유해트래픽 분석 시스템 설계

Design of Harmful Traffic Analysis System

장문수, 구향옥, 오창석
충북대학교

Chang Moon-Soo, Koo Hyang-Ohk, Oh Chang-Suk
Chungbuk Univ.

요약

최근 정보통신의 급속한 발전으로 인터넷을 이루는 컴퓨터 및 네트워크 환경은 초유의 성장과 발전을 거듭했지만, 잠재적인 취약점을 많이 가지고 있다. 이러한 취약점을 이용한 웜 및 해킹으로 인한 피해는 날로 심각하다. 본 논문에서는 이런 문제점들을 해결하기 위하여 유해트래픽 분석시스템을 설계하여 새로운 공격에 대한 방어와 네트워크의 트래픽을 분석함으로써 침입 및 유해 정보 여부를 판단하여 실시간으로 대응한다.

Abstract

The rapid development of computing and network environment has brought about the potential vulnerability. Therefore the damage from this vulnerability like Worm, hacking increases continually. In order to resolve this problem, implement the analysis system for mischievous traffic for defending new types of attack and analyzing the traffic takes a real-time action against intrusion and harmful information packet.

I. 서 론

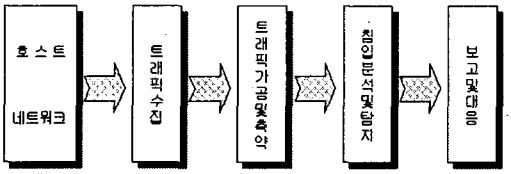
네트워크의 발달은 인터넷상에 접속된 컴퓨터가 데이터뿐만 아니라 음성, 영상 등의 멀티미디어 정보를 취급하도록 하였다. VoIP, 인터넷 방송 등으로 컴퓨터, 통신, 방송의 융합이 현실화 되고 있으며, 초유의 성장을 거듭하여 사이버 공간이 아닌 차세대 네트워크 컨버전스(NGcN), 광대역 통합망(BcN)을 통한 디지털 네트워크로 현실화되고 있다. 그러나 성장과 발전의 순기능이 존재하면 역기능이 존재하는 것처럼, 인터넷을 이루는 컴퓨터 및 네트워크 환경은 잠재적인 취약점을 내포하고 있다. 이러한 취약점을 이용하여 웜, 바이러스, 해킹 등의 악의적인 목적으로 유해트래픽 발생 및 공격으로 인한 업무장애, 불건전 정보 유통의 증가, 사생활 침해 등 정보화의 역기능이 폭발적으로 증가하여 크나큰 문제가 아닐 수 없다.

이에 본 논문에서는 이러한 네트워크 환경 변화와 문제점을 해결하기 위한 방법으로 네트워크의 트래픽을 분석하여, 침입 혹은 유해정보 여부를 판단하여 웜이나 DDoS와 같은 유해트래픽 흐름을 탐지하고 차단할 수 있는 기능을 구현하여 적용하였다. 이를 통해서 기존 방법의 문제점을 보완할 수 있었으며 침입에 대한 탐지율과 방지율을 향상시켜 신뢰성 있는 트래픽 흐름을 유도할 수 있었다.

II. 기존의 트래픽 탐지

기존의 트래픽 탐지 방법에서는 트래픽을 수집하여 외부의 침입 위험으로부터 내부 네트워크를 보호하고 방화벽을 우회하는 공격이나 내·외부 네트워크로부터 위험을 사전에 탐지하는 시스템이다. 이때 트

래픽 축약이 제대로 이뤄지지 않아서 발생하는 문제와 오탐지에 의한 잦은 경보작동으로 관리자로 하여금 엄청난 불편을 초래하였다. 그림 1은 기존 시스템의 구성 요소를 나타낸다.



▶▶ 그림 1. 기존 시스템의 구성요소

또한 침입 탐지 모델을 기반으로 하기 때문에 오용탐지와 비정상 행위 탐지의 경우 false negative 오류를 줄일 수 있었다. 하지만, 정상행위 프로파일에 침입이 포함될 수 있으며 주기적인 행동프로파일의 갱신이 필요하게 되므로 실시간으로 발생되는 유해트래픽 패킷을 대상으로 시간대비 탐지율이 현저하게 낮은 것을 확인할 수 있었다.

[표 1] 침입 탐지 모델에 따른 침입탐지 방법

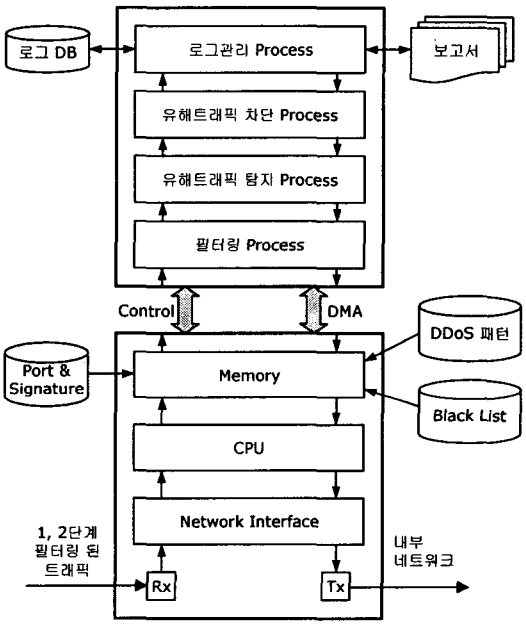
구분	침입탐지방법
오용탐지	조건부 확률
	전문가시스템
	상태전이 분석
	키입력 감시
	모델기반 침입탐지
비정상 행위탐지	통계적 접근
	특징 추출
	비정상행위 측정방법의 절차
	예측 가능한 패턴생성
	신경망

침입 탐지 모델에 따른 침입탐지 방법은 표 1과 같다.

III. 유해트래픽 분석을 통한 침입방지

1. 기본 개념

본 논문에서 제안한 유해트래픽 분석 시스템은 1단계로 라우터 보안을 통한 패킷 필터링을 거쳐 2단계로 네트워크 취약점을 점검하여 생성된 정보를 이용하며, BPF(Berkeley Packet Filter) 연산식을 적용, 규칙을 기반으로 필터링한다. 3단계로 취약점이 보완된 네트워크로 유입되는 트래픽을 대상으로 유해트래픽을 탐지하여 유해트래픽일 경우 drop 처리하고, 그렇지 않으면 forwarding 처리를 한다. 로그관리를 위하여 로그 테이블에 로그 정보를 저장하고, 보안관리자에게 보고서 작성의 용도로 활용된다.



▶▶ 그림 2. 제안 시스템 구성도

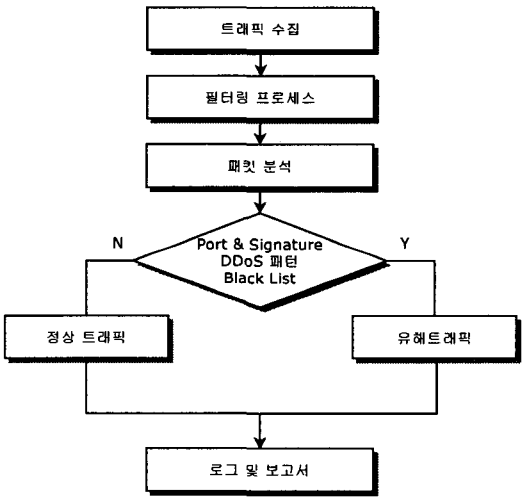
그림 2는 제안 시스템 구성을 나타내며 각각의 프로세스는 Thread로 구성되어 있으므로, 실시간으로 수집된 패킷을 바탕으로 유해트래픽 탐지 및 차단을 수행한다. 1단계와 2단계를 통해 필터링 된 트래픽을 대상으로 2단계에서 생성되고 지속적으로 갱신되는 취약성 데이터베이스와 비교 검색하여, 취약성 여부를 판단한다.

필터링 프로세스는 BPF(Berkeley Packet Filter) 연산식을 적용하여 필터링을 진행하며, 유해트래픽 탐지 프로세스는 필터링 된 트래픽을 기반으로 유해

성을 판단한다. 유해트래픽 차단 프로세스는 유해성 판단 여부에 따라 해당 패킷을 drop하거나 내부 네트워크로 forwarding 한다. 진행사항은 로그관리 프로세스에 의해 로그 데이터베이스에 축적되며, 향후 보고서 작성으로도 활용된다.

2. 트래픽 분석 방법

Ethernet 인터페이스에서 모든 트래픽을 볼 수 있도록 하는 "promiscuous mode" 기능을 설정하여 라우터로부터 유입되는 내부 네트워크를 지나는 모든 트래픽을 대상으로 트래픽 분석을 한다. 이때 엄청난 양의 트래픽 때문에 시스템에 과부하가 발생하게 되므로 BPF 연산식을 적용하여 필터링한다. 수집된 트래픽은 필터링이 완료된 후 2단계에서 취약점 점검으로 생성된 웜 관련 port 테이블, 시그너처 테이블, DDoS 패턴 테이블, 블랙리스트 테이블과 비교 검색된다.



▶▶ 그림 3. 트래픽 분석 방법

그림 3에서의 트래픽 분석 방법과 같이 정상트래픽일 경우에는 로그관리 프로세스를 통해 로그 데이터베이스에 로그 정보를 저장한 후 내부 네트워크로 forwarding 되며, 유해트래픽으로 판단될 경우에는 로그 데이터베이스에 로그 정보를 저장한 후 drop되어 내부 네트워크로의 진입을 허용하지 않는다.

3. 트래픽 테이블 관리

일반 트래픽 테이블은 Libpcap을 통하여 수집된 네트워크 패킷을 MySql과 연동하여 저장된다. 일반 트래픽 테이블의 구성은 TCP/IP 프로토콜에서 IP 헤더 구조 중 프로토콜, 출발지 주소, 목적지 주소를 참조하며, TCP/UDP 헤더 구조에서 출발지 포트, 목적지 포트 번호를 참조하였다.[1] 또한 수집된 패킷의 전체길이와 패킷의 프로토콜을 나타내는 타입정보와 수집된 시간 정보로 구성되어 있다. 표 2는 일반 트래픽 테이블이 스키마 구조를 나타낸다.

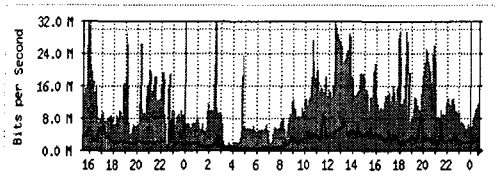
[표 2] 일반 트래픽 테이블의 스키마

필드이름	필드형식	내용
psize	smalint(5)	패킷의 전체길이
ptype	tinyint(3)	패킷이 프로토콜
sip	varchar(15)	출발지 주소
dip	varchar(15)	목적지 주소
sport	smalint(5)	출발지 포트번호
dport	smalint(5)	목적지 포트번호
logtime	datetime	패킷 수집 시간

트래픽 테이블에 수집된 트래픽 데이터는 웜 관련 port 테이블, 시그너처 테이블, DDoS 패턴 테이블, 블랙리스트 테이블과 비교 대상이 되며, 그림 2에서와 같이 필터링, 유해트래픽 탐지 및 차단하는 프로세스에서 활용된다.

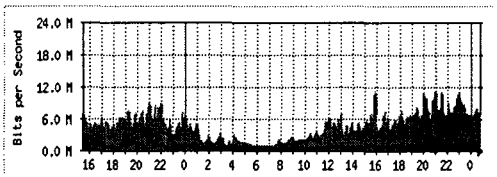
IV. 실험 및 결과

본 논문에서 제안한 알고리즘을 적용한 유해트래픽 분석 시스템을 실험하기 위하여 공격 도구로는 Trin00, TFN, 패킷 발생기를 사용하였다. 그림 4는 유해 트래픽을 발생하여 일반 트래픽과 함께 제안시스템을 통과하기 전의 트래픽을 모니터링 한 상황을 나타낸다.



▶▶ 그림 4. 기존시스템에서의 트래픽 모니터링

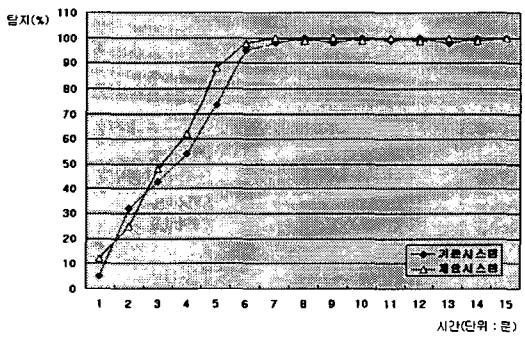
그림 5는 제안시스템인 유해트래픽분석 시스템을 통과한 후의 트래픽을 모니터링 한 상황을 나타낸다.



▶▶ 그림 5. 제안시스템에서의 트래픽 모니터링

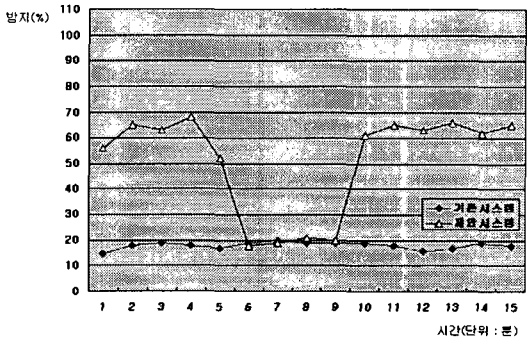
그림 5에서 보는 봐와 같이 유해트래픽이 현저하게 낮아졌음을 알 수 있다. 또한 네트워크가 안정적인 흐름으로 원활하게 서비스되고 있는 것도 파악할 수 있다.

기존시스템과 제안시스템의 유해트래픽 탐지율을 비교해 보면 그림 6과 같다. 제안시스템을 적용한 경우에는 81.93%의 탐지율이 발생했으며, 기존 시스템에서 발생된 76.66% 보다 5.27% 탐지율이 향상되었음을 알 수 있다.



▶▶ 그림 6. 기존방법과의 탐지율 비교

기존시스템과 제안시스템의 유해트래픽을 차단하는 방지율을 비교해 보면 그림 7과 같다. 제안시스템을 적용한 경우에는 50.93%의 성능을 나타냈으며, 이것은 기존시스템에서 발생된 18.06%보다 32.87%의 성능 향상을 가져왔다.



▶▶ 그림 7. 기존방법과의 방지율 비교

V. 결 론

본 논문에서는 일반트래픽을 대상으로 유해성 여부를 판단하는 유해트래픽 분석 시스템을 제안하여 웜이나 DDoS와 같은 유해트래픽 및 비정상 트래픽의 흐름을 탐지하고 차단하는 기능을 구현하였다. 실험결과를 통해 유해트래픽에 대한 탐지율이 높아졌다는 것을 확인하였으며, 무엇보다도 탐지된 유해트래픽을 차단하는 정도가 기존시스템에 비해 매우 높아졌다는 것을 확인할 수 있었다. 이것으로 유해트래픽으로부터 대응할 수 있는 네트워크 구성이 가능해졌으며, 보다 신뢰성 있고 안전한 네트워크 환경을 구성할 수 있었다. 향후 과제로 시스템 성능에 따른 유해트래픽 탐지와 방지가 어떻게 다른지에 대하여 연구가 이루어져야 할 것이다.

▌참 고 문 헌▐

[1] 오창석, 데이터 통신, 영한 출판사, 1999.
[2] W. Stevens, TCP/IP Illustrated Volume 1,2, Addision-Wesley, 1994
[3] Michael Rash, and Angela D., Intrusion Prevention And Active Response : Deploying Network and Host IPS, Oreilly & Associates Inc., 2005
[4] http://www.snort.org/