DDos 공격에서 효율적인 트래픽 분석

Effective traffic analysis in DDos attack

구향옥*, 백순화**, 오창석*
충북대학교*, 백석대학**

Koo hyang-ohk*, Baek sung-hwa**,
Oh chang-suk*
Chungbuk Univ.*, Baeksuk Univ.**,

요약

최근 해킹공격은 네트워크의 트래픽 폭주공격인 DDos공격이나 웜해킹으로 공격 트래픽을 추출하는 기술이 미흡한 상태이다. 본 논문에서는 SNMP를 이용하여 트래픽을 수집하여 정상으로 간주되는 트래픽이 발생 했을 때 경우, 트래픽 분석 유예 타이머 구동하여 트래픽부하를 줄여 처리효율을 높이고자 한다.

Abstract

Recently most of hacking attack are either DDos attack or worm attack. However detection algorithms against those attacks are insufficient. In this paper, we propose a method which is able to detect attack traffic very efficiently by reducing traffic overhead. In this scheme, network traffics are collected using SNMP and classified. if they are identified as normal traffic, traffic analysis delay timer is started to reduce traffic overhead.

I. 서 론

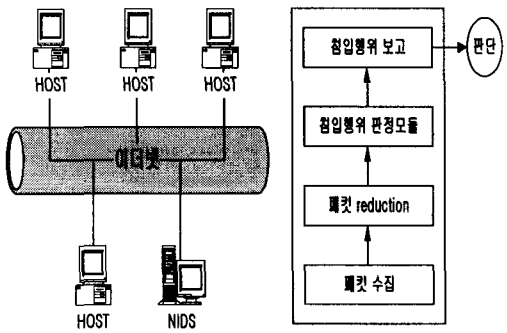
최근 정보 공유 마인드의 확산과 더불어 인터넷 및 네트워크의 사용이 급격이 증가하고 있다. 이러한 변화는 사용자에게 많은 편리성을 제공하기도 하지만 해커로 인한 트래픽 폭주 공격의 대상이 되기도 한다. 이전의 트래픽 폭주 공격은 DDos을 이용한 방법이 주류였지만, 최근 들어서는 웜을 이용한 트래픽 폭주 공격이 등장하였고, 이로 인해 피해 사례도 증가하고 있다. 웜에 의한 사례는 기업, 연구소, 국가 기관 등 다양한 분야로 확대되고 있다. 이러한 피해로 인해 많은 국가에서 대학교, 연구소를 중심으로 피해를 줄이기 위한 연구가 진행중에 있으나 아직도 트래픽 폭주 공격에 대한 분석 및 대응에 관한 연구는 미흡하다. 기존의 트래픽 폭주 공격에 대한 탐지는 방법은 대부분이 침입 탐지 시스템을 이용한 탐지였다. 침입 탐지를 이용한 방법은 트래픽 폭주 공격을 탐지하기 위해 네트워크상의 모든 패킷을 캡쳐하여 패킷 헤더 정보를 분석함으로써 많은 시스템의 부하와 정확한 트래픽 폭주 공격을 탐지 할 수 없었다. 따라서 본문에서는 이러한 문제를 해결하고 정확한 트래픽 탐지를 위해 SNMP를 사용하여 트래픽을 수집하고 공격으로 간주되는 트래픽이 발생 했을때의 분석시간 차이를 두어 정상트래픽일 경우 트래픽분석의 유예시간을 두어 트래픽분석의 처리효율을 높였다.

II. 관련연구

1. 트래픽 폭주 공격 정보 수집 및 분석의 개요

가. 침입탐지시스템에서 트래픽 정보 수집

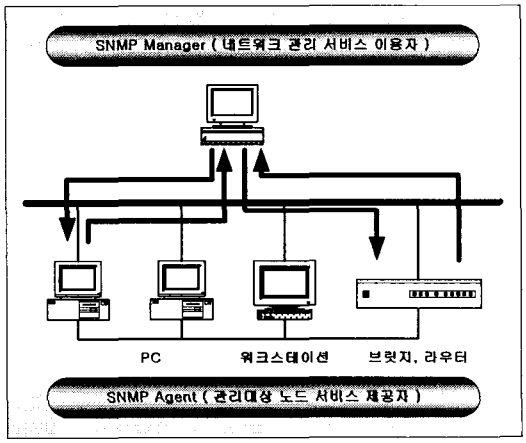
침입탐지시스템에 있어서 네트워크 트래픽의 모니터링과 수집된 패킷들을 분석하는 방법은 실시간 침입탐지에 있어서 아주 중요한 부분이다. 침입탐지시스템에서의 패킷의 수집과 분석은 주로 이더넷과 클라이언트/서버 시스템 모델이며, promiscuous mode로 동작하는 이더넷 네트워크 카드가 장착되어 있으므로 패킷 분석 도구를 탑재한 시스템에서는 패킷의 내용과 패킷의 헤더필드를 이용하여 모든 네트워크 트래픽을 분석할 수 있다. 이러한 특성을 이용하여 IP spoofing, packet floods와 같은 특별한 유형의 네트워크 공격을 찾아낼 수 있으며, 여러 가지 알림 기능이나 네트워크 세션을 단절시키는 방법을 이용하여 이러한 문제에 대처할 수 있다. 그림 1은 침입탐지시스템에서의 트래픽 정보 수집의 예를 보여주고 있다.



▶▶ 그림 1. 침입탐지시스템에서의 트래픽 정보 수집

나. NMS를 이용한 네트워크 모니터링

NMS(Network Management Service)를 이용한 네트워크 모니터링을 위해 주로 사용되는 프로토콜은 SNMP(Simple Network Management Protocol)이 있다. NMS에서는 바로 SNMP프로토콜을 이용하여 네트워크의 상황을 모니터링 하게 된다. SNMP를 이용하게되면 시스템 정보, 네트워크 트래픽, 고장관리, 성능관리, 구성관리에 대한 정보를 제공받을 수 있다. 이런 SNMP에는 여러 가지 객체가 있어 원하는 객체의 값을 불러와 트래픽 정보를 분석하게 된다. SNMP을 비롯한 대부분의 네트워크 관리 시스템에서의 가장 중요한 요소는 측정된 네트워크의 정보에 기초를 두고 구축된 데이터베이스이다. 구축된 데이터베이스를 바탕으로 질의를 사용하여 필요한 정보를 추출하고, 분석함으로써 효율적인 네트워크 관리를 구현할 수 있다. NMS를 이용한 네트워크 트래픽 수집 구조는 그림 2과 같다.

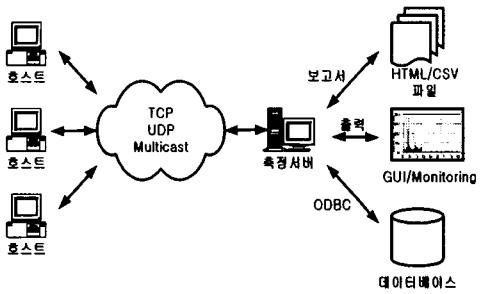


▶▶ 그림 2. NMS를 이용한 트래픽 수집 구조

다. 네트워크 트래픽 폭주 공격을 위한 정보 수집

트래픽 폭주 공격은 네트워크에 수많은 트래픽을 유발시켜 네트워크 자원을 고갈시키거나 종단 호스트의 기능을 마비시켜서 정상적인 서비스를 하지 못하도록 하는 공격 방법이다. 이에 대표적인 공격으로는 DDoS 공격과 웜 해킹 등이 있다. 트래픽 폭주 공격으로부터 네트워크 자원과 시스템을 보호하기 위한 방법들 중 하나의 방법이 네트워크에 흐르는 트래픽의 정보를 수집하고 분석하여 트래픽 폭주 공격에 대응하는 방법이다. 본 논문은 트래픽 폭주 공격을 대응하기 위한 방법에서 가장 중요한 트래픽의 정보 수집과 분석에 대한 연구를 하게 되었다. 그림 3은 네트워크 트래픽 폭주 공격에 대한 트래픽 정보 수집의

예를 보여주고 있다.



▶▶ 그림 3. 네트워크 트래픽 폭주 공격에 대한 트래픽 정보 수집

지금까지 현실적인 제안사항과 다양해지는 공격들의 침입을 정확하게 탐지하는 알고리즘은 아직 개발되지 못하는 실정이다. 기존의 침입 탐지 시스템을 이용한 트래픽 폭주 공격의 탐지는 폭주 공격이 이루어졌을 경우 침입 탐지시스템은 네트워크 상의 모든 패킷을 수집하기 때문에 시스템에 많은 과부하가 생성된다. 그러므로 정확한 트래픽 폭주 공격을 탐지하기 어려울 뿐만 아니라 침입 탐지 시스템은 기존에 분석된 공격에 한하여 탐지가 가능하므로 새로운 트래픽 폭주 공격이 이루어졌을 경우에는 탐지해내지 못하는 문제점을 가지고 있다. 이러한 문제를 해결하기 위하여 기존의 pcap 함수를 사용하는 방법에서 많은 응용 연구가 진행중에 있으나 아직 미흡한 실정이다. 최근 들어 SNMP를 이용한 네트워크 모니터링 기술이 확산됨에 많은 연구소에서 SNMP를 트래픽 폭주 공격과 연관하여 분석 중에 있으나 아직 미흡한 실정이다. 본 연구에서는 이러한 SNMP를 이용하여 여 패킷을 수집하여 네트워크를 관리하는 것이 아닌 SNMP의 MIB 객체를 분석하여 트래픽 폭주 공격 시 나타나는 특징을 검출하고 분석하여 이러한 문제점들을 해결하였다. 따라서 본 연구 과제에서는 앞에서 제시된 문제점들을 해결하고 좀 더 정확하고 효율적인 트래픽 폭주 공격을 검출하기 위해 SNMP를 이용한 트래픽 분석 알고리즘을 제안하고 구현하였다.

III. SNMP를 이용한 공격 트래픽 탐지

1. SNMP MIB를 이용한 공격 검출

트래픽 분석을 위해서는 기본적으로 에이전트와 매니저 시스템에서 SNMP 데몬이 실행되어야 한다. 그리고 모니터링 하고자 하는 시스템의 SNMP 데몬이 실행되어 있어야 하며 모니터링 하고자 하는 시스템의 SNMP를 이용하여 해당 시스템의 MIB 객체를 snmpget을 통해 가져와서 분석한다.

SNMP의 MIB는 시스템 정보, 네트워크 관리 정보 등 많은 기능을 제공하나 본 연구에서는 트래픽 폭주 공격을 검출하기 위해 실험을 통해 프로토콜별로 아래 표의 MIB 객체를 이용하여 트래픽을 분석 알고리즘을 도출하였다.

[표 1] 제안된 알고리즘에 사용된 MIB 객체

프로토콜	MIB객체	설명
TCP	tcpInSegs	오류로 수신된 세그먼트의 총 갯수
UDP	udpNoPorts	목적지 포트에 응용 프로그램이 없는 경우, 수신된 UDP 데이터그램의 총 갯수
ICMP	icmpInEchos	수신된 ICMP 요청 메시지의 갯수

표1은 IP 프로토콜의 ipInReceives 객체가 인터페이스로부터 수신된 입력 데이터그램의 총 개수로 오류로 수신된 것도 포함하는 상황에서 실험을 통해 공격으로 간주되는 객체를 찾아 본 논문에서 파라미터로 이용되고 있다.

2. 공격 검출 알고리즘

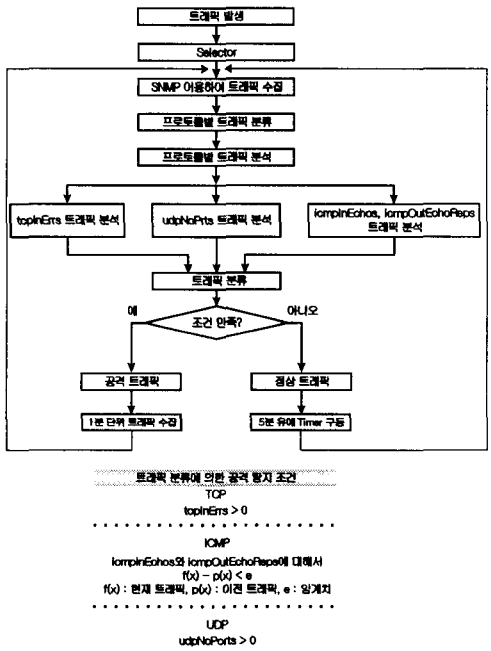
IP 데이터그램으로 수신한 트래픽을 해당 프로토콜별로 트래픽을 분해하여 처리한 후 각 서비스에 대한 정상 유무를 판별하게 된다.

TCP의 경우 쓰리웨이 핸드쉐이킹을 하지 않고 패킷을 전송하므로 tcpInErrs에 트래픽이 발생되고,

tcpInErrs에 5초 이상의 동일양의 패킷이 계속 유지된 다면 이것은 공격으로 탐지한다. UDP의 경우도 포트번호가 없는 것을 공격으로 탐지하고, ICMP는 공격 트래픽인 경우 크기가 일정하다는 특성을 근사 다항식에 적용시켜서 탐지한다. icmpInechos의 근사 다항식에 적용시켜 임계치 안에서 트래픽이 발생된 경우 공격으로 탐지하게 된다. 사용된 임계치는 실험에 의해서 얻어진 결과로 평균값은 1이고 알고리즘에 적용된 근사 다항식은 다음과 같다.

$$f(x) - p(x) = e \quad (1)$$

식1에서 f(x)는 실험에 의해 얻어진 트래픽 다항식이며, p(x)는 공격 트래픽 다항식이고, e는 임계값을 나타낸다.

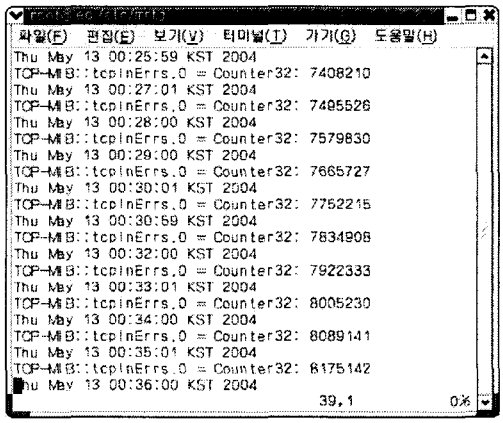


▶▶ 그림 4. SNMP를 이용한 트래픽 수집 및 분석 알고리즘

그림 4은 알고리즘은 각 프로토콜 별로 1분 단위로 트래픽을 수집하여 분석한다. 1분의 차이로 이전상태와의 값을 비교하여 정상적이라면 5분의 유예 타이머를 구동하여 트래픽의 분석 부하를 줄인다.

IV. 실험 및 결과

본 논문에서 제안한 알고리즘을 수행하기 위하여 Tfn의 공격 툴을 사용하였으며, ftp 사용으로 인해 발생되는 트래픽 폭주와 tcp의 flooding 공격에 의해 발생되는 트래픽을 공격과 비공격으로 구분하여 1분 단위로 분석 후 정상일 경우 트래픽 수집의 5분 유예 타이머를 구동하여 수집의 빈도를 줄여 처리 부하를 줄였다. 이때 수집분석에서 공격이 유예상태 시작 1분 뒤 바로 발생하였을 경우 5분의 유예시간이 있어도 다음의 6분의 시간에서 트래픽 수집분석이 이루어지기 때문에 최근에 발생되는 공격들의 소요시간 7~8분 보다 작은 6분에 공격을 감지할 수 있다.



▶▶ 그림 5. 1분 단위 트래픽(tcpInErrs의 로그값)

그림 5는 snmpget으로 트래픽의 누적치를 수집하여 1분 단위의 트래픽 분석을 수행하는 것으로 N-1 상태의 로그값의 트래픽양과 N상태의 차이가 분석알고리즘의 임계치보다 작으면 공격으로 간주하여 처리하고 임계치보다 크거나 같으면 정상트래픽으로 간주하여 5분의 타이머를 구동하여 트래픽 수집 유예시간 후 다시 트래픽 수집, 분석 절차를 반복한다.

제안한 1분 단위의 트래픽측정방법에서 최악의 경우는 첫 1분 동안 트래픽 수집 분석 후 바로 공격이 들어온 경우, 5분의 유예시간 후 다시 재개된 분석으로 6분의 시점에서 공격이 진행되고 있음을 감지한다고 하더라도 현재의 일반적인 폭주공격이 7~8분 정도 소요되므로 공격을 검출할 수 있다. 따라서 5분 유예기간 중 공격이 있더라도 이후로 바로 공격을 검출하여 침입을 보안 할 수 있다.

위의 최악의 검출도 유예시간 후 바로 6분의 시간에서 검출 가능하므로 알고리즘은 높은 검출률을 갖으며, 향후 해킹기법의 발달로 침입시간이 평균 5분 이내로 감소할 경우에도 유예시간을 줄여 공격검출이 가능하다.

V. 결론 및 향후과제

본 논문은 대부분의 네트워크의 모든 패킷을 캡쳐하여 트래픽을 분석하는 침입탐지시스템의 과부하를 줄이기 위해 트래픽 폭주 공격에 대비 SNMP의 snmpget를 1분 단위로 트래픽을 수집하여 공격이 없으면 패킷분석 5분의 유예시간을 두어 처리하였다. 이로써 과부하감소는 물론 폭주 공격에 대해 빠른 대처를 할 수 있었으며, 웜 해킹에 대해서 트래픽 특성을 분석하여 본 알고리즘을 적용시킨다면 트래픽폭주 공격에 대해 포괄적으로 대응할 수 있을 것이다.

▌참고문헌▐

[1] 김선영, 유대성, 원승영, 김근영, 신현준, "트래픽 폭주 공격 유형 분석 및 대응 방법 연구", 충북대학교, 2003.
[2] 오창석, 데이터통신(수정판), 영한출판사, 2001.
[3] J. S. Baras, A. A. Cardenas, V. Ramezani, "ON-LINE DETECTION OF DISTRIBUTED ATTACKS FROM SPACE-TIME NETWORK FLOW PATTERNS", Uiversity of Maryland, 2003
[4] E. Lemonnier, "Protocol Anomaly Detection in Network-based IDSs", Defcom, 2001
[5] F. Baker, K. Chan, A. Smith, "Management Information Base for the Differentiated Services Architecture", RFC3289, 2002
[6] http://staff.washington.edu/dittrich/misc/ddos/
[7] http://net-snmp.sourceforge.net/
[8] http://www.cisco.com/