제로트러스트 환경의 eBPF 활용 연구 동향 및 국가 망 분리(N2SF) 적용 방안 연구

지동혁*, 최상훈[1], 박기웅†

세종대학교 SysCore Lab. (대학원생, 연구교수[1])

**세종대학교 정보보호학과 (교수†)

A Study on Research Trends of eBPF Utilization in Zero Trust Environments and Application Strategies for N2SF

Dong-Hyeok Ji*, Sang-Hoon Choi[1], Ki-Woong Park†

*Syscore Lab., Sejong University

**Dept. of Computer and Information Security, Sejong University

(Graduate Student*, Research Professor[1], Professor†)

요 약

본 논문은 공공기관의 클라우드 전환과 국가 망 보안체계(N2SF) 도입에 맞춰 기존 에이전트 기반 보안의 성능 저하 문제를 해결하기 위해 eBPF 기반의 제로트러스트 프레임워크를 제안한다. 업무 중요도(C/S/O)에 따른 동적 패킷 태깅을 통해 비인가된 정보 이동을 커널 레벨에서 차단하며, eBPF 기반 감사 로그 수집을 통해 등급별 데이터 접근 이력을 실시간으로 기록하고 보안 사고 발생 시 포렌식 분석에 활용하는 구조를 제시한다. 또한 국내 공공기관의 윈도우 운영체제 종속성으로 인한 eBPF 적용의 한계를 분석하고, 이를 극복하기 위한 대안으로 DaaS 환경과 'eBPF for Windows'의 활용 방안을 제시한다.

I. 서론

최근 운영의 편의성과 지속성을 위해 클라우드 기술을 도입하는 기업이 증가하고 있다 [1]. 대한민국의 기업과 공공기관 또한 적극적으로 마이그레이션을 진행하고 있다. 특히 정부는 2030년까지 공공기관 정보시스템의 90% 이상을 클라우드로 전환하는 대규모 사업을 국가적 차원에서 추진하고 있다.

이러한 클라우드 전환은 다양한 이점을 제공하지만 동시에 보안 위협에 노출될 위험이 있어, 민감 데이터를 다루는 공공기관에는 보안 전략이 요구된다. 이에 국가정보원은 공공분야 보안 가이드라인인 '국가 망 보안체계(N2SF)'를 수립하였다. N2SF는 제로트러스트 원칙을 기반으로 내부 시스템과 관리자까지 지속적으로 검증하는 보안 프레임워크이다 [2, 3]. 업무 중요도에 따라 시스템을 기밀(C), 민감(S), 공개(O) 등급으로 분류해 접근통제와 데이터 활용을 동시에 보장한다. 현재 여러 기업이 N2SF 환경에 맞춘 보안 프레임워크를 제안하고 있으나, 단말 및 서버마다 보안 에이전트를 설치해야 하는 기존 방식의 특성상 시스템 오버헤드가 발생한다 [4]. 이러한 한계를 극복할 수 있는 기술로 기존에 단순한 패킷 필터링 용도로 사용되던 BPF에서 발전한 eBPF가 주목받고 있다. eBPF는 별도의 에이전트 설치 없이 커널 레벨에서 보안 기능을 수행할 수 있다. 이러한 특성을 기반으로, 최근에는 eBPF 기술을 활용하여 제로

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 연구은 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보보호핵심원천기술개발(Project No. RS-2026-25519773, 30%; RS-2024-00438551, 10%), 실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 20%), 대학ICT연구센터(ITRC) (Project No. ,10% IITP-2026-RS-2021-II211816, 10%), 한국연구재단(NRF) 핵심연구사업(Project No. RS-2026-25481431 30%)의 지원을 받아 수행된 연구임.

트러스트 아키텍처를 구현하기 위한 연구가 진행되고 있다 [5]. 본 논문은 이러한 선행 연구를 분석하고, 이를 바탕으로 N2SF 환경에서 eBPF의 적용 방법과 방향성을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 소개하고, 3장에서는 적용 방안 및 한계에 대해 기술한다. 4장에서는 해결 방안에 대해서 기술하고 5장에서는 결론 및 향후 연구에 대해 기술한다.

II. 관련 연구

2.1 eBPF 기반 네트워크 접근 제어 연구

Bajaber et al. [4]은 APT 공격을 방지하기 위해 eBPF와 P4 프로그래머블 스위치를 결합한 'P4CONTROL'을 제안하였다. 호스트 내부에서 프로세스가 기밀 파일에 접근하면 eBPF 에이전트가 해당 프로세스에 DIFC 라벨을 부여하고, 이 프로세스가 생성하는 송신 패킷에 라벨을 자동으로 삽입한다. 네트워크 경로상의 P4 스위치는 패킷의 라벨을 속도 저하 없이 실시간으로 검사하여 정책에 위배되는 패킷을 차단한다.

Zaheer et al. [5]에 따르면 마이크로서비스 환경은 IP 주소 기반의 기존 접근 제어 방식이 대규모 클라우드에 적합하지 않다. 이러한 문제를 해결하기 위해 제로트러스트 보안 프레임워크인 'eZTrust'를 제안하였다. eZTrust는 송신 측에 eBPF 프로그램을 부착하여 모든 패킷에 워크로드 컨텍스트 태그를 삽입하고, 수신 측에서 태그를 검증하여 정책에 따라 허용 여부를 결정한다. 기존 대비 패킷 처리 지연을 2~5배, CPU 오버헤드를 1.5~2.5배 낮추었다.

Zhang et al. [6]은 eZTrust가 태깅 시 평문을 사용하여 기밀성이 보장되지 않는 점과, 태그 매칭 실패 시 중앙 컨트롤러와의 통신 오버헤드를 한계로 지적하였다. 이를 개선하기 위해 eBPF 기반 동적 경계 프레임워크인 'EDP'를 제안하여, 송신 시 인증 데이터를 암호화하여 패킷에 내장하고, 수신 측 XDP 단계에서 복호화 및 검증을 수행한다. 이를 통해 eZTrust 대비 연결 설정 지연 시간을 약 80% 감소시켰다.

2.2 eBPF 기반 컨테이너 보안 연구

Nam et al. [7]은 XDP/eBPF 기반의 컨테이너 간 보안 통신 브리지인 'Bastion+'를 제안하였다. Bastion+는 각 컨테이너에 독립된 eBPF 기반 보안 필터를 부착하여, 사전에 정의된 컨테이너 간 통신 관계에 따라 비인가 통신을 차단한다. 또한 필요한 트래픽에만 심층 패킷 검사 등 추가 보안 기능을 선택적으로 적용할 수 있다. 기존 iptables 기반 방식 대비 단일 호스트에서 25.4%, 교차 호스트 환경에서 17.7%의 처리 성능 향상을 달성하였다.

He et al. [8]에 따르면 클라우드 환경에서 eBPF가 공격 벡터로 악용될 수 있다. eBPF의 트레이싱 기능과 헬퍼 함수를 이용하여 컨테이너 간 데이터 탈취, 프로세스 메모리 조작 등의 공격을 시연하였다. 또한 Cilium, Tetragon 등 실제 보안 도구도 이러한 공격을 탐지하지 못함을 확인하였다. 대응책으로 프로세스별 eBPF 권한을 세분화하는 'CapBits' 권한 모델을 제안하였으며, 기존 LSM 기반 방식 대비 CPU 및 지연 시간 오버헤드를 5% 미만으로 줄였다.

2.3 eBPF 기반 감사 로그 수집 연구

Sekar et al. [9]은 감사 도구인 CamFlow, PROVBPF 등의 이벤트 손실과 시스템 오버헤드를 줄이기 위해 eBPF 기반 감사 시스템 'eAudit'를 제안하였다. eAudit는 압축 인코딩, 2단계 버퍼 설계, 시스템 콜 분류를 통해 이벤트 손실 0%, 오버헤드를 평균 4.5%, 데이터 용량을 약 11배 감소를 달성하였다.

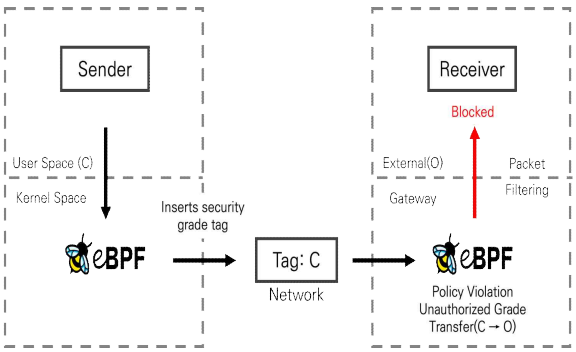
Zhao et al. [10]은 eAudit의 위변조 방지 미지원 한계를 해결하기 위해 eBPF 기반 감사 시스템 'Nitro'를 제안하였다. 기존 시스템은 커널 재컴파일이 필요하거나, 변조된 개별 로그를 특정할 수 없었다. Nitro는 커널 재컴파일 없이 eBPF만으로 구현되며, XLog 암호학적 기법으로 개별 로그 단위의 무결성을 보장한다. 또한 커널 내 로그 축소 모듈로 중복 로그를 실시간으로 제거하여 I/O 오버헤드를 줄인다. 고부하 환경에서 기존 대비 10~25배의 성능 향상을 달성하면서 데이터 손실을 거의 0에 가깝게 유지하였다.

III. N2SF에서의 eBPF 적용과 한계

본 장에서는 관련 연구를 바탕으로 N2SF 환경에 맞는 eBPF 적용 방안과 실제 공공기관 인프라 도입 시 발생하는 한계점에 대해 기술한다.

3.1 동적 패킷 태깅 및 접근 통제

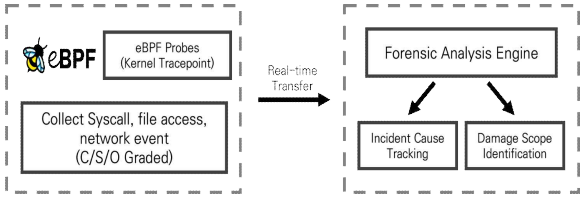
N2SF의 정보 이동 원칙은 하위 등급으로의 비인가된 정보 이동을 통제한다. eBPF 기반 패킷 태깅 및 XDP 기술을 통해 이를 커널 레벨에서 통제할 수 있다. (그림 1)과 같이 송신 측 eBPF 프로그램이 패킷에 보안 등급 태그를 동적으로 삽입한다. 만약 기밀(C) 서버의 데이터를 외부(O)로 전송하려는 비정상적인 행위가 발생할 경우, 수신 측 게이트웨이의 eBPF가 상위 계층에 도달하기 전에 태그를 검증한다. 정책에 위배되는 비인가 패킷은 즉시 차단되며, 이를 통해 정보 유출을 방지할 수 있다.



(그림 1) eBPF 기반 패킷 태깅 흐름도

3.2 eBPF 기반 감사 로그 수집

N2SF는 제로트러스트 원칙에 따라 내부 시스템과 관리자까지 지속적으로 검증할 것을 요구한다. 이를 위해서는 C/S/O 등급별 데이터 접근 이력을 기록하고, 보안 사고 발생 시 포렌식 분석에 활용할 수 있는 감사 로그가 필수적이다. eBPF 프로브를 커널 트레이스 포인트에 부착하여 에이전트 설치 없이 파일 접근, 네트워크 이벤트 등 보안 관련 시스템 콜을 실시간으로 수집한다. 이를 통해 (그림 2)와 같이 비인가 접근이나 내부자 위협 발생 시 사고 원인 추적과 피해 범위 파악이 가능하다.



(그림 2) 이상 행위 탐지 및 차단 구조

3.3 공공기관 엔드포인트 환경의 한계점

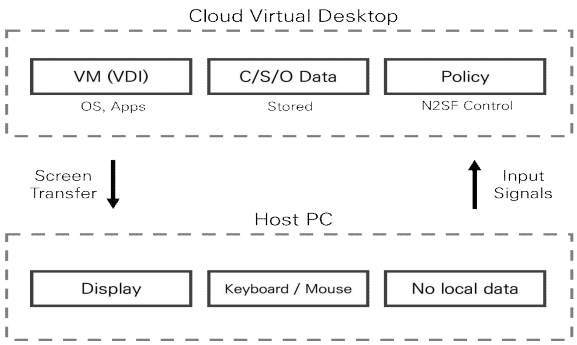
eBPF 기술은 리눅스 환경을 바탕으로 발전해왔으며, 시스템 제어 기능 역시 리눅스 커널에 최적화되어 있다. 반면, 국내 공공기관의 PC는 대부분 윈도우 운영체제를 기반으로 한다. 외부망에서 내부망으로 들어오는 트래픽은 서버를 거치므로 eBPF를 통해 이상 행위를 탐지하고 차단할 수 있다. 하지만 내부에서 일어나는 이상 행위는 eBPF 기술만으로는 통제하기 어렵다.

IV. eBPF 적용 한계 극복 방안

본 장에서는 공공기관 엔드포인트 환경의 한계를 극복하는 방안으로, DaaS 환경의 활용과 최신 기술인 'eBPF for Windows'의 도입 전망을 기술한다.

4.1 DaaS 환경을 활용한 eBPF 적용 방안

DaaS 환경은 (그림 3)과 같이 호스트 PC와 실제 클라우드 내부의 가상 공간이 논리적으로 격리된 구조를 갖는다. 이러한 구조는 공격자가 호스트 PC를 장악하더라도 내부망으로 곧바로 접근할 수 없다. 설령 공격자가 DaaS 환경으로 침투한다 해도 eBPF를 활용해 이상 행위를 차단할 수 있다.



(그림 3) DaaS 환경의 논리적 격리 구조

4.2 eBPF for Windows

최근 마이크로소프트와 오픈소스 커뮤니티의 주도하에 'eBPF for Windows'가 개발 중이다. 현재 네트워크 패킷 필터링과 소켓 접근 제어 영역은 구현이 완료되었으나, 커널 트레이싱 및 보안 감사 기능은 아직 미구현 상태이다. 기능이 고도화될 경우, 예산 부족이나 레거시 시스템 호환성 문제로 DaaS 도입이 어려운 기관에 대안이 될 수 있다.

V. 결론 및 향후 연구

본 논문은 공공기관의 클라우드 전환 및 국가 망 보안체계 도입에 맞추어, eBPF 기반의 제로트러스트 보안 적용 방안을 제시하였다. 선행 연구를 통해 C/S/O 등급 기반의 패킷 태깅과 eBPF 기반 감사 로그 수집 적용 방안을 제시하였다. 국내 공공기관의 단말 종속성에 대한 한계와 이를 보완하기 위한 대안으로 DaaS 환경과 eBPF for Windows의 도입 가능성을 제안하였다. 향후 연구에서는 eBPF for Windows를 활용하여 C/S/O 등급 기반 패킷 태깅 및 WFP(Windows Filtering Platform) 기반 접근 통제 프레임워크를 구현하고, 처리 지연 시간, CPU 오버헤드 등의 성능 평가를 수행하고자 한다.

[참고문헌]

[1] Y.Zhong, P.Chen and H.Zhang, ESX: A Self-Generated Control Policy for Remote Access With SSH Based on eBPF, IEEE Access, August, 2024.

[2] S.K.Mani, K.Hsieh, S.Segarra, R.Chandra, Y.Zhou and S.Kandula, Securing Public Cloud Networks with Efficient Role-based Micro-Segmentation, 22nd USENIX Symposium on Networked Systems Design and Implementation, April, 2025.

[3] A.Mehrban, Z.Abou El Houda, H.Moudoud and L.B.Le, Integrating Zero Trust Architecture in O-RAN: A Comprehensive Survey and Analysis, IEEE Open Journal of the Communications Society, December, 2025.

[4] O.Bajaber, B.Ji and P.Gao, P4CONTROL: Line-Rate Cross-Host Attack Prevention via In-Network Information Flow Control Enabled by Programmable Switches and e BPF, 2024 IEEE Symposium on Security and Privacy, May, 2024.

[5] Z.Zaheer, H.Chang, S.Mukherjee and J.Van der Merwe, eZTrust: Network-Independent Zero-Trust Perimeterization for Microservices, ACM Symposium on SDN Research, April, 2019.

[6] L.Zhang, H.Li, J.Ge, Y.Wu, L.Li, B.Wu and H.Deng, EDP: An eBPF-based Dynamic Perimeter for SDP in Data Center, 23rd Asia-Pacific Network Operations and Management Symposium, September, 2022.

[7] J.Nam, S.Lee, P.Porras, V.Yegneswaran and S.Shin, Secure Inter-Container Communications Using XDP/eBPF, IEEE/ACM Transactions on Networking, vol. 31, no. 2, 2023.

[8] Y.He, R.Guo, Y.Xing, X.Che, K.Sun, Z.Liu, K.Xu and Q.Li, Cross Container Attacks: The Bewildered eBPF on Clouds, 32nd USENIX Security Symposium, August, 2023.

[9] R.Sekar, H.Kimm and R.Aich, eAudit: A Fast, Scalable and Deployable Audit Data Collection System, 2024 IEEE Symposium on Security and Privacy, May, 2024.

[10] R.Zhao, M.Shoaib, V.T.Hoang and W.U.Hassan, Rethinking Tamper-Evident Logging: A High-Performance Co-Designed Auditing System, ACM Conference on Computer and Communications Security, October, 2025.