Journal of the Korea Academia-Industrial cooperation Society
Vol. 15, No. 11 pp. 6845-6848, 2014

http://dx.doi.org/10.5762/KAIS.2014.15.11.6845
ISSN 1975-4701 / eISSN 2288-4688

DDoS공격감지 및 방어를 위한 침입방지 시스템의 설계

홍성식[1*]
[1]혜전대학교 인터넷보안과

System Design of IDS for DDoS Detect and Defense

Seong-Sik Hong[1*]
[1]**Dept. of Internet Security, HyeJeon College**

요 약 본 논문에서는 네트워크를 통해 이루어지고 있는 DDoS공격을 감지하고 이를 방어할 수 있는 시스템을 설계한다. 제안하는 시스템은 경고 에이전트(Alert Agent), 공격분석 에이전트(Attack Analyzer Agent), 방어 에이전트(Defence Agent)의 3-티어(3-tier) 시스템으로 구성한다. 경고에이전트는 서버에서 서버의 자원이 부족해지는 시점에 공격분석에이전트로 서버의 트래픽을 복사하여 전송한다. 공격분석 에이전트로 전송되는 트래픽은 송수신자 주소 및 패킷번호만을 처리하여 분석에이전트의 부하를 감소한다. 공격분석 에이전트는 받은 트래픽을 분석하여 DDoS의 패턴과 일치하는지 검사한 후 DDoS공격으로 판단하면 방어에이전트에게 해당 발신자의 트래픽을 소멸하도록 지시한다. 이 시스템에서는 서버가 DDoS공격으로 인하여 과부하가 발생하여 작동이 중지되더라도 공격분석 에이전트가 DDoS트래픽을 선별하여 방어 에이전트에게 차단하도록 지시하여 서버가 최대한 빨리 복구되도록 동작한다.

Abstract This paper proposes a system design of IDS for detecting and defending against DDoS attacks on a network. The proposed system has three parts; the Alert, Attack Analyzer and Defense agent. When the server resource was reduced too much by incoming traffic, the Alert Agent sends message and traffic information to the Attack Analyzer. The message and traffic to the Attack analyzer include only the sender & receiver address and packet numbers for minimizing the overload of Attack Analyzer. Message Received Attack Analyzer investigates the Message. If the pattern of traffic is the same as the DDoS Style, the Analyzer sends a message to the Defense Agent to block that traffic. In this system, at the serious state of the server-down, the Attack analyzer uncovers the DDoS Attacker and send a message to the Defense Agent to block that traffic. This works for server reactivation as soon as possible.

Key Words : DDoS Attack, IDS

1. 서론

DoS(Denial of Service)공격은 시스템이나 네트워크의 구조적인 취약점을 공격하여 시스템의 성능을 저하시키거나 마비시키는 공격방식을 의미한다. DoS공격은 공격 방법이 비교적 간단하고 손쉽게 이루어질 수 있다는 측면에서 상당한 위험요소를 내포하고 있다. 그러나 한 대의 공격자가 한 대의 서버를 마비시키기에 충분한 공격 트래픽을 전송하는 것은 매우 어려운 일이다[1]. 또한 공격자가 충분한 공격의 성과를 얻을 만한 인원의 동료 공격자를 확보한다는 것도 어려운 일이었다. 하지만 IT 기술의 발전과 네트워크의 보급으로 인하여 수많은 컴퓨터들이 네트워크를 이루어 운영되는 현재의 컴퓨터 통신 환경에서는 상황이 달라졌다. 공격자는 공격자의 지시를 따르는 악성코드를 유포시켜 DoS 공격에 충분한 공격자를 거느릴 수 있게 되었다[2,6]. 해커의 공격명령에 따

*Corresponding Author : Seong-Sik Hong(HyeJeon College)
Tel: +82-10-3785-9143 email: sshong@hyejeon.ac.kr
Received October 24, 2014 Revised October 4, 2014 Accepted November 6, 2014

르는 악성 코드가 탑재된 PC를 좀비PC라고 정의 한다. DDoS(Distributed Denial of Service)는 DoS 공격을 수행하는 다수의 공격시스템을 두어 공격하는 방식이다. 악성 코드 등에 감염된 좀비PC들이 주로 하부 공격자의 역할을 담당한다.

KT와 같은 ISP(Internet Solution Provider)레벨에서 DDoS공격이 발생하고 있는 상황은 특정 네트워크 사용량이 폭주하거나 동일 수신자에 대한 패킷의 증가로 예견할 수는 있으나 이를 실제 공격으로 판단하고 동일 수신자에 대한 모든 접속을 해제하는 것은 대상 서비스를 중단시키려는 DDoS의 공격목적과 일치하므로 오히려 공격을 도와주는 상황을 초래한다. 또한 정상적인 과다 사용자의 트래픽이 제한을 받을 수 있다[5]. 그러므로 본 연구에서는 DDoS공격에 대한 감지와 방어를 피공격 대상서버와 연동하여 수행할 수 있는 해결책을 제시하여 피공격대상자 입장에서 판단하고 이를 방어하는 시스템을 설계한다.

2. DDoS 공격의 유형

DDoS 공격 및 이를 응용한 공격 유형은 매우 다양하다. 그 중에서 본 논문에 중점적으로 관심을 가지고 살펴본 공격 유형은 3가지이다. 이는 가장 구현하기 쉽고, 그 피해 규모가 매우 넓어 위험성이 높은 것으로 분류된다[2,7].

2.1 Ping of Death 공격

Ping은 일반적으로 32바이트 크기를 갖는다. 그러나 Ping 패킷을 매우 큰 크기로 만들어 전송할 경우 네트워크에서는 이를 적절한 크기로 나누어 전송하게 된다. 수많은 개수로 나누어진 각각의 핑은 동일한 목적지를 향하게 되므로 핑 수신자는 이를 처리하기 위하여 쉽게 시스템 자원 고갈 상태에 빠지게 된다. 리눅스커널 2.0.32이하의 커널을 사용하는 서버에 유효하다[7].

2.2 SYN Flooding 공격

SYN Flooding 공격은 공격자 시스템이 피공격대상자 시스템에 TCP/IP의 SYN 시그널을 전송하여 전송 개시를 알린 후 이에 대한 응답을 무기한 지연 시킨다. 피공격자는 연결 설정 요구에 응답하기 위하여 포트를 할당하고 수신 프로세스를 가동한다. 이런 공격이 반복되어 피공격대상자의 자원을 고갈 시키는 방법이다.

2.3 Boink, Bonk 및 Tear Drop 공격

Boink, Bonk 및 Tear Drop 공격은 수신측에서 정상적인 패킷을 수신하기 위하여 전송 및 재전송을 요구하는 특성을 이용한 공격방법이다. 부적절한 패킷 번호를 포함한 패킷을 전송하므로써 이를 처리하기 위한 피공격대상 시스템 자원을 고갈 시킨다.

2.4 Land 공격

Land공격은 공격자가 패킷을 조작하여 발신자 주소와 수진자 주소를 모두 수신자 주소로 설정하여 보내는 방법이다. 피 공격자는 발신자에 대한 전송 요구를 받아들이고 대기하게 된다. 그러나 발신자 주소가 피공격자의 시스템 주소로 설정 되어 있으므로 패킷은 무한반복 전송을 수행하게 되어 수신자의 시스템 자원을 고갈 시킨다.

2.5 Smurf 공격

Smurf공격은 피공격자 주소를 발신자로 하여 ICMP 패킷을 발생시켜 네트워크에 흘려보내고 이를 응답한 시스템들은 모두 피공격자에게 응답을 하게 되어 이를 처리하기 위해 피 공격자의 시스템 자원을 고갈 시키는 방법이다.

3. DDoS감지 및 방어 시스템의 설계

본 연구에서는 DDoS 공격을 감지하고 방어하기 위해서 주변의 감지 PC들이 협조체계를 구축하고, 공격 감지를 위해 임계값을 설정해 두고 이를 넘는 경우에 대한 감지와 협동 방어 시스템으로 설계하고자 한다[1,3,4].

3.1 Alert Agent 알고리즘

DDoS공격을 당하는 서버는 메모리 자원과 포트자원의 지정된 임계값을 초과하는 경우 Alert Agent가 Attack Analyzer Agent에 통보하여 트래픽을 분석하도록 한다. 분석을 위하여 전송되는 트래픽은 송수신 주소 및 패킷번호만을 전송하여 Attack Analyzer의 부담을 최소화 하였다. 임계값은 서버의 접속율 및 성능에 따라 조정되어야 한다.

```
//Alert Agent
#define Limit 90  // 90% 임계값
Status_Check()
{
    while(1)
     if ( (Memory.Resource < Limit) ||
          (Port.Resource < Limit) )
         Alert(alert);
     else
         Alert(none);
}
```

3.2 Attack Analyzer Agent 알고리즘

Attack Analyzer Agent는 서버로 들어오는 트래픽의 송수신자와 패킷번호, 송수신 주소를 확인하여 해당 트래픽이 DDoS공격의 패턴과 유사한가를 판단하여 패턴과 일치하는 트래픽의 소멸을 Defence Agent에게 지시한다. 또한 DDoS공격으로 판단된 발신자의 주소를 데이터베이스에 블랙리스트 테이블에 저장하여 300초간 접속을 중지하도록 하였다. 공격자가 아닌 경우 지연시간을 0으로 하여 Defence Agent가 해당 트래픽은 통과시키도록 하였으며 이로 인하여 정상적인 사용자들이 접속해제가 발생되지 않도록 하였다.

```
// Attack Analyzer Agent
Analyzer(Alert alert)
{
    if( (alert.traffic == PingOfDeath(alert)) ||
        (alert.traffic == SynFlooding(alert)) ||
        (alert.traffic == BBTD(alert)) ||
        (alert.traffic == Land(alert)) ||
        (alert.traffic == Smurf(alert)) ||
        (alert.traffic == BadTraffic(alert)) )
    {
        insert(alert.source, BlackList);
        alert.Delay = 300;
        Defence(alert);
    }
    else
        alert.Delay = 0;
}
```

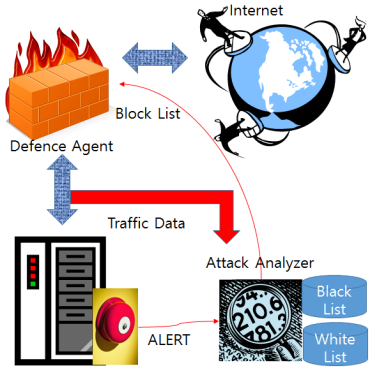
3.3 Defence Agent 알고리즘

Defence Agent는 Attack Analyzer가 지시한 발신자의 트래픽을 Delay시간동안 무시하여 소멸시킴으로써 서버의 부하를 낮춘다. Defence Agent는 Attack Analyzer Agent의 메시지에 따라 실시간으로 트래픽 전송을 제어한다.

```
// Defence Agent
Defence(Alert alert)
{
    if( alert.Delay > 0 )
        Remove(Traffic,alert.Delay);
    else
        Bypass(Traffic);
}
```

3.4 시스템 구성

DDoS공격은 자원고갈 공격방식의 특성상 공격트래픽을 차단하면 서버가 원래 상태로 복구된다.



[Fig. 1] System Floaw

DDoS공격은 집중된 시간에 자원고갈을 시도하려고 하므로, 방어에이전트는 일정시간동안 공격으로 의심되는 트래픽을 차단하여 지속적인 DDoS 공격을 무산시키는 방법을 사용한다. 또한 공격분석에이전트는 화이트리스트와 블랙리스트 테이블을 사용하여 화이트리스트의 트래픽은 항시 통과시키고 블랙 리스트의 트래픽은 지속적으로 Delay시간을 증가시키는 방법을 사용한다.

4. 결론

본 논문에서는 DDoS공격을 당하는 피공격자의 시스템이 자원고갈 상태에 빠지기 전에 DDoS Alert를 발생시켜 Analyzer에게 분석을 의뢰하므로 서버 자원 고갈 이전에 DDoS공격을 회피할 수 있으며 Alert 발생 이후에 자원 고갈 상태에 도달하였어도 Analyzer 와 Defence Agent에 의해 자발적으로 DDoS공격에서 회생할 수 있

는 방법을 제시하였다.

본 연구는 DDoS 공격 검출 및 방어에 국한하였다. 그러므로 Defence Agent를 WebKnight와 같은 공개형 방화벽에 추가하여 다양한 공격에 대비할 수 있도록 하고, SYN Flood, UDP Flood, TCP Flood, ICMP Flood, No Cache Get Flood, CC Attack등 새로 만들어지거나 변형 공격이 이루어지고 있는 DDoS 공격 유형에 대한 Attack Analyzer의 판별 능력 개선연구가 필요하다.

Reference

[1] Jin-won Seo, Jin Kwak, “The Design of Anti-DDoS System using Defense on Depth ”, Journal of the Korean Institute of Information Security and Cryptology, 22-3, pp,679-689, 2012/06.

[2] Jeonn Yong Hee, Jang Jong Su, Oh Jin Tae, “DDoS Attack & Defence Tequnics”, KIISC, 19-3, pp.46-57, 2009/06.

[3] Jeong Chung Gyo, Oh Ji Hyeon, “Defence of Distributed Denial of Service with User Cooperation”, KICS, No.33-4, pp.136-142, 2008/04.

[4] Ruoyu Yan, Qinghua Zheng, Haifei Li, “Combining Adaptive Filtering and IF Flows to Detect DDoS Attacks within a Router”, KSII Transactions on Internet and Information Systes(TIIS), vol.4, no.3, pp.428-451, June, 2010.

[5] Yoon Young Jin, Lee Jung Il, Gu Kyeong ok, Oh Chang Seok, “DDoS Attack Detect by Traffic variance“, KEIA, book No.7, pp.123-128, 2010/11

[6] Choi Yang Seo, Oh Jin Tae, Jang Jong Su, Ryou Jae Cheol, “A research of Total Defence system for DDoS Attack“, KIISC, No.19-5, pp.11-20, 2009/10.

[7] Yang Dae Il, Fundamental of Information Security, HanBit Academy

홍 성 식(Seong-Sik Hong) **[정회원]**

- 1992년 2월 : 광운대학교 전자계산학과 (이학석사)
- 2007년 2월 : 광운대학교 광운대학원 컴퓨터공학과 (공학박사)
- 1994년 9월 ~ 현재 : 혜전대학교 교수

<관심분야>
정보통신, 정보보호