역추적 방식을 이용한 분산 서비스 거부 공격 대응에 관한 연구

권윤주°,이만희, 정상길, 김국한, 변옥환
한국과학기술정보연구원
{yulli°, mhlee, lovej, ghkim, ohbyeon}@kisti.re.kr

Study on the Response of Distributed Denial of Service Using Backtracking Method

Yoonjoo Kwon°, Manhee Lee, Sangkil Jung, Gookhan Kim, Okhwan Byeon
Dept. of High Performance Research Networking, Korea Institute of Science Technology Information

요 약

인터넷의 발달은 지리적인 문제들로 인하여 시간의 소비를 가져왔던 문제들을 해결시켜주었다. 지리적인 문제의 해결은 더더욱 모든 일에 대한 인터넷의 의존도를 높여갔지만, 1969년도에 생겨난 인터넷은 조금씩 구조적인 문제들을 드러내고, 이러한 구조적인 문제들은 해커들로 하여금 사이버공간에서의 범죄를 일으키는 데 이용되고 있다.

다른 해킹들보다 최근 몇 년간 그 수위를 높여가고 있는 분산 서비스 거부 공격은 불특정다수의 인터넷 사용자들에게 네트워크 사용 또는 서비스 사용에 심각한 영향을 미친다는 점에서 그 공격기법에 대한 대응방안 모색이 시급한 실정이다. 따라서 본 논문은 효율적인 네트워크 자원 사용을 저해하는 분산 서비스 거부 공격의 근원지를 탐색하여 차단하는 메커니즘을 제안한다.

1. 서론

인터넷의 발달은 지리적인 문제들로 인하여 시간의 소비를 가져왔던 문제들을 해결시켜주었다. 지리적인 문제의 해결은 더더욱 모든 일에 대한 인터넷의 의존도를 높여갔지만, 1969년도에 생겨난 인터넷은 조금씩 구조적인 문제들을 드러내고, 이러한 구조적인 문제들은 해커들로 하여금 사이버공간에서의 범죄를 일으키는 데 이용되고 있다.

다른 해킹들보다 최근 몇 년간 그 수위를 높여가고 있는 분산 서비스 거부 공격은 불특정다수의 인터넷 사용자들에게 네트워크 사용 또는 서비스 사용에 심각한 영향을 미친다는 점에서 그 공격기법에 대한 대응방안 모색이 시급한 실정이다. 이러한 공격의 경우 공격자가 신분을 감추기 위하여 IP Spoofing 기술을 기반으로 공격하므로, 공격 대상 시스템뿐만 아니라 공격 대상의 루트에 있는 시스템들까지 성능저하를 야기시킨다.

따라서 본 논문은 효율적인 네트워크 자원 사용을 저해하는 분산 서비스 거부 공격의 근원지를 탐색하여 차단하는 분산 서비스 거부 공격 대응 메커니즘을 제안한다.

2. 관련연구

2.1 분산 서비스 거부 공격 정의

분산 서비스 거부(Distributed Denial of Service, 이하 DDoS) 공격은 인터넷에 연결된 일단의 시스템들을 이용해 단일 사이트에 대한 Flood 공격을 시도하는 것이다[3]. 해커들은 취약한 시스템에 대한 권한을 획득하여 그 시스템에 원격에서 실행할 수 있는 소프트웨어를 설치하고, 원격에서 이를 실행시켜 원격에서 공격을 개시한다. DDoS 공격을 개시하는 데 사용되는 프로그램으로는 TrinOO, TFN, TFN2K, Stacheldraht 등이 있다.

2.2 분산서비스 거부 공격의 유형

대표적인 분산 서비스 거부 공격의 유형은 다음과 같다.

① Trinoo

Trinoo는 1999년 7월에 처음으로 발견되었다. 공격 방법으로는 그림 1에 보는 것처럼, UDP flood를 사용하고, IP Spoofing은 사용하지 않는다[1,4]. DDoS 공격툴의 초기 모델로서, Attacker와 Master간, Master와 Agent간 통신을 위하여 각각 TCP 또는 UDP 포트를 사용하고 있으므로 그 포트가 노출될 경우 외부에서 검출될 수 있다는 단점이 있다.

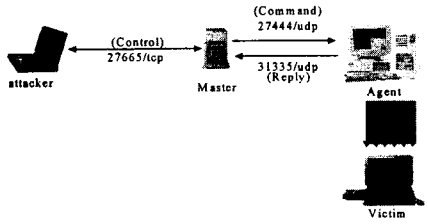

그림 1 Method of Trinoo

② TFN

"Tribe Flood Network"의 약자로서, Mixer라는 독일의 해커에 의해서 개발되었다. TFN의 Trinoo와는 달리 Attacker가 Master로 접속하기 위한 별도의 Port 번호가 준비되어 있지 않다. 따라서 Attacker는 Master로 접근하기 위해 TELNET등의 프로그램을 사용해서 Master를 구동시켜야 한다. 그림 2에서 보는 것처럼,

ICMP/TCP SYN/UDP floods, 그리고 Smurf 공격등 다양한 공격방법이 가능하다.

Master와 Agent의 통신에 ICMP ECHO_REPLY 메시지를 사용하므로 별도의 Port 번호를 열어둘 필요가 없어서 쉽게 탐지되지 않는다[1,4].

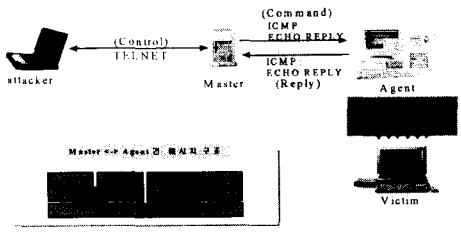

그림 2 Method of TFN

③ Stacheldraht(barbed wire : 철조망)

그림 3에서 보는 것처럼, Stacheldraht는 "Trinoo"의 네트워크 구조와 "TFN"의 다양한 공격방법 그리고, 통신상의 암호화기능을 포함한 DDoS 공격도구이다[1,4].

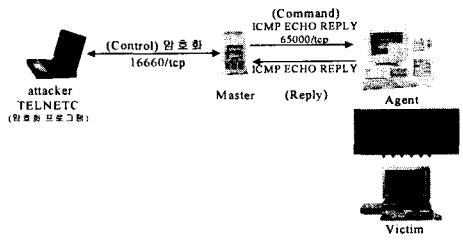

그림 3 Method of Stacheldraht

암호화를 위해서 Attacker가 직접 사용하는 TELNET과 비슷한 프로그램을 제공하는 데 이 프로그램이 Attacker와 Master간의 암호화된 통신을 보장한다.

2.3 분산 서비스 거부 공격의 예방, 탐지 및 대응에 있어서 문제점

① DDoS 공격으로 전송되는 트래픽은 서비스의 합법적인 사용을 위한 트래픽과 구분되지 않는다[3]. 따라서 DDoS Stream에는 필터링하거나 탐지할 수 있는 일반적인 특성이 없다[1,2].

② 분산된 DDoS 공격 근원지간의 협동은 DDoS 공격을 역추적하기 어렵게 한다. 분산된 근원지에 대처할 수 있도록 관리 도메인간 협력이 필요한 반면 관리 도메인 간의 협력이 부족하다[1,2].

③ DDoS 공격 코드와 자동화된 툴은 인터넷으로부터 쉽게 다운받을 수 있어서 초보 해커(intruder)도 쉽게 강력한 공격을 실행시킬 수 있다[1,2].

④ Attacker는 공격 시스템의 신분(identity)를 숨기기 위해 IP Spoofing을 사용하기 때문에 공격하는 시스템을 유추하기 어렵다.[1,2]

3. DDR (DDoS Detection and Response) System

본 논문에서는 DDoS 공격으로 인해 피해를 받게 되는 공격 대상 시스템뿐만 아니라 DDoS 공격 루트 상의 네트워크 자원 남용을 막기 위하여 DDoS 공격 근원지를 탐색하여 차단시켜주는 시스템인 DDR(DDoS Detection and Response) System을 제안한다.

3.1 DDR 시스템 원리

DDR 시스템은 하나의 단위구간에서의 DDoS 공격을 탐지 및 대응을 하는 데, 여기서 대응이라는 것은 두 가지 방향에서의 대응을 의미한다. 한 가지는 자신이 탐지하고 있는 네트워크의 라우터에 대한 대응을 의미하고, 또 한 가지는 DDoS 공격이 유입되는 해당 라우터의 입력 인터페이스와 연결된 그 전(previous) 라우터들로 DDoS공격 사실을 알리기 위한 DDoS 공격 탐지 정보 전달을 의미한다.

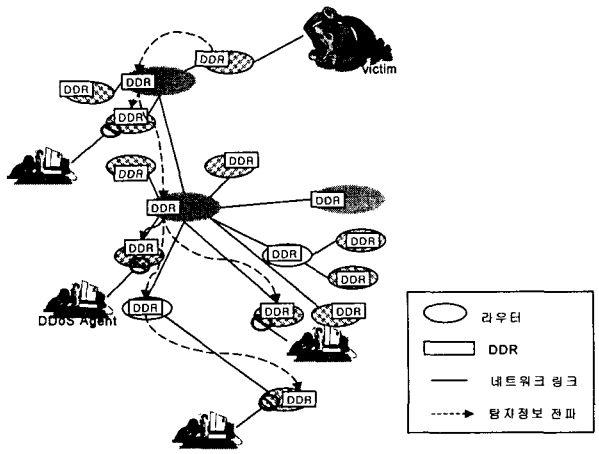

그림 4 DDR을 통한 DDoS 공격의 근원지 차단 메커니즘의 예

근원지를 차단하는 데 있어서 IP 헤더의 근원지 주소는 충분히 신뢰할 수 있는 정보가 되지 못하고 Spoofing 가능성이 높다. 따라서 DDR은 근원지를 차단하기 위해서는 그림 4에서 보는 바와 같이 라우터와 연계하여 라우터가 가지고 있는 정보를 이용하여 근원지를 탐색한다. 라우터는 기본적으로 자신을 통하여 흘러간 플로우에 대한 정보를 가지고 있으므로, DDR은 이를 이용하여 DDoS 공격을 탐지한 라우터로부터 공격 루트의 역방향으로 근원 라우터까지 탐색해나간다.

3.2 DDR System 구조

DDR System은 그림 5에서 보는 바와 같이 Detection Module, Control Module, Communication Module로 구성되어 있다. Detection Module의 역할은 자신이 담당하

고 있는 라우터에서 DDoS 공격이 일어나고 있는 지 탐지하는 것이고, Control Module의 역할은 Detection Module에서 탐지된 DDoS 공격에 대하여 제어를 수행하는 것이다. Communication Module은 DDR 간 상호 정보교환이 이루어 질 수 있도록 메시지를 구성하고 받은 메시지를 해석하는 모듈이다.

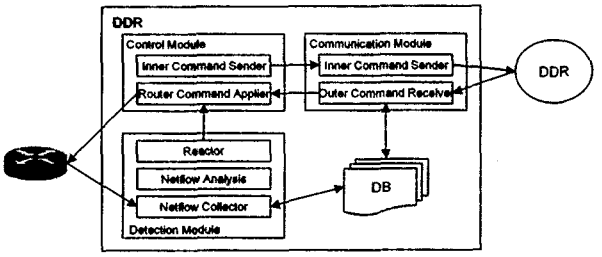

그림 5 DDR 시스템 구조

3.2.1 DDR 시스템의 세부 요소

① Detection Module

DDoS 공격에 대한 탐지는 라우터로부터의 Netflow 정보를 분석하여 수행되고, Netflow Collector, Netflow Analysis, Reactor로 구성되어 있다.

② Control Module

Detection Module의 Reactor 또는 Communication Module로부터 DDoS 공격 탐지에 대한 정보를 받게 되면 Control Module의 Router Command Applier에서는 자신이 담당하고 있는 라우터로 직접 DDoS공격의 목적 시스템으로의 패킷량을 줄이는 명령을 전달하고, 외부 DDR로 자신의 라우터를 통해 탐지한 DDoS 공격 메시지를 전파하도록 Inner Command Sender를 통하여 Communication Module에 요청한다.

③ Communication Module

Control Module로부터 DDoS 공격 메시지 전파에 대한 요청이 오면 Inner Command Sender를 통해 공격 루트 상에 있는 DDR System으로 메시지를 전파한다. 반대로 타 DDR System으로부터 DDR 공격 메시지 전파를 받게 되면 Control Module에게 Outer Command Receiver를 통해 DDoS 공격 메시지를 전달한다.

3.2.2 DDR System 간 Information Exchange Format

DDR은 DDoS 공격을 탐지하게 되면, 탐지한 정보에 대해서 DDR간에 공유하여 DDoS 공격을 일으키는 방식대로 분산 대응을 적용한다. 이때 DDR 간 정보를 전달하는 프로토콜을 DDIP(DDoS Detection Information Protocol)이라하고, 그림 6과 같이 구성되어 있다.

Congestion Signature(CS)
IP
Target Protocol(TP)
of propagation node(PN)
Time to Apply(TA)

그림 6 DDIP 구조

① CS : DDoS 공격에 대하여 Destination 위주로 제어를 해야 하는 지, Source를 위주로 제어해야하는 지를 명시

② IP : DDoS 공격의 타겟 시스템

③ TP : DDoS 공격을 일으키고 있는 타겟 프로토콜

④ PN : DDIP를 통하여 DDoS 공격 정보를 전파하고자 하는 라우터 Depth

⑤ TA : 각 라우터가 제어명령을 적용해야 할 시간

4. 결론 및 향후 계획

최근에 몇 번의 인터넷 대란을 통하여 잘 알려진 분산 서비스 거부 공격은 시스템과 네트워크를 마비시키어 업무처리 불능 상태를 초래하므로 단순히 네트워크 부분만의 문제라기보다 점차 사회적인 문제로 부각되고 있다.

앞서 언급한 것처럼 분산 서비스 거부 공격은 발생을 예방하는 것도 어렵거니와 한 곳에서 그 공격을 탐지하여 대처하였다고 하여도 보안 연계체제가 갖추어져 있지 않다면 빙산의 일각을 막은 효과밖에 없으므로 원천적인 분산 서비스 거부 공격에 대하여 대응하기 위해서는 분산 서비스 거부 공격의 모든 루트를 제어하여야 한다. 따라서 본 논문은 라우터를 이용한 공격 루트 역방향으로의 공격의 근원지 탐색 및 차단 메커니즘을 제안하고 있다. 이러한 방식으로의 보안 연계체제를 통하여 분산 서비스 거부 공격 루트 상의 모든 네트워크 자원의 남용을 방지할 수 있다.

향후 계획으로는 단위 도메인에서의 보안 연계체제를 넘어서 단위 도메인간 협력 체제를 가능하게 할 수 있도록 일반화된 또는 표준화된 보안 정보 공유포맷의 정의에 관하여 연구할 것이다.

참고문헌

[1] Jelena Mirkovic, "D-WARD : DDoS Network Attack Recognition and Defense", PhD Proposal, 2002년 1월.

[2] Jelena Mirkovic, "Source Router Approach to DDoS Defence", Usenix Security Symposium 2001, 2001

[3] Felix Lau, et al., "Distributed Denial of Service Attacks", Systems, Man, and Cybernetics, 2000 IEEE International Conference on, Vol. 3, pp 2275-2280, 2000

[4] 이철호, "DDoS 공격도구 분석", 2002년 2월, http://rpa.ajou.ac.kr/project/linux_q_team/seminar_doc/L_ts020204-DDOS공격도구분석.pdf