ETRI

2014
Electronics and
Telecommunications
Trends

소프트웨어 기술동향 특집

패스워드 없는 인증기술–FIDO

Passwordless Authentication Technology-FIDO

조상래 (S.R. Cho) 인증기술연구실 책임연구원
최대선 (D.S. Choi) 인증기술연구실 실장
진승헌 (S.H. Jin) 사이버보안기반연구부 부장
이형효 (H.H. Lee) 원광대학교정보과학연구소 교수

패스워드 기반의 사용자 인증은 비용이 적게 들고 편리성 때문에 보안상 취약점이 있어도 현재까지 광범위하게 사용되고 있다. 이러한 패스워드 기반 인증의 보안 취약성을 개선하기 위해 생체 인증을 사용하거나 다중 요소 인증기술을 적용하려는 시도는 그동안 계속되어 왔다. 하지만 기술에 따라 사용자의 편리성이 떨어지거나 광범위하게 설치하기에 비용부담이 증가하여 응용서비스에 적용하기에는 무리가 있었다. FIDO(Fast IDentity Online)는 인증 프로토콜과 인증수단을 분리하여 패스워드 없이 인증강도를 높이면서 사용자의 편리성도 높이려는 시도를 하는 기술로 패스워드의 문제를 극복하여 스마트 모바일 환경에 적합한 인증기술로 활용될 수 있다.

Ⅰ. 서론

사용자가 사용하는 네트워크나 디바이스들은 눈부신 발전을 거듭하여 이제는 손안에서도 전세계에 저장된 정보를 조회할 수 있고 다른 사람들과도 자유롭게 소통할 수 있다.

IT의 급속한 발전은 정보에 대한 접근을 용이하게 한 대신에 개인정보에 대한 보안을 취약하게 한 문제가 발생하였다. 현재 사용자 정보는 인터넷 또는 웹에 산재한 다양한 서버에 분산 저장되어 유출될 가능성이 높고 예전과 달리 한 개인이 여러 디바이스를 사용하기 때문에 분실 시 중요한 정보가 유출될 가능성이 많다. 현재 대부분의 웹서비스에서 패스워드를 이용하여 사용자를 인증하고 개인정보에 대한 접근을 허용하고 있다.

하지만 패스워드는 치명적인 보안 취약성이 두 가지가 있다. 하나는 사용자들이 패스워드를 기억하기 쉽게 간단한 문자열을 이용한다는 것이고 두번째는 본인 가입한 여러 사이트에 동일한 패스워드를 사용한다는 점이다. 보안이 취약한 웹사이트에서 사용자의 패스워드가 해킹되면 연쇄적으로 다른 사이트들도 침입이 가능한 상황이 발생한다. 현재 많은 개인정보 유출 및 ID 도용은 패스워드 인증의 취약성을 활용하여 발생하고 있다.

초창기 컴퓨터나 서버에는 단일 계정이 있어서 사용자는 ID와 패스워드를 이용하여 로그인을 하였다. 하지만 이러한 패스워드 기반의 사용자 인증방식은 여러 세대가 지났지만 여전히 오늘날에도 가장 많이 사용되는 인증방식이다. 단일 디바이스에서 패스워드로 로그인하던 방식은 네트워크 환경에서도 지속적으로 사용되었고 인터넷과 웹이 등장하면서 일반 사용자들도 모두 패스워드를 이용하여 웹서비스에 로그인하여 사용하고 있다. 현재 패스워드의 사용은 웹서비스를 넘어 스마트 모바일 환경에서도 여전히 가장 많이 사용하는 인증수단이다.

패스워드는 사용하는 문자열을 충분히 어렵게 하고 재사용을 하지 않으며 주기적으로 변경하면 비용 대비 간편하면서도 자체적으로 가지고 있는 보안 취약성을 많이 감소시킬 수 있다. 문제는 사용자가 현실적으로 그렇게 관리하기가 쉽지 않다는 데 있다.

이렇게 문제가 있는 패스워드를 대체하기 위해 다양한 인증방식들이 그동안 등장하였다. 이들의 간단한 내용은 Ⅱ장에서 살펴볼 예정이다.

패스워드를 보완하기 위해 패스워드와 다른 인증요소를 결합하는 다중 요소 인증기술이 널리 보급되었는데 Ⅲ장에서 이 기술에 대해 사례를 중심으로 간략하게 알아본다. Ⅳ장에서는 패스워드를 사용하지 않고 사용자를 인증하는 FIDO(Fast IDentity Online) 기술에 대해 자세히 검토하고 Ⅴ장에서는 결론으로 FIDO를 사용하는데 필요한 고려사항을 정리한다.

Ⅱ. 인증방식의 분류

사용자 인증기능을 위해 사용되는 인증방식들은 크게 지식 기반, 소유 기반, 생체 기반으로 구분되며 각 인증방식은 사용자 편의성, 보안성 등에서 차이점을 가지고 있다.

1. 지식 기반

지식 기반(knowledge-based) 사용자 인증방식은 사용자와 서버가 미리 설정하여 공유한 비밀정보를 기반으로 사용자를 인증하며, 별도의 하드웨어가 필요 없어 적용하는데 비용이 아주 적은 점과 함께 사용자 편의성도 높은 장점을 가지고 있다. 그러나 사용의 편리성이란 장점에 반해 인증강도가 다른 방식들에 비해 낮아 보안 취약점이 가장 많이 발견되고 있는 문제점을 가지고 있다.

지식 기반 인증방식은 정적방식(shared secret)과 동적방식으로 다시 구분될 수 있다. 정적 지식 기반 인증방식은 현재 가장 널리 사용되고 있는 지식 기반 인증방

(그림 1) 지식 기반 인증

(그림 2) 하드웨어형태의 소유 기반 인증사례

식으로 사용자 회원 등록과정 등에서 사용자가 서버에 자신의 인증정보를 미리 입력하고 회원 등록과정을 정상적으로 마친 후 서비스 사용을 위한 인증과정에서 미리 설정한 인증정보를 입력하는 방식을 의미한다. 또한 사용자가 비밀번호를 기억해 내지 못할 경우(fall-back)를 대비하여 설정한 힌트 정보도 정적 지식 기반 인증방식으로 분류된다((그림 1) 참조).

동적 지식 기반 인증방식은 사용자의 신원을 확인하는 지식 기반 인증방식 중 가장 높은 검증강도를 제공하는 방식이다. 이 방식에서는 사용자와 서버 간 사전접촉 없이 질문을 통해 사용자의 신원을 확인하게 된다. 즉, 서버는 사용자에 대한 공개된 정보, 수집된 마케팅 데이터 또는 신용보고정보 등을 이용하여 즉석에서 질문을 사용자에게 제시하는 방식이다.

패스워드 인증은 지식 기반 인증의 한 종류이며 많은 종류의 시스템들이 패스워드를 기반으로 사용자를 인증하기 대문에 타인에게 노출 시 바로 시스템 보안이 무력화되는 단점이 있다.

2. 소유 기반

소유 기반 사용자 인증방식은 인증토큰을 소유하고, 이를 기반으로 사용자를 인증하는 방식을 말한다. 소유 기반 사용자 인증방식은 사용자가 토큰을 소유하고 있어야 하기 때문에, 지식 기반(knowledge-based) 방식의 인증방법보다 보안성이 높다. 그러나 인증시스템 구축이 어렵고, 사용자가 서비스 신청을 위해 CA(Certification Authority) 또는 RA(Registration Authority)와 최소 1번의 대면으로 본인 확인이 필요하며, 늘 소유하고 있어야 하기 때문에 편리성이 낮다는 단점이 있다.

토큰의 구성방식은 하드웨어 형태와 소프트웨어 형태 두 가지로 분류할 수 있다. 먼저 하드웨어 형태의 토큰은 OTP(One Time Password) 단말기를 예로 들 수 있다. 하드웨어 형태의 토큰은 사용자가 물리적인 형태의 토큰을 소유를 하고 있어야 하기 때문에 휴대성과 편리성이 낮다.

소프트웨어 형태의 토큰은 공인인증서(X.509)를 예로 들 수 있다. 하드웨어 형태의 휴대성과 편리성이 낮은 단점을 보완할 수가 있지만, 논리적인 형태로 저장매체에 저장이 되어 있어서 유출의 위험이 높은 단점을 가지고 있다((그림 2) 참조).

3. 생체 기반

생체 기반 인증방식은 사용자가 가지고 있는 고유한 형태의 신체구조 또는 사용자가 신체를 이용하여 행동했을 때 나타나는 행동결과를 기반으로 사용자를 인증하는 방법이다. 사용자가 특별하게 별도의 인증토큰을 소유하지 않아도 되고, 별도로 알고 있어야 할 정보도 없기 때문에 편리성이 높으며, 사용자 본인 신체의 고유

(그림 3) 다양한 종류의 생체인증 기기들

한 정보들을 사용하기 때문에 보안성이 높다. 그러나 시스템 구축 및 관리가 힘든 단점이 있다. 생체구조를 활용한 특징들을 이용하여 시스템을 구축하려면, 생체구조로부터 일련의 패턴을 분석해야 하는데 이를 위한 연구가 어려우며, 패턴화한 정보를 활용하기 위한 시스템을 구축하는데 많은 비용이 소비된다. 또한 사용자의 쉽게 변경할 수 없는 고유한 형태의 생체구조를 사용하기 때문에 사용자의 고유 생체정보에 대한 패턴값의 비밀성(Confidentiality)과 무결성(Integrity)이 훼손되었을 경우에는 큰 문제가 발생할 수가 있다.

생체 기반 인증수단은 사용자 신체구조를 활용한 생체적 특징방식과 사용자가 신체를 활용하여 어떠한 행위를 하였을 때 도출되는 정보들을 활용한 행동적 특징방식 이렇게 두 가지로 나뉜다. 먼저 생체적 특징 방식은 얼굴인식, 홍채인식, 지문인식, 정맥인식, 심박도, 심전도인식 등이 있다. 행동적 특징방식은 목소리인식, 타이핑리듬인식, 서명패턴인식, 서명압력인식 등이 있다((그림 3) 참조).

Ⅲ. 다중 요소 인증기술

1. 개요

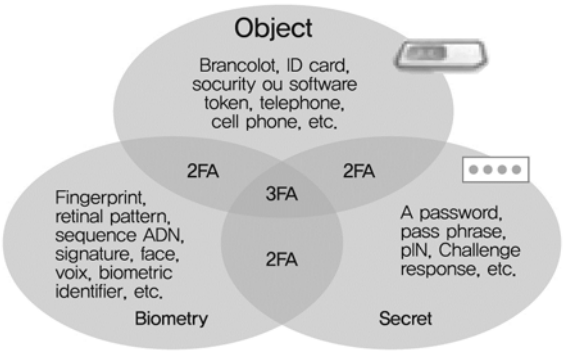
Ⅰ장에서 언급한 바와 같이 일반적으로 사용자를 인증하는 방식은 사용자가 특별한 정보를 알고 있는지를 확인하는 지식요소(knowledge factor, something the user knows, secret), 사용자가 특별한 하드웨어를 가지고 있는지를 확인하는 소유요소(possession factor, something the user has, object), 사용자가 생체적으로 특별한 특성을 보유하고 있는지를 확인하는 내재요소(inherence factor, something the user is, biometry) 등으로 구분된다.

다중 요소 인증(multi-factor authentication)이란 2가지 이상의 인증요소로 인증하는 방식을 의미한다. 즉, 2가지 이상의 인증요소로 본인 여부를 판단하는 것으로 패스워드와 같이 자신이 알고 있는 것과 하드웨어 토큰이나 바이오 메트릭스(Biometrics)와 같이 자신이 소유하고 있는 것을 동시에 이용하여 인증하는 방식이다. 따라서 다중요소 인증은 단일 요소만을 이용한 인증방식보다 강화된 인증서비스를 제공할 수 있는 장점을 제공할 수 있게 된다((그림 4) 참조).

다중 요소 인증은 위와 같은 3가지 인증방식에서 서로 다른 2가지 이상의 인증방식을 이용하여 사용자의 신원을 확인하는 과정을 의미하며, 동일한 방식의 인증기법을 2가지 이상 이용하는 경우는 다중 요소 인증에 해당되지 않는다. 강력한 인증(strong authentication)은 인증 대상 사용자에게 여러 개의 시험 데이터(challenge)를 전달하고 그에 대한 응답(response)을 기준으로 인증여부를 판단하는데 이 때 전달되는 여러 개의 시험 데이터의 종류가 지식요소, 소유요소, 내재요소 중 한 종류에 해당되는 경우 다중 요소 인증으로 분류되지 않는다.

그러나 다중 요소 인증방식이 사용자 신분을 위장하려는 공격자의 위협을 감소시키는 장점이 있지만, 이 방식도 중간사용자 공격(MITM: Main-in-the-Middle)이나 MITB(Man-in-the-Browser) 공격에 취약점을 가지고 있다.

다중 요소 인증이 단일 요소 인증에 비해 보안강도가 향상되는 장점이 있지만 다중요소 인증에서 채택하는 각 인증기술의 안전성도 고려되어야 한다. 예를 들어 다중 요소 인증에 사용되는 인증방식의 안전강도, 하드웨어 인증을 이용한 인증방식의 경우 해당 하드웨어와 비



(그림 4) 다중요소 인증

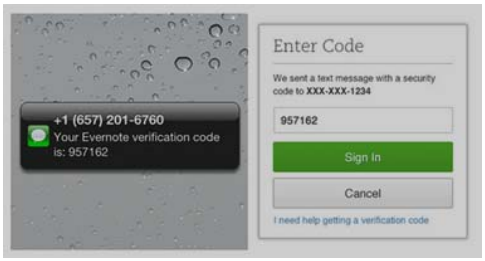
밀번호가 적법한 사용자에게 안전하게 전달되는지에 대한 관리, 사용자 인증정보를 알아내기 위한 인증시도를 능동적으로 판단하고 대처하는 방법들도 함께 고려되어야 한다.

2. 다중 요소 인증사례

가. 패스워드+휴대폰(2 Factor)

일반적으로 패스워드와 휴대폰을 이용한 2단계 인증으로는 패스워드+휴대폰 인증코드방식이 많이 활용되고 있다. 먼저 사용자가 패스워드로 인증 후, 휴대폰 통신사와 주민번호, 전화번호를 입력하면, 해당 정보가 맞을 경우에 임의의 인증코드가 해당 휴대폰으로 전송이 된 뒤, 이를 인증코드 창에 입력하여 최종 인증을 하는 절차이다((그림 5) 참조).

계정에 맞는 비밀번호를 알고, 사용자의 휴대폰번호, 통신사, 주민등록번호를 아는 것은 모두 지식요소에 속



(그림 5) 에버노트에서의 패스워드+휴대폰 인증

(그림 6) ATM

(그림 7) OTP와 보안카드

하기 때문에 다중요소 인증이 아닌 강력한 인증에 해당된다. 그러나 여기에 휴대폰을 소유해야만 확인할 수 있도록 인증번호를 메시지로 알려주는 것은 소유요소에 속하기 때문에 다중 요소 인증방식이라고 할 수 있다.

나. 패스워드+체크카드(2 Factor)

흔히 볼 수 있는 방식으로, 주로 은행 ATM 업무에서 볼 수 있다. 체크카드를 ATM 기기에 삽입하고(소유요소), 체크카드 비밀번호를 입력하는(지식요소) 절차이기에 2단계 인증으로 볼 수 있다((그림 6) 참조).

다. 공인인증서+보안카드/OTP(2 Factor)

스마트폰뱅킹이나 인터넷뱅킹에서 볼 수 있는 방식으로 계좌 비밀번호와 공인인증서 비밀번호를 알고 있어야하며, 해당 공인인증서 파일과 보안카드 또는 OTP를 소유하고 있어야만 인증이 가능한 2단계(Two-Factor) 인증의 모습을 보여주고 있다((그림 7) 참조)

라. 심장박동/심전도+NFC팔찌(2 Factor)

Bionym社의 Nymi라는 NFC 팔찌는 사용자의 심전도

(그림 8) NFC 인증 팔찌
〈출처〉: Bionym 社

와 심박수를 이용하여 사용자를 인증하는 방식의 NFC 기반 인증 팔찌를 선보였다. 이는 소유요소(전자 팔찌)+내재요소(심전도, 심박수)를 이용한 2단계 인증의 사례이다((그림 8) 참조).

Ⅳ. FIDO 기반 인증기술

FIDO Alliance는 2006년 6월 설립된 온라인 보안인증 관련 글로벌 기업들의 연합체다. FIDO 연합은 온라인 환경에서 보다 편리하고 안전한 인증시스템을 공동으로 구축하고 인증시스템에 대한 기술표준을 제시하는 역할을 하는 연합체이다.

현재 가입된 기업으로는 Google, Lenovo, Visa & Master Card, PayPal 등등의 회사들과 한국 기업인 Crucialtec이 이사회로 속해 있고, 온라인 인증 및 생체인증에 대한 기술개발을 하는 회사들이 스폰서, 정회원의 등급으로 구분된 약 30여 개의 기업들이 연합을 이루고 있다.

FIDO 연합이 추구하는 온라인 인증방식은, 온라인상의 빠른 신원 확인을 위해 간단하고(Simpler), 강력한(Stronger) 인증방식을 개발하는 것이라고 한다. 정회원으로 등록되어있는 대부분의 기업들이 위에서 언급된 SurePassID와 Certus와 같이 알려진 큰 기업은 아니지만 획기적인 기술들을 이사회로 등록된 회사들의 평가를 통해 실제 서비스로 개발되는 사례가 많다. 향후 새로운 모바일 및 온라인상에서의 새롭게 개발된 인증체계가 많이 보여질것으로 기대된다.

1. FIDO 인증 개념

인증기술의 가장 큰 문제점은 패스워드를 이용하는 것이며 온라인 인증 또는 디바이스 인증에 뚜렷한 대안이 없다는 것이었다. 특히 온라인 인증의 경우에는 현재 대부분의 인증방식이 패스워드를 기반으로 하고 있어 보안에 취약한 문제를 안고 있지만 마땅한 해결책이 나오고 있지는 않다. 우리나라의 경우에는 공인인증서를 이용하여 보다 강도 높은 인증기술을 사용하고 있지만 공인인증서도 패스워드를 사용한다 점에서는 여전히 취약점을 가지고 있다.

인증기술의 메가트렌드는 간편하고 안전한 인증기술이 사용된다는 점이다. 현재 사용하고 있는 PC(Personal Computer)나 노트북의 인증은 주로 패스워드를 기반으로 하고 있다. 얼마 전에는 노트북에 지문인식을 사용하기도 했지만 요즘은 사용하지 않고 다시 패스워드를 사용하는 추세이다. 이것은 대부분의 운영체제들의 로그인 방식이 패스워드로 되어 있기 때문이다.

하지만 이러한 추세는 스마트폰과 같은 디바이스들이 등장하면서 바뀌었다. 스마트 디바이스들은 일단 화면이 작아 입력이 불편하고 노트북보다는 단시간 자주 이용하는 경향이 있어 패스워드를 입력하기가 쉽지 않다. 또한 노트북과는 달리 개인적으로 들고 다니기 때문에 타인이 사용할 가능성이 낮다. 이러한 이유로 스마트 디바이스에서는 숫자로 된 PIN을 입력하거나 패턴을 그리거나하는 방법으로 사용자 인증을 수행하는 것이 추세이다. 이러한 디바이스에서의 인증은 점차 발전되어 요즘은 음성인식, 지문인식, USIM(Universal Subscriber Identity Module) 기반 인증기술들이 사용되어 사용자는 간편하지만 보안강도는 높은 인증기술을 적용하는 추세이다.

FIDO에서 제안하는 것은 이러한 스마트 디바이스에서 사용하는 인증기술을 온라인에도 적용하는 것은 어떨까 하는 아이디어이다. 한마디로 특정 웹서버에 인증하기 위해 패스워드를 사용하지 않고 디바이스 인증을

이용하면 사용자는 편리하고 웹서비스는 필요에 따라 인증기술을 선택할 수 있는 장점이 있다. 이것이 FIDO의 가장 핵심적인 필요성이다[1].

2. FIDO 구성요소

FIDO 표준은 두 가지 프로토콜을 제안하고 있다. 첫 번째는 UAF(Universal Authentication Framework) Protocol로 사용자의 디바이스에서 제공하는 인증방법을 온라인 서비스와 연동하여 사용자를 인증하는 기술이다[3]. 두번째는 U2F(Universal 2nd Factor) Protocol로 기존 패스워드를 사용하는 온라인 서비스에서 두번째 인증요소로 강한 인증을 사용자 로그인 시에 추가할 수 있는 프로토콜이다[2].

(그림 9)는 FIDO 구성요소를 보면 FIDO는 크게 클라이언트와 서버 그리고 두 개체 간에 주고 받는 프로토콜로 구성되어 있다. FIDO 클라이언트는 FIDO 인증 토큰과 인증토큰 API라는 인증토큰 추상화 단계에서 연동하는 역할을 하고 있다. 이 의미는 API만 준용하면 어떤 종류의 인증토큰이라도 FIDO 클라이언트에서 사용할 수 있다는 것이다. 클라이언트의 다른 역할은 FIDO 서버와 프로토콜을 송수신하며 등록, 인증, 조회 서비스를 제공하는 것이다.

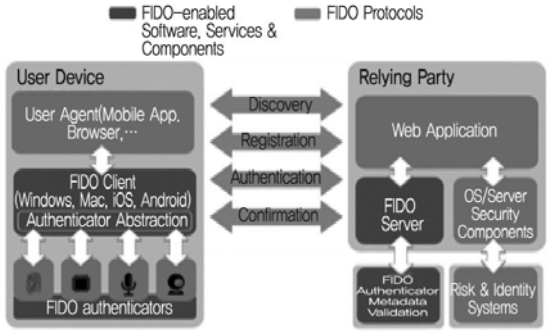
FIDO 서버는 클라이언트와 UAF 프로토콜을 주고 받아 서비스를 제공하는 것이 주 역할이다. 서버는 클라이언트가 제시하는 인증토큰을 검증하고 등록하는 과정을 수행하고 등록된 인증토큰을 관리하여 사용자가 인증을 요청할 때 평가하는 작업도 수행한다.

FIDO 프로토콜은 사용자 디바이스와 서버 간에 세가지 메시지를 전달한다. 첫번째는 등록 메시지로 사용자 디바이스에 있는 인증토큰을 조회하고 검증하여 등록하는 기능을 수행한다. 두번째는 인증 메시지로 도전(Challenge)과 응답(Response) 형태로 이루어진 프로토콜을 수행하여 사용자를 인증한다. 마지막은 안전거래 확인 메시지로 특정거래에 대해 서버가 클라이언트에게 전자서명으로 거래내용을 확인하는 기능을 수행한다.

3. FIDO 프로토콜

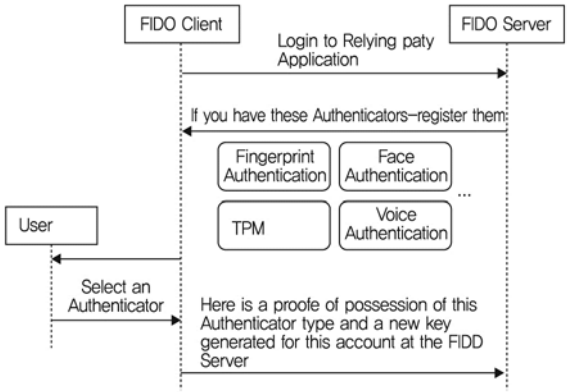
가. Registration

FIDO 프로토콜에서 등록은 사용자의 인증토큰과 공개키를 등록하는 과정이다. FIDO 클라이언트가 FIDO 서버에 로그인을 시도하면 서버는 클라이언트에게 로그인시에 사용 가능한 인증토큰 리스트를 보내준다. 사용자는 화면으로 인증토큰 리스트에서 원하는 인증토큰을 선택하고 본인인증을 수행한 후 키쌍를 생성한다. 클라이언트는 이렇게 생성된 키쌍에서 공개키를 서명하여 FIDO 서버에 보낸다. FIDO 서버는 사용자가 선택한 인



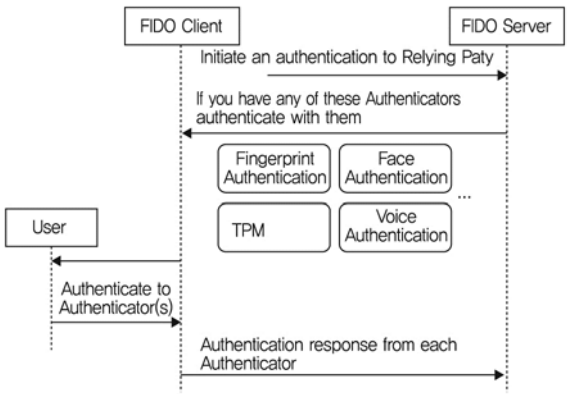
(그림 9) FIDO 구성 요소

〈출처〉: FIDO Alliance



(그림 10) FIDO 등록과정

〈출처〉: FIDO Alliance



(그림 11) FIDO 인증과정

〈출처〉: FIDO Alliance

증토큰과 공개키를 등록하여 나중에 인증 또는 전자서명 검증에 사용한다((그림 10) 참조).

나. Authentication

인증의 프로토콜 흐름은 등록보다 더욱 간단하다. FIDO 서버는 클라이언트에 인증에 필요한 Challenge 값인 난수와 사용 가능한 인증토큰을 보내 인증을 요청한다. 클라이언트에서는 디바이스에서 등록된 인증토큰으로 사용자를 인증하고 서버에 등록된 공개키에 대한 쌍인 비밀키를 복호화하여 서버에서 보내온 요청 메시지 대한 응답으로 전자서명을 생성하여 서버로 보낸다. 서버는 클라이언트가 보내온 전자서명을 등록된 공개키로 검증하여 사용자를 인증한다((그림 11) 참조).

V. 결론

패스워드 인증은 기존의 웹환경이나 새로운 스마트 모바일 환경에서도 지속적으로 사용하기에는 보안 취약성이 커 대체해야 하는 기술로 모두가 인정하고 있다.

FIDO는 사용자가 인증하는 인증토큰 부분과 클라이언트와 서버가 사용하는 인증 프로토콜을 분리하여 패스워드 사용없이 인증방식을 다양화했다는 의의를 둘 수 있다. 사용자는 생체 기반 인증 또는 패턴인식 등을 이용하여 서비스에 로그인할 수 있어 편리성을 경험할 수 있고 클라이언트와 서버 간은 공개키 기반으로 사용자를 인증하여 패스워드보다 더욱 안전성을 보장할 수 있다.

하지만 FIDO를 적용하기 위해서는 모든 서버에 새로운 프로토콜을 처리할 수 있는 라이브러리를 설치해야 하는 문제가 있다. 또한 사용자 환경에도 FIDO를 지원하는 하드웨어들이 설치돼야 사용자 인증에 사용할 수 있다. 또한 FIDO는 스마트 모바일 환경에 더욱 적합하며 웹브라우저를 사용하는 기존의 PC 환경에 적용하기에는 현재는 무리가 있다.

현재 FIDO는 일반적인 서비스에서의 인증보다는 온라인 지불에서 결제 시 인증수단으로 사용하려는 움직임을 보이고 있다. 페이팔은 삼성전자의 갤럭시 S5에 FIDO로 연동하여 결제하는 서비스를 선보였고 최근에는 신용카드 회사인 Visa가 이사회 멤버로 가입하여 결제에 활용하려는 움직임을 보이고 있다. 향후 FIDO가 차세대 인증기술로 주목을 받을지 기대가 되는 대목이다.

약어 정리

CA	Certification Authority
FIDO	Fast IDentity Online
MITB	Man-in-the-Browser
MITM	Main-in-the-Middle
OTP	One-Time Password
PC	Personal Computer
RA	Registration Authority
U2F	Universal 2nd Factor
UAF	Universal Authentication Framework
USIM	Universal Subscriber Identity Module

참고문헌

[1] R. Philpott, S. Srinivas, and J. Kemp, “UAF Architectural Overview,” Version v1.0-rd-20140209, FIDO Alliance, Feb. 2014.

[2] S. Srinivas, D. Balfanz, and E. Tiffany, “Universal 2nd Factor (U2F) Overview,” Version v1.0-rd-20140209, FIDO Alliance, Feb. 2014.

[3] R. Lindemann, D. Baghdasaryan, and E. Tiffany. “FIDO Universal Authentication Framework Protocol.” Version v1.0-rd-20140209, FIDO Alliance, Feb. 2014. http://fidoalliance.org/specs/fido-uaf-protocol-v1.0-rd-20140209.pdf