https://doi.org/10.5392/JKCA.2017.17.07.276

USB 장치 정보를 이용한 사용자 인증방안

User Authentication System Using USB Device Information

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

Jin-Hae Lee(ljh1852@pcu.ac.kr)*, In-June Jo(injune@pcu.ac.kr)*,
Seon-Joo Kim(sunjoo@tta.or.kr)**

요약

ID/PW(Identifier/Password) 인증방식은 다양한 보안취약성이 존재함에도 사용이 편리하고 구축비용이 저렴하여 아직까지 폭 넓게 사용하고 있으며, 유추해내기 어려운 복잡한 패스워드의 사용과 주기적인 변경을 요구하고 있다. 하지만 사용자 입장에서는 복잡한 패스워드를 기억하고 주기적으로 변경하는 것은 매우 불편한 일이다. 이에 본 논문에서는 USB(Universal Serial Bus) 메모리를 활용하여 복잡한 패스워드를 주기적으로 변경할 필요가 없는 인증시스템을 제안하였다. 사용자 인증시마다 자동으로 재생성 되도록 하고 기존의 인증데이터는 재사용이 불가능하도록 설계하였다. 이를 바탕으로 ID/PW 인증시스템을 크게 고치지 않으면서 사용이 편리하고, 인증서 / 지문인식 수준의 보안성을 제공할 수 있다.

■ 중심어 : | 식별 및 인증 | USB 메모리 | 인증시스템 | USB 장치 설명자 | USB 컨테이너 ID |

Abstract

Password-based authentication is vulnerable because of its low cost and convenience, but it is still widely used. In order to increase the security of the password-based user authentication method, the password is changed frequently, and it is recommended to use a combination of numbers, alphabets and special characters when generating the password. However, it is difficult for users to remember passwords that are difficult to create and it is not easy to change passwords periodically. Therefore, in this paper, we implemented a user authentication system that does not require a password by using the USB memory that is commonly used. Authentication data used for authentication is protected by USB data stored in USB memory using USB device information to improve security. Also, the authentication data is one-time and reusable.Based on this, it is possible to have the same security as the password authentication system and the security level such as certificate or fingerprint recognition.

■ keyword : | Identification and Authentication | USB Memory | Authentication System | USB Device Descriptor | USB Container ID |

I. 서 론

우리나라는 공인인증서 기반의 사용자를 식별 및 인증하는 방법이 널리 사용되고 있다. 하지만 공인인증서를 사용하기 위해서는 Active-X를 설치 후 매번 복잡한 사용자 인증절차를 거쳐야 한다. 또한 공인인증서는 은행을 비롯한 쇼핑몰, 공공기관 등에서 사용자 인증을 위해서는 필수항목이다[1][2]. 공인인증서는 보안성이

* 이 논문은 2017학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 것임.
접수일자 : 2017년 04월 24일
수정일자 : 2017년 06월 12일
심사완료일 : 2017년 06월 12일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

뛰어나지만 구축 비용이 많이 들고 사용자 편리성이 많이 떨어진다. 이러한 문제점을 해결하기 위해서 FIDO, 사용자 ID를 이용한 간편 인증 방안 등이 제안되고 있다[3][4].

사용자 인증 기술은 ID/PW[5], 공인인증서[6], OTP[7], 보안카드[8], 지문인식[9] 등 다양한 기술이 있다. 먼저, ID/PW는 구축비용이 저렴하고 사용이 편리하여 다양한 보안 취약점이 있지만 아직까지도 많이 사용되고 있다[10]. ID/PW를 쉽게 유추하지 못하도록 영문자, 숫자, 특수문자를 3가지 조합하여 최소 9자 이상을 사용하며, 또한 3개월이나 6개월마다 주기적으로 패스워드를 변경하도록 요구한다. 공인인증서, OTP, 보안카드 등은 보안성이 뛰어나지만 사용성이 떨어지고 비용이 비싼 단점이 있으며 지문인식 인증방식은 편리성이 높지만 별도의 생체인식 장비가 필요한 단점이 있다.

본 논문에서는 ID/PW 기반의 인증방식의 취약점을 극복한 사용자 인증 방안을 제안한다. ID/PW 기반의 인증방식을 준용하여 ID 입력을 그대로 사용했으며 USB 메모리에 정당한 사용자임을 증명하는 인증데이터를 저장하는 방식을 사용하였다. 제안방안을 통해 패스워드 기반의 인증 방식의 취약점을 개선하였으며, 웹사이트나 응용시스템에 적은 비용으로 적용 할 수 있기 때문에 범용성으로 사용할 수 있을 것으로 기대한다.

II. 관련연구

2-1 사용자 인증 기술

사용자 인증기술은 정보시스템에서 사용자가 본인임을 주장하는 요청에 대해 해당 정보 시스템에 등록되어 있는 올바른 사용자임을 증명하는 것이다. 사용자 인증기술은 이용정보에 따라 지식기반, 소유기반, 생체기반으로 구분되며, 다음과 같은 특징이 있다.

지식기반 사용자 인증방식은 사용자와 서버간의 미리 공유된 비밀정보(패스워드)를 기반으로 하여 올바른 사용자인지를 확인하는 방식이다. 별도의 H/W가 필요 없고 구축 및 운영비용이 적게 들지만, 제 3자가 쉽게 유추하거나 도용 될 수 있다.

소유기반 사용자인증은 사용자가 소유하고 지니고 있는 정보(인증토큰)를 이용하여 사용자를 인증하는 방식이다. 인증토큰을 항상 소유하고 있으므로 보안성이 높지만 구축 및 운영비용이 비싸고 항상 인증토큰을 지니고 다녀야 한다는 단점이 있다.

생체기반 인증은 사용자의 생체 정보나 행동 정보를 이용하여 사용자를 인증하는 방식이다. 사용자가 별도로 보안토큰을 소지하지 않아도 되고, 기억해야할 정보도 없어서 편리하고, 보안성이 뛰어나다. 하지만 생체인식 시스템 구축비용이 비싸고, 생체정보가 비밀성과 무결성이 손상되거나 노출되었을 경우 매우 치명적인 보안 취약점을 갖게 된다[11].

2-2 USB 메모리

파일 이동이나 파일 보관 용도인 USB 메모리는 작고 가벼운 휴대성과 저렴한 가격 때문에 널리 사용 된다.

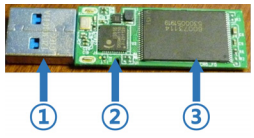

그림 1. USB 메모리 구조

[그림 1]은 USB 메모리의 구조를 표시한 것으로 ① USB 커넥터, ②컨트롤러, ③플래시메모리로 구분된다. ①USB 커넥터는 PC나 다양한 IT기기의 USB포트에 연결되어 데이터 전송을 한다. ②컨트롤러는 플래시 메모리와 USB 커넥터 사이에서 데이터 전송을 제어한다. ③플래시 메모리는 데이터를 저장하는 반도체 장치로 전원이 차단되어도 데이터를 보관할 수 있다. 이처럼 USB 커넥터, 컨트롤러, 플래시 메모리를 결합한 장치를 USB 플래시 메모리 (이하 USB 메모리)라고 한다[12].

2-3 USB 디바이스 디스크립터

USB 디스크립터는 USB제조사, 일련번호, USB 장치 타입, 장치 정보 등이 포함되어 있다[13]. [그림 2]는

USB 디스크립터의 정보를 확인할 수 있으며, ②번 문자열에 제조사(Sandisk), 장치 시리얼번호 등의 값을 확인할 수 있다.

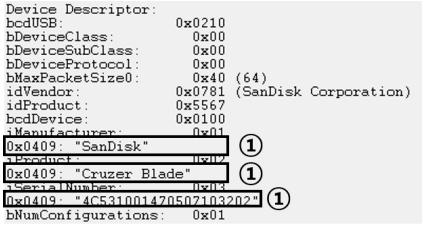

그림 2. USB 디바이스 디스크립터

2-4 USB 컨테이너 ID

USB 메모리가 PC와 연결되면 PnP관리자는 USB 메모리 장치의 드라이버를 설치하고, 해당 USB 메모리 장치를 저장매체로 마운트 시킨 후 USB 메모리 정보를 레지스트리에 기록한다. 이때, USB 레지스트리에 저장되는 USB 메모리 관련 정보 즉, 장치 클래스 ID, 고유 인스턴스 ID, 제조사 ID와 제품 ID, 볼륨 시리얼 번호 등을 활용하여 운영체제에서 사용할 수 있는 문자열 형태의 USB 컨테이너 ID를 생성하여 사용한다[14]. 아래 그림 [그림 3]은 USB 메모리 장치를 PC에 연결 했을 때 생성되는 USB 컨테이너 ID 값이다.

그림 3. USB 컨테이너 ID

Ⅲ. 제안시스템 개요

본 논문에서는 USB 메모리 정보(USB 디스크립터, USB 컨테이너 ID)를 이용하여 패스워드를 기억하지 않아도 되는 새로운 인증방안을 제안하였다. 제안시스템은 인증정보 생성 모듈, 사용자 인증모듈, 인증정보 재생성 모듈로 구성된다.

3.1 인증정보 생성

사용자 ID와 USB 메모리를 이용한 사용자 인증정보 생성절차는 다음과 같다.

그림 4. 인증정보 생성 절차

① 난수발생기를 통해 난수(RN)을 생성 후 사용자 ID, 디바이스 디스크립터를 조합 후 해시하여 세션키암호화키(SEKey)를 생성한다.
② 난수발생기를 통해 세션키(SKey)를 생성한다.
③ 디바이스 디스크립터와 컨테이너 ID를 해시하여 사용자 인증데이터 암호화키(AEKey)를 생성한다.
④ 타임스탬프, 컨테이너 ID, 난수값을 이용하여 인증시 필요한 사용자인증데이터(AuthInfo)를 생성

하고, 세션키(SKEY)로 암호화된 사용자인증데이터(E_AuthInfo)를 한다.

⑤ 세션키암호화키(SEKey)로 세션키(SKEY)를 이용하여 암호화 한다.

⑥ ④에서 암호화 되지 않은 사용자인증정보(AuthInfo)를 해시값으로 변환 후 Database에 저장된다.

⑦ USB메모리에 저장할 인증데이터를 암호화된 인증정보(E_AuthInfo), 암호화된 세션키(E_SKey), 난수(RN)를 조합하여 생성한다. 생성된 인증데이터는 인증데이터암호화키(AEKey)를 이용하여 암호화 한 후 사용자의 USB 메모리에 저장한다.

3.2 사용자 인증

사용자 ID, USB 장치 정보, USB 메모리에 저장된 암호화된 인증데이터를 이용하여 사용자 인증을 진행한다. 절차는 다음과 같다.

① 사용자의 USB메모리로 부터 디바이스 디스크립터, 컨테이너 ID와 암호화된 인증데이터(E_AuthData)를 읽어 온다. 디바이스 디스크립터와 컨테이너 ID를 이용하여 인증데이터 암호화키를 생성 후 암호화된 인증데이터를 복호화 한다.

② 사용자의 ID와, 디바이스 디스크립터, 인증데이터로부터 얻은 난수를 해시함수를 이용하여 세션키 암호화키를 생성한다.

③ 세션키 암호화키를 이용하여 암호화된 세션키를 복호화 후 암호화된 인증정보를 복호화 한다.

④ 데이터베이스로부터 저장된 인증정보와 복호화된 인증정보를 비교함으로써 사용자 인증을 수행한다.

⑤ ④에서 사용자 인증에 성공하면 인증정보 재생성 절차를 진행하고, 사용자 인증에 실패하면 사용자 인증을 종료한다.

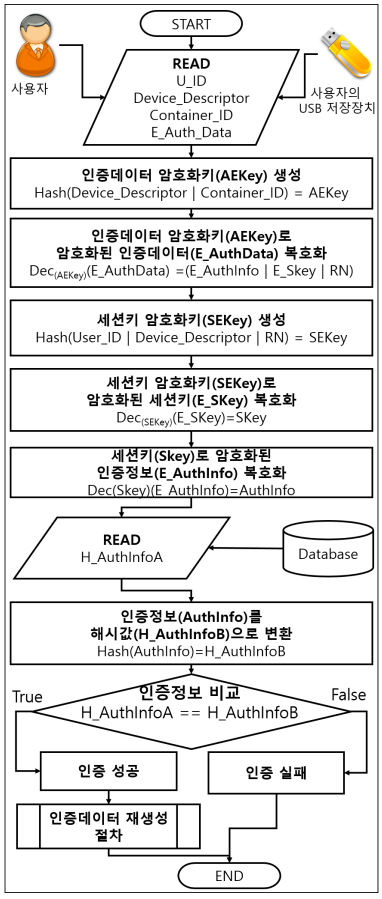

그림 5. 인증데이터 복호화 및 인증

3.3 인증정보 재생성

인증정보 재생성 과정은 사용자 인증이 성공했을 때 이루어지는 과정으로, 기존에 사용된 인증정보를 폐기하고 새로운 인증정보를 생성하는 과정이다.

① PRNG를 이용하여 새로운 난수(NRN)을 생성하여 사용자 ID, 디바이스 디스크립터를 해시함수를 사용하여 세션키암호화키(SEKey)를 생성한다.

② PRNG를 이용하여 새로운세션키(NSKey)를 생성한다.

③ 디바이스 디스크립터와 컨테이너ID를 해시함수를 사용하여 인증데이터 암호화키(AEKey)를 생성한다.

④ 타임스탬프, 컨테이너 ID, NARN을 이용하여 인증 시 필요한 인증데이터를 생성한다. 생성된 인

증정보는 세션키(SKEY)로 암호화 한다.

⑤ 세션키(SKEY)는 세션키암호화키(SEKey)를 이용하여 암호화를 한다.

⑥ 암호화 되지 않은 인증정보는 해시값으로 변환하여 Database에 저장된다.

⑦ 암호화된 인증정보(E_AuthInfo), 암호화된 세션키(E_SKey), 난수(NRN)를 조합하여 생성 후 인증데이터는 인증데이터 암호화키(AEKey)로 암호화하여 사용자가 소유한 USB메모리에 저장한다.

그림 6. 인증데이터 및 인증정보 재생성

Ⅳ. 고찰

제안 시스템은 ID/PW방식에서 패스워드를 입력 받지 않고 USB 메모리에 저장된 인증데이터를 활용하여 편의성을 높였다. 또한 USB 메모리 정보를 이용하여 인증데이터를 암호화 하여 다른 USB 메모리에서 사용이 불가능하도록 하여 보안성을 높였다. 시스템 구축비용 역시 낮출 수 있으며 사용자가 편리하게 사용할 수 있도록 고안되었다. 이를 위해 기존의 여러 가지 사용자 인증 방법과 비교하여 제안 시스템의 장점을 객관적으로 제시하였다.

표 1. 타 인증시스템 비교

	ID/PW	OTP	지문인식	인증서	제안시스템
사용성	높음	낮음	높음	낮음	보통
특성	정적	동적	정적	정적	동적
PW 변경여부	필요	불필요	불가능	필요	불필요
인증정보 재사용 여부	가능	불가능	가능	가능	불가능
인증 요소	사용자 지식 정보	사용자 매체 정보	사용자 소유정보	사용자 소유 정보	사용자 소유 정보 + 사용자 매체 정보
휴대성	높음	보통	높음	보통	보통
보안강도	하	상	상	상	중
구축비용	저비용	고비용	고비용	고비용	저비용

다음 [표 1]에서 살펴본 바와 같이 제안 시스템은 사용성 면에서 USB 메모리를 연결한 후 패스워드를 직접 입력하지 않고 인증이 가능하게 때문에 인증이 간편하다. 또한 패스워드를 변경할 필요가 없고 숫자, 알파벳, 특수문자를 고려하여 복잡한 패스워드를 생성할 필요가 없기 때문에 패스워드 관리가 필요 없는 장점이 있다. 또한 인증데이터는 1회만 사용되며 인증 후 재생성되어 기존의 인증데이터는 재사용이 불가능 하도록 설계 하였다. 인증데이터는 USB 장치 정보로 암호화되기 때문에 다른 USB에서 사용 할 수 없는 장점을 가지고 있다. 인증요소로써 USB 장치 정보와 USB 메모리에 저장된 인증데이터 2가지를 사용하여 보안성을 향상시켰다. 휴대성 면에서 OTP는 별도의 단말기를 소유해

야 하지만 제안시스템은 흔히 가지고 다니는 USB 메모리를 바로 활용 할 수 장점이 있다. 구축비용면에서 기존의 ID/PW기반 인증 시스템에 적용이 가능하기 때문에 타 인증시스템보다 저렴하게 구축이 가능하고 ID/PW기반 인증방식보다 보안성이 향상된 인증 시스템을 적용할 수 있다.

V. 결론 및 향후 연구

본 논문에서는 패스워드 기반의 인증방식의 패스워드 노출과 사용자에게 불편을 안겨주는 패스워드 관리의 해결방안 제시하였다. 제안 시스템은 패스워드 필요 없이 ID를 입력하고 몇 번의 클릭 과정만 거치면 바로 인증이 가능하기 때문에 패스워드 인증방식과 사용성 면에서 비교해 봤을 때 크게 차이가 나지 않는다. 또한 패스워드를 일정한 기간을 두고 변경 할 필요가 없으며 다양한 문자열을 조합하여 기억하기 어려운 패스워드를 생성할 필요가 없다. 제안 시스템 구축 또한 패스워드 기반 인증시스템 구조를 크게 변경할 필요 없이 적용이 가능하기 때문에 타 인증 시스템에 비해 구축비용이 저렴한 장점이 있다. 또한 인증데이터는 1회성으로 재사용이 불가능하고 USB 장치 정보를 이용하여 암호화했기 때문에 다른 USB에서 사용이 불가능하다. 따라서 제안 시스템은 패스워드 기반 사용자 인증 방식을 사용하는 웹사이트, 기업 업무시스템, 학교 전산 시스템에서 사용자 인증방안으로 활용이 가능할 것으로 사료된다.

향후 연구 방향으로 USB메모리 분실 시 발생할 수 있는 문제점을 보완할 수 있는 방안을 연구해야 할 것이다.

참 고 문 헌

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

[2] 전자 서명법[법률 제1008호, 2010.02.04. 시행]

[3] 김선주, 조인준, "사용자 ID만을 활용한 간편한 사용자 인증방안," 한국콘텐츠학회논문지, 제15권, 제11호, pp.501-508, 2015.

[4] 김선영, 김선주, 조인준, "이동 저장매체를 활용한 패스워드 기반 사용자 인증 강화 방안," 한국콘텐츠학회논문지, 제14권, 제11호, pp.533-540, 2014.

[5] 김영수, 나중찬, 손승원, "패스워드 인증프로토콜 동향," 전자통신동향분석, 제16권, 제6호, 2001.

[6] 김선주, 조인준, "OTP를 이용한 PKI 기반의 개인키 파일의 안전한 관리방안," 한국콘텐츠학회논문지, 제14권, 제12호, pp.565-573, 2014.

[7] 최동현, 김승주, 원동호, "일회용패스워드(OTP: One-Time Password) 기술 분석 및 표준화 동향," 정보보호학회지, 제17권, 제3호, pp.12-17 2007.

[8] 이형우, "안전한 로그인을 위한 소프트 보안카드 기반 다중 인증 시스템," 한국콘텐츠학회논문지, 제9권, 제3호, pp.28-38, 2009.

[9] 김학일, 한영찬, "[특집]지문인식 호환을 위한 국제 표준화 동향," 전자공학회지, 제33권, 제1호, pp.17-35, 2006

[10] 조상래, 최대선, 진승헌, 이형효, "패스워드 없는 인증기술-FIDO," 한국전자통신연구원, 2014

[11] 생체인증 보안문제 없나 유출되면 대체불가, http://www.yonhapnews.co.kr, 2016.08.14

[12] USB 메모리, http://it.donga.com/3966/

[13] USB Descriptor, http://www.beyondlogic.org/

[14] "Container ID. MSDN, https://msdn.microsoft.com

저 자 소 개

이 진 해(Jin-Hae Lee) 준회원

- 2015년 2월 : 배재대학교 컴퓨터공학 학사
- 2015년 3월 ~ 현재 : 배재대학교 사이버보안학과 석사 과정

<관심분야> : 소프트웨어 개발, 암호학, 정보보안

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

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 수석연구원

<관심분야> : 클라우드 컴퓨팅, SW테스팅, 정보보호제품 CC 평가