Zero Trust 환경에서의 다중 인증 기술 설계 및 분석 연구

장예나, 유용상, 방인규*■, 김태훈■
국립한밭대학교 컴퓨터공학과, *국립한밭대학교 지능미디어공학과
{20222006, 20211884}@edu,hanbat.ac.kr, {ikbang, thkim}@hanbat.ac.kr

Analysis of Multi-Factor Authentication Technologies in a Zero Trust Environment

Yena Jang, Yongsamg Yu, Inkyu Bang*■, Taehoon Kim■
Department of Computer Engineering, Hanbat National University
*Department of Intelligence Media Engineering, Hanbat National University

요 약

최근 클라우드 서비스와 원격 근무 확산으로 인해 기존 경계 기반 보안 모델의 한계가 두드러지면서, 사용자의 신원을 지속적으로 검증하는 MFA의 필요성이 강조되고 있다. 이를 위해 본 연구에서는 FastAPI와 MongoDB를 이용한 서버 환경과 React 및 Firebase 기반 클라이언트 환경을 구성하여 MFA 인증 절차를 실험적으로 구현한다. 이를 통하여 제로 트러스트 환경에서 동적 위험 평가 기반의 다중 인증 정책이 보안성과 사용성의 균형을 달성할 수 있는 효과적인 접근임을 확인한다.

Ⅰ. 서론

코로나 팬데믹 이후 원격근무와 클라우드 기반 업무 환경이 급격히 확산되면서, 기업은 내부망 중심의 전통적 보안 모델만으로는 다양한 접속 환경을 안전하게 관리하기 어려워졌다. 이에 따라 Zero Trust 보안 패러다임이 새로운 대안으로 주목받고 있으며, 기업의 네트워크 접근 통제 및 인증 체계 전반에 변화를 가져오고 있다 [1]. 국내 보안 환경에서도 이러한 흐름에 발맞추어 제로 트러스트 기반 접근제어, 인증 구조 개선, 기업 보안 체계 강화를 다루는 연구가 활발히 진행되고 있다 [2].

본 논문에서는 Zero Trust 환경에서 적용 가능한 MFA 방식을 직접 구현하는 데 중심을 두고, 보안성과 사용자 친화성을 기반으로 TOTP 방식과 Push 인증 각 방식의 장단점을 분석한다. 나아가서, 실제 구현을 통해 얻어진 비교 결과는 Zero Trust 적용 환경에서의 MFA 선택과 설계에 실질적인 가이드라인을 구축할 수 있는 기반을 제안한다. 추가로, 이상 행위 탐지나 리스크 기반 인증 모듈의 초기 단계 설계로 확장할 수 있는 기초를 마련하는 데이터를 확인하고자 한다.

Ⅱ. MFA 개념

Zero Trust의 핵심 원칙 중 하나는 항상 검증하는 것이며, 이를 실현하는 대표적 수단이 다중 인증 (Multi - Factor Authentication, MFA)에 해당한다. 전통적인 비밀번호 기반 인증은 피싱, 크리덴셜 스터핑, 재사용 공격 등 다양한 위협에 취약하므로, 단일 인증 수단에 의존하는 모델로는 Zero Trust의 요구사항을 충족하기 어렵다. 이를 보완하기 위해서 최근의 보안 시스템들은 TOTP (Time - based One - Time Password), Push Notification 인증, 디바이스 바인딩(Device-bound Token) 등의 방식을 조합하여 보안을 강화한다.

MFA는 지식(비밀번호), 소유(휴대기기, 인증 토큰), 내재(생체정보)의 서로 독립적인 인증 요소를 결합하면서 단일 요소를 탈취하는 것만으로는 접근 권한을 얻을 수 없도록 설계된다. 특히 이러한 다중 인증 과정에서 생성되는 로그 정보(IP, User-Agent, 타임스탬프, 디바이스 ID 등) 는 사후 분석 및 이상 행위 탐지(Anomaly Detection)의 기반 데이터로 활용될 수 있다. 이러한 원리는 NIST SP 800-207(Zero Trust Architecture) 와 SP 800-63B(Digital Identity Guidelines)에 명시된 표준적 권고사항이다 [3].

본 논문에서는 기술적으로 MFA를 크게 다음 세 범주로 구분하여 수행하였다. OTP 기반 인증은 TOTP 알고리즘(RFC 6238)을 기반으로 주기적으로 새로운 코드를 생성하는 방식으로, 서버 상태를 최소화하면서 재사용 공격에 대한 저항성을 확보한다. 다만 사용자의 직접 입력이 필요하고, 코드 만료나 시간 동기 오차로 인한 UX 저하가 발생할 수 있다. 다음으로, Push Notification 인증은 서버가 모바일 기기로 승인 요청을 전송하고, 사용자가 승인/거부만 수행하면 인증이 완료되는 방식이다. 이 방식은 평균 응답 시간이 짧고 직관적인 UX를 제공하지만, 네트워크 중계 서비스(FCM, APNs)에 대한 의존성과 기기 탈취·루팅 시 승인 권한이 노출될 위험이 존재한다. 또한 디바이스 기반 인증은 특정 장치에 토큰을 바인딩하거나 승인된 디바이스만 접근하도록 제한함으로써, 계정 탈취 이후의 비인가 접근을 방지한다.

이러한 세 가지 범주의 MFA 중에서도 TOTP와 Push 기반 인증을 중심으로 구현·비교하며, 이에 디바이스 신뢰 기반 접근(device_login)을 결합하여 Zero Trust 환경에서의 다단계 검증 구조를 실험적으로 제시한다. 이 비교는 단순히 보안성을 평가하는 것을 넘어, 재현성, 운영 부담, 사용자 경험이라는 실무적 관점에서 MFA의 적용 가능성을 검증하기 위한 것이다.

■ Corresponding Authors: Inkyu Bang (ikbang@hanbat.ac.kr), Taehoon Kim (thkim@hanbat.ac.kr)

Ⅲ. MFA 구현 전략 및 실험

본 연구의 구현은 단순한 개념 검증이 아닌, 실제 서비스 환경을 모사한 엔드투엔드(End-to-End) 실험 구조로 설계되었다. 서버는 FastAPI 프레임워크를 기반으로 하며, MongoDB를 사용자·기기·세션 로그의 저장소로 활용한다. 클라이언트는 React 기반 웹 UI와 Firebase Cloud Messaging(FCM) 을 연동한 모바일 앱으로 구성하여 푸시 승인 플로우를 구현하였다. 각 구현은 basic_login, otp_login, device_login 세 브랜치로 분리되어 기능적 확장 과정을 체계적으로 검증할 수 있도록 설계되었다.

1. 구현 환경 및 진행 과정

basic_login 단계에서는 이메일/비밀번호 기반 인증과 이메일 링크 검증 절차를 포함하였다. 비밀번호는 Argon2 해시를 적용하여 고강도 해싱을 보장하고, 이메일 검증 토큰은 itsdangerous 시리얼라이저로 서명 및 만료 시간 검증을 수행한다. otp_login 단계에서, RFC 6238 기반 TOTP 알고리즘(pyotp) 을 도입하였다. 가입 과정은 이메일 코드 검증, 시크릿 발급, 최초 TOTP 검증으로 구성되며, 백업 코드(10자리 영숫자)를 생성해 해시로 DB에 저장한다. device_login 단계에서 디바이스 승인 토큰(devtk) 을 쿠키 기반으로 발급하여, 승인된 기기에서의 자동 로그인을 허용하였다. 미승인 기기는 이메일을 통해 1회 승인 과정을 거치며, 승인된 기기는 MongoDB의 devices 컬렉션에 해시화된 기기 정보를 저장한다. 이 구조는 Zero Trust의 '기기 신뢰도 기반 접근 제어'를 실제로 구현하였다. 최종적으로 실험 결과는 반복 시뮬레이션을 진행하며 수집된 인증 요청·응답의 타임스탬프, 검증 결과 코드, 응답 지연(ms) 로그 데이터에 기반하여 분석하였다.

표 1 구현 환경

항목	구성 내용
서버	python 3.11 / FastAPI 0.110 / Uvicorn 0.29
데이터베이스	MongoDB 7.0 (Atlas Cluster)
인증 라이브러리	pyotp (RFC 6238 TOTP 지원), argon2-cffi (비밀번호 해싱)
클라이언트	React 18 / Firebase Cloud Messaging (FCM)
실험 환경	Windows 11 / Chrome 브라우저 v120 / 테스트용 Android FCM 앱
측정 지표	인증 성공률, 응답 지연 (ms), 재사용 공격 차단율, 기기 승인 성공률

2. 실험 결과 및 분석

세 가지 구현은 보안성, 편의성, 운영성 측면에서 상호 보완적 특성을 보였다. TOTP는 시간 기반 일회용성(Time-based One-Time Password)으로 인해 재사용 공격에 강한 저항성을 보였으며, 서버 상태 유지가 불필요해 우수한 확장성을 보였다. 다만 사용자의 직접 입력과 시간 동기 오차로 인한 인증 실패 가능성이 존재했다. 이에 비해 Device 기반 인증은 승인된 기기 외 접근을 원천적으로 차단하였고, Push 인증은 평균 응답 시간이 1초 미만으로 가장 빠르며, 승인/거부만 수행하는 단순한 UX로는 우수한 편의성을 가졌다. 그러나 중계 서비스(Firebase) 의존성과 기기 분실 시 승인 탈취 위험이 확인되었다. 운영 측면에서 TOTP는 독립적으로 동작해 유지 비용이 낮았고, Push 인증은 네트워크 상태에 따라 가용성이 영향을 받았다. Device 기반 인증은 초기 승인 과정이 필요하지만, 이후 로그인 절차가 단축되어 장기적으로 효율성이 높았다. 이상의 결과를 종합하면, TOTP는 보안성, Push는 편의성, Device는 신뢰도에서 각각 강점을 보였으며, Zero Trust 환경에서는 이를 상황 기반으로 혼합 적용하는 Adaptive MFA 정책이 가장 합리적임을 확인하였다.

표 2 MFA 방식별 기능적 비교

구분	보안성	편의성	평균 응답 시간	관리 복잡도
Basic	낮음	보통	350 ± 20	낮음
TOTP	높음	중간	420 ± 25	낮음
Push	중간	높음	210 ± 15	중간
Device	높음	중간	300 ± 18	중간

Ⅳ. 결론

본 연구는 Zero Trust 환경에서 MFA 기술을 실제로 구현하고, 보안성과 사용자 경험(UX)의 상충 관계를 실험적으로 분석하였다. 단일 MFA 방식의 한계를 넘어, 리스크 기반 동적 정책(Risk-Based Adaptive MFA) 을 결합해야 한다. 향후 연구에서는 AI 기반 이상 행위 탐지 모델과의 결합을 통해, 본 연구에서 수집된 인증 로그(TOTP 실패 패턴, Push 승인 지연, Device 재등록 빈도 등)를 입력 피처로 활용하여 MFA 기반 행위 분석형 보안 시스템으로 확장할 예정이다. 이를 통해 Zero Trust 기반 디바이스 인증 체계와 이상 행위 탐지 시스템의 교차점을 제시함으로써, 향후 실무 보안 아키텍처 설계의 기초적 토대를 제공할 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 국립한밭대학교 공학교육혁신센터의 「창의융합형공학인재양 성지원사업」의 지원 및 2025년도 교육부 및 대전광역시의 재원으로 대전RISE센터의 지원을 받아 수행되었음 (2025-RISE-06-002)

참 고 문 헌

[1] 김민규 외, 「제로트러스트 동향 분석 및 기업 보안 강화 연구」, 정보보호학회논문지, 2023.

[2] 이성훈 외, 「제로트러스트 기반 접근제어를 위한 기업 보안 강화 연구」, 디지털융복합연구, 2023.

[3] 미국 국립표준기술연구소(NIST), 「SP 800-207: 제로 트러스트 아키텍처(Zero Trust Architecture)」, 2020 / 미국 국립표준기술연구소(NIST), 「SP 800-63B: 디지털 신원 가이드라인 (Digital Identity Guidelines)」, 2020.