ITRC 대학정보통신연구센터협의회 Information Technology Research Center

제로트러스트 클라우드 보안 연구센터 ZeroTrust Cloud Security Research Center

부산대학교 PUSAN NATIONAL UNIVERSITY

ZeroTrust Cloud Security Research Center

제로트러스트 클라우드 보안 연구센터

센터장, 부산대학교 정보컴퓨터공학부 최윤호 교수

사업 개요

사 업 명	**정보통신방송혁신인재양성사업**(연구지원 - 대학 ICT연구센터)
연구기간	2023. 07. 01. – 2030. 12. 31. (7년 6개월)
연구개발과제명	제로트러스트 클라우드 보안 신기술 연구 및 혁신인재 양성
지원기관	과학기술정보통신부, 부산시, 정보통신기획평가원
참여교수	부산대학교 정보컴퓨터공학부 | 최윤호, 백윤주, 권준호, 안성용, 권동현, 김태운, 전상률, 손준영 연세대학교 미래캠퍼스 소프트웨어학부 | 최석환 고려대학교 컴퓨터공학과 | 전유석 단국대학교 소프트웨어학부 | 조성제
참여학생	박사과정 30명 , 석사과정 52명 (총82명) 2026. 2. 기준
참여기업	클라우드 서비스 개발, 수요 및 공급 기업 / 정보보안 솔루션 개발 및 서비스 기업 / 제로트러스트 보안 서비스 도입 기업

연구내용

- 01 제로트러스트 클라우드 보안 원천 신기술 연구개발
- 02 Tri-Zero(Zero-Copy, Zero-Positive, Zero-Shot) 기반 지능형 이상행위탐지 핵심기술 연구개발
- 03 블록체인 및 Confidential Computing 기반 데이터/인스턴스 신뢰성 보호기술 연구개발
- 04 제로트러스트 및 클라우드 보안 신기술 실증

제로트러스트 클라우드

보안 핵심 신기술 개발 및 혁신인재 양성
지역 거점 클라우드/정보보호 클러스터 산업 활성화 지원

01 클라우드 보안 신기술 확보

- 제로트러스트 원천 기술
- Tri-Zero 기반 이상행위탐지기술
- 블록체인 및 Confidential Computing 기반 데이터 / 인스턴스 신뢰성 기술
- 서비스 실증

02 혁신인재 양성

- 다전공 학생선발
- 산학협력 기반 교육 과정
- 지속적 포트폴리오 관리
- 지역 연계 취업 및 진학
- 양성 인력 사후 관리

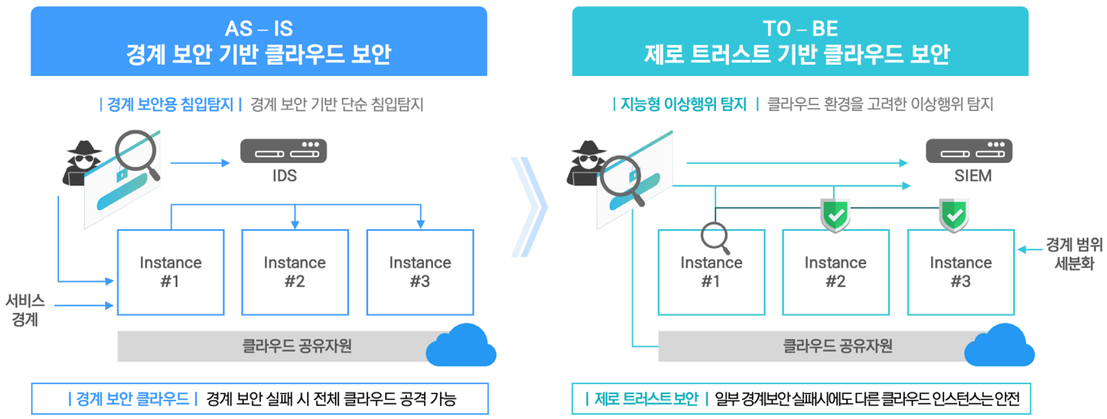
03 지역 산업 활성화

- 센텀 클라우드 클러스터 연계
- 동남권 정보 보호 클러스터 연계
- 에코 델타 시티 연계
- 산학연구 실증

연구배경 클라우드 보안 패러다임 변화

Cloud Security Alliance(CSA)의 클라우드 보안 위협 정의 및 제로트러스트 솔루션 연구개발

- 클라우드 시스템의 발전에 따라 **클라우드 보안 위협 모델이 더욱 세분화되고 정교하게 변화**하고 있음
- **연구 프로젝트별 역할을 분담하여 클라우드 시스템 계층별 보안성 향상**을 위한 **차세대 클라우드 보안 연구 수행**

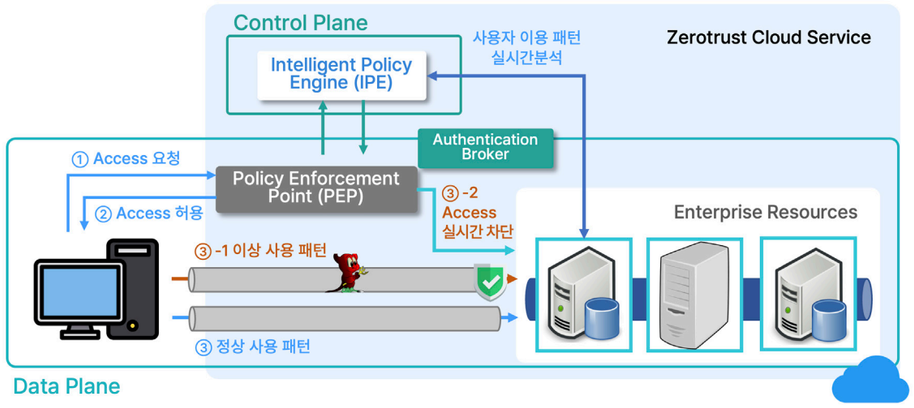


01 제로트러스트 클라우드 보안 원천기술 연구 개발

① 세부과제

- 혁신도약형과제
- 제로트러스트 클라우드보안을 위한 핵심 원천 기술
- 외부 클라우드 서비스/어플리케이션 연동 기술

제로트러스트 클라우드 아키텍처 | 실시간 동적 접근제어 IAP | User Context기반 Policy Engine | 외부 서비스 연동 브로커(Broker)



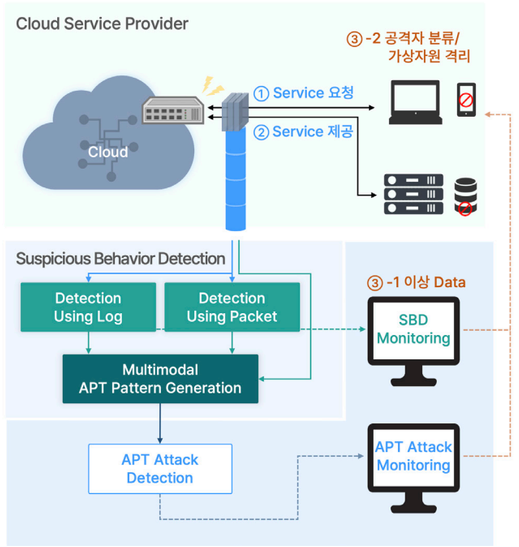
02 Tri-Zero (Zero-Copy, Zero-Positive, Zero-Shot)

기반 지능형 이상행위탐지 신기술 연구

② 세부과제

· Tri-Zero(Zero-Copy, Zero-Positive, Zero-Shot) 기반의 지능형 이상행위 탐지기술
· 클라우드 환경을 고려한 분석 데이터 수집 파이프라인 구축
· APT공격의 불완전한 패턴(Missing Link)에도 대응

- Zero-Copy데이터 수집 파이프라인
- Zero-Positive 이상행위탐지
- Multimodal APT 공격 패턴 생성
- Zero-Shot APT 탐지기술

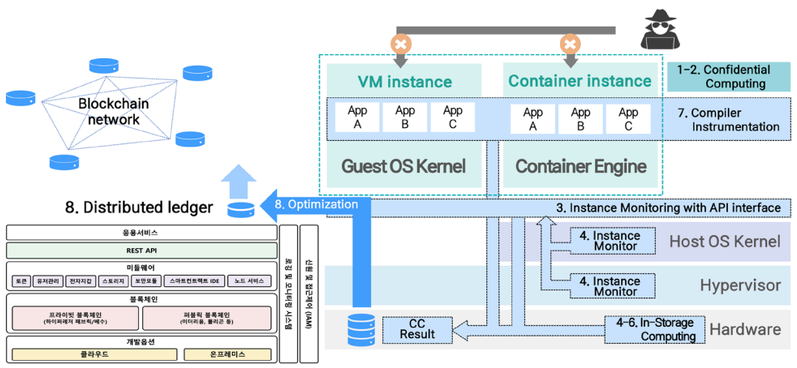


03 고신뢰 클라우드 보안 신기술 연구

③ 세부과제

· 블록체인 및 H/W보안 기술 기반 클라우드 데이터 / 인스턴스 보호 기술 연구개발
· H/W트레이싱 기술을 활용한 인스턴스 보호 및 복원
· 블록체인 기반의 Identity &Access Management(IAM)

- In-Storage 암호화
- Container & BM 인스턴스 보호
- 블록체인 기반 IAM
- BaaS기반 메타데이터 보호



04 클라우드 서비스에 대한 보안기술 실증

④ 세부과제

· 제로트러스트 보안 요소기술의 클라우드 환경 실증
· 클라우드 보안 요소 기술 및 통합 시스템 실증 수행

- 클라우드 보안 요소기술 검증 플랫폼
- 제로트러스트 보안 기술 검증 플랫폼

1단계 클라우드 보안 테스트베드 설계 및 구축 [기술1]

Cloud Common Base

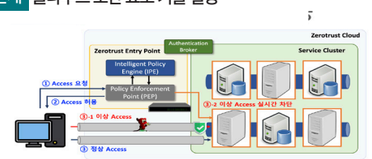
Service Management & Provisioning

VM 저장소	VM 관리 DB	VM 모니터링	VM 프로비저닝	VM 할당	서비스 모니터링

Security Plane

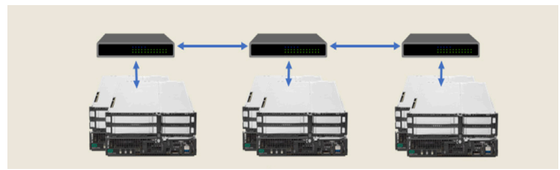
네트워크ACL 관리	네트워크 감시	사용자 인증	세션 관리	Auditing	데이터 암호화

2&3단계 클라우드 보안 요소 기술 실증



제로트러스트 보안 요소 기술 실증 [기술2]

위협 시나리오



테스트 베트 기반 실증

- 클라우드 보안 서비스
- Zero-Positive 모델
- 로그 데이터 무결성/기밀성
- CC 환경 동작
- APT 공격 패턴
- In-Storage 암호화
- 인스턴스 보호
- Tri-Zero 기반 이상행위 탐지 시스템
- BaaS기반 클라우드 로그 보호 시스템

지능형 이상탐지, 고신뢰 클라우드 보안 기술 실증 [기술3]

인재양성 목표

· 제로트러스트 클라우드 보안 신기술 분야 전문지식을 겸비하며, 미래 클라우드 보안 기반 융합 보안기술을 선도할 현장 중심형 창의 인재
· 클라우드 보안 및 제로트러스트 기술에 대한 전문지식과 문제해결 능력을 갖춘 다학제적 클라우드 보안 인재
· 다양한 해외 경험과 글로벌 경쟁력을 갖춘 글로벌 클라우드 보안 인재
· 산학과제와 PBL(Problem-Based Learning) 수업을 통해 현장 문제해결 능력을 갖춘 클라우드 보안 인재
· SCIE 논문 및 Top-conference 논문 작성/발표 능력을 갖춘 글로벌 선도 인재

제로트러스트 클라우드 보안 신기술을 선도할 **현장중심형 창의 인재 양성**

01 **국내1위의 클라우드 보안기술 및 플랫폼 인력양성**

· 제로트러스트 개념 정립 및 클라우드 보안 신기술 개발을 위한 혁신도약형 과제 수행
· 산업 현장 문제 기반 산학협력 과제,공동연구 진행
· 현실문제 해결 및 미래선도형 차세대 클라우드 보안 인재 양성

02 **클라우드 보안 플랫폼/ 신기술 개발 생태계 조성**

· 지역내/국가적 핀테크, 스마트시티, 항만/물류 분야 클라우드 보안 신기술 적용
· 클라우드 보안 기술/서비스 성능 검증을 위한 테스트베드 역할
· 산업체 클라우드 보안 기술/서비스 실증을 통한 클라우드 서비스 산업 생태계 조성 기여

03 **글로벌 제로트러스트 인재 육성을 통한 국가 경쟁력 강화**

· 다양한 해외 연수 경험을 통한 글로벌 인력 육성
· 국외 특허 출원/등록 지원
· Top 컨퍼런스 참여 활동 지원 (우수 연 1회 이상)
· 국제적 전공 전문성 향상

창의융합 인재양성 교육공간 클라우드 보안 플랫폼 리빙랩

01 전시 및 회의공간

- 우수 PBL 프로젝트 결과물에 대한 상시 전시 공간 마련
- 클라우드 보안기술 전시를 위한 홍보 공간 운영 프로젝트 회의 공간 제공

02 연구개발공간

- 창의적 인력양성을 위한 클라우드 보안 플랫폼 아이디어 실습·실험 환경 운영
- 신기술 연구개발을 위한 연구 환경 조성

리빙랩 연구개발

Private Cloud플랫폼 환경
보안 모니터링/관제
이상행위탐지 실습
제로트러스트 보안
프로토콜 보안
인증 및 접근제어 실습환경

리빙랩 기반 지역산업 협력방안

실무적 클라우드 보안 기술지원
클라우드 보안 테스트베드
공동연구 및 보안교육
실무적 현장교육
멘토링 및 현장 데이터

인재양성 리빙랩 소개 02 연구센터 소개

Private Cloud

클라우드 보안 플랫폼 개발 및 서비스 운영에 활용되는 설비/네트워크/클라우드 플랫폼으로,
클라우드 보안 기반 융합 보안 시험을 위한 시험 환경 서비스 제공

- 클라우드 보안 기반 융합 보안 시험을 위한 산업체 연계망/DMZ/클라우드 서비스 시험 환경 제공
- 클라우드 시스템의 보안 취약점 분석 도구 및 실험 장비, 환경 제공
- OS 보안, 임베디드 보안, 전자지갑 등 HW 디바이스 보안 실험 환경 제공
- 산업프로토콜/장비 보안 실습을 위한 실험기자재 제공

클라우드 보안 분석 및 연구 환경 구축

01 가상화 기반 클라우드 보안 플랫폼 연구

- 클라우드 보안 플랫폼 분석 및 연구환경 제공
- 클라우드 기반 블록체인 기술 테스트 환경
- 교육 실습관리
- Agile기반 프로젝트

02 제로트러스트 보안 테스트베드(부산대)

- 이상행위 탐지 클라우드 보안 플랫폼 운영
- 데이터 보안 클라우드 보안 플랫폼 운영
- 클라우드 보안 실습 및 분석/개발 장비 제공

03 실증 테스트베드 (부산광역시, 협력기업)

- 클라우드 보안 플랫폼/보안 기술 결과물 실증
- 현장 시스템 및 데이터 활용 실증
- 결과물에 대한 현장 적용 및 피드백 제공

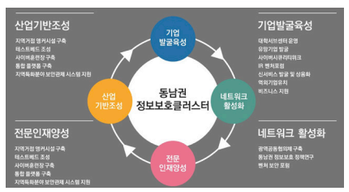
클라우드 보안기술의 지역수요

클라우드 관련 지역우수인재 필요성 증대

현재 부산광역시 센텀 클라우드 클러스터에 국내에서 활동 중인 우수 클라우드 기업이 입주해 있으나 클라우드 관련 우수 지역 인재의 부족으로 인해 당초 채용 예정 인력을 충원하지 못하는 상황

신생/추가 클라우드 관련기업 유치

클라우드 관련 지역 우수인재 부족으로 인해 센텀 클라우드 클러스터에 입주할 신생/역외 클라우드 기업의 이전이 미비한 상황으로 역내 우수 인재 배출이 시급한 상황임



지역거점 정보보호 클러스터 선정

최근 부산시가 과학기술정보통신부의 지역거점 정보보호 클러스터 사업지역으로 선정('23.05)됨에 따라 보안관련 지역 우수 인재에 대한 요구사항이 점차 더욱 커지고 있는 상황임

부산대제로트러스트클라우드보안신기술연구센터입지

지역사회협력 연구센터 지역 사회 협력 02 연구센터 소개

연구센터 역할

역할	지역사회 협력 방안
지역 기업 대상 양질의 인력 공급	수도권 출신 고급인력(석사급 이상)의 동남권(부/울/경남) 이동은 찾아보기 힘들 정도로 드문 상황으로 지역기업들은 고급 인력확보에 난항을 겪고 있음. **부산대학은 지역 내 석박사급 고급 우수인력 전문양성기관으로 지역기업에서 요구하는 클라우드 및 클라우드 보안 관련 고급인력을 교육 및 공급 가능**
맞춤형 클라우드 보안 컨설팅 제공	본 연구센터는 **동남권(부산/울산/경남) 지역 기업들 대상 클라우드 맞춤형 보안 컨설팅 및 기술지원 수행 가능**
산학협력 파트너	**역내 클라우드 업체 대상 클라우드 컴퓨팅 및 보안 기능 향상을 위한 산학협력 연구 수행 파트너**
지자체 및 국가사업 협력	**지자체(부산/울산/경남)와 중앙정부에서**는 디지털경쟁력강화와 양질의 일자리 창출을 위해 **각각 수백억 및 수조 원을 투자하여 클라우드 관련 사업을 진행 중** 국내외 정책, 산업계의 다양한 실제적인 요구사항들을 파악하고 이를 지원하는 **클라우드 컴퓨팅 및 보안 기술 및 인력을 공급할 수 있는 지역내 고등 연구개발 및 교육 기관의 역할 수행**

지역사회협력 연구센터 지역 사회 협력 02 연구센터 소개

기업 경쟁력 강화와 지역 산업 활성화를 위한 협력 수요기업 모집

수요기업 연구센터와 함께 신기술 공동 연구개발과 기술사업화를 수행하여, 기업 경쟁력 강화를 통한 지역 산업 활성화에 기여하고자 하는 기업

수요기업 협력 방향

01 연구개발

- 연구개발 컨설팅
- 공통 연구과제 참여
- 신기술 현장 적용 및 검증

02 교육 및 인프라 지원

- 클라우드기반테스트환경제공(Private Cloud)
- ITC 기술 세미나 제공
- 인턴십 프로그램 연계

03 산학협력

- 기술 · 노하우 이전
- 그 외 산학협력

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

Service Mesh

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

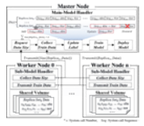
- **As-Is**: 기존 클라우드-네이티브 이상 탐지 시스템은 컨테이너별 특성을 반영하지 못 하고 수동 학습 의존으로 Human Error 및 운영 비효율 발생
- **To-Be**: 컨테이너별 이상 탐지를 위한 사이드카 기반 서비스 메시를 통한 실시간 이상 탐지 및 Online Learning을 통한 컨테이너 특화 모델 학습 및 지속적인 모델 성능 유지

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		· 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 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		**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

제로트러스트 클라우드 보안 연구센터

SecurityHero RMF: Cloud Risk Management Framework

클라우드 자산 분석과 정량적 위험 평가, 권한 상승 탐지 및 대응을 통합 및 자동화한 클라우드 위험 관리 프레임워크(RMF)

적용분야

클라우드 보안

자산 관리

공격 경로 분석

보안 위험 평가

연구목적

- 클라우드 환경 복잡성 증가로 자산 간 접근 경로가 다양해지면서 공격 가능 경로가 식별되지 않고 방치될 위험이 증가함에 따라, 자산 관계 및 접근 경로 기반의 체계적인 보안 위험 분석·관리 필요
- 클라우드 자산의 위험을 정량적으로 평가하는 체계 부재로 심각도 판단이 주관적이고 대응 우선순위 도출이 어려움에 따라, 위험 평가, 대응 및 영향 분석을 연계하는 통합 관리 체계 구축 필요

- **As-Is**: 클라우드 자산 관계를 반영한 위험 분석과 정량적 평가 체계가 부족하여, 실제 공격 가능 경로가 식별되지 않고 위험 대응 우선순위와 영향 범위 판단이 주관에 의존함
- **To-Be**: 자산 관계 분석 및 접근 경로 분석, 정량적 위험 평가를 통해 대응 우선순위 도출과 영향 분석까지 통합 지원하는 위험 관리 체계 구축

**관련 표준 : NIST SP 800-30(Assessment), NIST SP 800-37(RMF), NIST SP 800-53(Controls)

연구내용

통합형 클라우드 위험 관리 프레임워크

- **자산 관계 정의 및 시각화**
  클라우드 내 자산을 수집 및 관계를 시각화하는 토폴로지 제공
  - Network Graph: 네트워크 구성 및 트래픽 흐름 시각화
  - Asset Graph: 권한 및 리소스 간 관계 시각화
- **공격 경로 분석**
  IAM 권한 상승 경로 분석을 통한 권한 탈취 및 공격 확산 가능성 식별
- **자산 위험 평가**
  클라우드 설정 오류 기반 자산의 위험 수준 평가
  - 위험 평가 기준: NIST SP 800-30 참고
- **대응 및 영향 분석**
  분석한 위험에 대한 수정 방안 제시 및 보안 상태 변화 분석

1. 자산 관계 정의 및 시각화

2. 공격 경로 분석

3. 자산 위험 평가

4. 대응 및 영향 분석

기술 경쟁력

기존기술	기술 차별성	대상기술
· 자산 관계 및 접근 경로를 통합하여 고려하지 못해 전체 보안 위험 구조 파악이 어려움 · 위험을 정량적으로 평가하는 체계가 부족하여 대응 우선순위 도출이 어려움		· 자산 관계 및 접근 경로를 시각화하여 보안 위험을 구조적으로 파악 · 위험 평가 결과와 대응 방안 및 영향 분석을 연계하여 통합적 위험 관리 체계 제공
기술적 한계 · 자산 시각화: 자산 관계 및 접근 경로 통합 분석 미지원 · 위험 평가: 표준 기반 정량적 위험 평가 체계가 미흡 · 공격 분석: 자산 간 공격 경로 및 확산 가능성 분석 제한 · 대응 연계: 대응에 따른 영향 분석 미제공		**기술적 우위** · 자산 시각화: 자산들의 관계를 기반으로 접근 경로 시각화 · 위험 평가: 설정 오류 기반의 정량적 위험 평가 수행 · 공격 분석 자산 간 공격 확산 가능성을 식별 · 대응 연계: 대응 방안 적용 시 보안 상태 변화 분석

지식재산권

발명의 명칭	출원(등록)번호	출원(등록)일자
클라우드 컴퓨팅 환경의 IT 자산에 대한 시각화/위험 관리 방법 및 장치	10-2024-0142299	2024.10.17

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

제로트러스트 클라우드 보안 연구센터

PNU Cloud Access Security Broker (CASB)

클라우드 내 서비스에 대한 접근 제어, 데이터 보호, 모니터링 및 위협 식별 기능을 제공하는 클라우드 접근 보안 브로커 (CASB)

적용분야

ZeroTrust | Multi Cloud | 기업/공공 자산 | 네트워크 보안

연구목적

- 클라우드 내 서비스에 대한 접근 제어 관리의 어려움과 네트워크를 통한 데이터 유출 및 내외부 위협이 증가함에 따라, 클라우드 환경을 보호하기 위한 Broker 기반 보안 강화 필요
- CASB는 클라우드 서비스와 사용자 사이에서 중개자로써 보안 통제 지점 역할을 수행하여 기업이 클라우드 서비스를 보다 안전하게 활용할 수 있도록 접근 관리, 데이터 보호, 사용자 모니터링 및 위협 탐지 등의 다양한 보안 정책을 적용할 수 있도록 지원함
- **As-Is**: 기존의 CASB는 SaaS 영역에서 발생하는 사이버 공격 및 데이터 유출을 줄이는 데 기여해왔으나, IaaS 및 PaaS 등의 클라우드 인프라 영역에 보안을 제공하는데 한계를 가짐
- **To-Be**: 멀티 클라우드 인프라에 대한 접근 제어, 데이터 보호, 사용자 모니터링 및 위협 탐지 등의 보안 기능을 제공하기 위해 CASB을 개발하였음

연구내용

Cloud Access Security Broker (CASB)

- **CASB Client**
  클라우드 서비스 사용자의 단말기에서 실행되는 프로그램으로 VPN 연결을 통한 네트워크 보안 기능과 악성 문서 업로드 방지를 위한 위협 요소 제거 기능 제공
- **CASB Server**
  클라우드 사용자 및 서비스를 위한 VPN 인증서 발급 및 VPN 연결 제공, 클라우드 동기화 및 Private IP 할당을 통한 ACL (Access Control List) 생성, 클라우드 서비스 모니터링 및 위협 분석, 클라우드 위협도 기반 세분화된 접근 제어 적용
- **CASB Agent**
  클라우드 서비스를 위한 Agent 프로그램으로 VPN 연결을 통한 네트워크 보안 기능 제공 및 서비스 내 이벤트/시스템 로그 수집 및 전송


1. CASB 아키텍처


2. 위험도 기반 세분화된 접근 제어 적용


3. 클라우드 서비스 모니터링 및 위협 분석


4. 클라우드 서비스내 악성 행위에 대한 선제적 방어

기술 경쟁력

기존기술	대상기술
· SaaS 앱 을 대상으로만 보안 기능을 적용하기에 IaaS, PaaS 등의클라우드 인프라를 대상으로 한 CASB 기술이 부재함 · 멀티 클라우드 환경을 대상으로 통합적인 클라우드 접근 제어 기술의 부재로 인한 정책 관리의 어려움	· 클라우드 인프라를 대상으로 세분화된 접근 제어, 데이터 보호, 사용자 모니터링, 위협 탐지 등 보안 기술을 제공하는 CASB 제안 · 멀티 클라우드 환경을 대상으로, 자동화된 클라우드 동기화 및 접근 제어 리스트 생성 및 세분화된 접근 제어 정책 적용
기술적 한계 · 적용 범위: SaaS 앱을 대상으로만 보안 기능 제공 · 접근 제어: SaaS 앱 대상 접근 제어 기능 제공 · 위협 탐지: 네트워크 트래픽 및 리소스를 통한 위협 탐지	기술적 우위 · 적용 범위: 멀티 클라우드 인프라를 대상으로 보안 기능 제공 · 접근 제어: 멀티 클라우드 대상 세분화된 접근 제어 기능 제공 · 위협 탐지: 실시간 시스템 로그 분석을 통한 위협 탐지 · 프로파일링: 인프라 모니터링을 통한 패턴 분석 및 프로파일링

지식재산권

발명의 명칭	출원(등록)번호	출원(등록)일자
프라이빗 클라우드 환경에서의 제로샷 학습 기반 비정상 행위 탐지 방법 및 시스템	10-2024-0133547	2024.10.02

제로트러스트 클라우드 보안 연구센터 | 부산대학교 PUSAN NATIONAL UNIVERSITY
문의처 제로트러스트 클라우드 보안 연구센터 csrc@pusan.ac.kr 051.510.7212

제로트러스트 클라우드 보안 연구센터

MITRE ATT&CK based Penetration Testing Tool for Security System Demonstration

보안 시스템의 실증을 위한 MITRE ATT&CK 프레임워크 기반의 침투 테스트 도구

적용분야

ZeroTrust | Multi Cloud | 기업/공공 자산 | 네트워크 보안

연구목적

- 사이버 보안 공격의 고도화에 따라, 보안 시스템의 취약점을 효과적으로 진단하고 강화하기 위해 다양한 공격을 수행할 수 있는 침투 테스트 도구의 필요성이 부각됨
- 실제 사이버 공격을 기반으로 정리한 MITRE ATT&CK 프레임워크를 활용한 공격, 각 시스템의 알려진 취약점(CVE)을 스캔 및 악용, HashValue 크래킹과 접근 권한 탈취를 위한 무차별 대입 공격으로 구성함
- 기존 ATT&CK 기반 정형화된 공격 수행 구조에 LLM Agent 기반 지능형 의사결정 모듈을 추가하여, 공격 기법 선택 및 공격 계획, 우선 순위 판단 등을 자동화하고 환경 반응에 따라 공격 전략을 동적으로 조정할 수 있도록 확장함

연구내용

- **AI Agent 기반 공격**
  자율적 의사결정 기반 공격 시나리오 생성 및 실행
  - 취약점 및 악용 공격 시나리오를 Attack Tree 구조로 구현
  - LLM의 공격 설계 성능 향상을 위해 RAG 기반 외부 지식 확장 메커니즘을 적용
  - 공격 수행 결과를 반영하여 공격 경로를 반복적으로 확장 및 최적화
- **MITRE ATT&CK 기반 공격**
  TTPs를 기반으로 구현된 약 1,200개 공격 자동화 및 결과 보고
- **CVE 스캐닝 및 Exploitation**
  포트 스캐닝 및 알려진 취약점(CVE) 탐색 시도 및 악용 공격
  - 무차별 대입 공격을 통한 Credential Access 및 Hash Cracking을 포함


공격 유형 1. AI Agent 기반 공격


공격 유형 2. MITRE ATT&CK 기반 공격


공격 유형 3. CVE 스캐닝 및 Exploitation

기술 경쟁력

기존기술	대상기술
· 사전 정의된 공격 시나리오 및 규칙(rule)에 따라 침투테스트를 수행하는 방식으로, 공격 절차가 고정되어 있음 · MITRE ATT&CK과 같은 프레임워크를 활용하더라도 실제 테스트는 미리 설계된 순서에 따라 단계적으로 실행	· LLM 기반 AI Agent가 탐색 결과를 분석하여 취약점을 자동으로 판단 및 Attack Tree 구조로 공격 계획 구성 · RAG 기반 MITRE ATT&CK TTP 검색 및 공격 수행 결과 피드백을 통한 공격 경로 동적 생성 및 확장
기술적 한계 · 환경 변화에 대응하는 동적 공격 수행 불가 · 공격 간 연계 부족으로 전체 공격 흐름 파악이 어려움 · 사용자 의존도가 높아 자동화 수준의 제한 · 공격 결과를 활용한 지속적 의사결정 기능 부재	기술적 우위 · 환경 변화를 반영한 자율적 공격 의사결정 가능 · 공격 흐름의 가시성 및 확장성 확보 (Attack Tree 구조화) · RAG를 통한 공격 지식 활용으로 공격 설계 정확도 향상 · 공격 계획-실행-분석 전 과정 자동화로 사용자 개입 최소화

지식재산권

SW 명칭	출원(등록)번호	출원(등록)일자
PoC(Proof of Concept) 구현을 통한 클라우드 보안 공격 자동화 플랫폼	C-2024-042500	2024.10.30

제로트러스트 클라우드 보안 연구센터 | 부산대학교 PUSAN NATIONAL UNIVERSITY
문의처 제로트러스트 클라우드 보안 연구센터 csrc@pusan.ac.kr 051.510.7212

ZeroTrust Cloud Security Research Center

제로트러스트 클라우드 보안 연구센터 ZeroTrust Cloud Security Research Center

부산대학교 PUSAN NATIONAL UNIVERSITY

ITRC 대학정보통신연구센터협의회 Information Technology Research Center

TEL 051-510-7212
E-MAIL csrc@pusan.ac.kr

제작년도 | 2026