P4 기반의 라우팅 경로 난독화 및 자원 고갈 공격 완화

김수연[1], 박태준[2]
[1]전남대학교 정보보안융합학과 석사과정
[2]전남대학교 인공지능학부 교수
rlatndus6205@jnu.ac.kr, taejune.park@jnu.ac.kr

P4-based routing path obfuscation and resource exhaustion attack mitigation

SooYeon Kim[1], Taejune Park[2]
[1]Dept. of Information Security Convergence, Chonnam National University
[2]Dept. of Artificial Intelligence, Chonnam National University

요 약

네트워크를 대상으로 하는 공격자는 네트워크 트래픽을 분석하고 이를 통해 네트워크 토폴로지를 추론하고 Link Flooding이나 DoS와 같은 공격을 수행한다. 본 논문에서는 이러한 공격에 대응하기 위해 P4 기반의 새로운 라우팅 경로 난독화 알고리즘을 제안한다. 이 알고리즘 방식은 네트워크 중간에 배치된 P4 스위치에서 패킷 포워딩 시 다음 홉을 무작위로 선택하여 라우팅 경로를 난독화함으로써 공격자가 라우팅 경로나 네트워크 토폴로지를 파악하는 것을 어렵게 한다. 또한, P4를 통해 몇 가지 변수를 정의함으로써 패킷이 네트워크에서 무한 루프에 빠지는 것을 방지하고 목적지에 도달하는 것을 보장한다. 더불어, 이러한 무작위 포워딩은 대규모 트래픽 공격이 발생했을 시 트래픽을 분산시켜 네트워크 자원 고갈 공격의 영향을 완화하는 효과를 가진다. 또한, 본 논문은 P4의 프로그래밍 가능성을 통한 유연한 난독화 가능성을 제시한다.

1. 서론

현대 사회에서 네트워크는 금융, 교육, 의료, 국방 등 다양한 디지털 인프라의 핵심 요소이다. 그러나, 네트워크의 사용이 증가함과 동시에 이를 대상으로 하는 공격 또한 규모가 증가하고 복잡해지고 있다. 네트워크 공격자들은 공격을 본격적으로 수행하기 전에 네트워크 포트/취약점 스캐닝을 통해 공격 대상을 분석하고 공격 벡터를 설정한다. 심지어, traceroute와 같은 기본적인 명령어를 통해 패킷의 경로를 추적하여 라우팅 경로나 네트워크 토폴로지를 추론하고 이를 통해 최적의 공격 경로를 탐색할 수 있다[1]. 이러한 탐색은 방화벽이나 침입 탐지 시스템과 같은 보안 장비를 우회하는 경로를 찾거나 보안 장비 자체의 취약점을 이용해 공격을 시도하는 것까지 이어질 수 있다. 더욱 심각한 문제는 공격자가 라우팅 경로 및 네트워크 토폴로지 분석을 통해 네트워크에서 중요한 역할을 수행하는 스위치나 라우터를 파악하고 이들을 대상으로, 또는 이들을 활용하여 공격을 수행할 수 있다는 것이다. 특히, 중요한 스위치나 라우터를 대상으로 하는 Link Flooding 공격이나 DoS 공격의 경우 네트워크의 링크나 이러한 중요한 장비와 같은 자원을 고갈시켜 서비스가 중단되는 심각한 결과를 초래할 수 있다.

Link Flooding 및 DoS 공격은 네트워크 자원을 고갈시켜 정상적인 서비스 이용을 방해하는 공격이다[2]. 이러한 공격들은 단시간에 막대한 양의 트래픽을 특정 대상이나 네트워크 링크에 집중시켜 네트워크의 가용성을 저하시키거나 네트워크 서비스 자체를 마비시킬 수 있다. 이러한 상황에서, 공격자가 네트워크 토폴로지 정보를 활용하여 공격 경로를 최적화할 경우, 공격에 대응하는 것은 더 어려워진다.

본 논문에서는 기존의 네트워크 난독화 방식의 한계를 극복하고, 라우팅 경로나 네트워크 토폴로지 정보 노출로 인해 발생하는 보안 취약점을 해결하기 위해 트래픽을 분산하는 방식을 활용한다. 구체적으로, 네트워크 스위치 수준에서 패킷의 라우팅 경로를 무작위로 선택하여 공격자가 네트워크를 파악하는 것을 어렵게 하고, 대규모 트래픽이 발생했을시 트래픽을 분산시켜 Link Flooding 및 DoS 공격을 완화하는 접근법을 제안한다.

2. 배경지식

1) P4

기존의 네트워크 스위치나 라우터는 하드웨어 공급업체에서 제공하는 고정된 기능에 의존하며, 네트워크 환경의 변화나 새로운 요구사항에 유연하게 대응하기 어렵다. 이는 네트워크 운영자가 새로운 기능을 추가하고자 하거나, 예상치 못한 문제가 발생했을 경우 신속하게 대응하기 어렵다는 한계로 이어진다.

이러한 한계를 극복하고 네트워크의 유연성과 프로그래밍 가능성을 향상시키기 위해 P4(Programming Protocol-independent Packet Processors)[3]가 등장했다. P4는 특정 프로토콜에 종속되지 않고 네트워크 장비의 패킷 처리 방식을 정의할 수 있는 언어이다. P4를 통해 네트워크 관리자는 하드웨어에 종속되지 않고 데이터평면에 패킷 처리 로직을 자유롭게 구현하고 적용할 수 있다. 이는 네트워크 관리자가 변화하는 네트워크 환경에 유연하게 대처할 수 있게 해준다. 또한, 새로운 헤더 필드를 정의하고 이를 패킷 처리에 활용할 수 있으므로 네트워크 모니터링이나 포워딩 설정과 같은 다양한 네트워크 서비스를 구현할 수 있게 한다.

2) 난독화

네트워크 난독화는 공격자가 네트워크 트래픽을 분석하여 얻을 수 있는 민감한 정보를 숨겨 공격을 방해하는 보안 기술이다. 네트워크 트래픽은 통신하는 주체, 전송되는 데이터의 종류와 양, 통신 패턴 등 다양한 정보를 포함하며, 공격자는 이를 분석하여 사용자의 활동을 추적하고 취약점을 식별할 수 있다. 따라서, 네트워크 트래픽 자체를 난독화하여 공격자의 정보 수집을 방해하는 난독화 기술이 등장하였다. 대표적인 난독화 기법으로는 패킷 크기 난독화와 트래픽 경로 난독화 등이 있다.

패킷 크기 난독화는 네트워크를 통해 전송되는 패킷의 크기 정보를 숨기거나 무작위화하는 기술이다. 패킷의 크기는 이용하고 있는 서비스의 종류나 데이터 특성에 대한 단서를 제공할 수 있으므로, 공격자가 이를 분석하여 정보를 추론하는 것을 방지하기 위해 패킷 크기 정규화, 랜덤 패딩 등을 사용한다.

트래픽 경로 난독화는 패킷의 이동 경로를 복잡하게 만들거나 공격자가 추적하기 어렵게 하는 기술이다. 공격자는 traceroute 등의 명령어를 통해 패킷의 경로를 파악하고 네트워크 토폴로지 추론, 보안 장비 위치 확인, 잠재적인 공격 지점 식별 등 다양한 작업을 수행할 수 있다. 트래픽 경로 난독화는 경로 우회, 믹스 네트워크, 네트워크 토폴로지 가상화 등을 통해 공격자가 네트워크에 대한 정보를 수집하는 것을 방해한다.

3. 관련 연구

네트워크 공격자가 사용자의 활동을 추적하고 네트워크에 대한 정보를 수집하는 것을 방해하기 위해 여러 네트워크 난독화 연구가 진행되어 왔다. 특히, 데이터평면에서 패킷 처리 방식을 직접 정의할 수 있는 P4를 활용한 네트워크 난독화 기법은 P4의 유연성을 바탕으로 기존의 난독화 기법을 개선하거나 새로운 난독화 방식을 설계할 수 있다는 점에서 활발히 연구되고 있다.

Datta 등이 제안한 SPINE[4]은 트래픽이 신뢰할 수 없는 중간 네트워크를 통과하는 동안 실제 출발지/목적지 IP와 TCP 순서 번호 등 관련 필드를 암호화하여 숨기는 시스템이다. 이를 통해 고속으로 네트워크 트래픽 정보를 숨길 수 있다.

Meier 등이 제안한 Ditto[5]는 P4로 프로그래밍 가능한 스위치를 활용하여 WAN 환경에서 라인 레이트로 동작하는 트래픽 분석 방지 시스템이다. Ditto는 패킷 버퍼링, 패딩, 채프 패킷 삽입의 세 가지 주요 연산을 통해 트래픽을 정해진 패턴에 맞춰 내보냄으로써 난독화를 수행하여 공격자가 패킷의 크기, 패킷 간 시간 간격을 알 수 없게 한다.

기존 연구인 SPINE과 Ditto는 네트워크 난독화를 통해 공격자가 사용자 또는 네트워크에 대한 정보 수집을 방해하는 효과적인 방법들을 제시하였다. 허나, SPINE과 Ditto는 Link Flooding이나 DoS 공격과 같이 네트워크에 대규모 트래픽이 한꺼번에 유입되는 상황에서는 대응이 어렵다는 한계가 있다. 이러한 상황에서는 난독화 기법만으로는 네트워크의 가용성을 보장하기 어려우며, 과도한 트래픽은 난독화된 경로를 포함한 네트워크 전체를 마비시킬 수 있고, 나아가 정상적인 서비스 제공을 방해하는 문제가 발생할 수 있다.

본 연구는 이러한 한계점을 인식하고, 네트워크 라우팅 경로 난독화와 동시에 대규모 트래픽 공격에 대한 완화 기능을 통합적으로 제공하는 새로운 알고리즘을 제안한다. 본 논문에서 제안하는 P4 기반의 라우팅 경로 난독화 알고리즘은 P4 스위치에서 패킷 포워딩을 무작위로 수행하여 라우팅 경로를 난독화할 뿐만 아니라, 트래픽을 네트워크 내 여러 경로로 분산시켜 Link Flooding이나 DoS 공격으로 인한 네트워크 마비를 방지한다. 이는 공격자가 네트워크 정보를 획득하는 것을 어렵게 하는 동시에, 네트워크의 안정성과 가용성을 향상시키는 데 기여한다.

4. 접근법

본 섹션에서는 앞서 언급한 네트워크 공격의 위협과 기존 난독화 기술의 한계를 극복하기 위한 새로운 접근법을 제시한다. 구체적으로, 라우팅 경로에 대한 정보 노출을 방지하고 네트워크 자원 고갈 공격에 효과적으로 대응하기 위해 P4를 활용한 새로운 패킷 라우팅 경로 난독화 알고리즘을 제안한다. 제안하는 알고리즘은 P4의 프로그래밍 가능성을 활용하여 데이터평면에서 패킷 포워딩 경로를 동적으로 난독화하고, 트래픽을 분산시키는 것을 목표로 한다.

1) P4 기반 랜덤 포워딩

P4 기반 난독화의 가장 큰 특징은 네트워크 중간에 위치한 P4 스위치에서 패킷의 출력 포트를 무작위로 선택하여 포워딩하는 메커니즘이다. 기존의 방식과 달리 본 방식은 각 스위치에서 패킷을 포워딩할 때 미리 결정된 고정된 출력 포트로 포워딩하는 것이 아니라, 여러 개의 가능한 출력 포트 중에서 하나를 무작위로 선택한다.

네트워크 트래픽이 P4 스위치로 들어오면, 스위치는 우선 수신된 패킷의 목적지를 확인한다. 이후, 이를 기반으로 사전에 설정된 Match-Action Table을 참조하여 해당 패킷을 포워딩할 수 있는 가능한 출력 포트들의 집합을 파악한다. 이후, 이 출력 포트 집합에서 하나의 출력 포트를 무작위로 선택하여 패킷을 포워딩한다.

이러한 스위치 수준에서의 랜덤 포워딩은 공격자가 traceroute 등의 명령어를 사용하여 패킷의 이동 경로를 추적 및 예측하는 것을 어렵게 만든다. 패킷이 매번 다른 경로를 통해 목적지에 도달할 수 있으므로, 공격자는 네트워크 토폴로지를 정확하게 파악하고 경로 분석을 통해 공격 전략을 세우는 것이 복잡해진다.

2) 가중치 기반 루프 방지

단순히 각 스위치에서 무작위로 패킷을 포워딩할 경우, 패킷이 네트워크 내에서 무한 루프에 빠지거나 최종 목적지까지 도달하지 못하는 상황이 발생할 수 있다. 이를 방지하기 위해 본 연구에서는 네트워크 내 각 P4 스위치에 가중치를 부여하며, 목적지와 가까운 스위치일수록 높은 가중치를 부여한다. 기본적인 포워딩 흐름은 패킷이 가중치가 높은 스위치로 포워딩되도록 함으로써 패킷이 목적지 방향으로 포워딩되도록 하는 것이다.

그러나 라우팅 경로 난독화를 달성하기 위해, 본 알고리즘에서는 패킷이 가중치가 낮은 스위치로도 포워딩될 수 있도록 한다. 이러한 상황에서 패킷이 무한 루프에 빠지는 것을 방지하기 위해 일정한 임계값을 설정하고 이 임계값 범위 내에서만 패킷이 가중치가 낮은 스위치로도 포워딩될 수 있도록 한다. 이를 통해, 패킷의 라우팅 경로에 예측 불가능성을 추가함으로써 난독화를 효율적으로 진행하며, 패킷이 무한 루프에 빠지는 상황을 방지하고 목적지까지 도달하는 것을 보장한다.

3) 잘못된 경로 처리

본 난독화 알고리즘은 스위치가 패킷의 목적지로 향하는 유효한 다음 홉을 결정할 수 없는 상황, 즉 '잘못된 경로'에 대한 직면했을 때, 패킷을 어떻게 처리할지에 대한 절차를 포함한다.

만약 스위치가 패킷을 목적지로 보낼 수 없는 적절한 다음 홉을 찾지 못하면, 스위치는 해당 패킷의 헤더에 잘못된 경로와 관련된 플래그 값을 설정하고 패킷을 스위치로 들어왔던 입력 포트로 되돌려보낸다. 이 잘못된 경로 플래그가 설정된 패킷을 수신한 다음 스위치는 패킷이 들어왔던 포트, 즉 잘못된 경로를 제외한 다른 가능한 포트 중 하나를 무작위로 선택하여 패킷을 포워딩한다. 이러한 매커니즘은 패킷이 막다른 경로에 갇히는 것을 방지하고 예측 불가능한 경로를 추가하여 공격자가 라우팅 경로를 추적하고 네트워크 토폴로지를 추론하는 것을 더욱 어렵게 만드는 난독화 효과도 제공한다.

4) 난독화 수준 조절

이 알고리즘은 또한, 추가 난독화 플래그를 통해 네트워크 환경의 변화나 특정 공격에 대응하여 난독화의 수준을 조절할 수 있는 유연성을 제공한다. P4 스위치는 패킷의 추가 난독화 플래그를 확인하여 패킷이 잘못된 경로로 포워딩되는 상황에서도 의도적으로 더 많은 중간 노드를 거칠 수 있게 한다. 이러한 과정에서 이전과 마찬가지로 무한루프에 빠지는 것을 방지하고 최종 목적지에 도달하는 것을 보장하기 위해 임계값을 추가로 설정한다.

이 기능을 활성화하면, 목적지로 향하는 경로가 없더라도 사전에 설정한 임계값에 도달하기 전까지는 무작위로 선택된 경로를 따라 패킷을 포워딩하여 난독화 정도를 극대화할 수 있다. 이후, 임계값에 도달하면 패킷을 더 이상 무작위로 포워딩하지 않고 되돌려보내는 방식을 활용해 목적지로 향하는 경로가 있는 스위치로 패킷을 포워딩한다.

이는 공격자의 트래픽 분석을 더욱 복잡하게 만들고, 실제 네트워크 토폴로지를 파악하는 것을 어렵게 해 공격에 필요한 비용을 높이는데 기여한다.

5) Match-Action Table

네트워크 관리자는 P4 언어를 활용하여 앞서 언급한 임계값과 같은 변수나 '잘못된 경로' 및 '추가 난독화' 플래그 값을 사전에 설정할 수 있다.

패킷이 P4 스위치로 들어오면 패킷의 헤더에 저장되어 있는 변수와 플래그 값을 추출하고 이 값을 미리 설정된 값들과 비교함으로써 해당 패킷에 적용할 적절한 포워딩 테이블을 선택한다. 각 포워딩 테이블은 P4에서 제공하는 Match-Action Table 형태로 구성되며, 가중치나 잘못된 경로 플래그와 같은 패킷의 특성을 기반으로 수행해야 할 Action을 정의한다. 이러한 Action은 패킷을 포워딩할 수 있는 가능한 출력 포트 집합에서 무작위로 하나의 출력 포트를 결정하는 작업을 수행하며, 각각의 포워딩 테이블은 가능한 출력 포트 집합의 차이가 있다. 예를 들어 패킷이 가중치가 작은 스위치로 이동할 수 있는 임계값을 초과한 경우, 해당 패킷은 더 이상 가중치가 작은 스위치로는 전달될 수 없으며, 반드시 가중치가 더 큰 스위치로만 포워딩되어야 한다.

이와 같이, 다양한 조건과 규칙들을 P4의 Match-Action Table에 정의하고, 패킷 포워딩 과정을 정밀하게 제어함으로써 라우팅 경로 난독화를 효율적으로 수행하며, 패킷이 목적지까지 반드시 도달할 수 있게끔 하여 네트워크의 안정성과 신뢰성을 유지한다.

6) 트래픽 분산을 통한 자원 고갈 공격 완화

본 논문에서 제안하는 알고리즘은 라우팅 경로를 난독화하는 주요 목표 외에도, Link Flooding이나 DoS와 같은 네트워크 자원 고갈 공격에 대한 효과적인 완화 전략을 제공할 수 있다. 네트워크에 막대한 양의 트래픽이 단시간에 유입되는 공격 상황이 발생했을 경우, 각 P4 스위치는 단순히 해당 트래픽을 사전에 설정된 단일 경로로만 포워딩하지 않고 가능한 여러 출력 포트 중에서 하나를 무작위로 선택하여 포워딩한다. 이는 네트워크 트래픽을 분산시켜 특정 스위치나 경로에만 트래픽이 집중되어 과부하가 생기는 것을 방지하여 전반적인 네트워크 가용성을 유지하는데 기여한다.

5. 결론

본 논문에서는 Link Flooding이나 DoS와 같은 공격에 대한 효과적인 대응 방안으로 P4 기반의 라우팅 경로 난독화 알고리즘을 제안하였다. 이 알고리즘은 P4 스위치에서 패킷의 포워딩 경로를 무작위로 선택함으로써 공격자가 네트워크 토폴로지 정보를 수집하는 것을 어렵게 만든다. 또한, 이러한 무작위 포워딩 방식은 대규모 트래픽이 네트워크로 유입되었을 경우 트래픽을 네트워크 내 여러 경로로 분산시켜 특정 스위치나 링크가 과부화되는 것을 방지하고, 네트워크 자원 고갈 공격의 영향을 완화할 수 있다.

본 연구는 P4를 활용하여 네트워크의 데이터평면에서 패킷의 포워딩 경로를 능동적으로 난독화하는 새로운 접근 방식을 제시했다는 점에서 의의를 가진다. 향후 연구에서는 시뮬레이션 및 실제 네트워크 환경에서 프로토타입을 구현하여 본 알고리즘의 실제 성능을 측정하고자 한다. 또한, P4의 프로그래밍 가능성을 활용하여 다양한 네트워크 환경 및 공격 시나리오에 대한 적응성을 향상시키는 방향으로 연구를 진행하고자 한다. 이를 통해, 공격자가 네트워크에 대한 정보를 수집하는 것을 방해하여, 네트워크 안정성 및 안전성에 기여하고자 한다.

Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 인공지능융합혁신인재양성사업(IITP-2023-RS-2023-00256629) 및 대학ICT연구센터사업(IITP-2024-RS-2024-00437718)의 연구결과로 수행되었음.

참고문헌

[1] Jajodia, Sushil, Steven Noel, and Brian O'berry. "Topological analysis of network attack vulnerability." Managing Cyber Threats: Issues, Approaches, and Challenges (2005): 247-266.

[2] Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." IEEE communications surveys & tutorials 15.4 (2013): 2046-2069.

[3] Bosshart, Pat, et al. "P4: Programming protocol-independent packet processors." ACM SIGCOMM Computer Communication Review 44.3 (2014): 87-95.

[4] Datta, Trisha, et al. "{spine}: Surveillance protection in the network elements." 9th USENIX Workshop on Free and Open Communications on the Internet (FOCI 19). 2019.

[5] Meier, Roland, Vincent Lenders, and Laurent Vanbever. "ditto: WAN Traffic Obfuscation at Line Rate." NDSS. 2022.