http://dx.doi.org/10.5392/JKCA.2014.14.11.533

이동 저장매체를 활용한 패스워드 기반 사용자 인증 강화 방안

Enhanced Password Based User Authentication Mechanism Using Mobile Storage Medium/Channel

김선영, 김선주, 조인준
배재대학교 사이버보안학과

Seon-Young Kim(carran@pcu.ac.kr), Seon-Joo Kim(sunjoo@tta.or.kr),
In-June Joe(injune@pcu.ac.kr)

요약

현재 응용시스템 혹은 시스템에서 사용되고 있는 사용자 인증방법은 단순한 ID/PW를 비롯하여 인증서, 지문/홍채, 전화, 보안카드, OTP 등 다양한 기술들이 사용되고 있다. 하지만 단순한 ID/PW, 전화인증 등은 보안에 취약한 단점이 있고, 인증서, 지문/홍채, 보안카드/OTP 등은 보안에 취약점은 상당 부분 해소했으나 이를 활용하기에는 소요되는 비용 및 복잡성이 내재되어 있다.

본 논문에서는 보안강도를 제고하면서 흔히 소장하고 있는 USB와 같은 이동형 저장매체를 활용하여 저비용으로 사용자 인증을 보다 안전하게 할 수 있는 새로운 방안을 제안하였다.

■ 중심어 : | 사용자 인증 | 저장 매체 | 난수 | 패스워드 기반 |

Abstract

As for the application system or the user authentication scheme that is used in the system, various technologies including simple ID/PW, certificate, fingerprint/iris, phone, security card, and OTP are being used. But simple ID/PW and phone certification lack security features. As for the certificate, fingerprint/iris, and security card/OTP, the weakness in security has been quite strengthened, but there are costs and complexity involved to use these.

This paper proposes a new measure of much safer and low-cost user authentication that improves the security level and uses mobile external storage media such as USB that people commonly have.

■ keyword : | User Authentication | USB | Nonce | Password Based |

I. 서 론

최근 들어 정부가 규제개혁의 필요성을 부각시키는 과정에서 그 대표적인 사례로 전자상거래에서 공인인증서의 불편한 사용성이 쟁점이 되었다. 즉, 우리나라만이 일정 규모 이상의 전자거래시 사용자 인증을 공인인증서로 하도록 한 전자상거래 법이 문제가 되었다[1][2]. 따라서 국외에서 국내 쇼핑몰 전자상거래를 제한시키는 결과를 가져와 세계화 시대에 역행한다는 점이 부각되었다.

사용자 인증에 공인인증서를 사용하는 것은 안전성은 매우 높은 편이나 이를 활용하기 위한 부대비용 및

접수일자 : 2014년 08월 07일
수정일자 : 2014년 09월 17일
심사완료일 : 2014년 09월 17일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

사용의 수월성은 낮은 것이 사실이다. 따라서 보안 강도를 높이면서 사용의 수월성이 좋은 제 3의 사용자 인증방법이 필요한 것이 또한 사실이다.

현재 사용 중인 사용자 인증방법은 초보적인 ID/PW 방식으로부터 공인인증서에 이르기 까지 다양한 기술들이 있다. 하지만, 공인인증서를 제외하고는 안전하게 전자상거래에 사용할 수 있는 사용자 인증방법은 흔하지 않다.

기존 연구를 살펴보면 참고문헌 [3]에서는 다중인증 시스템을 제안하고 있다. ID/PW뿐만 아니라 소프트웨어 보안카드와 생체정보를 이용하여 다중인증시스템을 제안하고 있으나 소프트웨어 보안카드를 별도로 발급받아야 한다는 불편함과 소프트웨어 보안카드는 보안에 취약하다는 약점을 가지고 있다. 또한 생체정보를 이용하여 보안의 강도는 높였으나 이 또한 성능의 저하를 가져온다. [4]에서는 OTP의 취약점에 대해 분석했다. PC에 S/W 방식으로 구현된 OTP는 역공학을 통해 분석한 결과 마스터키, 시간 정보가 노출되었고, PIN·마스터키·시간 정보의 위·변조가 가능하다고 설명하고 있다. [5]에서는 홍채 인식을 통한 사용자 인증을 제안하고 있으나 이 시스템은 마우스를 활용해야 하기 때문에 치우침 현상이 발생한다는 오류와 이동식이 아닌 고정식이라는 것과 무엇보다도 자동 초점 조절 기능이 없어 선명한 영상을 위해서는 수동으로 영상을 획득해야 한다는 단점을 가지고 있다.

본 논문에서는 이러한 시대적인 요구에 부응할 수 있는 대안으로 새로운 사용자인증 방안을 제안하였다. 즉, 기존에 가장 기본적이면서도 사용에 익숙한 ID/PW 인증방법을 준용하면서도 ID/PW기술에서 발생하는 대부분의 보안 취약점을 해소한 방안이다. 또한 어떤 응용 시스템에서나 손쉽게 구현이 가능하고 이에 소요되는 추가적인 비용부담이 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

4대 요소는 기밀성, 무결성, 인증, 부인봉쇄를 말한다. 이중에서 인증은 사용자 인증과 메시지 인증으로 분류된다. 사용자 인증은 다양한 시스템에 접근 허용 유무를 결정하는 중요한 보안 서비스이다. 본 논문은 사용자 인증시스템에 관한 내용이다. 사용자 인증시스템이 취약하면 그 시스템이 해킹의 대상이 되어 시스템에 막대한 피해를 주는 것이 사실이다. 즉, 해커가 시스템을 해킹하여 그 시스템에 들어가 실 사용자로 위장하여 실 사용자처럼 행세할 수 있음을 의미한다.

2. 사용자 인증 기술

사용자 인증기술의 기본 아이디어는 해당 사용자만이 알고 있거나 혹은 소유하고 있는 것을 활용한다. 즉, 시스템에 등록할 때, 제시한 해당 사용자의 패스워드나, 해당 사용자만이 가지고 있는 인증서, 보안카드, 전화, 전자메일, 지문, 홍채 등을 활용한다.

가장 간단하면서 범용적으로 사용되는 사용자 인증 시스템은 ID/PW방식이다. 이는 시스템에 사용자를 등록할 때, 해당 사용자가 제시한 식별자(ID, Identifier)와 이에 대응하는 패스워드(PW, Password)를 시스템에 저장한다. 등록 후 사용시 제시된 ID에 대응하는 PW가 일치하면 시스템에 접근을 허용하는 단순한 기술이다. 이러한 시스템의 취약점은 그 시스템에서 사용하는 ID/PW파일이 해킹 당했을 때, 그리고 시스템 관리자가 ID/PW파일을 읽을 수 있을 때 막대한 피해를 감수해야 한다. 이러한 공격에 대비하여 ID/PW파일을 암호화하거나 일방향 해쉬함수를 사용하여 패스워드가 직접 노출되지 않도록 한다. 또 하나의 취약점은 사전에 있는 단어를 입력하여 암호를 알아내거나 해독하는 컴퓨터 공격법인 사전공격, 똑같은 환경에서 똑같이 일어나는 재현공격, 네트워크 트래픽을 도청하는 스니핑 공격을 통해서 ID에 해당하는 PW가 노출되거나, 이전의 ID/PW를 가로채서 재현했을 때, 무방비로 위장공격을 당할 수 있다. 이러한 ID/PW방식의 사용자 인증시스템은 간단하게 구현하여 사용할 수 있는 장점이 있는 반

면에 ID/PW 해킹에 취약하다는 절대적인 약점이 내제되어 있다[6].

이러한 ID/PW 사용자 인증시스템의 약점을 보완하기 위해 보다 복잡하고 추가적인 비용이 유발되는 방식이 도입되었다. 대표적인 방안으로 인증서를 활용하는 방식이다. 즉, 공개키 인프라(PKI, Public Key Infrastructure)를 통해서 인증서를 발행 받고, 사용자가 시스템에 접근시에 발행 받은 인증서를 제시하여 PKI를 통해서 본인임을 확인 받는 방식이다. 이 방식은 ID/PW방식보다 보안 강도가 뛰어나 인증서를 도난당하지 않는 한 현재까지 해킹을 당한 사례가 없는 것으로 알려져 있다. 하지만, 이러한 사용자 인증 시스템은 PKI를 운영해야 하는 부담, 인증서를 발급하여 안전하게 유지하는 부담 등이 동반 되어 사용의 수월성이 낮은 것이 약점이다[1].

또 하나의 사용자 인증방식으로 널리 사용되는 방식이 보안카드와 일회용 패스워드(OTP, One Time Password), 핸드폰 및 메일 인증을 들 수 있다. 이들은 독자적으로 사용되기 보다는 상기에서 언급한 ID/PW 및 인증서 방식과 혼합시켜 사용자 인증을 강화하는 측면에서 채택되어 사용하는 경향이다. 보안카드는 인쇄된 제한적인 개수의 보안번호만 사용하기 때문에 이를 타겟으로 한 보안 공격에 노출된 사례가 발생하였다[7][8]. 따라서 일회용 패스워드를 생성하는 생성기인 OTP로 대체하여 사용자 인증을 강화하는 방향으로 진화하고 있다[9][10]. 이들은 사용자 인증강화에는 도움이 되지만, 보안카드나 OTP를 제작하여 사용자에게 분배하는 비용이 수반되는 단점이 내제되어 있다. 다음으로 핸드폰 및 메일인증은 각각 통신사 및 메일시스템이 사용자 확인 수단으로 개입되기 때문에 안전한 인증 수단으로 볼 수는 없다.

마지막으로 언급할 수 있는 방식은 지문이나 홍채를 이용하는 인간의 생체적인 특성을 이용하는 방식이 있으나 이 또한 지문이나 홍채를 인식하는 기기가 필요하여 비용적인 측면에서 범용적으로 적용이 쉽지 않은 것이 또한 사실이다.

3. 제안 동기

앞 절에서 살펴보았듯이 사용자 인증방식이 단순하면 사용성은 우수하나 보안 취약점이 많고, 복잡하면 보안취약점은 대부분 해소되나 사용의 제약 및 추가적인 비용이 유발되는 것이 단점이다. 따라서 가장 중요한 사용자 인증 강도를 높이면서도 사용의 수월성을 확보할 수 있는 새로운 방안을 모색하는 것은 자연스러운 현상이다[11].

본 논문에서는 기존에 사용자에게 익숙한 ID/PW방식을 준용하면서 사용자 인증강도를 인증서 수준에 이를 수 있는 새로운 사용자 인증 시스템을 제안하였다. 즉, ID/PW방식의 사용법을 그대로 수용하고, 현재 보편적으로 활용되고 있는 USB와 같은 범용 이동저장매체만 가지고 있으면 인증서 수준의 사용자 인증 강도를 제공할 수 있는 시스템이다.

또한, 제안시스템은 어떤 시스템에서도 도입이 편리하도록 설계 되었으며 사용자는 USB와 같은 범용 이동저장매체만 있으면 사용자 등록과 시스템 사용을 가능하도록 하였다.

따라서 제안 시스템은 인증서 방식과 같이 PKI와 같은 무거운 기반설비가 필요 없고 보안카드나 OTP와 같은 것을 제작하여 배포할 필요도 없고, 지문이나 홍채와 같이 이를 인식하는 인식기기가 필요 없기 때문에 구축비용이 저렴하고 어떤 시스템에서나 적용이 가능하여 활용의 범용성을 확보하였다.

지금까지 현재 사용되는 사용자 인증기술들의 특성정리와 더불어 본 논문의 사용자인증 시스템을 제안하게 된 동기를 설명하였다. 다음 장에서는 본 논문에서 새롭게 제안한 사용자 인증시스템의 설계내용 및 동작절차를 설명하였다.

Ⅲ. 제안 방안

본 논문의 기본 아이디어는 응용시스템에서 사용하는 기본적인 ID/PW방식의 보안 취약점 개선에 초점을 맞추었다. ID/PW방식의 가장 큰 취약점은 패스워드의 노출을 들 수 있다. 패스워드가 기술적으로 스니핑을

당하거나 패스워드 사전공격으로 노출되거나 기록해 놓은 패스워드 파일을 도난당한 경우 등 다양한 패스워드 공격이 성공했을 때 속수무책으로 당할 수밖에 없는 것이 현실이다. 따라서 이러한 공격으로부터 사용자를 보호하기 위해 패스워드를 수시로 바꿀 것을 권고하고 있다.

본 논문에서는 한번 패스워드를 등록하면 수시로 패스워드를 바꾸지 않아도 안전성을 보장하는 새로운 사용자인증 방안을 제안하였다. 즉, 패스워드가 노출되어도 안전성을 보장하는 방안이다. 이를 위해서 사용자는 흔히 소지하고 있는 이동저장매체(USB)에 사용자 인증정보를 추가적으로 저장하여 소지하도록 하였다. 이를 위해 설계한 제안시스템을 설명하면 다음과 같다. 아래 절에서 사용되는 기호에 대한 표기법은 다음과 같은 의미를 갖는다.

표 1. 표기법

부호	의미
ID_Un	사용자 Un의 식별자 ID
PW_Un	사용자 Un의 패스워드
En(m)	n이란 키로 m을 대칭 암호화
Dn(m)	n이란 키로 m을 대칭 복호화
(I+m+n…)	I , m, n ..항목으로 구성된 레코드
Un(I+m+n…)	사용자 Un의 레코드에서 사용자 ID를 제외한 항목들

1. 사용자 등록 절차

본 절에서는 응용시스템에서 사용자 Un을 등록하여 시스템을 사용할 수 있도록 하는 절차에 대해 설명한다. 사용자 Un을 등록하는 절차는 [그림 1]과 같다.

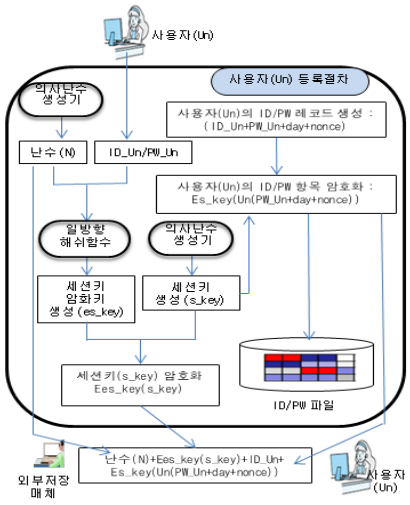

그림 1. 사용자 Un 등록 절차

[그림 1]에서 본 바와 같이 단계별 등록절차를 상세히 설명하면 다음과 같다.

Step 1) 사용자 Un이 ID_Un/PW_Un를 입력한다.

Step 2) 제안 시스템은 의사난수 생성기를 통해서 난수 N을 생성한다.

Step 3) 입력된 패스워드 PW_Un과 생성된 난수 N을 일방향 해쉬함수에 입력하여 출력물로 하나의 키 es_key를 생성한다. 이 키는 한 세션에서만 인증정보를 보호하기 위해 사용하는 세션키(s-key)를 보호하기 위한 키이다.

Step 4) 의사난수 생성기를 사용하여 등록 세션에서 인증정보를 보호하기 위한 세션키(s-key)를 생성한다.

Step 5) 사용자 Un의 인증정보를 시스템 ID/PW파일에 저장하기 위해 사용자 Un의 인증정보레코드를 생성한다. 즉, {ID_Un+PW_Un+day+nonce}이다. ID_Un은 사용자 ID이고, PW_Un은 Un의 패스워드이

고, day는 세션등록일이고, nonce는 등록세션 인증정보를 재현하는 공격을 방어하기 위한 비표이다.

Step 6) 등록세션 step 3)에서 만들어진 es-key로 세션키(s-key) 노출을 방지하기 위해 s_key를 암호화 한다.
⇒ Ees_key(s-key)

Step 7) 등록세션 Step 5)에서 만들어진 Un의 인증정보 레코드 노출을 방지하기 위해 step 4)에서 만들어진 s_key로 Un의 레코드에서 ID_Un 항목을 제외한 모든 항목을 암호화한다.
⇒ Es_key(Un(PW_Un+day+nonce))

Step 8) Step 7)에서 인증정보가 암호화된 Un의 레코드 Es_key(Un(PW_Un+day+nonce))를 시스템 ID/PW파일에 저장한다.

2. 사용자 인증 절차

이절에서는 앞 절에서 등록된 사용자 Un이 시스템에 접근했을 때 구체적인 인증절차를 설명한다. 사용자 Un이 등록된 시스템에서 인증을 받는 절차는 [그림 2]와 같다.

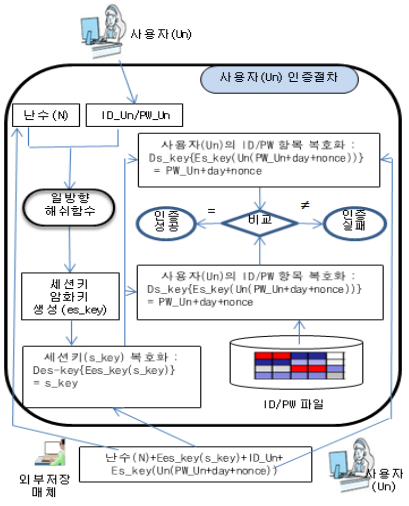

그림 2. 사용자 Un 인증 절차

[그림 2]에서 본 바와 같이 사용자 Un의 단계별 인증절차는 다음과 같다.

Step 1) 사용자 Un이 ID/PW를 입력한다.

Step 2) 외부저장매체(USB)로부터 난수 N과 step 1)에서 입력된 패스워드(PW)를 일방향 해쉬함수에 입력하여 출력물로 세션키 암호화키 es_key를 재생성한다.

Step 3) 외부저장매체(USB)로부터 암호화된 세션키 Ees_key(s_key)를 step 1)에서 재생성된 세션키 암호화키 es_key를 사용하여 복호화 한다.
⇒ Des_key{Ees_key(s_key)} = s_key

Step 4) 외부저장매체(USB)로부터 암호화된 사용자 Un의 인증정보를 Step 3)에서 복호화된 s_key로 복호화한다.
⇒ Ds_key{Es_key(Un(PW_Un+day+nonce))}
= PW_Un+day+nonce

Step 5) ID/PW파일로부터 Un의 인증정보를 Step 3)에서 복호화된 s_key로 복호화한다.
⇒ Ds_key{Es_key(Un(PW_Un+day+nonce))}
= PW_Un+day+nonce

Step 6) Step 4)와 Step 5)에서 복호화된 인증정보를 비교하여 동일하면 인증에 성공하고 다르면 인증에 실패한다.

3. 인증에 성공한 사용자의 인증정보 재구성 절차

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

[그림 3]에서 본 바와 같이 단계별 인증정보 재구성 절차를 살펴보면 다음과 같다.

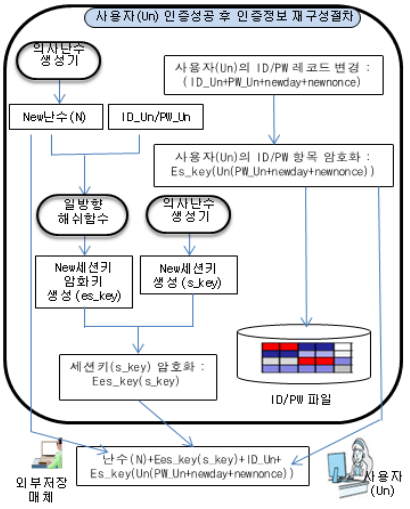

그림 3. 사용자 Un의 인증정보 재구성 절차

Step 1) 제안 시스템은 의사난수 생성기를 통해서 새로운 난수 N을 생성한다.

Step 2) 입력된 패스워드 PW_Un과 생성된 새로운 난수 N을 일방향 해쉬함수에 입력하여 출력물로 하나의 키 es_key를 생성한다. 이 키는 한 세션에서만 인증정보를 보호하기 위해 사용하는 세션키(s-key)를 보호하기 위한 키이다.

Step 3) 의사난수 생성기를 사용하여 등록 세션에서 인증정보를 보호하기 위한 새로운 세션키(s-key)를 생성한다.

Step 4) 사용자 Un의 인증정보를 ID/PW파일에 저장하기 위해 사용자 Un의 인증정보레코드를 변경한다. 즉, 이 기존의 날짜를 세션이 이루어진 날짜로 변경하고, 기존의 nonce값을 새로운 nonce값으로 변경한다.

Step 5) Step 2)에서 만들어진 새로운 es-key로 새롭게 만들어진 세션키(s-key) 노출을 방지하기 위해 새로운 s_key를 암호화 한다.

⇒ Ees_key(s-key)

Step 6) Step 4)에서 변경된 Un의 인증정보 레코드 노출을 방지하기 위해 Step 3)에서 만들어진 s_key로 Un의 레코드를 암호화한다.
⇒ Es_key(Un(PW_Un+day+nonce))

Step 7) Step 6)에서 인증정보가 암호화된 Un의 레코드(Es_key(Un(PW_Un+day+nonce)))를 시스템 ID/PW파일에 저장한다.

Step 8) Step 1)에서 생성된 새로운 난수 N, Step 5)에서 암호화된 새로운 Ees_key(s_key), Step 6)에서 변경된 인증정보가 암호화된 Un의 레코드(Es_key (Un (PW_Un+day+nonce))를 모두 외부정장매체(USB)에 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 사용자 인증이 필요한 모든 시스템에서 인증의 안전성을 확보하고 저비용으로 사용할 수 있도록 고안되었다. 따라서, 제안시스템이 기존의 사용자 인증 방법과 비교하여 우수한 안전성 및 활용의 수월성을 객관적으로 제시할 필요가 있다.

본 장에서는 기존 시스템에서 사용되고 있는 기본적인 ID/PW 사용자 인증 방법, 인증서를 통한 사용자 인증 방법, 지문을 활용한 사용자 인증 방법, 보안카드 및 OTP를 활용한 사용자 인증 방법 등과 비교하였다.

표 2. 기존 인증방법과 제안 인증방법 비교분석

	ID/PW	인증서	지문	OTP	제안 방안
특성	정적	정적	정적	동적	동적
PW 변경	필요	필요	-	불필요	불필요
재사용	가능	가능	가능	불가 (1회 사용)	불가 (1회 사용)
인증 요소	사용자 소유정보	사용자 소유정보	사용자 소유정보	사용자 매체를 통한 정보	사용자 소유정보⊕사용자매체정보
휴대성	높음	보통	높음	보통	높음
구축 비용	저비용	고비용	고비용	고비용	저비용
위변조 가능성	높음	낮음	낮음	낮음	낮음
보안 강도	하	상	상	상	상

[표 2]에서 살펴본 바와 같이 다른 인증 방법에 비해 반복적인 패스워드의 변경이 요구되지 않고, 패스워드가 노출되더라도 해당 세션에서만 사용되는 1회성이므로 재사용할 수 없고, 암호화 되어 저장되므로 위변조 가능성이 적으면서도 보안성이 뛰어남을 알 수 있다. 또한, 저렴한 이동형 저장매체를 활용할 수 있으므로 휴대성 및 구축비용이 적게 드는 장점이 있음을 알 수 있다.

제안한 인증방법은 설치가 간편하다는 경제성과 휴대성, 사용의 간편성, 강화된 보안 등의 이유로 다양한 분야에 적용가능하다. 전자적 해킹 위협의 증가로 강한 인증을 필요로 하는 금융, 전자정부, 게임, 포털사이트 등에 적용할 수 있다.

V. 결 론

본 논문에서는 기존 ID/PW기반의 사용자 식별 및 인증방식에서 발생할 수 있는 ID/PW 노출로 인한 위험성에 대한 해결 방안으로 이동 저장매체를 활용한 패스워드 기반 사용자 인증 강화 방안을 제시하였다. 즉, 이동형 저장매체에 암호화된 사용자 인증정보를 저장하고, 필요시 이동형 저장매체의 정보를 사용할 수 있도록 설계하였다.

향후 이동형 저장매체를 활용함으로 인해 발생할 수 있는 분실위험과 추가적인 공격 가능성을 고려하여 보다 안전하고 효율적으로 저장할 수 있는 매커니즘에 대한 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] 이형우, “안전한 로그인을 위한 소프트 보안카드 기반 다중 인증 시스템”, 한국콘텐츠학회논문지, 제9권, 제3호, 2009.

[4] 홍우찬, 이광우, 김승주, 원동호, “PC에 탑재된 OTP의 취약점 분석”, 정보처리학회논문지C, 제17-C권, 제4호, 2010(8).

[5] 문순환, 김신홍, 노광현, “홍채 정보 기반 마우스를 활용한 사용자 인증 시스템”, 한국콘텐츠학회논문지, 제6권, 제1호, 2006.

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

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

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

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

[10] “One Time Password Authentication for Open High Performance Computing Environments,” http://www.doegrids.org

[11] 히로시 유키, *알기쉬운 정보보호개론 : 흥미로운 암호기술의 세계,* 인피니트북스, 2012.

저 자 소 개

김 선 영(Sun-Young Kim) 정회원

- 1999년 2월 : 배재대학교 컴퓨터공학과 졸업
- 2001년 2월 : 배재대학교 컴퓨터공학과 석사
- 2013년 2월 : 배재대학교 컴퓨터공학과 박사
- 1991년 2월 ~ 현재 : 법무부치료감호소

<관심분야> : 정보보호, 포렌식, 모바일 보안

김 선 주(Sun-Joo Kim) 정회원

- 1998년 2월 : 배재대학교 컴퓨터공학과 졸업
- 2001년 2월 : 배재대학교 컴퓨터공학과 석사
- 2013년 2월 : 배재대학교 컴퓨터공학과 박사
- 2001년 1월 ~ 2003년 9월 : ㈜케이사인 선임연구원
- 2013년 9월 ~ 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