MFA기반 제로 트러스트 시스템 구축

김민지[1], 김현지[2], 임소희[3], 장유정[4], 박인상[5]
[1] 서울여자대학교 정보보호학과 학부생
[2] 서울여자대학교 정보보호학과 학부생
[3] 서울여자대학교 정보보호학과 학부생
[4] 서울여자대학교 정보보호학과 학부생
[5] 이글루코퍼레이션 책임연구원
qpfk0522@swu.ac.kr, khj5276@swu.ac.kr, 2022111341@swu.ac.kr, wkddbwjd010@swu.ac.kr, insang1983@naver.com

Enhancing Security through Zero Trust Systems Using Multi-Factor Authentication

Min-Ji Kim[1], Hyun-Ji Kim[2], So-Hee Lim[3] ,You-Jeong Jang[4], In-Sang Park[5]
[1]Dept. of Information Security, Seoul Women's University
[2]Dept. of Information Security, Seoul Women's University
[3]Dept. of Information Security, Seoul Women's University
[4]Dept. of Information Security, Seoul Women's University
[5]Igloo Corporation

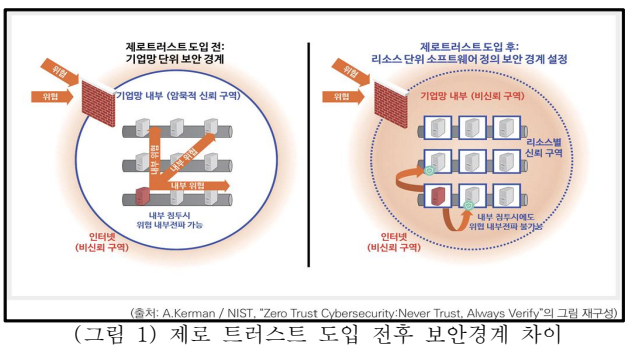
요 약

최근 기업 및 기관은 온-프레미스에서 클라우드로 전환이 급증하였다. 이에 따라 기존의 경계 보안장비 방식이 아닌 제로 트러스트 시스템 구축이 확대되고 있다. 제로 트러스트 시스템은 MFA 인증을 통해 접근 인증이 된 사용자만 리소스 접근이 가능해져 보안 강화를 더 용이하게 할 수 있다. 각 기업에서 관리자는 대시보드를 통해 실시간으로 시스템을 모니터링 할 수 있으며, 사용자들은 자동화된 시스템을 통해 리소스를 편리하게 사용할 수 있도록 구성했다.

1. 서론

2021년 5월 12일, 바이든 대통령의 국가 사이버 보안 개선을 위한 행정명령(EO-14028)을 발표했다. [1] 백악관 산하 관리예산실(OMB)은 제로 트러스트 사이버 보안 원칙을 향한 미연방 정부 전략에 관한 각서 'M-22- 09'를 발표한 바가 있다.[2] 또한 과학기술정보통신부는 2023년 7월 제로 트러스트 가이드라인 1.0을 발표해 제로 트러스트 보안 모델을 적용하는 방법을 제시했다.[3]

제로 트러스트는 '절대 신뢰하지 말고 항상 검증하라(Never Trust, Always Verify)' 라는 의미로 내부 네트워크에 접속하는 모든 사용자를 잠재적 위협 요소로 간주하여, 기존의 신뢰 기반 보안 모델을 대체하는 프레임워크이다.



(그림 1) 제로 트러스트 도입 전후 보안경계 차이

기본 보안경계 모델에서는 (그림 1)과 같이 내부 트래픽이나 네트워크 위치만으로 신뢰성을 부여해 공격, 침해 경로가 다양해지는 문제가 있었다. 제로 트러스트 모델은 '비 신뢰'를 기반으로 강화된 인증 및 기기 상태 모니터링 등을 통하여 접근 제어가 가능하다.

이에 따라 본 연구는 MFA 기반 제로 트러스트 시스템 구현 방법에 대해 제시하고자 한다. 제로 트러스트 시스템 요구사항과 동작 원리를 제시하고 최적화 방안을 제안한다.

2. 제로 트러스트 시스템의 요구사항

제로 트러스트 시스템은 MFA(Multi Factor Authentication)를 제공한다. 사용자는 인증을 위해 지식, 소유, 생체, 특징 기반 인증 방식 중 2가지 이상의 방식을 혼합한다. 지식 방식 인증을 위해 사용자계정(User ID)과 패스워드(Password) 방식으로 인증한다. 소유 방식을 위해 OTP(One Time Password) 방식으로 인증한다. 사용자는 화면에서 QR코드를 모바일 기기의 카메라로 촬영하고 인증 앱을 통해 사용자를 인증한다.

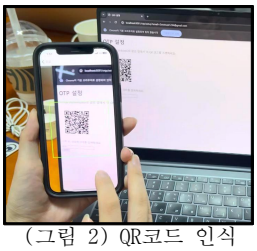
비 신뢰를 기반으로 사용자의 접근을 통제하고, 로그인 시 MFA 인증 절차를 거쳐 관리하게 된다. 이 모든 과정은 로그로 기록되고, 비정상적인 접근이 있을 경우 바로 차단할 수 있도록 동작하는 제로 트러스트 모델을 구축한다.

3. 동작 원리

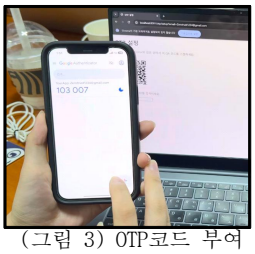
제로 트러스트 시스템을 구축했으며, MFA 활성화를 통한 접근 제어 정책에 따라 보안 정책을 적용하도록 했다. 사용자가 1차 로그인을 거치면 MFA 인증이 되지 않은 최초에는 QR코드 인식(그림 2)을 통해 구글 Authenticator 앱으로 OTP 코드(그림 3)를 부여받는다. 이후 로그인 시 OTP 코드 입력을 통해 2차 본인인증을 거쳐야 보호된 리소스가 위치하는 홈 화면으로 접속 가능하게 된다.

로그인 계정의 경우 사용자 계정과 관리자 계정이 있다. 관리자 계정으로 로그인을 할 경우 사용자의

로그 기록과 사용자 목록을 조회할 수 있다.

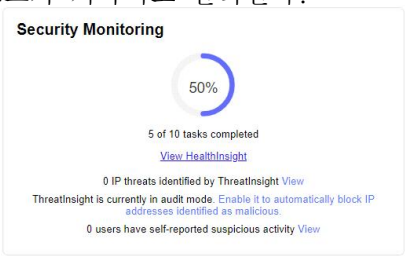


(그림 2) QR코드 인식



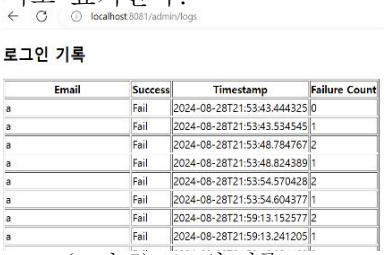
(그림 3) OTP코드 부여

관리자 계정으로 로그인하면 사용자들의 로그인 로그를 확인할 수 있다. 이 시스템은 사용자의 Email, Success, Timestamp, Failure Count, MFA와 같은 주요 정보를 제공한다. 사용자가 로그인할 때마다 로그가 자동으로 저장되며, 누적된 실패 횟수를 통해 사용자의 신원과 신뢰도를 지속적으로 검증한다. 또한, 각 로그인 시각이 표시되어 중앙 집중식으로 히스토리를 확인할 수 있는 가시성을 제공한다. 사용자는 로그인 시 반드시 MFA 인증 과정을 거치며, 이와 관련된 모든 로그가 기록되고 관리된다.

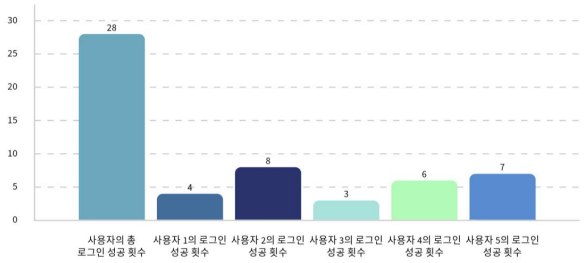


(그림 4) Security Monitoring

대시보드 인터페이스의 일부인 (그림 4)는 관리자 계정에서 관리자가 관리해야 할 항목들을 점검하고 그 결과를 수치로 표기한다.



(그림 5) 로그인 기록



(그림 6) 사용자의 로그인 기록 차트

(그림 5)는 total_user_count(사용자의 총 로그인 성공 횟수), login_success_user_count(사용자별 총 로그인 성공 횟수), login_fail_user_count(사용자별 총 로그인 실패 횟수), date_login_success_user_count(날짜별 사용자의 총 로그인 성공 횟수), date_login_fail _user_count(날짜별 사용자의 총 로그인 실패 횟수), MFA_success(MFA의 총 성공 횟수)를 표로 나타내어 세분된 영역으로 구분하였다. 또한, 이를 (그림 6)과 같이 차트로 나타내어 가시성을 높여 사용자의 로그 기록 관리 편의성을 높였다. 이를 통해 관리자에게 세밀한 수준에서의 핵심 요소 간 상호 운용성을 제공하였다.

(그림 7) 사용자 목록

(그림 7)은 session id, email, password, name 등을 조회할 수 있도록 구성되어 있다. password는 해시화되어 저장되기 때문에 관리자의 권한에도 불구하고 최소한의 권한 접근만을 허용한다. 앞서 언급한 내용과 동일하게 사용자의 로그인 기록을 로그로 남기기 때문에 로그인 실패 기록이 비이상적으로 많은 사용자의 경우에만 관리자의 권한으로 임의로 사용자의 계정을 삭제할 수 있다.

위의 기능들을 통해 관리자는 시스템 내에서 발생하는 모든 로그인 활동을 한눈에 파악할 수 있으며, 사용자 관리 및 접근 권한 설정을 보다 직관적이고 체계적으로 수행할 수 있다. 이러한 기능을 적용한 대시보드를 통해 관리자의 운영 효율성을 크게 향상한다.

4. 결론

본 논문은 비 신뢰 기반의 제로 트러스트 원칙을 로그인 시스템에 적용하여 보안을 강화하는 모델을 제시한다. 본 연구에서는 로그인 성공 이후에도 추가적인 MFA 인증 절차를 요구함으로써 반복적인 인증 과정을 통해 보안성을 강화하고, 사용자 계정에 따라 차등화된 접근 권한을 부여하는 방식을 채택하였다. 또한, 관리자에게 효율적인 로그인 기록 및 사용자 활동 모니터링 기능을 제공하여 관리 편의성을 강화하는 데 중점을 두었다.

최근 클라우드와 같이 정보 기술 환경의 급속한 발전과 함께 사이버 보안 위협도 증가하고 있다. 그중 내부 네트워크에 침투한 공격자가 데이터에 접근하거나 시스템을 제어하는 사례가 빈번해지고 있다. 이러한 상황에서 제로 트러스트 모델이 사이버 보안의 필수적 대응 전략으로 주목받고 있다.

대기업을 포함한 약 60% 이상의 기업이 제로 트러스트 전략을 도입하거나 검토 중인 것으로 나타났다.[4] 제로 트러스트 모델의 확산은 기업들이 보안 격차를 줄이는 데 핵심적인 역할을 할 것으로 예상된다. 향후 구체적인 연구를 통해 각 기업 및 기관의 특성에 맞춘 보안 전략 제시가 필요하며, 이를 통해 보다 안전한 환경을 구축하는데 기여하기를 바란다.

참고문헌

[1] The White House. (2021, May 12). Executive order on improving the nation's cybersecurity.
[2] Office of Management and Budget. (2022, January 26). Moving the U.S. Government toward zero trust cybersecurity principles (M-22-09)
[3] 과학기술정보통신부. (2023, 7월 10일). 제로 트러스트 가이드라인 1.0
[4] Cunningham, C., Blankenship, J., Balaouras, S., Murphy, R., & Cyr, M. (2018). The zero trust eXtended (ZTX) ecosystem. *Forrester, Cambridge, MA*.

본 논문은 과학기술정보통신부
대학디지털교육역량강화사업의 지원을 통해 수행한
ICT 멘토링 프로젝트 결과물입니다.