가정용 IoT 시스템 보안 강화를 위한 제로트러스트 보안 원칙의 단계적 적용 연구

안나경, 김상대

순천향대학교 의료IT공학과

skrud1114@gmail.com, sdkim.mie@sch.ac.kr

Research on the Gradual Application of Zero Trust Security Principles for Enhancing Home IoT System Security

Nagyeong Ahn, Sangdae Kim

Dept of Medical IT Engineering, Soonchunhyang University

요 약

본 논문은 가정용 IoT 환경에서 보안 위협이 증가하고 있으나 제한된 자원으로 인한 제로트러스트 전면 적용의 어려움을 해결하고자, 가정용 IoT 홈캠에 제로트러스트 보안 모델을 선택적으로 적용한 보안 강화 방안을 제시하였다. 사용자 인증, 2단계 인증(OTP), 로그인 시간 제한, 로그인 기록 관리, 관리자 대시보드 모니터링 기능을 구현하여 다층 인증 체계와 최소 권한 원칙을 실현하였다. 고도화된 일부 기능은 제외되어 한계가 있으나, 소형 네트워크 환경에서 선택적 제로트러스트 적용의 실효성을 실증적으로 입증하였다.

Ⅰ. 서 론

사이버 보안 위협의 지능화와 네트워크 환경이 복잡해짐에 따라 제로트러스트 보안 모델이 주목받고 있다[1]. 이 모델은 지속적 검증과 최소 권한 원칙을 기반으로 내외부 위협에 효과적으로 대응한다. 그러나 제한된 자원과 높은 도입 비용으로 인해 전면적인 적용은 한계가 있다. 이에 과학기술정보통신부는 핵심 기능을 우선 적용하고 점진적으로 확장하는 전략을 공식 가이드라인으로 제시하고 있다[2]. 이러한 전략은 실제 사례에서도 적용되고 있다. 예를 들어, KB국민은행은 제로트러스트를 기반으로 인프라 구축, 접근 정책 고도화, AI 기반 위협 탐지 및 자동화 등 3단계 로드맵을 수립하여 보안 체계를 단계적으로 강화하고 있다[3].

선택적, 점진적 도입 전략은 전문 인력과 고성능 장비 확보가 어려운 소형 네트워크 환경에서 중요한 의미를 가진다. 최근 가정 내 IoT 기기 보급과 원격 접속 증가로 인해 전통적인 경계 기반 보안의 한계가 드러나고 있으며, 특히 홈캠과 같이 외부 접근이 잦은 장비는 보안 위협에 취약하다.

이에 본 연구는 제로트러스트 모델의 핵심 원칙 중 일부를 가정용 IoT 홈캠 환경에 선택적으로 적용함으로써, 자원이 제한된 네트워크 환경에서도 실효성 있는 보안 강화 방안을 실험적으로 제시하고자 한다. 구체적으로 사용자 인증, 2단계 인증(OTP), 로그인 시간 제한, 로그인 기록 관리, 관리자 대시보드 기반 모니터링 기능을 중심으로 구현하여, 소형 네트워크 환경에서 효과적인 접근 통제 및 지속적인 보안 검증이 가능함을 보이고자 한다.

Ⅱ. 본 론

본 연구에서는 소형 네트워크 환경, 특히 가정용 IoT 홈캠을 대상으로 제로트러스트 보안 모델의 핵심 원칙 중 일부를 선택적으로 도입하였다. 구현 흐름은 그림1의 시스템 구성 및 인증 흐름도에 따라 설계되었으며, 이 흐름도는 사용자, 관리자, 서버 간의 주요 요청/응답 과정을 시각적으로 나타내며, 인증 및 접근 제어 절차의 단계별 흐름을 보여준다.

주요 구현 기능은 다음과 같다.

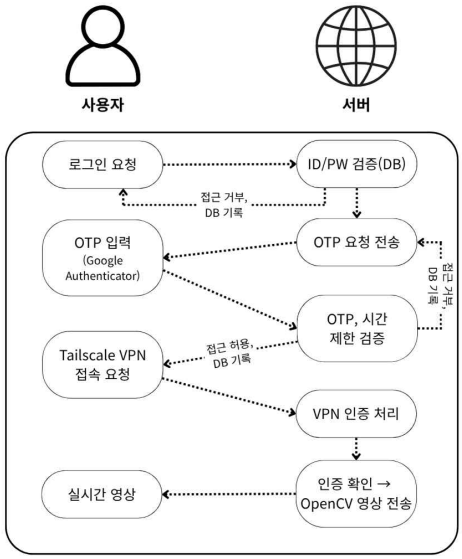


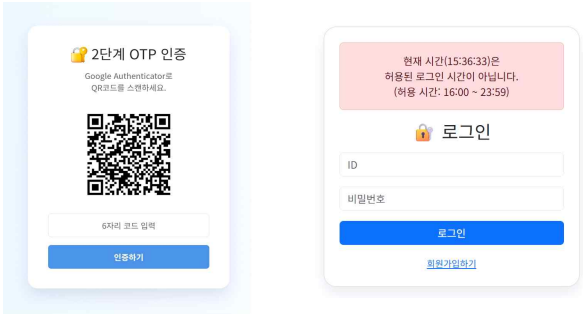
그림 1. 제로트러스트 기반 홈캠 보안 시스템 흐름도

첫째, 로그인 기능을 통해 사용자 인증 기반을 마련하였다. MySQL 데이터베이스와 연동하여 사용자 계정을 관리하며, 사용자 ID와 비밀번호를 검증한다. 이를 통해 접근 통제의 첫 단계인 신원 확인이 이루어진다.

둘째, 2단계 인증(OTP) 기능을 도입하여 인증 절차를 강화하였다. Google Authenticator와 연동되는 시간 기반 일회용 비밀번호(TOTP) 방식을 적용함으로써, 단순 비밀번호 외에도 추가 인증을 요구하여 계정 탈취 위험을 효과적으로 낮출 수 있다. 또한, QR코드를 활용한 OTP 설정 절차는 사용자 편의성과 보안성을 동시에 고려한 방식으로 구현되었으며, 해당 절차는 그림 2의 (a)에 나타나 있다.

셋째, 로그인 시간 제한 기능을 도입하여 사용자의 시스템 접근 가능 시간을 특정 시간대로 제한하였다. 그림 2의 (b)에서 보는 바와 같이, 사용자별 허용 로그인 시작 시간과 종료 시간을 데이터베이스에 저장하고, 로그

인 시도 시 해당 시점이 허용 범위 내에 있는지를 확인하여, 허용 시간 외의 접속을 차단하도록 구현하였다. 이를 통해 내부 사용자의 접근 권한을 시간 단위로 세분화함으로써 최소 권한 원칙을 강화하였다.



(a) (b)

그림 2. 사용자 OTP 인증 및 시간 기반 접근 제어 화면

넷째, 로그인 기록 기능을 추가하여 성공 및 실패한 로그인 시도를 기록하고 관리할 수 있도록 하였다. 로그인 시도 결과와 시각을 데이터베이스에 저장함으로써, 보안 사고 발생 시 추적과 감사를 수행할 수 있다(그림 3 참조). 이는 제로트러스트 모델의 지속적 검증과 모니터링 원칙 구현에 기여한다.

다섯째, 관리자 전용 대시보드 기능을 구현하여 시스템 가시성과 운영 효율성을 강화하였다. 해당 대시보드는 일별 로그인 통계, 시간대별 로그인 분포, 로그인 성공/실패 비율 등을 시각화한다. 그림 4는 구현된 대시보드의 주요 기능들을 보여준다. 또한, 최근 로그인 시도 내역을 테이블 형태로 제공하여, 관리자가 의심스러운 접근을 신속히 탐지하고 대응할 수 있도록 설계하였다. 이를 통해 시스템 전반에 대한 통합적 보안 모니터링이 가능해지며, 제로트러스트의 핵심 원칙인 지속적 검증 및 가시성 확보에 기여한다.

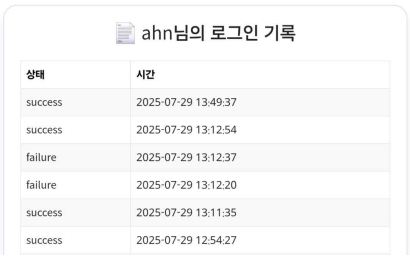


그림 3. 사용자 로그인 기록 조회

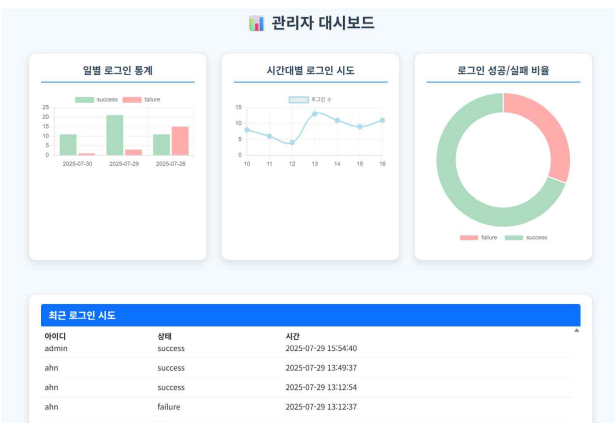


그림 4. 관리자 모니터링 화면

네트워크 경계 보호를 위해서는 Tailscale 기반 VPN을 적용하였다. Tailscale은 WireGuard 프로토콜 기반의 경량 VPN 솔루션으로, 포트 포워딩 없이 안전한 원격 접속이 가능하도록 하며, 외부 접근을 VPN 인증 및 암호화를 통해 제한한다.

또한, Flask 기반 웹 인터페이스와 OpenCV를 활용한 실시간 영상 스트리밍 기능을 통합함으로써, 인증된 사용자만이 안전하게 홈캠 영상을 조회할 수 있도록 구성하였다. 사용자는 로그인 → OTP 인증 → VPN 통과 → 스트리밍 화면 진입의 절차를 거치며, 각 단계에서 철저한 검증을 거쳐 불법 접근을 차단할 수 있다.

구현 결과, OTP 인증 및 시간 제한 제어 기능은 로그인 흐름에서 정상적으로 작동하였으며, 관리자 페이지를 통해 로그인 로그의 시각적 모니터링도 가능함을 확인하였다. 이는 제한된 환경에서도 제로트러스트 모델의 핵심 원칙 일부를 안정적으로 적용할 수 있음을 보여준다.

Ⅲ. 결 론

본 연구에서는 제로트러스트 보안 모델의 핵심 요소인 다층 사용자 인증, 2단계 인증, 시간대별 접근 제어, 로그인 기록 관리 기능을 가정용 IoT 홈캠에 적용하여 최소 권한 원칙을 구현하고, VPN 기반 원격 접속과 실시간 모니터링을 통해 보안성을 강화한 시스템을 설계하였다.

다만 본 연구는 마이크로 세그멘테이션, 리소스 기반 접근 정책, AI 기반 위협 탐지 등의 고도화된 기능들은 제외하여 일부 보안 위협 대응에 한계가 존재한다. 그럼에도 제한된 자원 환경에서 선택적 제로트러스트 적용이 실질적인 보안 대안이 될 수 있음을 실증하였으며, 향후 AI 기반 이상 탐지 및 자동 대응 기술과의 연계를 통한 정교하고 자동화된 보안 체계로의 확장이 기대된다.

ACKNOWLEDGMENT

“본 연구는 2025년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구 결과로 수행되었음”(2021-0-01399)

참 고 문 헌

[1] 과학기술정보통신부, 「제로트러스트 가이드라인 2.0 발표...기업에 구체적 방향성 제시」, 2023.

[2] 과학기술정보통신부·한국인터넷진흥원, 「제로트러스트 보안 아키텍처 가이드라인」, 2023.

[3] 나아영, “아무도 믿지 마라...금융보안원, KB국민은행 '제로트러스트' 선도 사례,” 녹색경제신문, 2025. 4. 9.
https://www.greened.kr/news/articleView.html?idxno=325407