분산서비스 거부공격에 대응하기 위한 효과적인 패킷 마킹 기법

임희란° 홍만표
아주대학교, 인터넷 면역시스템 연구실
lhr5456@empal.com°, mphong@ajou.ac.kr

Effective Packet Marking Approach to Defend Against DDoS Attack

Heeran Lim° Manphyo Hong
Internet Immune System Laboratory, Ajou University

요 약

분산 서비스 거부 (DDoS) 공격에 대응 하기 위한 수 많은 연구 결과들이 나와 있지만, 이 공격은 여전히 인터넷 보안의 위협요소중 하나로 남아있다. 대부분의 분산 서비스 거부 (DDoS) 공격들은 스푸핑한 IP주소를 이용하여 다량의 패킷을 발생 시키기 때문에 정상 패킷과 공격 패킷 간의 구분을 어렵게 만든다. 이 공격에 대응하기 위해 기존에 나와있는 연구중 하나인 Pi는 패킷이 지나온 경로를 마킹하는 방법으로 간단하면서 강건한 대응 방법이었다. 하지만 Pi 마킹 방법은 여러가지 결점을 갖고 있다. 이 논문에서는 기존의 Pi가 갖고 있는 문제를 개선하기 위한 새로운 패킷 마킹 방법을 제시한다.

1. 서 론

분산 서비스 거부(DDoS) 공격은 인터넷 보안의 위협 요소 중 하나로 여전히 해결되지 못하고 있다. 이러한 공격을 시도하는 대부분의 공격자들은 다수의 좀비 호스트를 구성하고, 스푸핑한 IP 주소와 자동 공격툴(Tribal Flooding Network (TFN), TFN2K, Trinoo, and Stacheldraht 등)을 이용하여 다량의 패킷을 발생 시키기 때문에 정상 패킷과 공격 패킷 간의 구분를 어렵게 만들고 대응방법 또한 복잡하게 만든다. 분산 서비스 거부(DDoS) 공격의 일례로 2002년 10월 21일 인터넷 Domain Name Servers (DNS)[1]에 의해 사용되는 13개의 루트 서버가 공격을 당한 사례가 있었고, 2003년 1월 25일에는 슬래머[2]라 불리는 웜 바이러스가 취약한 호스트의 90%를 10분안에 감염 시키는 사례가 있었다. 지금까지 이러한 공격에 대응하기 위한 많은 연구들이 진행 되어 왔지만 여전히 뾰족한 해결책은 나오지 않고 있다.

분산 서비스 거부 (DDoS) 공격에 대응하기 위한 연구중 하나인 Pi[3, 4]는 패킷이 지나온 경로를 마킹하는 방법으로 간단하면서 강건한 대응 방법이다. 이 방법은 패킷이 지나온 라우터 주소정보의 일부를 마크하여 정상 패킷이 지나온 경로와 공격 패킷이 지나온 경로를 구분 하고자 하였다. 하지만 패킷 마킹을 하는 라우터의 수가 극히 적을 때 발생하는 쓰레기 값에 의해 신빙성이 떨어지는 마킹 값을 생성함으로써 단점을 갖을 수 있다. 따라서 이 논문은 기존의 Pi의 마킹 기술이 가지고 있는 단점에 대해 언급하고 이를 개선하기 위한 새로운 마킹 기술을 제시한다.

2. 기존 Pi의 개요

Pi는 패킷들이 지나온 서로다른 경로들을 식별하기 위한 패킷 마킹 기술이다. Pi에서 라우터는, 패킷 마킹을 하는 Pi 라우터와 패킷 마킹을 하지 않는 legacy 라우터인 두가지 타입으로 구분한다. Pi 라우터는 라우터 주소의 마지막 n 비트를 패킷의 Identification 필드(16 bit 필드)인 마킹 필드에 마킹함

으로써 경로정보를 남긴다. Pi는 라우터 주소의 마지막 비트중 1 비트 또는 2 비트를 사용했다. 이 논문에서 이것을 1 bit 마킹, 2 bit 마킹라 명칭한다. 그리고 Pi는 라우터 주소의 마지막 비트 값이 좀더 균등하게 분포되도록 hash 함수인 MD5를 이용 했으며 마킹 필드 내에 마킹 위치를 결정 하기 위해 패킷의 TTL 값을 사용하였다. 마킹 필드는 16/n 개의 마킹 구역들로 분리한 후 마킹 필드내에 마킹 위치를 결정 하기 위해 TTL % (16/n) 값을 사용하였다. Pi는 이와 같은 방법으로 패킷들이 지나온 서로 다른 경로들을 식별 한다. Pi값은 크기가 작기 때문에 빠르게 필터링 될 수 있다. 공격자가 보낸 패킷들의 Pi값을 미리 알고 있다면 짧은 시간 내에 그 공격 패킷들을 쉽게 필터링 할 수 있을 것이다.

3. 동기

기존의 Pi는 패킷의 TTL값을 이용하여 마킹 위치를 결정하기 때문에 여러가지 문제점이 발생한다. Pi는 legacy 라우터가 있을 경우 마킹 필드 내에 몇몇 마킹 되지 않는 구역을 만든다.

패킷의 TTL 값은 라우터를 거치면서 그 값이 하나씩 작아진다. 기존의 Pi는 마킹필드 내에 마킹 위치를 결정 하기 위해 TTL값을 사용한다. legacy 라우터는 자신이 마킹 해야 할 마킹위치에 어떤 마킹도 하지 않는다. 그리고 다음 Pi 라우터는 legacy 라우터가 마킹해야 할 다음 마킹구역에 마킹을 하게 될 것이다. 따라서 legacy 라우터에 의해 발생한 마킹되지 않은 구역은 쓰레기 값이 남아있는 구역으로 공격자에 의해 악용 될 수 있는 취약한 부분이다.

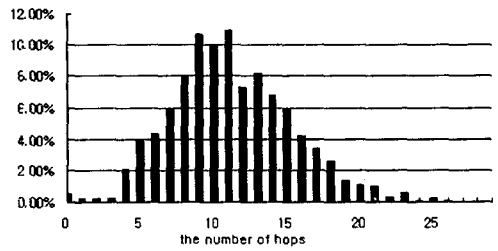

그림 1 홉 수의 따른 분포도

공격자가 패킷의 Identification 필드 초기 값을 위조 할 경우 마킹되지 않은 구역은 공격자가 위조한 쓰레기 값으로 채워 질 것이다. 따라서 의도했던 Pi 값과는 다른 다양한 값들이 만들어질 것이고 이로 인해 false positive 가 높아 지게 될 것이다. Pi논문에서 이와 같은 문제는 패킷이 좀더 많은 라우터들을 거치면서 마킹되지 않는 구역이 다른 Pi 라우터에 의해 마킹 되면서 해결 될수 있다라고 했지만 이는 적절할 해결책이라 볼수 없다. 이 문제는 두가지 경우로 생각해 볼수 있다.

우선 1 bit 마킹을 사용했을 경우 전체 마킹 구역을 모두 채우려면 적어도 16개의 라우터 (패킷의 Identification field는 16bit 이다) 를 지나와야 한다. 하지만 실제 인터넷 토폴로지 (e.g., CAIDA's Skitter Map)[5]를 이용한 실험 결과인 그림 1은 16개 이상의 라우터를 지나오는 경우는 전체의 20%에 지나지 않음을 보여주고 있다. 따라서 쓰레기 값을 갖는 Pi값을 만들어낼 확률이 클수 밖에 없다. 2 bit 마킹을 사용했을 경우 모든 마킹 구역을 채우기 위해 적어도 8개 이상의 라우터 (16/2) 를 지나와야 한다. 그림1은 8개 이상의 라우터를 지나오는 경우는 전체의 88%임을 보여주고 있지만 legacy 라우터가 너무 많이 존재 하게 되면 이 또한 위의 문제를 완전히 해결하기 위한 방법이 되기는 어렵다. 따라서 다음장(4 장)은 기존의 Pi가 갖는 이러한 문제점을 해결 하기 위한 새로운 마킹 기술을 소개한다.

4. 제안하는 Pi 마킹 기술

기존의 Pi 마킹 방법이 갖고 있는 취약점은 legacy 라우터에 의해 발생하는 마킹 되지 않는 구역이였다. 이 문제를 해결 하기 위해서는 legacy라우터가 존재 하더라도 마킹 되지 않는 구역이 생기지 않도록 하는 방법이 필요하다. 필드내에 위와 같은 문제가 발생하지 않도록 하기위해 패킷의 TTL값을 사용하지 않는 마킹 방법을 제안하려 한다. 제안하고자 하는 방법은 다음과 같다. 마킹 필드는 기존의 방법과 마찬 가지로 16/n 개의 마킹 구역들로 나눈다. 하지만 마킹 필드내에 마킹 위치를 결정하기 위해 기존의 방법처럼 패킷의 TTL값을 이용하지는 않는다. Pi 라우터는 패킷을 받으면 패킷의 Identification field에 있는 Pi 값을 모두 왼쪽으로 n bit shift 한 후, 필드의 가장 오른쪽에 라우터 자신의 주소중 마지막 n bit를 마킹한다. Legacy라우터는 패킷을 받으면 다음 라우터로 전송하는 일만 한다. 기존의 방법과는 달리 제안하는 방법은 마킹되지 않는 구역의 발생률을 최소화 한다. 그림 2와 그림 3은 제안하는 Pi 마킹 방법과 기존 Pi 마킹의 시나리오를 보

여준다. 두 시나리오 모두 간단히 마킹 필드의 구역은 4개로 설정 하였다. 패킷이 거쳐가는 6개의 라우터중 어두운 원은 Legacy 라우터로 나머지 원은 Pi 라우터로 지정 한다.

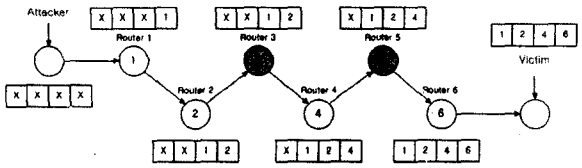

그림 2 제안하는 Pi 마킹 시나리오

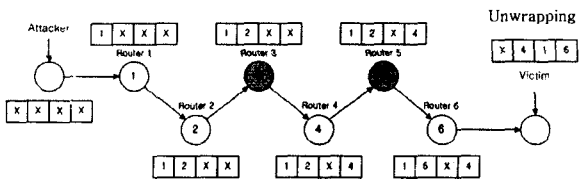

그림 3 기존 Pi 마킹 시나리오

그림2 와 그림3 이 보여주듯 같은 경로를 지나왔음에도 불구하고 서로 다른 마킹 값을 만들어 낸다. 기존의 Pi 마킹방법은 마킹되지 않은 1개의 마킹 구역에 의해 2^n 가지의 Pi값을 만들어 낸다. 하지만 같은 조건 내에서 제안하는 Pi 마킹 방법은 마킹 필드 내에 마킹되지 않는 구역을 만들지 않는다.

제안하는 방법을 이용하면 2 bit 마킹의 경우 패킷이 지나오는 Pi 라우터의 수가 적어도 8개 이상만 되면 마킹 필드가 모두 채워진다. 이 새로운 마킹 방법의 가장 큰 장점은 마킹된 값들 중간에 쓰레기 값이 들어가는 일이 없기 때문에 기존의 Pi보다 좀더 정확한 Pi값을 얻을 수 있다는 점이다. 그리고 패킷의 TTL값이 공격자에 의해 위조될 수 있는 취약한 부분도 해결 될 수 있기 때문에 기존의 마킹방법보다 좀 더 효율적임을 알 수 있다.

5. 결론

제안하는 방법의 근본적인 목적은 마킹 필드의 중간중간에 쓰레기 값이 들어가는 것을 최소화 하는 것이다. 제안 하는 방법은 기존 방법과는 달리 패킷의 TTL 값을 사용하지 않기 때문에 마킹 필드의 중간에 쓰레기 값이 들어가지 않는다. 2bit 마킹을 하고 Pi라우터가 8개 미만일 경우, 제안하는 방법은 마킹 필드의 왼쪽 k (8 구역 - 마킹구역)개의 마킹 구역이 마킹되지 않기 때문에 쓰레기 값으로 채워지겠지만 이 문제는 Postfix matching을 사용함으로써 해결 할 수 있다. 하지만 같은조건에서 기존 방법은 마킹 필드내에 마킹 값들이 띄엄띄엄 마킹 되어 있기 때문에 Postfix matching을 사용 할 수 없다.

따라서 기존의 Pi 마킹 방법보다 제안하는 마킹 방법이 분산서비스 거부 공격에 대응함에 있어 좀 더 효과적인 방법이 될 수 있을 것이다.

Reference

1. Ryan Naraine. Massive DdoS Attack Hit DNS Root Servers, eSecurityPlanet.com (Oct 2002) http://www.esecurityplanet.com/trends/article.php/10751_1486981
2. Inside the Slammer Worm http://www.computer.org/security/v1n4/j4wea.htm
3. A. Perrig, D. song, and A. Yaar. Pi: A Path Identification Mechanism to Defend against DDoS Attacks, In Proceedings of the 2003 Security and Privacy Symposium (May. 2003)
4. A. Perrig, D. song, and A. Yaar. Pi: A new defense mechanism against IP spoofing and DDoS attacks, Technical Report CMU-CS-02-207, Carnegie Mellon University, School of computer Science (Dec. 2002)
5. Caida. Skitter. http://www.caida.org/tools/measurement/skitter/ (2000)
6. XiaoFeg Wang, Michael K. Reiter. Defending Against Denial-of-Service Attacks with Puzzle Auctions, In Proceedings of the 2003 Security and Privacy Symposium (May. 2003)
7. Denial of Service Attacks, CERT (1997)
8. Jelena Mirkovic, Peter Reiher. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms