2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

분산서비스거부 공격 대응 시스템을 위한 악성에이전트 제거 모듈 설계

채연주**○ 서진철** 임채호* 원유헌**
**홍익대학교 컴퓨터공학과 *한국정보보호센터
**{yjchae, jcseo, won}@cs.hongik.ac.kr *chlim@kisa.or.kr

Design of Removal Module of Malicious Agent for Distributed Denial of Service Attack Response System

Youn-Ju Chae**○ Jin-Cheol Seo** Chae-Ho Lim* Yoo-Hun Won**
**Dept. of Computer Engineering, HongIk University
*Korea Information Security Agency

요 약

분산서비스거부(Distributed Denial of Service or DDoS)를 이용한 공격은 공격목표시스템이 보안이 철저하다고 해도 쉽게 공격을 가할 수 있는 공격법이다. 근래에 들어 이러한 공격법은 여러 해킹툴의 보급과 함께 급격히 증가하고 있다. 하지만, 시스템 자체의 보안만으로 대처 방안이 되지 못하고 있는 실정이다. DDoS 공격을 방지하기 위해서는 전체 시스템들이 모두 보안체계를 갖추고 있어야 하지만, 이것은 현실적으로 불가능하다. 결국 DDoS 공격을 탐지하고 대처하기 위해서는 라우터와 네트워크를 기반으로 한 대응시스템 설계가 요구된다. 또한 DDoS 공격의 재발을 막기 위해서는 DDoS 공격 시스템으로 이용된 시스템을 찾아 악성프로그램을 탐지하고 제거할 수 있는 악성에이전트 탐지 및 제거 시스템을 설계하였다.

1. 서론

서비스거부공격(Denial of Service or DoS)은 오래전부터 잘 알려진 공격법이다. 과거에는 DoS 공격으로 인한 피해는 사용자의 불편함 정도였다. 하지만 인터넷을 통한 수입창출구조가 많아지면서 DoS 공격으로 인한 피해는 단순한 불편함을 넘어서서 자원과 재원을 낭비하는 결과를 가져왔다. 근래에는 DoS 공격의 발전된 형태를 지닌 분산서비스거부(Distributed Denial of Service or DDoS) 공격을 이용해 조직적이고 파괴적인 공격이 시도되고 있다. 현재 인터넷을 통해 사업을 하는 상거래 사이트, 검색사이트, 방송사이트 등은 DoS 공격을 당하면 큰 경제적 손실을 가져오게 된다. 대표적인 예로 2000년 2월 yahoo를 비롯한 다수의 대표적 인터넷 사이트가 DDoS 공격을 받아 서비스를 중단한 사고가 있었다. 이러한 사이트들은 DDoS 공격으로 인해 경제적 손실 뿐 만 아니라 사용자들에게 기업의 신용도가 떨어지게 되어 잠재적 손실도 크다. 또한 국방, 금융, 수송, 전력 등 다양한 분야에서 정보시스템에 대한 의존율이 높아짐에 따라 정보시스템의 가용성(Availability)에 대한 고의적인 방해 행위가 다른 어떤 취약점 공격이나 일반적인 정보시스템 고장으로 인해 발생되는 문제보다 훨씬 심각하다[1].

DoS 공격의 경우 공격대상 호스트의 권한을 획득하지 않아도 공격이 가능하므로 호스트 자체의 보안만으로는 방어가 어렵다. DDoS 공격은 목표 호스트 이외에 공격에 이용된 호스트와 네트워크의 자원을 낭비하므로 트래픽이 증가하여 여러 지역에서 동시에 피해가 발생한다. 이러한 특징 때문에 DDoS 공격탐지를 위해 라우터와 네트워크에서 탐지하고 즉각 대응하는 시스템이 제안되었다[16]. 본 논문은 DDoS 공격 대응시스템에서 효과적인 악성에이전트 제거를 위해 사용되는 악성에이전트 제거 모듈을 설계하였다. 2장에서는 DoS와 DDoS의 공격에 대해 분석하고 현재의 대응방법에 대해 알아보고 3장에서는 제안된 DDoS 공격 대응시스템을 설명하며, 4장에서는 악성에이전트에서 악성프로그램을 탐지하고 제거하는 시스템을 설계하고 5장에서는 이 시스템의 효과적 활용 방안 등에 대해 알아보도록 한다.

2. 관련연구

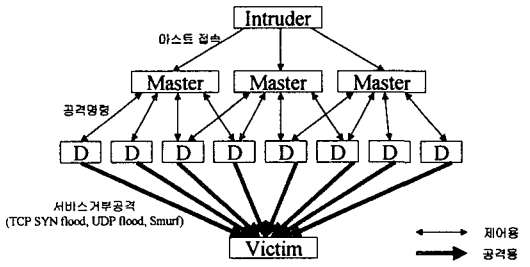
2.1 서비스거부(Denial of Service)공격

포괄적인 의미에서 서비스거부(DoS) 공격은 정보시스템 또는 서비스의 정상적인 운영을 방해하는 모든 행위를 말한다[9]. 따라서 시스템 관리자나 사용자의 실수에 의해서 발생될 수도 있으며, 의도적으로 이러한 공격행위를 유발시킬 수도 있다. DoS 공격은 공격방법도 대단히 다양하고, 단순한 공격방법이 많으며, 공격 목표 시스템의 사용자권한을 가지지 않고도 공격이 가능하므로 누구나 쉽게 공격할 수 있는 반면 공격 피해자 입장에서는 대응이 쉽지 않고 공격자를 추적하기 힘든 특징을 가지고 있다. 물리적으로 컴퓨터 시스템에 접근하거나 로컬 시스템에 사용자 계정을 가진 상태에서 가능하며, 간단한 C코드나 쉘스크립트를 이용해서 공격할 수 있는 **내부공격**과 원격지에서 네트워크를 통하여 비정상적인 패킷이나 다량의 패킷을 전

일반적으로 말하는 서비스거부 공격은 외부에서의 공격을 말하는 것으로 네트워크 서비스거부(Network Denial of Service) 공격 또는 원격 서비스거부(Remote Denial of Service)공격이라고도 한다[6]. 네트워크 DoS공격은 Ping flooding, SYN flooding, smurf 등 공격 기법이 대단히 다양하며, 유닉스시스템 뿐만 아니라 윈도우즈 시스템에서도 Winnuke, Teardrop, Land 등의 공격기법이 존재한다[13]. 이 공격들은 공격 목표 시스템에 아무런 사용자 권한이 없이도 가능하며, TCP, IP, ICMP 등 네트워크 프로토콜의 설계상 취약점을 이용한 공격이다.

2.2 분산서비스거부(Distributed Denial of Service)공격

비교적 단순한 전통적인 DoS 공격에 비해 DDoS 공격은 지능화, 자동화, 대규모화, 분산화된 공격기법이다. DDoS 공격 개요도는 (그림 1)과 같다.



(그림 1) 분산서비스거부 공격 개요도

DDoS 공격 시스템은 마스터와 데몬이라는 시스템들로 구성되어 있다[2,3,4,10,11]. 마스터이란 공격자로부터 접속을 허용하여 명령어를 입력받아 데몬에 그 명령을 전달하는 시스템이고, 데몬이란 마스터 시스템으로부터 공격 명령을 받아 공격대상 호스트에 다량의 데이터 패킷을 전송하는데 이용당하는 시스템이다. 공격자는 몇 개의 마스터 프로그램이 설치된 호스트를 제어하며, 이 마스터 프로그램은 또한 데몬 프로그램이 설치되어 있는 다수의 호스트를 제어한다. 이 데몬 프로그램들이 실제 목표 시스템에 DoS 공격 패킷을 보내게 된다. 공격 패킷은 SYN flooding, UDP flooding, ICMP echo requesting, ICMP broadcasting 등 다양하다. DDoS 공격은 이처럼 다수의 마스터와 그보다 훨씬 많은 수의 데몬들로 이루어져 있어 피해자 입장에서는 수십개 혹은 수백개의 호스트에서 동시에 엄청난 패킷을 받게 되는 것이다. 그러므로 DDoS 공격의 목표 시스템이나 네트워크는 물론이고 공격에 이용되는 마스터와 데몬이 설치된 호스트들도 서비스가 지연되거나 마비된다.

DDoS 공격에는 주로 Trinoo, TFN, Stacheldraft, TFN2K, Shaft 등의 공격툴이 이용되는데 최근에 윈도우즈용 DDoS 공격 도구도 등장하여 DDoS 공격에 윈도우즈 시스템까지도 이용되고 있음을 보여준다. 이러한 다양한 공격툴들은 파괴력이 한층 증가되었고, 또한 자동 업그레이드 기능을 가지고 있다.

공격자들이 이미 공격한 타 시스템을 DDoS 공격에 이용하여 자신의 공격 출처를 숨김과 동시에 자원을 이용한다. 이처럼 DDoS 공격은 전통적인 DoS 공격에 비해 훨씬 지능적이고 복잡해지고 있기 때문에 이에 대한 대응 또한 쉽지 않다.

2.3 DoS 및 DDoS 탐지 및 대응 기술

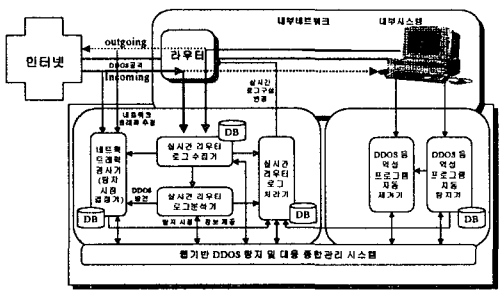
DoS 공격은 효율성에 중점을 둔 프로토콜 설계상의 보안취약점을 이용한 것이므로 프로토콜 설계가 바뀌지 않는다면 궁극적인 대응이 힘들다. 또한 대부분 공격 출처를 속여서 공격을 하고 있어 공격자를 찾기가 쉽지 않다. 더군다나 최근 발생되고 있는 DDoS 공격은 많은 시스템을 공격한 후 DoS 공격용 프로그램들을 분산 설치하여 이들을 후면에서 제어하고 있기 때문에 공격자를 찾기는 훨씬 힘들어지고 있다. DDoS 공격이 여러 시스템을 이용하여 공격하고 있으므로 자신의 시스템이나 네트워크만 보안 관리한다고 해서 이 공격으로부터 안전할 수는 없다.

기술적으로 DDoS 공격에 대응하기 위한 노력들이 논의되고 있고 기술들이 제안되고 있다[1,7]. 라우터 혹은 firewall을 이용하여 위장된 IP가 밖으로 나가거나 들어오는 것을 방지하거나 단위시간 동안 일정량 이상의 패킷은 통과시키지 않도록 하는 기술(Committed Access Rate, CAR)등 라우터를 이용한 차단 기술과 네트워크 스캔도구 및 모니터링 도구를 이용하거나 침입탐지시스템을 이용한 탐지가 가능하다. DDoS 공격은 많은 양의 패킷을 동시에 보내 네트워크/시스템의 부하를 증가시켜 서비스를 방해하는 기술이므로 load balancing 기술을 이용할 수 있다. 또한 DDoS 공격이 이루어지기 위해서는 우선 여러 시스템들에 공격 프로그램을 설치해야 하므로 각 호스트들의 rpc.statd, automountd, ttdbserverd, rpc.cmsd, amd, mountd등의 네트워크 프로그램의 보안취약점을 제거하여야 한다. 바이러스 백신처럼 각 호스트에 DDoS 공격툴이 설치되어 있는지 탐지하는 기술을 이용한다.

3. DDoS 공격 대응시스템

DDoS 공격을 탐지 - 대응 - 예방하기 위해서는 네트워크, 시스템, 응용 프로그램 등의 보안 요소를 모두 고려해야 하며, 특정 부분에 대한 보안보다는 모든 부분의 보안 요소를 관리할 수 있는 통합된 보안 관리 시스템이 요구된다. DDoS 공격 대응시스템은 크게 두 가지 모듈로 구성한다[16].

첫 번째 모듈은 네트워크 패킷을 분석하거나 라우터에서 발생된 로그를 분석하여 DDoS 공격을 탐지하고 실시간으로 라우터의 구성정보를 변경함으로써 효과적으로 DDoS 공격을 차단할 수 있는 **실시간 공격탐지 및 차단 모듈**이다. 두 번째 모듈은 DDoS 공격에 이용된 호스트들 즉, 악성에이전트에서 DDoS 공격 도구 등을 자동으로 찾아내어 제거하는 **악성에이전트 제거 모듈**이다.



(그림 2) 전체 시스템 구조

이 두 가지의 모듈을 동시에 통합하여 사용함으로써 DDoS 공격으로부터 신속한 방어와 각 호스트들이 DDoS 공격에 이용당하는 것을 봉쇄할 수 있도록 한다. (그림 2)는 실시간 공격탐지 및 차단 시스템과 악성프로그램 자동 탐지 및 제거 시스템으로 구성된 DDoS 공격대응 시스템의 전체적인 구조이다.

실시간 공격탐지 및 차단 시스템은 DDoS 공격을 라우터와 네크워크에서 수집 가능한 로그 정보들을 효율적인 알고리즘을 이용하여 로그들을 분석, 라우터의 설정을 변경하여 공격에 대응하고, 공격에 이용된 호스트들에 대한 정보를 데이터베이스화시킨다[16]. 악성에이전트 제거 시스템은 공격호스트들의 정

보를 실시간 공격 탐지 및 차단 시스템에서 만든 공격에 이용된 시스템, 즉 악성에이전트에 대한 정보를 데이터베이스에서 참조하여 대상 호스트에 조취를 취함으로 악성프로그램을 탐지하고 제거한다.

4. 악성프로그램 탐지 및 제거 시스템 설계

DDoS 공격에 신속한 대처와 재발을 방지하기 위해서는 마스터와 데몬으로 이용된 서버들을 복구시키는 것이 중요하다. 그러므로 DDoS 공격을 탐지한 후 대응시스템에서 수집한 정보를 기반으로 하여 마스터와 데몬으로 이용된 호스트를 찾아내고, 이러한 호스트들 내부의 악성프로그램을 탐지하고 제거 해야만 한다.

4.1 요구사항 분석

악성프로그램 탐지시에는 DDoS 공격에 주로 이용되는 악성프로그램들을 분석하고 그들의 특징을 데이터베이스로 구체화 시켜 정보를 가지고 있어야한다. 또한 악성프로그램들이 이용하는 네트워크 프로토콜들의 허점을 분석해야 한다. 악성프로그램 제거를 위해서는 악성프로그램으로 의심되는 파일을 찾았을 때 무조건 제거할 경우 시스템에 문제를 일으킬 수 도 있다. 탐지된 프로그램이 명백한 악성프로그램인지 치밀한 검사가 필요하고, 악성프로그램이라고 판명 될 시에는 관리자에게 확인절차를 거친 후 제거하기로 한다. 또한 백도어 발견 시에는 관리자에게 경고를 보내어 호스트의 설정을 바꾸도록 한다.

4.2 고려사항

악성프로그램을 탐지하고 제거하기 위해서는 이일을 수행하는 프로그램이 로컬에서 실행되어야 한다. 마스터나 데몬으로 이용된 호스트들이 침입탐지시스템을 설치하지 않았거나, 설치했더라도 활용했을 가능성은 희박하다. 그러므로 원격에서 이러한 일을 대신 하는 프로그램을 수행 시킬 수 있다면 보안에 취약한 호스트들을 많이 감소시킬 수 있을 것이다. 또한 빠르게 변화하는 해킹툴에 새로운 기술로 대처 가능하게 된다. 프로그램을 원격 호스트에서 실행 시키기 위해서는 모빌에이전트(Mobile Agent) 기술을 적용한다. 하지만, 이 모빌에이전트는 자신이 실행 할 플레이스(Place)가 있어야만 한다[15]. 본 논문에서는 모빌에이전트를 적용하기 위해 Java 기반의 이동 에이전트 시스템을 활용한다.

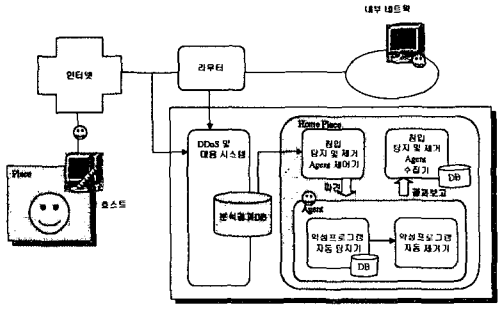
4.3 시스템 설계

악성프로그램 탐지 및 제거 시스템은 DDoS 공격 탐지 및 대응시스템이 분석해 놓은 자료를 바탕으로 악성에이전트를 결정한다. 대응시스템이 DDoS 공격으로 판단하였을 경우 패킷 분석을 통해서 DDoS 공격에서 마스터와 데몬으로 이용된 호스트들을 찾아낼 수 있다. 이러한 호스트들에 즉각 악성프로그램 자동 탐지 및 제거 에이전트를 파견하여 신속히 대처함으로써 DDoS 공격을 중단시키고 재발을 방지하도록 한다. (그림 3)은 악성에이전트 제거 모듈의 구조이다.

악성에이전트 제거 시스템은 크게 세 부분으로 이루어진다.

o 악성프로그램 자동 탐지 및 제거 에이전트

자동으로 악성프로그램을 탐지하고 제거하는 모든 기능을 가지고 있는 에이전트이다. 이 에이전트는 DDoS 공격이 발생한 후 검출된 마스터와 데몬, 즉 악성에이전트들에게 파견하므로 에이전트로 인한 오버헤드는 보통 때는 거의 없게 된다. DDoS 공격 탐지 때가 아닌 주기적으로 악성프로그램 자동 탐지 및 제거 에이전트를 파견하여 호스트들은 관리 할 수도 있다.



(그림 3) 악성에이전트 제거 모듈의 구조

o 중앙 제어 시스템 (또는 Home Place)

DDoS 공격 대응시스템이 만들어 놓은 자료를 통하여 악성프로그램 자동 탐지 및 제거 에이전트를 파견할 호스트를 결정하고, 이 에이전트에 관한 모든 제어를 해주는 부분이다. DDoS 공격이 발견 될 때는 물론이고 각 호스트에 에이전트를 파견하는 주기를 결정하고 파견한다. 수행 후 돌아온 에이전트에서 결과 보고를 받아 로그를 작성한다.

o 플레이스 프로그램(Place Program)

악성프로그램 자동 탐지 및 제거 에이전트가 각 호스트로 이동할 수 있는 기본 환경을 마련하기 위한 프로그램이다. 이 프로그램은 에이전트 파견 대상 호스트의 자원을 거의 사용하지 않게 설계한다. 그리고 한번 설치 이후에는 자동으로 기능 등을 업데이트하고 새로운 해킹툴에 대한 대응법을 탑재한 새로운 악성프로그램 자동 탐지 및 제거 에이전트들이 와서 실행 가능하도록 한다.

이러한 시스템을 활용하기에 가장 중요시 되는 점은 보안문제이다. 본 논문에서 제시하는 시스템도 원격에서 각 호스트에 영향을 미치는 것이기 때문에 각 호스트 입장에서 볼 때는 해커의 공격과 다른 점이 없다. 그러므로 시스템에서 파견하는 에이전트들 또는 그들이 행하는 모든 작업들은 각 호스트에 대한 실행 권한을 가져야 한다. 그러기 위해서 악성프로그램 탐지·제거 에이전트는 인증을 받아야 한다. 이러한 방법의 하나로 각 에이전트는 전자서명(Digital Signature)을 이용하겠다. 또한 인증받은 에이전트일지라도 권한 이상 행위를 취할 수도 있으므로 Java의 보안모델을 적용한다[17]. Java는 네트워크를 통해 전송 받은 코드에 대해 시스템의 안전성을 보장하기 위해 보안 관리자(security manager)를 사용한다. JVM(Java virtual machine)의 보안 관리자는 네트워크를 통해 수신한 코드에 대해 로컬시스템의 상태를 얻거나 변경할 수 있으며 자신의 코드를 전송한 소스 시스템 이외의 곳과는 통신 할 수 없도록 하는, SandBox라 불리는 제한을 적용한다. 그러므로 Place를 사용하기 위해 악의로 만들어진 프로그램은 시스템에 어떠한 영향도 미치지 못하게 한다. 이러한 방법에 의해서 악성프로그램 자동 탐지 및 제거 에이전트를 파견함으로 발생하는 보안문제를 해결하고자 한다.

4.4 DDoS 프로그램 검색

DDoS 공격에 이용되는 주요한 공격툴에는 Trinoo, TFN, stacheldraft, Shaft, TFN2K, mstream 등이 있다. 이와 같은 DDoS 프로그램은 코드 내에 특정 문자열을 가지고 있어 구별

이 가능하다. 또한 공격툴들이 인터넷상에서 배포될 때 디폴트로 지정된 파일 이름, 파일 사이즈, 사용하는 포트 검색 등을 이용하는 방법도 있다. <표1>에서 보이듯이 대표적인 DDoS 공격툴, Trinoo에서는 마스터 프로그램은 "..."라는 이름의 파일에 데몬들의 목록을 암호화된 형태로 저장하고 데몬들은 ns, http, rpc.trinoo, rpc.listen, trinix, rpc.irix, irix 라는 이름으로 설치되므로 이러한 파일들을 찾아내어 분석하기로 한다. 공격툴들은 각자 특정한 포트를 이용하는 경우가 많고 특정한 패킷이 주로 등장하므로 이를 분석하여 활용하고자 한다. 또한 악성프로그램이 발견된 호스트의 경우 보안에 대한 대책이 취약한 경우가 대부분일 것이다. 악성프로그램이 설치될 때 이용되었을 백도어등도 함께 탐지하여 제거하고 안전한 호스트 구축을 위한 설정을 제시해주기로 한다.

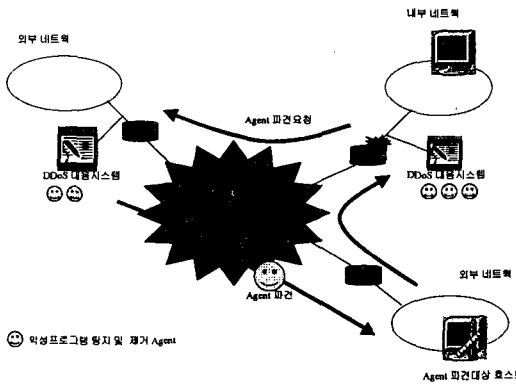
a : attacker / **m** : master / **d** : deamon

사용port	a->m:27665/tcp m->d:27444/udp d->s:31335/udp d->m:27444/udp
문자열	*HELLO* PONG
마스터와 데몬이름	m: rpc.listen, tserver1900 d: httpd, tsolnmb, rpc.trinoo, rpc.listen, trinix, rpc.irix, irix
이용 패킷	UDP flooding
탐지방법	1. 트윅 트래픽 성능저하가 발생할 경우 snoop, tcpdump 명령을 이용하여 UDP,ICMP,TCP 패킷증가를 검사 2. nmap을 이용 포트검색
제거방법	· trinoo프로그램 이름 찾아본다. · crontab에서 trinoo위치찾기. #more /var/spool/cron/crontabs/root ****** /dev/isdn/.subsys/tsolnmb > /dev/null 2> &1 · netstat , ps명령사용

<표 1> Trinoo의 대표적 특징정리

4.5 DDoS 에이전트 제거

DDoS 공격 발생시 라우터는 현재 트래픽이 폭주한 상태일 것이므로 에이전트 파견이 라우터의 트래픽에 영향을 미칠 수 있다. 그러므로 DDoS 공격을 탐지한 라우터 근처의 대응시스템에서는 대상 호스트를 결정, 파견을 명령하고 실제로 에이전트 파견은 네트워크 부하가 적은 다른 대응시스템이 이행한다. (그림 4)와 같은 에이전트의 이동을 보이게 된다.



(그림 4) 악성에이전트 탐지 및 제거 개요도

악성프로그램 자동 탐지 및 제거 에이전트의 악성프로그램 자동 탐지기에서 찾아진 결과는 악성프로그램과 백도어들이다. DDoS 공격에 이용되는 툴의 경우 관리자에게 존재 사실을 알리고 제거한다. 백도어들에 대해서는 관리자에게 존재 사실과 그에 대한 정보와 백도어 유발 가능한 취약점을 알려주어 대응책을 알려준다.

파견된 악성프로그램 자동 탐지 및 제거 에이전트는 전자서명(Digital Signature)을 통해 인증되어 로컬시스템내의 악성프로그램을 탐지 및 제거하는 권한을 부여받았지만 시스템 전체에 영향을 미치는 시스템 설정 파일 등을 변경시키는 권한은 부여받지 않았으므로 관리자에게 호스트의 취약 사실을 경고함으로써 대체한다.

5. 결론

근래에 뉴스를 장식했던 yahoo 해킹사건을 시작으로 세계 주요 인터넷 사이트의 해킹은 DDoS 공격에 대한 위험성을 증명하기에 충분했다. DoS 와 DDoS 공격은 자신의 호스트 보안을 철저히 해도 공격당하는 위협은 변하지 않는다. 이러한 특성 때문에 DDoS 공격 탐지를 위해 라우터와 네트워크에서 탐지를 시도하고 정보를 모아 분석하는 시스템 제안되었고, 본 논문에서는 DDoS 공격에 대해 빠른 대처와 재발을 막기 위해 DDoS 공격대응 시스템의 악성에이전트를 탐지하여 제거하는 모듈을 제안하였다. 이 대응시스템은 어느 한 네트워크에서 사용되는 것보다 주요지점에 설치하고 상호 협조하여 이루어지면 큰 효과를 얻을 수 있겠다. 특히, 악성에이전트 제거 시스템은 각 호스트에 기본 Place설치만 하면 중앙시스템에서 새로운 공격에 대응하는 기능과 기존의 대응법, 그리고 취약점 분석까지 해주는 에이전트를 파견하여 침입탐지기능을 해줄 수 있다. 기본 플레이스만을 설정해줌으로써 광대한 범위의 호스트들까지 제어가 가능하므로 네트워크 관점에서 접근하는 DDoS 공격에 대응하는 시스템을 보다 효과적으로 만들어준다.

<참고문헌>

[1] Mixter, *"A guide to improving network security to protect the Internet against future forms of security hazards"*, http://www.packetstorm.securify, 2000.

[2] CERT, *"Distributed Denial of Service Tools"*, http://www.cert.org, 1999.

[3] CERT, *"Results of the Distributed-Systems Intruder tools Workshop"*, http://www.cert.org, 1999.

[5] *"Stacheldraht Analysis"*, http://staff.washington.edu/, 1999.

[6] NIPC, *"Trinoo/Tribal Flood Net/tfn2k"*, http://www.nipc.gov/, 1999.

[7] Hans Husman, *"Introduction to Denial fo Service"*, 1996.

[8] *"Essential IOS Features Every ISP Should Consider Version 2.82"*, Cisco Systems, 1999.

[9] *"99 해킹 · 바이러스 현황 및 대응"*, 한국정보보호센터, 1999.

[10] *"98 해킹 현황 및 대응"*, 한국정보보호센터, 1998.

[11] 한국정보보호센터, *"RPC 관련 보안취약점 및 대책"*, http://www.certcc.or.kr/, 2000.

[12] 한국정보보호센터, *"분산환경에서의 서비스거부 공격 분석 보고서"*, http://www.certcc.or.kr/, 1999.

[13] 한국정보보호센터, *"Stacheldraht에 의한 서비스 거부공격 분석보고서"*, http://www.certcc.or.kr/, 2000.

[14] 정현철, *"분산서비스거부공격 등 최신 해킹기법과 대응방안"* 정보처리학회지, 2000.

[15] 정현진, *"네크워크 보안관리를 위한 이동에이전트 시스템의 설계와 구현 "*, 1998

[16] 임채호, *"분산서비스거부 공격 분석 및 대응시스템 설계"*.

[17] 안상훈, *"이동 에이전트 기술을 이용한 망 관리", 1998*