SNMP를 이용한 유해 트래픽 분석

Noxious Traffic Analysis using SNMP

유대성, 구향옥, 오창석
충북대학교

Yoo Dae-sung, Koo Hyang-Ohk, Oh Chang-suk
Chungbuk National University

요약

네트워크망의 급속한 발전 속에서 해커에 의한 많은 피해 사례가 증가되고 있다. 최근에는 트래픽 폭주 공격에 의해 많은 네트워크와 시스템 자원들이 피해를 보고 있다. 이에 따라 네트워크상에서 유통되는 트래픽 분석을 통한 자원의 보호가 중요한 이슈로 대두되고 있다. 이에 본 논문에서는 기존의 SNMP를 이용한 트래픽 분석 방법에 있어서 시간과 탐지력을 향상시킨 알고리즘을 제안하고 구현하였다.

Abstract

A rapid development of the network brought increasing of many damage cases by hacker's attack. In recently many network and system resources are damaged by traffic flooding attacks. For this reason, the protection of network resources by analyzing traffic on the network is on the rise. In this paper, algorithm that improves the executing time and detection rate than traffic analysis method using SNMP is proposed and implemented.

Ⅰ. 서 론

네트워크의 발달을 통해 사용자들은 인터넷을 통해 많은 정보를 획득하게 되었다. 대용량의 정보를 빠르게 획득할 수 있으며 자신의 정보를 인터넷을 통해 게시할 수 있게 되었다. 이러한 긍정적인 측면과 함께 최근에는 트래픽 폭주 공격에 위해 많은 피해를 보고 있다. 트래픽 폭주 공격은 시스템과 네트워크의 자원을 고갈시켜 정상적인 서비스를 하지 못하게 하는 공격으로 그 대상이 불특정하고 자동화, 은닉화 및 지능화 되면서 탐지 및 대응이 어려운 실정이다. 이러한 유해 트래픽을 네트워크 상에서 조기에 발견하여 시스템과 네트워크의 자원을 보호하기 위한 방법이 연구되어 지고 있으며, 최근 SNMP를 이용한 방법이 새로운 해결책으로 연구되어지고 있다. 하지만 기존의 방법은 탐지 시간이 오래 걸린다는 단점과 공격 트래픽이 발생되는 과도기적 시점에서 임계치의 적용이라는 문제로 인해 분류하지 못하는 큰 취약점을 가지고 있다. 이에 본 논문에서는 이러한 문제를 해결하기 위하여 일주 트래픽 추이 분석, 프로토콜별 추이 분석 그리고 특정 MIB 객체의 트래픽 발생 유무의 3단계의 트래픽 분석을 적용하였다. 이를 통해서 기존 방법의 문제점을 해결할 수 있으며 시간상의 큰 단축을 통해 빠르고 신뢰성 있는 트래픽 분석을 할 수 있었다.

Ⅱ. 기존의 트래픽 분석

기존의 트래픽 분석 방법은 선정된 MIB 객체를 통해 관리하고자 하는 대상의 트래픽을 수집하고 수집된 트래픽 값에 대해서 임계치를 적용하여 공격 트래

픽을 분류하게 된다. 사용된 MIB 객체는 실험을 통해서 공격에 반응하는 몇 개의 MIB객체를 선택하게 된다. 사용된 MIB 객체는 표1과 같다.

[표 1] 기존의 방법에서 사용된 MIB 객체

구분	MIB
TCP	tcpInSegs, tcpOutSegs, tcpInErrs
IP	ipInReceives, ipInDelivers, ipOutRequests, ipReasmReqds, ipFragCreates
ICMP	icmpInMsgs, icmpOutMsgs, icmpOutDestUnreachs, icmpInEchos, icmpOutEchoReps
UDP	udpNoPorts, udpInErrors

위에 선정된 MIB 객체를 통해 수집된 트래픽은 공격 트래픽이 발생될 경우 tcpInErrs, udpNoPorts, icmpInEchos에서 공격 트래픽을 확인할 수 있다. 이는 트래픽 폭주 공격의 특징으로 인한 것으로 공격으로 인한 트래픽이 해당 프로토콜의 에러로 발생되기 때문이다. 또한 ICMP Flooding 공격의 경우는 대량의 ICMP echo 패킷을 보내기 때문에 위의 MIB 객체를 통해 공격 트래픽을 확인할 수 있다. 또한 발생되는 트래픽은 일정한 대역폭 안에서 발생된다. 이는 공격자가 이미 지정한 슬레이브를 통해서 공격을 행하기 때문에 일정한 크기로 발생되는 것이다. 이 2가지 특징을 이용하여 공격 트래픽을 분류해 낼 수 있다. 그림 1은 UDP Flooding 공격이 발생되었을 때 udpNoPorts에서 발생되는 트래픽을 보여준다.

▶▶ 그림 1. udpNoPorts에서의 공격 트래픽 발생

III. SNMP 기반의 트래픽 추이 분석

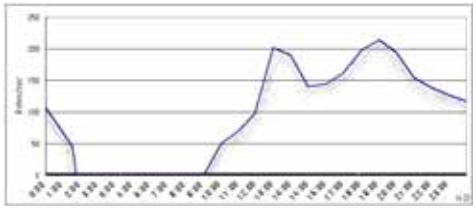
1. 기본 개념

본 논문에서 제안한 3단계 트래픽 분석 알고리즘은 기존의 SNMP MIB 객체를 이용한 트래픽 분석 시 공격 트래픽을 정확하게 찾아내는 장점을 활용하고 과도기적 시점에서의 유해 트래픽을 분석해내지 못하는 단점을 보완한 방법이다. 이를 위해 임계치에 의존적이던 기존의 방법에서 일주 트래픽 추이 분석, 프로토콜별 추이 분석 그리고 MIB 객체에 의한 분석을 통해 정확하게 유해 트래픽을 분석할 수 있다. 본 논문에서 사용된 MIB 객체는 다음과 같다.

[표 2] 제안된 알고리즘에서 사용된 MIB 객체

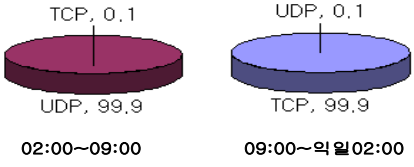
분석 방법	MIB
일주 트래픽 추이 분석	ipInReceives
프로토콜별 추이 분석	tcpInSegs
	udpInDatagrams
	icmpInEchos
특정 MIB에 의한 분석	tcpInErrs
	udpNoPorts
	icmpOutEchoReps

위의 표에서 선정된 MIB 객체를 통해 트래픽을 수집하게 되며, 추이 분석을 위해 미리 기준이 되는 트래픽 변동량을 선정하게 된다. 이는 실험을 통해 기준이 되는 트래픽 추이양을 구하게 된다. 그림 2는 실험을 통해 구해진 일주 트래픽 추이 기준량이다. 시간을 기준으로 해서 발생되는 트래픽 양을 구하게 되고 모든 트래픽을 수용할 수 있는 최대값을 연결하여 기준이 되는 트래픽 제한선을 구하게 된다. 이는 시간대별로 발생되는 트래픽의 발생 추이가 일정하게 반복된다는 사실에 근거하였다.



▶▶ 그림 2. 일주 트래픽 추이

다음으로 프로토콜별 추이 분석을 위해 사용되어질 기준 데이터는 그림 3과 같다. 시간대별로 TCP와 UDP의 비율이 틀려지며, 새벽 시간대에 UDP 트래픽이 대부분을 차지하는 이유는 정상적인 사용자들이 접속하지 않고 단지 관리를 위한 SNMP 프로토콜에 의한 통신을 하고 있기 때문이다.



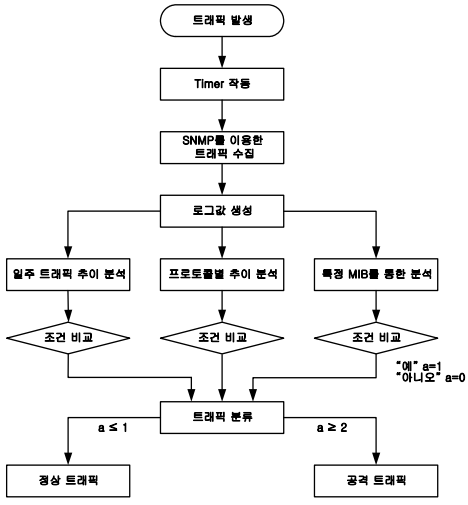
▶▶ 그림 3. 프로토콜별 트래픽 추이

2. 트래픽 분석 방법

본 논문에서의 트래픽 분석 방법은 미리 선정된 MIB 객체를 통해 1분 단위로 트래픽을 수집하고 수집된 정보를 일주 트래픽 추이 분석, 프로토콜별 추이 분석 그리고 특정 MIB 객체의 트래픽 발생 유무와 비교하여 유해 트래픽을 분류하게 된다. 본 논문에서의 분석 방법은 기존의 임계치를 이용한 방법과는 달리 각 분석 방법에서 이상 유무를 판단하게 되고, 기준과 상이한 트래픽이 발생시 이상 가중치를 부여하게 된다. 마지막에서 총 부여된 이상 가중치가 α보다 크게 되면 유해 트래픽으로 분류하게 된다. 이는 이상 트래픽 발생시 위의 세가지 분석 방법중 한 곳에서만 독자적으로 발생되지 않고, 두가지 이상의 분석 방법에서 이상 트래픽을 감지하게 되기 때문이다.

3. 트래픽 분석 알고리즘

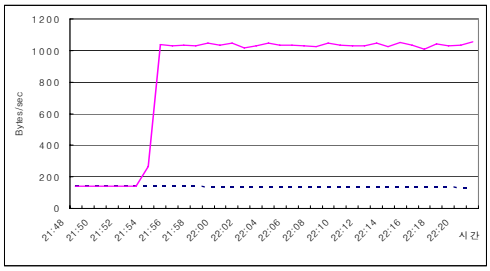
분석 알고리즘은 이상 트래픽 발생시 분석 방법에서 독자적으로 발생되지 않고 두 가지 이상의 분석 방법에 의해 분류될 수 있다는 특징을 이용하여 분석하게 된다. 사용된 알고리즘은 그림 4와 같다. 그림에서 보는 바와 같이 관리 대상 시스템으로 트래픽이 발생시 일분 단위로 트래픽을 수집하게 된다. 수집되는 대상은 미리 선정된 각 MIB 객체를 통해 수집되어 진다.수집된 정보는 일주 트래픽 추이 분석, 프로토콜별 추이 분석 그리고 특정 MIB 객체를 통한 분석 방법을 통해서 유해 트래픽 유무를 검사하게 된다. 만약 이 분석에서 이상 트래픽이 발생될 경우 가중치를 1을 부여하게 되며, 최종적으로 가중치의 합이 2 이상일 경우 유해 트래픽으로 분류하게 된다.



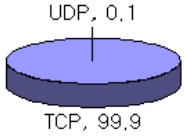
▶▶ 그림 4. 트래픽 분석 알고리즘

Ⅳ. 실험 및 결과

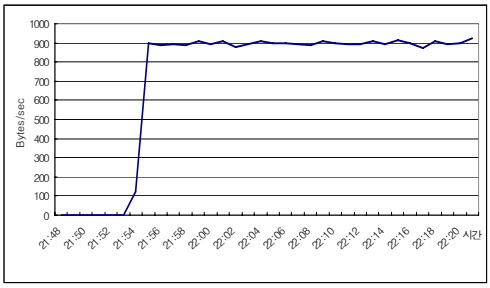
본 논문에서 제안한 알고리즘을 실험하기 위해 사용된 공격 툴로는 Trin00, TFN을 사용하였다. 그림 5는 공격이 발생되었을 경우의 트래픽의 발생을 트래픽 추이 분석 기준량과 비교한 것이다.



▶▶ 그림 5. 일주 트래픽 기준량과 비교



▶▶ 그림 6. 프로토콜별 트래픽 기준량과 비교



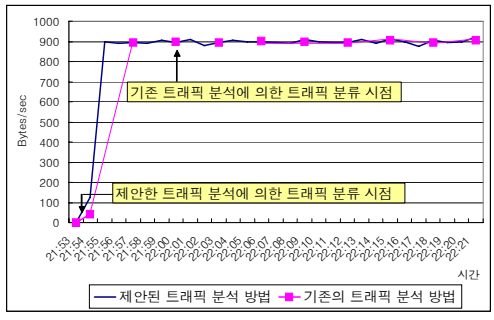
▶▶ 그림 7. 특정 MIB 객체에서의 트래픽 발생 유무

그림 5에서 보는 바와 같이 현재 입력되는 트래픽의 양이 일주 트래픽 기준량과 비교하여 크게 발생되고 있는 것을 확인할 수 있다. 또한 tcpInErrs에서 트래픽이 발생되고 있는 것을 그림 7을 통해 알 수 있다. 현재 일주 트래픽 추이 분석과 특정 MIB의 트래픽 발생 분석에서 이상 트래픽이 발생되고 있음을 확인할 수 있으며 이로 인해 이상 가중치는 2가 된다. 즉, 현재 발생되고 있는 트래픽중 tcpInErrs에서 발생되고 있는 트래픽이 유해 트래픽임을 분류해 낼 수 있다. 기존 방법과의 비교는 표 3과 같다.

[표 3] 기존방법과 제안된 방법과의 비교

트래픽 분류 방법	탐지하는데 걸린 시간(분)
기존의 방법	7
제안된 방법	1

표에서 보는 바와 같이 제안된 방법에서는 임계치를 적용한 기존의 방법과 달리 유해 트래픽이 발생되는 시점부터 트래픽을 분류해 낼 수 있었다. 하지만 기존의 방법에서는 임계치로 인해 비교할 수 있는 시간까지 유해 트래픽을 분류해내지 못했다. 그림 8은 제안된 방법과 기존의 방법에서의 유해 트래픽을 분류해 내는 시점을 그래프로 비교한 것이다.



▶▶ 그림 8. 기존방법과의 비교

V. 결 론

본 논문에서는 유해 트래픽을 분석함에 있어 시간상의 단축과 정확한 분류를 위해 일주 트래픽 분석, 프로토콜별 추이 분석 그리고 특정 MIB 객체에 의한 분석 방법을 중첩하여 사용하였다. 실험 결과값을 통해 시간상 단축된 사실을 확인하였으며, 무엇보다 기존의 방법에서 분류해내지 못했던 유해 트래픽을 정확하게 분류해 낼 수 있었다. 향후 과제로 트래픽 추이 분석에 있어 지속적인 업데이트를 통한 신뢰성 향상과 서비스 포트별 추이 분석을 포함한다면 더욱더 정확하고 신뢰성있는 트래픽 분석이 가능할 것이라고 생각된다.

▌참고문헌▐

[1] 박한상, 유대성, 오창석, "SNMPGET을 이용한 DDoS 공격 탐지", 한국콘텐츠학회 2004 춘계 종합학술대회, (pp.278-282), 2004.

[2] 김선영, 박원주, 유대성, 서동일, 오창석, "SNMP를 이용한 트래픽 폭주 공격 검출", 한국콘텐츠학회 논문지, 제3권 4호, (pp. 48-54), 2003.

[3] 이종엽, 윤미선, 이훈, "DoS 공격의 유형 분석 및 탐지 방법", 창원대학교, 2004.

[4] RFC 1271, "Remote Network Monitoring Management Information Base", S.Waldbusser, Febraury 1993

[5] 트래픽 추이분석 기반의 조기예경보시스템, http://www.securitymap.co.kr