論文
6-5-4

웹 트래픽 추이 분석 기반 비정상행위 탐지 모델의 설계 및 구현 (A Design and Implementation of Anomaly Detection Model based the Web Traffic Trend Analysis)

장성민(Sung-Min Jang)[1] 박순동(Soon Dong Park)[2]

요 약

최근 들어 폐쇄 환경에서 동작하던 많은 주요 시스템들이 웹 서비스를 제공하면서 호스트는 물론 제공되는 웹기반의 서비스들이 쉽게 공격의 주요 대상이 되고 있다. 뿐만 아니라 웹 컨텐츠나 어플리케이션의 다양성은 새로운 공격 기술을 개발하는 원인이 되기도 한다. 반면 기존의 오용기반 탐지 기법으로는 공격 기술의 발전 속도를 따라가지 못할 뿐더러 새로운 보안 위협을 처리하는 능력이 없다. 따라서 기존의 공격 유형과 함께 새롭게 개발되는 공격과 침입을 탐지하고 대처할 수 있는 기술이 연구되고 개발되고 있다.

본 논문에서는 HTTP 트래픽 패턴과 패킷 정보를 분석하여 HTTP 트래픽 모델에서의 비정상행위 발생을 실험하였으며, 그 실험 결과를 적용하여 비정상행위를 탐지 가능한 HTTP 트래픽 모델을 설계하고 구현하였다.

<ABSTRACT>

Recently many important systems that used to be operated in a closed environment are now providing web services and these kinds of web-based services are often an easy and common target of attacks. In addition, the great variety of web content and applications cause the development of new various intrusion technologies, while the misuse-based intrusion detection technology cannot keep the peace with the attacks and it seems to lack the capability to deal with such various new security threats. As a result it is necessary to research and develop new types of detection technologies that can detect newly developed attacks and intrusions as well as to be able to deal with previous types of exploits.

In this paper, a HTTP traffic model is tested for its anomaly by using a HTTP request traffic pattern analysis and the field information analysis of the HTTP packet. Consequently, the HTTP traffic models by applying anomaly tests is designed and established.

Keywords : Anomaly detection, Misuse detection, False-Positive, False-Negative, Snort, Web traffic analysis, Intrusion detection system

논문접수 : 2005. 11. 15.
심사완료 : 2005. 12. 1.

1) 비회원 : 홍익대학교 과학기술연구소 연구원
2) 정회원 : 숭의여자대학 인터넷정보과 조교수

1. 서 론

인터넷의 급속한 보급과 다양한 응용으로 인하여 네트워크 트래픽은 급속하게 증가하고 있으며, 인터넷 웜을 비롯한 알려지지 않은 공격으로 인해 대량의 트래픽이 유발되고 있다. 또한 최근에는 스트리밍, P2P와 같은 새로운 응용에 의해서 새로운 대용량의 트래픽이 네트워크의 가용성을 위협하고 있는 실정이다. 인터넷 침해 사고로부터 피해를 최소화하기 위해서는 발생 가능한 보안 위협을 조기에 탐지하고 대응할 수 있어야 한다[2][5].

그러나 최근 들어 공격 패턴이 더욱 더 다양해지고 있으며, 알려지지 않은 새로운 공격의 출현으로 기존의 네트워크 방화벽이나 오용 탐지(Misuse Detection) 기반의 침입 탐지 시스템 기술로는 적절하게 감당하지 못할 상황에 이르고 있다.

특히 오용 탐지 기반의 침입 탐지 시스템은 오탐지(False-Positive) 및 미탐지(False-Negative) 등의 문제점과 지속적으로 탐지 규칙을 업데이트해야 하는 관리상의 문제점이 있으며, 고속의 네트워크 환경에서 트래픽이 폭주할 경우 침입 탐지에 한계를 드러내고 있다. 즉, 인터넷 해킹 기술이 기존의 정보보호 기술을 능가하게 됨으로써 문제의 심각성은 더욱 커지고 있는 상황이다[6].

오랫동안 폐쇄된 환경에서 외부와 접촉 없이 운영을 하던 중요 시스템들이 인터넷 환경으로 전환하는 시점에서 오프라인상의 위협뿐만 아니라 온라인상의 위협에도 노출되고 있다. 그러나 방화벽, 침입 탐지 시스템, 침입 방지 시스템, VPN 등의 보안 시스템의 노력에도 불구하고 외부와의 통신을 위한 메일과 웹 서비스는 해커들에게 노출되어 있다.

더욱이 모든 서비스가 웹 기반으로 변화되어 가는 최근의 추세에 웹 애플리케이션의 취약성에 대한 공격은 늘어나고 있다. 기존에 알려진 공격 기술 등이 어플리케이션 및 웹을 경유한 공격으로 발전함에 따라 기존의 네트워크에 중점을 둔 오용 탐지 기반의 침입 탐지 시스템들은 일반적으로 알려지지 않은 웹 공격에는 무력하다. 즉, 웹 컨텐츠와 어플리케이션의 다양함만큼이나 웹 공격의 방법은 무수히 많아질 수 있기 때문에 기존의 오용 탐지 기반의 침입 탐지 시스템으로는 성능 및 보안 측면에서 역부족이다[8].

본 논문에서는 웹 트래픽에 대한 정보를 수집, 분석하여 미리 준비된 정상 트래픽 패턴과 비교함으로써 비정상적인 트래픽의 파라미터 패턴 모델을 제안한다. 이를 바탕으로 Snort 모듈을 수정하여 웹 비정상행위 탐지 모델을 구현하고 실험하였다.

논문의 구성은 다음과 같다. 1장에서는 서론 및 연구 방향을 기술하고, 2장에서는 관련 연구, 3장에서는 웹 트래픽 추이 분석 기반의 웹 비정상행위 탐지 모델을 제안하고, 4장에서는 구현 및 실험 그리고 결과에 대한 분석을 한다. 마지막으로 5장에서는 결론 및 향후 과제에 대해 설명한다.

2. 관련 연구

2.1 네트워크 트래픽 분석

지난 2003년 1월 25일 발생한 슬래머 웜에 의한 인터넷 대란은 엄청난 웜의 전파 속도로 인해 불과 10분 만에 인터넷을 마비시킨 사건이다. 즉, 인터넷 웜 등의 공격으로 인한 네트워크의 성능 이상 현상을 관리자나 보안담당자가 인식하기까지 걸리는 시간은 10분 이내여야 한다.

그러나 기존의 네트워크 보안 기법의 경우 공격이 발생하면 사후에 해당 공격에 대한 특성을 분석하여 규칙을 생성하고 이를 기반으로 이후 공격에 대해 탐지를 한다. 이 경우 탐지의 범위 및 성능이 해당 공격의 규칙에 의존하므로 과다한 트래픽을 유발하는 등의 새로운 공격 방식이 출현하는 경우 이의 탐지와 적절한 대응이 어렵다.

따라서 네트워크 성능 저하를 가져올 수 있는 비정상적인 트래픽에 대한 상세 분석보다는 빠른 분석을 통해 우선적으로 트래픽의 비정상 가능성 정도를 판단하여 신속히 대응하고, 비정상 가능성이 높은 트래픽 부분만을 분리하여 상세 분석을 수행하는 것이 효율적이다. 일반적으로 네트워크 트래픽 분석은 네트워크 원시 트래픽 데이터의 수집, 네트워크 트래픽 데이터의 통합 및 단순화, 네트워크 트래픽 패턴 모델링, 비정상 네트워크 트래픽의 분석 및 감지의 기능을 갖는다[9].

네트워크 트래픽 데이터의 수집 방법 및 종류에는 SNMP MIB2 Interface 그룹, RMON I 그룹, RMON II 그룹, CISCO의 NetFlow, MeterMIB 등이 있다[8]. 네트워크 트래픽 수집 및 분석에 있어 고려할 사항은 단순한 트래픽 양이 아니라 어떤 네트워크 트래픽 특성에 대해 분석을 수행할 것인가를 먼저 정의한 후에 실제 데이터의 수집 방법 및 종류를 결정할 수 있다[12].

비정상 네트워크 트래픽을 판단하는 방법은 일반적인 침입 탐지 시스템에서의 경우와 마찬가지로, 첫째 알려진 공격에 대한 네트워크 트래픽 패턴을 기반으로 하여 해당 공격을 구성하는 트래픽을 분석 및 탐지하는 방법이 있다. 두 번째로 정상 상태의 트래픽 패턴을 모델링하고, 이를 바탕으로 이상 트래픽을 판별하는 방법이 있을 수 있다.

그러나 두 가지 방법 모두 대상 트래픽에 대한 네트워크 트래픽 모델링과 그에 따른 이상 트래픽의 분석 및 탐지 기능이 요구된다.

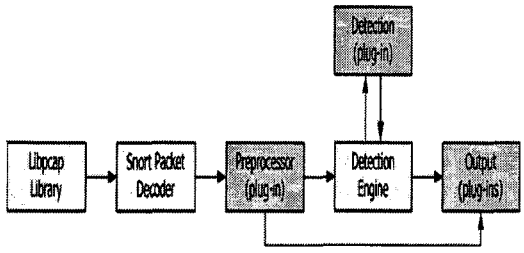
네트워크 트래픽 수집 분석 도구로는 웹 기반의 트래픽 모니터링 및 분석 어플리케이션인 Ntop을 비롯하여 tcpdump, Ethereal, FlowScan, CoralReef, PMA, IPMON, Snort 등이 있다.

2.2 Snort

snort는 네트워크에서 실시간 트래픽 분석과 패킷 로그를 뛰어나게 수행하는 행위 기반, 혹은 규칙 기반의 네트워크 침입 탐지 시스템(NIDS)이다. snort는 프로토콜 분석과 패킷의 내용 조사와 패턴매칭이 가능하며, 버퍼 오버플로우나 스텔스 포트스캔, CGI 공격, SMB 탐지, OS fingerprinting 시도 등 다양한 공격과 탐지를 발견하는데 사용할 수 있다.

또한 트래픽을 잡아내기 위해 유용한 모듈 플러그 인 구조를 가진 탐지 엔진과 같은 매우 유연한 규칙 언어를 사용한다. snort는 syslog, 사용자가 지정한 특정 파일, UNIX의 소켓이나 Sambaclient를 이용한 윈도우즈 팝업(popup) 메시지와 일체된 경고 기법 같은 실시간 경보가 가능하며, 주요 세 가지 기능은 다음과 같다[4][13].

첫째로 tcpdump와 같은 패킷 스니퍼(sniffer)로 바로 사용할 수 있다. 둘째로 네트워크 트래픽 디버깅에 유용한 패킷 로거 기능이 있다. 마지막으로 완벽한 네트워크 침입 탐지 시스템(NIDS) 기능을 가지고 있다. snort는 경량 침입 탐지 시스템으로 libpcap 라이브러리를 사용하여 현재 Linux, FreeBSD, NetBSD, OpenBSD, Windows 같은 x86 시스템 등 여러 플랫폼에서 동작한다[4][13].



[그림 2-1] snort의 구조

snort는 [그림 2-1]에서 보는 바와 같이 libpcap이라는 패킷 캡쳐 라이브러리를 사용하여 트래픽 패킷을 스니핑한다. 스니핑된 패킷은 디코더를 거치면서 snort에서 인식 가능한 형태로 가공이 된다. 이후 전처리기와 탐지 엔

진을 거치면서 미리 정의되어 있는 탐지 규칙과의 비교를 통해 침입을 탐지하게 된다.[13]

snort는 비교적 쉽게 구체적인 규칙을 사용자가 제작할 수 있으며, 여러 전처리기를 이용한 플러그인 형태의 동작 방식, 다양한 경고 및 로그 형태가 가능하다는 장점이 있다. 무엇보다 오픈 소스 형태로 개발되면서 최신의 공격에 적응이 빠르다는 점을 들 수 있다. 반면, 단순한 패턴 매칭으로 인해 공격 오탐지 가능성이 높으며, 새로운 공격에 대한 탐지는 불가능하다.

그렇지만 snort는 침입 공격 패턴 데이터베이스에 새로운 공격 패턴을 추가하거나 인터넷을 통하여 계속적으로 업데이트하고, 사용자는 새로운 네트워크 공격에 대한 공격 패턴을 생성하여 snort 침입탐지 패턴 메일링 리스트(http://www.snort.org/lists.html)로 제출함으로써 모든 snort 사용자들이 혜택을 함께 누리게 한다. 그런 이유로 snort는 가장 업데이트 잘 되고 강력한 네트워크 기반 침입 탐지 시스템 중 하나로 자리하고 있다[13][14].

2.3 비정상행위 탐지 기반의 침입 탐지 시스템

침입이란 자원의 기밀성, 무결성, 가용성을 훼손하는 제반 행위를 말한다[12]. 침입 탐지 시스템이란 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 규정하는 시스템으로 가능하면 실시간으로 처리하는 시스템, 또는 침입을 시도하거나, 침입행위가 일어나고 있거나, 침입이 발생한 것을 확인하는 절차이다. 침입 탐지 시스템의 본래의 의미는 침입을 탐지하는 것이지만, 현재의 상황을 고려한 침입 탐지 시스템의 의미를 재정의 하자면 탐지된 내용을 바탕으로 능동적인 대처까지 해주는 의미도 내포하고 있다[6][12]. 침입 탐지 시스템은 데이터베이스화한 해킹 기법을 기반으로 해커의 침입을 탐지하므로 신기술 적용이 빠르고, 외부뿐만 아니라 내부 사용자의 해킹도 차단할 수 있으며, 해킹 사실을 인지하면 즉시 그 내용을 관리자에게 알려줌으로써 시스템 보안을 유지할 수 있도록 해 줄 수 있다.

일반적으로 네트워크 기반 침입 탐지 시스템은 실시간으로 네트워크를 모니터링하고 사용자가 정의한 보안정책을 적용하여 불법적인 침입에 대응할 수 있지만, 실시간으로 패킷을 분석하기 위한 처리 능력과 저장의 한계를 극복해야 하고, 네트워크 트래픽 증가에 따른 별도의 하드웨어 및 소프트웨어가 필요하다. 반면 호스트 기반 침입 탐지 시스템은 별도의 하드웨어 없이 시스템을 감시할 수는 있지만, 서버마다 소프트웨어를 설치해야 하고, 서버의 리소스 부하를 증가시켜 성능 저하를 가져올 수 있는 단점이 있다[11].

현재 침입 탐지 시스템에 대한 많은 연구들이 비정상행위 탐지기술을 중심으로 이루어지고 있으나, 아직 많은 솔루션들은 단순한 오용(Misuse) 등의 비정상 행위들에 대한 탐지를 주로 사용하고 있다.

2.4 어플리케이션 기반 비정상행위 탐지 시스템

네트워크 프로토콜 분석 기반의 비정상행위 탐지는 주로 패킷의 헤더 검사에 초점이 맞추어져 있다. 반면에 어플리케이션 기반의 비정상행위 탐지는 어플리케이션 계층의 페이로드 같은 패킷의 확장 정보가 기본이 된다[10][11]. 예를 들면 DNS, HTTP, FTP, TELNET 등과 같은 서비스 대상 공격을 탐지하기 위해서는 페이로드 분석이 요구된다. 특정 서비스마다 페이로드 구조 및 트래픽 패턴이 다르기 때문에 서로 다른 서비스마다 서로 다른 정상 프로파일이 필요하다. 이전의 네트워크 계층 및 전송 계층의 비정상행위 탐지는 개별 서비스에 대한 공격의 탐지가 어렵다. 어플리케이션 기반의 비정상행위 탐지 기법은 서로 다른 서비스에 대한 공격의 탐지를 가능하게 하는 반면 각 서비스마다 정확한 행위 모델을 구성

하기 위해 서비스에 대한 충분한 지식이 요구된다[5][6][11].

3. 제안된 비정상 행위 탐지 모델

HTTP 탐지 모델은 <표 3-1>에서 보는 바와 같이 4가지로 구분한다. 크게 HTTP URI 필드에 관련되지 않은 출발지 주소, 메소드, 데이터 크기와 HTTP URI 필드내의 정보에 관련한 URI의 크기, URI 필드내의 파라미터 수, URI 필드내의 개별 파라미터 값의 크기로 나눌 수 있다.

대상	측정값	위험지표
출발지 주소	출발지 주소별 트래픽의 양	$A_{ip}(X)$
메소드	HTTP 메소드별 트래픽의 양	$A_m(X)$
데이터 크기	데이터 크기별 트래픽의 양	$A_{ds}(X)$
URI 파라미터의 길이	HTTP URI 개별 파라미터에 대한 길이별 트래픽의 양	$A_{up}(X)$

[표 3-1] HTTP 트래픽 탐지 모델과 위험 지표

위험 지표는 HTTP 탐지 모델에 대한 비정상 정도를 나타내는 측정값이다. 위험 지표는 해당 패킷을 수신할 확률에 대한 원시 비정상행위 값(Raw Anomaly Score)으로 계산되며 [식 3-1]과 같다.

$$a(X) = -1 * \log_2 (P(X)) \qquad [식\ 3\text{-}1]$$

a(X) : 탐지 모델의 원시 비정상행위 값
P(X) : 탐지 모델의 수신할 확률

예를 들어 특정 웹 서버에 대한 HTTP 트래픽 메소드 중에서 GET 명령 패킷이 도착한 확률이 90%이고, POST 명령 패킷은 5%라고 할 때, GET 명령 패킷에 비교하여 POST 명령 패킷이 일반적이지 않다는 것을 알 수 있다. 이를 [식 3-1]에 대입하여 계산하면 다음과 같다.

$$a(GET) = -\log_2(P(GET)) = -\log_2(0.9) = 0.152003$$
$$a(POST) = -\log_2(P(POST)) = -\log_2(0.05) = 4.321928$$

보는 바와 같이 원시 비정상행위 값이 작을수록 좀 더 일반적이라고 할 수 있다. 그러나 비교하기 쉽게 하기 위해서 [식 3-2]를 사용하여 상대 비정상행위 값(Relative Anomaly Score)을 구한다.

$$A(X) = a(X) / a_{max}(X) \qquad [식\ 3\text{-}2]$$

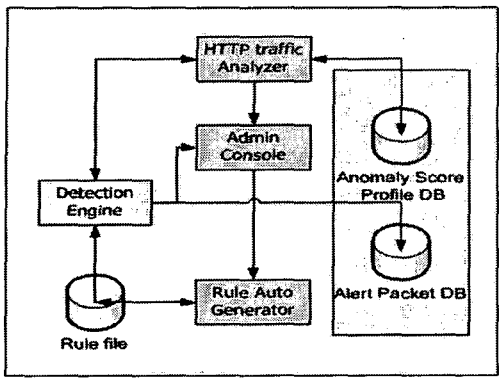
a(X) : 탐지 모델의 원시 비정상행위 값
$a_{max}(X)$: 탐지 모델의 최대 원시 비정상행위 값

상대 비정상행위 값은 0에서 1까지의 값을 갖게 되며 0에 근접할수록 정상적, 즉 일반적이라 할 수 있고 1에 근접할수록 일반적이지 않음을 의미한다.

HTTP 트래픽 패킷의 비정상 탐지를 위해서는 상대 비정상행위 값의 임계값(threshold)을 설정해야 한다. 임계값은 프로파일링 기간에 정상 HTTP 트래픽 탐지 모델의 상대 비정상행위 값에 따라 관리자가 설정할 수 있으며, 상황에 따라 변경할 수 있다.

4. 구현 및 실험

3장에서 제안한 웹 트래픽 탐지 모델 구현은 2.2절에서 설명한 snort의 패킷 탐지 엔진을 [그림 4-1]과 같은 구조로 수정하여 구현하였다. 일정기간 웹 서버의 프로파일을 기반으로 비정상 트래픽을 탐지하고 새로운 공격에 대응할 수 있도록 하였다.



[그림 4-1] Snort 탐지 엔진 수정 구조

4.1 HTTP 트래픽 분석기

탐지 엔진으로부터 제공받은 HTTP 트래픽 패킷을 파싱하여 탐지 데이터를 추출하고 분석하는 기능을 수행한다. HTTP 트래픽 분석기는 두 가지 운영모드를 가지고 동작한다.

첫째, 프로파일링 동작모드이다. 정해진 프로파일링 기간 동안에 snort 패킷 디코더를 통해 수집된 패킷 데이터로부터 웹 서버로 들어오는 HTTP 트래픽 패킷을 파싱하여 출발지 IP 주소, HTTP 메소드, 데이터 사이즈, URI 필드의 길이, URI 필드 내의 파라미터 수, URI 필드 내의 파라미터의 길이 등의 탐지 데이터를 추출한다.

이 때, 개별 탐지 데이터 별로 [식 3-1], [식 3-2]에 따라 원시 비정상행위 값 및 상대 비정상행위 값을 계산하게 된다. 계산된 비정상행위 값은 탐지 단계에서 비정상 HTTP 트래픽 탐지를 하기 위한 단위 시간동안의 트래픽 모델과의 비교, 분석을 위해 데이터베이스로 저장된다.

둘째, 탐지 모드이다. 탐지 모드에서는 프로파일링 기간에 정의된 정상 트래픽 모델과 단위 시간동안의 수집, 추이 분석을 통해 새로 생성된 트래픽 모델과의 비교, 분석을 통해 HTTP 트래픽의 비정상 여부를 평가한다. 먼저 [식 3-1]과 [식 3-2]와 같이 단위 시간 동안의 개별 탐지 데이터의 원시 비정상행위 값과 상대 비정상행위 값을 구한다. 계산된 비정상행위 값은 프로파일링 기간에 정의된 정상 트래픽 값과 비교를 통해 HTTP 트래픽의 비정상 여부를 평가하게 된다.

비정상 행위로 판단된 패킷은 데이터베이스에 저장되고, 관리자 콘솔로 출력하여 관리자가 프로파일을 갱신할 수 있도록 하거나 새로운 규칙을 생성, 추가할 수 있도록 한다.

4.2 관리자 콘솔

관리자 콘솔은 HTTP 트래픽 분석기와 규칙 자동 생성기와 통신하면서, 비정상행위 탐지 시스템의 실시간 상황과 주어진 시간별 비정상행위 트래픽을 관리자에게 보고하는 기능을 수행한다.

관리자는 정해진 네트워크 보안 정책에 따라 제공된 도구를 사용하여 트래픽의 프로파일 갱신, 새로운 탐지 규칙 생성 및 적용, 그리고 바이 패스를 수행할 수 있도록 한다.

4.3 규칙 자동 생성기

규칙 생성기는 HTTP 트래픽 분석기로부터 수신한 정보를 바탕으로 snort가 인식할 수 있는 형태의 탐지 규칙을 생성한다. 규칙 등록기는 새로 생성된 탐지 규칙을 등록한다. 또한 탐지 규칙의 제거를 담당한다. 규칙 헤더는 서명의 핵심 부분으로 규칙의 결과 행위, 프로토콜, 출발지와 목적지 정보(포트, IP 주소, 네트워크)를 포함한다.

규칙 본문에 있는 데이터는 규칙 헤더에 비해 비중이 작다. 규칙 헤더는 규칙 동작, 프로토콜, 출발지 정보, 목적지 정보를 가지고 있다. 출발지 정보와 목적지 정보를 구분하기 위해 방향 연산자(->)를 사용한다. 규칙 본문은 반드시 필요하지는 않지만 복잡한 공격을 파악하기 위해 꼭 필요하기 때문에 규칙 헤더만큼 중요하다. 규칙 본문은 세미콜론(;)으로 분리된

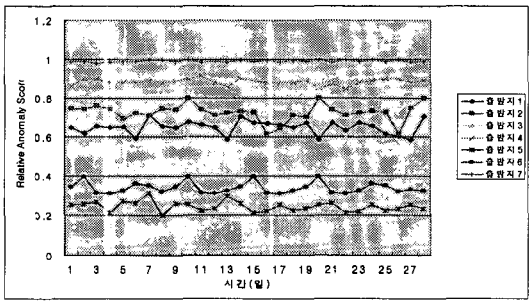
여러 부분으로 구성된다. 각 부분은 옵션과 옵션 값으로 구성된다[14].

4.4 프로파일 데이터베이스

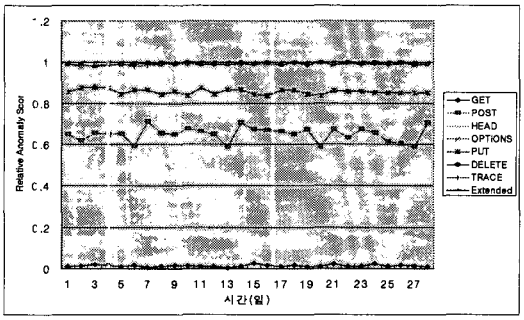
프로파일 데이터베이스는 날짜별, 시간별, 데이터 크기별, 그리고 파라미터 길이별로 상대 비정상행위 값을 저장하며, 각 날짜와 시간별로 연결 리스트를 구성하고 수신된 패킷과 비교한다.

4.5 실험

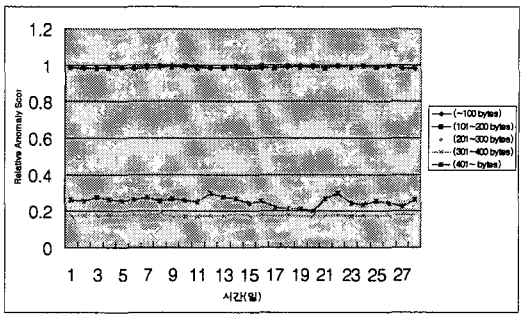
국내 S 대학의 웹서버 트래픽을 한 달 프로파일링 기간 동안 1시간마다 개별 HTTP 탐지 모델에 대하여 [식 3-1]과 [식 3-2]를 사용하여 상대 비정상행위 값을 구하였다.



[그림 4-2] 출발지 IP 주소별 상대 비정상행위 값



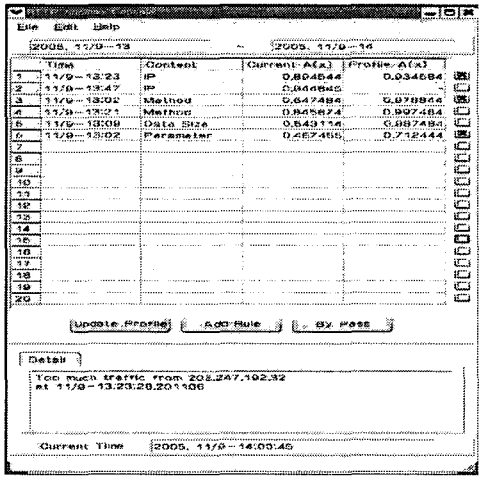
[그림 4-3] HTTP 메소드별 상대 비정상행위 값



[그림 4-4] 데이터 크기별 상대 비정상행위 값

결과는 [그림 4-2], [그림4-3], [그림 4-4]에서 알 수 있듯이, 일정한 패턴의 값을 보임을 알 수 있었다.

이러한 프로파일링 데이터를 이용하여 정상적인 트래픽 프로파일링 기간의 특정 날짜, 시간 HTTP 트래픽을 조작하여 비정상 트래픽에 대한 탐지 여부를 실험하였다. 프로파일 데이터와 다른 상대 비정상행위 값을 보이는 트래픽이 관리자 콘솔로 시간별로 보고됨을 볼 수 있었다. 또한 시간대별 프로파일링을 통하여 HTTP 탐지 모델의 미세한 변화에 대하여 쉽게 탐지할 수 있음을 보여주었다.



[그림 4-5] 관리자 콘솔

[그림 4-5]는 관리자 콘솔로 보고된 트래픽을 보여준다. 관리자는 탐지된 결과에 대하여 정해진 네트워크 정책을 기반으로 하여 프로파일링, 규칙 추가, 바이 패스의 세 가지 선택을 하게 된다. 첫째 프로파일링할 경우에는 해당 시간의 프로파일링 데이터베이스를 갱신하고 적용한다. 둘째, 규칙 추가는 snort 규칙 서명을 추가하여 지속적인 트래픽 관리를 할 수 있도록 한다. 셋째 바이 패스의 경우 해당 시간의 프로파일링에 관여치 않고 탐지 결과를 무시한다.

5. 결론 및 향후 연구 방향

본 논문에서는 웹 트래픽에 대한 정보를 수집, 분석하여 미리 준비된 정상 트래픽 패턴과 비교함으로써 현재 트래픽의 위험 상황을 평가하여 경보하고, 비정상적인 트래픽의 파라미터 패턴 모델을 제안하고 기존의 Snort를 수정하여 모델을 구현하고 실험하였다. 일정기간의 프로파일링 기간을 이용하여 비정상 행위를 탐지할 수 있음을 보였다. 이를 이용하여 새로운 공격을 미리 예측하고 탐지할 수 있도록 하였다. 향후에는 웹 트래픽에서 HTTP 요청 메시지, 즉 수신 트래픽만이 아닌 양방향 트래픽 모두에 대한 정상 트래픽 패턴 모델을 구축함으로써 탐지 대상 시스템의 침입 여부에 대한 연구가 필요하다. HTTP 패킷 중 URI 내용에 대한 정규화를 통한 일반적인 규칙의 생성도 고려해야 한다. 감시 서버에 대한 자가 점검 및 취약성 분석을 위해서 비정상행위 트래픽 패킷을 이용한 가상 공격을 통하여 탐지 규칙의 자동 생성 및 추가도 생각해 볼 수 있다.

참고문헌

[1] R. Fielding et al(1997), "Hypertext Transfer Protocol - HTTP/1.1", RFC 2068.

[2] Magus Almgren, Herve Debar, Marc Dacier(2000), "A Lightweight Tool for Detecting Web Server Attacks", In Proceedings of the ISOC Symposium on Network and Distributed Systems Security.

[3] Joseph L. Hellerstein, Fan Zhang, Perwez Shahabuddin(2001), "A statistical approach to predicteive detection", Computer Networks, pp.77-95.

[4] Raven Alder, etc. al.(2003), *Snort 2.1 Intrusion Detection,* Syngress Publishing, Inc.

[5] Christopher Kruegel, Giovanni Vigna, William Robertson(2005), "A multi-model approach to the detection of web-based attacks", Computer Networks: The International Journal of Computer and Telecommunications Networking, pp.717-738.

[6] C. Krugel, G. Vigna(2003), "Anomaly detection for Web-based attacks", Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS'03), ACM Press pp.251~261.

[7] C. Kruegel, T. Tuth, E. Kirda(2002), "Service specific anomaly detection for network intrusion detection", Proceedings of the Symposium on Applied Computing (SAC), ACM Press, pp.201-208.

[8] Fredrik Valeur, Darren Mutz and Giovanni Vigna(2005), "A learning-based approach to detection of SQL attacks", Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA).

[9] Matthew V. Mahoney, Philip K. Chan(2003), "Learning Rules for Anomaly Detection of Hostile Network Traffic," icdm, p. 601, Third IEEE International Conference on Data Mining (ICDM'03).

[10] Matthew V. Mahoney, Philip K Chan(2001), "PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic", Florida Institute of Technology Technical Report CS-2001-04.

[11] InSeon Yoo(2004), "Protocol Anomaly Detection and Verification", Proceeding of the IEEE, pp.30-37.

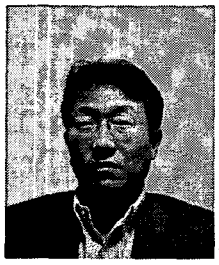
[12] G. Vigna, W. Robertson, V. Kher and Richard A. Kemmerer(2003), "A Stateful Intrusion Detection System for World-Wide Web Servers", Proceedings of the Annual Computer Security Applications Conference (ACSAC) pp. 34-43.

[13] M. Roesch(1999), "Snort - Lightweight Intrusion Detection for Networks", Proc. of the 13th USENIX Conference on System Admin, pp.229-238.

[14] Snort Home pages, " http://www.snort.org"

장성민(Sung-Min Jang)

1999. 2. : 홍익대학교 컴퓨터이학박사 수료
1993. 3.~ 2001. 2 : 퓨처시스템 정보통신 연구소 근무
관심분야 : Mobile IPv6, VPN, Internet Security



박순동(Soon-dong Park)
1993년 2월 : 홍익대학교 컴퓨터 이학박사 수료
1996년 ~ 현재 : 숭의여자대학교수
관심분야 : 컴파일러, 컴퓨터 보안, 위성통신