제로트러스트 기반 보안 아키텍처: 소규모 네트워크 규모에서의 성능

나권엽, 김용강*
국립공주대학교
peter261104@smail.kongju.ac.kr, *ygkim@konju.ac.kr

Zero Trust-Based Security Architecture: Performance Metrics in Small-Scale Networks

Gwonyeop Na and Yonggang Kim*
Kongju National Univercity

요 약

본 연구는 과학기술정보통신부의 제로트러스트 가이드라인 2.0에서 제시하는 보안성과 가용성의 양립을 실현하기 위해 리스크 기반 적응형 재신뢰 모델을 제안했다. 이를 위해 동시 접속자 500명 환경에서 총 2시간 동안 약 190만 건의 트래픽을 처리하는 장기 부하 테스트를 수행하였다. 실험 결과, 제안하는 적응형 모델은 전 구간에서 에러율 0%의 안정적인 가용성을 보였으며, 상시 전수 검증 모델 대비 약 3.2%의 응답 시간 개선 효과를 입증하였다. 특히 서비스 최악 조건인 99퍼센타일(P99) 지표에서 레거시 모델과 동일한 130ms를 유지함으로써, 고강도 보안 로직 추가가 시스템 전체 가용성에 부정적인 영향이 적다는 점을 시사한다.

Ⅰ. 서 론

시장 조사 기관인 Market Growth Reports에 따르면 글로벌 제로트러스트 시장은 2030년까지 연평균 17.2%의 높은 성장률을 보이며 지속적으로 확대될 전망이다[1]. 이에 따라 보안성과 가용성을 동시에 확보하기 위한 학술적 연구가 활발히 진행 중이나, 기존 성능 연구들은 실제 운영 환경을 반영하기에 다소 한계가 있다.

특히 Sarkar 등의 실험[1]과 NIST의 실증 테스트[2]는 대개 고성능 인프라를 활용하여 10분 내외의 극히 짧은 시간 동안만 성능을 측정했다는 문제점이 존재한다. 10분이라는 제한된 측정 시간은 실운영 환경에서 발생할 수 있는 네트워크 변동성이나 장기 가동에 따른 메모리 누수, 세션 관리의 병목 현상 등 누적 오버헤드를 포착하기에 턱없이 부족하다. 또한 모든 요청을 재검증하는 전수 검증 모델이 일반적인 컴퓨팅 자원 환경에서 장시간 가동될 때 서비스 안정성에 미치는 정량적 영향에 대해서는 여전히 데이터가 미비한 실정이다.

이에 본 연구는 기존의 단기 실험 방식에서 벗어나, 제로트러스트 가이드라인 2.0을 바탕으로 설계된 리스크 기반 적응형 모델을 일반적인 컴퓨팅 환경에 구축하고 2시간 동안 총 190만 건의 트래픽을 투입하는 장기 부하 테스트를 수행하였다.

Ⅱ. 이론적 배경

2.1 제로트러스트의 등장 배경

최근 클라우드 네이티브 환경의 확산과 지능형 위협 고도화로 기존 경계 보안 모델의 한계가 드러나며 제로트러스트 도입이 가속화되고 있다. 기존 모델은 경계 침입 후 내부에서의 자유로운 이동과 탈취를 제어하지 못하는 취약점이 있으며, 이에 NIST SP 800-207[3, 4]는 모든 접근에 대한 지속적 검증 필요성을 역설하였다.

정책적으로는 2014년 미국 인사관리처(OPM)의 대규모 정보 유출 사고가 전환점이 되었으며[5], 이후 행정명령 14028호[6] 등을 통해 국가 차원의 도입이 의무화되었다.

2.2 제로트러스트 아키텍처(ZTA)의 논리적 구성

제로트러스트를 구현하기 위해서는 정책 결정 지점(PDP)과 정책 시행 지점(PEP) 중심의 논리적 아키텍처 설계가 필요하다. 이 모델은 기존 접근 제어 모델과 논리적 구조가 유사하나, 인증 및 신뢰도 평가가 완료될 때까지 모든 연결을 비신뢰 상태로 간주한다는 점에서 차이가 있다.

이러한 구조는 내부 사용자에게 무조건적인 신뢰를 부여하지 않으며, 모든 접근 요청 시 신뢰도를 평가하여 동적으로 승인 여부를 결정하는 제로트러스트의 철학을 반영한다.

3.1. 보안 모델별 접근 제어 매커니즘 설계

본 연구에서는 제로트러스트 보안 모델의 특성을 검토하기 위해 세 가지 접근 제어 시나리오를 설정하였다. 첫째는 네트워크 내부 접속자에게 암묵적 신뢰를 부여하는 전통적인 경계 기반 보안 모델이다. 둘째는 모든 접근 요청에 대해 매번 정책 엔진을 호출하여 권한을 재확인하는 상시 전수 검증 모델이다. 이 모델은 보안 수준은 높으나 모든 요청에 동일한 검증 부하가 수반되는 특성이 있다. 셋째는 본 연구에서 제안하는 리소스 기반 적응형 재신뢰 모델로, 접근하려는 리소스의 중요도에 따라 검증 강도와 부하를 다르게 적용하도록 설계하였다.

3.2. 리스크 기반 적응형 재신뢰 모델의 도입 타당성

적응형 재신뢰 모델을 실험 대상으로 설정한 이유는 보안 수준과 시스템 가용성 사이의 관계를 파악하기 위함이다. 제로트러스트 가이드라인 2.0에 따르면 제로트러스트 도입은 업무 환경의 특성 및 구성원의 업무 신속성과 편의성 등 다양한 요인을 고려해야 한다고 명시되어 있다 [7]. 또한 기업의 규모와 리소스 종류에 따라 보안 정책을 재정의할 수 있음을 언급하고 있다 [8]. 이에 따라 본 실험의 적응형 모델은 민감도가 낮은 일반 데이터와 재무 데이터와 같은 핵심 자산에 대해 검증 강도를 차등 적용하여, 가이드라인이 제시하는 전략적 보안 선택의 기술적 적용 사례를 보여주고자 한다.

3.3. 실험 환경 및 부하 모델링

설계된 모델의 특성을 확인하기 위해 로커스트(Locust)를 활용하여 동시 접속자 500명 환경에서 성능 측정을 수행하였다. 500명이라는 수치는 국내 중소 및 중견기업의 표준 네트워크 규모 및 클라우드 보안 기준을 참조하여 설정한 것이다 [9]. 정책 시행은 브이엠웨어(VMware) 솔루션을 통해 이루어지며, 검증 결과에 따라 해당 세션을 제어함으로써 리소스 특성에 맞는 보안 검증 체계를 실제 인프라 수준에서 구성하였다. 이를 통해 대규모 트래픽 상황에서의 모델별 응답 시간 및 시스템 변화를 관찰하고자 한다.

Ⅳ. 실험 결과

4.1 장기 부하 테스트를 통한 시스템 안정성 검증

본 연구에서는 제안하는 제로트러스트 보안 아키텍처의 동작을 검토하기 위해 동시 접속자 500명 환경에서 총 2시간 동안 부하 테스트를 수행하였다. 실험 과정에서 1,905,379건의 요청을 처리하는 동안 시스템 오류나 실패는 기록되지 않았으며, 이를 통해 대규모 접속 상황에서의 정책 결정 지점(PDP)과 시행 지점(PEP)의 운영 상태를 관찰하였다. 이러한 장시간의 실험 데이터는 시스템의 구조적 상태를 파악하는 기초 자료로 활용된다.

4.2 응답 시간 분석에서 백분위수 지표의 학술적 타당성

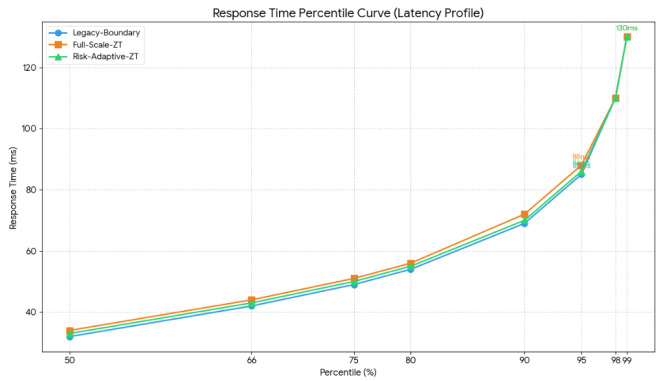

그림 1. 응답 시간 백분위수 분포 곡선

본 실험은 시스템 성능의 실제 분포를 관찰하기 위해 평균값 대신 백분위수 지표를 채택하였다. 학술적으로 평균 응답 시간은 소수의 극단적인 지연 값에 의해 수치가 좌우되는 경향이 있으나, 백분위수는 190만 건의 표본 전체 분포를 반영하므로 통계적 보완이 가능하다. 특히 95퍼센타일(P95)과 99퍼센타일(P99) 지표는 실제 사용자가 경험할 수 있는 최악의 지연 시간을 나타내며, 이는 제로트러스트 가이드라인 2.0에서 언급하는 사용자 편의성과 보안성의 관계를 파악하는 지표로 활용된다.

4.3 보안 모델별 성능 대조 및 적응형 모델의 효율성

백분위수 분포 곡선을 통해 보안 모델별 성능 변화 결과, 전수 검증을 수행하는 상시 전수 검증 모델(Full-Scale-ZT)은 평균 응답 시간 39.14ms를 기록하며 레거시 모델 대비 약 5.7%의 성능 차이를 보였다. 반면 리스크 기반 적응형 재신뢰 모델(Risk-Adaptive-ZT)은 리소스 민감도에 따른 차등 검증을 통해 레거시 모델과의 성능 격차를 2.3% 수준으로 유지하였으며, 전 구간에서 상시 전수 검증 모델보다 낮은 응답 시간을 기록하였다. 특히 95%의 요청이 86ms 이내에 완료된 적응형 모델의 결과는 부하 상황에서의 보안 적용과 실질적인 서비스 운영 가능성을 검토하는 자료가 된다.

V. 결론

본 연구에서는 리소스 리스크에 따라 검증 강도를 조절하는 적응형 제로트러스트 모델을 설계하고, 대규모 부하 환경에서의 성능 변화를 기술하였다. 연구의 주요 내용은 다음과 같다.

첫째, 적응형 모델의 성능 특성이다. 2시간의 장기 실험에서 적응형 모델은 평균 37.90ms의 응답 속도를 기록하여 전수 검증 모델(39.14ms)과의 차이를 보였다. 이는 리소스 민감도에 따른 차등 검증이 보안 적용 시 발생하는 오버헤드 관리에 영향을 줄 수 있음을 나타낸다.

둘째, 데이터 분포 및 시스템 상태 기술이다. 190만 건 이상의 표본을 통한 백분위수 분석 결과, 적응형 모델은 상위 95% 구간까지 레거시 모델의 성능 곡선에 근접한 수치를 보였다. 또한 P99 지표의 수렴을 통해 보안 정책 적용이 시스템의 극단적 지연 상황에 미치는 영향이 제한적일 가능성을 시사했다.

결론적으로 본 연구의 적응형 재신뢰 아키텍처는 보안 정책 적용과 서비스 운영을 병행할 수 있는 모델 중 하나로 검토될 수 있다. 향후 연구에서는 실시간 리스크 탐지 기능을 추가하여 보안 정책의 정밀도를 보완할 계획이다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학ICT연구센터(ITRC)의 지원을 받아 수행된 연구임 (IITP-2026-RS-2024-00438430).

참 고 문 헌

[1] Market Growth Reports, "Global Zero Trust Security Market Research Report," 2024.

[2] Sinshk Sarkar et al., "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," Communications in Computer and Information Science, 2023.

[3] NIST SP 1800-35, "Implementing a Zero Trust Architecture," National Institute of Standards and Technology, 2024.

[4] Rose, S., Borchert, O., Mitchell, S., & Connelly, S., "Zero Trust Architecture," NIST Special Publication 800-207, 2020.

[5] U.S. House of Representatives Committee on Oversight and Government Reform, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," 2016.

[6] The White House, "Executive Order on Improving the Nation's Cybersecurity (EO 14028)," 2021.

[7] 과학기술정보통신부, 한국인터넷진흥원, "제로트러스트 가이드라인 2.0," p. 23, 2024. 12.

[8] Dean, J. and Barroso, L. A., "The Tail at Scale," Communications of the ACM, 2013.

[9] 한국인터넷진흥원(KISA), "클라우드 서비스 보안인증(CSAP) 기준 해설서," 2021.