情報保護學會論文誌
第 22 卷 第 4 號, 2012. 8

Content-Length 통제기반 HTTP POST DDoS 공격 대응 방법 분석*

이 대 섭,† 원 동 호‡
성균관대학교 정보통신공학부

Analysis of Defense Method for HTTP POST DDoS Attack base on Content-Length Control*

Dae-seob Lee,† Dong-ho Won‡
School of Information and Communication Engineering, Sungkyunkwan University Korea

요 약

OSI 7계층 DDoS 공격 기법중 하나인 HTTP POST DDoS 공격은 서버의 자원을 고갈시켜 정상적인 서비스를 방해하는 서비스 거부 공격 기법이다. 이 공격은 적은 양의 공격 트래픽만으로도 효과적인 공격이 가능하며 정상적인 TCP 연결을 이용하고 있어 정상적인 사용자 트래픽과 공격 트래픽을 구분하는 것이 어렵다. 본 논문에서는 HTTP POST DDoS 공격에 대한 대응 방안으로 비정상 HTTP POST 트래픽 탐지 알고리즘과 HTTP POST 페이지별 Content-Length 제한기법을 제안한다. 제안한 방안은 HTTP POST 공격도구인 r-u-dead-yet과 자체 개발한 공격 도구를 이용하여 HTTP POST DDoS 공격을 오탐 없이 탐지 대응하였음을 보여주었다.

ABSTRACT

One of the OSI 7 Layer DDoS Attack, HTTP POST DDoS can deny legitimate service by web server resource depletion. This Attack can be executed with less network traffic and legitimate TCP connections. Therefore, It is difficult to distinguish DDoS traffic from legitimate users. In this paper, I propose an anomaly HTTP POST traffic detection algorithm and http each page Content-Length field size limit with defense method for HTTP POST DDoS attack. Proposed method showed the result of detection and countermeasure without false negative and positive to use the r-u-dead-yet of HTTP POST DDoS attack tool and the self-developed attack tool.

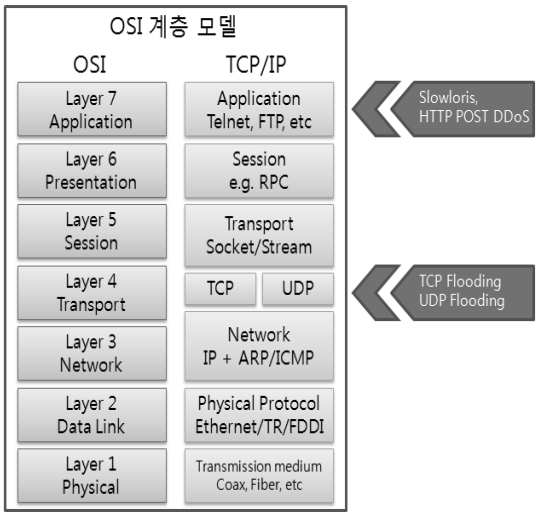
Keywords: HTTP post DDoS, HTTP get flooding, Content-Length, Tree-way Handshaking, Denial of Service attack

I. 서 론

분산서비스거부공격(DDoS : Distributed Denial of Service)은 여러 대의 좀비 PC들을 이용하여 특정 웹서버나 시스템을 공격하여 과부하를 유발시킴으로써 정상적인 서비스를 방해하는 것이다.[1]

DDoS 공격은 대부분 〔그림 1〕의 Transport Layer를 대상으로 하지만 최근에는 Application Layer와 두 계층을 혼합한 공격방법이 급증하고 있다.[3][4][5] Transport Layer공격의 특징은 공격 성공을 위해서 짧은 시간에 대량의 트래픽을 전송시켜 네트워크의 자원을 고갈시키거나 접속처리 한계를 초

접수일(2012년 1월 9일), 수정일(2012년 3월5일), 게재확정일(2012년 3월 23일)
* 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 중점연구소지원사업으로 수행된 연구임 (2012-0005861)
† 주저자, dslee@security.re.kr
‡ 교신저자, dhwon@security.re.kr



〔그림 1〕 OSI 계층과 DDoS 공격 위협

과하도록 한다. 그러므로 기존의 DDoS 방어 알고리즘 및 장비들은 시간당 TCP 및 UDP 트래픽 양이나 Connection 수를 기준으로 하여 대응하도록 설계되어 있다. OSI 7계층 DDoS 공격[7]은 HTTP, SMTP, FTP 등과 같은 Application Layer 프로토콜의 구조적 결함을 이용하여 공격을 시도하므로 기존 방식으로는 대응이 어렵다.

그 중 2010년부터 소개된 HTTP POST DDoS 공격[2]은 매우 적은 수의 좀비 PC만으로도 공격 효과를 크게 나타낼 수 있으며 아직도 많은 웹서버들이 이 공격에 노출되어 있다.

본 논문에서는 이러한 HTTP POST DDoS 공격의 특징을 분석하고 대응 방안에 대하여 기술하였다. 본 논문의 구성을 아래와 같다.

제2장에서는 기존 OSI 7계층의 DDoS 공격 및 대응방법을 설명한다. 제3장에서는 HTTP POST DDoS 공격의 특징을 기술한다. 제4장에서는 HTTP POST DDoS 공격의 대응 방안을 제안한다. 제5장에서는 제안한 대응 방안에 대한 실험결과를 기술한다. 마지막으로 제6장에서는 결론을 기술한다.

II. 기존 OSI 7계층의 DDoS 공격 및 대응방법

2.1 Slowloris 공격

OSI 7계층 DDoS 공격의 대표적인 것은 Slowloris 공격이 있다.[6][8] Slowloris 공격은 2007년도에 그 위험성이 소개되었다. Slowloris는 Apache 웹서버가 GET 요청시 Header를 받기만 해도 웹 서버의 세션 수가 증가하는 서버의 구조적 특징을 이용한 공격이다. 이 공격은 기존의 DDoS 공격과는 다르게 많은 수의 접속 요청을 천천히 보내서 대상 시스템의 자원을 고갈 시킨다. 이 공격은 〔그림 2〕의 정상적인 웹 요청과 같이 \r\n로 종료되지 않아 〔그림 3〕과 같이 웹 요청이 지속된다.

```
GET / HTTP/1.1\r\n
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg \r\n
Accept-Language: ko\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0\r\n
Accept-Encoding: gzip, deflate\r\n
Host: www.google.com\r\n
Connection: Keep-Alive\r\n
Cookie: PREF=ID=11cc36618b343bea:U=0abc82dd9ac68539:FF=4:LR=lang_ko|lang_en:LD=en\r\n
\r\n
```

〔그림 2〕 정상 HTTP GET 요청

```
GET / HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322;
3.0.4506.2152; .NET CLR 3.5.30729; MSOffice 12)
Content-Length: 42
X-a: b
X-a: b
X-a: b
```

〔그림 3〕 Slowloris 공격 요청

결국 이 공격은 웹 서버와의 오랜 시간 세션 연결을 유지시키며, 동시에 처리할 수 있는 연결 센션 수의 한계로 인해 웹서버는 응답 불가 상태에 빠진다. 이 공격 방식은 정상적인 TCP, UDP 연결을 이용하기 때문에 비정상적인 TCP, UDP 연결을 이용한 탐지 방법으로는 탐지 대응이 어렵다.

Slowloris 공격에 대한 대응 방법에는 HTTP Header 전송시간 타임아웃, HTTP 요청 메시지 분산 및 제한, Delayed Binding 이 소개 되고 있다. HTTP Header 전송시간 타임아웃은 Header가 전부 전송되기 까지 서버가 기다리는 특성을 이용하여 공격에 대응하는 방법으로서 MS의 웹 서버에서 적용되고 있다. HTTP 요청 메시지 분산 및 제한은

reverse proxy등을 이용하여 요청을 분산시키는 방법이며 Delayed Binding은 HTTP 요청 메시지가 모두 전송된 이후에만 웹 서버로 직접 연결되도록 하여 공격을 방어하는 방법이다.

2.2 기존 OSI 7계층 DDoS 공격 대응 방법

OSI 7계층 DDoS 공격에 대한 대응 방법 연구는 여러 가지가 진행 되고 있다.[9][10] 대표적인 것은 웹 서비스를 이용하는 사용자의 패턴을 활용하는 방법이다. 이는 사용자들이 유사하거나 동일한 웹 서비스를 반복적으로 이용한다는 특징을 가지고 있으므로 기존 사용자와 새로운 사용자간의 웹 서비스 이용 특성의 비율을 이용하여 DDoS 공격을 탐지하는 방안이다. 또한 사용자의 평소 이용패턴을 분석하여 공격자로 의심되는 Source IP를 분류하는 DDoS 공격 연구[11]가 진행되었다. 홈페이지 URL에 대한 사용자의 사용 특징을 이용하는 방법은 각 페이지의 URL page hit distribution을 통계적 방식으로 학습하고 일시적인 폭주와 DDoS 공격을 구별하는 방법[12]과 Admission Control을 이용하여 허용된 사용자에 한해 웹 서비스 접속을 허용하는 방법 등이 있다.[13]

이들 방법들은 웹서버에서 제공하는 콘텐츠 및 사용자의 사용 패턴 변화에 따라 임계값을 조정해야하므로 임계값 설정에 어려운 단점이 있다. 또한 사용자의 사용 특징을 학습하는데 있어 많은 연산이 필요하다는 문제점 뿐만 아니라 기존 네트워크 트래픽 모니터링 기반의 상용 DDoS 대응 장비에 적용하기가 어렵다. 본 논문에서는 Slowlris 공격방법에 대해서는 대응방안이 다수 연구되어 제외하고 최근에 이슈화된 HTTP POST DDoS 공격에 대하여 상용 장비에서 쉽게 적용이 가능한 대응 기술을 제안하고자 한다.

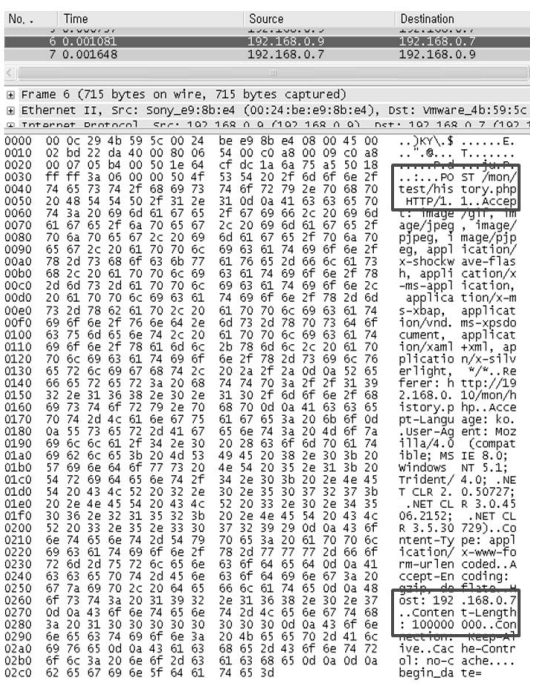
III. HTTP POST DDoS 공격 특징 분석

HTTP POST DDoS 공격은 HTTP POST 프로토콜의 특징을 이용한 공격으로 기존 공격 방법들과 다르게 매우 적은 수의 좀비 PC만으로도 DDoS 공격 효과가 크다는 특징을 가지고 있다. 이 장에서는 HTTP POST DDoS 공격의 특징을 알아본다.

3.1. 정상 HTTP POST 요청

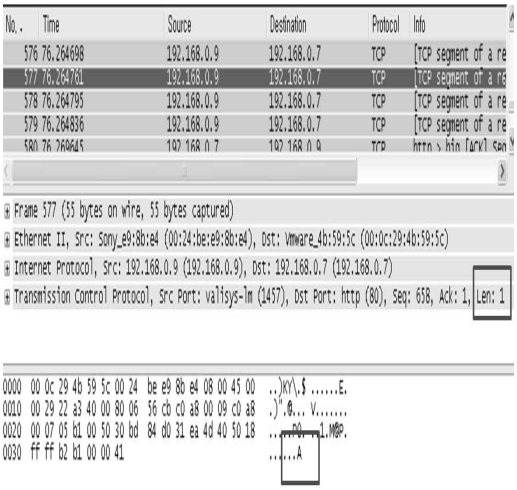
HTTP POST는 사용자가 웹서버에 ID 및 Password, 게시 글, 첨부파일 등을 전송할 때 사용한다. HTTP POST는 [그림 4]와 같이 Header와 Body로 구성되어 있으며 Header에는 데이터를 전송 할 URL 정보, 호스트 정보와 함께 전송할 Data의 크기인 Content-Length값이 정의되어 있다. 웹서버는 Header 정보를 분석하여 Content-Length값 크기(최대 2GB)의 Data가 Body를 통해 모두 수신되기까지 접속을 유지한다.

[그림 4] HTTP POST 요청 Header, Body



[그림 5] HTTP POST Header 전송

3.2. HTTP POST DDoS 공격 방법



〔그림 6〕 1byte씩 전송되는 Data

HTTP POST DDoS 공격자는 홈페이지에서 ID 및 Password, 게시 글 등 HTTP POST 요청이 가능한 공격 페이지를 찾는다. 공격자는 공격 도구를 이용하여 정상적인 홈페이지 접속과 동일하게 POST Header를 웹 서버에 전송한다. 이때 〔그림 5〕와 같이 Content-Length 값을 큰 값으로 설정한다.

그리고 공격 전송데이터(HTTP Body)를 〔그림 6〕과 같이 작은 크기로 긴 시간에 걸쳐서 웹 서버로 전송한다.

3.3. HTTP POST DDoS 공격 특징

HTTP POST DDoS 공격의 첫 번째 특징은 정상적인 HTTP POST 요청을 이용한다는 것이다. 웹 서버는 정상적인 HTTP POST 요청을 처리하기 위해서 Content-Length에 설정된 전송 Data가 모두 수신될 때까지 접속을 유지하는데 HTTP POST DDoS 공격에도 이와 동일한 메커니즘을 이용한다.

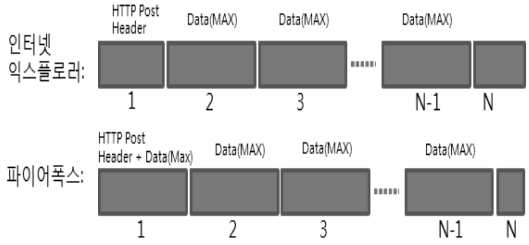
두 번째 특징은 적은 트래픽으로 긴 연결을 장시간 유지한다는 것이다. 대부분의 통신 프로토콜들이 네트워크가 연결된 상태를 오래 지속하지 않는 상태로 동작하기 때문에 짧은 접속 수를 늘리는 방법으로 공격하는 반면 HTTP POST DDoS 공격의 경우에는 웹 서버가 POST 요청에 대해서 Content- Length에 정의되어 있는 전송 Data가 모두 수신될 때까지 기다리므로 쉽게 세션 연결 상태를 오랫동안 유지시킬 수 있다. 웹 서버는 세션을 유지하기 위하여 CPU와 Memory 자원 사용을 계속 증가하게 된다.

IV. HTTP POST DDoS 공격 대응 방안

HTTP POST DDoS 공격은 앞에서 설명한 것과 같이 정상적인 HTTP POST 요청과 유사하고 대량의 트래픽도 발생하지 않아 기존의 대응 방법으로 탐지 대응이 어렵다. 이에 본 장에서는 HTTP POST DDoS 공격 대응 방안으로 HTTP POST DDoS 공격에서 나타나는 비정상 HTTP POST 트래픽에 대한 탐지 알고리즘과 POST 페이지별 Content-Length 제한 기법을 제안한다.

4.1. 비정상 HTTP POST 트래픽 탐지 알고리즘

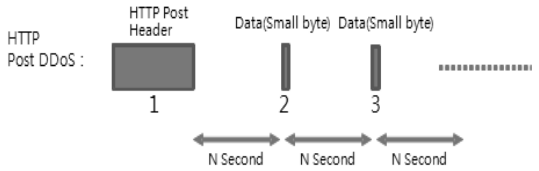
웹 브라우저를 이용하여 PC에서 웹 서버로 HTTP POST를 요청하는 경우 〔그림 7〕과 같이 Best Effort로 동작하는 특징이 있다. 이는 데이터를 최대한 효율적으로 전송하고 브라우저의 성능을 최적화하기 위해서이다. 인터넷 익스플로러의 POST 요청을 보면 HTTP POST Header를 보낸 후 두 번째 패킷부터는 최대치의 Data를 서버로 순차적으로 보낸다. 파이어폭스의 경우에는 처음부터 HTTP POST Header와 Data를 붙여서 최대치의 Data를 서버로 순차적으로 보내는 특징을 가진다. 그러므로 정상적인 HTTP POST 요청을 구성하는 패킷은 패킷 수가 3개 이상일 때 최대 크기는 두 번째 패킷이라는 특징을 가진다.



〔그림 7〕 브라우저 별 HTTP POST 요청 트래픽 형태

하지만 HTTP POST DDoS 공격 트래픽은 〔그림 8〕과 같이 HTTP POST Header를 전송한 이후부터는 작은 Data를 긴 시간에 걸쳐서 전송한다. 이는 공격 성공을 위해서는 오랜 동안 연결을 유지해야 하기 때문이다.

HTTP POST DDoS 공격 트래픽 탐지 알고리즘은 위에서 설명한 브라우저에서 정상적인 Data 전송



〔그림 8〕 HTTP POST 공격 트래픽 형태

메커니즘과 공격 Data 전송 메커니즘의 차이를 이용한다. 첫 번째 조건은 패킷이 순차적으로 N개 까지 전송될 때 세 번째 패킷이 가장 큰 경우 공격으로 판단한다. 이는 두 번째 패킷이 가장 큰 크기의 패킷인 정상 트래픽과 다른 경우이다.

두 번째 조건은 세 번째 패킷과 N-1 번째의 패킷이 최대 크기보다 작은 패킷이 발생한 경우 공격으로 판단한다. 이 경우는 두 번째 패킷을 가장 큰 크기로 보낸 브라우저가 이후에 계속 Best effort로 동작하지 않은 경우이므로 비 정상적 공격 패킷으로 판단하는 것이다. 공격 탐지 알고리즘의 의사코드는 〔표1〕 과 같다.

〔표 1〕 공격 탐지 알고리즘 의사코드

```
expect_exit = FALSE;

packet = receive_packet();
if( packet == error ) return;
first_packet_size = packet.size;
//첫 번째 패킷 크기

packet = receive_packet();
if( packet == error ) return;
second_packet_size = packet.size
// 두 번째 패킷 크기

packet = receive_packet();
if( packet == error ) return;
max = second_packet_size;

if( first_packet_size > max ) "HTTP POST DDoS"
if( packet_size > max ) "HTTP POST DDoS"
// 세 번째 패킷과 두 번째 패킷 크기 비교

while( !exit_condition )
{
    packet = receive_packet();
    if( expect_exit )
    if( packet != error ) "HTTP POST DDoS"

    if( packet.size > max ) "HTTP POST DDoS"
    else if( packet.size < max )
       expect_exit = TRUE;
}
* exit condition은 부하를 감내할 수 있을 정도로 설정
  (패킷 개수, 세션 유지 시간등으로 설정)
```

4.2. HTTP POST 페이지별 Content-Length 제한

앞에서 제안한 HTTP POST DDoS 공격 트래픽 탐지 알고리즘은 네트워크 트래픽 특성을 파악하여 HTTP POST DDoS 공격을 탐지할 수 있다. 하지만 정상 브라우저의 Data 전송 메커니즘과 동일하게 Best effort로 동작하는 공격이 발생한 경우에는 대응이 어렵다. 이에 Best effort로 동작하는 공격이 발생하는 경우에 대응하기 위하여 HTTP POST 페이지별 Content-Length 제한 방법을 제안한다.

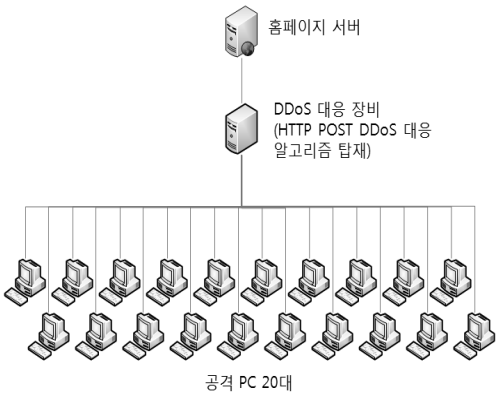
HTTP POST요청은 최대 2GB까지 설정이 가능하지만 홈페이지는 HTTP POST 페이지에 따라 필요로 하는 Content-Length 크기가 정해져 있다. 예를 들어, ID 및 Password 입력 페이지의 경우 20~30byte와 같은 작은 크기의 Content-Length가 요구된다. 파일 업로드 기능이 있는 게시판의 경우에는 첨부파일 크기 정도의 Content-Length가 요구된다. IIS와 Apache의 경우, Directory마다 다른 Content-Length 제한이 가능하다. 그러므로 필요로 하는 Content-Length를 설정을 통해서 Best effort의 탐지 알고리즘을 우회하는 공격을 근본적으로 차단할 수 있다.

V. 실험 결과

본 장에서는 제안한 비정상 HTTP POST 트래픽 탐지 알고리즘과 POST 페이지별 Content- Length 제한하는 방안이 HTTP POST DDoS 공격에 오탐 없이 대응한 실험 결과를 기술한다.

5.1. 실험 환경 구축

HTTP POST DDoS 공격 대응 방안을 실험하기 위하여 IPS 기반의 DDoS 대응장비에 비정상 HTTP POST 트래픽 탐지 알고리즘 적용하였다. 실험을 위하여 HTTP POST 요청을 처리할 수 있는 Apache 기반의 홈페이지를 구축하였으며 좀비 PC는 20대를 준비하여 진행하였다. 실험 구성도는 〔그림 9〕와 같다.

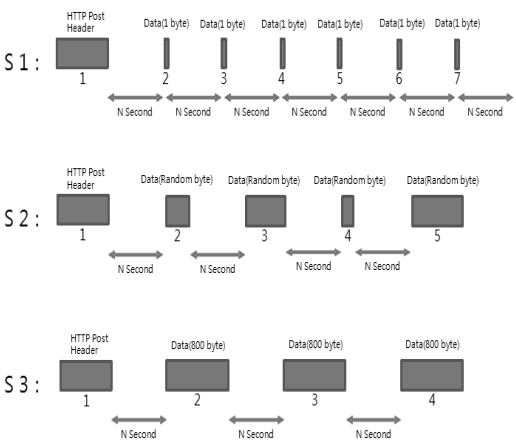


〔그림 9〕 실험환경 구성도

5.2. 실험 시나리오

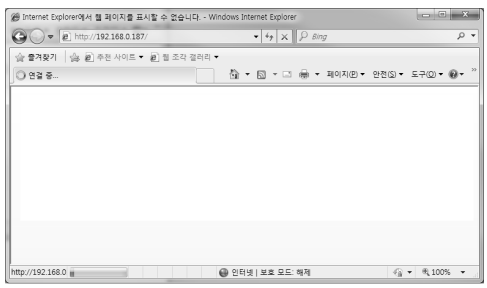
실험은 기존에 알려져 있는 RUDY[9]도구와 패킷 사이즈를 변화시키면서 공격할 수 있도록 실험도구를 개발하여 이용하였다.

시나리오는 〔그림 10〕과 같이 세 가지로 진행하였다. 각각의 시나리오들은 가능한 HTTP POST DDoS 공격 트래픽을 모두 처리하도록 구성하였다. 첫 번째 시나리오는 RUDY도구를 사용하여 HTTP POST DDoS 공격을 수행하는 것으로서 1번 패킷에 HTTP Header를 보내고 2번 패킷부터는 1byte의 패킷을 지속적으로 보내는 것이다. 두 번째 시나리오는 자체 개발한 실험도구를 이용하여 1번 패킷은 HTTP Header를 보내고 2번 패킷부터 랜덤 byte의 패킷을 지속적으로 보내도록 하였다. 랜덤 byte의 크기는 600 byte, 700 byte, 800 byte 중에서 선택되도록 하였다. 마지막 세 번째 시나리오는 1번 패킷에 HTTP Header를 보내고 2번 패킷부터는 800byte의 패킷을 지속적으로 서버로 보내는 방법으로서 브라우저의 Best effort 상황을 가정한 경우이다.



〔그림 10〕 실험 시나리오별 전송 데이터 형태

세 가지 실험 시나리오를 통해서 본 논문에서 제안한 비정상 HTTP POST 트래픽 탐지 알고리즘과 HTTP POST 페이지별 Content-Length 제한 기법이 공격을 오탐 없이 탐지하는지를 확인하였다. 실험에 사용된 공격 PC들은 동시에 1000개의 연결을 시도하였으며 제안한 대응기법을 적용시키지 않은 상태에서 공격하는 경우에는 〔그림 11〕과 같이 홈페이지 접속이 이루어 지지 않았다.



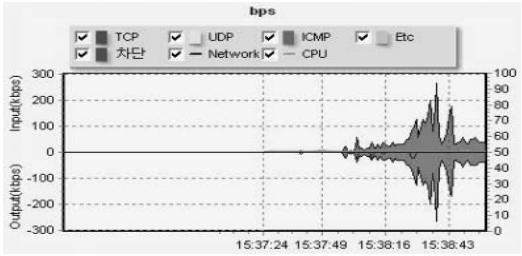
〔그림 11〕 웹 서버 접속 불가 화면

5.3. 비정상 HTTP POST 트래픽 탐지 알고리즘 실험결과

첫 번째 실험결과는 〔그림 12〕와 같이 공격 트래픽은 3번 패킷 이후에는 탐지 및 차단되어 유입되지 않았다. 탐지 알고리즘은 3번 패킷이 유입되었을 때 1번 패킷이 가장 크고 작은 패킷이 연속하여 유입되었으므로 HTTP POST DDoS 공격으로 판단하였다. 〔그림 13〕은 첫 번째 실험에서의 시간별 전체 트래픽 추이다. 트래픽 추이 그래프의 녹색은 유입된 트래픽을 나타내고 붉은 색은 차단된 트래픽을 나타낸다. 시나

카테고리	공격코드	공격명	공격자	대상자	시도횟수	상태
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.10	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.11	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.12	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.13	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.14	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.15	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.16	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.17	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.18	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.19	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.20	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.21	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.22	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.23	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.24	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.25	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.26	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.27	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.28	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.29	192.168.1.187:http	3	차단

〔그림 12〕 시나리오 1 탐지/차단 내역



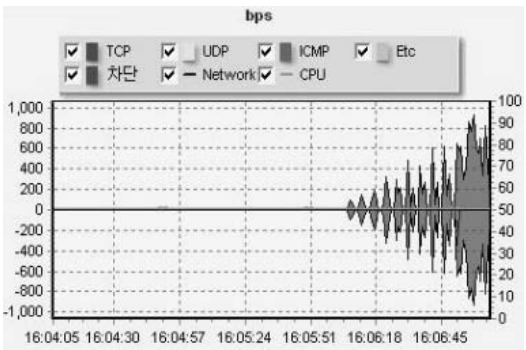
〔그림 13〕 시나리오 1 트래픽 추이

카테고리	공격코드	공격명	공격자	대상자	시도횟수	상태
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.10	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.11	192.168.1.187:http	5	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.12	192.168.1.187:http	6	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.13	192.168.1.187:http	10	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.14	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.15	192.168.1.187:http	8	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.16	192.168.1.187:http	6	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.17	192.168.1.187:http	6	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.18	192.168.1.187:http	9	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.19	192.168.1.187:http	5	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.20	192.168.1.187:http	6	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.21	192.168.1.187:http	7	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.22	192.168.1.187:http	5	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.23	192.168.1.187:http	3	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.24	192.168.1.187:http	7	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.25	192.168.1.187:http	8	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.26	192.168.1.187:http	10	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.27	192.168.1.187:http	6	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.28	192.168.1.187:http	4	차단
서비스 거부	678	HTTP POST DDoS ATTACK	192.168.1.29	192.168.1.187:http	3	차단

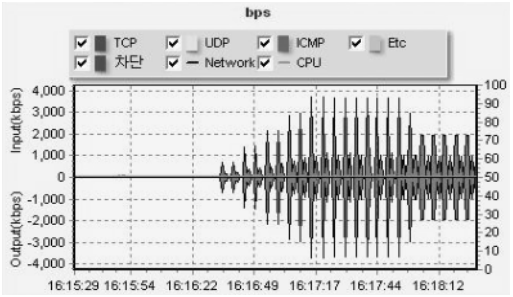
〔그림 14〕 시나리오 2 탐지/차단 내역

리오 1의 경우에 공격 시작 후 바로 탐지되어 차단되었으며 녹색으로만 표시된 유입 공격 트래픽이 소량인 것을 확인할 수 있다.

두 번째 실험결과는 〔그림 14〕와 같이 공격 트래픽은 3번 패킷부터 최대 10번 패킷사이에 탐지 및 차단되어 유입되지 않았다. 두 번째 시나리오는 랜덤 사이즈로 패킷이 유입되었으므로 2번 패킷부터 같은 크기의 패킷이 계속 나오는 동안에는 트래픽이 유입되었으나 다른 크기의 패킷이 유입되는 경우 HTTP POST DDoS 공격으로 판단하였다. 〔그림 15〕은 두 번째 실험에서의 시간별 전체 트래픽 추이다. 시나리오 2의 경우에는 공격 시작 후 어느 정도 시간이 경과 시부터



〔그림 15〕 시나리오 2 트래픽 추이



〔그림 16〕 시나리오 3 트래픽 추이

공격이 탐지되어 붉은 색 차단 트래픽이 표시되는 것을 확인 할 수 있다.

세 번째 실험결과는 〔그림 16〕의 트래픽 추이 그래프와 같이 탐지 및 차단되지 않고 지속적으로 공격 트래픽이 유입되었다. 시나리오 3의 경우는 붉은색 차단 트래픽이 없으며 모든 트래픽이 유입되었음을 확인 할 수 있다. 이 경우에는 정상적인 HTTP POST 요청과 같은 형태의 Best effort 트래픽이므로 탐지 알고리즘은 동작하지 않았다.

5.4. 페이지별 Content-Length 제한 기법 실험결과

실험에서 이용한 Apache 서버는 〔그림 17〕과 같이 Directory 별로 서로 다른 Content-Length 제한 값을 LimitRequestBody 값으로 설정할 수 있다. 〔그림 17〕에서는 (/)는 모든 파일의 사이즈를 500byte로 제한하고 (/home/user/dir) Directory에 대해서는 100byte로 제한하였다. IIS 서버의 경우, Web.config 파일상에 maxAllowed Content Length값 설정을 통해 Content-Length값 제한이 가능하다.

```
〈Directory /〉
   LimitRequestBody 500
〈/Directory〉
〈Directory /home/userdir/〉
   LimitRequestBody 100
〈/Directory〉
```

〔그림 17〕 Apache 웹서버 Content-Length 제한 설정

실험은 HTTP POST 요청이 100byte로 제한된 Directory에 간단한 HTTP POST 요청 페이지를 두고 수행하였다. Content-Length는 최대 2GB까지 지원 가능하나 대부분의 HTTP POST 요청 페이

〔표 2〕 Content-Length 제한에 따른 시나리오별 유입 공격 패킷 차단 여부

시나리오 번호	공격 PC IP (192.168.1.xx) 별 차단 여부 (유입 패킷 개수)																			
	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)
2	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)
3	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)	차단 (1)

지는 ID 및 Password 입력 페이지와 같이 20~30byte와 같은 작은 크기의 Content-Length가 요구되고 있다. 대용량 파일 업로드와 같은 일부 긴 HTTP POST 요청이 요구되는 서비스의 경우 Login 등 인증 후에 접속 가능하므로 인터넷에 노출되어 공격대상이 될 수 있는 대부분의 POST 요청 페이지들은 100byte 이하의 작은 값이 된다.

실험 결과는 〔표 2〕와 같이 첫 번째 패킷 유입 이후 바로 차단되었다. 이는 첫 번째 패킷에 HTTP POST Header 상에 표시된 Content-Length값이 모두 100byte 이상이기 때문이다.

페이지별 Content-Length 제한 기술이 적용된 홈페이지는 인터넷에 노출되어 공격대상이 될 수 있는 대부분의 POST 요청 페이지들을 100byte 이하의 작은 값으로 설정한다. 공격자가 이러한 홈페이지를 공격하기 위해서는 제한된 값 이하로 Content-Length를 설정하여 공격해야 하며 공격의 성공을 위해 긴 시간동안 연결을 유지해야 하므로 시나리오 1과 같이 Header를 전송한 이후부터는 작은 양(1byte)의 데이터를 보내야 한다. 이 경우에는 실험을 통해서 증명한 것처럼 비정상 HTTP POST 트래픽 탐지 알고리즘에 의해 공격이 탐지 차단되는 것을 알 수 있다.

VI. 결 론

본 논문에서는 HTTP POST DDoS 공격에 대한 대응 방안으로 비정상 HTTP POST 트래픽 탐지 알고리즘과 POST 페이지별 Content-Length 제한 기법을 제안하였다. 제안한 알고리즘은 웹 브라우저와 동일하게 Best Effort로 발생하는 공격 외에 모든 HTTP POST DDoS 공격을 탐지하는 것을 실험을 통해 증명하였다. 또한 본 논문에서는 Best Effort로 공격하는 방법을 대응하기 위해 웹 페이지별 Content-Length 제한하는 기법을 제안하였다. Content-Length 제한 기법 실험 결과, 요청 페이지에 설정된 Content-Length보다 큰 값으로 설정된 트래픽은 첫 번째 패킷 이후 바로 차단되는 것을 확인 하였다. 또한 제안한 방법은 상용 DDoS 대응장비 및 웹서버 적용에 매우 용이하여 HTTP POST DDoS 공격 대응에 효과가 클 것으로 기대한다.

참고문헌

〔1〕 Felix Lau, Stuart H. Rubin, Michael H. Smith, and Ljiljana Trajkovic, "Distributed Denial of Service Attacks," 2000 IEEE International Conference on Systems, Man and Cybernetics, Volume:, pp. 2275-2280, March 2000.

〔2〕 W. O Chee and T. Brennan "H...t....t...p...p...o...s...t," presentation at OWASP AppSec Conference, Washington, D.C., 2010. Copyright ⓒ The OWASP Foundation http://www.owasp.org

〔3〕 J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attacks and Defense Mechanisms," ACM CCR, April 2004.

〔4〕 A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks and counter strategies," IEEE/ACM Trans. Netw., vol. 14, no. 4, pp. 683-696, 2006

〔5〕 T.Peng, C.Leckie, and K.Ramanohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problem," ACM Computing Surveys, vol. 39, no.1, pp. 1-42, 2007.

〔6〕 ModSecurity Advanced Topic of the

Week: Mitigating Slow HTTP DoS Attacks. SpiderLabs Anterior - The Official Blog of Trustwave's SpiderLabs http://blog.spiderlabs.com/2010/11/advanced-topic-of-theweek-mitigating-slow-http-dos-attacks.html
〔7〕 Y. Xie and S.-Z. Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," IEEE/ACM Transaction on Networking, vol. 17, No. 1, Feb. 2009.
〔8〕 C. Zhang, J. Yin, Z. Cai, and W. Chen, "RRED: Robust RED Algorithm to Counter Low-rate Denial-of-Service Attacks," IEEE Communications Letters, Vol. 14, pp. 489-491, 2010.
〔9〕 Alefiya Hussian, John Heidemann, and Christos Papadoopoulos, "A Framework for Classifying Denial of Service Attacks," SIGCOMM pp. 99-110, 2003.
〔10〕 Song Huang, Ling Zhang, and Shou-Ling Dong, "A Behavior-based Ingress Rate-Limiting Mechanisms against DoS/DDoS Attacks," LNCS, vol. 3783, pp. 231-242, 2005.
〔11〕 http://sniper.wins21.co.kr
〔12〕 http://www.radware.com/Thank_you_down load.aspx?ID=6949
〔13〕 M.Srivatsa el al., "Mitigating Application Level Denial of Service Attacks on Web Servers," ACM Transactions on WEB. Vol. 2 Issue. 3, July 2008
〔14〕〔14〕 r-u-dead-yet HTTP POST Denial of Service Tool, http://code.google.com/p/r-u-dead-yet

〈著者紹介〉

사 진

이 대 섭 (Daeseob Lee) 학생회원
2007년 3월~현재: 성균관대학교 컴퓨터공학 박사과정 수료
〈관심분야〉 보안평가인증, DDoS 대응, 보안관제, 정보보호

원 동 호 (Dongho Won) 평생회원
1976년~1988년: 성균관대학교 전자공학과(공학사, 공학석사, 공학박사)
1978년~1980년: 한국전자통신연구원 전임연구원.
1985년~1986년: 일본 동경공업대 객원연구원
1998년~2003년: 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장장.
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, BK21 사업단장, 한국정보보호학회 명예회장.
〈관심분야〉 암호이론, 정보이론, 정보보호