eBPF 계층 간 교차검증: 커널 백도어 실시간 탐지 기법

정진욱, 권영우*
경북대학교, *경북대학교

dsa04156@knu.ac.kr, *ywkwon@knu.ac.kr

eBPF Cross-Layer Validation: Real-time Detection of Kernel Backdoors

Jin-uk Jung, Young-woo Kwon*
Kyungpook Univ., * Kyungpook Univ.

요 약

eBPF 기술의 등장으로 커널에서 다양한 작업을 수행할 수 있게 되었지만, BPFDoor 같은 백도어를 통해 기존 보안 체계를 우회할 수도 있다. 본 논문은 이러한 한계를 극복하기 위해, 커널의 다계층에 eBPF 프로브를 배치하여 실시간으로 트래픽 흐름의 일관성을 교차 검증하는 새로운 보안 기법을 제안한다. 제안된 기법은 저수준 네트워크 계층에서 관찰된 패킷 정보가 상위 계층이나 특정 분석 도구에서 누락되거나 변조되는 불일치를 탐지하여, 악성 eBPF 프로그램의 행위를 식별하고 차단하는 것을 목표로 한다. 본 연구는 다계층 교차 검증 접근을 통해 기존 단일 지점 감시의 한계를 넘어 커널 내부 위협에 대한 방어 능력 확보의 새로운 가능성을 제시한다.

Ⅰ. 서 론

N2SF 는 공공기관을 비롯한 주요 정보 자산을 중요도에 따라 분류하고, 경계 제어와 로그 분석을 통해 위협을 관리하도록 가이드하고 있다[1]. 하지만 이 같은 지침만으로는 커널 내부에서 흔적 없이 작동하는 커널 백도어에는 무력하다. 대표적인 사례인 BPFDoor 는 파일 시스템이나 로그에 남지 않고 커널 메모리에 숨어 있다가, 특정 매직 패킷을 수신했을 때만 리버스 셸 또는 C2 통신을 열어 방화벽을 우회한다[2]. 이로 인해 N2SF 가이드만으로는 존재조차 포착하기 어렵다.

본 논문에서는 BPFDoor 같은 커널 백도어를 차단하기 위해, 커널 네트워크 스택 전 구간에 eBPF 프로브를 배치하고, 각 계층에서 수집한 패킷 흐름을 교차 검증하는 방법론을 제안한다. 저수준 네트워크 계층에서는 포착되지만, 소켓 계층에서는 누락되는 계층 간 불일치를 식별하고 탐지하여 커널 내부의 위협에도 효과적으로 대응할 수 있음을 입증하고자 한다.

Ⅱ. 관련 연구 및 배경

1. eBPF 악용 사례

eBPF 는 커널에 검증된 바이트코드를 로드 및 JIT 컴파일해 네이티브로 실행하여 kprobe, tracepoint, 소켓 필터 등에 로직을 삽입할 수 있는 경량 런타임 환경이다. 이는 컨테이너 탈출, 권한 상승, DoS 공격 등 악성 행위에도 이용된다[3]. BPFDoor 는 매직 패킷 수신 시에만 활성화되고 커널 내부에서 리버스 셸·C2 통신을 수행하며, Symbiote 는 setsockopt 훅을 통해 tcpdump 등 사용자 영역에서만 트래픽을 숨긴다[4,5].

2. N2SF 보안체계의 한계

N2SF 는 정보 자산을 중요도(C/S/O 등급)에 따라 분류하고, 이를 기반으로 방화벽 운영, 파일 무결성 검사, 로그 수집 및 분석 등 다양한 보안 통제를 차등적으로 적용하여 시스템의 보안을 강화하는 것을 목표로 한다[1]. 그러나 커널 내부에서 파일이나 로그에 흔적을 남기지 않고 작동하는 BPFDoor 같은 최신 커널 백도어를 실시간으로 탐지하고 대응하는 데에는 한계를 보인다. 이러한 백도어는 정상 트래픽으로 위장하거나 리버스 셸 연결을 통해 보안을 우회할 수 있으며, 로그를 남기지 않고 파일 시스템에 의존하지 않기 때문에 기존의 탐지로는 효과를 발휘하기 어렵다.

3. 기존 연구 동향 및 한계

기존 연구 중 LKRG 와 같은 커널 무결성 보호 및 정적 분석은 알려진 커널 변조나 악성 시그니처를 탐지하는 데 효과적이나, 정상적인 메커니즘을 악용하는 커널 백도어 탐지에는 한계를 갖는다. 가상화 환경에서 VMI 를 통한 하이퍼바이저 감사나 HyperBee 같은 eBPF 프로그램 사전 검증 연구도 진행되었으나, 이미 실행 중인 백도어 활동 탐지에는 한계가 있다[6].

Ⅲ. 제안 기법

본 논문은 BPFDoor 와 같은 eBPF 악용 위협을 방어하기 위해, 다계층 eBPF 프로브를 배치하고 각 프로브에서 수집된 패킷 메타데이터 및 시스템 호출 정보를 실시간으로 교차 검증하여 악성 행위를 탐지하는 새로운 방어 기법을 제안한다.

1. 시스템 아키텍처 및 구성 요소

제안된 시스템은 커널 영역과 사용자 영역으로 나누어진다. 커널 영역에서는 네트워크 및 시스템 호출 경로 상의 주요 지점에 설치된 다계층 eBPF 프로브가 패킷과 관련된 메타데이터 및 시스템 이벤트 정보를 수집한다. 사용자 영역에서는 중앙 분석 및 제어 에이전트가 커널 프로브로부터 수집된 데이터를 실시간으로 취합하고, 이를 분석하여 위협 여부를 최종 판단한 후 즉각 대응한다.

2. 다계층 eBPF 프로브

제안된 eBPF 프로브는 네트워크 패킷 흐름 감시를 위해 세 계층으로 구분된다. 먼저, 저수준 네트워크 계층

프로브는 XDP 지점과 TC(Ingress) 지점 모두에 설치되어, NIC 로부터 패킷이 도착하는 즉시 원시 메타데이터를 수집한다. 소켓 계층 프로브는 RAW 소켓 필터를 통해 애플리케이션에 전달되기 직전의 패킷 상태를 관찰하여, 저수준 계층에서 은폐되거나 변형된 트래픽을 탐지한다. 마지막으로 시스템 호출 계층 프로브는 connect()·sendto() 등 네트워크 관련 시스템 호출 지점에 삽입되어, 저수준 계층에서 포착되지 않은 직접적인 연결 시도를 식별한다. 각 프로브가 수집한 데이터는 커널 내부의 BPF 맵과 perf 이벤트를 통해 사용자 영역의 중앙 분석 에이전트로 전송되며, 에이전트는 이를 실시간으로 연계 분석하여 이상 행동을 탐지하고 대응한다.

3. 트래픽 일관성 검증 및 탐지

중앙 분석 에이전트는 각 계층으로부터 수신한 메타데이터를 기반으로 네트워크 흐름을 시간 순서대로 재구성하고, 서로 다른 계층에서 관찰된 이벤트의 일관성을 분석한다. 이를 위해 목적지 IP 주소와 목적지 포트를 조합한 고유 식별자(ID)를 생성하여 계층 간 데이터를 비교하였다. 정상적인 조건에서는 네트워크 패킷 및 관련된 시스템 호출 정보가 저수준 계층에서부터 상위 계층까지 일관되게 나타나야 한다. 그러나 저수준 계층(XDP, TC)에서 탐지된 패킷이 고수준 계층(소켓 필터, 시스템 호출 프로브)에서 관찰되지 않거나, 시스템 호출 프로브가 저수준 계층의 네트워크 이벤트 기록 없이 직접적인 연결 시도를 탐지할 경우 악성 eBPF 프로그램의 은폐 행위 가능성이 있다.

특히 시스템 호출 프로브에서 네트워크 연결 시도가 포착되었으나 저수준 계층의 프로브가 이를 감지하지 못한 상황은 주요한 탐지 지표로 활용된다. 중앙 분석 에이전트는 이러한 계층 간 불일치가 발생하면 즉시 감지하고, 관련된 프로세스 정보와 로드된 eBPF 프로그램 목록 등 추가적인 컨텍스트를 분석하여 악성 여부를 최종적으로 판단한다.

IV. 실험 및 결과

1. 실험 환경

Ubuntu 22.04 LTS 가상 머신 환경에서 수행되었으며, 피해 호스트의 IP 주소는 192.168.100.1, 악성 호스트의 시스템의 IP 주소는 192.168.100.2로 설정되었다. 실험에서는 실제 BPFDoor 모델을 사용하여, 악성 호스트가 특정 UDP 포트로 제작된 매직 패킷을 송신하여 백도어를 활성화하였다. 또한 내부 네트워크에 속하는 정상 트래픽을 분석 대상에서 제외하여 오탐률을 최소화하였다. 피해 호스트로 UDP 기반의 매직 패킷을 전송하면, BPFDoor 백도어가 활성화되어 리버스 셸이 연결되었다. 이 과정에서 피해 호스트에 설치된 다계층 eBPF 프로브는 네트워크 패킷과 시스템 호출 관련 데이터를 실시간으로 수집하였다.

2. 실험 결과 및 분석

```
[XDP]  192.168.100.2:52937 -> 192.168.100.1:5555 proto=17 (id=1677792691)
[TC ]  192.168.100.2:52937 -> 192.168.100.1:5555 proto=17 (id=1677792691)
[SOCK] 192.168.100.2:52937 -> 192.168.100.1:5555 proto=17 (id=1677792691)
[SOCK] 192.168.100.1:0 -> 192.168.100.2:0 proto=1 (id=1677852672)
[CTRL] cpu=2 event=SYSCALL_CONNECT id=1677857116 proto=6 dport=4444
[ALERT] totally invisible syscall: id=1677857116 proto=6 dport=4444
[XDP]  192.168.100.2:4444 -> 192.168.100.1:58730 proto=6 (id=1677845866)
[TC ]  192.168.100.2:4444 -> 192.168.100.1:58730 proto=6 (id=1677845866)
[SOCK] 192.168.100.2:4444 -> 192.168.100.1:58730 proto=6 (id=1677845866)
```

그림 1 연결 시도 탐지

실제 로그 분석 결과를 시각화한 그림에서는 이러한 현상이 명확하게 드러난다. 초기 연결 요청은 모든 계층에서 일관되게 탐지되었으며, 관련된 시스템 호출도 함께 기록되었다. 반면, 이후의 연결은 시스템 호출 계층에만 기록되고, 저수준 계층에서는 전혀 감지되지 않았다. 이와 같은 이벤트는 'totally invisible syscall'로 표시되며, 통상적인 흐름과 일치하지 않는 비정상적인 행위로 분류된다. 이러한 불일치 상황은 BPFDoor 가 저수준 계층을 우회하거나 필터링 우선순위를 조작함으로써 탐지를 회피한 사례로 볼 수 있다. 제안된 탐지 시스템은 이러한 불일치 흐름을 실시간으로 식별하였고, 커널 내부에서의 공격에 효과적으로 대응할 수 있음을 입증하였다.

V. 결론

본 연구에서는 다계층 eBPF 프로브를 통한 실시간 교차 검증 기법을 통해 eBPF 기반 악성 eBPF 프로그램의 탐지 가능성을 확인하였다. 제안된 방법론은 BPFDoor와 같은 실제 eBPF 악용 사례에 효과적으로 대응할 수 있음을 실험으로 입증하였다. 그러나 실환경에서의 적용을 위해서는 정상 패킷에 대한 보다 광범위한 테스트가 필요하며, 탐지 효율성 및 확장성 향상을 위한 추가적인 프로브 최적화와 실시간 대응 기술 개발이 후속 연구 과제로 제안된다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(RS-2021-NR060080).

참 고 문 헌

[1] 국가정보원 국가사이버안전센터, "국가 망 보안체계 보안 가이드라인(Draft)," 2025

[2] J. Ramamoorthy, C. Varol and N. K. Shashidhar, "APT Warfare: Technical Arsenal and Target Profiles of Linux Malware in Advanced Persistent Threats," Cyber Security in Networking Conference (CSNet), Paris, France, pp. 190- 196, 2024

[3] 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 (USENIX Security '23), Anaheim, CA, pp. 5971- 5988, 2023.

[4] CrowdStrike Intelligence Team. "BPFDoor: An Evasive Linux Backdoor Technical Deep-Dive," 2022, (https://sandflysecurity.com/blog/bpfdoor-an-evasive-linux-backdoor-technical-analysis/).

[5] The BlackBerry Research & Intelligence Team and Inteze0r. "Symbiote: A New, Nearly-Impossible-to-Detect Linux Threat," 2022, (https://blogs.blackberry.com/en/2022/06/symbiote-a-new-nearly-impossible-to-detect-linux-threat).

[6] Y. Wang, D. Li, and L. Chen, "Seeing the Invisible: Auditing eBPF Programs in Hypervisor with HyperBee," In Proceedings of the 1st Workshop on eBPF and Kernel Extensions, pp.28- 34.

[7] Z. Chen, H. Kong, S. Ding and W. Guo, "Efficient DDoS Detection and Mitigation in Cloud Data Centers Using eBPF and XDP," Security and Privacy in Computing and Communications (TrustCom '24), Melbourne, Australia, Dec. 2024, pp. 1869- 1874.