제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

IP 역추적을 위한 Admission Packet Marking 기법

정세준*, 송주석*
*연세대학교 컴퓨터과학 · 산업시스템공학과
e-mail:{hooa,jssong}@emerald.yonsei.ac.kr*

Admission Packet Marking Scheme for IP Traceback

Se-Joon Jung*, Joo-Seok Song*
*Dept of Computer Science and Industrial System Engineering,
Yonsei University

요 약

최근 IP 역추적을 위한 다양한 연구가 진행되고 있다. 그 중 주목할 만한 역추적 시스템인 확률적 패킷 마킹 기법은 대량의 패킷을 필요로 하는 분산 서비스 거부 공격의 특징을 이용한 매우 효율적이고 실용적인 접근 방식이다. 그러나 이 방식은 모든 라우터의 수정이 불가피하다는 점과 공격을 당한 피해 시스템에서 완벽한 공격 경로를 재구성하기 위해 엄청난 부담을 짊어지게 되는 문제점을 드러냈다. 이러한 문제점에 대한 해결책으로 본 논문에서는 네트워크에 유입되는 패킷에 출발지 라우터의 주소만을 마킹하는 Admission Packet Marking 기법을 제안하고 기존 연구와의 비교 분석을 통해 기존 인터넷에의 적용 가능성을 판단한다.

1. 서론

서비스 거부 공격은 최근 가장 빈번하게 발생하는 공격 형태중의 하나로 시스템이나 네트워크의 자원을 고갈시킴으로써 더 이상의 서비스를 불가능하게 만드는 공격 방법이다.[1] 이러한 서비스 거부 공격은 구현하기는 쉬운 반면 방어가 어렵고 이를 역추적 하기는 더더욱 어렵다는 특징을 지니고 있다. 따라서, 서비스 거부 공격에 대한 최근의 연구는 주로 공격을 감내하는 데에 초점을 맞춰 진행되어 왔으나 이는 공격의 근원지를 차단하지 못해 잠재적으로 재 공격에 대한 가능성을 열어둘 수 있는 문제점을 가지고 있다.

서비스 거부 공격은 대부분 TCP/IP 프로토콜의 근본적인 취약점을 이용한 IP 스푸핑 기법을 사용하여 패킷의 출발지 주소를 위조하기 때문에 공격을 당한 피해 시스템에서는 직관적으로 공격의 근원지를 파악할 수 있는 방법이 없다. 물론 IP 역추적 문제점을 해결하기 위한 다양한 시도와 연구가 계속 진행되어 오고 있으나 시스템과 네트워크에 가중되는 막대한 오버헤드와 기존 인터넷 체계의 불가피한 변경 등이 해결해야 할 과제로 남아있다.

본 논문에서는 현재까지 제시되어 온 다양한 IP 역추적 기법들과 각각의 문제점들에 대해 살펴본 후 새롭게 제안하는 Admission Packet Marking 기법에 대해 설명하고 기존 연구와의 비교 및 분석을 행할 것이다.

2. 관련연구

2.1 Link testing

대부분의 IP 역추적 기법들은 피해 시스템으로부터 가장 근접한 라우터에서부터 시작하여 상위 라우터로의 링크를 반복적으로 테스트함으로써 공격 데이터의 흐름이 어떤 링크로부터 흘러왔는지를 식별하는 방식을 사용한다.

먼저 라우터의 input debugging을 이용하여 근원지를 역추적 하는 방식은 피해 시스템으로부터 생성된 attack signature를 네트워크 관리자가 상위 라우터에 설치하여 해당 공격 패킷들이 어떤 포트로 유

입되는지를 파악하는 방식이다. 이와 같은 과정은 상위 라우터에 반복적으로 적용되어 결국 공격자의 대략적인 위치를 파악할 수 있게 된다.[2]

그러나 이 방식에는 네트워크 관리자의 상당한 관리 부담이 뒤따르게 되며 ISP간의 긴밀한 협조가 필요하다는 단점이 있다.[3]

다음으로 Burch와 Cheswick이 제안한 Controlled flooding 방식은 서비스 거부 공격이 행해지고 있는 동안 피해 시스템에서 상위의 모든 링크에 대량의 트래픽을 발생시켜 이로 인한 공격 데이터의 변화를 주시함으로써 어떤 링크가 공격 데이터의 유입 경로로 사용되었는지를 파악하는 방법을 이용한다.[4]

이 방식의 가장 큰 문제점은 역추적 자체가 서비스 거부 공격이 될 수 있다는 것이다.

위에 언급된 두 가지 Ling testing 방식은 모두 서비스 거부 공격이 행해지고 있는 동안에만 역추적이 가능하다는 한계점 또한 가지고 있다.

2.2 Logging

IP 역추적을 위한 또 다른 접근 방식은 각 라우터에서 자신을 거쳐가는 패킷들에 대한 기록을 유지하는 것이다. 이 방식은 공격이 완료된 이후에도 그 근원지를 추적할 수 있다는 특징이 있으나 패킷 기록을 위한 막대한 저장 공간이 라우터에 필요하다는 점과 라우터간의 데이터 통합 문제를 해결해야 하는 부담이 있다.[5]

2.3 Packet Marking

IP 역추적에 관한 최근의 연구에서 가장 각광받고 있는 방식 중의 하나인 패킷 마킹 기법은 라우터를 거쳐가는 패킷에 해당 라우터의 주소 혹은 라우터간의 경로를 마킹하여 피해 시스템에서 이를 이용하여 공격 경로를 재구성하는 방법이다.[6]

2.3.1 Node append

가장 간단한 패킷 마킹 기법으로 공격 시스템에서 피해 시스템까지의 경로 상에 있는 라우터들이 패킷의 끝에 자신의 주소를 계속적으로 추가하는 방식이다. 이 방식을 사용하면 피해 시스템에서는 경로를 재구성 할 필요 없이 근원지를 파악할 수 있고 단 하나의 패킷만으로도 전송 경로를 알아낼 수 있다는 장점이 있다. 그러나 전송 경로 상의 모든 라우터가 마킹에 참여해야 하므로 높은 오버헤드가 뒤따르게 되며 누적되는 경로 데이터로 인해 패킷의 크기가 비대해지는 단점 또한 존재한다.

2.3.2 Node sampling

라우터의 오버헤드를 줄이고 패킷의 경로 저장 공간을 최소화하기 위하여 한번에 하나의 노드만 표본화하는 방식이다. 서비스 거부 공격에 이용되는 패킷의 양이 충분히 많다고 가정하면, 각 라우터에서 확률 p에 따라 패킷의 노드 필드에 자신의 주소를 기입하는 것만으로도 추후 피해 시스템에서 이를 이용하여 공격 경로를 재구성할 수 있다는 접근 방식이다.

이 알고리즘은 구현하기에 용이한 반면 두 가지의 심각한 결점을 안고 있다. 첫째, 샘플의 분포로 모든 라우터의 순서를 매기는 작업이 많은 시간을 필요로 하며 둘째, 분산 서비스 공격이 행해진 경우에는 같은 거리를 갖는 수많은 라우터들이 존재하게 된다. 따라서 이 방식은 여러 근원지를 가지는 서비스 거부 공격에는 취약하다고 할 수 있다.

2.3.3 Edge sampling

위와 같은 문제를 해결하기 위해 특정 노드의 주소 대신 공격 경로 상에 있는 edge들을 기입하는 방식이다. 이 방식은 시작 라우터를 나타내는 start, 끝 라우터를 나타내는 end, 그리고 각 edge가 피해 시스템으로부터 얼마나 떨어졌는지를 나타내는 distance 필드의 조합을 이용하여 피해 시스템에서 일련의 처리과정을 거쳐 경로를 재구성하게 된다.

이 방식 역시 IP 패킷 헤더에 추가의 저장 공간이 필요하게 되어 기존 인터넷 체계와 호환되지 않는 한계가 있었으나 최근 근래에는 거의 사용되지 않는 IP identification 필드를 이용하여 효율적으로 마킹이 가능한 수정된 Edge sampling 기법이 소개되기도 했다.

하지만 다양한 연구 결과에서 보여지듯이 이 방식 또한 피해 시스템에서의 경로 재구성 시 막대한 계산량이 필요하며 마킹에 참여하는 라우터에 대한 인증 기법이 없다는 한계를 가진다.[7]

3. Admission Packet Marking 기법

3.1 배경

최근까지 연구된 대부분의 패킷 마킹 기법들은 공격에 이용된 패킷의 전송 경로를 완전히 재구성하는 것을 목표로 하고 있다. 이로 인해 기존 인터넷

에 산재해 있는 거의 모든 라우터들이 마킹에 참여하게 되어 전체 네트워크에 막대한 오버헤드를 가중시킬 수 있으며 또한 피해 시스템은 공격 경로 재구성이라는 또 하나의 임무를 떠 안게 되는 문제점이 나타났다.

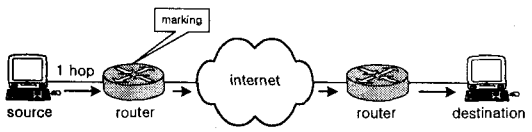
3.2 가정

패킷 마킹 시스템에서는 여러 가지 상황에 따라 다양한 고려 사항이 존재할 수 있으므로 다음과 같이 기본적인 사항을 가정하기로 한다.

- 공격자는 어떠한 패킷이든 생성할 수 있다.
- 공격자는 하나 이상일 수 있다.
- 공격자는 자신이 추적 당할 수 있다는 사실을 알고 있다.
- 공격자는 하나 또는 그 이상의 패킷을 보낼 수 있다.
- 마킹에 참여하는 라우터는 안전하다.
- 마킹에 참여하는 라우터는 올바르게 설정되어 있다.

3.3 개요

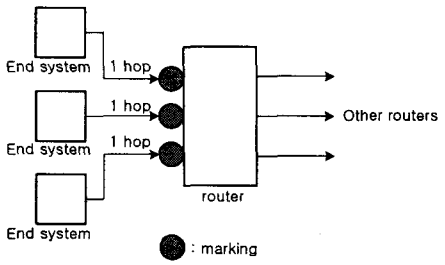
Admission Packet Marking 기법의 핵심은 네트워크의 경계선상에서 네트워크에 진입하려는 모든 패킷에 신뢰할 수 있는 라우터의 주소를 기입하는 것이다. 즉, 공격자에 의해 위조될 가능성이 있는 소스 IP 주소와는 별개로 해당 패킷이 첫 번째로 거치는 라우터에서 자신의 IP 주소를 마킹하여 추후 피해 시스템에서 공격자와 가장 근접한 라우터를 알 수 있게 되는 것이다.



[그림 1] Admission Packet Marking 기법

3.4 마킹 라우터 설정

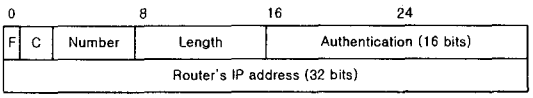
마킹에 참여하는 라우터는 개념적으로 네트워크의 진입로가 되어야 하므로 단말 시스템들과 직접적으로 연결되어 있는, 즉 단말 시스템들로부터 1 hop 거리에 있는 라우터이어야 한다. 또한 단말 시스템들로부터 외부 네트워크로 흘러나가는 패킷에 대해서만 마킹이 되어야 하므로 마킹 기능은 단말 시스템들과 연결되어 있는 입력포트 쪽에 설치되어 활성화되어야 한다. 이와 같은 모든 과정은 네트워크 관리자에 의해 이루어지는데 라우터의 설정 변경은 네트워크의 초기 설치 시와 변경 시에만 적용되므로 관리에 따르는 부담은 그다지 크지 않을 것으로 여겨진다.



[그림 2] 마킹 라우터 설정

3.5 마킹 필드

기존의 패킷 마킹 기법은 대부분 IP 헤더의 IP identification 필드를 마킹 필드로 이용하였다. 이는 근래에 IP fragmentation의 빈도가 낮음을 이용한 것으로 확률적 마킹 기법에서는 Do not fragment 플래그를 세팅함으로써 가능하였다.[6] 그러나 Admission Packet Marking 기법은 확률적 마킹이 아닌 관계로 identification 필드를 이용할 경우, 즉 Do not fragment 플래그를 세팅할 경우 만약 전송 경로 중 fragmentation 되어야 하는 부분이 있다면 해당 패킷은 손실될 수밖에 없다는 문제점이 있다. 따라서, 약간의 오버헤드를 감수하고 여기서는 IP의 option 필드를 이용하기로 한다.



[그림 3] IP option의 마킹 필드 포맷

위 option 포맷에서 볼 수 있듯이 모든 필드의 값은 이미 준비되어 있는 혹은 계산되어진 값들로 구성된다. 이것은 실제 마킹 시의 오버헤드를 최소한으로 줄이고자 의도된 것이기도 하다. 먼저 F, C, Number, Length 등은 각 필드에 해당하는 적절한 값을 선택해주면 되고 마킹 라우터의 IP 주소는 하단의 32 비트 공간에 들어가게 된다.[8] 마지막으로 authentication 필드에 관한 내용은 3.6에서 다루기로 한다.

3.6 인증

제안하는 시스템 역시 마킹 라우터 이후의 중간 라우터가 침해당했을 경우에는 공격자가 임의로 마킹 필드의 내용을 위조할 수 있는 잠재적인 가능성이 존재한다. 따라서, 마킹 필드에 대한 적절한 인증 메커니즘이 요구된다.

먼저 모든 마킹 라우터는 자신의 개인키와 공개키를 가지며 공개키는 인증된 공개 디렉토리에 저장되어 있다고 가정한다. 그리고 마킹 라우터는 자신의 IP 주소를 단방향 해시를 통해 결과값을 산출한 후 이를 자신의 개인키로 암호화하여 저장하고 있다. 패킷이 도착하면 마킹 라우터는 자신의 IP 주소를 마킹 필드에 적어넣고 저장되어 있던 해시값을 16비트의 authentication 필드에 복사한다. 패킷을 받은 시스템에서는 마킹 필드에 있는 IP 주소를 가진 라우터의 공개키를 공개 디렉토리로부터 얻은 후 이를 이용하여 암호화되어 있던 해시값을 도출한 후 자신이 해시한 값과 비교하여 인증 절차를 간단히 완료할 수 있다.

만약 공격자가 중간 라우터에서 마킹 필드에 있는 IP 주소를 위조하려 해도,

i) 위조하려는 IP 주소에 해당하는 공개키가 이미 인증된 디렉토리에 등록되어 있다면 그 공개키에 해당하는 개인키를 알 수 없어 실패할 것이며

ii) 위조하려는 IP 주소에 해당하는 공개키가 인증된 디렉토리에 등록되어 있지 않다면 새로운 키 쌍을 만들어 내야하고 이 중 공개키가 인증된 디렉토리에 저장되어 있어야 하는데 그렇지 못하므로 실패하게 된다.

4. 비교 분석

제안하는 Admission Packet Marking 기법은 기존 연구와 비교하여 다음과 같은 장점을 가진다.

- Link testing과 Logging에 비해 패킷 마킹 기법이 가지는 모든 장점을 그대로 수용한다.
- 전송 경로상의 중간 라우터들은 마킹에 참여하지 않으므로 수정이 불필요하며 따라서 기존 인터넷에의 실제적인 적용이 수월하다.
- 마킹에 참여하는 라우터마다 매번 확률 p를 계산해야 하는 오버헤드가 없다.
- 마킹 시 매번 행해져야 하는 XOR 연산과 해시 연산이 없으므로 이에 따른 오버헤드가 없다.
- 서비스 거부 공격뿐만이 아닌 궁극적으로 모든 패킷의 역추적이 가능해진다.
- 피해 시스템에서는 경로 재구성을 위한 복잡한 연산 및 이에 따른 오버헤드가 없다.

이와 같은 장점에도 불구하고 제안하는 시스템 역시 마킹 라우터에 모든 부하가 집중됨으로써 야기되는 라우터의 성능 감소와 전체적인 네트워크 통신 속도 저하라는 한계점을 가지고 있다. 그러나 이는 라우터의 하드웨어적인 성능 개선에 따라 충분히 수용 가능한 접근 방식이 될 수 있다고 생각한다.

5. 결론 및 향후 연구방향

본 논문에서는 IP 역추적을 위한 기존의 다양한 연구들과 각각의 문제점을 살펴본 후 이를 해결할 수 있는 Admission Packet Marking 기법을 제안하였다. 기존 인터넷에 점진적으로 배치 가능하고 피해 시스템에서의 경로 재구성 부담을 줄일 수 있는 역추적 시스템을 위해 네트워크의 경계선상의 라우터만이 마킹에 참여하는 이 기법은 마킹 라우터에 집중되는 부하만 적절히 처리 가능하다면 기존 네트워크에 충분히 적용 가능한 접근 방식이라고 하겠다.

참고문헌

[1] Kevin J. Houle, George M. Weaver "Trends in Denial of Service Attack Technology" October 2001.

[2] Robert Stone "CenterTrack: An IP Overlay Network for Tracking DoS Floods" October 1999.

[3] James Glave "Smurfing Cripples ISPs" Wired Technology News, January 1998.

[4] Hal Burch and Bill Cheswick "Tracing Anonymous Packets to Their Approximate Source" December 1999.

[5] Glenn Sager "Security Fun with OCxmon and cflowd" November 1998.

[6] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson "Practical Network Support for IP Traceback" August 2000.

[7] Kihong Park, Heejo Lee "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack"

[8] RFC 791 "Internet Protocol" September 1981