Storm Chaser: O-RAN에서 Signaling Storm DoS를 차단하는 eBPF/XDP 기반 보안 프레임워크

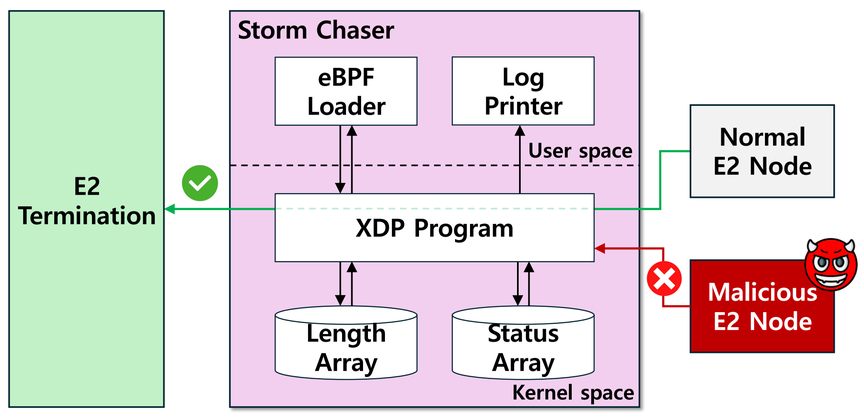
Storm Chaser: eBPF/XDP-based Security Framework to Defeat Signaling Storm DoS in O-RAN

Incheon National University, **Hyeonmoon Kim, Seungsoo Lee**

초 록

- 차세대 RAN 구조로 떠오르고 있는 Open RAN의 표준화를 위해 O-RAN Alliance는 O-RAN 구조를 제안.
- O-RAN은 개방형, 지능형 무선 접속망 개발을 촉진하고 있는 동시에, 공격 표면의 확장으로 새로운 보안 위협이 발생하는 중임.
- 본 논문은 O-RAN 구조에서 E2 Interface를 통해 통신하는 E2 Termination과 E2 Node간에서 발생할 수 있는 Signaling Storm DoS Attack에 대해 소개하고 이를 막기위해 eBPF/XDP를 활용한 보안 프레임워크인 Storm Chaser를 제안.
- Storm Chaser가 악성 RIC Indication Message를 담은 패킷을 효과적으로 차단하는 것을 실험을 통해 확인함.

디자인



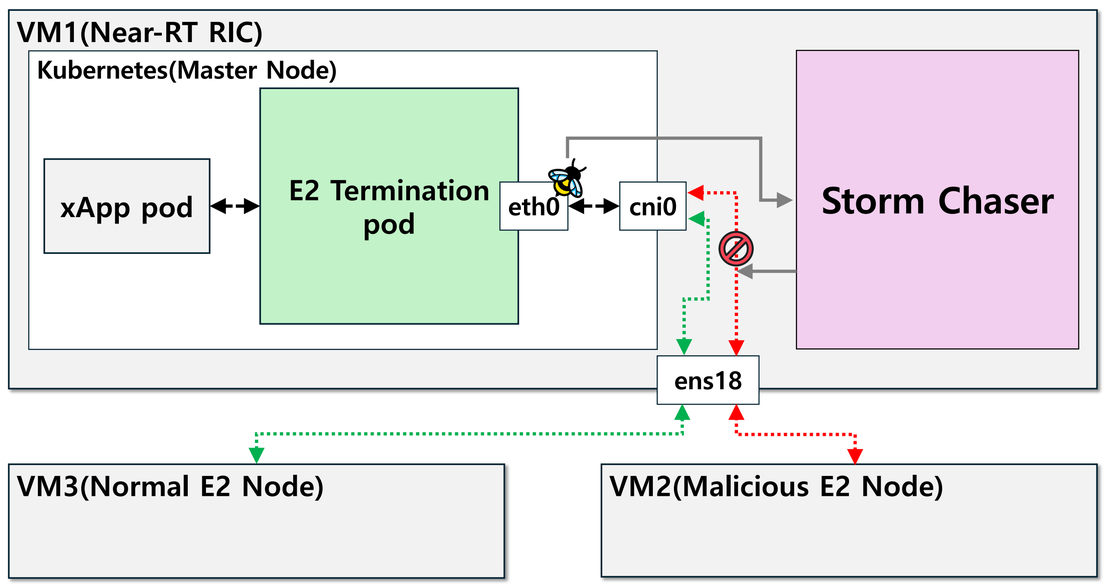
- eBPF Loader가 XDP Program과 eBPF Map을 커널로 로드.
- E2 Node로부터 트래픽이 전송되어 XDP Hook을 트리거
- 패킷 사이즈 기반 필터링 알고리즘을 통해 정상 패킷은 PASS
- 비정상 크기의 패킷을 지속적으로 보내는 E2 Node는 차단

Algorithm 1: Pseudo-code for traffic filtering

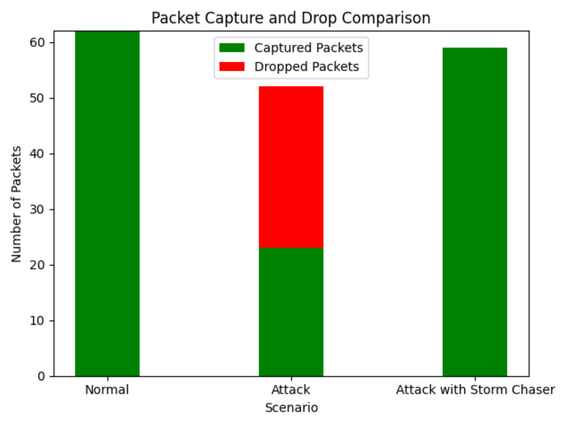
```
Input: xdp_md *ctx
Output: XDP_PASS or XDP_DROP
#1 Check 4-layer protocol
ip_header ← ctx.data + sizeof(ETH_header);
if ip_header.protocol ≠ sctp then
    return XDP_PASS;
#2 Check blacklist
if ip, port in blacklist_arr.address then
    if blacklist_arr.count > 5 then
        return XDP_DROP
#3 Check array is full
is_full ← status_arr[2];
if !is_full then
    go to #5;
#4 Check packet size
packet_length ← ctx.data_end - ctx.data;
avg ← status_arr[1];
if packet_length > avg + THRESHOLD then
    update blacklist_arr.count;
    return XDP_PASS;
#5 Update array
idx ← status_arr[0];
length_array[idx] ← packet_length;
avg ← new_avg;
status_arr ← idx, avg, is_full;
update status_arr & length_arr;
return XDP_PASS;
```

1) IP Header가 SCTP 프로토콜을 사용하지 않으면 패킷을 PASS
2) IP, Port 번호가 blacklist에 등록되어 있고 count가 5 이상이면 패킷을 DROP
3) Status Array가 가득 차지 않았으면(패킷 사이즈의 임계값이 정해지지 않았으면) #5 수행
4) 패킷의 크기가 임계값보다 크면 balcklist_arr에서 count값을 1 올리고 패스
5) 새로 들어온 정상 패킷의 값으로 status array의 값을 최신화

환경 구성 및 평가



- 5GSEC 에서 제공하는 O-RAN 환경 구축 가이드를 참고하여 구축
- 가상머신 3대로 Near-RT RIC과 2개의 가상 E2 Node를 구현




```
01:02:08.612081 IP (tos 0x2,ECT(0),  proto SCTP (132), length 452)
01:02:09.612098 IP (tos 0x2,ECT(0),  proto SCTP (132), length 452)
01:02:10.612129 IP (tos 0x2,ECT(0),  proto SCTP (132), length 452)
01:02:11.612091 IP (tos 0x2,ECT(0),  proto SCTP (132), length 452)
01:02:12.612119 IP (tos 0x2,ECT(0),  proto SCTP (132), length 452)
01:02:22.629122 IP (tos 0x2,ECT(0),  proto SCTP (132), length 452)
01:02:48.612093 IP (tos 0x2,ECT(0),  proto SCTP (132), length 452)
01:02:48.612468 IP (tos 0x2,ECT(0),  proto SCTP (132), length 452)
01:02:49.612125 IP (tos 0x2,ECT(0),  proto SCTP (132), length 452)
```

- 공격으로 인해 패킷이 정상적으로 캡처되지 않음

```
2024/11/05 04:19:51 Waiting for events..
2024/11/05 04:20:22 [INFO] Malicious Address Banned!
        Size : 1374
        Source : 163.0.17.172:46758
```

- 공격으로 감지되는 패킷을 보낸 Source를 차단

- 기존의 정상 E2 Message를 수신할 때와 공격이 진행 됐을 때, 공격 상황에서 Storm Chaser를 작동했을 때 패킷 캡처 결과
- 공격 상황에서 절반 이상의 패킷이 제대로 수신되지 못했음.
- 정상 메시지를 수신할 때와 Storm Chaser를 작동했을 때 결과를 비교해봤을 때 Storm Chaser가 공격을 충분히 잘 방어함을 확인.

결 론

- 본 연구가 제안하는 Storm Chaser를 통해 O-RAN 환경에서도 eBPF/XDP 프로그램으로 보안성을 높힐 수 있음을 확인했음.
- 최근 연구에서 xApp의 권한이 과도하여 문제가 될 수 있다는 내용이 있었음.
- 이를 바탕으로 향후 연구로 공격 표현을 조금 더 확장하여 악성 xApp에서 E2 Termination과 E2 Node의 취약점에 대해 조사하고 이에 대한 eBPF를 활용한 보안 프레임워크를 개발하는 연구를 진행할 예정임.