FIDO 인증의 최신 동향과 FIDO 인증 전문가 자격증 론칭 예정

염흥열 ITU-T SG17 국제 의장, 순천향대 교수

1. 머리말

FIDO 얼라이언스는 비밀번호를 대체하는 강력 하면서도 편리한 사용자 인증수단을 개발하기 위해 2012년 설립된 사실 표준화 단체이다. FIDO 4분기 총회와 Authenticate 2021 행사가 2021년 10월 18일부터 22일까지 미국 시애틀에서 열렸다. 한국에서는 필자를 비롯해 7명의 보안 인증 전문가가 참석했다. 본고에서는 최근 FIDO 얼라이언스의 주요 표준 개발 동향과 FIDO 인증 자격증 제도의 추진 현황을 제시하고자 한다.

2. FIDO 표준 개요

FIDO 얼라이언스의 온라인 인증 표준은 4가지로 구분된다.
첫 번째 표준은 U2F(Universal Second Factor)라 불리는 "범용 2차 인증" 표준이며, 아이디와 비밀번호 기반으로 1차 인증한 후 FIDO 시큐리티 키(security key) 또는 스마트 키로 2차 인증하는 방식이다.
두 번째 표준은 UAF(Universal Authentication Framework)로 불리는 "범용 인증 프레임워크" 표준으로, 스마트 폰을 사용한 모바일 환경에 주로 적용되는 온라인 인증 방식이며, 모바일 디바이스에 적용하여 사용자가 핀 넘버, 패턴, 지문인식, 안면인식 등으로 자신의 스마트폰을 '언락(unlock)'하는 방식으로 스마트폰에 보관되어 있는 개인키에 대한 접근권한을 획득해, 서버에서 보내온 난수에 대한 디지털 서명문을 생성해 서버로 되돌리는 방식으로 사용자를 인증한다. 그대로 로컬 인증하지만, 소지 기반 인증요소(모바일 기기)와 생체 기반 인증요소(생체정보), 또는 지식 기반 인증요소(핀 넘버, 패턴)를 적용하는 다중 요소 인증(MFA, multi-factor authentication)이라 볼 수 있다.
세 번째 표준은 FIDO2로 불리며, 지원되는 플랫폼과 웹 브라우저에서 웹 또는 모바일 상관없이 적용되는 인증방식 표준이다. FIDO2는 다음과 같이 플랫폼 인증자(authenticator)에 적용되는 WebAuthn과 로밍 인증자에 적용되는 CTAP(client to authenticator protocol)로 불리는 "클라이언트 대 인증자 프로토콜" 국제표준으로 구성된다.

- WebAuthn: 웹브라우저 및 플랫폼(OS)에 내장되는 플랫폼 인증자(Platform Authenticator)를 사용하며, 개인 컴퓨팅 환경에 적절하다.
- CTAP1: U2F는 FIDO2 출범 후 CTAP1으로 새롭게 명명되었다.
- CTAP2: CTAP2는 로밍 인증자(스마트폰, Security Key)를 사용하여 브라우저 및 플랫폼에

서 이중 요소 인증 또는 다중 요소 인증(2FA or MFA)을 적용한다. 공유된 컴퓨팅 환경에 적용하는 것이 적절하다.

네 번째 표준은 FDO(FIDO Device Onboard)로 불리는 FIDO 디바이스 온보드는 대규모 IoT 환경 구축과 관련된 보안, 비용, 복잡성 등의 문제를 해소하기 위해 마련되었다. 특정 제조사가 만든 IoT 장치가 수요자의 요구에 따라 다양한 클라우드 관리 플랫폼에 간편하고 안전하게 온보딩(onboarding) 될 수 있도록 한다.

3. 관련 주요 이슈

Authenticate 2021 첫째 날 기조연설자로 나선 미 민주당 전국위원회 최고 보안 책임자 Bob Lord(밥 로드)는 "전투 준비 명령: A Call To Arm)"이라는 제목의 세션을 통해서, "최근 일어나는 여러 해킹은 온라인 서비스 사용자의 아이덴티티를 보호하기 위한 가장 약한 부분인 온라인 인증(Authentication)을 중심으로 일어나고 있다"라고 밝혔다. 그는 이어 "FIDO는 HTTPS가 걸어왔던 길을 걸어가고 있다. 공공 및 민간기관이 HTTP의 약점을 활용한 공격으로부터 엄청난 피해를 당한 후 결국 HTTPS를 기본으로 도입하게 되었다"라고 강조했다. 대규모 형태로 정부나 기업형태로 움직이는 해커들에 맞서기 위해서는 비밀번호 기반 또는 SMS 기반 2차 인증과 같은 레거시 다중요소 인증(Legacy MFA)만으로는 충분하지 않다는 것을 강조했다.
행사 둘째 날 기조연설자로 나선 마이크로소프트 Dana Huang(다나 황) 이사는 "미국 내 전체 온라인 해킹 중 48%가 미 정부기관 대상이며 그중 70%는 온라인 피싱 공격 형태"라고 밝혔다. 지난 10월 초 미 연방총무청(GSA)이 싱글사인온(SSO) 플랫폼인 login.gov의 현대화 작업을 위해서 약 2,220억 원의 테크놀로지 현대화 펀드(TMF)를 확보한 것도 현 상황을 이해하고 대항하기 위한 미 정부의 노력을 보여주었다.
FIDO 얼라이언스에서는 FIDO 인증 전문가 자격증 제도를 2022년 1분기에 시작한다고 이번 총회에서 발표했다. FIDO 인증 전문가 자격증은 사용자 인증 비즈니스 요구사항을 분석하고, FIDO 인증 아키텍처를 제안하며, 조직이 FIDO 표준을 배치하고 통합할 수 있도록 지원하는 신원 및 온라인 인증 전문가 자격증 프로그램이다. FIDO 인증 전문가 자격증은 5가지 영역(FIDO 인증 솔루션 배포, 비즈니스 요구사항 분석, 비즈니스 및 기술 요구사항 설계 및 구현, 구현을 위한 비즈니스 및 기술 요구사항 검증, 온라인 인증에 대한 다른 사용자 교육)에 걸친 전문성을 평가한다.
이 프로그램은 FIDO 사용자 인증 시스템을 분석, 검증, 설계, 배포 및 교육할 수 있는 고급 지식 및 기술 역량을 검증하기 위함이다. 이 자격증이 필요한 주요 대상은 다음과 같다.

- 기술 설계자: 조직 전체에 걸쳐 광범위한 프로젝트를 담당하는 고위 엔지니어링 전문가
- 보안 전문가: 보안 사고의 대부분이 패스워드 분실 또는 도난으로 인한 것임을 이해하는 전문가
- 아이덴티티 및 액세스 관리 전문가: 조직 내 온라인 인증 책임자.
- 시스템 및 운영 엔지니어: 기업 전체에 걸쳐 중요한 인프라 및 자동화를 담당하는 인프라 및 개발 엔지니어.

약 20만 명의 잠재적 초기 수요자가 있을 것으로 보고된 FIDO 인증 전문가 자격증은 보안 전문가에게 경쟁 우위 확보, 향상된 효율성으로 프로젝트 수행, 잠재 수익 증대, 지식 및 기술 검증, 전문적 신뢰도 구축 등의 이점을 제공한다. 또한, 경영진에게는 지식과 전문 지식을 갖춘 인력 확보, 시장 내 신뢰도 향상, 효율성 및 리스크 감소, 직원을 위한 추가 혜택 등의 이점을 제공한다.

4. 향후 추진 전망

FIDO 국제표준은 피싱 공격을 막을 수 있는 온라인 인증 서비스를 제공하기 위해 그 활용이 확대될 예정이며, 계정 복구와 신원 검증을 위한 표준이 개발될 예정이다. 또한, 조직과 기관에서 이의 활용을 증대하기 위해 FIDO 인증 자격증도 도입될 예정이므로 국내 정보보호 전문가의 관찰이 요구된다.