FIDO 인증 기반의 웹서비스 간편 사용자 인증 설계

김현주*, 문상국**
*단국대학교 대학원 전자전기공학과 컴퓨터응용전공
e-mail: *chopinkhj@gmail.com
**동국대학교 대학원 경영정보학과 정보전략전공

Web Service Simple User Authentication Design Based on FIDO Authentication

Hyun-Joo Kim*, Sang-Guk Moon**
*Dept of Electronic & Electrical Engineering Graduate School Dankook University.
**Dept of Management & Information System Graduate School Dongguk University.

요약

기존의 웹서비스 접속 방법에는 전통적인 ID/PW(Identification/Password) 방식, OTP(One-Time Password), 공동인증서, 지문인식 등의 기술이 사용되고 있다. 특히 ID/PW 방식을 사용하는 사용자는 동일한 ID/PW를 대부분의 웹서비스에 사용하고 있다. 이는 개인의 ID/PW가 노출되면 개인이 사용하는 대부분의 웹서비스의 ID/PW가 노출됨과 동일하다고 볼 수 있다. 그러므로 웹서비스 운영자들은 영문자, 숫자, 특수문자 등을 조합하여 복잡한 패스워드를 사용을 권장하고 주기적으로 패스워드를 변경하도록 웹서비스 시스템을 구성한다. 최근 부각 되는 사용자 인증 기술이 FIDO(Fast Identity Online) 간편 인증 기술이다. 본 논문에서는 FIDO 기반의 사용자 인증 기술을 이용하여 대학 정보시스템에서 간편 사용자 인증을 설계한다. FIDO2.0은 웹 브라우저를 기반하므로 사용의 편리성과 잦은 암호 변경과 암호 설정의 한계로 인한 불편함을 해소해준다.

1. 서 론

기존의 웹서비스 접속 방법에는 전통적인 ID/PW(Identification/Password) 방식, OTP(One-Time Password), 공동인증서, 지문인식 등의 기술이 사용되고 있다. 특히 ID/PW 방식을 사용하는 사용자는 동일한 ID/PW를 대부분의 웹서비스에 사용하고 있다. 이는 개인의 ID/PW가 노출되면 개인이 사용하는 대부분의 웹서비스의 ID/PW가 노출됨과 동일하다고 볼 수 있다. 그러므로 웹서비스 운영자들은 영문자, 숫자, 특수문자 등을 조합하여 복잡한 패스워드를 사용을 권장하고 주기적으로 패스워드를 변경하도록 웹서비스 시스템을 구성한다. 또한, 이를 불편해하는 사용자는 공동인증서를 사용하거나 웹 지문인식을 사용하기도 한다. 그러나 공동인증서는 액티브X 프로그램을 설치해야 하고 복잡한 사용자 인증 절차의 불편함이 있다[1-2]. 공동인증서는 공개키 기반의 전자서명으로 개인이 보관하고 있는 비밀키(Private Key)와 누구나 알 수 있게 공개하는 공개키(PublicKey)로 구성된다. 공인인증기관은 공개되어 있는 공개키와 개인 소유의 비밀키를 공인인증서의 형태로 발급하여 사용되므로 비교적 안정성을 보장되므로 많은 사용자들이 공동인증서를 사용하고 있다. 그러나 공동인증서는 별도의 물리적 장치에 공동인증서를 보관하거나 주기적으로 공동인증서를 재발급받아야 하는 등의 불편함으로 사용자의 편의성을 저하시킨다.

최근 부각 되는 사용자 인증 기술이 FIDO(Fast Identity Online) 간편 인증 기술이다. FIDO는 비밀번호의 문제점을 해결하기 위해 FIDO 얼라이언스에 의해 제안된 사용자 인증 프레임워크다. FIDO Specification은 비밀번호 없이 인증을 하기 위한 Universal Authentication Framework(UAF) 프로토콜과 비밀번호를 보완해서 인증을 하기 위한 Universal 2nd Factor(U2F) 프로토콜로 구성되며 지문, 홍채 등 생체인증을 적용하기 위해 주로 사용된다. FIDO 인증 기술 개발로 다양한 생체 인증이 사용되고 있다[3].

본 논문에서는 FIDO 기반의 사용자 인증 기술을 이용하여 대학 정보시스템에서 간편 사용자 인

증을 설계한다. 기존 대학의 정보시스템은 전형적으로 ID/PW를 인증하여 사용자 인증이 사용되었다. 이는 기존 정보시스템에서 제약 없이 가장 손쉽게 구현이 가능하고 추가적인 소요 비용에 대한 부담이 적어서 범용적인 사용하기가 이롭기 때문이다. FIDO 기반의 사용자 인증은 현재의 ID/PW 방식 대신 지문 인식, 홍채 인식 혹은 얼굴 인식 등 다양한 생체 인식 기반의 새로운 인증시스템으로 인증 프로토콜과 인증수단을 분리하여 보안과 편리성이 높다는 평가를 받고 있는 신기술이다.

본 논문에서는 기존 대학의 정보시스템은 전형적으로 ID/PW 방식의 사용자 인증을 FIDO 기반의 사용자 인증으로 대체 설계하므로 잦은 패스워드 변경으로 인한 불편함을 해소하고 간편하고 빠른 인증이 가능한 시스템 접속을 설계한다.

2. 관련 연구

2.1. 인증 개요

합법적인 정보시스템에 접근하기 위해서는 사용자는 자신이 사용자 인증으로 자신이 정당한 사용자임을 증명해야 한다. 사용자 인증 시스템이 취약할 경우 해당 시스템은 해커의 공격 대상이 될 수 있으며 기밀성, 무결성, 가용성이 침해되어 대상 정보시스템은 막대한 피해를 입게 된다[4].

2.2. 사용자 인증 기술

사용자 인증 기술 중 가장 널리 사용되는 방식은 ID/PW의 사용이다. ID/PW는 대상 사용자만이 알고 있는 정보를 사전에 정보시스템에 등록하고 정보시스템에 로그인 시 사용자가 사전에 제시한 식별자(ID, Identifier)와 패스워드(PW, Password)가 저장된 내용과 일치하면 접근을 허용하는 인증 기술이다. PKI(Public Key Infrastructure) 공개키 기반의 공동인증서 기술은 인터넷에서 전자상거래에서 안전하게 사용하고 관리하기 위한 정보보호표준 방식으로 PKI 인증서를 이용하여 전자서명과 암호화를 지원한다. 공동인증서는 개인이 보관하고 있는 비밀키(Private Key)와 누구나 알 수 있게 공개하는 공개키(PublicKey)로 구성된다. 공인인증기관은 공개되어 있는 공개키와 개인 소유의 비밀키를 공인인증서의 형태로 발급하여 사용되므로 비교적 안정성을 보장되어 현재까지 비교적 많은 사용자들이 공동인증서를 사용하고 있다. 그러나 공동인증서는 별도의 물리적 장치에 공동인증서를 보관하거나 주기적으로 공동인증서를 재발급받아야 하는 등의 불편함이 있다. 그 외에도 보안카드와 일회용 패스워드(OTP, One Time Password), 휴대폰 본인 인증, 메일 인증 등이 사용되고 있다. 이 인증 방식은 주로 2차 인증으로 사용되는데 위에 논한 ID/PW, 공동인증서와 혼합된 형태의 2차 인증으로 사용자 인증을 강화하는 방안으로 사용되고 있다[4][5].

2.3. FIDO(Fast Identity Online) 인증 기술

FIDO는 Public-Key Cryptography(공개키 암호기술)"를 적용하고 있는 대표적 기술로 타원곡선암호기술(ECC)에 속하는 ECDSA 암호알고리즘만 사용한다. FIDO는 비밀번호를 공유하여 인증하는 공유방식 인증 방식을 사람의 생체정보(지문, 얼굴모양, 홍채 등)나 외부 인증장치(Yubikey, Titan Security key 등)을 사용하는 공개키 암호기술 방식으로 편리하고 안전하게 인증 기능을 제공하는 인증(Authentication) 프로토콜 표준이다. FIDO는 생체정보뿐만 아니라, USB Security Token, Smart Card 등 기존 Hardware 기반 Protection 장치를 포함한 모든 인증(authentication) 기술을 지원하며 기존 PKI 기술을 활용한다. FIDO 인증의 3가지 표준은 다음과 같다.

가. UAF(Universal Authentication Framework): ID/PW 인증 방식 대신 개인의 고유한 생체정보를 인증 과정에 사용하며 핸드폰에서 생체정보 스캔 기능을 지원하고 모바일 환경에 적합하다.

나. U2F(Universal 2nd Factor): 기존 ID/PW 인증 방식과 함께 생체정보 또는 별도의 2차 인증 장치를 별도로 사용한다. 외부 디바이스 인증 장치를 사용하므로 기존 PC 환경에 적합하다.

다. FIDO 2.0: Web 서비스를 사용하는 환경에서 사용 가능토록 UAF 와 U2F를 통합 확장한 형태이다. FIDO 2.0은 WebAuthn 표준이 제안되었고 WebAuthn은 2019년 W3C의 Recommendation이 되었다[7-9].

2.4. 기존 웹서비스에서의 사용자 인증

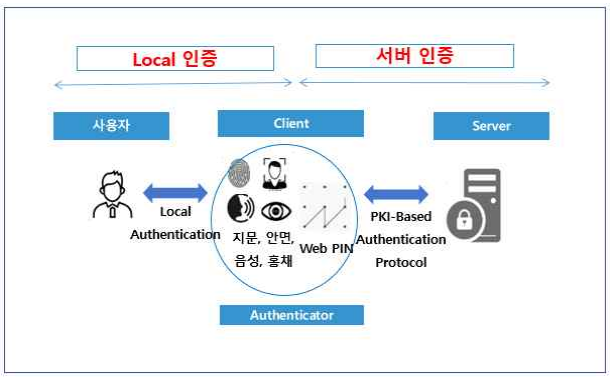
현재까지 사용되는 사용자 인증 방법은 ID/PW와 휴대폰 본인 인증이 가장 많이 사용되고 있다. 사용자 입장에서 가장 손쉽게 사용할 수 있는 방법이기 때문이다. ID/PW 방식은 코딩이 단순하고 유지 관리가 용이 하며 무엇보다 사용자 입장에서 접근이

가장 매우 용이하기에 보안에 취약하다는 단점에도 불구하고 대부분의 웹서비스 제공자가 주로 사용하고 있다. 그러나 대부분의 서비스 사용자는 많은 웹사이트의 접속 시 본인이 등록한 ID/PW를 기억하기가 쉽지 않아 한번 정한 ID/PW를 대부분의 웹서비스에 동일하게 사용하고 있다. 이는 개인의 ID/PW가 노출된다면 개인이 사용하는 대부분의 웹서비스의 ID/PW가 노출됨과 동일하다고 볼 수 있다. 그러므로 웹서비스 운영자들은 영문자, 숫자, 특수문자 등을 조합하여 복잡한 패스워드를 사용을 권장하고 주기적으로 패스워드를 변경하도록 웹서비스 시스템을 구성한다. 또한, 이를 불편해하는 사용자는 공동인증서를 사용하거나 웹 지문인식을 사용하기도 한다. 그러나 공동인증서는 액티브X 프로그램을 설치해야 하고 복잡한 사용자 인증 절차의 불편함이 있다.

3. FIDO 기반의 사용자 인증 설계

3.1. 제안시스템 개요

본 제안시스템은 대학에서 이용하는 웹서비스 정보시스템의 접속 방식을 기존의 ID/PW 방식을 개선하여 FIDO2.0 기반의 간편 인증으로 제안한다. FIDO2.0은 생체인식과 PIN 번호 설정이 가능하여 서비스를 제공받는 사용자 입장에서 한번 설정하면 별도의 인증 절차없이 정보서비스를 제공하므로 사용이 용이하며 무엇보다 모바일 환경에서 적합하여 대학 정보시스템을 이용하는 사용자에게 이롭다.



[그림 1] FIDO 기반의 사용자 인증 구조도

3.2. 제안시스템 설계

본 제안시스템은 대학의 정보시스템의 사용자 인증 로그인을 FIDO2.0 기반의 간편 인증으로 제안한다. [그림1]의 구조와 같이 사용자는 FIDO Authenticator을 이용하여 개인의 지문, 안면, 음성, 홍채 또는 pin 번호, 패턴을 이용하여 로그인 시 사용된다. 본 제안시스템에서는 이를 간편 인증이라 지칭하며 설계 과정은 다음과 같다.

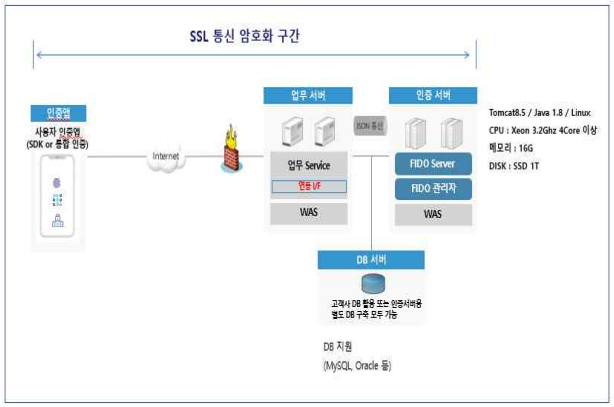
1. 정보서비스 사용자는 개인의 디바이스(휴대폰, PC, 태블릿 등)에 간편 인증 앱을 설치하고 본인의 인증 플랫폼을 설정한다.
2. 사용자가 로그인을 시도하면 간편 인증이 구동되어 FIDO 서버와 인증 검증 송수신을 시도하며 발급 코드를 요청한다.
3. FIDO 인증 서버는 사용자 인증 정보를 검증 후 발급 코드를 사용자에게 전달한다. 여기서 전송되는 전송 값은 사용자 요구에 따라 지문, 안면, 핀 번호, 패턴 등으로 사용자의 선택에 따라 전송된다. 일회용 OTP를 사용하면 OTP 값이 휴대폰 또는 이메일로 전송된다. 이때 전송되는 키는 PKI 인증 방식의 공개키를 기반한다.
4. FIDO 간편 인증 서버는 ID, 기관 코드, 발급 코드 등의 정보를 확인 후 사용자에게 접속 허가를 승인하면 로그인이 허용된다.

이 과정이 본 제안시스템에서 휴대폰에 안전하게 저장된 Private Key를 통해 서명 데이터를 생성하고 서버에서 서명 데이터의 검증을 수행하는 과정으로 FIDO2.0이 사용된다. 본 논문에서는 FIDO2.0을 이용한 간편 인증 등록, 삭제 등의 처리 과정은 제외하고 사용자 인증 부분만 논한다.

[그림 2] FIDO2.0 적용 정보서비스 서비스 흐름도

본 제안시스템의 서비스 흐름은 간편 인증 등록, 간편 인증, 간편 인증 검증, 간편 인증 삭제의 프로세스로 처리된다. 자세한 처리 프로세스 알고리

[그림 3] FIDO2.0 적용 WEB PIN 정보서비스 사용(예)



[그림4] FIDO2.0 정보서비스 구성도

즘은 추후 논하기로 한다.

4. 결 론

FIDO2.0 간편 인증은 현재의 아이디, 비밀번호 방식 대체하여 지문, 안면, 음성, 홍채 인식 등 다양한 생체 인식 기반의 새로운 인증 기술이다. FIDO2..0은 생체 인식 외에도 핀 번호, 패턴인식, 일회용 OTP 인증을 지원하고 프로토콜과 인증수단을 분리하여 보안과 편리성이 높다는 평가를 받고 있는 신기술이다. 또한 국제표준 기술로 FIDO 3가지 표준. UAF(Universal Authentication Framework), U2F(Universal 2nd Factor), FIDO 2.0을 이해하면 누구나 간단한 코딩 또는 기관 내 SSO에 연계하여 사용자 인증에 사용이 가능하다. 특히 FIDO2.0은 Web 서비스를 사용하는 환경에서 사용 가능토록 UAF 와 U2F를 통합 확장한 형태로 웹서비스를 사용하는 사용자에게 PC, 모바일 모두 용이성을 제공한다.

본 논문에서는 FIDO2.0을 이용하여 대학 내 웹 정보서비스에서 ID/PW 방식의 사용자 인증 과정에 이용하여 적용하였다. FIDO2.0은 웹 브라우져를 기반하므로 개인의 PC 브라우져가 이동되면 등록 과정을 재요청하나 모바일 환경에서는 사용의 편리성을 제공되며 무엇보다 잦은 암호 변경과 암호 설정의 한계로 인한 불편함을 해소해준다. 또한 FIDO 기술은 공개키 PKI 기반 기술이 이용하므로 휴대성과 비용 지불로 인한 공동인증서를 대체 할 수 있을 것으로 예상된다. 실제로 우리나라 금융권에서 FIDO 간편 인증 많이 사용되고 있다.

참고문헌

[1] J.H.LEE. “The Use and Problems of Public Certificates in a Smart Eenvironment,” Internet& Security Focus, Vol. 3, 2013.

[2] http://www.law.go.kr/법령/전자서명법 [법률 제10008호]

[3] https://ko.wikipedia.org/wiki/FIDO

[4] Yeong Su Park, Byoung Yup Lee. “User Authentication Mechanism based on Authentication Information using One-time Sessions”, Journal of The Korea Contents Association, Vol. 19 No. 7, pp. 421-426, 2019.

[5] Seon-Joo Kim. In-June Jo. “Convenient User Authentication Mechanism Using only User Identification”, The journal of the Contents Association, Vol. 15, Issue. 11, pp. 501-508, 2015. https://doi.org/10.5392/JKCA.2015.15.11.501

[6] Seon-Joo Kim, In-June Joe, “Management Method to Secure Private Key of PKI using One Time Password” Journal of The Korea Contents Association, Vol. 14 No. 12, pp. 565-573, 2014.

[7] Sang-Rae Cho et.al.,“Passwordless Authentication Technology-FIDO”, Electronics and Telecommunications Trends, 2014.

[8] Jaejung Kim, “Study on the Password-Free Certification System Using the FIDO (Fast IDentity Online)”, Communications of the Korean Institute of Information Scientists and Engineers, Vol. 33, No. 5, pp. 9-12, 2015.

[9] SuHyeong Kim, “FIDO Based PinTech Authentication Technology”, The Journal of The Korean Institute of Communication Sciences, Vol. 33, No. 2, pp. 59-65, 2016