SNMPGET을 이용한 DDoS 공격 탐지

DDoS Attack Detection using SNMPGET

박한상, 유대성, 오창석*
충북대학교*

Park han-sang, Yoo dae-sung, Oh chang-suk*
Chungbuk National University*

요약

최근의 트래픽 폭주 공격은 웜의 확산성과 공격 방법의 발달로 인하여 공격 전개시간이 단축되었다. 하지만 기존의 트래픽 분석 방법에서는 최근의 트래픽 폭주 공격의 빠른 진행을 탐지하기에는 시간의 제약점이 있다. 본 논문에서는 이러한 취약점을 보완하기 위해 트래픽을 수집하고 분석하는데 있어 시간을 향상시킨 트래픽 수집 및 분석 알고리즘을 제안하고 구현하였다.

Abstract

Recently traffic flooding attack has happened faster and faster owing to expansion of the worm attack and development of the method of traffic flooding attack. The method in the past time is problematic in detecting the recent traffic flooding attacks, which are running quickly. Therefore, this paper aims to establish the algorithm which reduces the time of detection to traffic flooding attack in collecting and analyzing traffics.

I. 서 론

최근 인터넷상에서의 최대 이슈는 트래픽 폭주 공격에 의한 피해이다. 많은 종류의 공격에 의해 많은 서버들이 피해를 보고 있으며 인터넷의 보급으로 인해 이러한 공격은 빠른 전파 및 발전을 가져왔다. 또한 최근의 트래픽 폭주 공격의 특징은 웜의 빠른 확산성을 통해서 이루어지고 있으며, 이는 기존의 트래픽 폭주 공격에의 탐지시간과 비교할 때 큰 취약점으로 여겨지고 있다. 본 논문에서는 최근의 트래픽 폭주 공격의 빠른 진행 속도에 민감하게 대처하기 위해서 탐지 시간을 향상시킨 SNMP를 이용한 트래픽 분석 알고리즘을 개발하고 구현하고자 한다. 이는 기존의 트래픽 분석에 소요되는 시간이 10분 이상의 시간으로는 현재의 트래픽 폭주 공격에 대응할 수 없으며 탐지에서 아무리 정확하더라도 시간안에 탐지할 수 없으면 대응할 수도 없기 때문이다. 본 논문에서의 트래픽 분석 알고리즘을 통해서 기존 방법보다 빠른 탐지를 할 수 있으며 또한 트래픽 분석측면에서도 정확한 분석을 할 수 있을 것이다.

II. SNMP와 MRTG를 이용한 트래픽 수집 및 분석

SNMP와 MRTG를 이용한 트래픽 수집 및 분석방법은 MIB 객체중에서 공격에 반응하는 객체를 선정하고 이를 MRTG를 이용하여 트래픽을 수집하게 된다. MRTG는 관리하고자 하는 대상에 대하여 정형화된 로그값과 그래프를 출력해주며 5분 단위로 수집을 하게된다. 수집된 데이터의 트래픽의 변화를 측정하여 공격 트래픽에 대한 특징을 도출하게 되고 이를

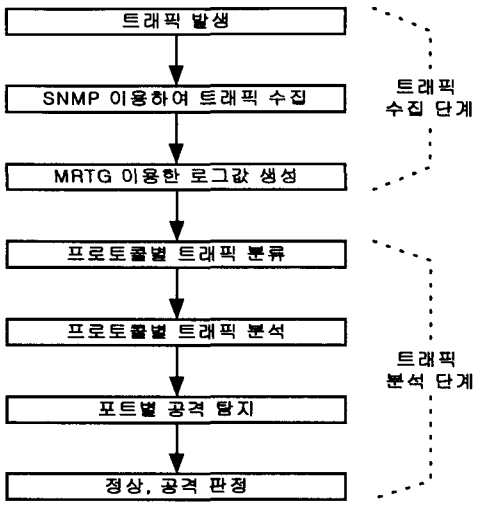
바탕으로 하여 정상 트래픽과 공격트래픽을 구분하게 된다. 공격 트래픽의 특징은 다음과 같다.

- 공격 트래픽은 특정 MIB에 반응한다
- 공격 트래픽은 변화량이 일정한 범위를 가지고 있다.

위의 두가지 특징을 이용하여 공격트래픽을 분석하게 되며 공격에 대하여 반응하는 MIB객체는 다음과 같다.

- TCP : tcpInErrs
- UDP : udpNoPorts
- ICMP : icmpInEchos, icmpOutEchoReps

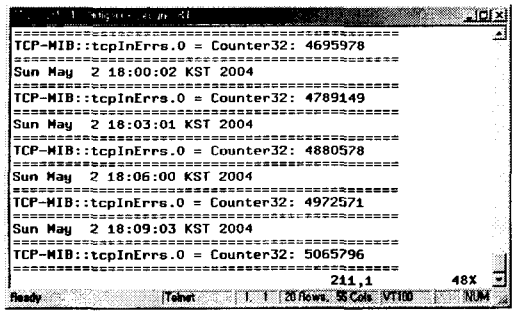
TCP Flooding 공격 경우 쓰리핸드쉐이크(Three Hand Shake) 방식의 연결설정에서의 취약점을 이용한 것으로 공격으로 발생된 패킷은 근원지 IP주소가 허위로 설정되어 있어 완전한 연결 설정을 하지 못하기 때문에 tcpInErrs에서 과다한 트래픽이 발생하게 된다. UDP Flooding 공격의 경우에는 해당하는 응용 서비스가 존재하지 않기 때문에 udpNoPorts의 트래픽이 과다하게 발생하게 되며, ICMP Flooding 공격의 경우에는 에코 요청과 이에 대한 응답에 의해 두 MIB 객체에 과다한 트래픽이 발생하게 된다. 또한 공격 시점시 일정한 수의 슬레이브를 통해서 공격이 행해지므로 공격에 대해 반응하는 MIB 객체의 트래픽은 일정한 변화량 안에서 발생하게 된다. 이 변화량을 바탕으로 임계값을 선정하여 정상 트래픽과 공격 트래픽을 구분하게 된다. 그림 2-1은 트래픽을 수집 및 분석하는 단계를 나타낸다.



▶▶ 그림 2-1. SNMP를 이용한 트래픽 분석 흐름도

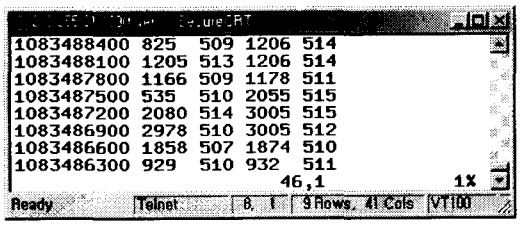
Ⅲ. 탐지시간을 향상시킨 트래픽 분석 알고리즘

트래픽 분석에서의 시간을 단축시키기 위해서 snmpget을 이용하여 트래픽을 수집하게 된다. snmpget은 SNMP 프로토콜에서 제공되는 내부 명령어로 요청된 시간에 대상 MIB 객체에 대한 정보를 출력해준다. 기존의 방법에서는 MRTG를 이용하여 MIB 객체 정보를 취득함으로써 트래픽을 수집하는데 5분이라는 최소 시간을 적용하였지만 snmpget을 이용할 경우 시간을 향상시킬 수 있다. crond 데몬을 통해서 주기적인 시간에 MIB 객체에 대한 정보를 취득하게 하였으며 본 논문에서는 3분단위로 SNMP 통신을 하도록 하였다. 그림 3-1은 snmpget을 주기적으로 실행시켜 얻어진 로그값을 나타낸다.



▶▶ 그림 3-1. snmpget을 통해 얻어진 로그값

snmpget을 통해서 얻어진 MIB객체에 대한 정보는 현 시점까지의 대상 객체에 대한 트래픽의 누적치를 나타낸다. 그림3-1에서 보듯이 현재 tcpInErrs에 대한 트래픽의 누적치를 3분단위로 나타낸 것을 볼 수 있다. 또한 snmpget에서 얻어진 데이터는 eth0과 lo에서 발생된 트래픽에 대해서 모두 수집하여준다. 이는 기존의 방법에서 MRTG를 이용해 MIB 객체에 대한 정보를 얻을 때는 eth0에서 MIB 객체의 정보를 수집하여 준다는 점과 다른점이다. 그림 3-2는 기존의 방법에서의 트래픽을 수집한 것이다.



▶▶그림 3-2. MRTG를 통해 얻어진 로그값

또 다른 특징으로는 snmpget을 통해서 얻어진 데이터는 Counter32 형식의 패킷에 대한 개수로 표시되며 기존의 MRTG를 이용한 트래픽 수집 방법에서는 Bytes 형식의 트래픽에 대한 양으로 표시된다. snmpget을 통해서 얻어진 데이터와 기존의 MRTG를 이용하였을 때의 차이점은 다음과 같이 같다.

- 출력되는 데이터의 값이 누적된 값이다.
- eth0와 lo 모두의 데이터를 획득한다.
- Counter32형식의 패킷 개수를 출력한다.

snmpget을 통해서 트래픽을 분석할 경우에는 얻어진 데이터에 대해서 기존의 분석 알고리즘을 적용하기 위해 다음과 같은 몇가지 변형과정을 거쳐야 한다. 공격 트래픽을 판별해내는 방법이 대상 MIB객체의 트래픽의 변화가 일정한 수준에서 일정하게 발생된다는 특징을 이용하기 때문이다. 변형과정에서 적용되는 알고리즘은 위의 3가지 특징을 바탕으로 하여 이루어졌다.

$Log_v = (P_{prev} - P_{curr}) / \alpha$

- Log_v : 정형화된 로그값
- P_{prev} : 이전에 입력된 트래픽 패킷의 수
- P_{curr} : 현재 입력된 트래픽 패킷의 수
- α : 보정치

▶▶ 그림 3-3. 로그값 변형 알고리즘

그림 3-3에서 얻어진 로그값을 통해서 각각의 프로토콜별 트래픽 분석을 하게 되며 본 논문에서 사용된 MIB 객체와 트래픽 분석에 사용된 알고리즘은 표 3-1과 같다.

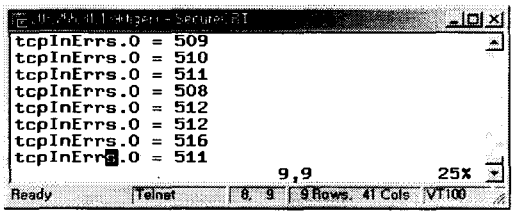
[표 3-1] 트래픽 분석에서의 MIB 객체와 분석 방법

프로토콜 / MIB	공격 탐지조건	비고
TCP /tcpInErrs	tcpInErrs > 0 F(x)-P(x) < ε	F(x) 현재 트래픽 P(x) 이전 트래픽 ε 임계값
UDP /udpNoPorts	udpNoPorts > 0 F(x)-P(x) < ε	
ICMP /icmpInEchos, icmpOutEchoReps	icmpInEchos, icmpOutEchoReps >0 F(x)-P(x) < ε	

트래픽 수집단계에서는 snmpget을 통하여 시간의 단축을 가져오며 트래픽 분석단계에서는 얻어진 데이터를 가공한 후 트래픽 분석 알고리즘에 적용하여 공격트래픽에 대하여 탐지하게 된다.

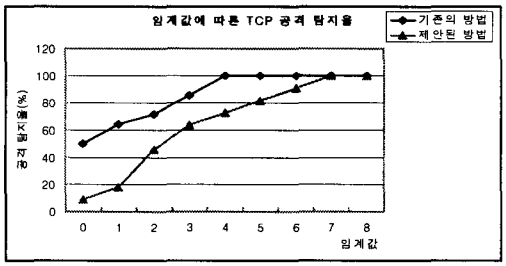
Ⅳ. 실험 및 결과

본 논문에서는 TFN을 사용하여 공격 트래픽을 발생 시켰으며 정상 트래픽을 출력하기 위해 FTP서버와 웹서버를 구동하였다. 기존의 MRTG를 이용한 트래픽 수집 방법과의 비교를 위하여 같은 시점에서 snmpget을 통하여 트래픽을 수집하고 분석하였으며 MRTG를 이용하여 트래픽을 수집하고 분석하였다. 다음은 각 MIB 객체중에서 snmpget을 통하여 트래픽을 수집한 후 로그값 변형 알고리즘에 대입하여 최종적으로 얻어진 tcpInErrs의 로그값을 나타낸다.

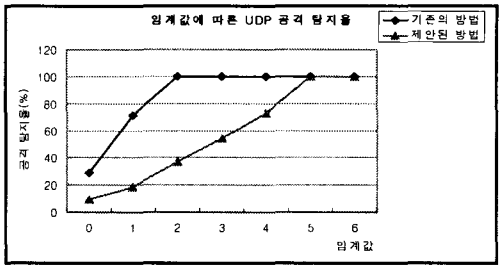


▶▶ 그림 4-1. 정형화된 tcpInErrs의 로그값

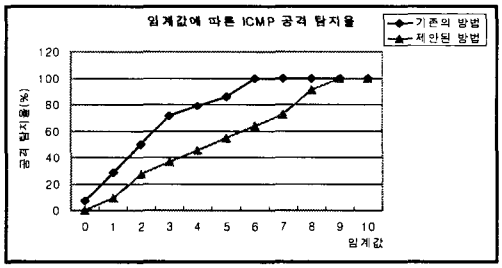
생성된 로그값을 이용하여 공격 트래픽을 분석하기 위해서는 임계값을 선정하게 되며 본 논문에서 제안된 snmpget을 이용하였을 경우와 기존의 방법에서의 임계값에 따른 공격 탐지율은 다음과 같다.



▶▶ 그림 4-2. 임계값에 따른 TCP 공격 탐지율 비교



▶▶ 그림 4-3. 임계값에 따른 UDP 공격 탐지율 비교



▶▶ 그림 4-4. 임계값에 따른 ICMP 공격 탐지율 비교

임계값은 기존의 방법에서 사용되었던 임계값보다 더 큰 값에서 공격을 100%탐지 할 수 있었다. 그 이유는 MRTG로 수집된 데이터는 5분동안의 평균값이지만 snmpget을 이용하였을 경우에는 snmpget으로 요청된 시간에서만 데이터를 수집하기 때문에 데이터 값의 변동이 MRTG보다 더 크기 때문이다. 본 논문에서 제안된 트래픽의 수집과 분석에서의 시간 소요는 다음과 같다.

[표 4-1] 수집 및 분석시간 비교

시간 / 방법	수집 시간	분석 시간
제안된 방법	3	6
기존의 방법	5	10

Ⅴ. 결 론

본 논문에서는 기존의 SNMP를 이용한 트래픽 수집 및 분석에서 10분대의 시간이 소요되는 문제점을

해결하기 위해 snmpget을 이용한 트래픽 수집 및 분석 방법을 제안하였다. 제안된 알고리즘을 통해서 트래픽 수집에서는 3분의 시간이 소요되었으며 트래픽 분석에서는 6분으로 시간을 단축시킬 수 있었다. 공격 트래픽을 분석하기 위해서 기존의 방법보다 더 큰 임계치를 필요로 하였지만 수정된 임계치를 적용하여 트래픽을 정확하게 분석해 낼 수 있었다. 차후에 snmpget으로 수집된 MIB 객체의 정보를 변환하는 과정에서의 변환 방법에 대한 연구와 시스템의 자원을 효율적으로 사용할 수 있는 시간대를 선정한다면 트래픽 분석에 있어서 효율적으로 분석해 낼 수 있을 것으로 기대된다.

▌참고문헌▐

[1] 김선영, 박원주, 유대성, 서동일, 오창석, "SNMP를 이용한 트래픽 폭주 공격 검출", 한국콘텐츠학회논문지, 제3권 제4호, pp.48-54

[2] J.Case, M.Fedor, M.Schoffstall, J. Davin, "A Simple Network Management Protocol", RFC1157, 1990

[3] 최재원, "웹 기반 네트워크 트래픽 분석 시스템", 한국정보처리학회 학술발표논문집, 제7권, 제2호, 2000