패스키 중심의 패스워드리스 기술적 특성 및 글로벌 도입 동향

최지호, 정수민 ,이학준

금오공과대학교 전자공학부

bonporte93@gmail.com, sumin.jeong@kumoh.ac.kr, hjlee@kumoh.ac.kr

Technical Characteristics and Global Adoption Trends of Passkey-centric Passwordless Technology

Ji ho Choi, Sumin Jeong, Hak-jun Lee

School of Electronic Engineering, Kumoh University

요 약

본 논문에서는 기존 비밀번호 인증의 지속적인 보안 취약점에 대한 해결책으로 부상한 패스워드리스(Passwordless) 기술, 특히 FIDO 표준의 핵심인 '패스키'를 심층적으로 분석한다. 이를 통해, 패스키는 강력한 보안성과 편의성을 제공하는 혁신적 기술이지만, 동시에 표준화된 '계정 복구' 절차 부재와 CTAP(Client to Authenticator Protocol) 하이재킹 등 운영적 과제와 기술적 취약점을 내포하고 있음도 확인한다. 나아가 이에 대한 해결 방안으로 보안 요구사항을 분석하며, 패스키 중심의 패스워드리스 글로벌 도입 동향을 살펴본다. 결론적으로, 패스키의 성공적인 도입과 운영을 위해서는 이러한 기술적·정책적 과제를 해결해야 하며, 이를 위한 산업계의 지속적인 노력이 필요하다는 것을 확인한다.

Ⅰ. 서 론

최근 비밀번호를 대체하는 패스워드리스(Passwordless) 인증이 글로벌 차세대 보안 표준 중 하나로 부상하고 있다. 기존의 비밀번호 인증 체계는 높은 직관성에 의해 수많은 차세대 기술의 등장에도 불구하고 현재까지 가장 보편적인 인증 수단으로 남아있다. 하지만 이와 같이 널리 사용되는 비밀번호 인증 방식에는 단순한 패턴, 피싱, 비밀번호 재사용, 전수 조사 공격(Total Enumeration Attack)과 같은 취약점이 존재한다고 오랫동안 지적되어 왔다. 이러한 결함을 보완하기 위해 인증 분야에서 키 배열 기반 인증을 대체하는 패스워드리스 기술이 주목받고 있다. Yusop 등의 연구에서는 패스워드리스 방식은 생체 인식, 토큰, 패스키 등 다양한 인증 수단을 사용하며, 이들이 비밀번호 방식보다 훨씬 뛰어난 보안 기능을 제공한다고 분석했다 [1]. 패스워드리스 기술의 확산은 국제 표준화 기구와 산업 연합체를 중심으로 활발히 논의되고 있고, 이 같은 흐름 속에서 FIDO(Fast IDentity Online) 표준은 패스워드리스 인증의 핵심 기술로 사용되고 있다. 현재 FIDO는 금융, 공공기관, 기업, 소비자 서비스 등 다양한 산업 분야에서 빠르게 도입되고 있다.

본 연구는 이러한 배경을 바탕으로 글로벌 차원으로 진행되고 있는 패스키에 대하여 논의하고, 이에 대한 패스워드리스 기술의 취약점 및 보안 요구사항을 확인하여 주요 사례와 국가별 기술 적용 동향에 대해 분석한다.

Ⅱ. 차세대 인증 기술: 패스키 심층 분석

보안 위협이 점차 증가하고 있음에도 불구하고, 국내외 다수 기업의 시스템은 여전히 단일 비밀번호 인증 방식에 머물러 있다. FIDO는 기존 기업들이 사용하던 비밀번호 기반 인증의 근본적인 문제점을 해결하기 위해 여러 기기 간 동기화를 지원하는 패스키 개념을 제시했다. 여기서 패스키는 생성된 개인 키를 마이크로소프트나 구글과 같은 클라우드 계정 제공 업체를 통해 사용자의 다른 기기들로부터 안전하게 동기화하여 기기를 교체해도 그대로 사용 가능하게 하는 기술을 의미한다 [2]. 이는 하드웨어의 종속성을 해결하고 편의성을 높이는 차세대 보안 인증 표준으로 자리 잡고 있다.

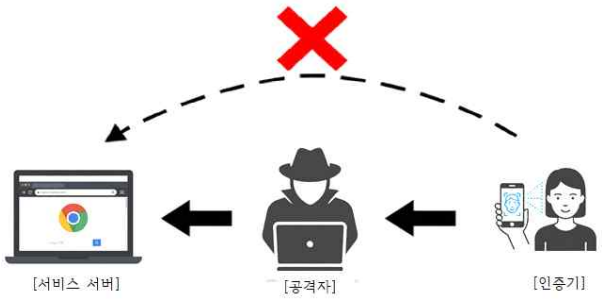
[그림 1] FIDO 패스키 작동 원리

이러한 사용자 편의성 향상은 서비스 만족도를 높일 뿐만 아니라 기업 운영 효율성과 보안성 강화에도 기여한다. 구체적으로, 기업은 피싱 공격을 방어하고 보안 관리 비용 절감을 통해 생산성을 향상시킬 수 있다. 이러한 장점에 의해 패스키는 보안과 편의성을 모두 갖춘 핵심적인 차세대 패스워드리스 인증 기술로 평가된다.

하지만 이론적 완성도와는 달리, 실제 기업 환경에 패스키를 도입하는 데에는 해결해야 할 현실적인 과제가 존재한다. Lassak 등 기업의 보안 전문가들이 실행한 연구에서는 계정 복구 문제로 사용자가 사용하는 모든 기기(스마트폰, 노트북 등)를 분실했을 경우 어떻게 본인임을 증명하고 새로운 기기를 안전하게 등록할 것인지에 대한 명확한 표준 절차가 존재하지 않는다고 지적한다 [3].

또한 Kim 등의 연구에서는 기존의 중간자 공격을 활용하여 패스키에 CTAP(Client to Authenticator Protocol) 하이재킹 공격이 가능하다는 것을 제시한다. 이는 공격자의 PC를 피해자의 인증기와 통신하도록 함으로써, 피해자의 인증 행위를 이용해 접근하는 기법이다 [4].

표적 웹사이트에서 생성되는 QR 코드를 획득한 공격자가 피싱 사이트에 표시하고, 해당 피싱 사이트로 유인한 뒤 QR코드를 스캔하게 하여 피해자의 인증 행위로 공격자의 세션 인가를 통해 로그인을 진행한다. 접근에 성공하여 계정 로그인이 되면 보안 설정으로 들어가 공격자의 스마트



[그림 2] CTAP 하이재킹 핵심 개념

폰이나 보안 키를 새로운 패스키로 등록 가능하다. 이는 나중에 피해자가 해킹 사실을 인지하고 기존 패스키를 삭제하더라도 공격자 자신이 등록한 패스키를 이용해 영구적인 접근 권한을 갖게 됨을 의미한다.

앞서 확인한 계정 복구의 불확실성과 HiPass와 같은 공격 시나리오는, 패스키 도입이 기술 구현을 넘어 체계적인 보안 정책 수립을 요구한다. 따라서 패스키 기반 시스템을 안전하게 도입하고 운영하기 위해서는, 전 세계 디지털 인증의 표준으로 통용되는 미국 국립표준기술연구소(NIST)의 SP 800-63B (Digital Identity Guidelines: Authentication and Lifecycle Management)에서 요구하는 보안 요구사항을 준수해야 한다 [5]. 이를 위해 적용 가능한 보안 요구사항을 다음 [표 2]와 같이 제안한다.

[표 2] 패스워드리스 인증 보안 요구사항

	보안 요구사항	적용 가능한 기술
프로토콜	피싱 방지와 신뢰적인 서명 검증이 가능한 표준 프로토콜을 사용해야 한다.	WebAuthn/FIDO2, TLS1.2+, RP ID/Origin
서버 키 보관	서버는 사용자의 공개키만 저장해야 하며, 개인키는 저장하면 안 된다.	HSM/KMS, PKI 구조
클라이언트 키 보관	클라이언트의 개인키는 안전한 공간에 보관해야 한다.	TPM/SE/TEE 요구, 루팅/탈옥 차단
접근제어	관리자나 앱이 직접 개인키를 읽을 수 없어야 한다.	OS 레벨 생체인증 API, RBAC/ABAC 정책
패스키 복구	복구 과정에서 개인키가 노출되지 않도록 암호화된 상태로 동기화해야 한다.	iCloud Keychain, 암호학적 백업 키+2FA

다음 장에서는 실제 산업 현장에서 어떻게 도입되고 있는지 그 동향과 대표적인 사례를 살펴본다.

Ⅲ. 패스워드리스 도입 동향 및 사례 분석

금융 인증기술의 발전 흐름을 통해 디지털 결제의 급격한 확산과 계정 보안의 중요성 증가로 다양한 인증 기술이 도입되고 있다. 최근 인도 중앙은행(RBI)의 발표에 따르면 비밀번호/PIN + SMS OTP 조합의 2FA 인증 중심인 이전과 달리 디지털 결제 환경에서 생체인식, 하드웨어/소프트웨어 토큰, 패스프레이즈(Passphrase) 등 다양한 2FA 인증 구성 요소로 선택의 폭이 넓어졌다 [6].

이번 인도 중앙은행의 발표는 공식적으로 패스워드리스를 인증 요소로 포함한 조치이며, 이는 인도 금융권에서 빠르게 발전하는 인증기술 방식을 반영하려는 것으로 나타난다. 이러한 동향은 다른 주요 국가에서도 다양한 방식으로 나타나고 있으며, 다음 [표 2]와 같다.

표를 통해 각 국가의 방식과 주체에는 차이가 있지만, 기존 비밀번호 체계의 한계를 인식하고 더 안전한 인증 환경으로 나아가는 공통된 방향성을 보여준다.

[표 2] 주요 국가별 패스워드리스 도입 동향 비교

국가	주요 동향 및 특징	도입 사례
미국	기술 대기업 주도로 시장 표준 형성 / 이커머스, 대형 콘텐츠 플랫폼(유튜브, 트위치 등) 중심 확산	Google, Amazon, PayPal, eBay
EU	강력한 규제(eIDAS)와 조율이 핵심 / 금융 공공 분야는 신중, 일반 서비스는 도입 증가	BMW, 독일 연방 고용청, Albert Heijn
일본	정부-기업 협력으로 빠른 도입 / 금융 및 통신 분야가 시장 선도	SBI 스미신 넷 은행, 야후 재팬
한국	플랫폼 대기업(네이버, 카카오) 중심의 대중화 / 모바일 서비스에서 강세	네이버, 카카오, 토스, 삼성

Ⅳ. 결론

패스워드리스의 기술 발전과 국제 표준의 선두주자인 FIDO를 토대로 본 연구는 기존 비밀번호 인증 방식의 한계를 분석하고, 그 대안으로 부상한 패스키 기술의 원리와 잠재력을 심층적으로 확인했다. 또한 계정 복구 문제 및 기술적 취약점에 대한 해결 방안으로 보안 요구사항이 선행되어야 함을 강조했다. 이와 더불어, 실제 사례분석을 통해 패스워드리스 전환의 글로벌 도입 동향을 확인했으며, 이를 바탕으로 이 과정에서 고려해야 할 핵심 요소들을 제시했다. 앞으로 업계 간 협력을 통해 패스워드리스 기술의 잠재적 취약점을 선제적으로 연구하고 보완해 나간다면, 강력한 규제를 가진 국가들의 보안 요구사항까지 충족시킬 수 있어 기존 비밀번호로부터의 전환을 앞당길 수 있을 것이다.

ACKNOWLEDGMENT

본 논문이 완성되기까지 아낌없는 지도와 조언을 해주신 정수민,이학준 교수님께 깊은 감사를 드립니다.

참 고 문 헌

[1] Mohd Imran Md Yusop, Nazhatul Hafizah Kamarudin, Nur Hanis Sabrina Suhaimi, Mohammad Kamrul Hasan “Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure UserIdentity”, pp1-2, 2025

[2] Khaled Zaky, Amazon Web Services “Replacing Password-Only Authentication with Passkeys in the Enterprise.”, pp4-7, 2023

[3] Leona Lassak, Elleen Pan, Blase Ur, Maximilian Golla “Why Aren’t We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication (Extended Version)” pp8-12, 2024

[4] DongHyun KIM, JuneSeok SHIN, GwonSang RYU, DaeSeon CHOI “HiPass: Hijacking CTAP in Passkey Authentication” pp8-12, 2025

[5] Paul A. Grassi, James L, “Digital Identity Guidelines:Authentication and Lifecycle Management”, 2025

[6] Reserve Bank of India (Authentication Mechanisms for Digital Payment Transactions) Directions, pp.2-3, 2025