제로트러스트 클라우드 보안 연구센터

Container-Specific Service Mesh for Lateral Movement Attacks

클라우드 네이티브 환경의 이질성과 동적 변화에 대응하는 온라인 러닝 기반 횡적 이동 공격 방지 서비스 메시

적용분야

Cloud-Native

Kubernetes (AKS, GKE, EKS)

Service Mesh (Istio, LINKERD)

Anomaly Detection

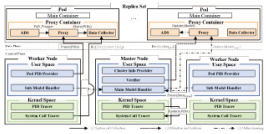
연구목적

- 클라우드-네이티브 환경은 다수의 컨테이너가 공존하는 특성상, 기존의 단일 인공지능 모델 기반의 이상 탐지는 컨테이너 차이를 충분히 반영하지 못해 성능 문제가 존재
- 컨테이너의 빈번한 업데이트로 정상 행위 패턴이 지속적으로 변화하며, 이에 따라 모델의 탐지 성능이 시간이 지남에 따라 떨어지는 Model Drift 현상이 발생
- **As-Is**: 기존 클라우드-네이티브 이상 탐지 시스템은 컨테이너별 특성을 반영하지 못 하고 수동 학습 의존으로 Human Error 및 운영 비효율 발생
- **To-Be**: 컨테이너별 이상 탐지를 위한 사이드카 기반 서비스 메시를 통한 실시간 이상 탐지 및 Online Learning을 통한 컨테이너 특화 모델 학습 및 지속적인 모델 성능 유지

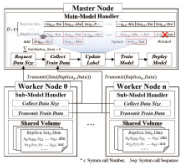
연구내용

Container-Specific Service Mesh

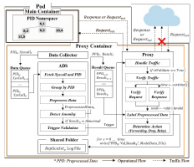
- **Zero-copy-based System Call Collection**
  메인 컨테이너와 프록시 컨테이너 (사이드카) 간 격리를 유지한 상태에서 eBPF 기반 커널 레벨 트레이싱을 통해 시스템 콜 직접 수집
- **Anomaly Detection and Container Isolation Process**
  프록시 컨테이너에서 수집한 시스템 콜 기반 ML 모델을 활용한 이상 탐지 및 탐지 결과 검증 모듈을 통한 컨테이너 격리 수행
- **Container-speicific Online Learning**
  프록시 컨테이너에서 이상 탐지 및 검증 과정을 통해 라벨링된 시스템 콜 데이터 기반으로 지속적인 온라인 러닝 수행 및 모델 배포·교체 수행



1. Container-Specific Service Mesh 아키텍처



2. Anomaly Detection & Container Isolation Process



3. Online Learning Process

4. 공격 및 온라인 러닝 시뮬레이션 대시보드

기술 경쟁력

기존기술 ▸▸▸▸ **기술 차별성** ▸▸▸▸ **대상기술**

- 클라우드-네이티브 환경에서 단일 모델 기반 이상 탐지 구조로 컨테이너 간 이질적 행위 특성 반영 한계 존재
- 정적 정책 기반 서비스 메시 및 오프라인 학습 중심 탐지 구조로 인해 컨테이너 업데이트에 따른 변화 반영 어려움

기술적 한계
- 적용 범위: 클러스터 또는 전체 시스템 단위 통합 모델
- 이상 탐지: 오프라인 학습 기반으로 사전 수집 데이터 의존
- 대응 방식: 탐지 이후 수동 대응 또는 제한적 자동화로 실시간 격리 및 대응 어려움

- 클라우드를 대상으로 전주기적 위험 관리를 수행하는 프레임워크(RMF) 제안
- 우선 대응해야 할 위험을 파악하기 위해, 위협과 위험 간의 연관성을 가진 위험 평가 프로세스 도입

기술적 우위
- 적용 범위: 멀티 컨테이너 기반 클라우드-네이티브 환경에서 컨테이너 단위 보안 기능 제공
- 이상 탐지: 프록시 컨테이너에서 시스템 콜 시퀀스 기반 실시간 이상 탐지 수행
- 대응 방식: 레플리카 간 트래픽 비교 검증을 통해 이상 여부 판단 후, 서비스 메시 기반 트래픽 제어로 컨테이너 격리

지식재산권

발명의 명칭	출원(등록)번호	출원(등록)일자
쿠버네티스의 보조 컨테이너에서 eBPF를 활용한 Zero-copy 기반의 메인 컨테이너의 시스템 콜 수집 장치 및 방법	10-2025-0067396	2025.05.23
쿠버네티스 환경에서의 횡적 이동 공격 방지를 위한 이상 행위 탐지 방법 및 시스템	10-2025-0067413	2025.05.23

제로트러스트 클라우드 보안 연구센터 ZeroTrust Cloud Security Research Center
부산대학교 PUSAN NATIONAL UNIVERSITY
문의처 제로트러스트 클라우드 보안 연구센터 csrc@pusan.ac.kr 051.510.7212