분산 서비스 거부 공격과 그 특징에 관한 연구*

김정윤*, 최형기*
*성균관대학교 전자전기컴퓨터공학과
e-mail : steal83@ece.skku.ac.kr

A Study on Distributed Denial of Service Attacks

Jung-Yoon Kim*, Hyoung-Kee Choi*
*Dept. of Electronic Electrical Computer Engineering, Sung-Kyun-Kwan University

요 약

분산 서비스 거부 공격은 서버 및 호스트의 메모리는 물론이고, 공격 대상 호스트가 속한 네트워크의 자원을 크게 소모시키는 치명적인 공격이다. 이러한 형태의 공격을 예측하고 방어하기 위해서는 우선적으로 해당 공격들의 특성을 파악하고 이해하는 과정이 필요하다. 우리는 다양한 종류의 분산 서비스 거부 공격을 직접 구현하여 이를 바탕으로 분산 서비스 거부 공격의 특징 및 공격 루트를 파악함으로써, 추후 관련 연구들이 활발히 진행될 수 있는 기반을 마련하고, 이러한 공격들을 방어하기 위한 정보들을 수집하였다. 우리가 구현한 분산 서비스 거부 공격은 그 종류에 따라 다른 치명도를 보였는데, 네트워크 및 호스트에 별 영향을 끼치지 않는 공격이 있는 반면, 서버가 더 이상 서비스를 제공할 수 없도록 만드는 치명적인 공격이 있었다. 본 논문에서 우리는 분산 서비스 거부 공격들의 특징을 분석하고, 이에 대한 방어책을 제시한다.

1. 서론

과거에 주로 발생했던 네트워크 상에서의 공격은 관리자 권한을 획득하거나 데이터를 유출시키는 형태로 이루어졌다. 그러나 지난 몇 년 사이, 대다수의 공격이 고의적으로 대량의 트래픽을 유발하여 네트워크 시스템을 교란시키는 공격법(Denial of Service, DoS)으로 변화한 것은 익히 알려진 사실이다. 최근의 해킹, 웜 등의 악성 코드는 단일 시스템을 대상으로 한 공격에서 발전하여 네트워크 인프라를 위협하는 대규모 공격 형태(Distributed Denial of Service, DDoS)로 발전하고 있다. 2000 년 Yahoo, Amazon, CNN 등 굴지의 인터넷 관련 기업들이 대규모 DDoS 공격으로 막대한 피해를 입었다. 최근에는 개인 PC 를 공격한 후 원격 제어가 가능한 bot 을 설치하여 수천~수만개의 zombie 시스템들을 거느린 botnet 을 형성하고 이를 이용한 대규모 공격도 커다란 위협으로 등장하고 있다. 이처럼 대규모 피해를 유발하는 주된 원인은 최근의 공격이 분산 서비스 거부 공격(DDoS)을 기반으로 하고 있다는 사실이다.

2. 서비스 거부 공격의 종류

최근의 분산 서비스 거부 공격은 서비스 거부 공격을 여러 대의 zombie 시스템으로부터 발생시키는 형태를 띄고 있다. 따라서, 분산 서비스 거부 공격을 이해하기 위해서는 우선적으로 서비스 거부 공격에 대한 이해가 이루어져야 한다.

서비스 거부 공격은 크게, 서버의 메모리 및 연산 능력을 소모시키는 공격과 네트워크의 자원을 소모시키는 공격으로 나눌 수 있다. 서버의 메모리 및 연산 능력을 소모시키는 공격의 경우, 공격을 당한 서버가 더 이상 정상적인 서비스를 제공할 수 없도록 만드는 것이고, 네트워크의 자원을 소모시키는 공격의 경우, 공격을 당한 네트워크가 가용한 bandwidth 를 모두 잃게 되어, 해당 네트워크로의 접근이 불가능해지는 것을 의미한다. 본 논문에서는 위 2 가지 종류의 서비스 거부 공격을 모두 구현하였다.

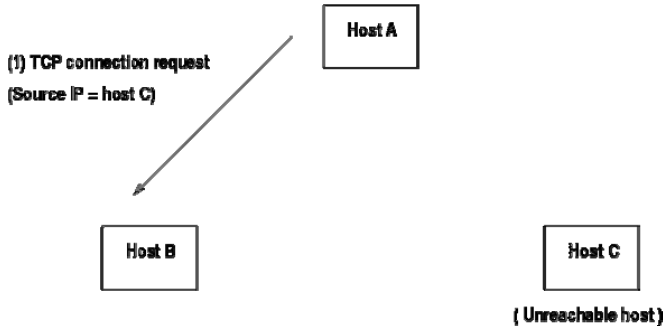
3. 서비스 거부 공격의 원리

1) SYN Flooding

대부분의 운영체제들은 연결 초기화 과정에서 제한된 자원을 사용한다. 일반적으로 각 포트 별로 동시 접속 연결이 수 백 개로 제한되어 있어서 자원이 다 소비되면 더 이상 연결을 받아들일 수 없다. SYN Flooding 은 TCP protocol 의 이러한 취약점을 공격대상으로 삼는다. 공격 방법은 일단 존재하지 않는 호스트의 주소로 공격대상에게 SYN 패킷을 보내는데, 연결 대기 시간 안에 주기적으로 백로그큐(연결 대기중인 큐)가 가득 찰 만큼의 SYN 패킷을 보낸다. 즉 연결을 요청하

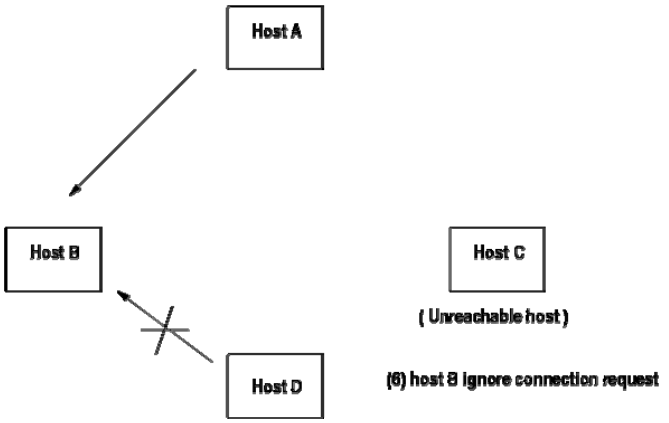
* "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음" (IITA-2006-C1090-0603-0028)

는 TCP 패킷을 호스트의 특정 포트에 보내어 이 포트의 대기 큐(backlog queue)를 가득차게 하여 이 포트에 들어오는 연결 요청을 큐가 빌 때 까지(connection time out 이 될 때 까지) 무시하도록 만드는 것이다. 큐(backlog queue) 크기는 시스템마다 다르지만 대략 5 에서 10 까지의 연결 대기 상태를 저장할 수 있다. 그러므로 실제 SYN Flooding 공격에서는 UDP Storm, Ping Flooding 과 같은 다른 종류의 Denial of Service 공격과 같이 대량의 패킷을 보내지 않아도 되므로, 공격이 쉽게 노출되지 않는다. 또한 출발지(Source) IP 주소를 임의의 주소로 만들어서 보내므로, 공격의 진원지를 알아내는 것 또한 어렵다.



(그림 1) SYN Flooding Attack 1

먼저 Source IP 주소에 들어갈 임의의 호스트를 찾아야 하는데 이 호스트는 연결할 수 없는(Unreachable) 호스트이어야 한다. 이 경우 공격자(호스트 A)가 보내는 TCP 연결 요청 패킷이 연결할 수 없는 호스트(호스트 C)의 IP 를 가지고 공격대상(호스트 B)에 전해지기 때문에, 호스트 B 는 호스트 C 로 SYN/ACK 를 하게 된다. 이 때, 호스트 C 는 unreachable 하기 때문에 응답을 하지 않을 것이고, 호스트 B 는 호스트 C 로부터 ACK 를 받기 위해 Connection time-out 이 걸릴 때까지 큐에 이 연결을 대기시켜 놓을 것이다.

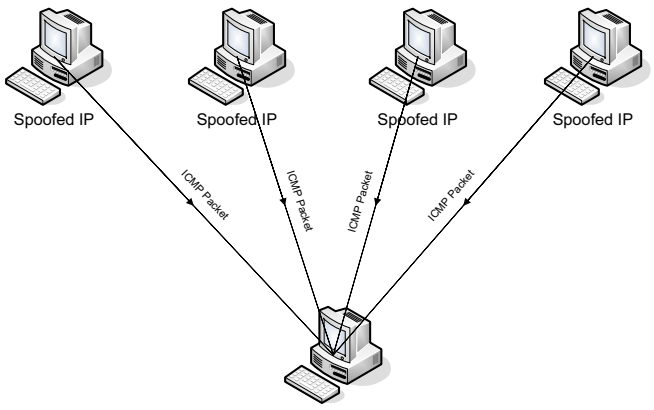


(그림 2) SYN Flooding Attack 2

그러면 결국 큐는 가득차게 되고 그 이후에 그 포트로 들어오는 연결 요청은 무시될 것이다. 만약 호스트 A 가 telnet 포트나 HTTP 포트에 연결을 요청하여 그 포트의 큐를 가득차게 했다면, 정상 사용자(호스트 D)는 호스트 B 에 그 포트로 정상적인 요청을 해도 연결을 맺을 수 없을 것이다.
그러나 최근에는 대부분의 운영체제 및 라우터에서 다량의 SYN 패킷이 유입되면 이를 적절히 차단하는 기능을 수행하기 때문에, 현재 SYN Flooding 공격의 치명도는 매우 낮다고 볼 수 있다.

2) ICMP Flooding

ICMP Flooding(Ping Flooding)은 다수의 ping 패킷을 공격대상에게 전송함으로써, 공격대상의 네트워킹 자원을 소모시키고 결국 정상적인 네트워킹을 불가능하게 만드는 공격이다. 이 공격은 지극히 일상적인 패킷인 ping 패킷을 다량으로 이용한다는 점에서 공격의 발견이 SYN Flooding 보다 어렵다고 볼 수 있다. SYN Flooding 의 경우 정상적인 Three-way Handshaking 에서 나타나는 SYN/ACK 및 ACK 패킷이 부재하기 때문에 공격의 발견이 비교적 쉽지만, Ping Flooding 의 경우 단일 ping 패킷의 다량 전송만으로 공격을 탐지하는 것은 쉬운 일이 아니다. 최근에는 네트워크의 bandwidth 가 과거에 비해 매우 크기 때문에, 이러한 ping 패킷으로 네트워크 자원을 소모시켜 정상적인 서비스를 불가능하게 만드는 것은 쉽지 않은 일이다. 그리고 상당 수의 서버들은 ping 패킷의 수신을 차단하고 있기 때문에, 이 공격 또한 치명도가 매우 낮다고 볼 수 있다.

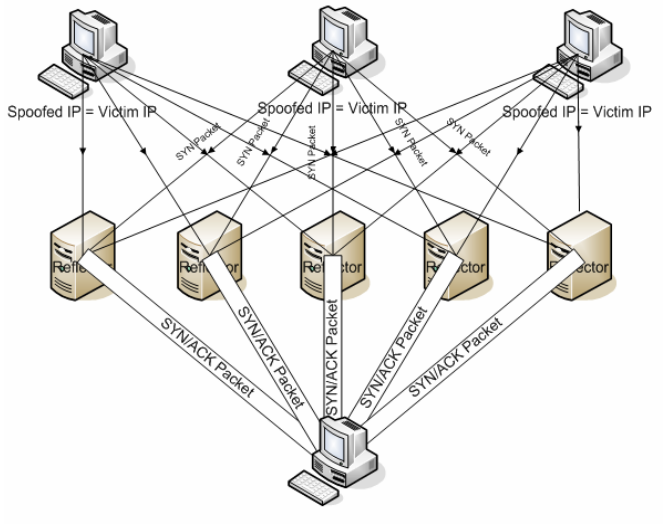


(그림 3) ICMP Flooding Attack

3) SYN/ACK Flooding

전형적인 DDoS 에서는 감염된 zombie 를 이용하지만, TCP SYN/ACK Flooding 은 새로운 공격법인 DRDoS (Distributed Reflection Denial of Service)로서 동작한다. Reflector(주로 웹서버, 라우터 등)에 Target IP 로 spoofing 된 TCP SYN 패킷을 보내면, 해당 Reflector 는 SYN/ACK 패킷을 target 에 일괄적으로 보냄으로써 해당 네트워크의 자원을 고갈시키는 공격법으로 동작한다.
SYN/ACK Flooding 은 궁극적으로 SYN/ACK 패킷의 다량 Reflection 을 이용하는 것인데, 최근 네트워크의

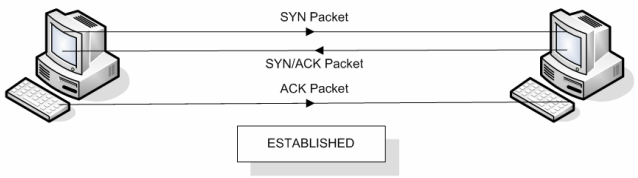
bandwidth 가 커짐에 따라 이러한 bandwidth 소모 공격은 그 치명도가 낮아지고 있다.



(그림 4) SYN/ACK Flooding Attack

4) NAPTHA

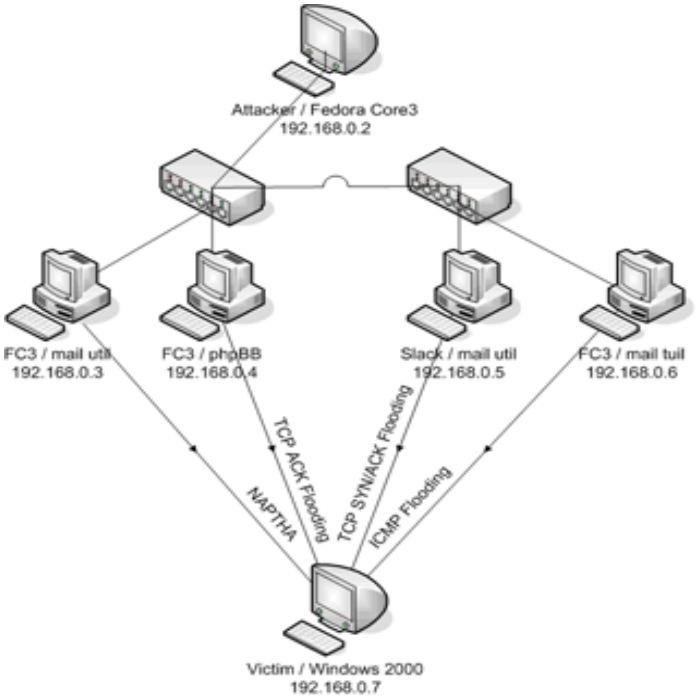
TCP 세션은 일련의 과정들을 거쳐 connection 을 맺고 처리한다. 이러한 TCP protocol 의 취약점을 이용하는 공격이 NAPTHA 이다. 실제로 존재하지 않는 IP 와 공격 대상 사이에 정상적인 세션(Three-way Handshaking)을 다수 개 만들어서 공격 대상 시스템의 자원(메모리)을 고갈시킨다. 존재하지 않는 IP 와의 세션을 맺기 때문에 공격 대상과 달리 공격자는 별 피해를 입지 않는다. NAPTHA 는 정상적인 사용자의 행동과 구분하는 것이 매우 어렵고, 공격대상 호스트의 메모리를 소모시키는 공격이기 때문에 그 치명도가 매우 높다고 할 수 있다.



(그림 5) NAPTHA Attack 에 이용되는 TCP protocol 의 취약점인 Three-way Handshaking

4. 구현 환경

먼저, 공격대상은 Windows 2000 으로 설정하였다. 그리고 공격자 및 zombie 호스트는 모두 Fedora Core3 를 사용하도록 하였다. Zombie 시스템은 실제로 감염시키는 과정까지 구현하였는데, 이러한 과정은 본 연구의 주요 연구 대상이 아니기 때문에 zombie 감염이 용이하도록 인위적으로 취약점을 노출시켰다. 각 zombie 호스트는 mail util, phpBB 등의 취약점을 가지도록 하였고, 공격자는 이러한 취약점을 활용하여 zombie 를 감염시키고 공격대상에게 DDoS 공격을 시도하도록 구성하였다.



(그림 6) 가상 DDoS 공격환경 (SYN Flooding, ICMP Flooding, SYN/ACK Flooding, NAPTHA)

5. 분산 서비스 거부 공격의 특징 및 대응책 분석

위에서 설명한 4 가지 공격을 구현해본 결과, SYN Flooding, ICMP Flooding, SYN/ACK Flooding 등 네트워크 자원을 소모시키는 공격은 현실적으로 그 규모가 매우 거대하지 않은 이상, 공격 대상에 별다른 영향을 미치지 않을 것으로 분석되었다. 실제로, 우리가 구현한 가상 공격환경은 4 대의 zombie 호스트만을 사용하였고, 이러한 규모에서의 공격은 호스트 및 네트워크에 거의 아무런 영향을 미치지 못했다.

그러나 호스트 및 서버의 자원(메모리)을 소모시키는 NAPTHA 공격은 그 치명도가 매우 높았으며, 이러한 가상 공격환경 뿐 아니라 최근의 네트워크 환경에서도 실제 적용이 가능한 것으로 분석되었다. 따라서 NAPTHA 공격을 효과적으로 막을 수 있는 연구 및 대응책 분석이 시급하다.

이러한 NAPTHA 공격에 대응하기 위해서는, SYN-COOKIE 등을 사용하거나, 혹은 호스트 자체를 인증하는 시스템이 필요할 것이다. 즉, 공격대상에 연결을 요청하는 호스트가 실제로 존재하는 IP 인지 확인하는 과정이 있어야 NAPTHA 공격을 원천적으로 막을 수 있다. 이는 TCP protocol 을 개선시키거나, 혹은 TCP 의 상위 layer 에서 인증 등의 절차를 제공할 필요가 있음을 의미한다.

6. 결론

우리는 다양한 DDoS 공격을 실제로 구현하고, 가상 공격환경을 만들어 이를 실제로 적용시켜봄으로써 DDoS 공격에 대한 특징들을 이끌어내었다. 실제 구현

을 토대로 각 공격들에 대한 특징들을 분석함으로써, 치명적인 공격의 종류를 파악할 수 있었고, 이에 대한 대비책을 구상할 수 있었다.
구현 결과, 네트워크 자원을 소모시키는 공격보다는 호스트 및 서버의 자원(메모리)을 소모시키는 공격이 훨씬 치명적이라는 사실을 알 수 있었다. 이는 최근의 네트워크 인프라가 빠른 속도로 고성능화, 안정화되고 있음을 의미한다. 물론 호스트 및 서버의 하드웨어나 소프트웨어 자체도 빠른 속도로 진화하고 있지만, 메모리를 고갈시키는 공격의 원리 자체는 여전히 가용한 공격으로써 사용되고 있기 때문에, 공격 자체를 원천 봉쇄하지 않는 한 그 피해는 계속해서 발생할 수 밖에 없다.
우리는 각종 공격들을 분석, 구현하는 과정에서 각 공격들의 원리들을 파악하고 설명하게 되었다. 본 논문에서 나타낸 각종 공격들의 원리를 바탕으로, 향후에는 더욱 다양한 공격에 대한 연구도 가능할 수 있고, 혹은 아직 나타나지 않은 공격에 대한 예측도 가능할 것이다. 본 논문을 기반으로 한 다양한 연구들이 진행됨에 따라, 궁극적으로는 안전한 네트워크 환경을 구축하고 안정적인 서비스를 제공할 수 있게 될 것이다.

참고문헌

[1] Behrouz A. Forouzan. "TCP/IP Protocol Suite, 2e"
[2] 정진욱. "TCP/IP 와 인터넷"
[3] 조기준, 김훈의. "해킹과 방어 완전 실무"
[4] 유동훈, InetCop Team. "실전해킹"
[5] W. Richard stevens. "Unix Network Programming Vol. 1"
[6] 김승현, 윤청원. "해킹과 보안"