분산 서비스 거부 공격 대응방법인 Pi의 효율적인 필터링 향상을 위한 후위 매칭 방법 연구

*김동수, *김동규
*아주대학교, 정보통신전문대학원, 정보통신 및 시큐리티 연구실
*dongsoo@ajou.ac.kr, *dkkim@ajou.ac.kr

A Study of Suffix Matching Method for the Efficient Filtering of Path Identification to Defend against DDoS Attack

*Dongsoo Kim, *Dongkyoo Kim
*Information Communication & Security Lab. Graduate School of Information Communication, Ajou Univ.

요 약

분산 서비스 거부 (DDoS) 공격은 정상적인 사용자가 서비스를 이용하는 것을 거부하게 만드는 것이다. 이러한 분산 서비스 공격으로 인한 사회적 피해가 상당하다. 그동안 분산 서비스 거부 공격을 막기 위한 연구가 많이 이루어 졌다. 그러나 확실하게 이 공격을 막는 방법은 아직까지는 연구되지 않았다. 이 공격의 특징중의 하나는 위장된 소스 아이피(Spoofed source IP) 주소로 공격 대상에 많은 양의 패킷을 보내는 겁니다. 이로 인해 피해 호스트에가 정상 패킷과 공격 패킷을 구별하기가 어렵게 만든다. Pi(Path Identification)는 패킷이 지나온 라우터의 경로의 정보를 마킹 비트(marking bits)를 이용해 패킷에 마킹하게 된다. 마킹 비트의 크기는 Pi 필터링에서 성능에 있어서 중요한 요소이다. 기존 Pi 필터링은 TTL 값을 이용하여 마킹을 하면 legacy 라우터가 있는 부분은 알 수 없는 값이 들어간다. 그러나 TTL을 이용하지 않는 마킹을 하지 않는 방법이 연구되었고 1비트 마킹과 2비트 마킹에 대한 필터링 효율에 관한 연구도 이루어 졌다. 이 논문에서는 1비트 마킹을 했을 경우 suffix matching 방법을 통하여 효율적으로 공격을 차단할 수 있는 구현 방안을 제안하고자 한다.

1. 서론

인터넷의 규모가 급속도로 확장되면서 최근 분산 서비스 거부 (DDoS) 공격은 더욱더 심각한 문제를 야기하고 있다. 이 공격은 인터넷의 인프라를 소모시켜 정상 사용자들이 인프라를 이용할 수 없도록 만드는 공격 형태이다. 2003년 1월 25일 Sapphire/Slammer 웜에 의해 취약한 호스트의 90%가 10분안에 감염 되어서 인터넷을 마비되었던 "1.25 인터넷 대란"이 그 한 예이다 [1].

분산 서비스 공격을 방어하기 위해선 이 공격이 어디로부터 오는 패킷인가를 확인해야 한다. 그런 다음 패킷 필터링을 통해서 분산 서비스 공격을 차단할 수 있다. 그러나 공격자들은 위장된 소스 아이피 이용하여 패킷을 보내기 때문에 공격의 근원지를 추적하는 것이 어렵다. 그러므로 소스 아이피를 이용한 차단이 아닌 다른 방법이 필요하게 되었다. 이에 대한 대응책으로 일반적인 기법으로 IP traceback이 있다[2]. 그러나 이 방식은 피해 호스트가 정확한 공격 패킷의 경로를 재구성하기 위해서는 일정량 이상의 패킷을 수집해야 하는 결점이 있다[3]. 패킷 범람 형태의 공격에 대해서는 경로를 재구성하는 것이 어렵게 된다.

Pi(Path Identification)는 패킷이 지나온 경로를 마킹하는 방법으로 정상 패킷이 지나온 경로와 공격 패킷이 지나온 경로를 구분하여 필터링하는 방식을 제안했다[3]. Pi는 경로를 재구성