[5A-44]

분산 서비스 공격 대응을 위한 액티브 네트워크 기법 적용 방안

*이원구, *이재광
*한남대학교 컴퓨터공학과 컴퓨터네트워크실험실
e-mail:wglee@netwk.hannam.ac.kr

Applying Method of Active Network to DDoS Attack

*Won-Goo Lee, *Jae-Kwang Lee
*Dept of Computer Engineering, Hannam University

요 약

최근 컴퓨터 기술의 발달과 인터넷의 발전으로 인해 업무 효율이 높아졌고 생활의 질이 높아졌다. 하지만 컴퓨터 기술과 인터넷 기술의 발전은 긍정적인 효과뿐만 아니라 외부 시스템의 불법 침입, 중요 정보의 유출, 서비스 거부 공격 등 역기능도 생겨났다. 이러한 사이버 공격에 대한 능동적으로 대응할 수 있는 기술이 요구되는데 능동적인 대응의 가장 기본적으로 요구되는 기술이 공격자의 실제 위치를 파악하는 역추적 기술이라고 할 수 있다. 이에 본 논문에서는 분산 서비스 거부 공격에 대하여 효율적으로 역추적 하기 위해서 액티브 네트워크 기반의 역추적 시스템을 분석 및 설계한다.

1. 서론

최근 컴퓨터 기술의 발달과 인터넷의 발전으로 인해 업무 효율이 높아졌고 생활의 질이 높아졌다. 하지만 컴퓨터 기술과 인터넷 기술의 발전은 긍정적인 효과뿐만 아니라 외부 시스템의 불법 침입, 중요 정보의 유출, 서비스 거부 공격 등 역기능도 생겨났다.

이에 최근의 정보보호 관경에서는 자신의 관리 도메인 내로 침입하게 되는 공격을 어떻게 효율적으로 탐지할 것인가와 탐지된 공격을 어떻게 효율적으로 차단하여 자신의 도메인을 잘 보호할 것인가에 초점이 맞추어지게 되었다. 하지만 탐지된 침입에 대한 대응도 자신의 도메인 경계에서 해당 트래픽을 차단하는 수동적인 방법 이외에는 별다른 방법이 없는 상태이다. 그래서 자신의 도메인 입구에서만 해당 트래픽을 차단함으로써 침입자는 인터넷을 통하여 제2, 제3의 공격을 할 수 있게 된다. 인터넷을 통한 경제 활동이 점차 증가하는 요즘 사이버 공격으로 입는 피해는 기업의 생존을 위협하는 수준에 도달하게 되었다. 따라서 이러한 사이버 공격에 대한 능동으로 대응할 수 있는 기술이 요구된다고 할 수 있다. 이런 능동적인 대응의 가장 기본적으로 요구되는 기술이 공격자의 실제 위치를 파악하는 역추적 기술이라고 할 수 있다[1].

이에 본 논문에서는 분산 서비스 거부 공격에 대하여 효율적으로 역추적 하기 위해서 액티브 네트워크 기반의 역추적 시스템을 설계한다. 2장에서는 분산 서비스 거부 공격과 역추적 기법을 살펴보고, 3장에서는 액티브 네트워크와 IDIP, AN-IDR에 대해서 분석하며 4장에서는 액티브 네트워크 기술을 이용한 역추적 방법을 제시하고 5장에서는 결론을 맺고 향후 연구방향을 기술하였다.

※ 본 연구는 한국과학재단 목적기초연구(R01-2002-000-00127-0)지원으로 수행되었음

2. 관련연구

2.1 DDoS(Distributed Denial of Service)

해킹 사건에 사용된 수법인 분산 서비스 거부공격(DDoS: Distributed Denial of service)은 마스터 서버에 접속하여 하나 혹은 여러 개의 IP 주소를 대상으로 서비스 거부 공격을 수행하게 된다. 이럴 경우 트리누 마스터는 특정한 기간에 하나 혹은 여러 개의 IP 주소를 공격하도록 하부 서버와 통신한다. 이는 공격자의 명령에 의해 공격 도구가 설치된 대량의 서버들을 제어해 공격 대상 시스템에 치명적인 서비스 거부 공격을 수행하기 때문에 인터넷을 교란시키려는 해커들에 의해 악용될 수 있다. 분산 서비스 거부 공격은 IP 패킷에 근원지 IP 주소를 스푸핑하여 공격하기 때문에 공격경로와 패킷의 경로는 서로 다르다.

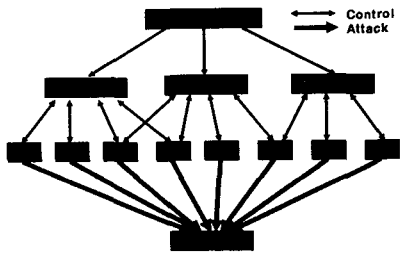

그림 1. DDoS 공격 구조