Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.4, August 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.4.729

DNS을 목표한 DDoS공격에 효과적인 대응 방법 제안*

최 지 우,† 천 명 진, 홍 도 원, 서 창 호‡
공주대학교

A Proposal Countermeasure to DDoS attacks targered DNS*

Ji-Woo Choi,† Myung-Jin, Chun, Do-Won Hong and Chang-Ho Seo‡
Kongju National University

요 약

최근 이슈가 되고 있는 DDoS 공격은 주요 정부기관 및 금융기관 인터넷 사이트를 마비시키는 사이버 테러의 수단으로 사이버 안위를 위협하고 있다. 현재 사용되고 있는 공격 방법은 기존의 방법보다 진화된 방법으로 차단이 쉽지 않아 그로 인한 피해가 커지고 있는 상황이다.

이어서, 본 논문에서는 최근 계속적으로 진화하고 있는 DDoS 공격 중에서 DNS를 목표로 하는 DDoS 공격이 발생하는 사례를 보여주었다. 그러나 현재는 DNS를 목표로 하는 DDoS 공격에 대한 방어가 미비하다. 이를 보완하기 위해서 한국인터넷진흥원에서 운영 중인 사이버대피소에 착안하여 DNS에 대한 DDoS 공격의 대응 방안으로 DNS 사이버대피소를 제안하고자 한다.

ABSTRACT

The recent issue of distributed denial of service attack paralyze major government and financial institution in internet sites. They threatened to the cyber security. There hasn't been easy defense of now using attack. There seems to be increases in damage. In this paper, The recent continue to evolve of distributed denial of service attack. DNS target of distributed denial of service attack give specific examples. but, DNS target of DDoS attacks about defense is insufficient. The DNS Cyber-shelter system was created based on the Cyber-shelter system for DDoS attack in Kisa.. We proposal DNS Cyber-shelter system.

Keywords: DNS, DDoS, Cyber Urgent Shelter

I. 서 론

과거 인터넷은 연결이 필요할 때, 모뎀이나 전화 접속하여 인터넷에 연결하는 형태이기 때문에 방화벽으로 사용자를 보호하지 않아도 별다른 문제가 되지 않았다.

또한 연결 지속 시간이 짧고 할당된 IP 주소가 유동적이었으므로 해커와 다른 외부 위협이 PC로 침투하기가 어려웠다. 하지만 현재 인터넷은 단일 매체를 통하여 수많은 정보를 공유하고 사회 문화 경제 교류를 확대하며, 편리한 생활을 제공하는 등 우리 생활의 다방면에서 삶의 질을 높여주는 긍정적인 효과를 제공하고 있다. 하지만 인터넷만 들어가면 수많은 해킹 관련 도구들을 자유롭게 얻을 수 있어 초보 해커들도 컴퓨터의 취약점을 쉽게 찾아내 악용하고 있으며 정보 소스를 자유롭게 제공하기 때문에 전산망 침입자들의 위협이 항상 도사리고 있다. 이러한 문제점은 개인뿐만 아니라 기업과 정부 등 국가 기반에 까지 영향을 미쳐, 향후 큰 사회적 문제를 일으킬 수 있는 잠재적

접수일(2013년 4월 22일), 수정일(1차: 2013년 6월 7일, 2차: 2013년 7월 1일), 게재확정일(2013년 7월 8일)
* 본 연구는 한국연구재단 연구과제 지원 및 지역혁신인력 양성 사업에 의해서 수행하였습니다.
(No. 2013R1A1A2010382, 2013H1B8A2032077)
† 주저자, liewhite@kongju.ac.kr
‡ 교신저자, chseo@kongju.ac.kr(Corresponding author)

위험성을 내포하고 있다. 현재 보유한 보안 시스템만으로 DDoS 공격을 효과적인 대응을 하기 위해서는 공격 방법에 따라 적절한 대응이 필요하게 된다[1].

본 논문의 구성은 다음과 같다. 1장에서는 서론에 이어 2장에서는 DDoS의 정의와 여러 가지 공격기법과 방어기법에 설명하고, 3장에서는 DNS의 구조 및 DNS를 목표로 하는 DDoS공격 기법들을 설명하였다. 4장에서는 논문에서 제안하고자하는 DNS 사이버대피소의 구조 및 제안 알고리즘으로 구성하였다, 5장에서는 실험 예측 결과를 작성하였다. 마지막으로 6장에서는 결론을 도출한다.

II. 관련 연구

2.1 DDoS(Distribute Denial of Service)란?

DDoS(Distributed Denial of Service, 분산 서비스거부) 공격이란 해당 시스템의 정상적인 서비스를 방해하는 사이버 공격을 뜻한다. DDoS는 다수의 PC를 이용하여 특정 시스템으로 대량의 유해 트래픽을 전송함으로써 해당 시스템을 공격한다. DDoS 공격에 사용되는 PC는 DDoS가 유포시킨 바이러스성 프로그램에 감염된 일반 PC이다.

2.2 DDoS 공격의 유형 및 특징

DDoS 공격 유형으로 2가지가 있다. 첫 번째로, 악성 봇(Bot)을 이용한 DDoS 공격이 있는데, 해커는 다양한 방법으로 일반 사용자 PC에 봇을 감염시키고, 봇에 감염된 PC에 공격 명령을 지령하여 DDoS 공격을 수행하게 된다. 다른 유형으로는 신종 악성코드를 이용한 공격이 있다. 이 유형의 특징은 명령 및 제어 서버의 접속 없이 악성코드에 감염된 컴퓨터를 실행하면 자동으로 특정한 사이트를 공격하도록 제작·유포되어 서비스를 방해한다[2].

위와 같이 DDoS 공격은 공격자가 일반 사용자들의 PC에 악성 코드를 심어 감염시킨 후 감염된 PC를 이용하여 특정 웹 사이트나 서버에 대량의 트래픽을 송신하는 공격방법으로서 감염자의 PC를 이용하기 때문에 공격자 스스로가 외부에 노출되지 않으면서도 대량의 데이터를 보낼 수 있다는 특징이 있다. 현재에 들어서는 C&C(Command and Control)서버 등을 이용하여 손쉽게 목적지를 변경 가능하며, 공격 방식 또한 여러 가지 형태로 바꾸는 형태로 계속적으로 진화해 나가고 있다.

2.3 DDoS 공격 기법

UDP Flooding, ICMP Flooding 공격을 수행할 때, 단일 Zombie PC에서 발생시키는 패킷은 그 크기가 다양하며, 전송 간격 또한 다양화하게 된다. 하지만 Firewall로 모든 패킷이 집중되어 단일 시간에 대량의 패킷이 한 곳으로 집중되는 현상이 발생한다.

Cache-Control Attack은 지난 2010년 7.7사건에서 주 공격기법으로 사용된 이후 매우 강력한 DDoS 기법중 하나로 인식되었다. 이 공격은 HTTP User-Agent 헤더에 불필요한 값을 추가하여 웹서버의 오동작을 일으킨다. 공격은 수백에서 수 천개의 Zombie PC가 1분에 300~400개의 Syn패킷을 보내며, 불규칙한 시간 간격을 두고 공격하는 기법이다.

2.4 DDoS 방어 기법

DDoS 공격은 대부분 특정한 목표를 정하고 이에 대해 집중적인 공격을 하게 된다. 이를 효과적으로 방어하기 위해서는 각 기관의 담당자의 네트워크 단에서의 상호 협조가 필요하며, 또한 공격을 방어하는 것이 아닌 공격이 시작되기 전에 Zombie PC가되는 것을 예방하는 것 또한 DDoS에 대한 효율적인 방어 방법이 될 수 있다.

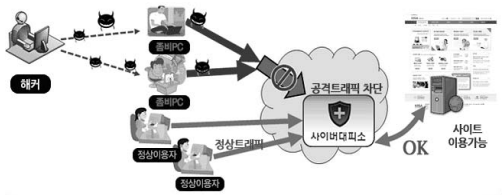
DDoS 방어 기법에는 ISP 라우팅, DNS-Sinkhole이 있다. ISP 라우팅은 각 ISP에서 Null0 Routing을 통하여 악성 트래픽을 ISP 자체에서 방어하는 방법이다. DNS-Sinkhole은 DDoS의 가장 큰 적인 좀비PC를 막는 방법으로서 좀비PC가 C&C로 접속하여 공격 지령을 받는 것을 방지하기 위하여 C&C 도메인으로 접속하는 모든 트래픽을 우회시켜 지령을 받지 못하게 함으로써 DDoS공격을 원천 차단하는 방어 방법이다.

2.5 사이버 대피소

DDoS 공격기법이 변화함에 따라 이에 대한 방어기법도 변화하고 있다. DDoS공격은 대용량의 트래픽 전송을 통한 네트워크 대역폭 마비에서 시작하여 근래에 들어서는 시스템 자원 고갈 형태로 진화하고 있다. 이 때문에 정상 트래픽과 공격 트래픽을 분류하기가 매우 어려워지고 있으며, 좀비 PC를 이용한 동시 다

발적인 공격으로 시스템 자원 고갈 현상 및 대역폭 마비 현상까지 발생함으로 방어가 어려워지고 있다. 위와 같은 공격에 대해서 방어하기 위해서, 한국인터넷진흥원에서는 사이버 대피소를 만들어 운영하고 있다.

사이버 대피소는 DDoS공격이 발생 시 피해 시스템이 등록된 DNS의 IP주소를 변경하여 피해 시스템이 아닌 사이버 대피소로 모든 트래픽을 우회토록 하여 총 3단계의 구성을 통해 원활한 서비스 운영을 가능하도록 하는 방어 기법이다[3].



[그림 1] DDoS 사이버 대피소

2.5.1 사이버 대피소의 구조

사이버 대피소는 3단계의 구조로 나타낸다.

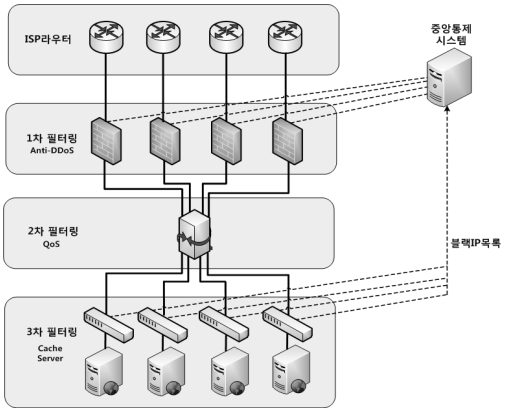
1단계에서는 DDoS전용 대응장비와 ISP와의 협업을 통해 UDP·ICMP Flooding과 같은 전통적인 네트워크 자원 소모성 공격에 대한 방어를 수행 한다.

2단계에서는 QoS장비를 활용하여 사이버대피소로 유입되는 발신지 IP를 좀비 PC와 정상 사용자로 구분하여 적절한 가용량을 할당한다.

3단계에서는 L7스위치와 웹캐싱을 통해 트래픽을 단순화하고 부하를 분산시켜 공격대상 웹서버의 가용성을 확보한다.

또한 이 단계에서는 공격 트래픽의 헤더와 페이로드를 상세하게 분석하여 공격 차단에 활용한다.

위의 [그림 2] 사이버 대피소는 DNS 우회 변경을 수행하여 보호대상 웹서버의 물리적인 이동 없이 DDoS 공격 방어를 수행한다. 일반적으로 사용자의 홈페이지 접속은 웹브라우저에 접속하고자 하는 홈페이지 도메인 정보를 입력하면 DNS로 해당 도메인의 IP를 질의(DNS Query)하게 되며 DNS는 도메인의 IP정보를 확인하여 사용자에게 전달하게 되고 사용자는 홈페이지에 접속하는 과정을 거치며, 방어대상 홈페이지의 도메인정보 질의 값을 사이버 대피소 IP로 변경함으로 서 본래 홈페이지의 웹서버로 향하는 모든 트래픽이 사이버대피소를 통과하도록 한다. 사이버대피소는 공격 트래픽은 차단하고 정상 접속요청만



[그림 2] 사이버 대피소 구조

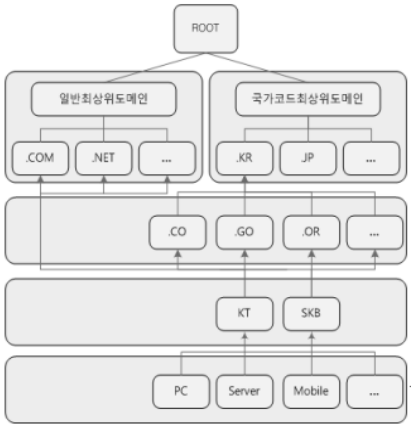
을 웹서버로 전달하며 이때 Cache기능을 통해 본래 홈페이지의 웹서버의 부하를 최소화한다.

III. DNS(Domain Name System)란?

도메인 네임 시스템(domain name system, DNS)는 호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행할 수 있도록 하기 위해 개발되었다. 특정 컴퓨터(또는 네트워크로 연결된 임의의 장치)의 주소를 찾기 위해, 사람이 이해하기 쉬운 도메인 이름을 숫자로 된 식별 번호(IP 주소)로 변환해준다. 도메인 네임 시스템은 흔히 "전화번호부"에 비유된다. 인터넷 도메인 주소 체계로서 TCP/IP의 응용에서, www.example.com과 같은 주 컴퓨터의 도메인 이름을 192.168.1.0과 같은 IP 주소로 변환하고 라우팅 정보를 제공하는 분산형 데이터베이스 시스템이다[4].

3.1 DNS 작동 구조

인터넷 상의 모든 도메인은 ROOT라 불리는 도메인 이하에 [그림 3]과 같은 역트리(Inverted Tree) 구조로 계층적으로 구성되어 있다 ROOT 도메인 바로 아래의 단계를 최상위 도메인(TLD, Top Level Domain)이며, 2단계 도메인(SLD, Second Level Domain)은 2단계 도메인 아래에서는 각각의 ISP(Internet Service Provider)가 운용하는 Recursive DNS서버가 운용되고 있다. 이러한 Recursive DNS서버는 일종의 Cache서버 및 다른 TLD나 SLD의 주소를 사용자에게 알려주는 역할을 하게 된다.



〔그림 3〕 DNS 구조

3.1.1 DNS Flooding Attack

DNS Flooding Attack은 대표적인 DNS에 대한 공격 방법이다 DNS Flooding Attack은 대량의 사용자가 DNS에 대한 대량의 질의를 보내어 DNS가 정상적인 서비스를 제공하지 못하도록 하는 일종의 DoS공격이라 할 수 있다 하지만 DNS는 자체적인 프로토콜 한계로 인하여 공격에 대한 자체적인 방어가 어렵다는 단점이 존재하고 서비스를 제공하기 위해서는 포트 차단 등 다른 방어방법을 사용할 수 없다는 한계가 존재하기 때문에 지금도 유효한 공격 기법이라 할 수 있다.

3.1.2 DNS Amplification Attack

DNS Amplification Attack은 2006년 발견된 DNS공격기법의 하나로서 미국US-CERT(United States Computer Emergency Readiness Team)에서 공식적으로 경고를 함으로서 널리 알려진 공격 방식이다.

DNS Amplification Attack은 재귀적 질의(Recursive Query)를 허용하는 DNS를 이용한 공격으로서 DNS간 데이터 전송에 이용되는 재귀적 질의는 전송되는 데이터량이 크고 다른 DNS 질의보다 우선된다는 점을 악용하여 재귀적 질의를 허용한 DNS를 이용하여 다른 DNS를 공격하는 방법이다〔5〕.

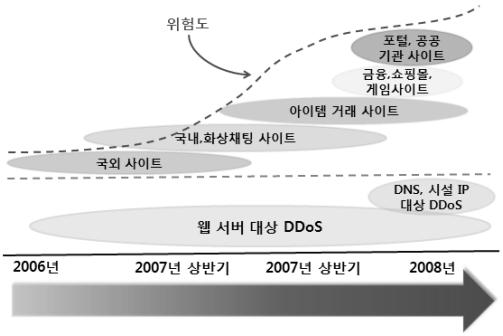
3.1.3 DNS Cache Poisoning

DNS Cache Poisoning 공격은 취약한 DNS 서버에 조작된 질의를 전송하여 주소 Cache정보를 임의로 변조하는 공격을 의미한다. DNS Cache Poisoning 공격은 먼저 재귀적 질의가 허용되는 DNS를 검색하는 것부터 시작한다. 재귀적 질의가 허용되는 DNS를 찾게 되면 먼저 해당 DNS에 질의를 하여 다른 DNS와의 통신 상태를 확인한 후 위조된 DNS 응답 Query를 전송해 해당 DNS가 잘못된 DNS 정보를 갖도록 공격 한다. 이로 인하여 정상적인 IP정보가 아닌 위조된 IP주소를 갖게 된 DNS는 다른 DDoS 공격 등에 사용되는 DNS서버로 악용되게 된다〔6〕.

3.2 DNS를 목표로 하는 DDoS 공격 사례

DNS는 인터넷의 핵심 서비스 중 하나이기 때문에 다른 서버들과 같이 많은 공격을 받아왔다. DNS에 대하여 가장 큰 공격은 2003년 1월 23일에 발생한 인터넷 대란일 것이다. 당시 Slammer Worm으로 인하여 발생한 DNS에 대한 DNS Flooding Attack 공격으로 인하여 국내 인터넷이 마비되는 초유의 사태가 벌어졌으며, 물론 의도된 DNS Flooding Attack공격은 아니었으나, 특정 DNS로 사용자가 몰리면서 발생한 DDoS는 실제 공격보다 더욱더 큰 피해를 가져오게 되어 국내 인터넷망의 마비라는 결과가 발생하게 되었다. 2009년 12월 크리스마스 시즌을 맞아 대대적인 매출을 기대하던 아마존 등 거대 쇼핑몰 일부가 접속이 불가능한 상황이 발생하였다. 이는 아마존 등의 쇼핑몰에 대한 공격이 아닌 해당 업체가 사용 중인 Ultra DNS의 DNS서버들이 공격을 받으면서 Utra DNS의 고객사였던 아마존 등의 쇼핑몰 사이트가 서비스 중단된 상황 이었다. 크리스마스 시즌에 대대적인 판촉행사를 벌이던 쇼핑몰사이트는 큰 피해를 입었다. 2011년 Anonymous라는 해킹그룹이 ROOT DNS를 DNS Amplification Attack 공격기법을 통하여 공격하여 전 세계적으로 비상이 걸리기도 하였다. Anonymous 그룹에서는 DNS 공격용 툴인 LOIC(Low Orbit Ion Cannon)을 공개하여 화제를 모으기도 하였다. 2012년 DNS Changer라는 악성코드로 인하여 정상적인 DNS가 아닌 해커가 운영하는 DNS로 우회되는 사태가 발생하여 전 세계적으로 DNS정보가 정상적인지를 확인하는 사태가 벌어지기도 하였다.

〔그림 4〕와 위에 여러 공격 사례들을 보면 DNS를 목표를 하는 DDoS 공격사례가 늘어나고 있고 이러한

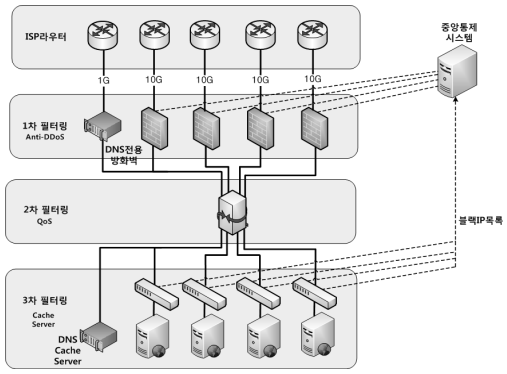


〔그림 4〕 DDoS 공격 추이

공격이 성공할 경우 큰 피해를 입을 수가 있다. DNS는 UDP를 이용하기 때문에 세션 정보 등 다른 정보가 존재하지 않고 패킷 한 두 개로서 서비스가 종료되는 단발성 서비스이다. 그러므로 DNS를 타켓으로하는 DDoS공격에 대해서 문제점을 가지고 있다.

IV. DNS 중심의 DDoS 공격에 대한 문제점 및 대응 방법 제안

DNS와 같이 인터넷 서비스와 밀접한 관계를 갖는 시설 장비에 공격이 발생할 경우 기존의 보안장비가 무력화될 수 있다. 더욱이 DNS가 문제가 생길 경우 웹 서비스 뿐만이 아니라 해당 DNS를 사용하는 일반 사용자까지도 인터넷사용에 문제가 발생하게 되므로 DNS와 같은 시설 장비의 방어가 매우 중요하다. 본 논문에서 제시하고자 하는 DNS사이버 대피소는 기존의 사이버 대피소가 갖는 구조적인 문제점인 웹서버에만 최적화된 점을 극복하기 위하여 DNS전용 장비 등을 갖춘 대용량의 DNS Cache서버를 이용하여 DNS서버 공격에 대응하는 방법을 제시하자 한다.



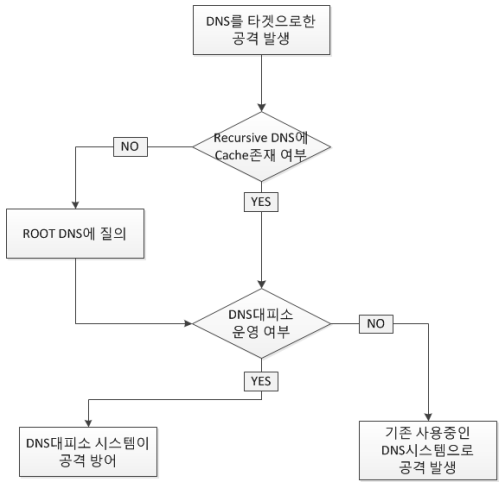
〔그림 5〕 제안한 DNS대피소 구성도

4.1 DNS 사이버 대피소 구조

DNS 사이버 대피소는 기존 사이버 대피소와 매우 흡사한 구조를 가지고 있다. DNS사이버 대피소는 DNS 전용 방어 장비 및 대용량 DNS서버를 사용하여 일종의 Recursive DNS로 운용, 기존에 사용되던 DNS를 대체할 수 있도록 한다.

4.2 DNS 사이버 대피소 대응 알고리즘

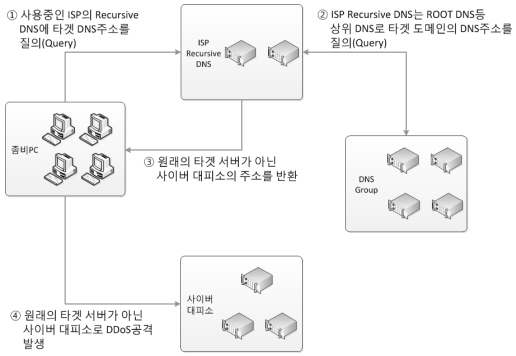
DNS 사이버 대피소의 핵심 구조는 서비스 중인 DNS로 발생하는 공격을 다른 DNS로 우회하여 대응하는 것이다. DNS서비스에서는 구조상 ROOT DNS나 다른 Recursive DNS가 캐쉬를 가지고 트리형 구조로 서비스가 되기 때문에 하위 DNS를 다른 DNS로 우회시키기 위해서는 Recursive DNS 및 ROOT DNS에서 DNS사이버 대피소 운용을 위하여 하위 DNS주소를 지정하고 적용하는 것이 필요하다.



〔그림 6〕 DNS 사이버 대피소 알고리즘

실제 공격이 발생하면 좀비PC는 ISP의 Recursive DNS에 공격 대상 DNS의 주소를 요청한다. 이때 Recursive DNS에 공격 대상 DNS의 주소가 캐쉬로 존재하면 해당 DNS주소를 공격자에게 리턴하게 된다. 그러나 캐쉬로 존재하지 않을 경우 ROOT DNS에 해당 주소를 질의하여 결과 값을 공격자에게 돌려주게 된다.

〔그림 7〕을 보면 DNS는 Recursive DNS가 동작하는 것은 다른 DNS와 동일하게 작동한다. 하지만



〔그림 7〕 DNS 사이버 대피소 Flow

ROOT DNS 및 Recursive DNS는 기존에 서비스 중인 DNS가 아닌 DNS사이버 대피소의 DNS주소를 공격자에게 돌려주게 된다. 이를 위해서는 각 ROOT DNS 및 Recursive DNS가 사이버 대피소를 사용하는 시스템에 대한 사전정보를 보유하고 있어야 하며 또한 사이버 대피소를 사용할 때와 사용하지 않을 때를 정확하게 인지하여 서로 다른 DNS주소를 반환하여야 한다. 기존 DNS가 아닌 사이버 대피소의 DNS를 반환하면 공격자의 모든 트래픽은 DNS 사이버 대피소로 보내지게 되며 DNS 사이버대피소는 대용량 DDoS방어 장비 및 대용량 Recursive DNS로서 DDoS 공격에 대응하게 되어 서비스 중단과 같은 상황에 대응 할 수가 있다.

V. 실험 예측 결과

실제 DNS DDoS 공격이 발생했을 경우를 구성하여 구성안의 성능에 대하여 실험을 해보았다.

아래와 같은 실험결과로 볼 때, DNS를 목표로 하는 DDoS 공격 1분간에 평균 트래픽을 가정하고, 1분간 웹 서비스가 되지 않을 때를 기준으로 작성하였다. 일반 DNS는 500MB 전후로 해서 실제 서비스에는 장애가 발생한 것으로 보인다. 그러나 DNS 사이버 대피소를 운영할 경우에는 500MB에서는 10 Sec으로 정상적인 서비스가 가능하다. 하지만 DDoS 공격 량이 평균 최대 2GB급 이상의 공격이 발생한다면 60.4 Sec으로 접속이 지연되어 정상적인 서비스가 어려워진다.

〔표 1〕 실험 결과

1분간 최대 트래픽	일반 DNS	Recursive DNS	DNS 대피소
100	12.474 msec	27.47 msec	8.283 msec
150	52.193 msec	95.38 msec	15.47 msec
200	2.7 sec	8.7 sec	50.12 msec
300	15.37 sec	29.39 sec	1.8 sec
500	58.89 sec	timeout	10.38 sec
1G	timeout	timeout	29 sec
1.5G	timeout	timeout	38.18 sec
2G	service down	timeout	60.40 sec

VI. 결 론

DDoS 공격 방법들이 다양하게 변화하고 있다. DDoS 공격을 살펴보면 모든 공격들을 효과적으로 차단한다는 것은 매우 어렵다는 것을 알 수 있다. 특히 최근에 발생한 DDoS 공격은 주로 특정 서버의 특정 서비스를 대상으로 하고 있어, 또한 더욱 치밀하게 전개 되고 있다. 이와 같이 문제점은 전체 인터넷의 마비로 인한 개인사용 및 국가전체의 불편함뿐만 아니라 경제적인 부분에서도 많은 손해를 입고 있다.

본 논문에서 제안한 DNS 사이버 대피소는 다양한 DDoS 공격 중에서 변화하는 특성화 공격인 DNS서버에 대한 공격을 대비하여 DNS 사이버 대피소를 제안함으로서, 웹 서버 뿐만 아니라 DNS 서비스 중단도 예방 할 수 있다.

참고문헌

〔1〕 최양서, 오진태, 장종수, 류재철, "분산서비스거부(DDoS) 공격 통합 대응체계 연구," 정보보호학회 학회지, 19(5), pp. 11-20, 2009년 10월.

〔2〕 침해예방단 웹보안지원팀 "DDoS공격r 대응에 대한 한계용량 측정 방법론 연구 최종연구보고서," KISA 연구보고서, KISA-RP-2010-0009, 2010년 09월.

〔3〕 한국인터넷진흥원, "DDoS 사이버 대피소," http://www.krcert.or.kr/kor/cyber/cyber_01.jsp

〔4〕 한국인터넷진흥원,"DNS소개," http://www.kisa.or.kr/business/address/address3_sub1.jsp

〔5〕 Georgios Kambourakis, Tassos Moschos, Dimitris Geneiatakis, Stefanos Gritzalis, "Detecting DNS Amplification

Attacks," Critical Information Infrastructures Security ser LectureNotes in Computer Science, vol. 5141, pp. 185-196, 2008.

〔6〕 US-CERT, "The Continuing Denial of Service Threat Posed by DNS Recursion(v2.0)," July. 2010.

〈저자소개〉

최 지 우 (Jil-Woo Choi) 학생회원
2009년 2월: 공주대학교 응용수학과 학사
2011년 2월: 공주대학교 바이오정보학과 석사
2011년 3월~현재: 공주대학교 바이오정보학과 박사과정
〈관심분야〉 정보보호, 네트워크 보안 등

천 명 진 (Myung-Jin Chun) 정회원
2010년 2월: 충남대학교 컴퓨터공학과 학사
2012년 2월: 공주대학교 바이오정보학과 석사
2006년~2008년: 한국과학기술정보연구원 연구원
〈관심분야〉 정보보호, 네트워크, 클러스터링 등

홍 도 원 (Do-Won Hong) 정회원
1994년 2월: 고려대학교 수학과 학사
1996년 2월: 고려대학교 수학과 석사
2000년 2월: 고려대학교 수학과 박사
2000년 4월~2012년 2월: 한국전자통신연구원 팀장, 책임연구원
2012년 3월~현재: 공주대학교 응용수학과 부교수
〈관심분야〉 암호기술, 프라이버시보호기술

서 창 호 (Chang-Ho Seo) 종신회원
1990년 2월: 고려대학교 수학과 학사
1992년 2월: 고려대학교 수학과 석사
1996년 08월: 고려대학교 수학과 박사
1996년 1월~1996년 7월: 국방과학연구소 선임연구원
1996년 8월~2000년 2월 : 한국전자통신연구원 선임연구원
2000년~현재: 공주대학교 응용수학과, 융합과학과 교수
〈관심분야〉 시스템 및 네트워크보안, 융합보안