동향,” 정보보호학회지, 제17권, 제3호, 2007(6).

[6] 이형우, “안전한 로그인을 위한 소프트 보안카드 기반 다중 인증시스템,” 한국콘텐츠학회논문지, 제9권, 제3호, 2009(3).

[7] 반성범, 문지현, 정용화, 김학일, “지문 인식 기술 동향,” 전자통신동향분석, 제16권, 제5호, 2001(10).

[8] 김영진, 반성범, 문대성, 길연희, 정용화, 정교일, “임베디드 생체인식기술 구현 : 지문 보안토큰 시스템,” 전자통신동향분석, 제17권, 제6호, 2002(12).

[9] 김근옥, 심희원, “OTP 기반 인증기술 국제표준화 동향,” 정보처리학회지, 제23권, 제3호, 2013(6).

[10] N. Haller, C. Metz, P. Nesser, and M. Straw, “A One-Time Password System,” RFC 2289, IETF, 1998.

[11] A. Jain L. Hong, and R. Bolle, “An Identity-authentication S. Pankanti, System Using Finger-prints,” Proceedings of the IEEE, 1997.

[12] 김영수, 나중찬, 손승원, “패스워드 인증 프로토콜 동향,” 전자통신동향분석, 제16권, 제6호, 2001(12).

[13] 김선주, 조인준, “OTP를 이용한 PKI 기반의 개인키 파일의 안전한 관리 방안,” 한국콘텐츠학회논문지, 제14권, 제12호, 2014(12).

[14] http://blog.skbroadband.com/764

[15] http://slownews.kr/12222

저 자 소 개

김 선 주(Seon-Joo Kim) 정회원

- 1998년 2월 : 배재대학교 컴퓨터공학과 졸업
- 2001년 2월 : 배재대학교 컴퓨터공학과 석사
- 2013년 2월 : 배재대학교 컴퓨터공학과 박사
- 2001년 ~ 2003년 : ㈜케이사인 선임연구원
- 2003년 ~ 현재 : 한국정보통신기술협회 책임연구원

<관심분야> : 클라우드 컴퓨팅, SW 테스팅, 정보보호 제품 평가

조 인 준(In-June Jo) 정회원

- 1982년 2월 : 전남대학교 계산통계학과 졸업
- 1985년 2월 : 전남대학교 전자계산학과 석사
- 1999년 2월 : 아주대학교 컴퓨터공학과 박사
- 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
- 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

<관심분야> : 정보보호, 컴퓨터네트워크보안, 전산조직응용